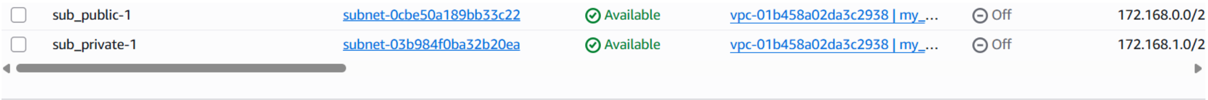
VPC_TASK-2

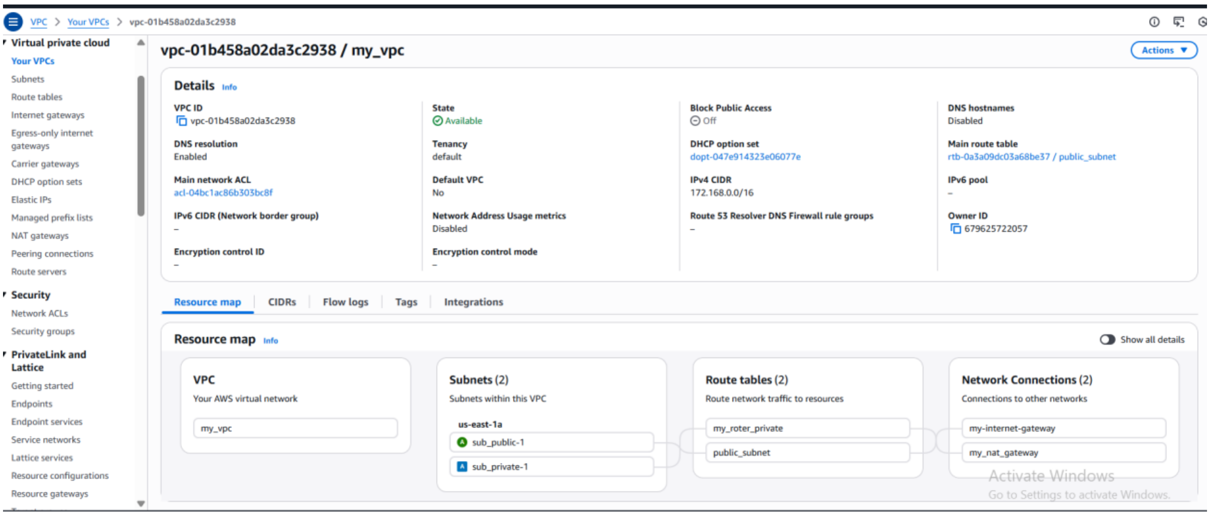
1. Create one VPC, with 1 public subnet and 1 private subnet.

Step 1: Create VPC

1. Go to **AWS Console → VPC**
2. Click **Create VPC**
3. Choose **VPC only**
4. Enter:
   - **Name**: my-vpc
   - **IPv4 CIDR**: 172.168.0.0/16
5. Created VPC.



□	sub_public-1	subnet-0cbe50a189bb33c22	✓ Available	vpc-01b458a02da3c2938 | my_...	⊖ Off	172.168.0.0/2
□	sub_private-1	subnet-03b984f0ba32b20ea	✓ Available	vpc-01b458a02da3c2938 | my_...	⊖ Off	172.168.1.0/2



vpc-01b458a02da3c2938 / my_vpc

Details

VPC ID: vpc-01b458a02da3c2938
State: ✓ Available
Block Public Access: ⊖ Off
DNS hostnames: Disabled
DNS resolution: Enabled
Tenancy: default
DHCP option set: dopt-047e914323e06077e
Main route table: rtb-0a3a09dc03a68be37 / public_subnet
Main network ACL: acl-04bc1ac86b303bc8f
Default VPC: No
IPv4 CIDR: 172.168.0.0/16
IPv6 pool: –
IPv6 CIDR (Network border group): –
Network Address Usage metrics: Disabled
Route 53 Resolver DNS Firewall rule groups: –
Owner ID: 679625722057
Encryption control ID: –
Encryption control mode: –

Resource map

VPC – Your AWS virtual network: my_vpc
Subnets (2) – Subnets within this VPC: us-east-1a: sub_public-1, sub_private-1
Route tables (2) – Route network traffic to resources: my_roter_private, public_subnet
Network Connections (2) – Connections to other networks: my-internet-gateway, my_nat_gateway

2. Enable VPC peering for cross-region.

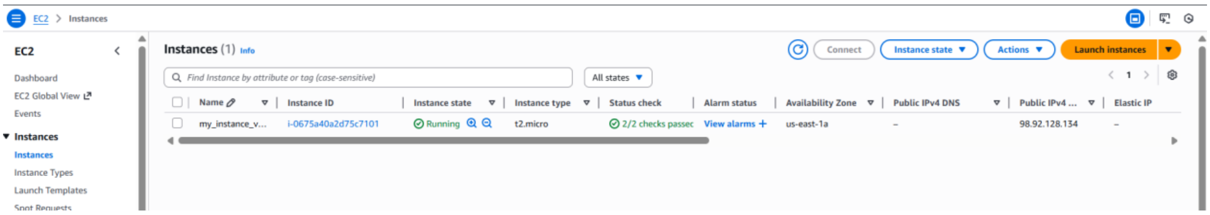
- **VPC A** in **ap-south-1**
- **VPC B** in **us-east-1**

Steps:

1. Go to **VPC → Peering Connections → Create**
2. Select:

- Requester VPC: **VPC A**
- Accepter VPC: **VPC B**

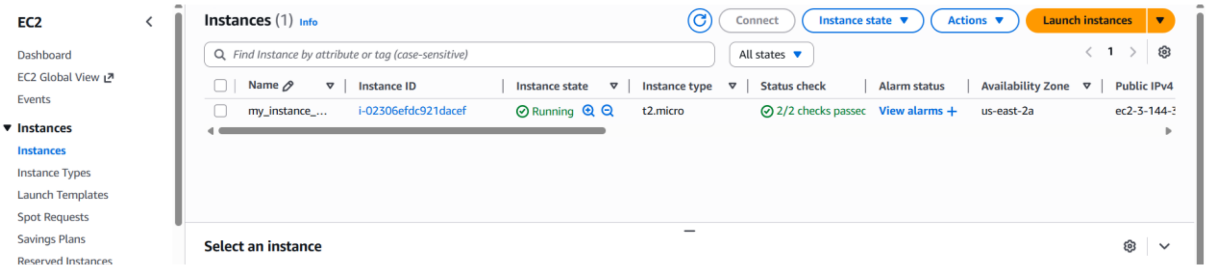
3. After request → go to **VPC B** (other region)
4. Accept the peering request.
5. Update route tables in **both VPCs**:
   - VPC A → add route to VPC B CIDR with **peering connection**
   - VPC B → add route to VPC A CIDR with **peering connection**
6. Add CIDR in security group (Edit inbound) in each instance where we are connecting. And make sure all traffic and 00000 source is also added.



Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
my_instance_v...	i-0675a40a2d75c7101	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1a	–	98.92.128.134	–

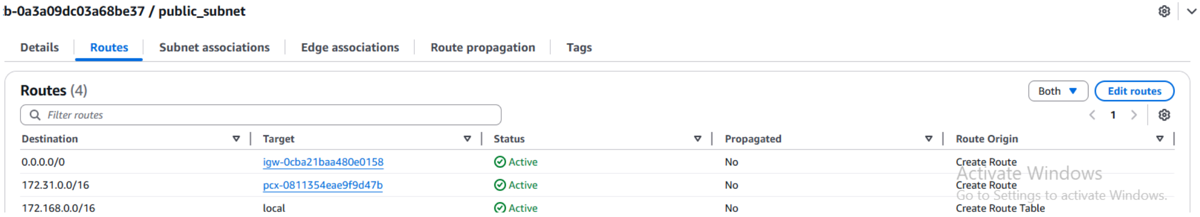


Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
my_instance_...	i-02306efdc921dacef	Running	t2.micro	2/2 checks passec	View alarms +	us-east-2a	ec2-3-144-:

Select an instance

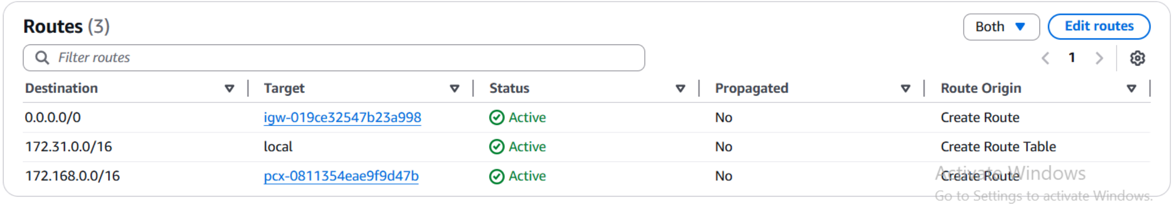


b-0a3a09dc03a68be37 / public_subnet

Routes (4)

Filter routes

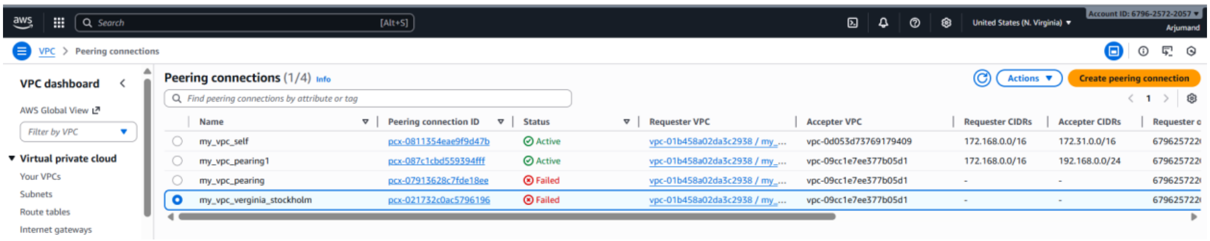
Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0cba21baa480e0158	Active	No	Create Route
172.31.0.0/16	pcx-0811354eae9f9d47b	Active	No	Create Route
172.168.0.0/16	local	Active	No	Create Route Table



Routes (3)

Filter routes

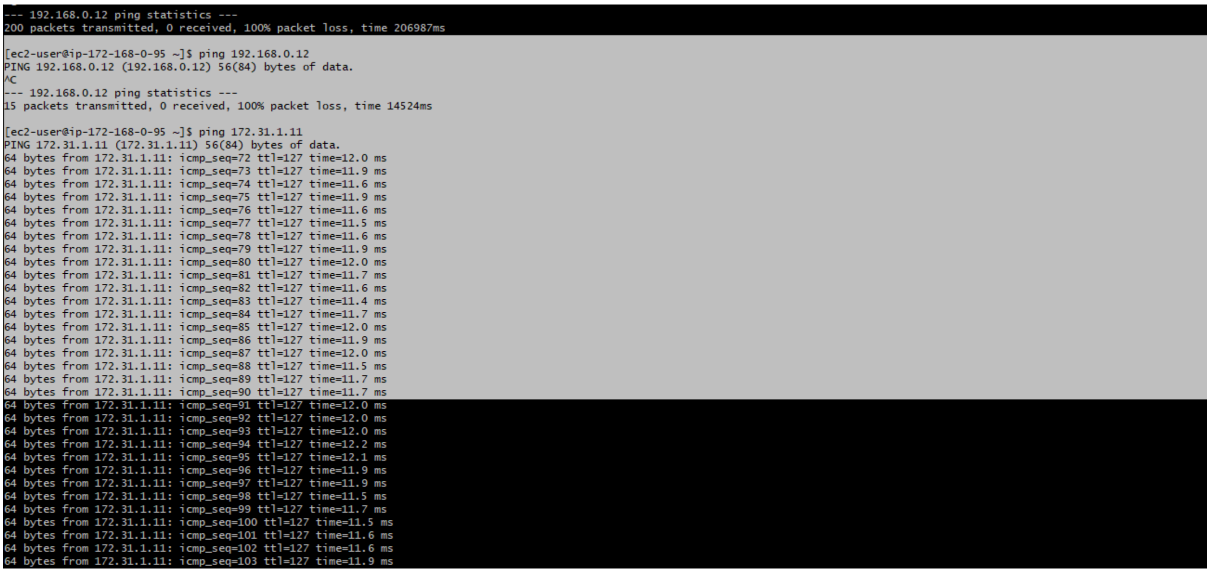
Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-019ce32547b23a998	Active	No	Create Route
172.31.0.0/16	local	Active	No	Create Route Table
172.168.0.0/16	pcx-0811354eae9f9d47b	Active	No	Create Route



Peering connections (1/4) Info

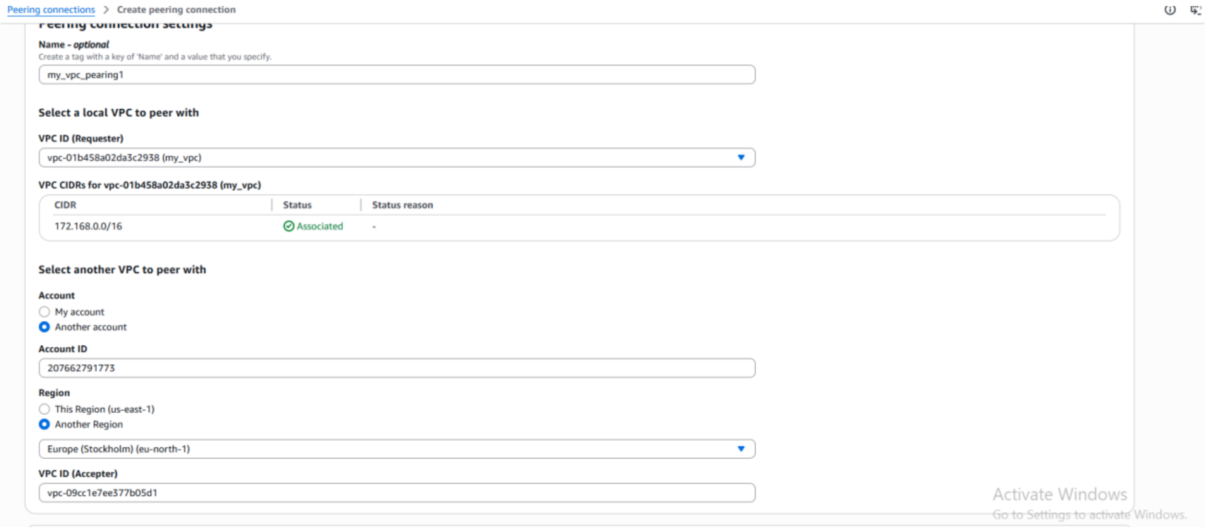
Find peering connections by attribute or tag

	Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester o
○	my_vpc_self	pcx-0811354eae9f9d47b	✓ Active	vpc-01b458a02da3c2938 / my_...	vpc-0d053d73769179409	172.168.0.0/16	172.31.0.0/16	679625722
○	my_vpc_pearing1	pcx-087c1cbd559394fff	✓ Active	vpc-01b458a02da3c2938 / my_...	vpc-09cc1e7ee377b05d1	172.168.0.0/16	192.168.0.0/24	679625722
○	my_vpc_pearing	pcx-07913628c7fde18ee	⊗ Failed	vpc-01b458a02da3c2938 / my_...	vpc-09cc1e7ee377b05d1	-	-	679625722
●	my_vpc_verginia_stockholm	pcx-021732c0ac5796196	⊗ Failed	vpc-01b458a02da3c2938 / my_...	vpc-09cc1e7ee377b05d1	-	-	679625722


```
--- 192.168.0.12 ping statistics ---
200 packets transmitted, 0 received, 100% packet loss, time 206987ms

[ec2-user@ip-172-168-0-95 ~]$ ping 192.168.0.12
PING 192.168.0.12 (192.168.0.12) 56(84) bytes of data.
^C
--- 192.168.0.12 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14524ms

[ec2-user@ip-172-168-0-95 ~]$ ping 172.31.1.11
PING 172.31.1.11 (172.31.1.11) 56(84) bytes of data.
64 bytes from 172.31.1.11: icmp_seq=72 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=73 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=74 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=75 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=76 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=77 ttl=127 time=11.5 ms
64 bytes from 172.31.1.11: icmp_seq=78 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=79 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=80 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=81 ttl=127 time=11.7 ms
64 bytes from 172.31.1.11: icmp_seq=82 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=83 ttl=127 time=11.4 ms
64 bytes from 172.31.1.11: icmp_seq=84 ttl=127 time=11.7 ms
64 bytes from 172.31.1.11: icmp_seq=85 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=86 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=87 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=88 ttl=127 time=11.5 ms
64 bytes from 172.31.1.11: icmp_seq=89 ttl=127 time=11.7 ms
64 bytes from 172.31.1.11: icmp_seq=90 ttl=127 time=11.7 ms
64 bytes from 172.31.1.11: icmp_seq=91 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=92 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=93 ttl=127 time=12.0 ms
64 bytes from 172.31.1.11: icmp_seq=94 ttl=127 time=12.2 ms
64 bytes from 172.31.1.11: icmp_seq=95 ttl=127 time=12.1 ms
64 bytes from 172.31.1.11: icmp_seq=96 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=97 ttl=127 time=11.9 ms
64 bytes from 172.31.1.11: icmp_seq=98 ttl=127 time=11.5 ms
64 bytes from 172.31.1.11: icmp_seq=99 ttl=127 time=11.7 ms
64 bytes from 172.31.1.11: icmp_seq=100 ttl=127 time=11.5 ms
64 bytes from 172.31.1.11: icmp_seq=101 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=102 ttl=127 time=11.6 ms
64 bytes from 172.31.1.11: icmp_seq=103 ttl=127 time=11.9 ms
```



Peering connection settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my_vpc_pearing1

Select a local VPC to peer with

VPC ID (Requester)
vpc-01b458a02da3c2938 (my_vpc)

VPC CIDRs for vpc-01b458a02da3c2938 (my_vpc)

CIDR	Status	Status reason
172.168.0.0/16	✓ Associated	-

Select another VPC to peer with

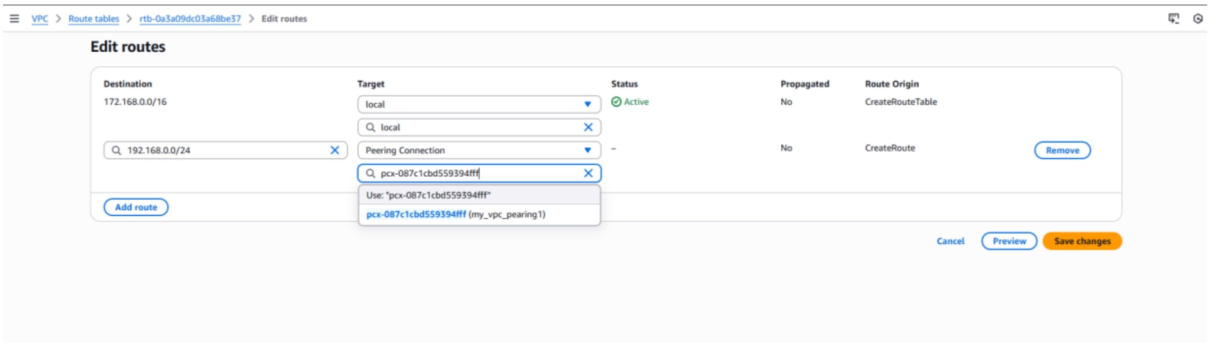
Account
○ My account
● Another account

Account ID
207662791773

Region
○ This Region (us-east-1)
● Another Region

Europe (Stockholm) (eu-north-1)

VPC ID (Accepter)
vpc-09cc1e7ee377b05d1



Edit routes

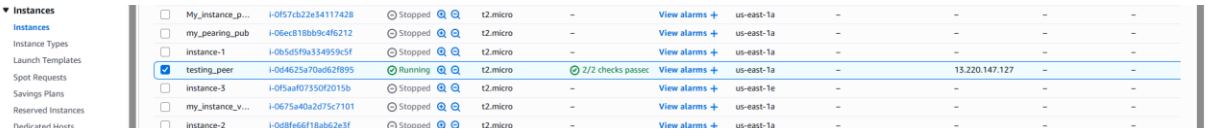
Destination	Target	Status	Propagated	Route Origin	
172.168.0.0/16	local local	✓ Active	No	CreateRouteTable	
192.168.0.0/24	Peering Connection pcx-087c1cbd559394fff	-	No	CreateRoute	Remove

Use: "pcx-087c1cbd559394fff"
pcx-087c1cbd559394fff (my_vpc_pearing1)

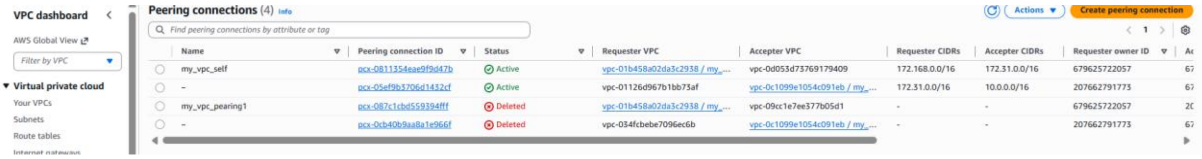
3. Enable VPC peering for cross-account (you can collaborate with your friend to do this task).

Steps:

1. **Your account (Requester):**
    - Create peering request
    - Provide **their VPC ID**
    - Provide **their AWS Account ID**
2. They (Accepter):
    - Login to VPC → Peering
    - Accept request
3. Update route tables on both sides.



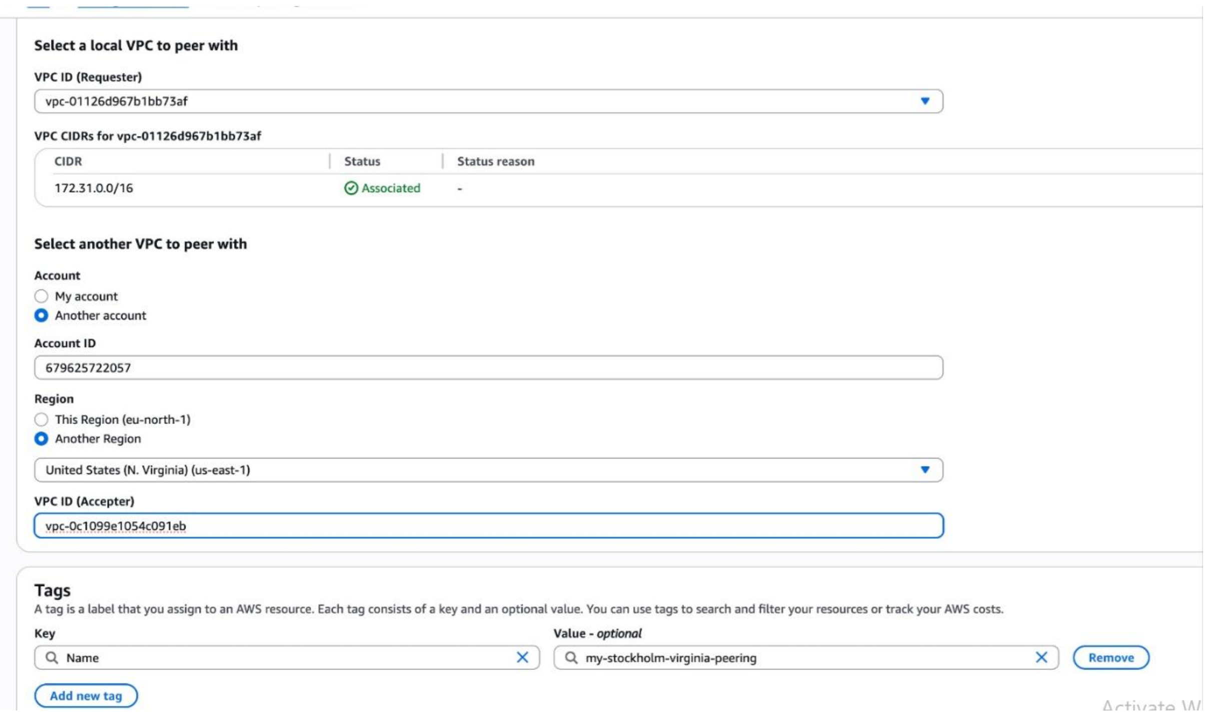
□	My_instance_p...	i-0f57cb22e34117428	⊖ Stopped	t2.micro	–	View alarms +	us-east-1a	–	–	–	–
□	my_pearing_pub	i-06ec818bb9c4f6212	⊖ Stopped	t2.micro	–	View alarms +	us-east-1a	–	–	–	–
□	instance-1	i-0b5d5f9a334959c5f	⊖ Stopped	t2.micro	–	View alarms +	us-east-1a	–	–	–	–
☑	testing_peer	i-0d4625a70ad62f895	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	us-east-1a	–	13.220.147.127	–	–
□	instance-3	i-0f5aaf07350f2015b	⊖ Stopped	t2.micro	–	View alarms +	us-east-1e	–	–	–	–
□	my_instance_v...	i-0675a40a2d75c7101	⊖ Stopped	t2.micro	–	View alarms +	us-east-1a	–	–	–	–
□	instance-2	i-0d8fe66f18ab62e3f	⊖ Stopped	t2.micro	–	View alarms +	us-east-1a	–	–	–	–



Peering connections (4) Info

Find peering connections by attribute or tag

	Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester owner ID	Ac
○	my_vpc_self	pcx-0811354eae9f9d47b	✓ Active	vpc-01b458a02da3c2938 / my_...	vpc-0d053d73769179409	172.168.0.0/16	172.31.0.0/16	679625722057	67
○	-	pcx-05ef9b3706d1432cf	✓ Active	vpc-01126d967b1bb73af	vpc-0c1099e1054c091eb / my_...	172.31.0.0/16	10.0.0.0/16	207662791773	67
○	my_vpc_pearing1	pcx-087c1cbd559394fff	⊗ Deleted	vpc-01b458a02da3c2938 / my_...	vpc-09cc1e7ee377b05d1	-	-	679625722057	20
○	-	pcx-0cb40b9aa8a1e966f	⊗ Deleted	vpc-034fcbebe7096ec6b	vpc-0c1099e1054c091eb / my_...	-	-	207662791773	67



Select a local VPC to peer with

VPC ID (Requester)

vpc-01126d967b1bb73af ▼

VPC CIDRs for vpc-01126d967b1bb73af

CIDR	Status	Status reason
172.31.0.0/16	✓ Associated	-

Select another VPC to peer with

Account

○ My account
● Another account

Account ID

679625722057

Region

○ This Region (eu-north-1)
● Another Region

United States (N. Virginia) (us-east-1) ▼

VPC ID (Accepter)

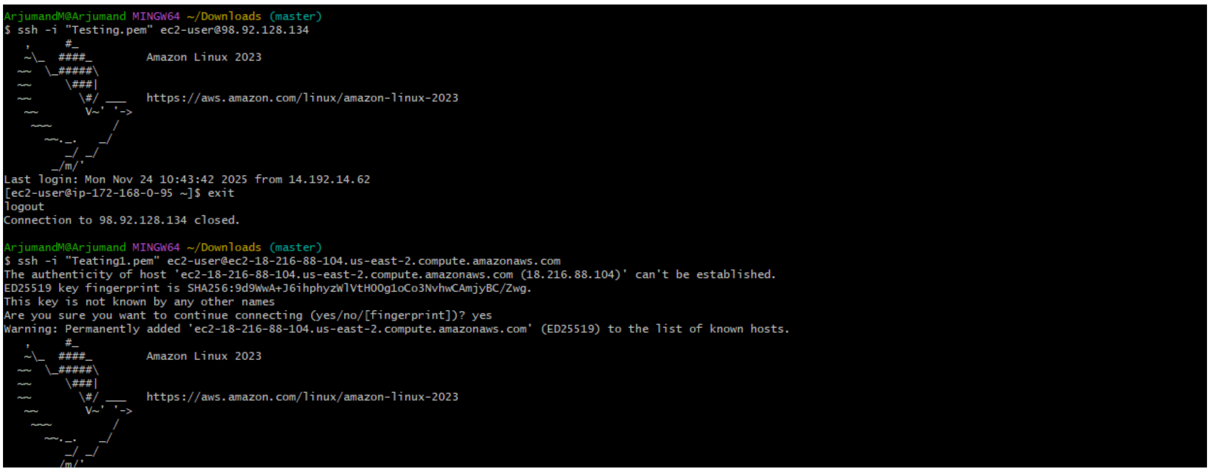
vpc-0c1099e1054c091eb

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

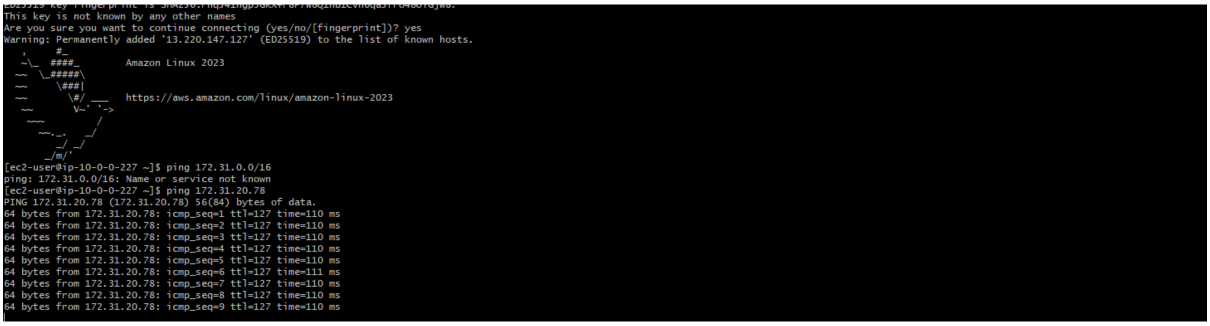
Key	Value - *optional*	
Name	my-stockholm-virginia-peering	Remove

Add new tag



```
ArjumandM@Arjumand MINGW64 ~/Downloads (master)
$ ssh -i "Testing.pem" ec2-user@98.92.128.134
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Mon Nov 24 10:43:42 2025 from 14.192.14.62
[ec2-user@ip-172-168-0-95 ~]$ exit
logout
Connection to 98.92.128.134 closed.

ArjumandM@Arjumand MINGW64 ~/Downloads (master)
$ ssh -i "Teating1.pem" ec2-user@ec2-18-216-88-104.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-18-216-88-104.us-east-2.compute.amazonaws.com (18.216.88.104)' can't be established.
ED25519 key fingerprint is SHA256:9d9WwA+J6ihphyzWlVtHOOg1oCo3NvhwCAmjyBC/Zwg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-18-216-88-104.us-east-2.compute.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```



```
ED25519 key fingerprint is SHA256:[illegible]
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.220.147.127' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-0-227 ~]$ ping 172.31.0.0/16
ping: 172.31.0.0/16: Name or service not known
[ec2-user@ip-10-0-0-227 ~]$ ping 172.31.20.78
PING 172.31.20.78 (172.31.20.78) 56(84) bytes of data.
64 bytes from 172.31.20.78: icmp_seq=1 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=2 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=3 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=4 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=5 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=6 ttl=127 time=111 ms
64 bytes from 172.31.20.78: icmp_seq=7 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=8 ttl=127 time=110 ms
64 bytes from 172.31.20.78: icmp_seq=9 ttl=127 time=110 ms
```

4. Set up a VPC Transit Gateway.

▯ Create Transit Gateway

- VPC → Transit Gateways → Create → default settings.

▯ Create VPC Attachment

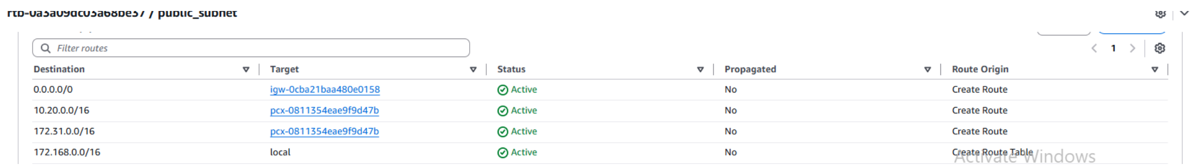
- Attach your VPC to the TGW.
- Select 1 subnet per AZ.

▯ Association happens automatically

- No need to change anything here.

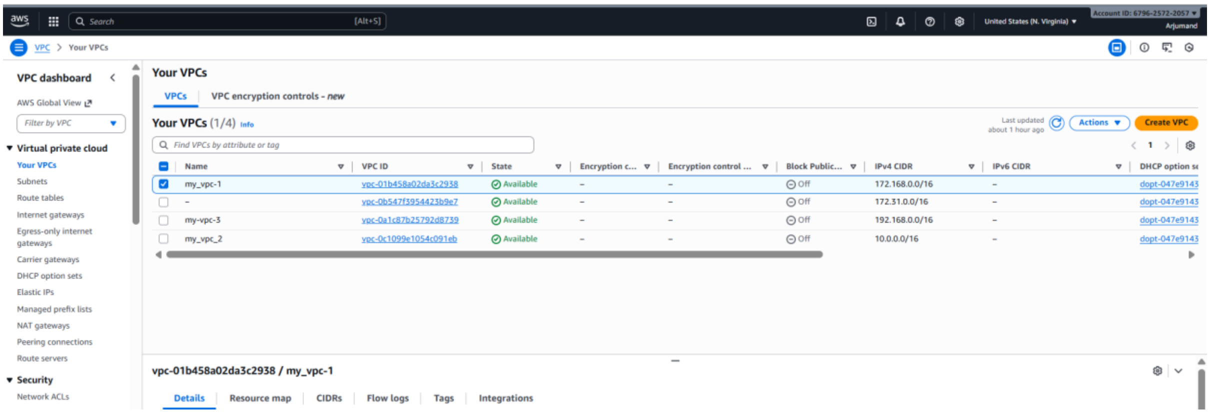
▯ Update VPC Route Table

- Add route → Destination = other VPC CIDR
- Target = **Transit Gateway**



rtb-0a3a09dc03a68be37 / public_subnet

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0cba21baa480e0158	Active	No	Create Route
10.20.0.0/16	pcx-0811354eae9f9d47b	Active	No	Create Route
172.31.0.0/16	pcx-0811354eae9f9d47b	Active	No	Create Route
172.168.0.0/16	local	Active	No	Create Route Table

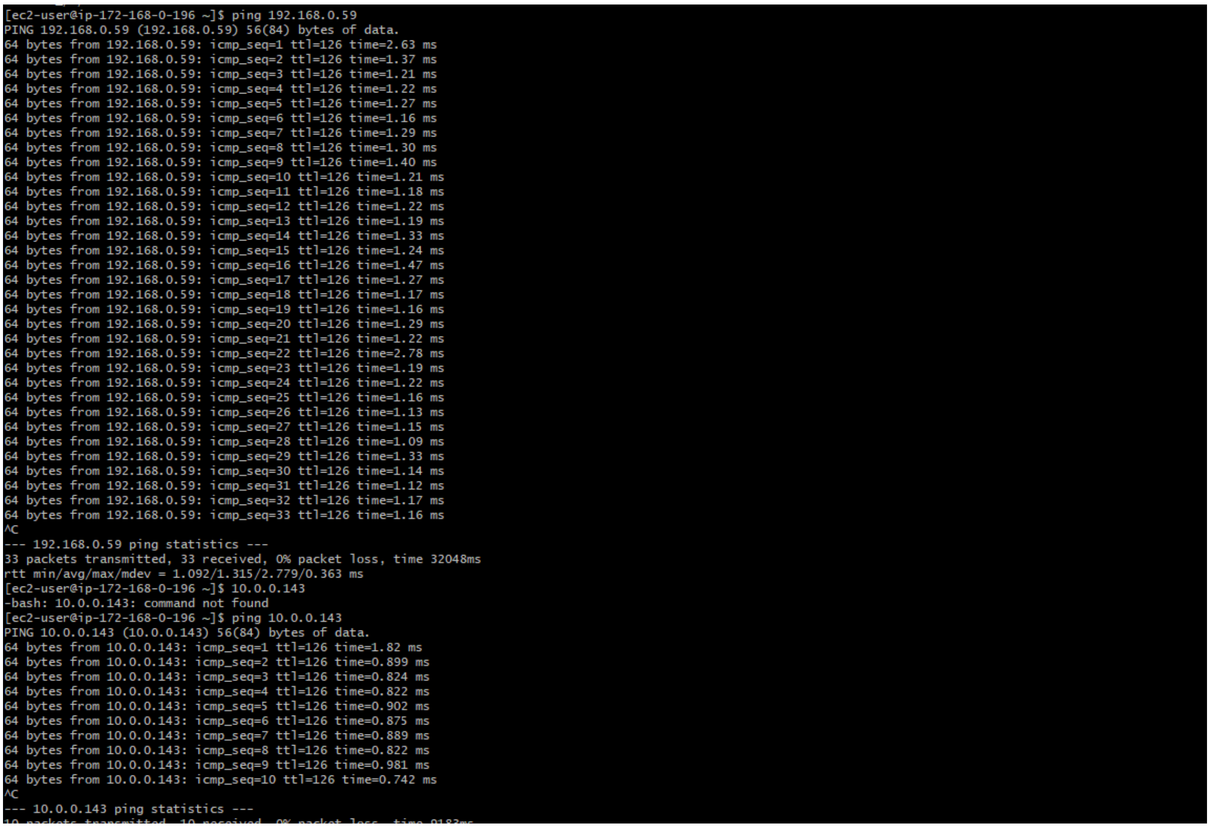


Your VPCs

Your VPCs (1/4) Info

	Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option se
☑	my_vpc-1	vpc-01b458a02da3c2938	Available	–	–	Off	172.168.0.0/16	–	dopt-047e9143
□	–	vpc-0b547f3954423b9e7	Available	–	–	Off	172.31.0.0/16	–	dopt-047e9143
□	my-vpc-3	vpc-0a1c87b25792d8739	Available	–	–	Off	192.168.0.0/16	–	dopt-047e9143
□	my_vpc_2	vpc-0c1099e1054c091eb	Available	–	–	Off	10.0.0.0/16	–	dopt-047e9143

vpc-01b458a02da3c2938 / my_vpc-1

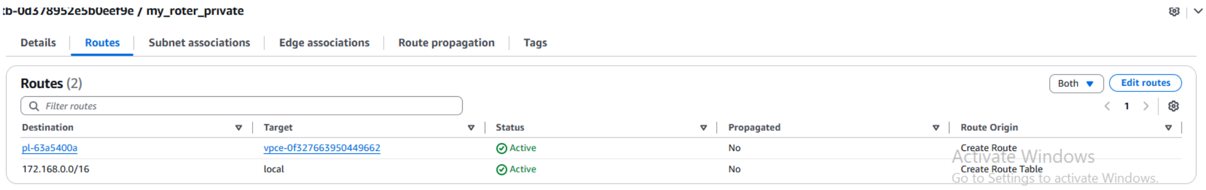


```
[ec2-user@ip-172-168-0-196 ~]$ ping 192.168.0.59
PING 192.168.0.59 (192.168.0.59) 56(84) bytes of data.
64 bytes from 192.168.0.59: icmp_seq=1 ttl=126 time=2.63 ms
64 bytes from 192.168.0.59: icmp_seq=2 ttl=126 time=1.37 ms
64 bytes from 192.168.0.59: icmp_seq=3 ttl=126 time=1.21 ms
64 bytes from 192.168.0.59: icmp_seq=4 ttl=126 time=1.22 ms
64 bytes from 192.168.0.59: icmp_seq=5 ttl=126 time=1.27 ms
64 bytes from 192.168.0.59: icmp_seq=6 ttl=126 time=1.16 ms
64 bytes from 192.168.0.59: icmp_seq=7 ttl=126 time=1.29 ms
64 bytes from 192.168.0.59: icmp_seq=8 ttl=126 time=1.30 ms
64 bytes from 192.168.0.59: icmp_seq=9 ttl=126 time=1.40 ms
64 bytes from 192.168.0.59: icmp_seq=10 ttl=126 time=1.21 ms
64 bytes from 192.168.0.59: icmp_seq=11 ttl=126 time=1.18 ms
64 bytes from 192.168.0.59: icmp_seq=12 ttl=126 time=1.22 ms
64 bytes from 192.168.0.59: icmp_seq=13 ttl=126 time=1.19 ms
64 bytes from 192.168.0.59: icmp_seq=14 ttl=126 time=1.33 ms
64 bytes from 192.168.0.59: icmp_seq=15 ttl=126 time=1.24 ms
64 bytes from 192.168.0.59: icmp_seq=16 ttl=126 time=1.47 ms
64 bytes from 192.168.0.59: icmp_seq=17 ttl=126 time=1.27 ms
64 bytes from 192.168.0.59: icmp_seq=18 ttl=126 time=1.17 ms
64 bytes from 192.168.0.59: icmp_seq=19 ttl=126 time=1.16 ms
64 bytes from 192.168.0.59: icmp_seq=20 ttl=126 time=1.29 ms
64 bytes from 192.168.0.59: icmp_seq=21 ttl=126 time=1.22 ms
64 bytes from 192.168.0.59: icmp_seq=22 ttl=126 time=2.78 ms
64 bytes from 192.168.0.59: icmp_seq=23 ttl=126 time=1.19 ms
64 bytes from 192.168.0.59: icmp_seq=24 ttl=126 time=1.22 ms
64 bytes from 192.168.0.59: icmp_seq=25 ttl=126 time=1.16 ms
64 bytes from 192.168.0.59: icmp_seq=26 ttl=126 time=1.13 ms
64 bytes from 192.168.0.59: icmp_seq=27 ttl=126 time=1.15 ms
64 bytes from 192.168.0.59: icmp_seq=28 ttl=126 time=1.09 ms
64 bytes from 192.168.0.59: icmp_seq=29 ttl=126 time=1.33 ms
64 bytes from 192.168.0.59: icmp_seq=30 ttl=126 time=1.14 ms
64 bytes from 192.168.0.59: icmp_seq=31 ttl=126 time=1.12 ms
64 bytes from 192.168.0.59: icmp_seq=32 ttl=126 time=1.17 ms
64 bytes from 192.168.0.59: icmp_seq=33 ttl=126 time=1.16 ms
^C
--- 192.168.0.59 ping statistics ---
33 packets transmitted, 33 received, 0% packet loss, time 32048ms
rtt min/avg/max/mdev = 1.092/1.315/2.779/0.363 ms
[ec2-user@ip-172-168-0-196 ~]$ 10.0.0.143
-bash: 10.0.0.143: command not found
[ec2-user@ip-172-168-0-196 ~]$ ping 10.0.0.143
PING 10.0.0.143 (10.0.0.143) 56(84) bytes of data.
64 bytes from 10.0.0.143: icmp_seq=1 ttl=126 time=1.82 ms
64 bytes from 10.0.0.143: icmp_seq=2 ttl=126 time=0.899 ms
64 bytes from 10.0.0.143: icmp_seq=3 ttl=126 time=0.824 ms
64 bytes from 10.0.0.143: icmp_seq=4 ttl=126 time=0.822 ms
64 bytes from 10.0.0.143: icmp_seq=5 ttl=126 time=0.902 ms
64 bytes from 10.0.0.143: icmp_seq=6 ttl=126 time=0.875 ms
64 bytes from 10.0.0.143: icmp_seq=7 ttl=126 time=0.889 ms
64 bytes from 10.0.0.143: icmp_seq=8 ttl=126 time=0.822 ms
64 bytes from 10.0.0.143: icmp_seq=9 ttl=126 time=0.981 ms
64 bytes from 10.0.0.143: icmp_seq=10 ttl=126 time=0.742 ms
^C
--- 10.0.0.143 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9183ms
```

5. Set up a VPC Endpoint.

- **Go to VPC → Endpoints → Create Endpoint**

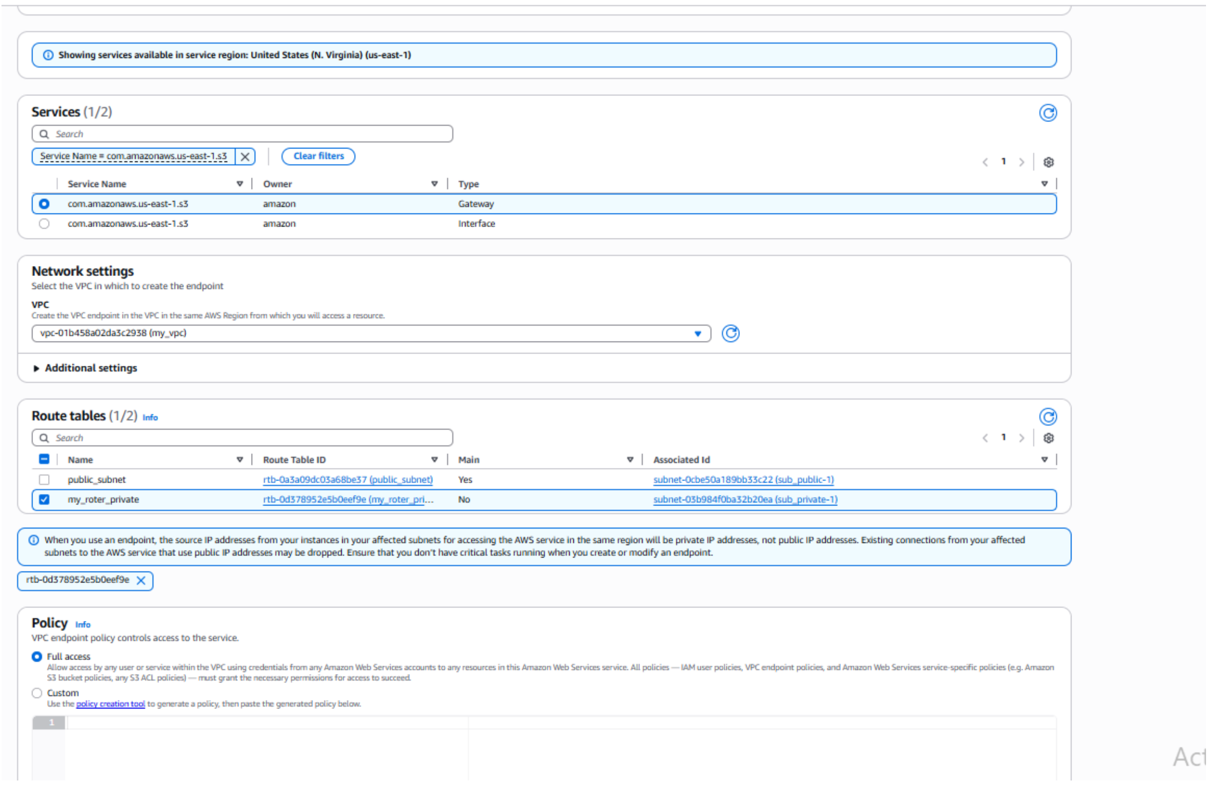
- **Choose service:**
  `com.amazonaws.<region>.s3` (Gateway type)
- **Selected my VPC**
- **Selected ONLY private route table**
- **Policy → Full Access**
- **Created Endpoint**



:b-0d378952e5b0eef9e / my_roter_private

Routes (2)

Destination	Target	Status	Propagated	Route Origin
pl-63a5400a	vpce-0f327663950449662	✓ Active	No	Create Route
172.168.0.0/16	local	✓ Active	No	Create Route Table



ⓘ Showing services available in service region: United States (N. Virginia) (us-east-1)

Services (1/2)

Service Name = com.amazonaws.us-east-1.s3

	Service Name	Owner	Type
●	com.amazonaws.us-east-1.s3	amazon	Gateway
○	com.amazonaws.us-east-1.s3	amazon	Interface

Network settings

Select the VPC in which to create the endpoint

VPC

Create the VPC endpoint in the VPC in the same AWS Region from which you will access a resource.

vpc-01b458a02da3c2938 (my_vpc)

▸ Additional settings

Route tables (1/2) Info

	Name	Route Table ID	Main	Associated Id
□	public_subnet	rtb-0a3a09dc03a68be37 (public_subnet)	Yes	subnet-0cbe50a189bb33c22 (sub_public-1)
☑	my_roter_private	rtb-0d378952e5b0eef9e (my_roter_pri...	No	subnet-03b984f0ba32b20ea (sub_private-1)

ⓘ When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

rtb-0d378952e5b0eef9e ✕

Policy Info

VPC endpoint policy controls access to the service.

● Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.