In Part 1 we did the following things:

1. Created a VPC A
2. Created four subnets(two Public subnet and two Private subnets) in VPC A in two availability zones i.e us-west-1a and us-west-1b.
3. Created a NaCL and associated all the Subnets to the NaCL
4. Created inbound and outbound rule with Rule number 100 and to allow all traffic from internet

Part 2:

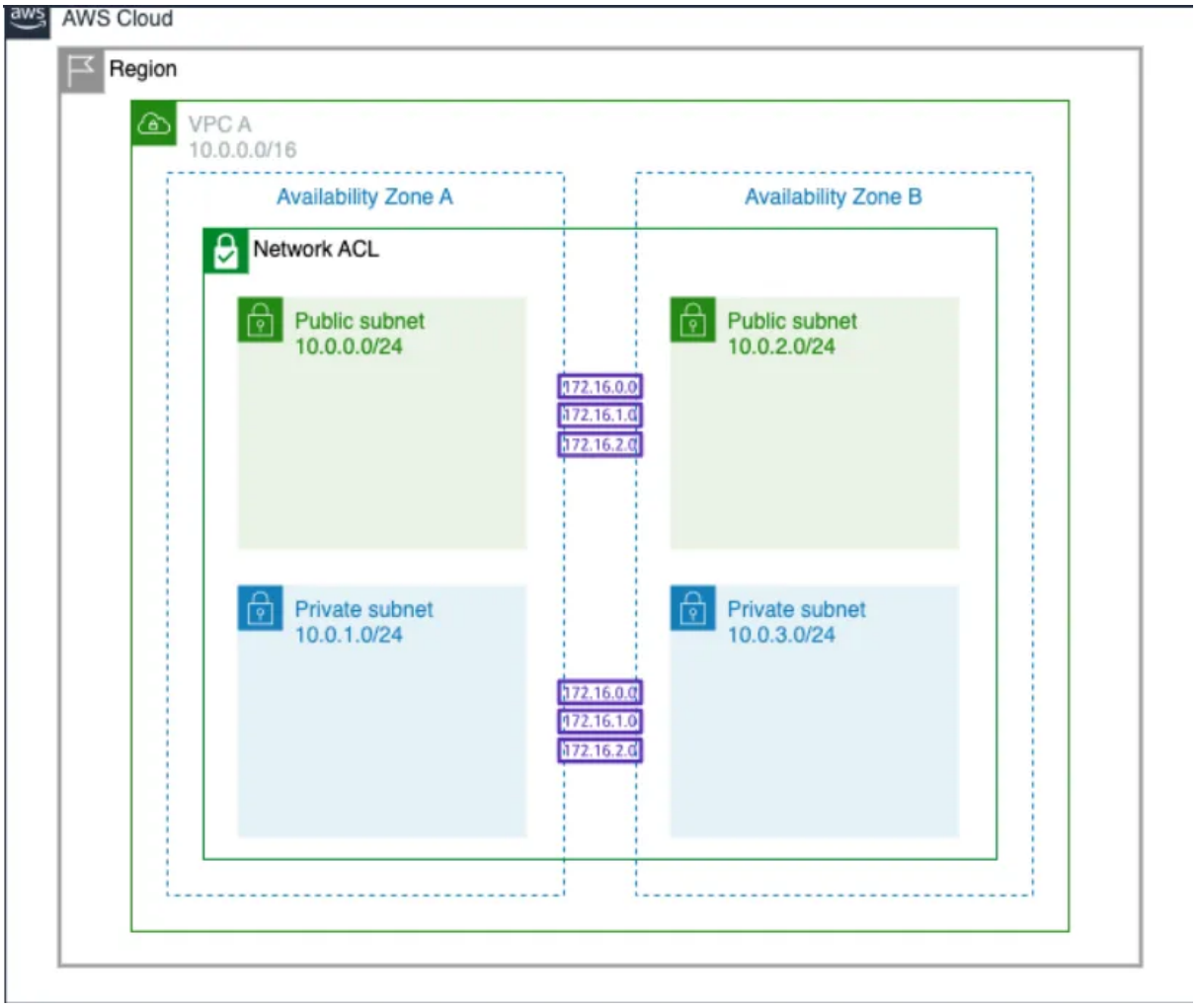
Route Tables:

There is an implicit router in the VPC you have created and route tables is used to control the network traffic.

A *route table* contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can

explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.



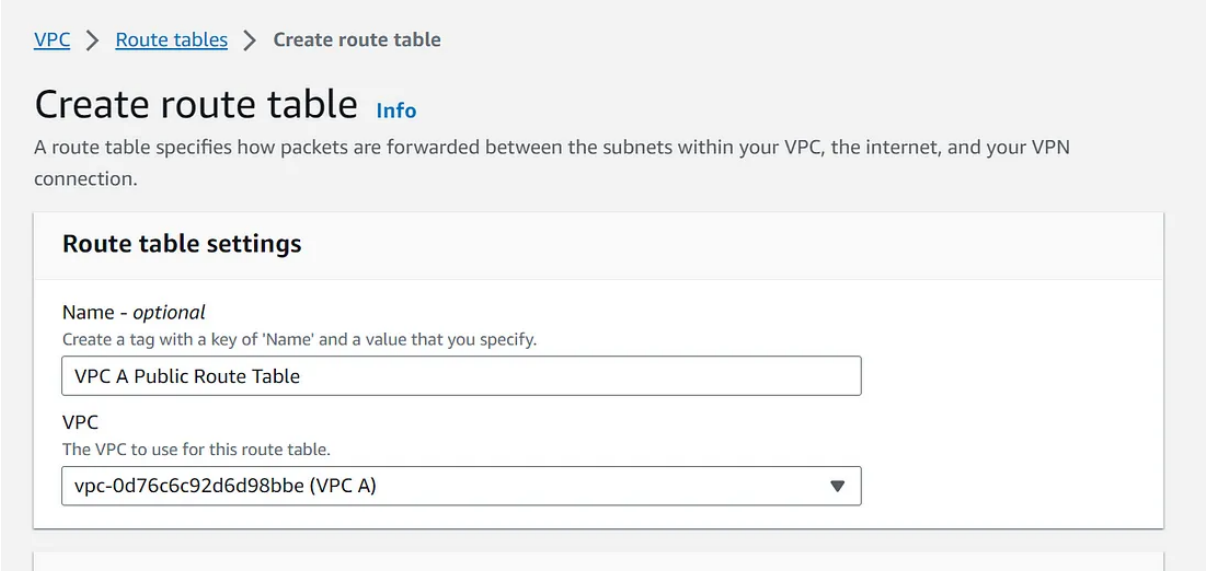
Create Route table for Subnets:

We will now create a new public route table for the public subnets with a route to the internet via the Internet Gateway.

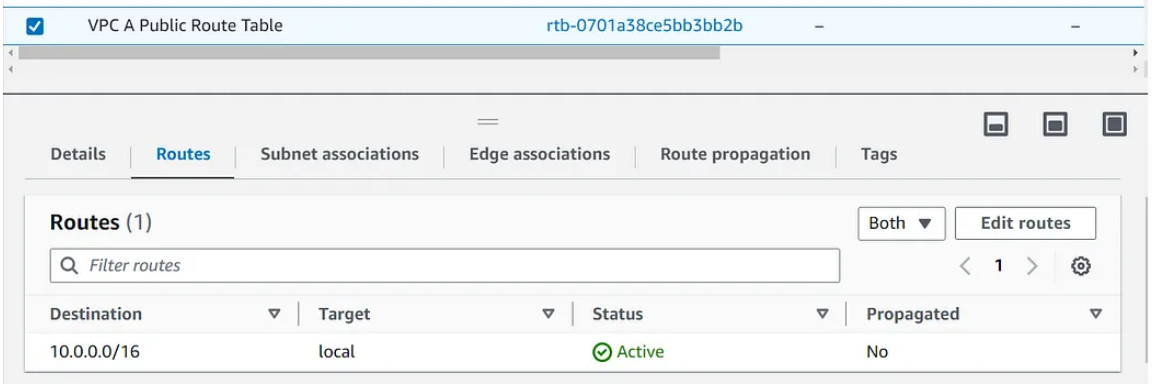
1. Click on Create route table
2. Enter Name as VPC A Public Route Table

3. Select VPC A

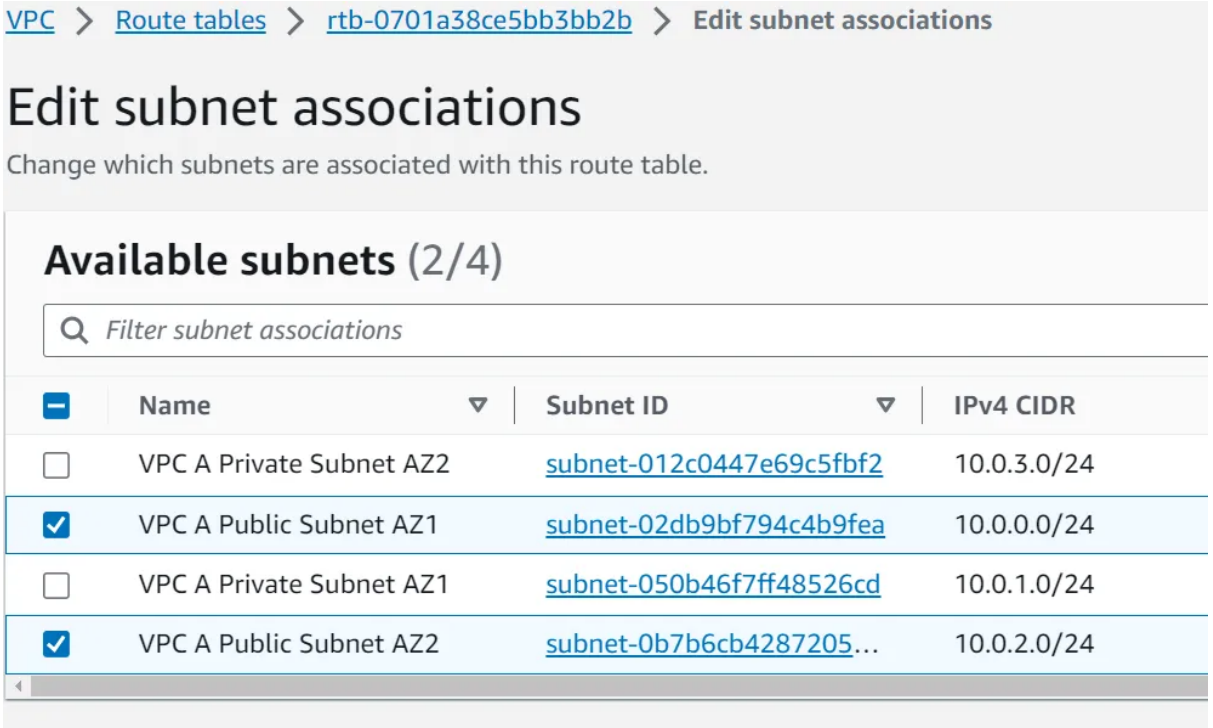
4. 4. Create route table



After the creation of route table we have to select the newly created route table and we can see we can there is only a local route, so we're going to enable internet access by adding a route to an Internet Gateway in a coming step.



5. Select VPC A Public Subnet AZ1 and VPC A Public Subnet AZ2 and click Save association



6. The two public subnets will now be associated with the public route table under Explicit Subnet Associations within the Subnet associations tab.

Create Route Table for Private Subnets:

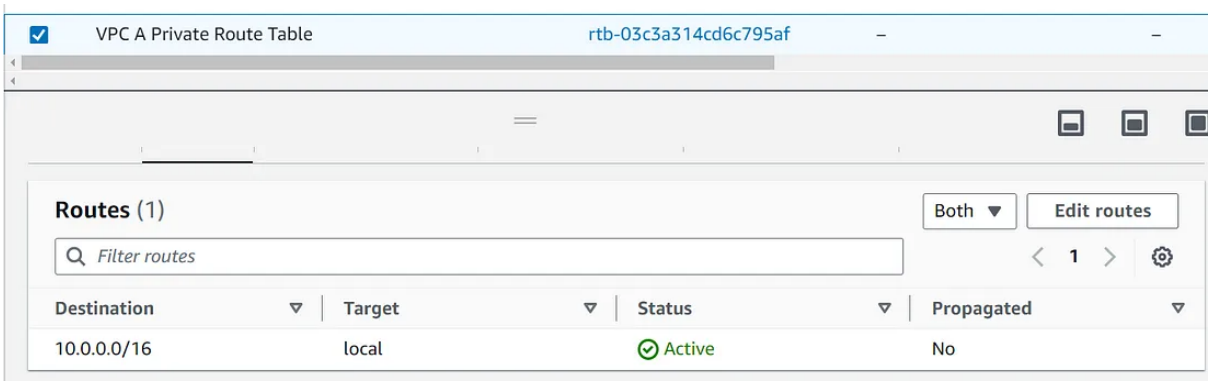
1. Click on Create route table
2. Enter Name as VPC A Private Route Table
3. Select VPC A
4. Create route table

A new route table will be created with a local route. Now in order to enable outbound access to internet we will add a route to internet via NAT Gateway, so we have to associate the Private Subnets to the route table

5. In the Subnet Associations tab click on Edit subnet associations

6. Select the VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2

and click Save associations

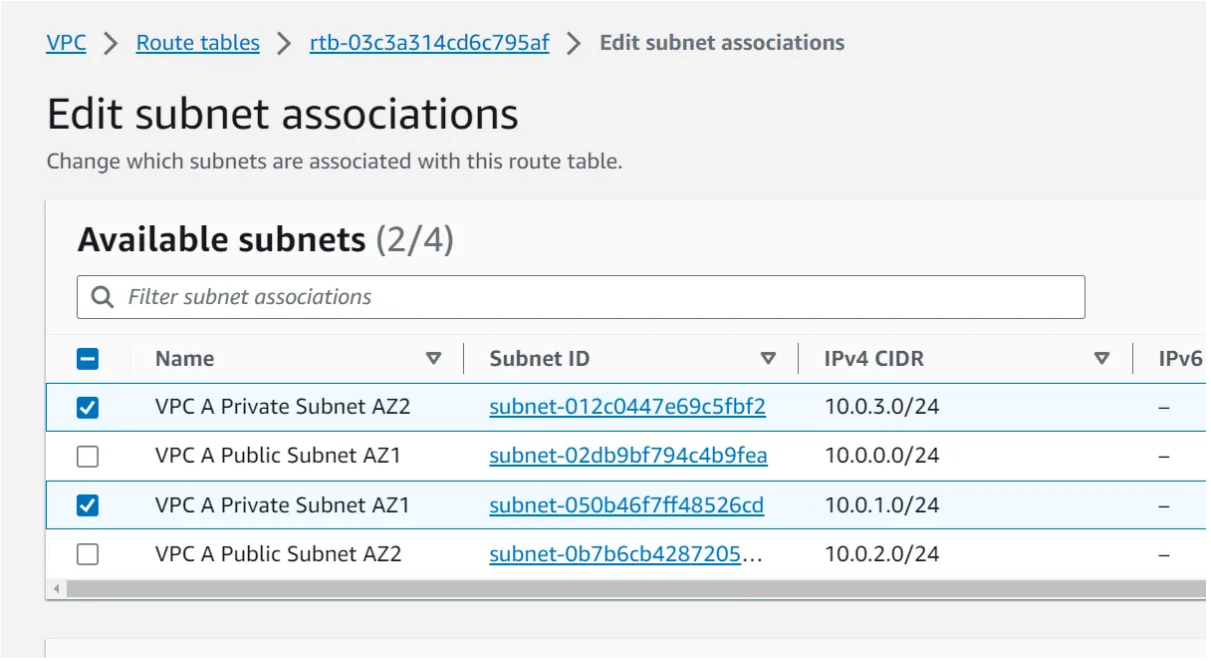


A new route table will be created with a local route. Now in order to enable outbound access to internet we will add a route to internet via NAT Gateway, so we have to associate the Private Subnets to the route table

5. In the Subnet Associations tab click on Edit subnet associations

6. Select the VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2

and click Save associations



7. Now click on Route tables and confirm that there are three route tables under VPC A: main/default, Public and Private.

Internet Connectivity

Internet Gateway:

Internet Gateway is component of VPC that allows communication between your VPC and the internet. It supports IPv4 and IPv6 traffic. IGw is highly available, horizontally scaled and redundant component of VPC.

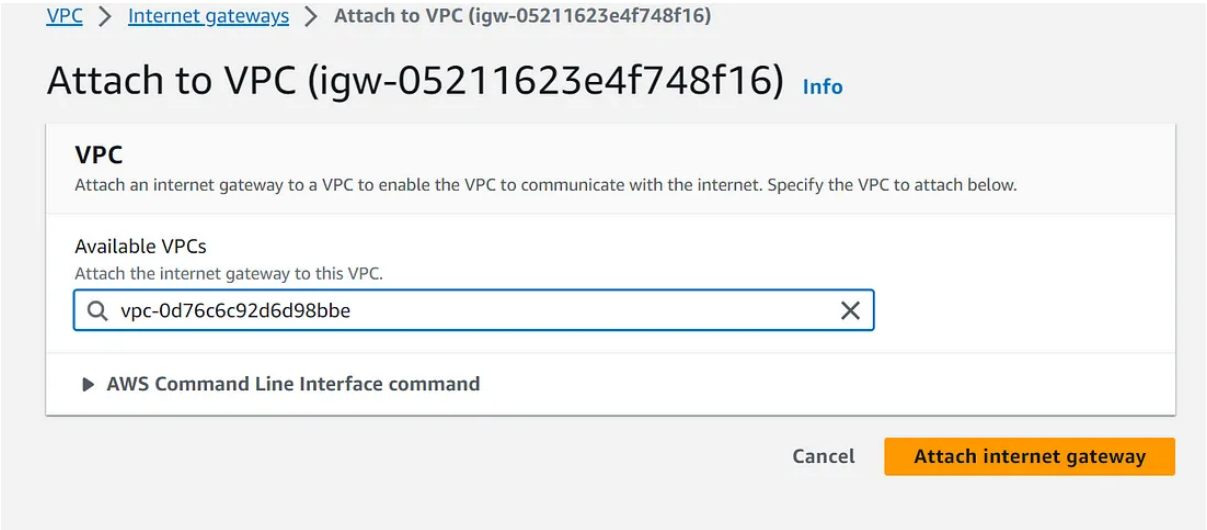
It provides inbound and outbound connectivity of resources in public subnets to the internet .

NAT Gateway:

NAT Gateway is a Network Address Translation Service, it provides access to the instances in private subnets to the services outside your VPC but external services cannot access the resources in

Deploy an Internet Gateway:

1. In the left panel select Internet Gateway and click on Create internet gateway
2. Give name as VPC A IGW and click on Create Internet Gateway
3. Click the newly created IGW and click on Attach to VPC:
4. Select VPC A and click on Attach internet gateway



5. The Internet Gateway should attach successfully.

We now have an internet access for our VPC, but in order to use the newly created Internet Gateway, we need to update VPC routing tables

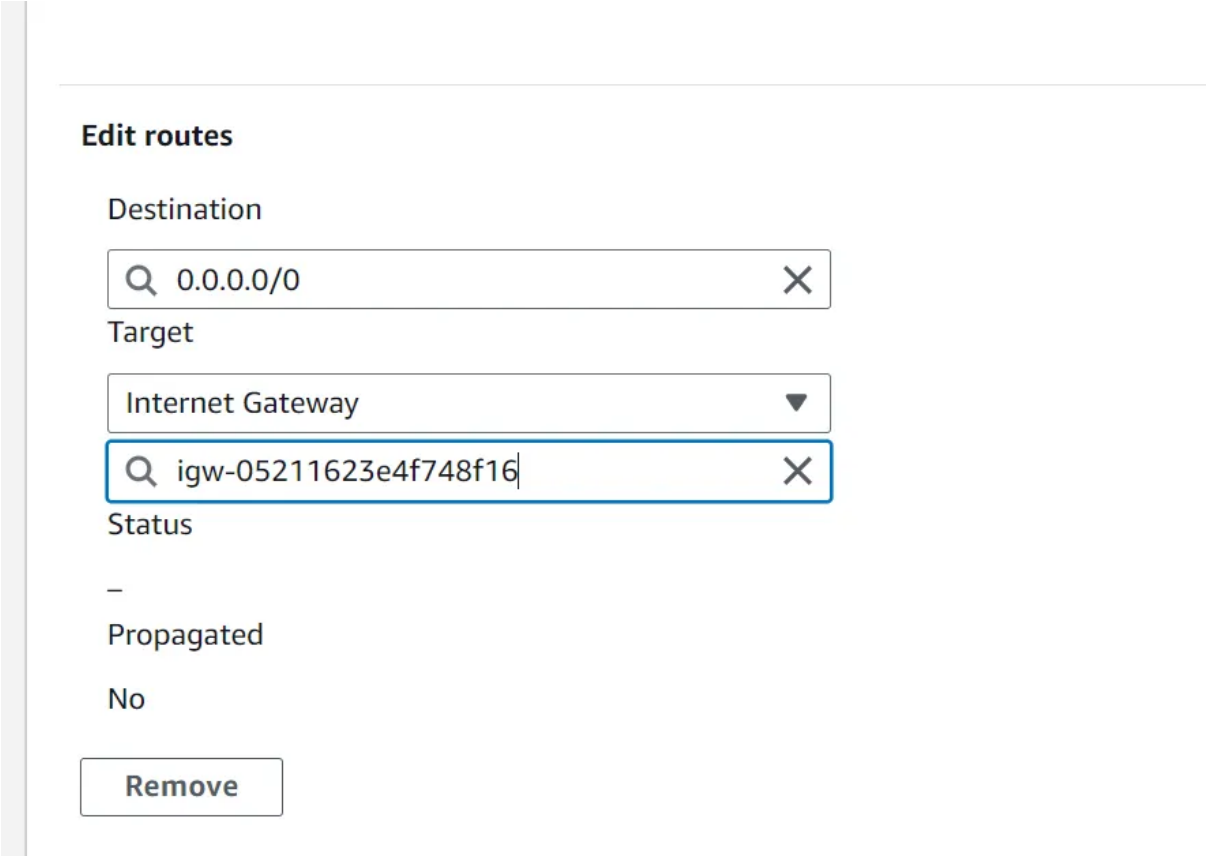
to point the default routes for our public subnets to this Internet Gateway.

[Update Route Table for Public Subnets]

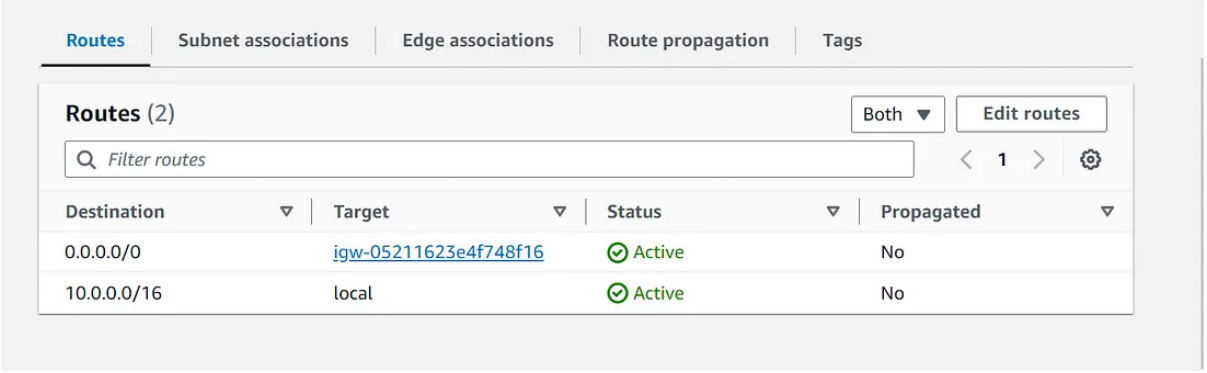
1. In left hand panel of the VPC Dashboard click on [Route Tables] and select `VPC A Public Route Table`

2. Go to the Routes tab and edit routes

- Click on Add route
- Enter `0.0.0.0/0` in the Destination
- Select `Internet Gateway` from the Target dropdown



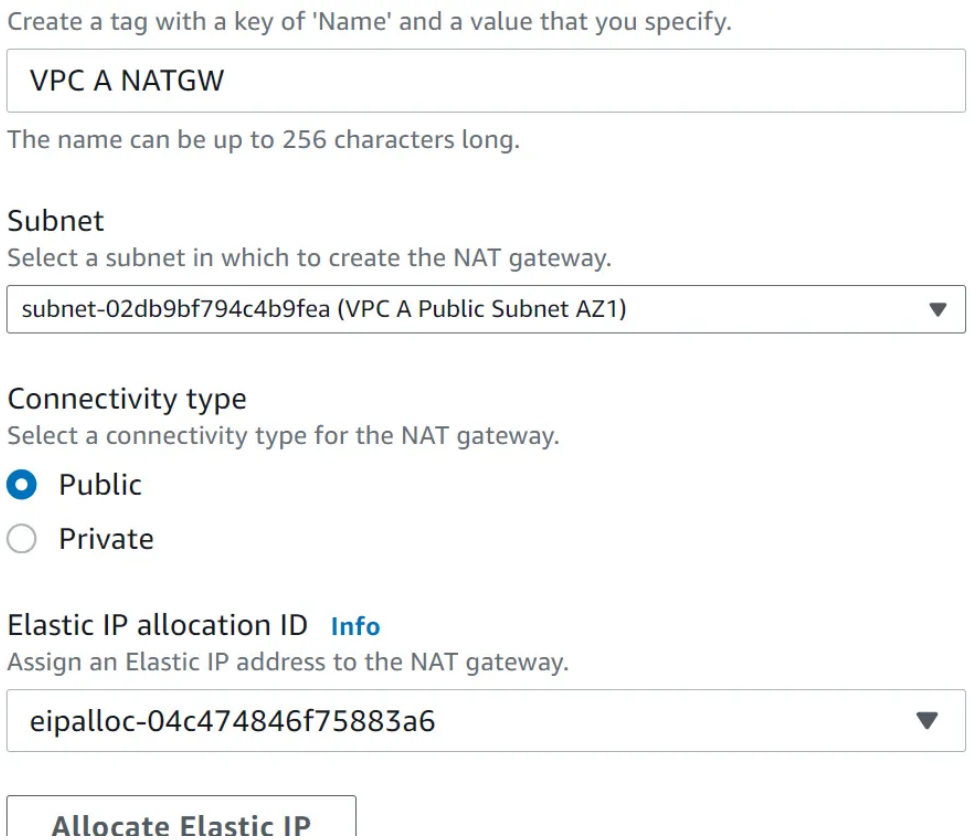
3. Click Save changes and confirm that a new route has been added to the Routes tab



Next we will add outbound connectivity from the private subnets by deploying a NAT Gateway in a public subnet for use by workloads that should not be directly exposed to the internet.

Create NAT Gateway

1. In the left hand panel of the VPC Dashboard click on NAT Gateways and click on Create NAT gateway
2. In the Create NAT gateway screen * Enter `VPC A NATGW` as the name * Choose `VPC A Public Subnet AZ1` * Click Allocate Elastic IP * Click Create NAT gateway

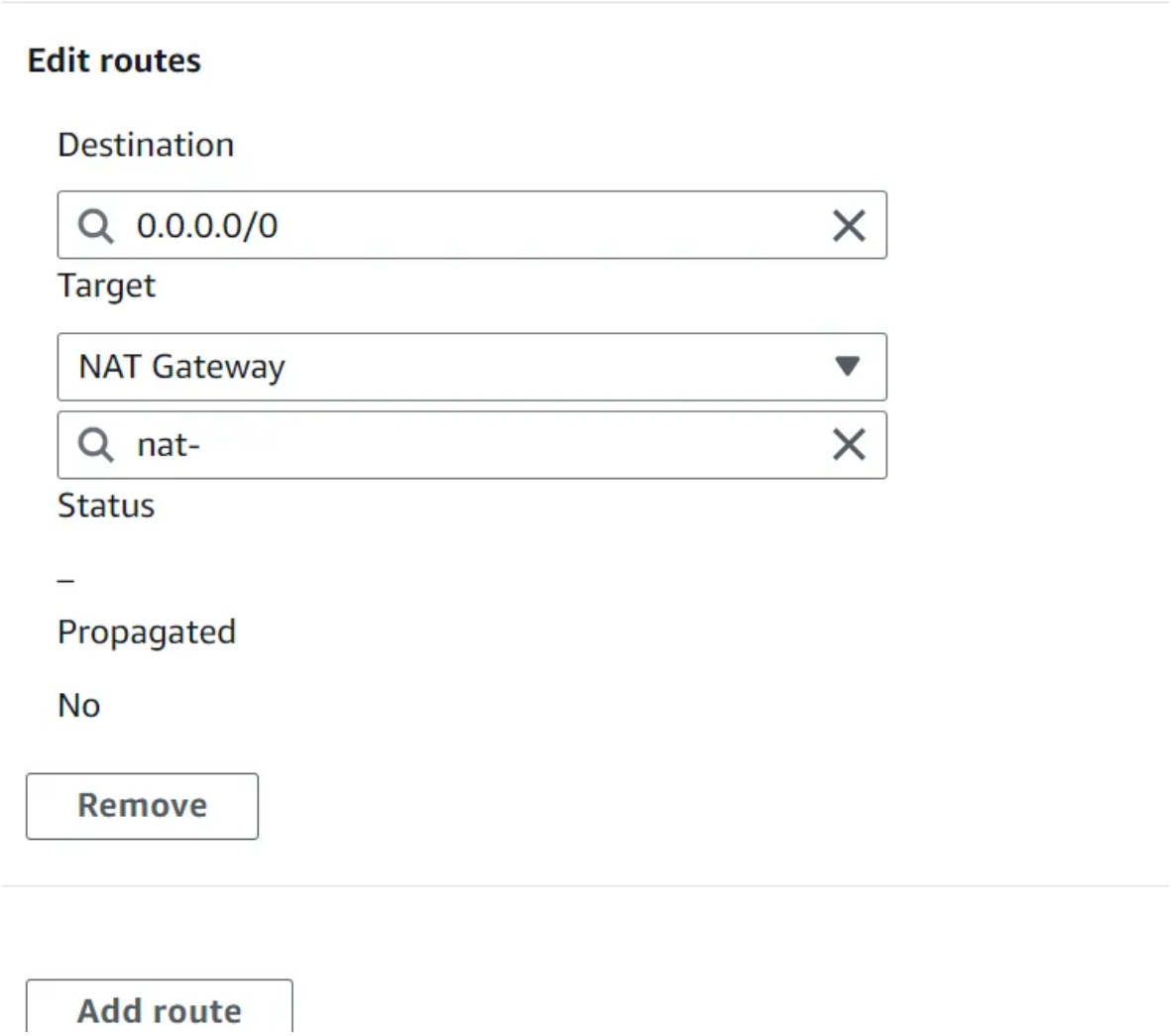


3. Upon creation the NAT Gateway details are displayedUpdate Route Table for Private Subnets

Now that we have a NAT Gateway in a public subnet we need to create a route to it from the private subnets and we will do that by adding an entry to the Route Table for the private subnets.

1.In the left hand panel of the VPC Dashboard click on [Route Tables]

2. Select VPC A Private Route Table, scroll down to the Routes tab and click on Edit routes



3. Choose VPC A NATGW and click on Save changes

** An *Elastic IP address* is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with

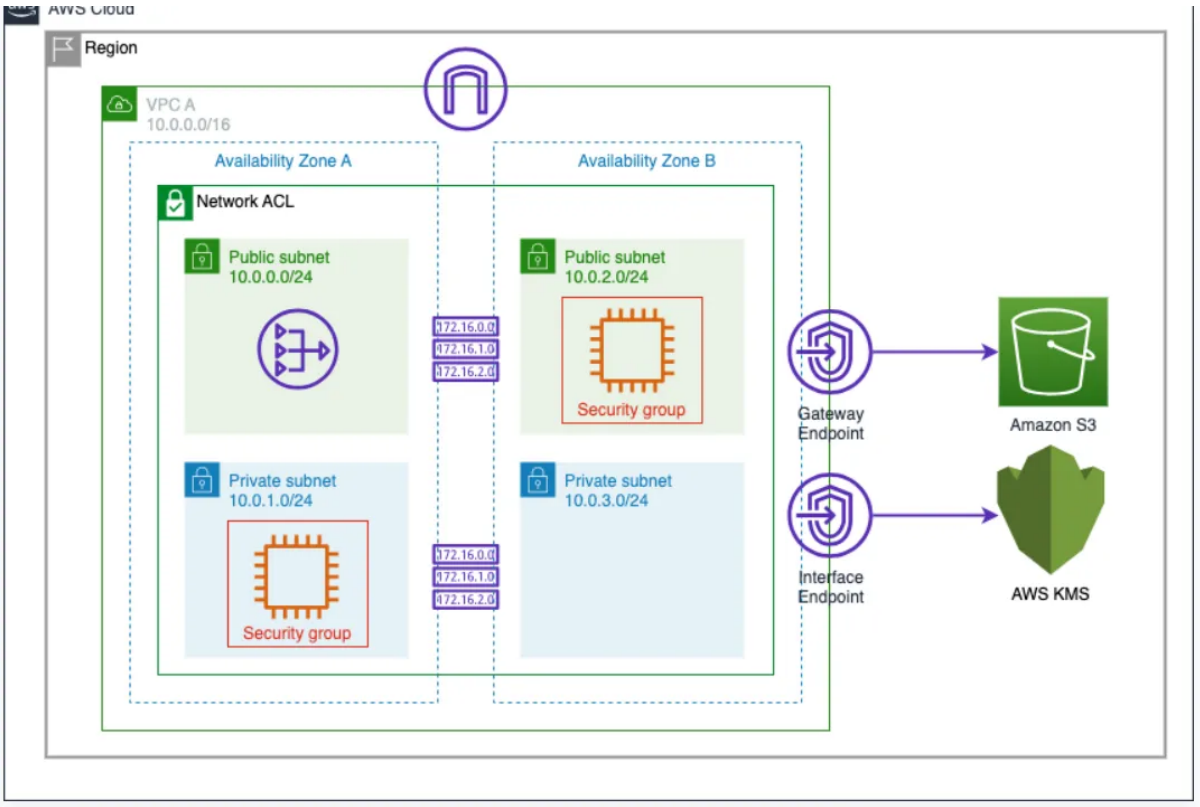
any instance or network interface in any VPC in your account. With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

VPC Endpoints

VPC Endpoints allows customers to privately connect to AWS resources. VPC Endpoints are powered by AWS Private Link .

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available Amazon VPC components that allow communication between instances in an Amazon VPC and services without imposing availability risks or bandwidth constraints on network traffic. There are two types of VPC endpoints:

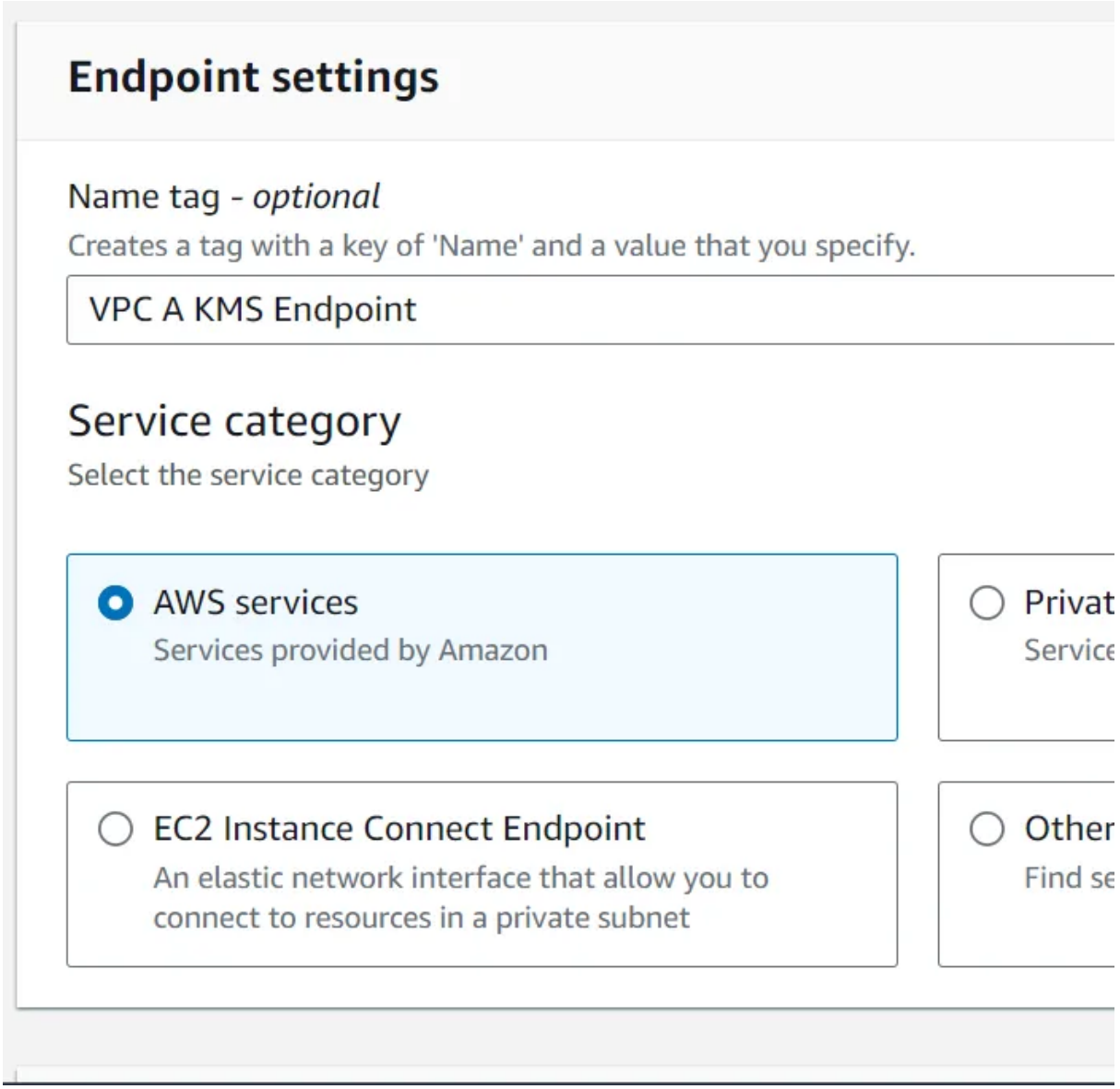
1. Gateway endpoints: It supports only S3 and DynamoDB and reach these services via a gateway from VPC.
2. Interface endpoints: It is a collection of one or more elastic network interfaces with a private IP address that serves as an entry point for traffic destined to a supported service.



[Create an Interface Endpoint for KMS]

1. Navigate to [Endpoints] with the VPC console and click on Create Endpoint to start creating a VPC Endpoint
2. In the Endpoint settings screen

- Enter `VPC A KMS Endpoint` as the Name tag
- Search for ‘kms’ under Services



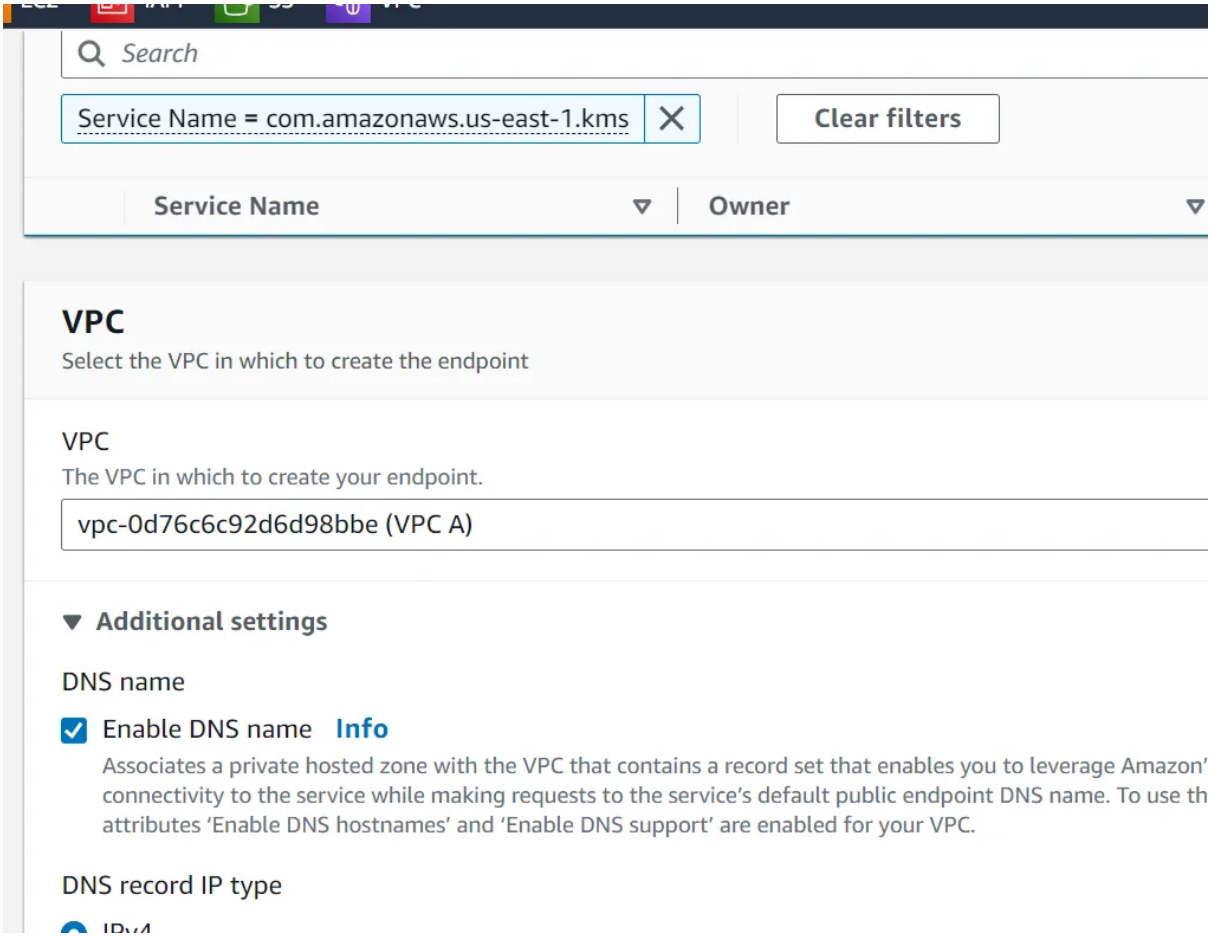
3. From the results select the KMS service name without the'-fips' suffix

4. In the VPC section

- Select VPC A from the dropdown
- Expand the Additional settings section
- Ensure that Enable DNS name is checked

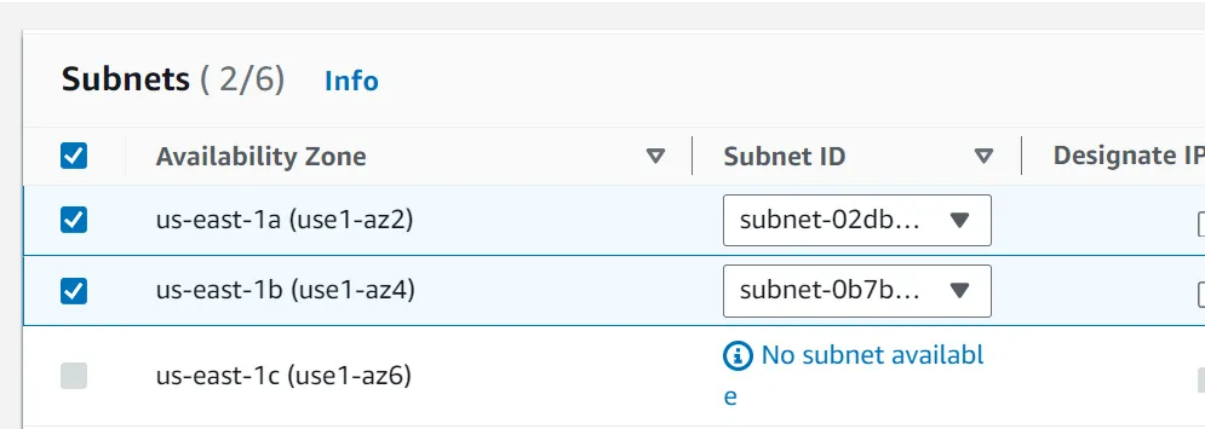
- Select the IPv4 radio button

-



5. Select VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2

from the subnets and check the IPv4 radio button.

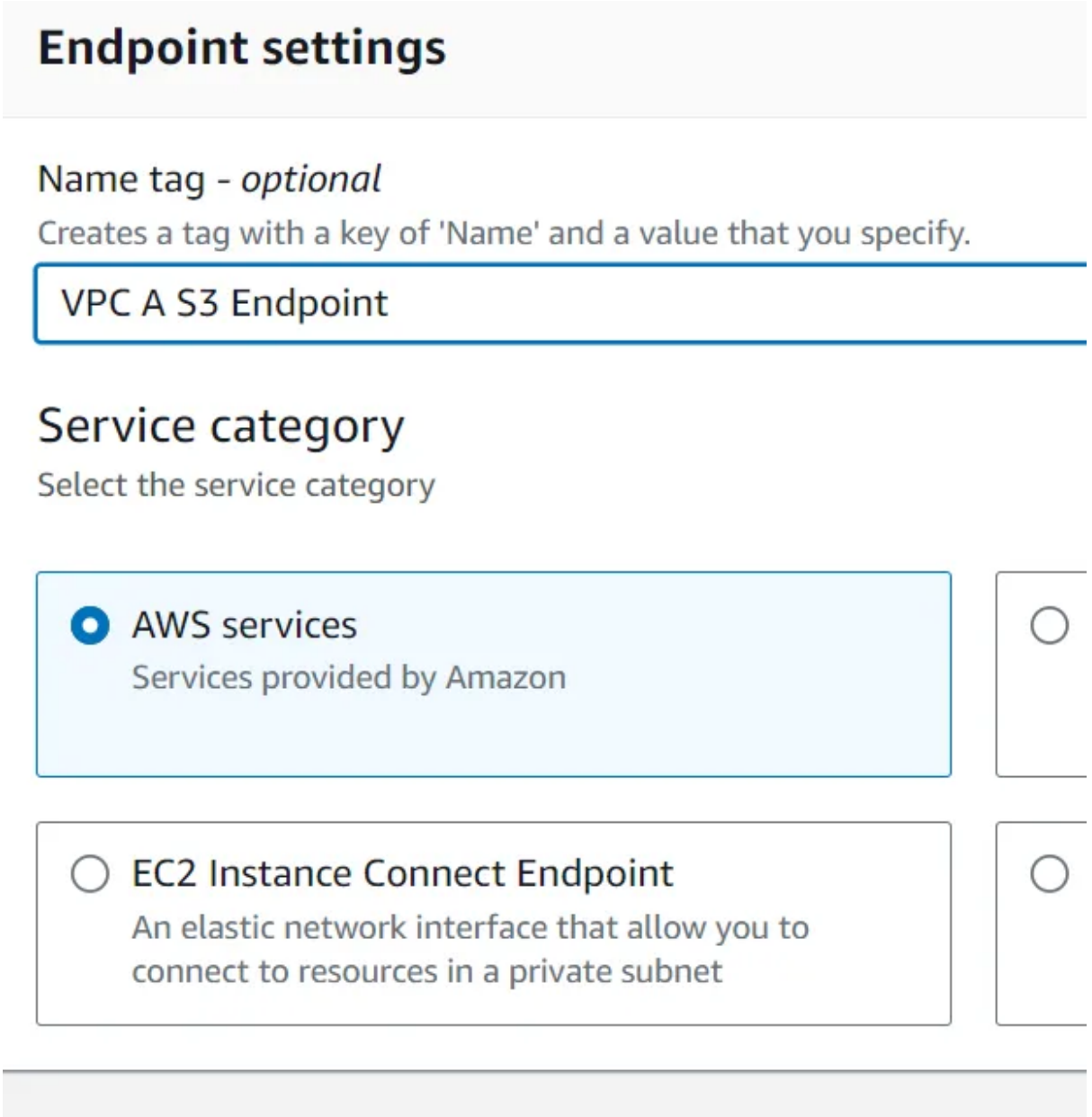


6. Select the default security group and leave the Policy as `Full Access`

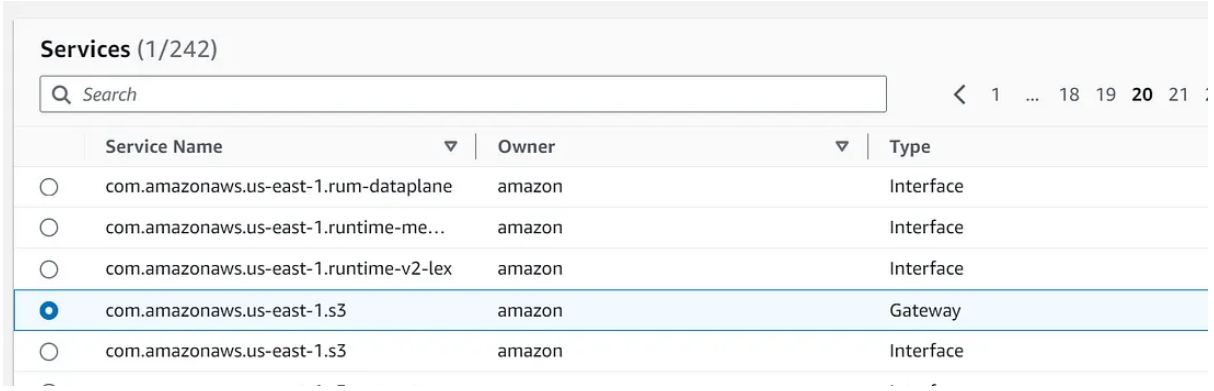
7. Click on Create endpoint button to create the VPC Endpoint for KMS in VPC A.

[Create a Gateway Endpoint for S3]

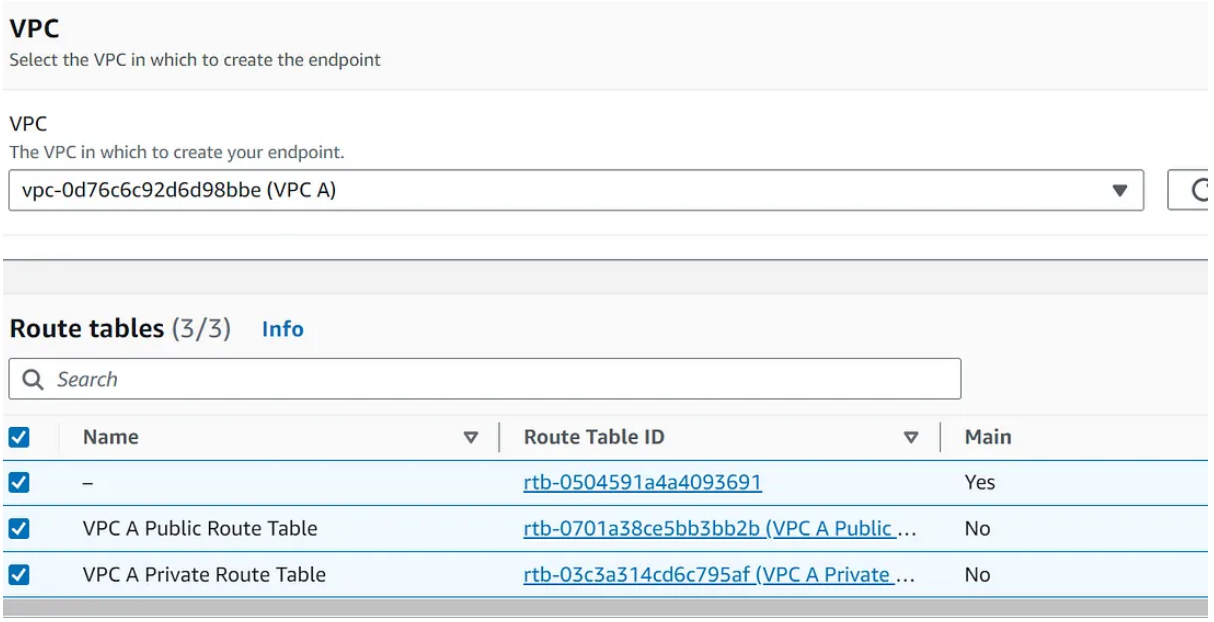
1. Click 'Create Endpoint' to start creating another VPC Endpoint



2. Select the endpoint that has a “Type” listed as “Gateway” and in the drop down box for VPC

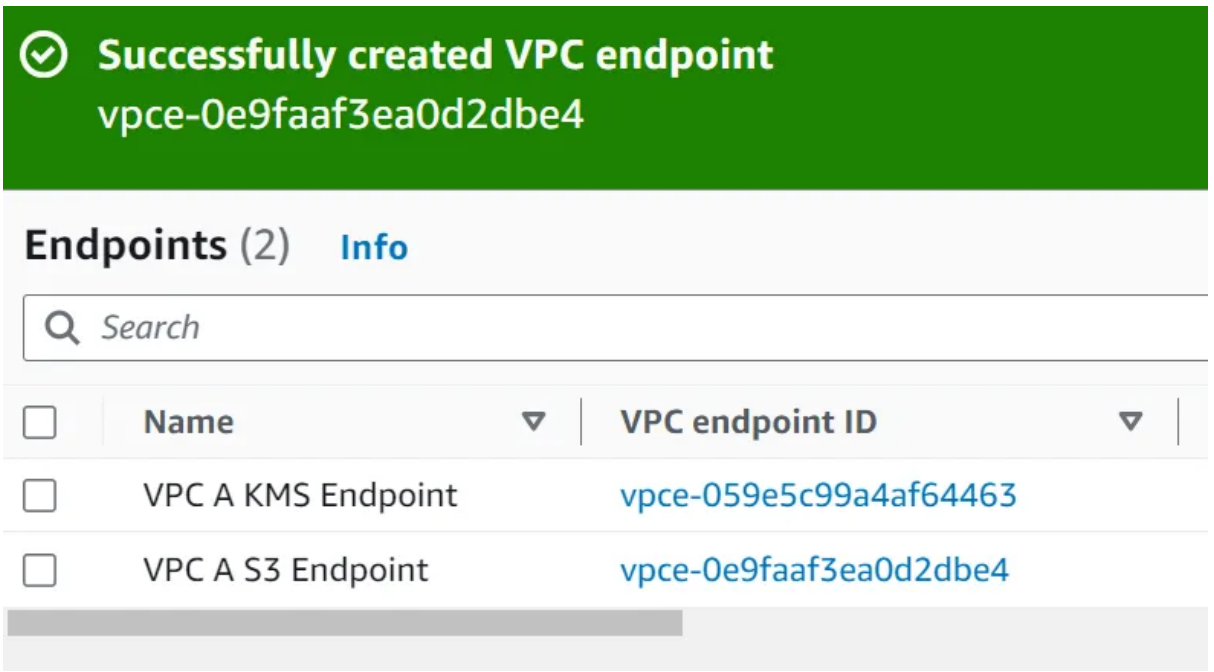


3. Select VPC A as the VPC and check the checkbox for all the route tables



4. Leave the Policy as Full Access

5. Click on Create endpoint button to create the VPC Endpoint for S3 attached to VPC A



We have now gone through the bread and butter of AWS networking and built a networking foundation of public and private subnets across two availability zones with internet access and private connectivity to AWS service endpoints.

Dear Friends, Thank you for reading all the way through. Catch you in the next part !!