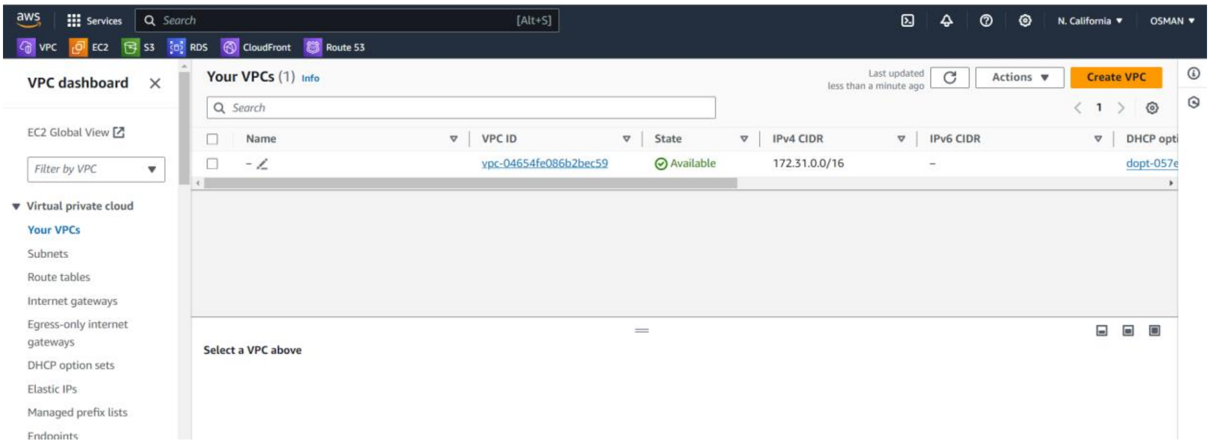
1) Create one VPC, with 1 one public subnet and 1 private subnet.

- To Create Vpc go to the AWS Console search for vpc.
- Just click on create vpc.

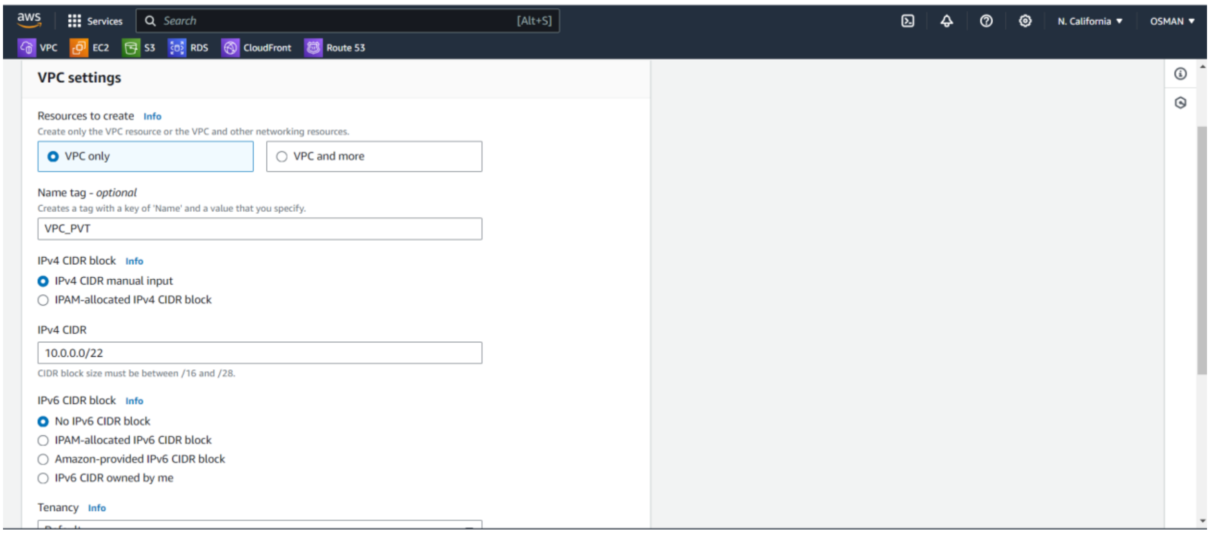


Your VPCs (1) Info

□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opti
□	–	vpc-04654fe086b2bec59	Available	172.31.0.0/16	–	dopt-057e

Select a VPC above

- You will see below the interface.
- Here Two options are
- VPC only ---- here we have to all subnets, route table, internet Gateway, these all things we have do manually
- Vpc more --- AWS will create for us all thing no need to worry.
- Based on requirement select.



VPC settings

Resources to create
Create only the VPC resource or the VPC and other networking resources.
● VPC only ○ VPC and more

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

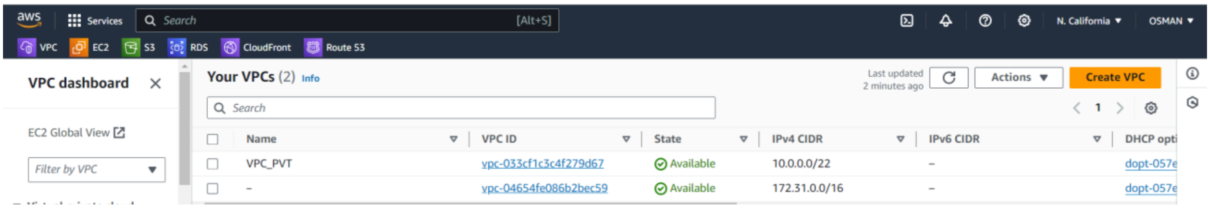
IPv4 CIDR block
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/22
CIDR block size must be between /16 and /28.

IPv6 CIDR block
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy

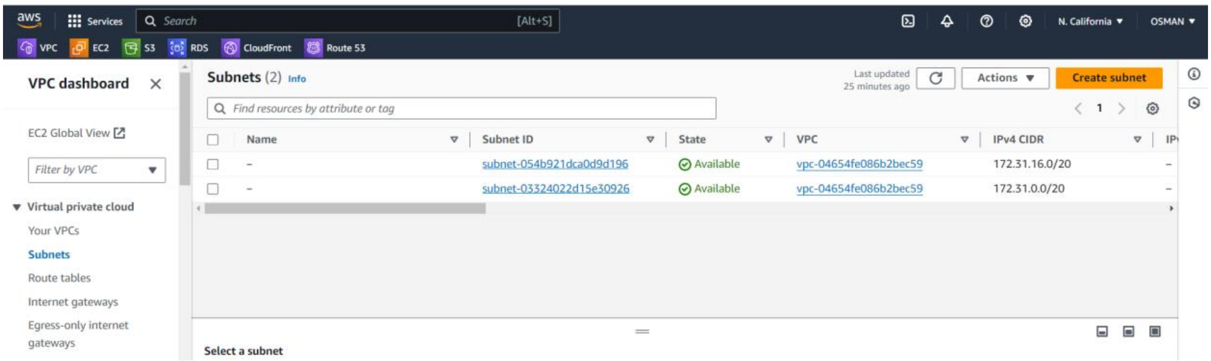
- Scroll down and Click on Create vpc.
- My VPC Created.



Your VPCs (2) Info

□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opti
□	VPC_PVT	vpc-033cf1c3c4f279d67	Available	10.0.0.0/22	–	dopt-057e
□	–	vpc-04654fe086b2bec59	Available	172.31.0.0/16	–	dopt-057e

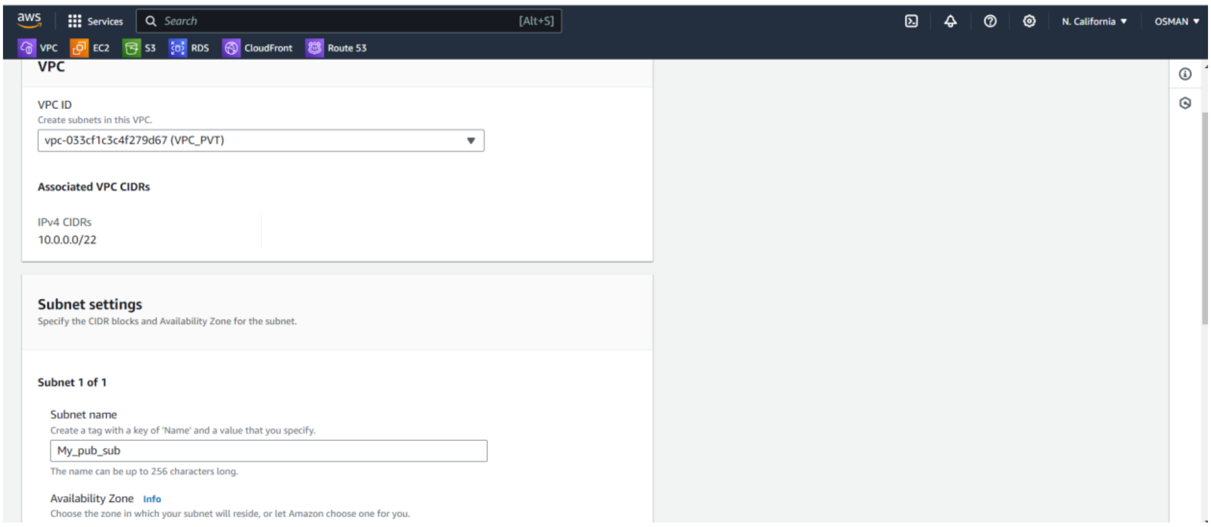
- Now go to the subnets create one Pub-sub And Pvt-sub.
- Left side you will see the option is subnets click and click on create subnet on right top.



Subnets (2)

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	IP
☐	–	subnet-054b921dca0d9d196	✓ Available	vpc-04654fe086b2bec59	172.31.16.0/20	–
☐	–	subnet-03324022d15e30926	✓ Available	vpc-04654fe086b2bec59	172.31.0.0/20	–

- You will see the below interface.
- Select vpc and give subnet name.



VPC

VPC ID
Create subnets in this VPC.
vpc-033cf1c3c4f279d67 (VPC_PVT) ▾

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/22

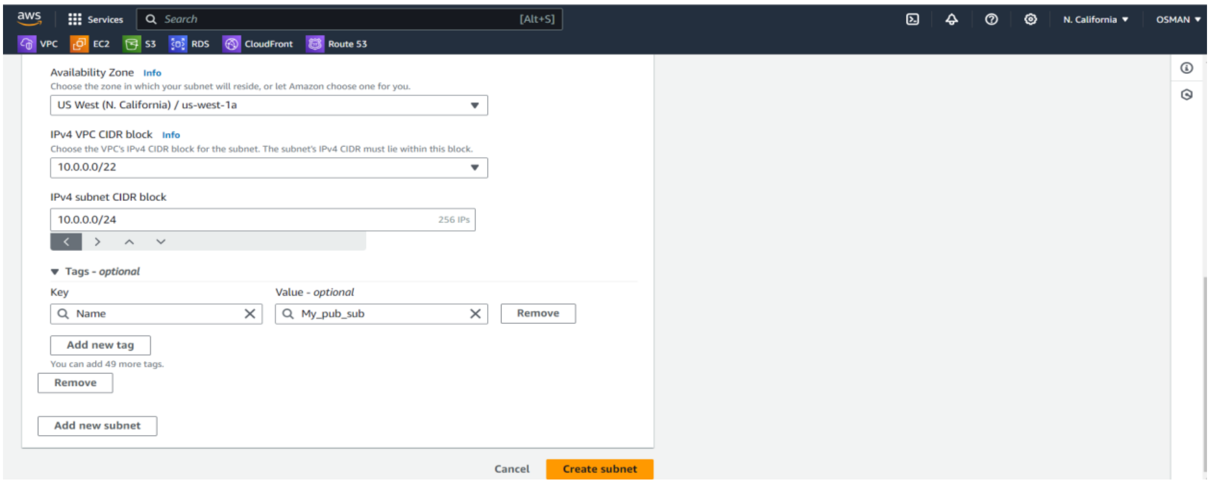
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
My_pub_sub
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

- If you want any specific AZ select that one.
- After give the subnet cidr Block.
- Just click on create subnet.



Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (N. California) / us-west-1a ▾

IPv4 VPC CIDR block
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/22 ▾

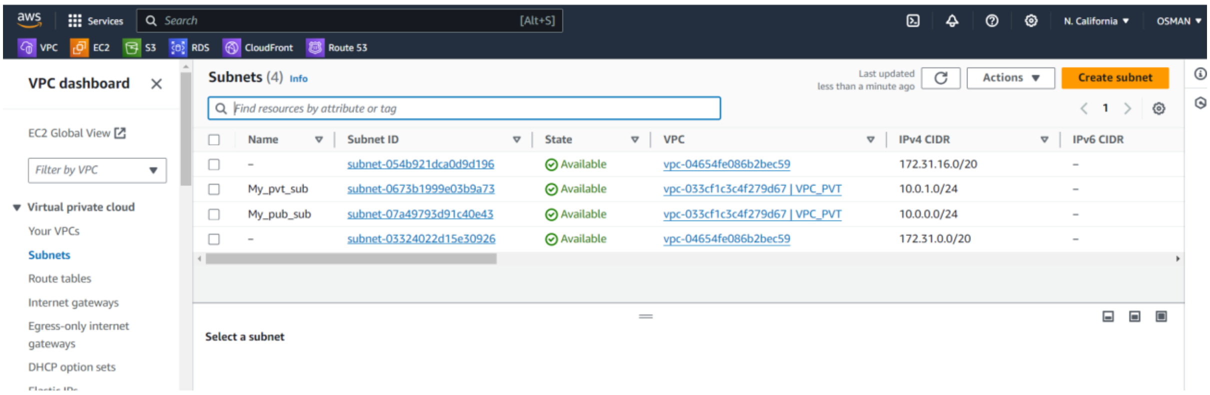
IPv4 subnet CIDR block
10.0.0.0/24 256 IPs

▾ Tags - *optional*

Key	Value - *optional*
Name	My_pub_sub

You can add 49 more tags.

- Create another subnet as private.
- Just change the Name and Cidr range --- 10.0.1.0/24
- Then click on create subnet.
- The below img you will see the my pub and private subnet are created.

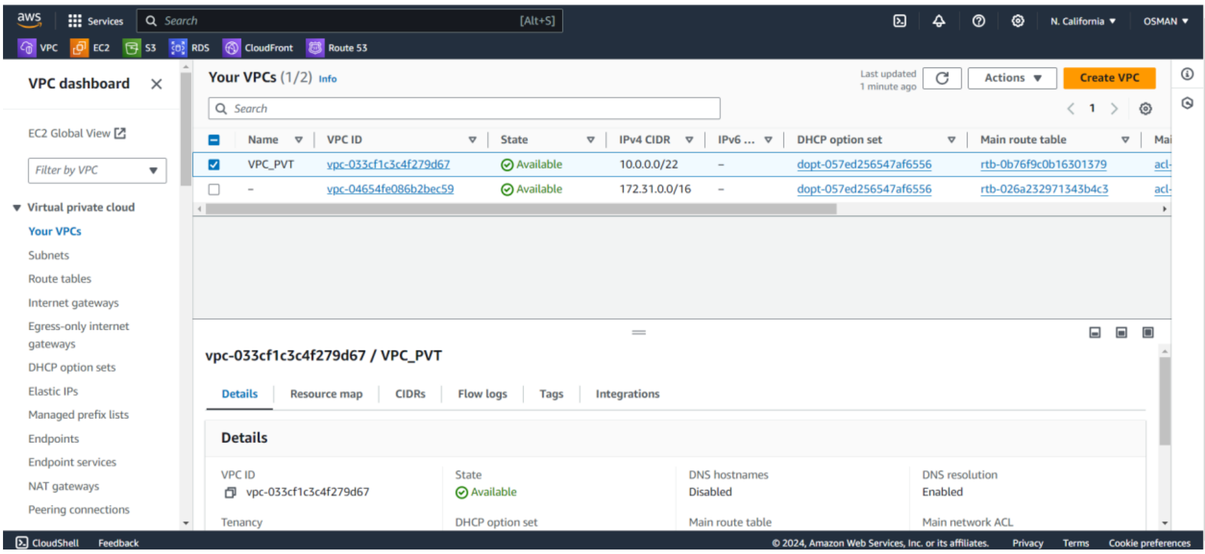


Subnets (4) Info

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
□	–	subnet-054b921dca0d9d196	Available	vpc-04654fe086b2bec59	172.31.16.0/20	–
□	My_pvt_sub	subnet-0673b1999e03b9a73	Available	vpc-033cf1c3c4f279d67 | VPC_PVT	10.0.1.0/24	–
□	My_pub_sub	subnet-07a49793d91c40e43	Available	vpc-033cf1c3c4f279d67 | VPC_PVT	10.0.0.0/24	–
□	–	subnet-03324022d15e30926	Available	vpc-04654fe086b2bec59	172.31.0.0/20	–

2) Enable VPC peering for cross region.

1) Now I have two VPC's in n.california.



Your VPCs (1/2) Info

	Name	VPC ID	State	IPv4 CIDR	IPv6 ...	DHCP option set	Main route table	Mai
☑	VPC_PVT	vpc-033cf1c3c4f279d67	Available	10.0.0.0/22	–	dopt-057ed256547af6556	rtb-0b76f9c0b16301379	acl-
□	–	vpc-04654fe086b2bec59	Available	172.31.0.0/16	–	dopt-057ed256547af6556	rtb-026a232971343b4c3	acl-

vpc-033cf1c3c4f279d67 / VPC_PVT

Details

VPC ID: vpc-033cf1c3c4f279d67
State: Available
DNS hostnames: Disabled
DNS resolution: Enabled
Tenancy
DHCP option set
Main route table
Main network ACL

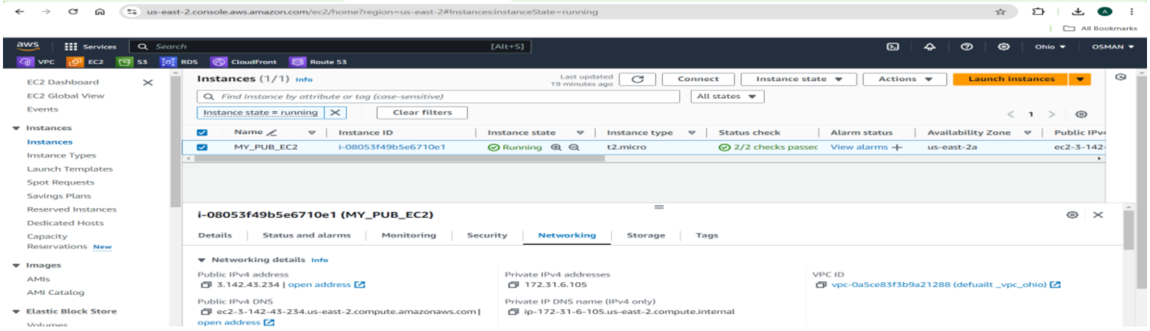
2) In ohio region I have one default vpc that will be default one is there.

3) Within the region pub server only connected.

4) Different region's not Connect even pub servers also.

5) Now I am trying to connect ohio region to N.california.

6) Ohio PUB_server TO N.california Pub_server.



Instances (1/1) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv
☑	MY_PUB_EC2	i-08053f49b5e6710e1	Running	t2.micro	2/2 checks passec	View alarms +	us-east-2a	ec2-3-142-

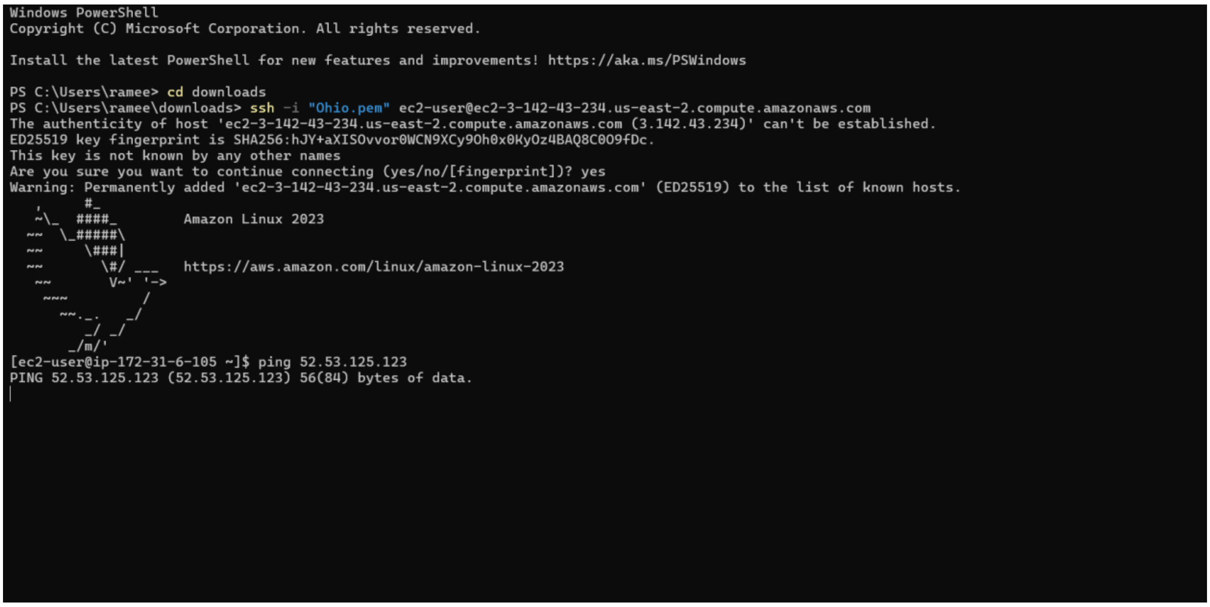
i-08053f49b5e6710e1 (MY_PUB_EC2)

Networking details Info

Public IPv4 address: 3.142.43.234 | open address
Private IPv4 addresses: 172.31.6.105
VPC ID: vpc-0a5ce83f3b9a21288 (defuailt _vpc_ohio)
Public IPv4 DNS: ec2-3-142-43-234.us-east-2.compute.amazonaws.com | open address
Private IP DNS name (IPv4 only): ip-172-31-6-105.us-east-2.compute.internal

Now connect ec2 instance off ohio server try to to communicate n.california server.

The server not communicate.



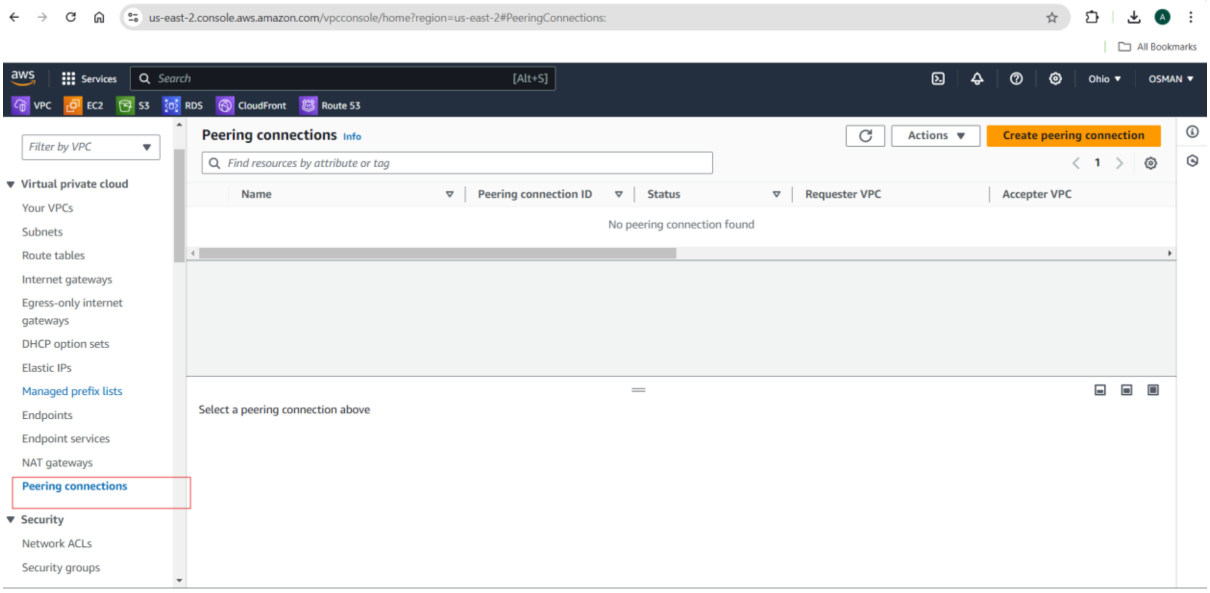
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ramee> cd downloads
PS C:\Users\ramee\downloads> ssh -i "Ohio.pem" ec2-user@ec2-3-142-43-234.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-3-142-43-234.us-east-2.compute.amazonaws.com (3.142.43.234)' can't be established.
ED25519 key fingerprint is SHA256:hJY+aXISOvvor0WCN9XCy9Oh0x0KyOz4BAQ8C0O9fDc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-142-43-234.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/'
[ec2-user@ip-172-31-6-105 ~]$ ping 52.53.125.123
PING 52.53.125.123 (52.53.125.123) 56(84) bytes of data.
```

Now go to the Vpc peering.

Click on Create peering connection.



us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#PeeringConnections:

Name	Peering connection ID	Status	Requester VPC	Accepter VPC

No peering connection found

Select a peering connection above

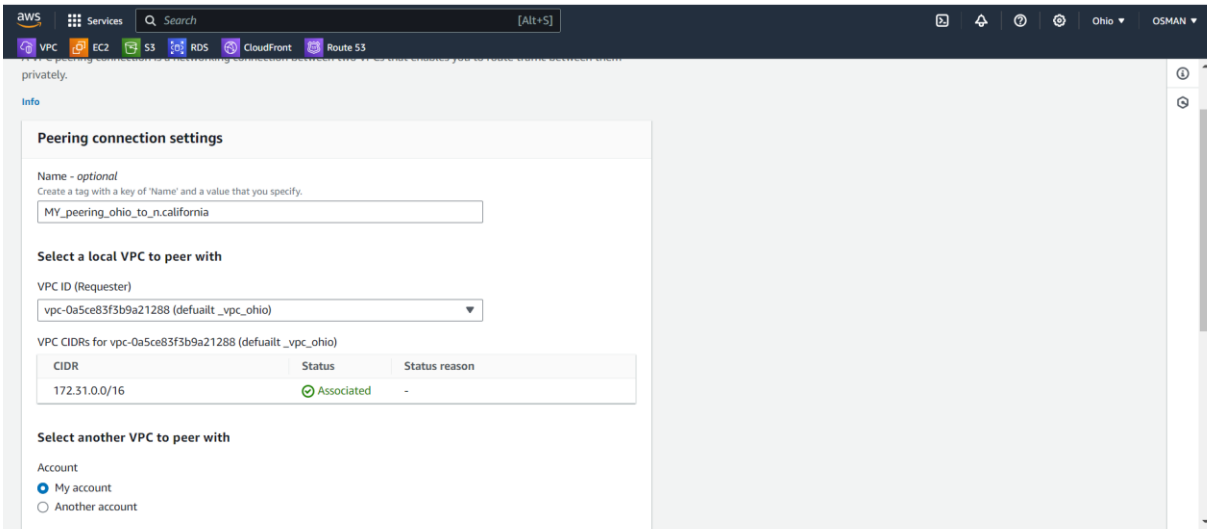
Then you will be seen the below interface.

Steps:

Give name

VPC ID ---- select the requester

Select the another vpc to peer with----- here select account your or another account.



privately.

Peering connection settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

MY_peering_ohio_to_n.california

Select a local VPC to peer with

VPC ID (Requester)

vpc-0a5ce83f3b9a21288 (defuailt _vpc_ohio)

VPC CIDRs for vpc-0a5ce83f3b9a21288 (defuailt _vpc_ohio)

CIDR	Status	Status reason
172.31.0.0/16	✓ Associated	-

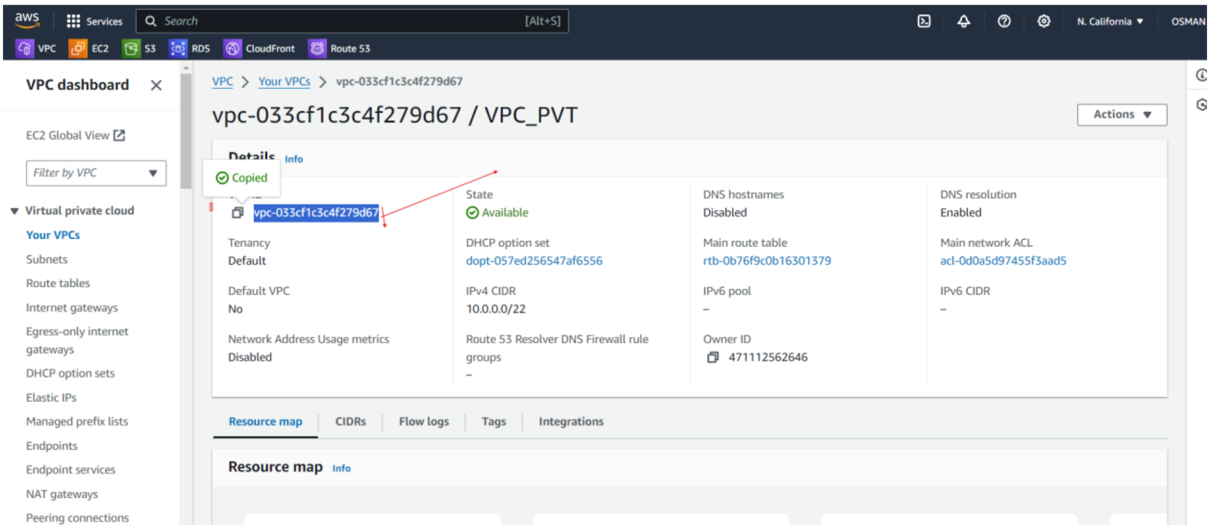
Select another VPC to peer with

Account

● My account

○ Another account

Go to the n.california copy the vpc id.



VPC > Your VPCs > vpc-033cf1c3c4f279d67

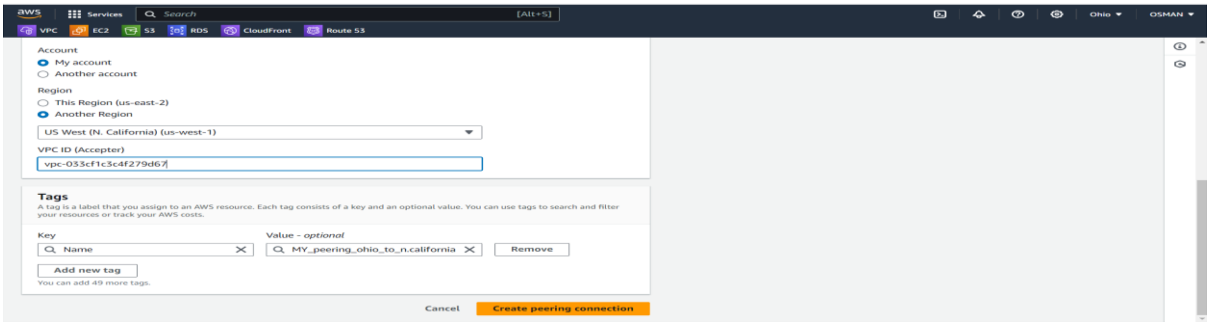
vpc-033cf1c3c4f279d67 / VPC_PVT

Details

✓ Copied

vpc-033cf1c3c4f279d67	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-057ed256547af6556	Main route table rtb-0b76f9c0b16301379	Main network ACL acl-0d0a5d97455f3aad5
Default VPC No	IPv4 CIDR 10.0.0.0/22	IPv6 pool –	IPv6 CIDR –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 471112562646	

Paste here and click on vpc peering.



Account

● My account

○ Another account

Region

○ This Region (us-east-2)

● Another Region

US West (N. California) (us-west-1)

VPC ID (Accepter)

vpc-033cf1c3c4f279d67

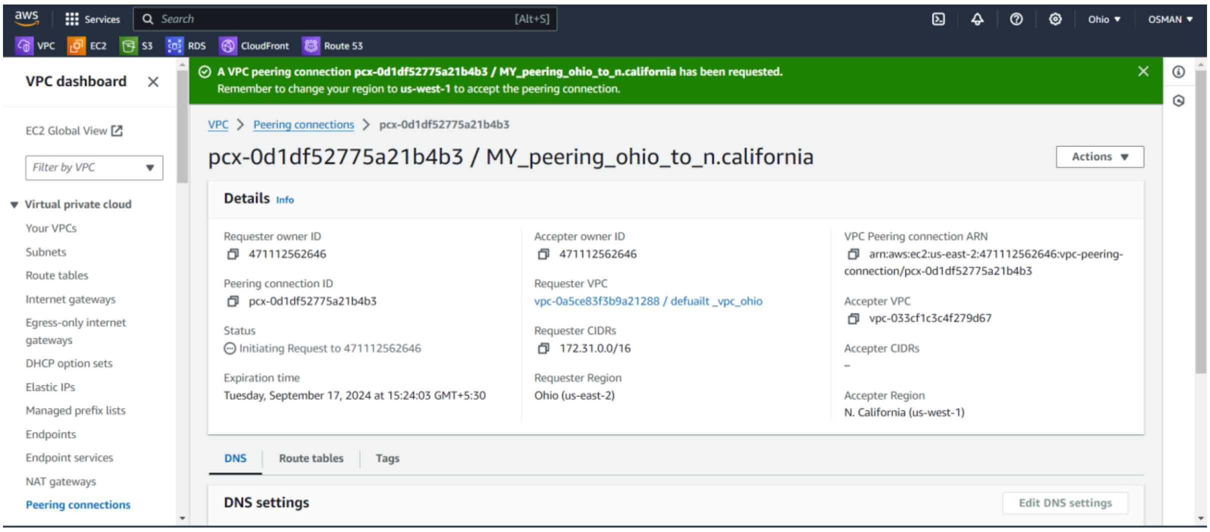
Tags

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_peering_ohio_to_n.california

You can add 49 more tags.

Now the Request goes to n.california.



A VPC peering connection pcx-0d1df52775a21b4b3 / MY_peering_ohio_to_n.california has been requested.
Remember to change your region to us-west-1 to accept the peering connection.

VPC > Peering connections > pcx-0d1df52775a21b4b3

pcx-0d1df52775a21b4b3 / MY_peering_ohio_to_n.california

Details Info

Requester owner ID: 471112562646

Peering connection ID: pcx-0d1df52775a21b4b3

Status: Initiating Request to 471112562646

Expiration time: Tuesday, September 17, 2024 at 15:24:03 GMT+5:30

Accepter owner ID: 471112562646

Requester VPC: vpc-0a5ce83f3b9a21288 / defauilt _vpc_ohio

Requester CIDRs: 172.31.0.0/16

Requester Region: Ohio (us-east-2)

VPC Peering connection ARN: arn:aws:ec2:us-east-2:471112562646:vpc-peering-connection/pcx-0d1df52775a21b4b3

Accepter VPC: vpc-033cf1c3c4f279d67

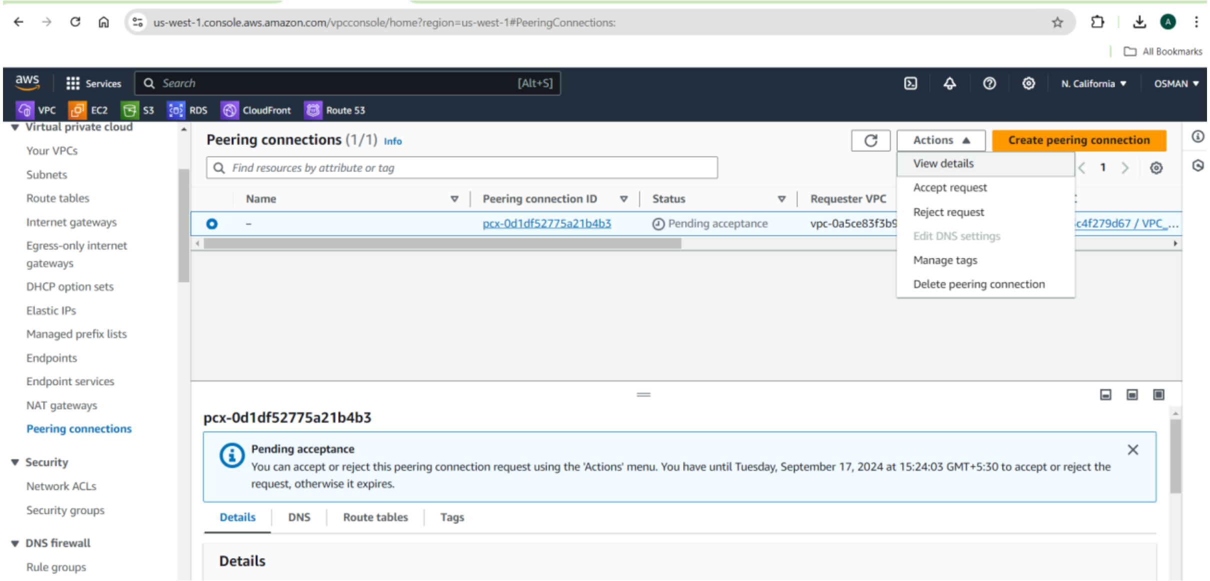
Accepter CIDRs: –

Accepter Region: N. California (us-west-1)

DNS settings

Go to the n.california and accept the request.

Now here we have to accept the request.



Peering connections (1/1) Info

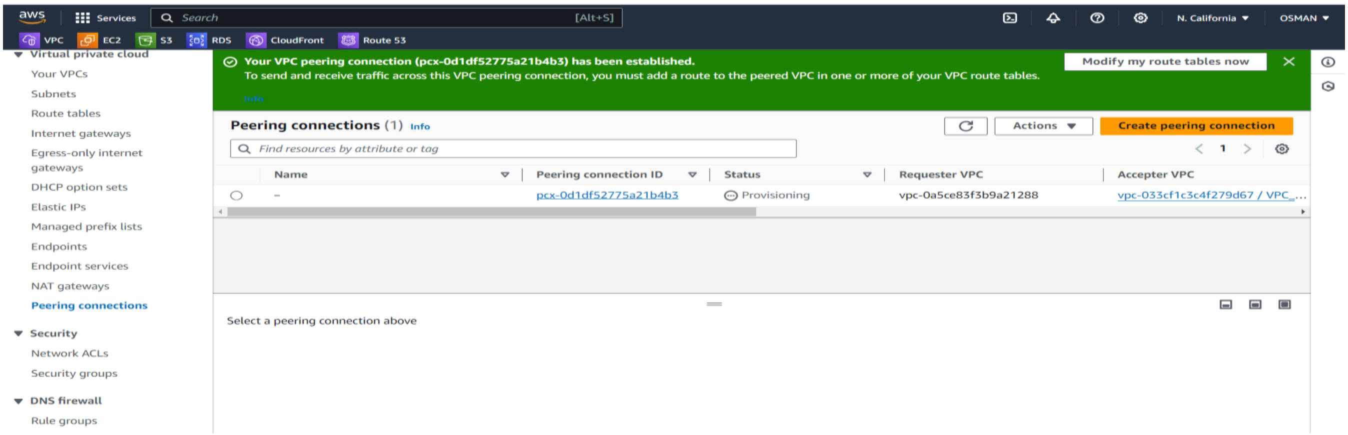
Name	Peering connection ID	Status	Requester VPC	
–	pcx-0d1df52775a21b4b3	Pending acceptance	vpc-0a5ce83f3b9	c4f279d67 / VPC_...

pcx-0d1df52775a21b4b3

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Tuesday, September 17, 2024 at 15:24:03 GMT+5:30 to accept or reject the request, otherwise it expires.

Details

After accept you will see the below interface.



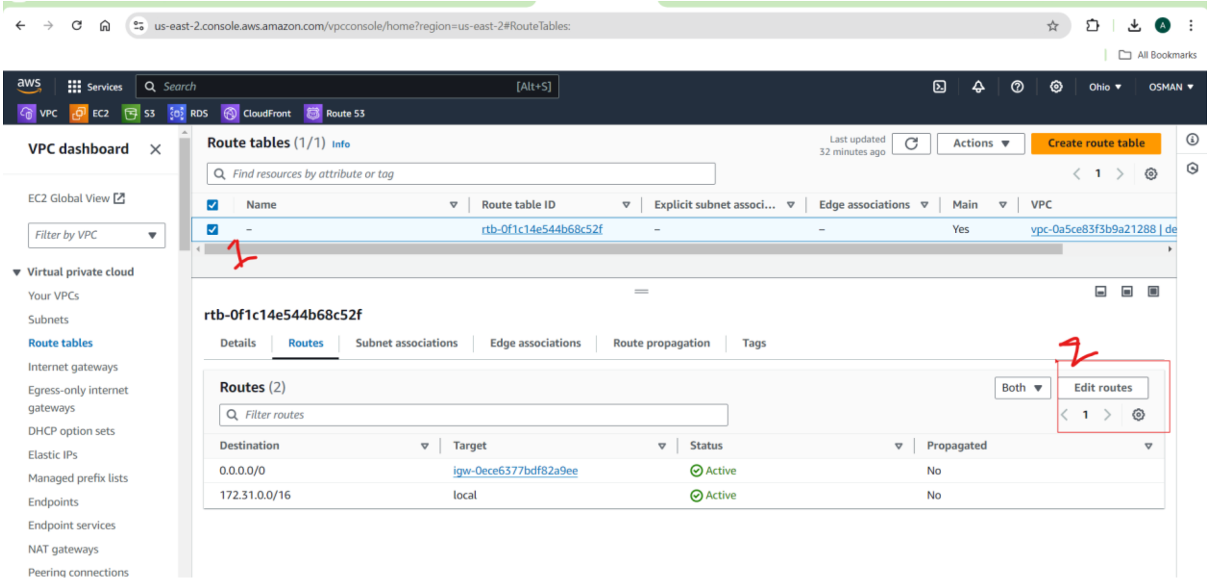
Your VPC peering connection (pcx-0d1df52775a21b4b3) has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables.

Peering connections (1) Info

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
–	pcx-0d1df52775a21b4b3	Provisioning	vpc-0a5ce83f3b9a21288	vpc-033cf1c3c4f279d67 / VPC_...

Select a peering connection above

- Once try to communication is happen or not?
- Now also not communicate because from rout table we not configure.
- So Go to the ohio public rout table and configure n.california vpc cidr range.
- Click on check box and below you see the edit routes and click.



us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#RouteTables:

VPC dashboard

Route tables (1/1) Info

Find resources by attribute or tag

☑	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
☑	–	rtb-0f1c14e544b68c52f	–	–	Yes	vpc-0a5ce83f3b9a21288 | de

1

rtb-0f1c14e544b68c52f

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

2

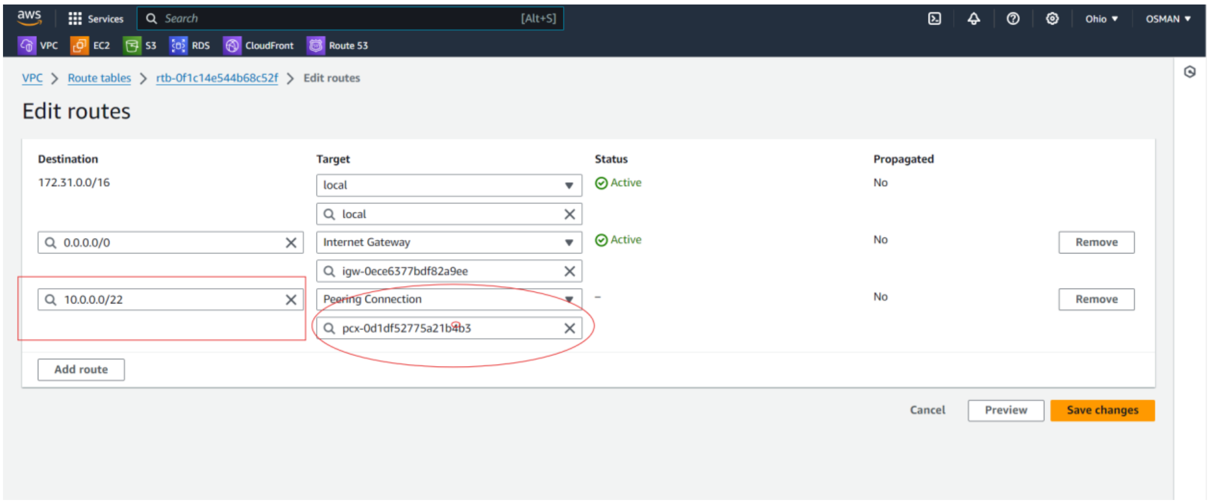
Routes (2)

Filter routes

Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0ece6377bdf82a9ee	Active	No
172.31.0.0/16	local	Active	No

- Copy cidr of n.california and paste below.
- Select peering and select the id of peering connection.
- Save the changes.



VPC > Route tables > rtb-0f1c14e544b68c52f > Edit routes

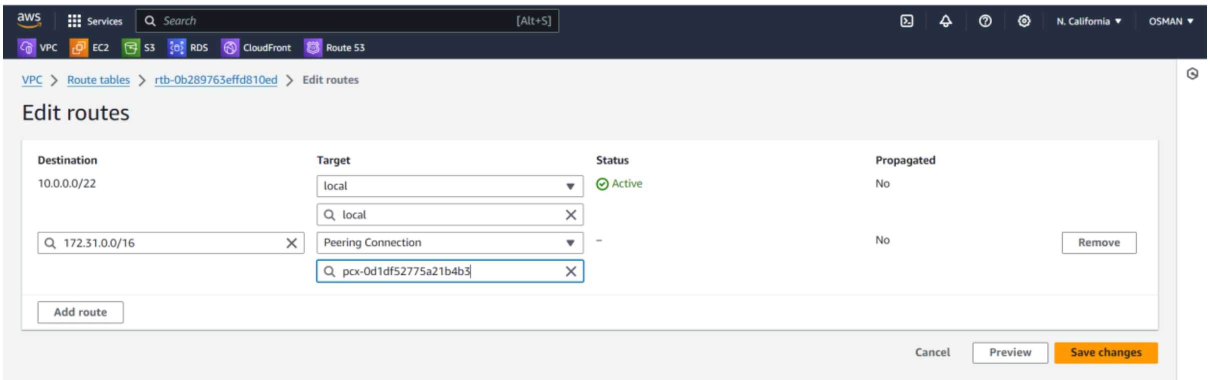
Edit routes

Destination	Target	Status	Propagated	
172.31.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-0ece6377bdf82a9ee	Active	No	Remove
10.0.0.0/22	Peering Connection pcx-0d1df52775a21b4b3	-	No	Remove

Add route

Cancel Preview Save changes

- Now go N.clifornia and configure and change the modification.
- What we did in the configuration like that change.



VPC > Route tables > rtb-0b289763effd810ed > Edit routes

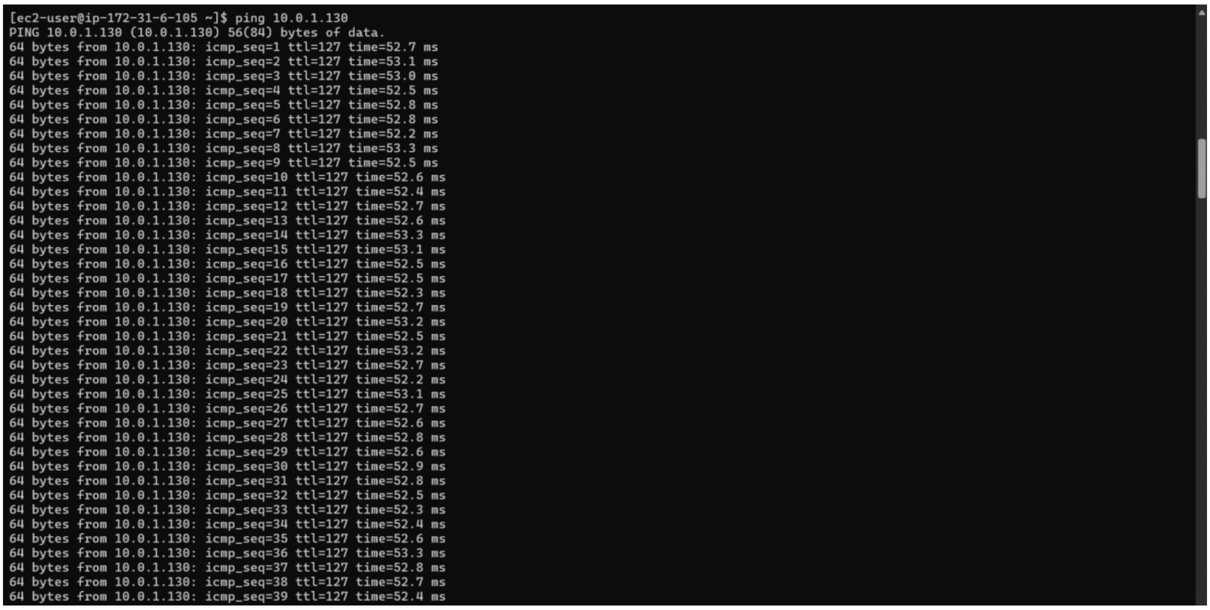
Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/22	local	Active	No	
172.31.0.0/16	Peering Connection pcx-0d1df52775a21b4b3	-	No	Remove

Click on the save the changes.

Now try to connect It will work.

Make sure you ec2 instances security groups is all traffic and anywhere.



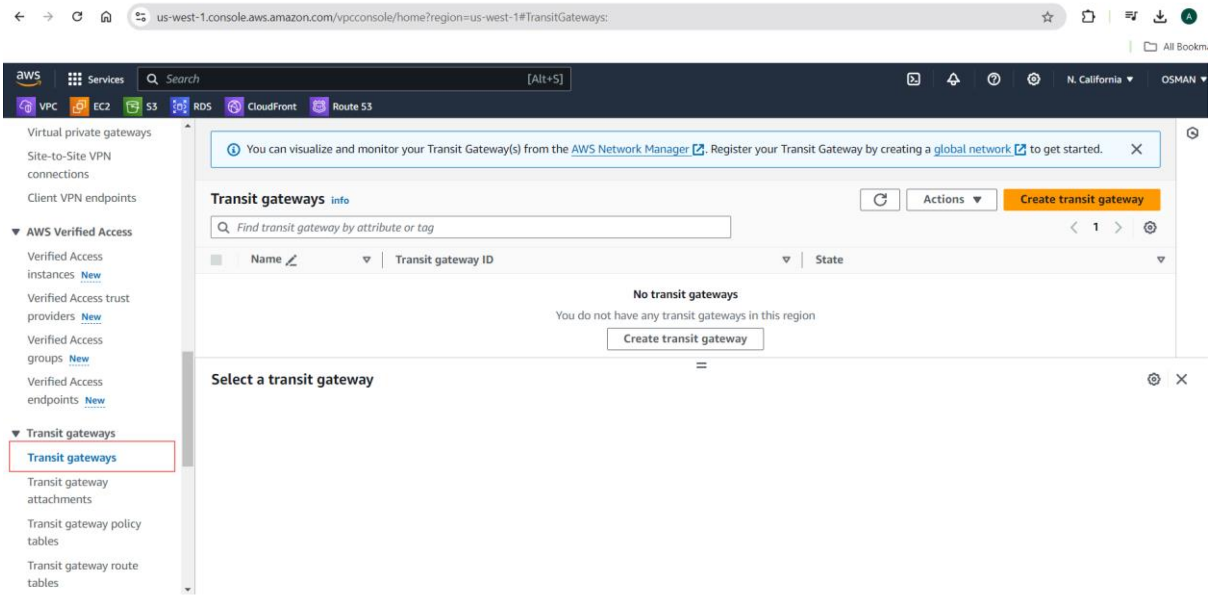
```
[ec2-user@ip-172-31-6-105 ~]$ ping 10.0.1.130
PING 10.0.1.130 (10.0.1.130) 56(84) bytes of data.
64 bytes from 10.0.1.130: icmp_seq=1 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=2 ttl=127 time=53.1 ms
64 bytes from 10.0.1.130: icmp_seq=3 ttl=127 time=53.0 ms
64 bytes from 10.0.1.130: icmp_seq=4 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=5 ttl=127 time=52.8 ms
64 bytes from 10.0.1.130: icmp_seq=6 ttl=127 time=52.8 ms
64 bytes from 10.0.1.130: icmp_seq=7 ttl=127 time=52.2 ms
64 bytes from 10.0.1.130: icmp_seq=8 ttl=127 time=53.3 ms
64 bytes from 10.0.1.130: icmp_seq=9 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=10 ttl=127 time=52.6 ms
64 bytes from 10.0.1.130: icmp_seq=11 ttl=127 time=52.4 ms
64 bytes from 10.0.1.130: icmp_seq=12 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=13 ttl=127 time=52.6 ms
64 bytes from 10.0.1.130: icmp_seq=14 ttl=127 time=53.3 ms
64 bytes from 10.0.1.130: icmp_seq=15 ttl=127 time=53.1 ms
64 bytes from 10.0.1.130: icmp_seq=16 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=17 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=18 ttl=127 time=52.3 ms
64 bytes from 10.0.1.130: icmp_seq=19 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=20 ttl=127 time=53.2 ms
64 bytes from 10.0.1.130: icmp_seq=21 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=22 ttl=127 time=53.2 ms
64 bytes from 10.0.1.130: icmp_seq=23 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=24 ttl=127 time=52.2 ms
64 bytes from 10.0.1.130: icmp_seq=25 ttl=127 time=53.1 ms
64 bytes from 10.0.1.130: icmp_seq=26 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=27 ttl=127 time=52.6 ms
64 bytes from 10.0.1.130: icmp_seq=28 ttl=127 time=52.8 ms
64 bytes from 10.0.1.130: icmp_seq=29 ttl=127 time=52.6 ms
64 bytes from 10.0.1.130: icmp_seq=30 ttl=127 time=52.9 ms
64 bytes from 10.0.1.130: icmp_seq=31 ttl=127 time=52.8 ms
64 bytes from 10.0.1.130: icmp_seq=32 ttl=127 time=52.5 ms
64 bytes from 10.0.1.130: icmp_seq=33 ttl=127 time=52.3 ms
64 bytes from 10.0.1.130: icmp_seq=34 ttl=127 time=52.4 ms
64 bytes from 10.0.1.130: icmp_seq=35 ttl=127 time=52.6 ms
64 bytes from 10.0.1.130: icmp_seq=36 ttl=127 time=53.3 ms
64 bytes from 10.0.1.130: icmp_seq=37 ttl=127 time=52.8 ms
64 bytes from 10.0.1.130: icmp_seq=38 ttl=127 time=52.7 ms
64 bytes from 10.0.1.130: icmp_seq=39 ttl=127 time=52.4 ms
```

7) 3) Enable VPC peering for cross account. (You can collaborate with your friend and do this task).

4) Setup VPC Transist gateway.

- A VPC Transit Gateway is like a central hub or router that helps connect multiple VPCs (Virtual Private Clouds) and even on-premises networks. Instead of connecting VPCs one by one, you connect them all to the gateway.

- To setup transist gateway.
- Go to the transist gateway and top right side click on that create transist gateway.



us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#TransitGateways:

You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

Transit gateways Info

Find transit gateway by attribute or tag

Name	Transit gateway ID	State

No transit gateways

You do not have any transit gateways in this region

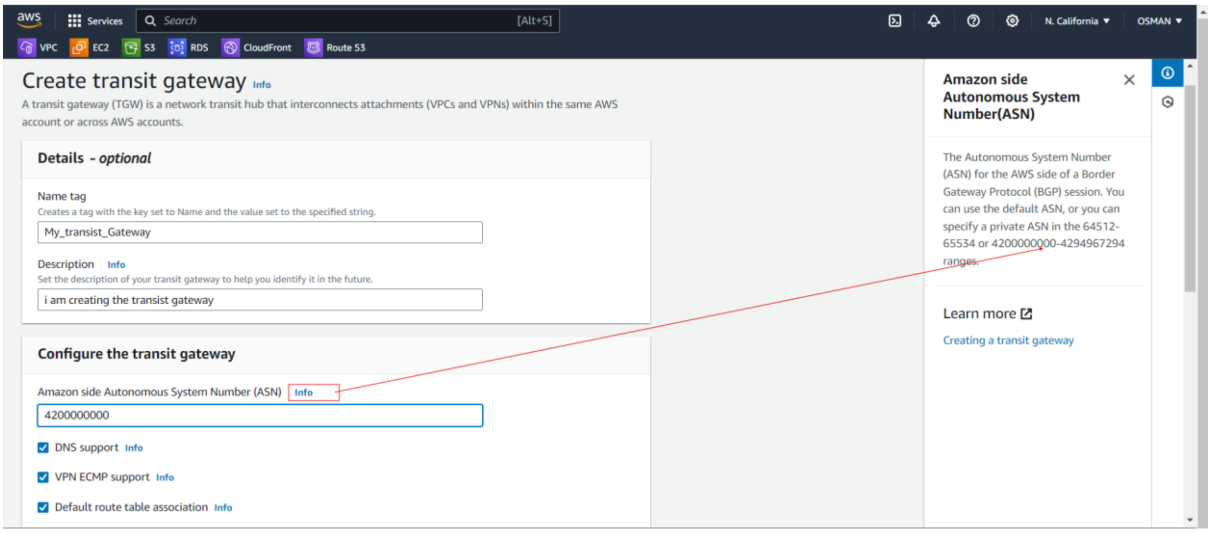
Create transit gateway

Select a transit gateway

All Bookm
aws
Services
Search
[Alt+S]
N. California
OSMAN
VPC
EC2
S3
RDS
CloudFront
Route 53
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Actions
Create transit gateway
1

You will seen below interface and fill .

- Name what you want give
- You just click on the ASN info you wiil get default Number.
- After click on the create transist gate way.
-



Create transit gateway Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details - *optional*

Name tag

Creates a tag with the key set to Name and the value set to the specified string.

My_transit_Gateway

Description Info

Set the description of your transit gateway to help you identify it in the future.

i am creating the transist gateway

Configure the transit gateway

Amazon side Autonomous System Number (ASN) Info

4200000000

☑ DNS support Info

☑ VPN ECMP support Info

☑ Default route table association Info

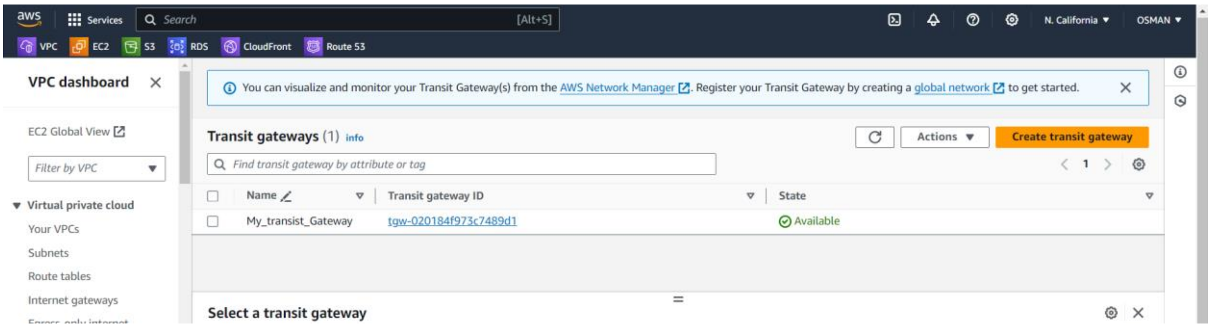
Amazon side Autonomous System Number(ASN)

The Autonomous System Number (ASN) for the AWS side of a Border Gateway Protocol (BGP) session. You can use the default ASN, or you can specify a private ASN in the 64512-65534 or 4200000000-4294967294 ranges.

Learn more

Creating a transit gateway

Transist gateway is available.



ⓘ You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

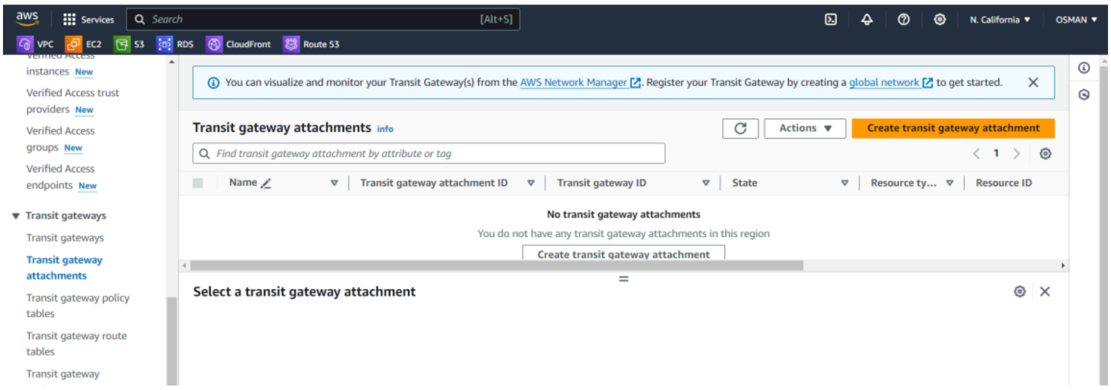
Transit gateways (1) Info

Find transit gateway by attribute or tag

□	Name	Transit gateway ID	State
□	My_transist_Gateway	tgw-020184f973c7489d1	Available

Select a transit gateway

- Now go to transit gateway attachments.
- Click on transit gateway attachments.


aws
Services
Search
[Alt+S]
N. California ▾
OSMAN ▾
VPC
EC2
S3
RDS
CloudFront
Route 53
instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New
▾ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway
Actions ▾
Create transit gateway attachment

ⓘ You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

Transit gateway attachments Info

Find transit gateway attachment by attribute or tag

□	Name	Transit gateway attachment ID	Transit gateway ID	State	Resource ty...	Resource ID

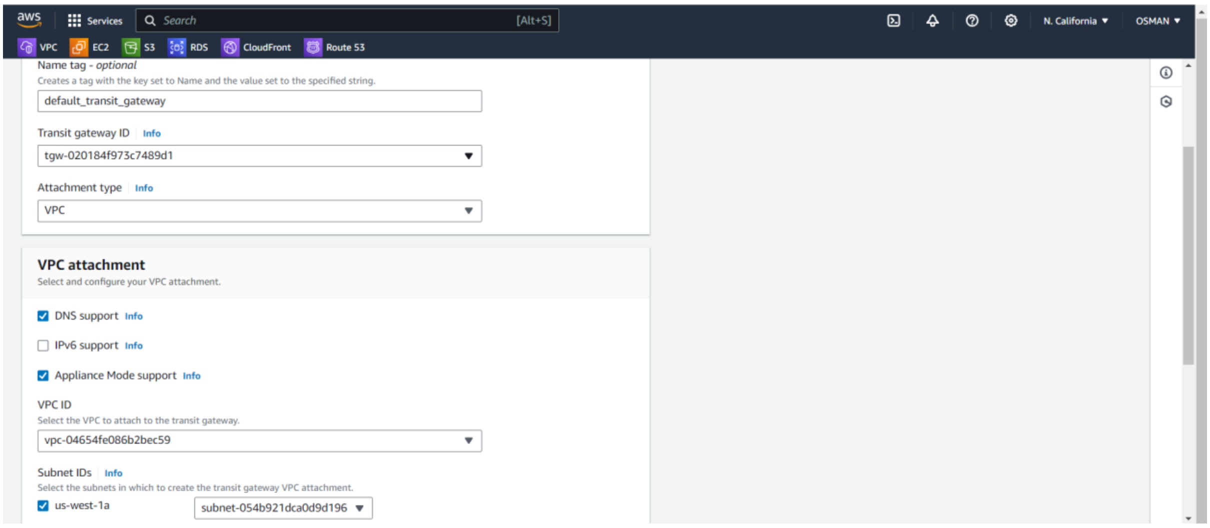
No transit gateway attachments

You do not have any transit gateway attachments in this region

Create transit gateway attachment

Select a transit gateway attachment

- Give transist Gateway Id
- Attachment Type is --- VPC
- VPC Attachment in you have to select the vpc



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

Transit gateway ID Info
tgw-020184f973c7489d1 ▾

Attachment type Info
VPC ▾

VPC attachment
Select and configure your VPC attachment.

☑ DNS support Info

□ IPv6 support Info

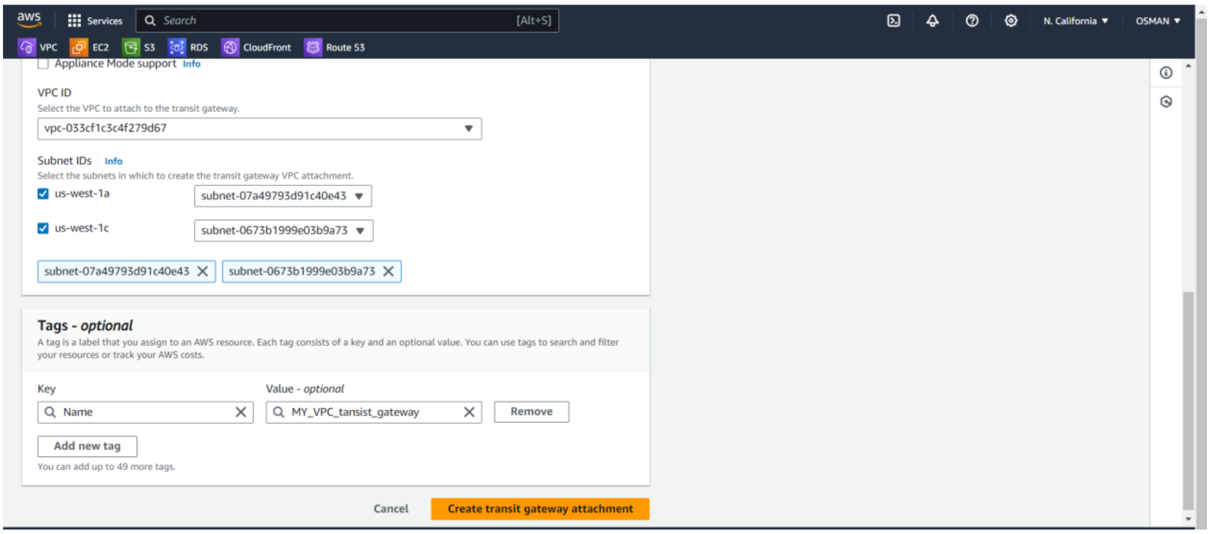
☑ Appliance Mode support Info

VPC ID
Select the VPC to attach to the transit gateway.
vpc-04654fe086b2bec59 ▾

Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.
☑ us-west-1a subnet-054b921dca0d9d196 ▾

- After click on the create tansist gateway attachment.

- Again you have to similar but only change is the vpc attachment you have select another vpc.



□ Appliance Mode support Info

VPC ID
Select the VPC to attach to the transit gateway.
vpc-033cf1c3c4f279d67

Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.
☑ us-west-1a subnet-07a49793d91c40e43
☑ us-west-1c subnet-0673b1999e03b9a73

subnet-07a49793d91c40e43 ✕ subnet-0673b1999e03b9a73 ✕

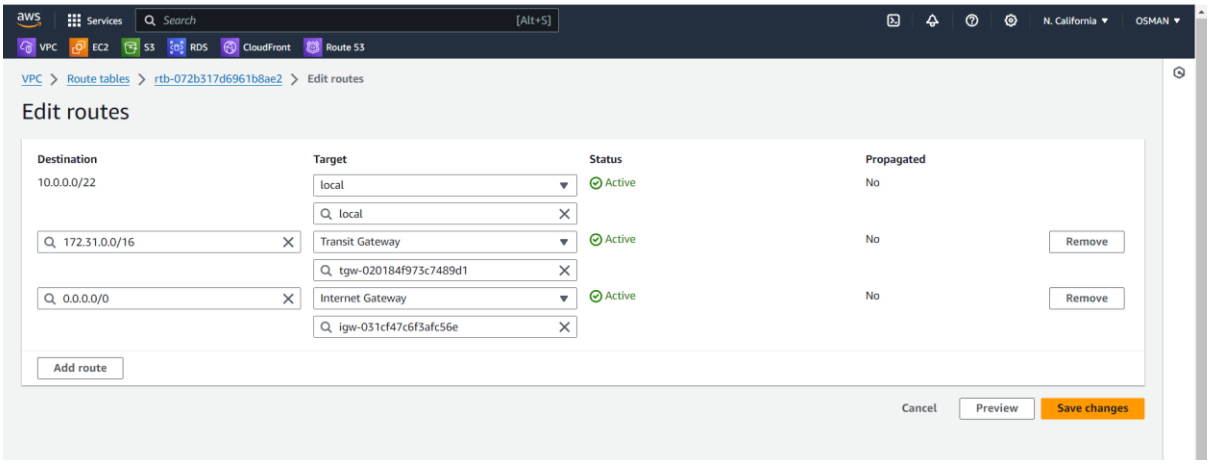
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	MY_VPC_tansist_gateway	Remove

Add new tag
You can add up to 49 more tags.

Cancel Create transit gateway attachment

- Just click on the create transist gateway attachment.
- Go to route table and conifugre the VPC cidr range and attach transist gateway.



VPC > Route tables > rtb-072b317d6961b8ae2 > Edit routes

Edit routes

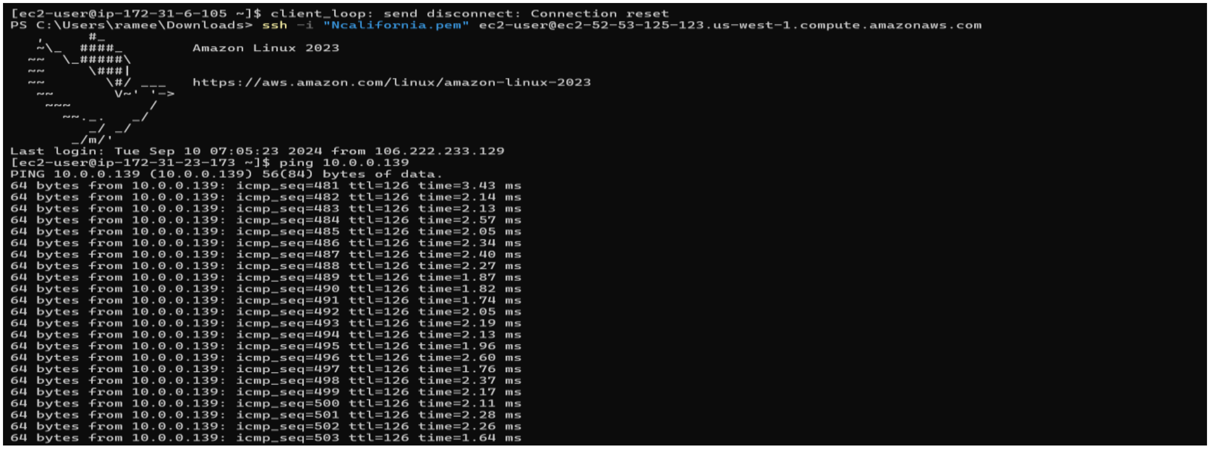
Destination	Target	Status	Propagated	
10.0.0.0/22	local local	Active	No	
172.31.0.0/16	Transit Gateway tgw-020184f973c7489d1	Active	No	Remove
0.0.0.0/0	Internet Gateway igw-031cf47c6f3afc56e	Active	No	Remove

Add route

Cancel Preview Save changes

Changes made in two route tables .

Now you able to communicate.

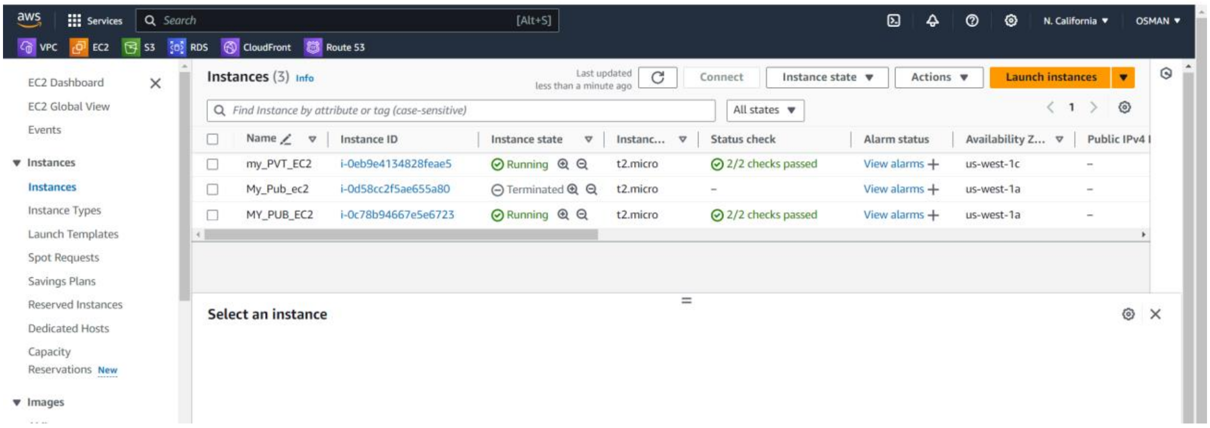


```
[ec2-user@ip-172-31-6-105 ~]$ client_loop: send disconnect: Connection reset
PS C:\Users\ramee\Downloads> ssh -i "Ncalifornia.pem" ec2-user@ec2-52-53-125-123.us-west-1.compute.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Sep 10 07:05:23 2024 from 106.222.233.129
[ec2-user@ip-172-31-23-173 ~]$ ping 10.0.0.139
PING 10.0.0.139 (10.0.0.139) 56(84) bytes of data.
64 bytes from 10.0.0.139: icmp_seq=481 ttl=126 time=3.43 ms
64 bytes from 10.0.0.139: icmp_seq=482 ttl=126 time=2.14 ms
64 bytes from 10.0.0.139: icmp_seq=483 ttl=126 time=2.13 ms
64 bytes from 10.0.0.139: icmp_seq=484 ttl=126 time=2.57 ms
64 bytes from 10.0.0.139: icmp_seq=485 ttl=126 time=2.05 ms
64 bytes from 10.0.0.139: icmp_seq=486 ttl=126 time=2.34 ms
64 bytes from 10.0.0.139: icmp_seq=487 ttl=126 time=2.40 ms
64 bytes from 10.0.0.139: icmp_seq=488 ttl=126 time=2.27 ms
64 bytes from 10.0.0.139: icmp_seq=489 ttl=126 time=1.87 ms
64 bytes from 10.0.0.139: icmp_seq=490 ttl=126 time=1.82 ms
64 bytes from 10.0.0.139: icmp_seq=491 ttl=126 time=1.74 ms
64 bytes from 10.0.0.139: icmp_seq=492 ttl=126 time=2.05 ms
64 bytes from 10.0.0.139: icmp_seq=493 ttl=126 time=2.19 ms
64 bytes from 10.0.0.139: icmp_seq=494 ttl=126 time=2.13 ms
64 bytes from 10.0.0.139: icmp_seq=495 ttl=126 time=1.96 ms
64 bytes from 10.0.0.139: icmp_seq=496 ttl=126 time=2.60 ms
64 bytes from 10.0.0.139: icmp_seq=497 ttl=126 time=1.76 ms
64 bytes from 10.0.0.139: icmp_seq=498 ttl=126 time=2.37 ms
64 bytes from 10.0.0.139: icmp_seq=499 ttl=126 time=2.17 ms
64 bytes from 10.0.0.139: icmp_seq=500 ttl=126 time=2.11 ms
64 bytes from 10.0.0.139: icmp_seq=501 ttl=126 time=2.28 ms
64 bytes from 10.0.0.139: icmp_seq=502 ttl=126 time=2.26 ms
64 bytes from 10.0.0.139: icmp_seq=503 ttl=126 time=1.64 ms
```

5) Setup VPC End Point.

- VPC end point service will help us to communicate with aws services without internet.
- Means the communication will private and will be within the Vpc.
  To do setup vpc.

- Create two EC2-instances
- One is public server and another one is the Private server.

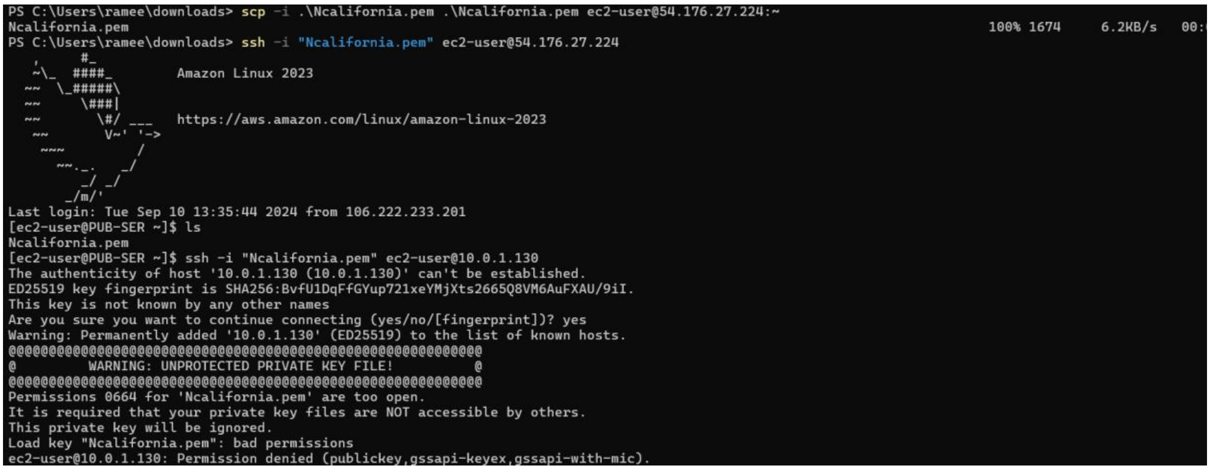


	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability Z...	Public IPv4
□	my_PVT_EC2	i-0eb9e4134828feae5	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1c	–
□	My_Pub_ec2	i-0d58cc2f5ae655a80	Terminated	t2.micro	–	View alarms +	us-west-1a	–
□	MY_PUB_EC2	i-0c78b94667e5e6723	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1a	–

Now connect to the public server.

First I am transfer the pem file local to remote public server.

After I am connecting the instance and change the permissions.



```
PS C:\Users\ramee\downloads> scp -i .\Ncalifornia.pem .\Ncalifornia.pem ec2-user@54.176.27.224:~
Ncalifornia.pem                                                                             100% 1674     6.2KB/s   00:
PS C:\Users\ramee\downloads> ssh -i "Ncalifornia.pem" ec2-user@54.176.27.224
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Sep 10 13:35:44 2024 from 106.222.233.201
[ec2-user@PUB-SER ~]$ ls
Ncalifornia.pem
[ec2-user@PUB-SER ~]$ ssh -i "Ncalifornia.pem" ec2-user@10.0.1.130
The authenticity of host '10.0.1.130 (10.0.1.130)' can't be established.
ED25519 key fingerprint is SHA256:BvfU1DqFfGYup721xeYMjXts2665Q8VM6AuFXAU/9iI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.130' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'Ncalifornia.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Ncalifornia.pem": bad permissions
ec2-user@10.0.1.130: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

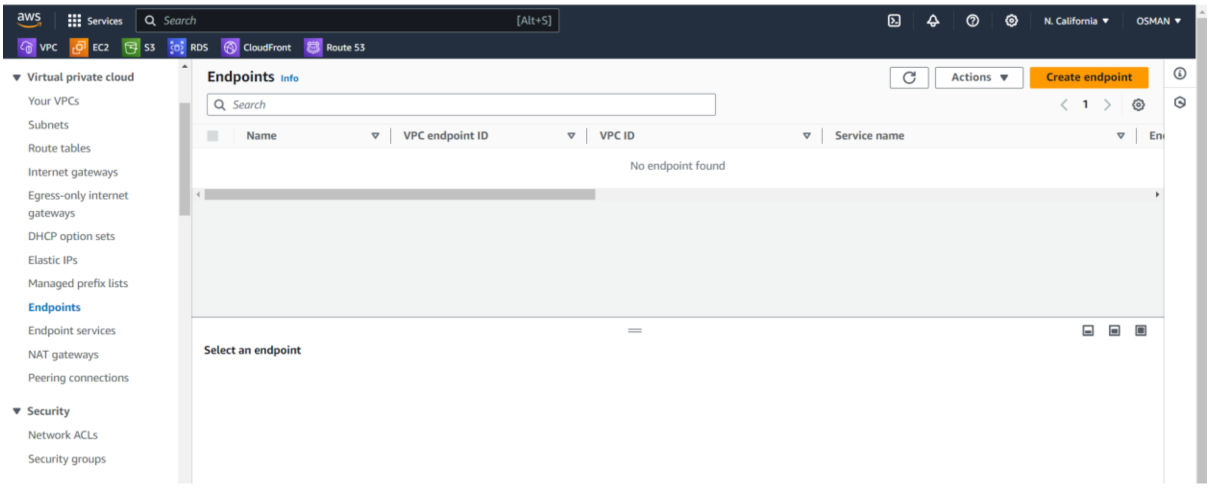
Now I am trying to private server it connect.

- Now I am I installing the git but it not install. Because there no internet gateway attach to the private server.
- Now we are using vpc end point to get internet connection install packages.

Steps to create VPC_ENDPOINTS

Click on endpoints and top right you will see one option create endpoint.

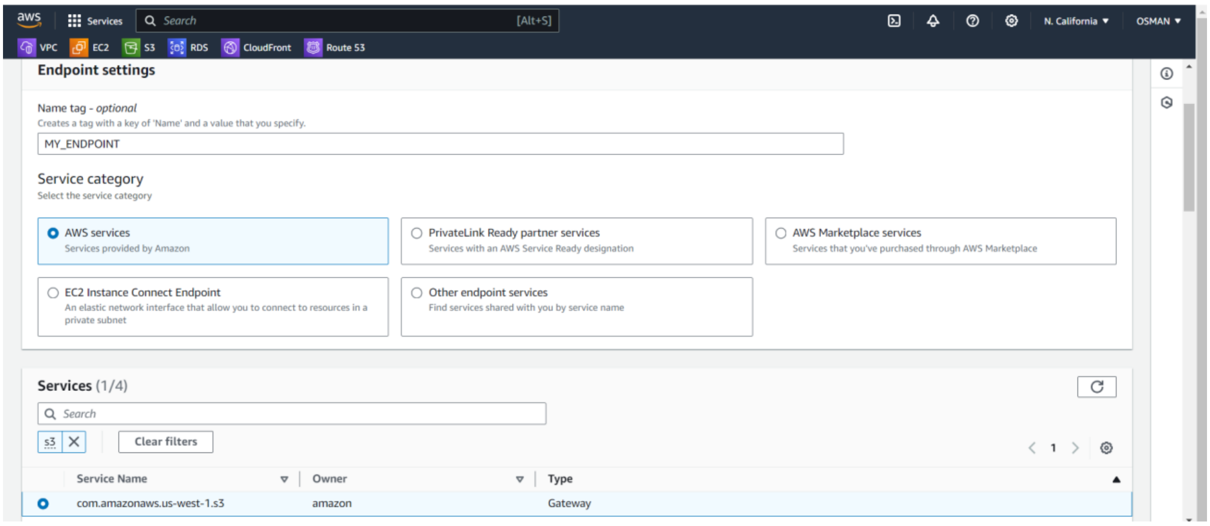
Click on that.



Name	VPC endpoint ID	VPC ID	Service name
No endpoint found			

Select the ASW Services

Services---- slect s3 --- gateway



Endpoint settings

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

Service category
Select the service category

● AWS services
Services provided by Amazon

○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

○ AWS Marketplace services
Services that you've purchased through AWS Marketplace

○ EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet

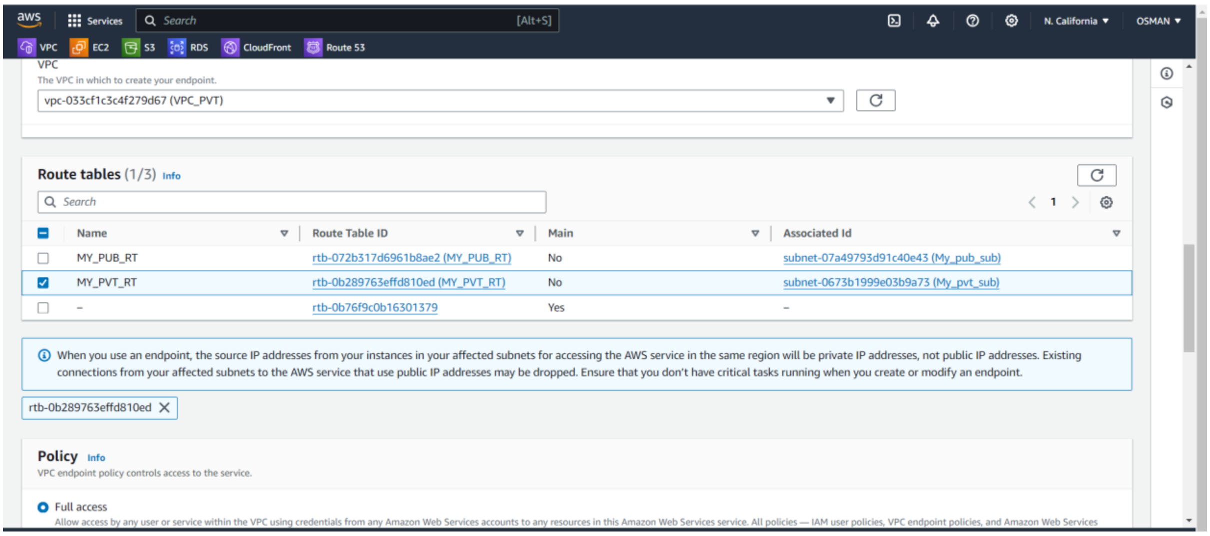
○ Other endpoint services
Find services shared with you by service name

Services (1/4)

s3 ✕

	Service Name	Owner	Type
●	com.amazonaws.us-west-1.s3	amazon	Gateway

- Select vpc and select PVT_RT
- Give full acess and click on create endpoint.



VPC
The VPC in which to create your endpoint.
vpc-033cf1c3c4f279d67 (VPC_PVT)

Route tables (1/3) Info

	Name	Route Table ID	Main	Associated Id
□	MY_PUB_RT	rtb-072b317d6961b8ae2 (MY_PUB_RT)	No	subnet-07a49793d91c40e43 (My_pub_sub)
☑	MY_PVT_RT	rtb-0b289763effd810ed (MY_PVT_RT)	No	subnet-0673b1999e03b9a73 (My_pvt_sub)
□	–	rtb-0b76f9c0b16301379	Yes	–

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.

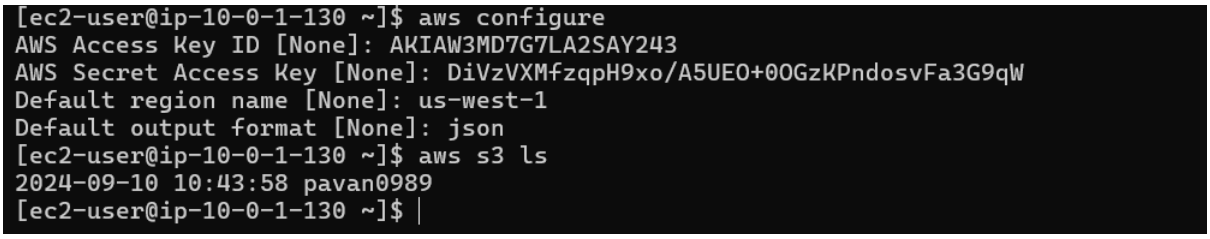
rtb-0b289763effd810ed ✕

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

Now go to the ec2 .

CMD ---- aws s3 ls – now you will be able get information for s3.



```
[ec2-user@ip-10-0-1-130 ~]$ aws configure
AWS Access Key ID [None]: AKIAW3MD7G7LA2SAY243
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-1
Default output format [None]: json
[ec2-user@ip-10-0-1-130 ~]$ aws s3 ls
2024-09-10 10:43:58 pavan0989
[ec2-user@ip-10-0-1-130 ~]$ |
```