Transit Gateway

- Transit Gateway in AWS is used to connect multiple VPC connections together
- It acts like a central hub to connect multiple VPC.
- Transit Gateway simplifies the network management for large-scale environments by centralizing connectivity.
- TGW routes traffic between all attached VPCs and on-premises networks automatically.
- Instead of creating peering connections between every VPC (which becomes more complex when number VPC increased), TGW is best option for large-scale environment.

Target -> Connecting Three VPC using Transit Gateway

Procedure to Create Transit VPC:

Step1: Create VPC1

1. Enter the VPC Name
2. Enter the IP Range in IPV4 CIDR block
3. Select Tenancy, which is Default

- Tenancy in VPC describes how your EC2 instances are deployed on physical hardware within AWS cloud.
- By Selecting **Default** as a Tenancy type, it allows a greater flexibility in instance deployment.

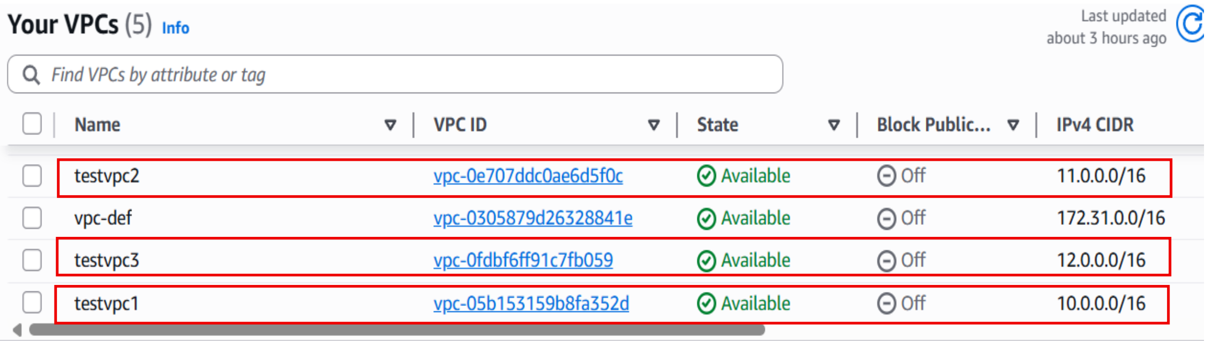
4. Add Tag with Key and Value, which is optional

Step2: Create Internet Gateway

1. Enter the Internet Gateway Name
2. Add Tag (optional)

Step3: Attach the Internet Gateway into VPC

1. Now, internet gateway is currently in detached mode
2. Select the Internet Gateway, Goto Action 'Click' Attach VPC , Select the VPC.



Your VPCs (5) Info

Last updated about 3 hours ago

Find VPCs by attribute or tag

□	Name	VPC ID	State	Block Public...	IPv4 CIDR
□	testvpc2	vpc-0e707ddc0ae6d5f0c	✓ Available	⊖ Off	11.0.0.0/16
□	vpc-def	vpc-0305879d26328841e	✓ Available	⊖ Off	172.31.0.0/16
□	testvpc3	vpc-0fdbf6ff91c7fb059	✓ Available	⊖ Off	12.0.0.0/16
□	testvpc1	vpc-05b153159b8fa352d	✓ Available	⊖ Off	10.0.0.0/16

Step4: Create the Subnet

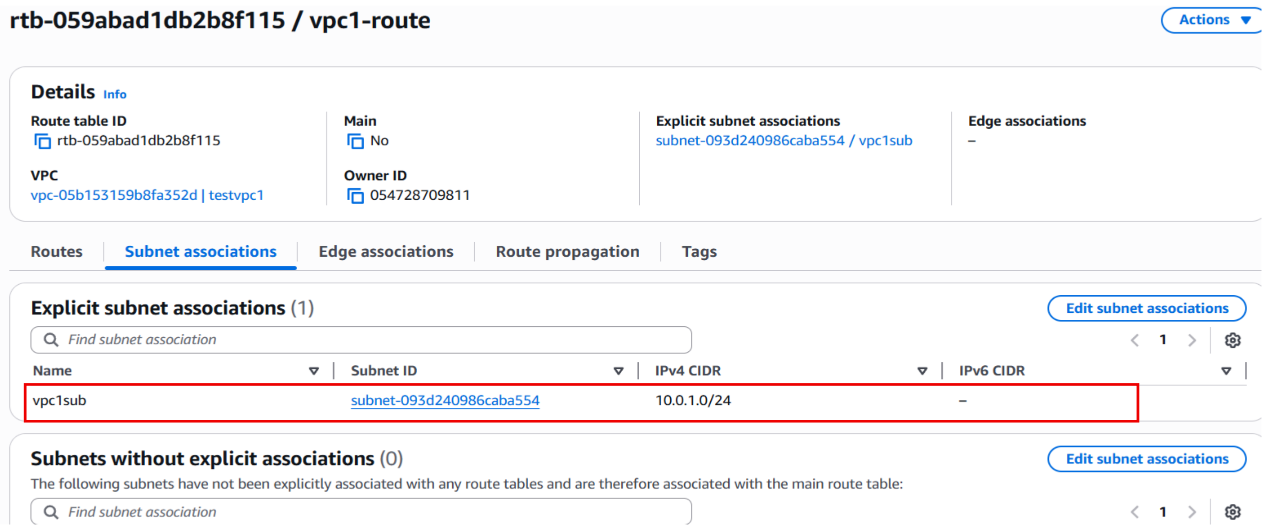
1. Select the VPC
2. Enter the Subnet Name, Select the Availability Zone
3. Enter the IP range.
4. Add Tag.

Step5: Create Route Table

1. Enter Route table Name
2. Select the VPC
3. Add Tag

Step6: Edit Route and Associate Subnet

1. Select the Route table, 'Click' Subnet associations, Select the subnet we created.
2. 'Click' Edit route, Add route -> Add Internet Gateway we created.



rtb-059abad1db2b8f115 / vpc1-route

Details Info

Route table ID: rtb-059abad1db2b8f115

Main: No

Explicit subnet associations: subnet-093d240986caba554 / vpc1sub

Edge associations: –

VPC: vpc-05b153159b8fa352d | testvpc1

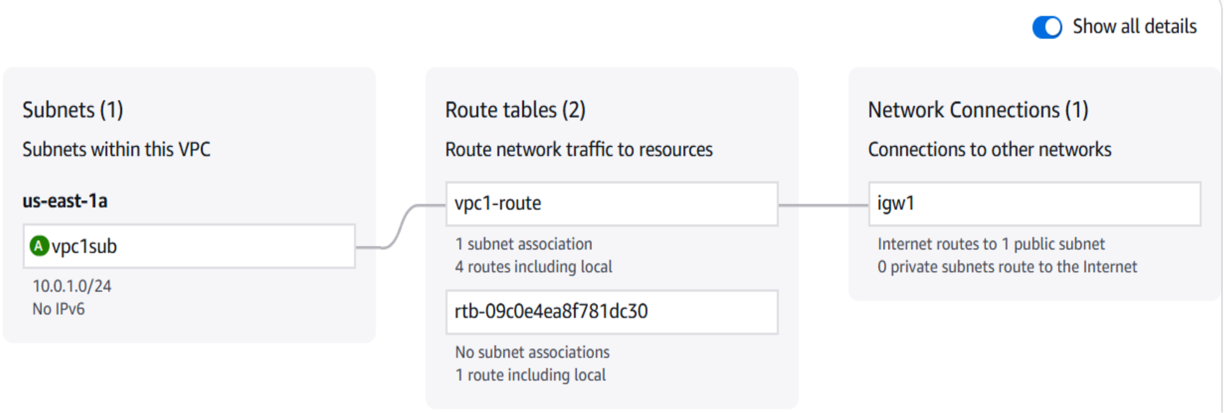
Owner ID: 054728709811

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
vpc1sub	subnet-093d240986caba554	10.0.1.0/24	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:



Subnets (1)
Subnets within this VPC
us-east-1a
vpc1sub
10.0.1.0/24
No IPv6

Route tables (2)
Route network traffic to resources
vpc1-route
1 subnet association
4 routes including local
rtb-09c0e4ea8f781dc30
No subnet associations
1 route including local

Network Connections (1)
Connections to other networks
igw1
Internet routes to 1 public subnet
0 private subnets route to the Internet

Step7: Create EC2 Instance

1. Enter Name for Ec2 server
2. Select AMI Template
3. Instance type
4. Key pair
5. Network settings:
    - Select VPC
    - Select Subnet
    - Auto Assign IP: Enable
    - Firewall (security group) -> Enable SSH, Http

6.Configure Storage

- by default min (windows 30gb, linux 8gb).

Step8: Add UserData

Advanced Details -> Add userdata

User data in an Amazon EC2 instance refers to a set of commands or scripts that can be provided to an instance at launch time. This data is executed automatically on the instance during its initial boot process, allowing for the automation of various setup and configuration tasks.

```
#!bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
echo "Hiii All! ..Welcome to VPC1 server" > /var/www/html/index.html
```

Step9: Similarly remaining VPC2 and VPC3 is created in same procedure.

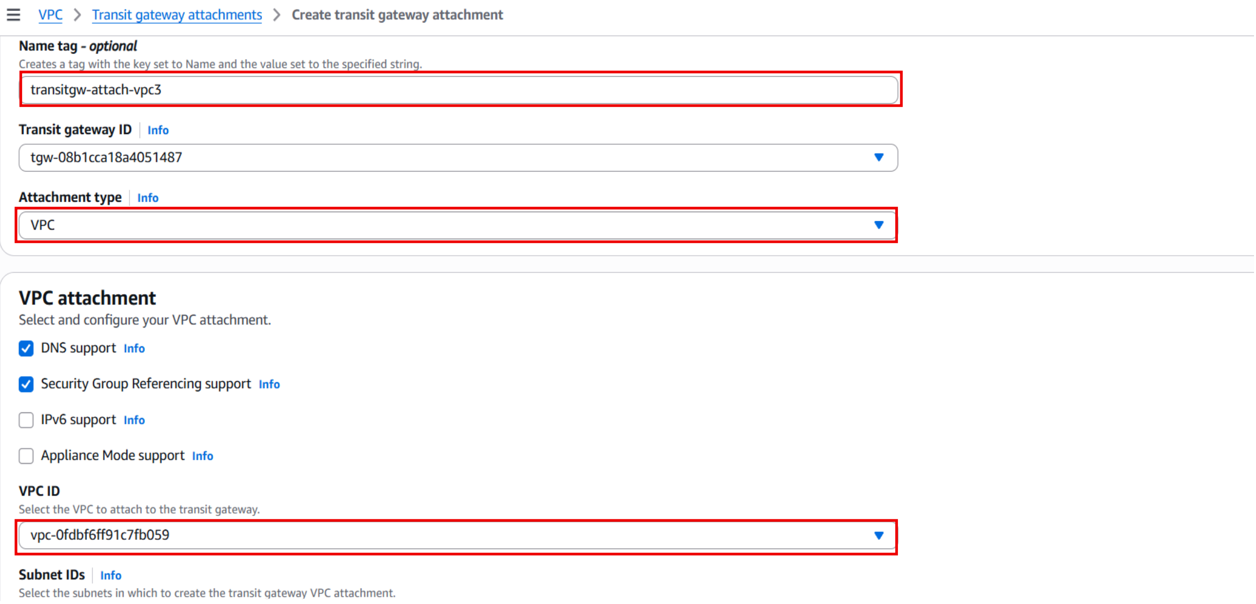
Step10: Create Transit Gateway

1. Enter Transit Gateway Name
2. Enter Description
3. Configure the Transit gateway, ASN (Amazon Site Autonomous System Number), AWS will assign the ASN.

    - An ASN is a unique identifier assigned to a network or a group of networks that operate under a single administrative entity and exchange routing information with other autonomous systems using Border Gateway Protocol (BGP)
    - VPC will find the route based on the ASN.

Step11: Create Transit Gateway Attachment for All VPC

1. Enter Name for Transit Gateway Attachment
2. Attachment type : VPC
3. Select VPC, Select subnet.



VPC > Transit gateway attachments > Create transit gateway attachment

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.
transitgw-attach-vpc3

Transit gateway ID Info
tgw-08b1cca18a4051487

Attachment type Info
VPC

VPC attachment
Select and configure your VPC attachment.

☑ DNS support Info

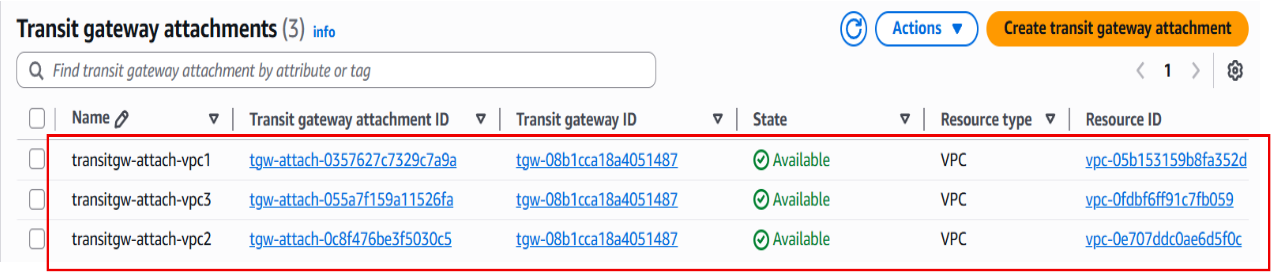
☑ Security Group Referencing support Info

□ IPv6 support Info

□ Appliance Mode support Info

VPC ID
Select the VPC to attach to the transit gateway.
vpc-0fdbf6ff91c7fb059

Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.



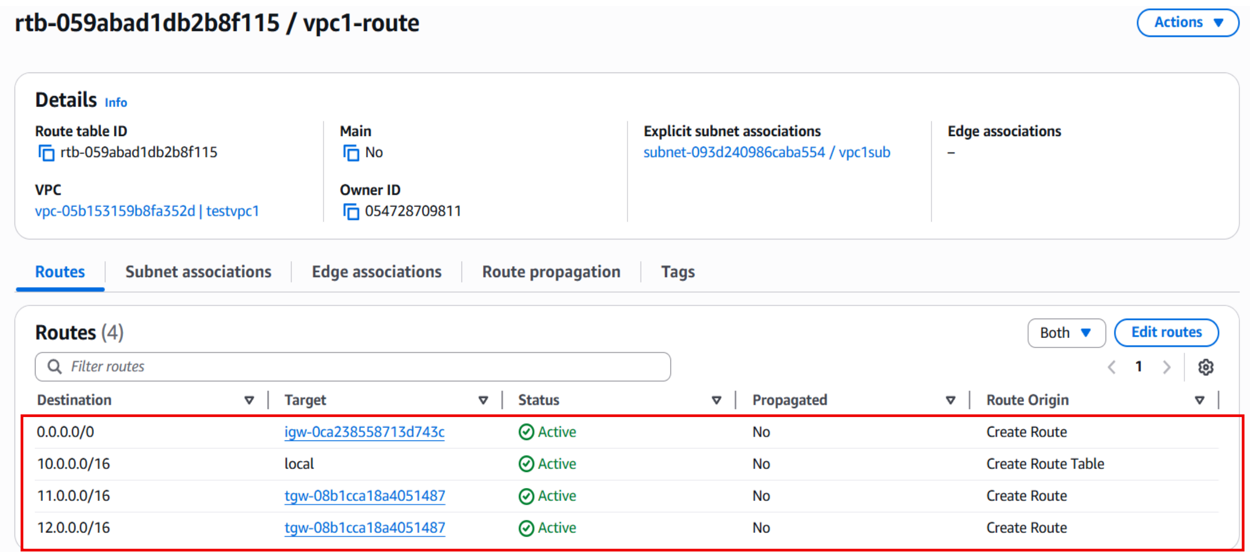
Actions ▼
Create transit gateway attachment
Find transit gateway attachment by attribute or tag
1

Transit gateway attachments (3) info

Name	Transit gateway attachment ID	Transit gateway ID	State	Resource type	Resource ID
transitgw-attach-vpc1	tgw-attach-0357627c7329c7a9a	tgw-08b1cca18a4051487	✓ Available	VPC	vpc-05b153159b8fa352d
transitgw-attach-vpc3	tgw-attach-055a7f159a11526fa	tgw-08b1cca18a4051487	✓ Available	VPC	vpc-0fdbf6ff91c7fb059
transitgw-attach-vpc2	tgw-attach-0c8f476be3f5030c5	tgw-08b1cca18a4051487	✓ Available	VPC	vpc-0e707ddc0ae6d5f0c

Step12: Update the VPC1 Route Table

1. Goto Edit Routes -> Add routes -> Add Ip range of VPC2 and select Transit Gateway Attachment VPC1
2. Goto Edit Routes -> Add routes -> Add Ip range of VPC3 and select Transit Gateway Attachment VPC1



rtb-059abad1db2b8f115 / vpc1-route

Details Info

Route table ID
rtb-059abad1db2b8f115

VPC
vpc-05b153159b8fa352d | testvpc1

Main
No

Owner ID
054728709811

Explicit subnet associations
subnet-093d240986caba554 / vpc1sub

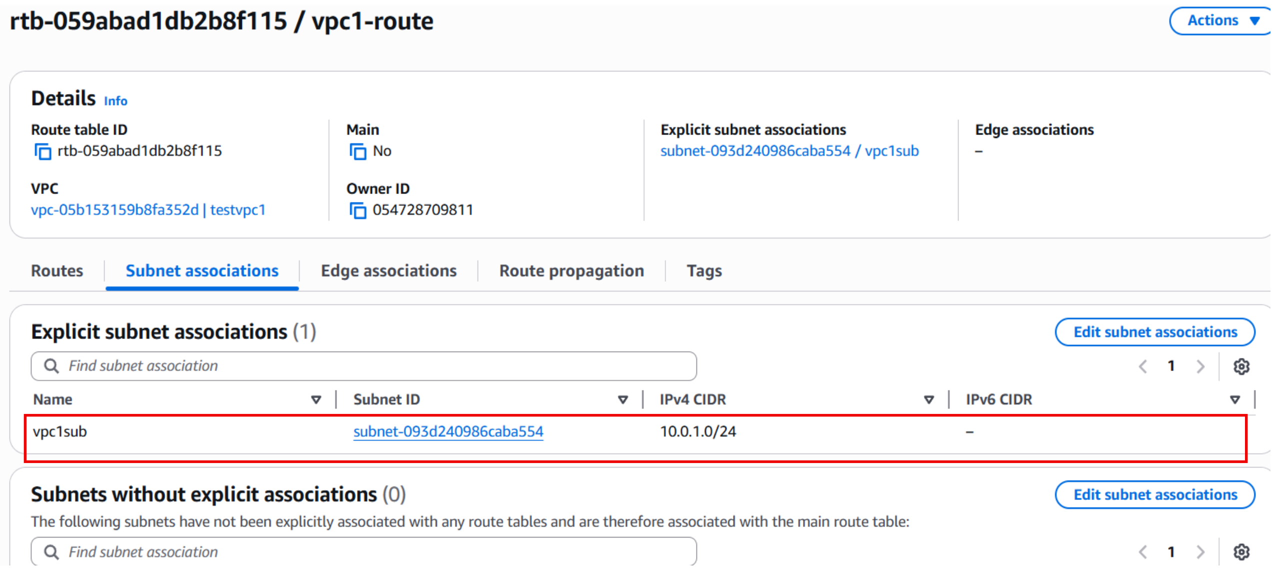
Edge associations
–

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (4)

Both ▼
Edit routes
Filter routes
1

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0ca238558713d743c	✓ Active	No	Create Route
10.0.0.0/16	local	✓ Active	No	Create Route Table
11.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route
12.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route



rtb-059abad1db2b8f115 / vpc1-route

Details Info

Route table ID
rtb-059abad1db2b8f115

VPC
vpc-05b153159b8fa352d | testvpc1

Main
No

Owner ID
054728709811

Explicit subnet associations
subnet-093d240986caba554 / vpc1sub

Edge associations
–

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

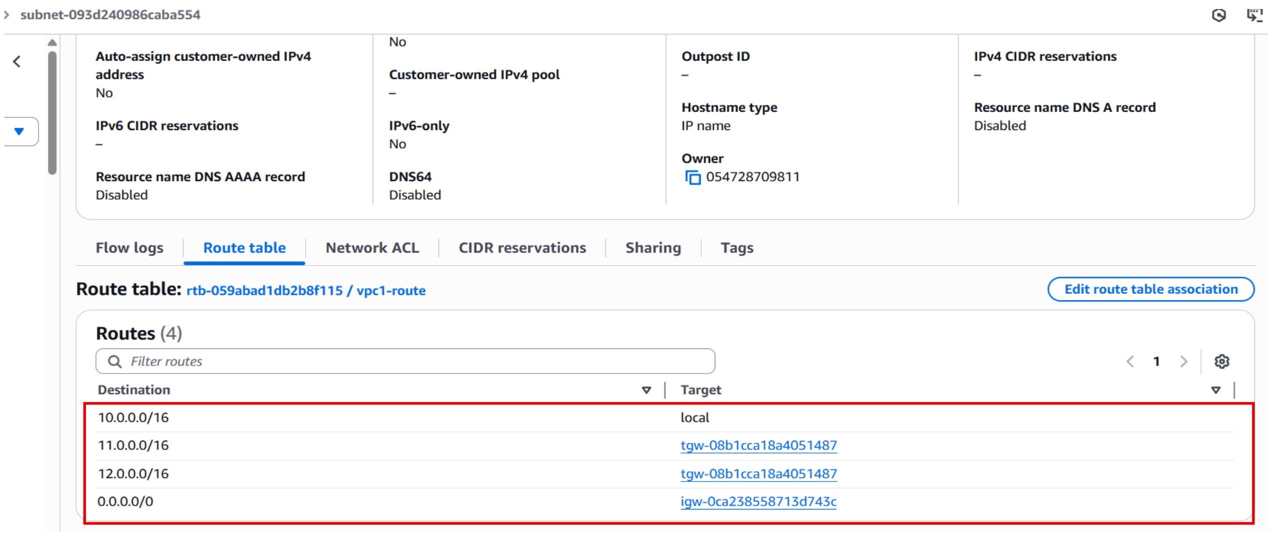
Edit subnet associations
Find subnet association
1

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
vpc1sub	subnet-093d240986caba554	10.0.1.0/24	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association
1



subnet-093d240986caba554

Auto-assign customer-owned IPv4 address No	No Customer-owned IPv4 pool –	Outpost ID –	IPv4 CIDR reservations –
IPv6 CIDR reservations –	IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled
Resource name DNS AAAA record Disabled	DNS64 Disabled	Owner 054728709811	

Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Route table: rtb-059abad1db2b8f115 / vpc1-route

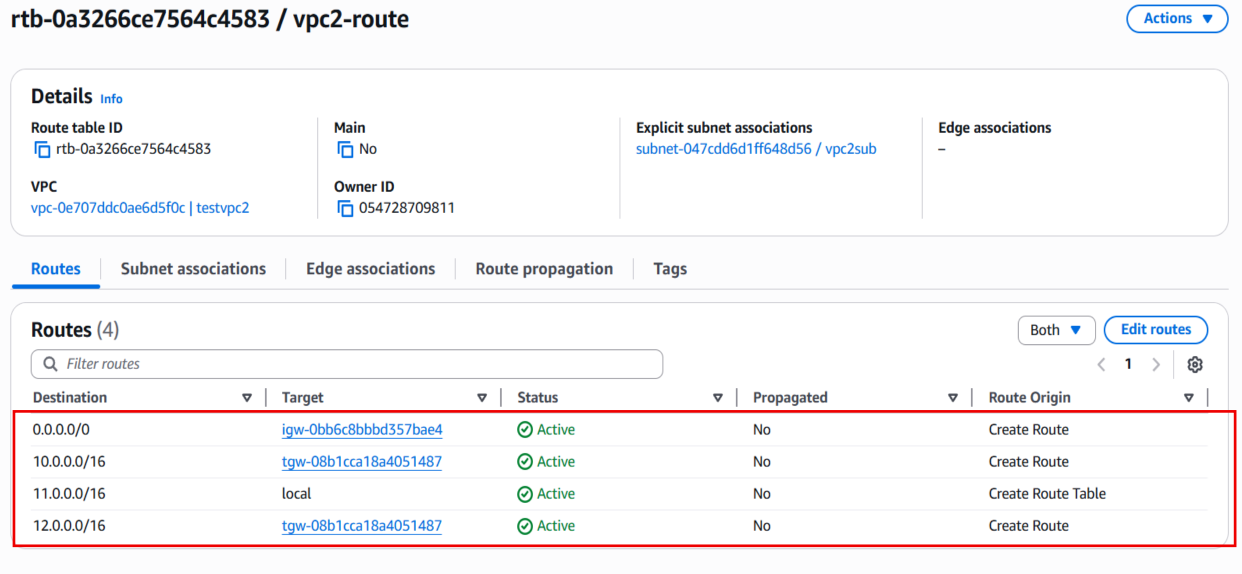
Edit route table association

Routes (4)

Destination	Target
10.0.0.0/16	local
11.0.0.0/16	tgw-08b1cca18a4051487
12.0.0.0/16	tgw-08b1cca18a4051487
0.0.0.0/0	igw-0ca238558713d743c

Step13: Update the VPC2 Route Table

1. Goto Edit Routes -> Add routes -> Add Ip range of VPC1 and select Transit Gateway Attachment VPC2
2. Goto Edit Routes -> Add routes -> Add Ip range of VPC3 and select Transit Gateway Attachment VPC2



rtb-0a3266ce7564c4583 / vpc2-route

Details Info

Route table ID: rtb-0a3266ce7564c4583

Main: No

Explicit subnet associations: subnet-047cdd6d1ff648d56 / vpc2sub

Edge associations: –

VPC: vpc-0e707ddc0ae6d5f0c | testvpc2

Owner ID: 054728709811

Routes | Subnet associations | Edge associations | Route propagation | Tags

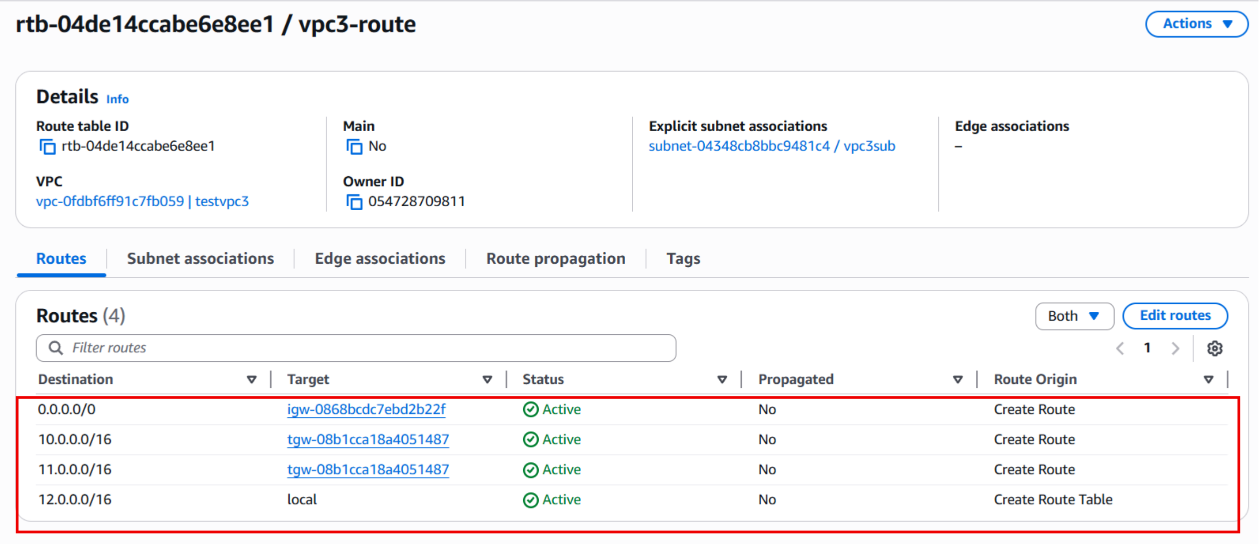
Routes (4)

Both ▼
Edit routes
Filter routes
1

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0bb6c8bbbd357bae4	✓ Active	No	Create Route
10.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route
11.0.0.0/16	local	✓ Active	No	Create Route Table
12.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route

Step14: Update the VPC3 Route Table

1. Goto Edit Routes -> Add routes -> Add Ip range of VPC1 and select Transit Gateway Attachment VPC3
2. Goto Edit Routes -> Add routes -> Add Ip range of VPC2 and select Transit Gateway Attachment VPC3



rtb-04de14ccabe6e8ee1 / vpc3-route

Details Info

Route table ID: rtb-04de14ccabe6e8ee1

Main: No

Explicit subnet associations: subnet-04348cb8bbc9481c4 / vpc3sub

Edge associations: –

VPC: vpc-0fdbf6ff91c7fb059 | testvpc3

Owner ID: 054728709811

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (4)

Both ▼
Edit routes
Filter routes
1

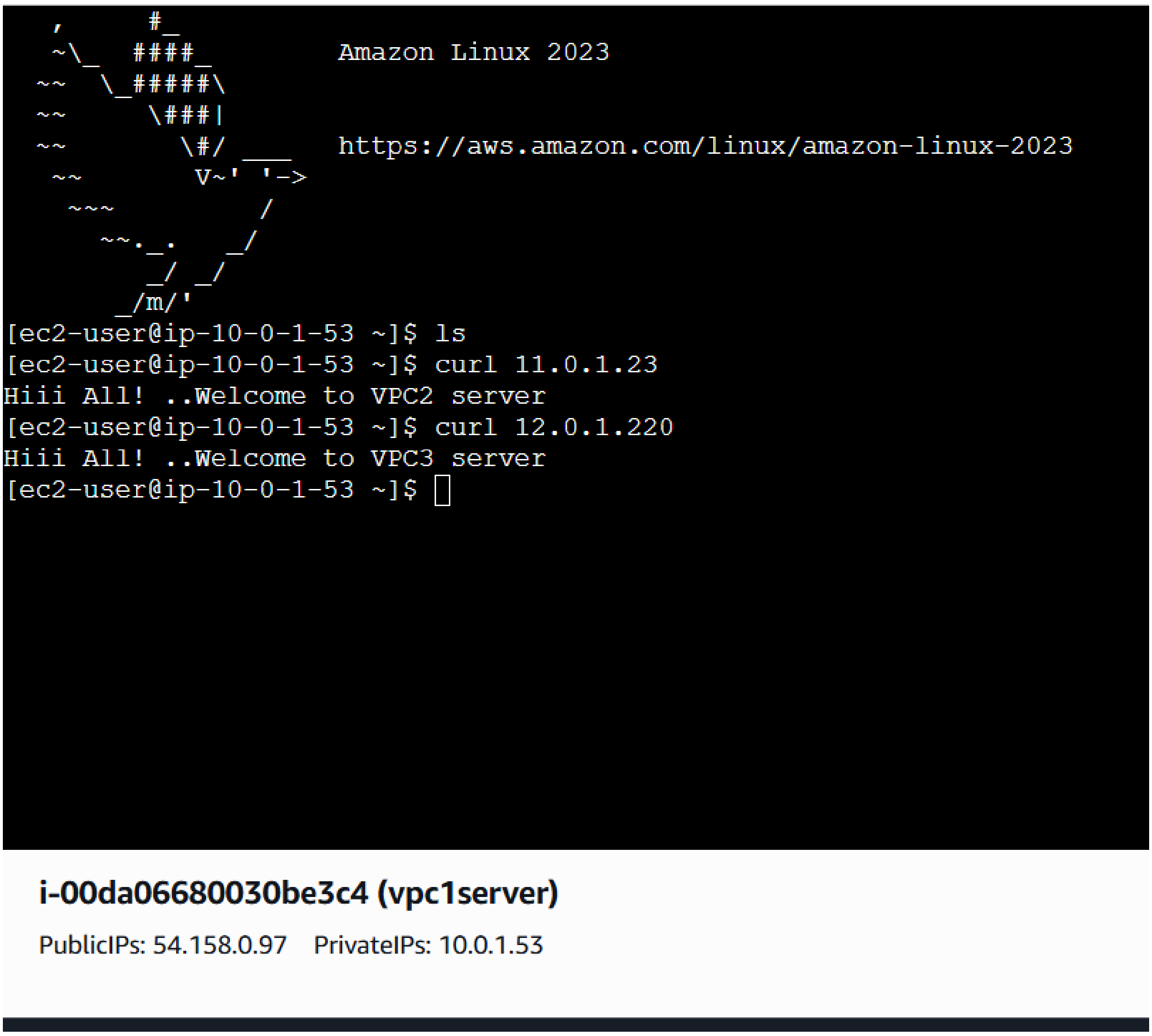
Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0868bcdc7ebd2b22f	✓ Active	No	Create Route
10.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route
11.0.0.0/16	tgw-08b1cca18a4051487	✓ Active	No	Create Route
12.0.0.0/16	local	✓ Active	No	Create Route Table

Step15: Now Let’s Test VPC Peering

1. Goto EC2 instance and Provide the ReadOnly Permission for Keypairs for three EC2 instance created.

   Command: chmod 400 key.pem

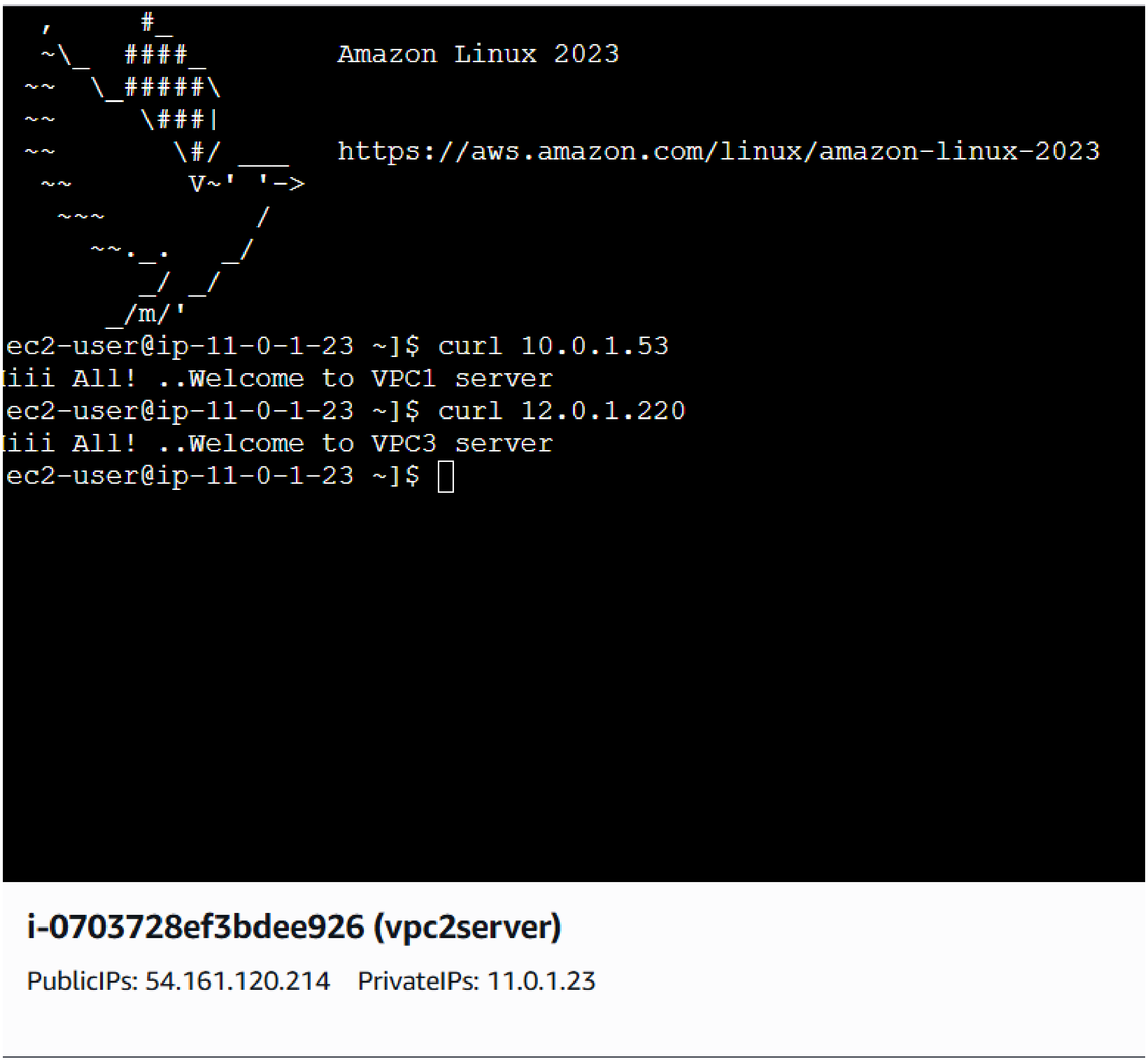
2. Now, check the VPC connection.



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-1-53 ~]$ ls
[ec2-user@ip-10-0-1-53 ~]$ curl 11.0.1.23
Hiii All! ..Welcome to VPC2 server
[ec2-user@ip-10-0-1-53 ~]$ curl 12.0.1.220
Hiii All! ..Welcome to VPC3 server
[ec2-user@ip-10-0-1-53 ~]$ 
```

i-00da06680030be3c4 (vpc1server)

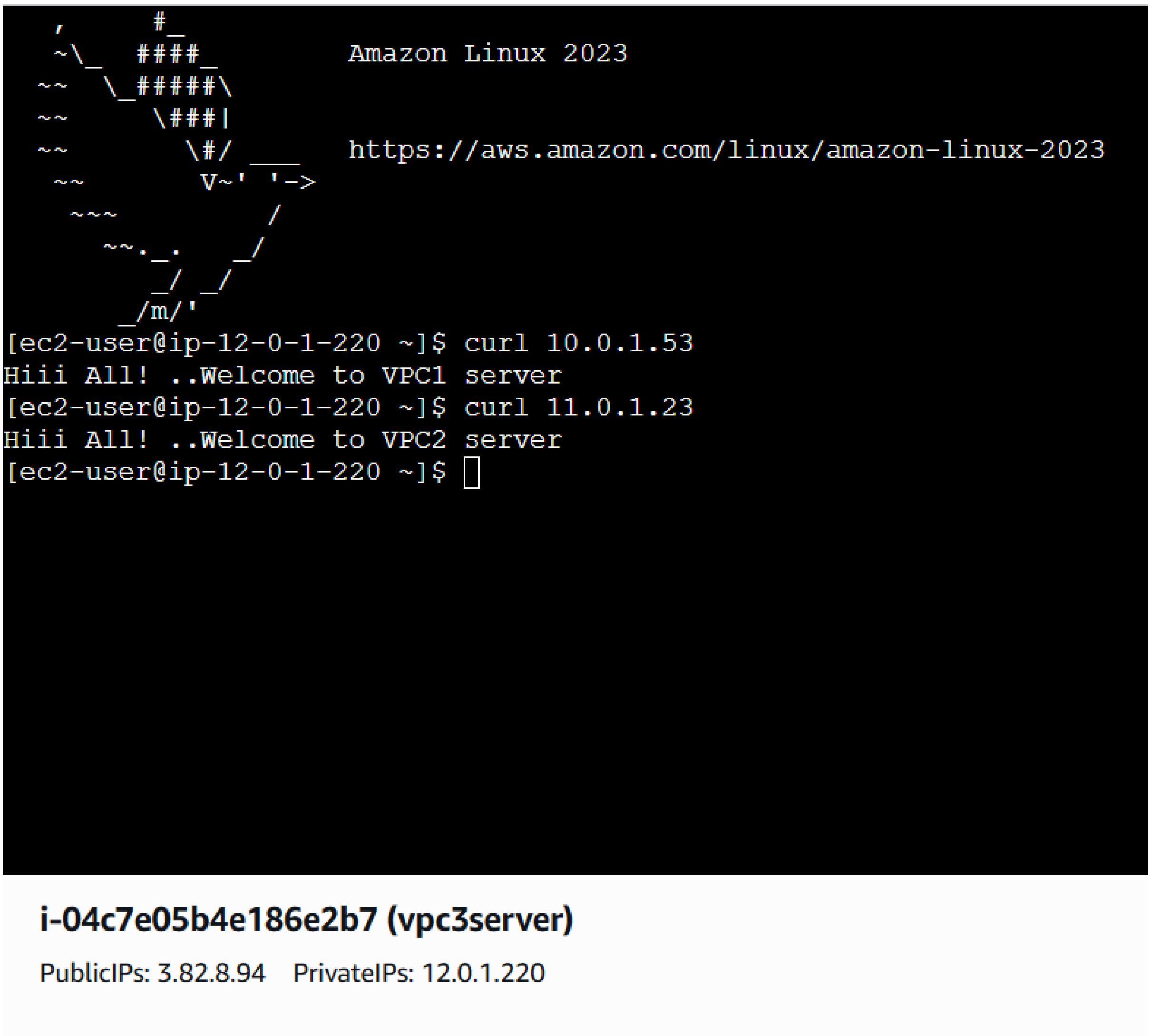
PublicIPs: 54.158.0.97   PrivateIPs: 10.0.1.53



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
ec2-user@ip-11-0-1-23 ~]$ curl 10.0.1.53
iii All! ..Welcome to VPC1 server
ec2-user@ip-11-0-1-23 ~]$ curl 12.0.1.220
iii All! ..Welcome to VPC3 server
ec2-user@ip-11-0-1-23 ~]$ 
```

i-0703728ef3bdee926 (vpc2server)

PublicIPs: 54.161.120.214   PrivateIPs: 11.0.1.23



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-12-0-1-220 ~]$ curl 10.0.1.53
Hiii All! ..Welcome to VPC1 server
[ec2-user@ip-12-0-1-220 ~]$ curl 11.0.1.23
Hiii All! ..Welcome to VPC2 server
[ec2-user@ip-12-0-1-220 ~]$ 
```

i-04c7e05b4e186e2b7 (vpc3server)

PublicIPs: 3.82.8.94   PrivateIPs: 12.0.1.220