

VPC-TASK2

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

The screenshot shows the 'Create VPC' page in the AWS Management Console. The page title is 'Create VPC' with an 'Info' link. Below the title, a description states: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' The 'VPC settings' section contains the following fields:

- Resources to create:** Two radio buttons are present. 'VPC only' is selected, and 'VPC and more' is unselected.
- Name tag - optional:** A text input field contains the value 'VPC_general'.
- IPv4 CIDR block:** Two radio buttons are present. 'IPv4 CIDR manual input' is selected, and 'IPAM-allocated IPv4 CIDR block' is unselected.
- IPv4 CIDR:** A text input field contains the value '192.168.0.0/16'.

Below the input fields, a note states: 'CIDR block size must be between /16 and /28.'

- Search for VPC and create VPC
- VPC setting → VPC only
- Select IPV4 CIDR manual input
- IPV4 CIDR as 192.168.0.0/16
- Click on create CIDR.

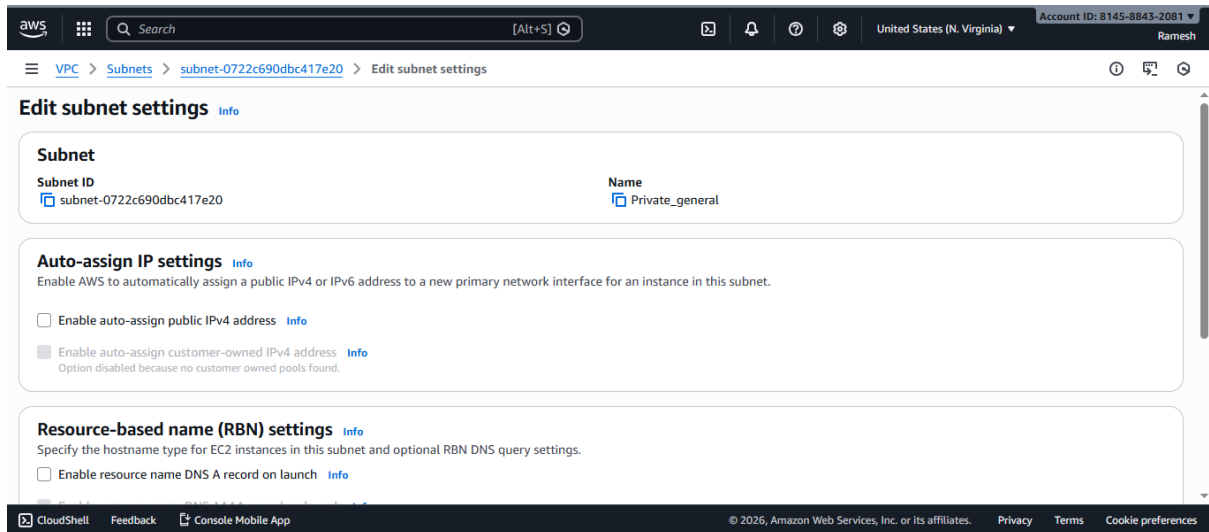
The screenshot shows the 'VPC dashboard' page in the AWS Management Console. A green notification banner at the top states: 'You successfully created vpc-04f856db8114e4c37 / VPC_general'. The page title is 'vpc-04f856db8114e4c37 / VPC_general' with an 'Actions' dropdown menu. The 'Details' section displays the following information:

Details	
VPC ID vpc-04f856db8114e4c37	State Available
DNS resolution Enabled	Tenancy default
Main network ACL acl-0c264144be62c3cdb	Default VPC No
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled
Encryption control ID -	Encryption control mode -
Block Public Access Off	DHCP option set dopt-068fb342b37621beb
DNS hostnames Disabled	IPv4 CIDR 192.168.0.0/16
Main route table rtb-0145f05ee723a2969	Route 53 Resolver DNS Firewall rule groups -
IPv6 pool -	Owner ID 814588432081

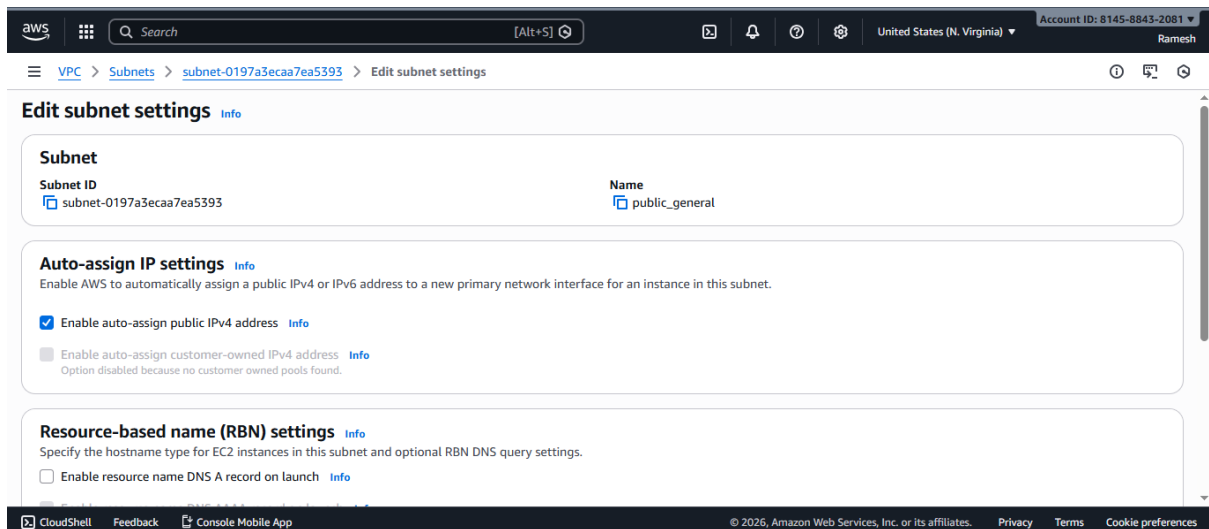
Below the details section, there are tabs for 'Resource map', 'CIDRs', 'Flow logs', 'Tags', and 'Integrations'.

- It shows successfully created VPC.

VPC-TASK2



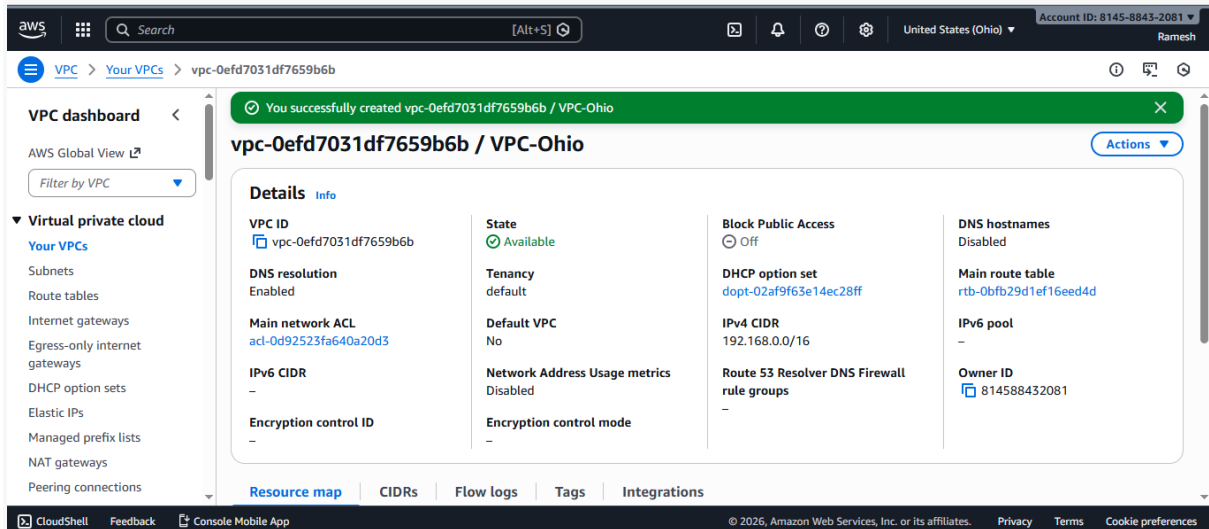
- Click on VPC, select on subnet create subnet as private subnet and public subnet.
- For private subnet we can should not enable auto-assign public IP4 address in edit subnet settings.
- CIDR Range should be within VPC range.



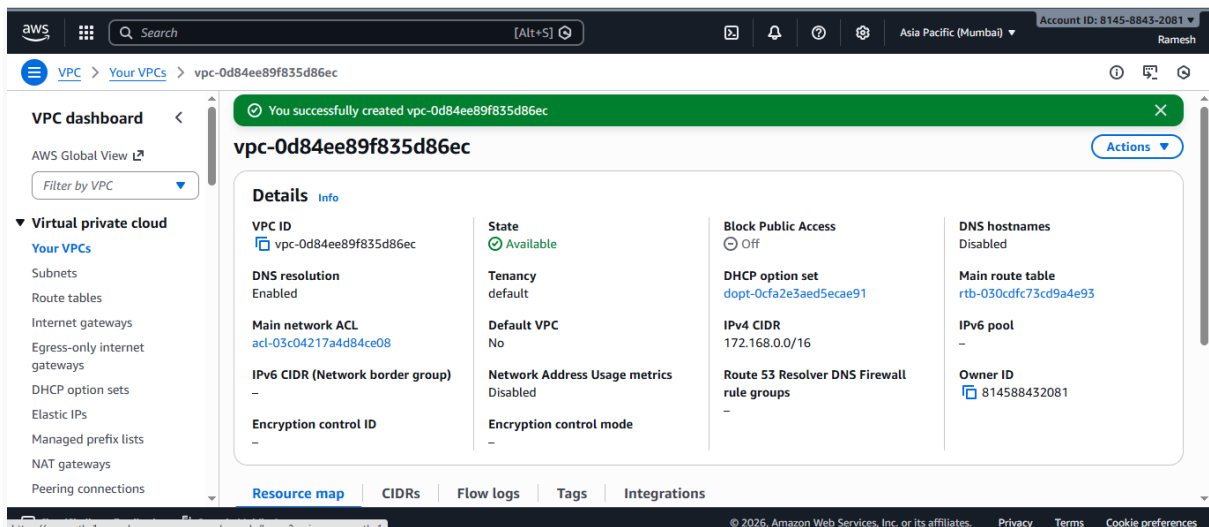
- Click on VPC, select on subnet create subnet as public subnet.
- For public subnet we can should enable auto-assign public IP4 address in edit subnet settings.
- CIDR Range should be within VPC range.

VPC-TASK2

2. Enable VPC peering for cross-region.

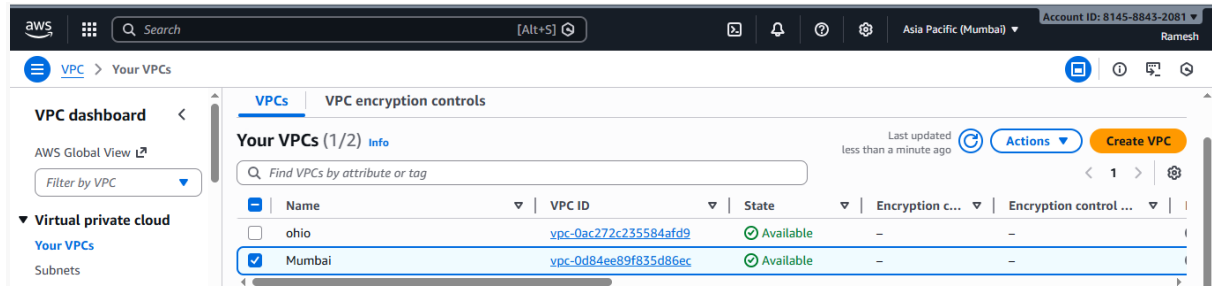


- Search for VPC, click on create VPC for ohio.
- Give IPV4 CIDR as manual input.
- Click on create VPC.

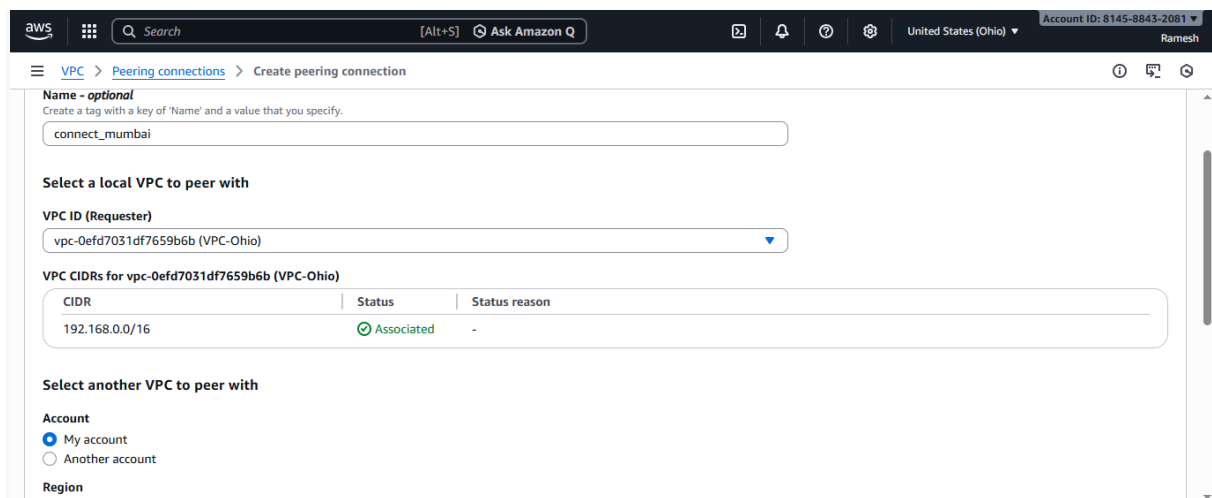


- Search for VPC, click on create VPC for Mumbai Region.
- Give IPV4 CIDR as manual input.
- Click on create VPC.

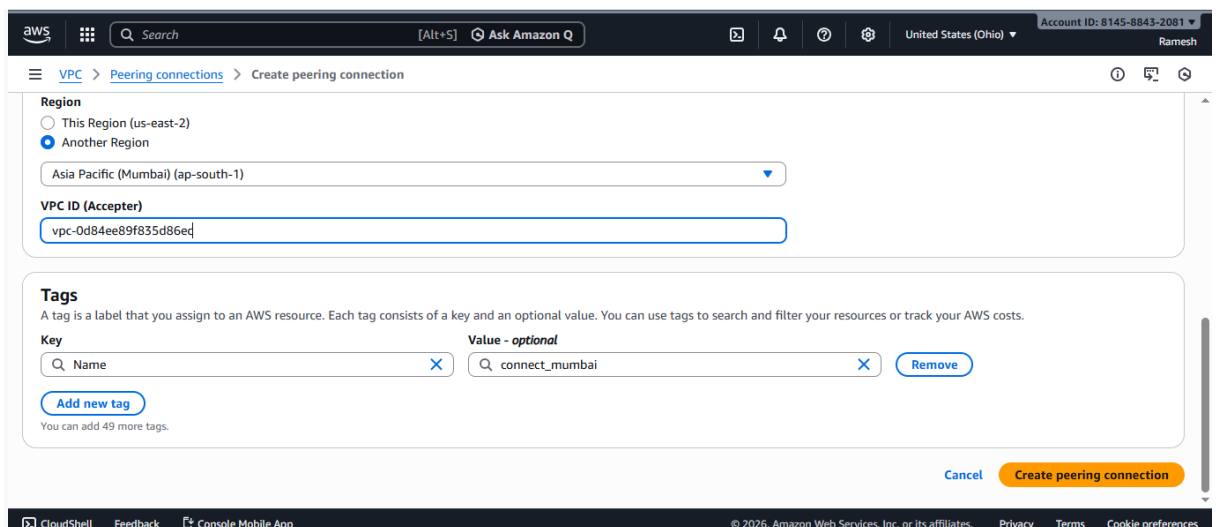
VPC-TASK2



- In Your VPCs we can all VPC what we have created.
- We can create two VPC for VPC cross peering connection

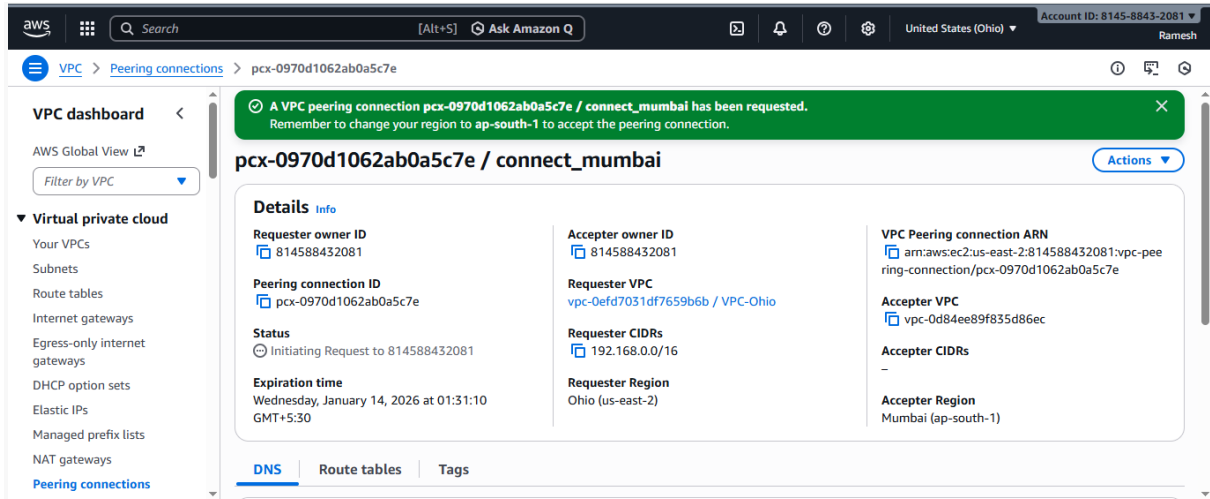


- In VPC we have to search for Peering connections
- Click on Create peering connection
- Select VPC ID (requester)
- Select another Vpc to peer with Account type as my account or another Account.

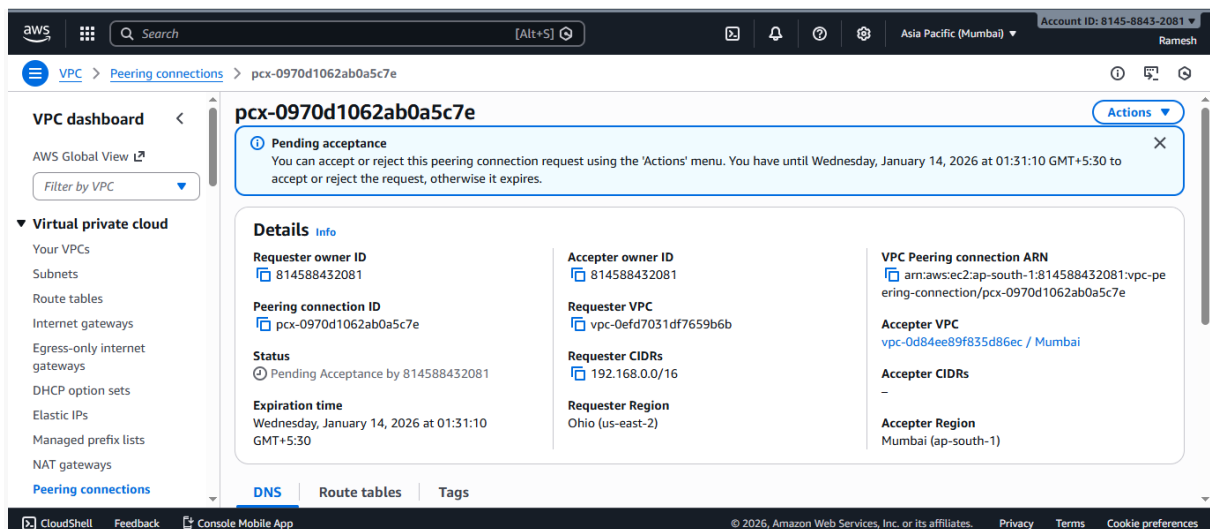


VPC-TASK2

- Select region and
- Acceptor ID-VPC-id
- Click on create on peer connection

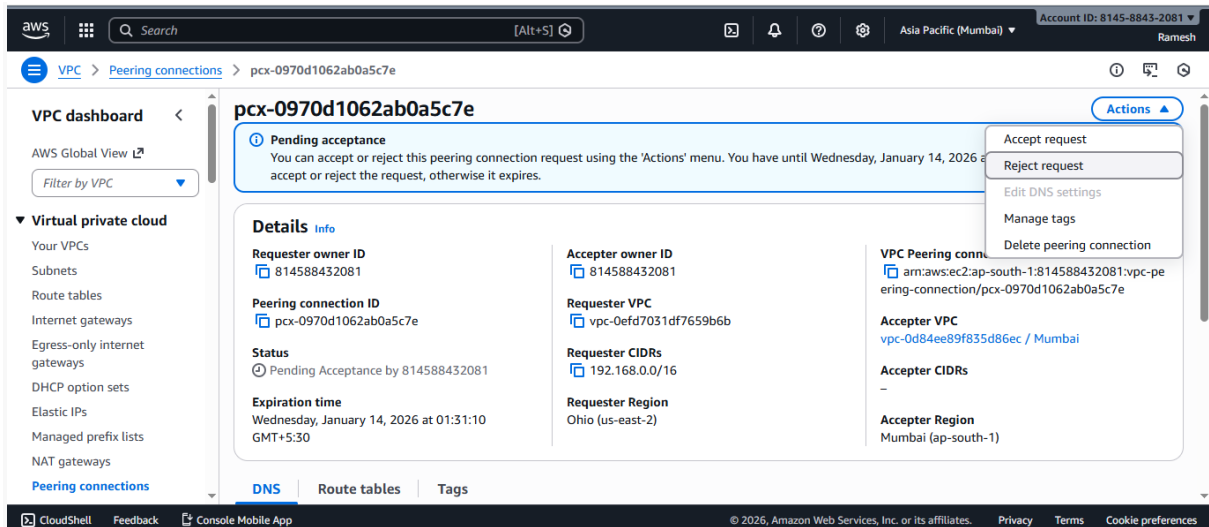


- Above image shows peering requesting send to other region through peering connections.

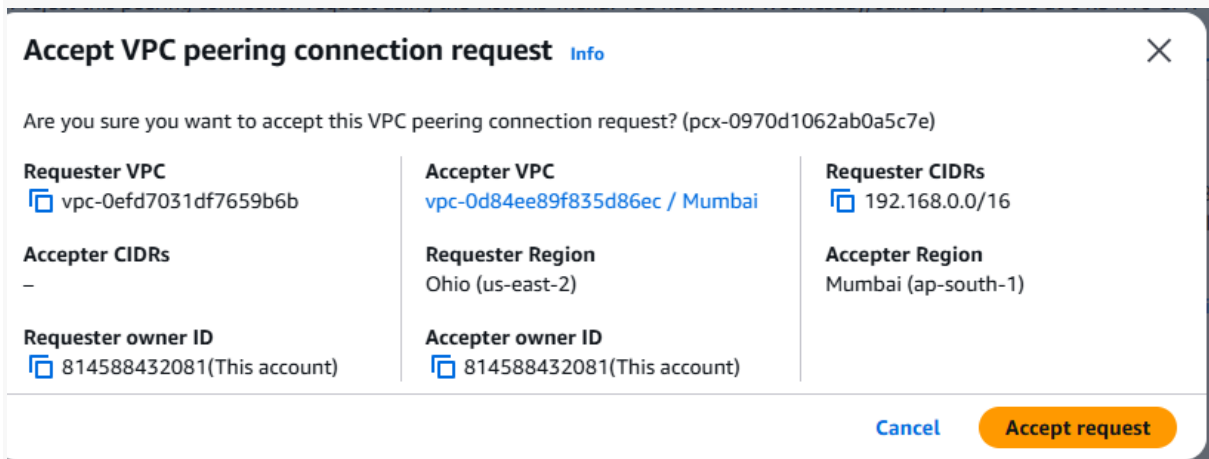


- We can notification of pending acceptance of peering connection as shown above.

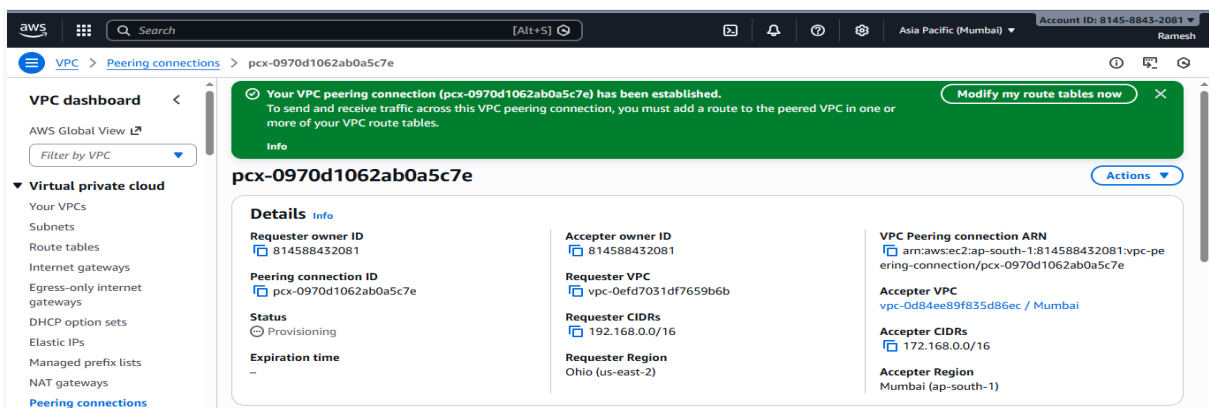
VPC-TASK2



- Click on actions so that we can accept request and reject request.



- After clicking on accept request so that we can accept peering connection.



- Above image say successful of peering connection established.

VPC-TASK2

Route table **rtb-057db1ef3b020155f / Peering-ohio**

Details

Route table ID rtb-057db1ef3b020155f	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0efd7031df7659b6b VPC-Ohio	Owner ID 814588432081		

Routes (1)

Destination	Target	Status	Propagated	Route Origin
192.168.0.0/16	local	Active	No	Create Route Table

- Click on Route table and create route table.

Route table **rtb-057db1ef3b020155f / Peering-ohio**

Details

Route table ID rtb-057db1ef3b020155f	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0efd7031df7659b6b VPC-Ohio	Owner ID 814588432081		

Routes (2)

Destination	Target	Status	Propagated	Route Origin
192.168.0.0/16	local	Active	No	Create Route Table
10.0.0.0/16	local	Active	No	Create Route Table

- Click on edit routed and so that we can add peer connection id.

VPC-TASK2

← → ↻ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#EditRoutes:RouteTableId=rtb-07a9665576c376a9f ☆ ⓘ

aws [Search] [Alt+S] 📄 🔔 ⚙️ Asia Pacific (Mumbai) ▼ Account ID: 8145-8843-2081 ▼ Ramesh

☰ VPC > Route tables > rtb-07a9665576c376a9f > Edit routes 🖨️ 🔍

Edit routes

Destination	Target	Status	Propagated	Route Origin
172.168.0.0/16	local	Active	No	CreateRouteTable
🔍 172.31.0.0/16 ✕	local ✕			
	Peering Connection	Active	No	CreateRoute
	pcx-0970d1062ab0a5c7e ✕			

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

- Here we can add peering connections as shown and save changes.

[illegible]

- Connection of EC2 which is created before.
- Checking of ping with private ip.

VPC-TASK2

```

user@DESKTOP-3KH1IRE MINGW64 ~/Downloads (master)
aws.com "Mumbai_keypair.pem" ec2-user@ec2-65-2-69-128.ap-south-1.compute.amazonaws
The authenticity of host 'ec2-65-2-69-128.ap-south-1.compute.amazonaws.com (65.2.69.128)' can't be established.
ED25519 key fingerprint is SHA256:KA8sF1hanODA03kVdg9V8Xa4wzDafpbe1MTEiZ0nflC.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-65-2-69-128.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.

#_
~\#### Amazon Linux 2023
~\#####
~\###\
~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~\V~'->
~_-.-
~-/_/
[ec2-user@ip-172-31-4-29 ~]$ ping 172.31.4.29
PING 172.31.4.29 (172.31.4.29) 56(84) bytes of data.
64 bytes from 172.31.4.29: icmp_seq=1 ttl=127 time=0.022 ms
64 bytes from 172.31.4.29: icmp_seq=2 ttl=127 time=0.029 ms
64 bytes from 172.31.4.29: icmp_seq=3 ttl=127 time=0.029 ms
64 bytes from 172.31.4.29: icmp_seq=4 ttl=127 time=0.030 ms
64 bytes from 172.31.4.29: icmp_seq=5 ttl=127 time=0.029 ms
64 bytes from 172.31.4.29: icmp_seq=6 ttl=127 time=0.033 ms
64 bytes from 172.31.4.29: icmp_seq=7 ttl=127 time=0.036 ms
64 bytes from 172.31.4.29: icmp_seq=8 ttl=127 time=0.027 ms
64 bytes from 172.31.4.29: icmp_seq=9 ttl=127 time=0.027 ms
64 bytes from 172.31.4.29: icmp_seq=10 ttl=127 time=0.031 ms
64 bytes from 172.31.4.29: icmp_seq=11 ttl=127 time=0.031 ms
64 bytes from 172.31.4.29: icmp_seq=12 ttl=127 time=0.030 ms
64 bytes from 172.31.4.29: icmp_seq=13 ttl=127 time=0.031 ms
64 bytes from 172.31.4.29: icmp_seq=14 ttl=127 time=0.029 ms
64 bytes from 172.31.4.29: icmp_seq=15 ttl=127 time=0.027 ms
64 bytes from 172.31.4.29: icmp_seq=16 ttl=127 time=0.031 ms
64 bytes from 172.31.4.29: icmp_seq=17 ttl=127 time=0.028 ms

```

- Checking connection for both EC2.

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

Account ID: 8145-8843-2081

Asia Pacific (Osaka)

Search

Search

Account ID: 8145-8843-2081

Ramesh

Menu

VPC > Peering connections > Create peering connection

1

Help

Close

Select a local VPC to peer with

VPC ID (Requester)

vpc-011ba177838f2eff3 (VPC_1)

VPC CIDRs for vpc-011ba177838f2eff3 (VPC_1)

CIDR	Status	Status reason
10.0.0.0/16	Associated	-

Select another VPC to peer with

Account

☐ My account

☒ Another account

Account ID

285253872042

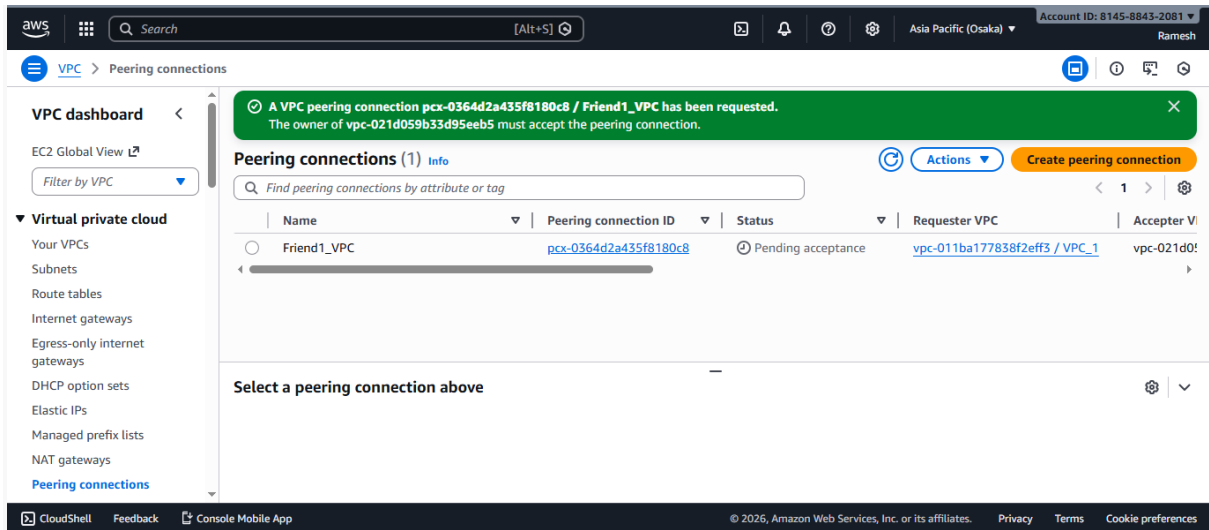
Region

☐ This Region (ap-northeast-3)

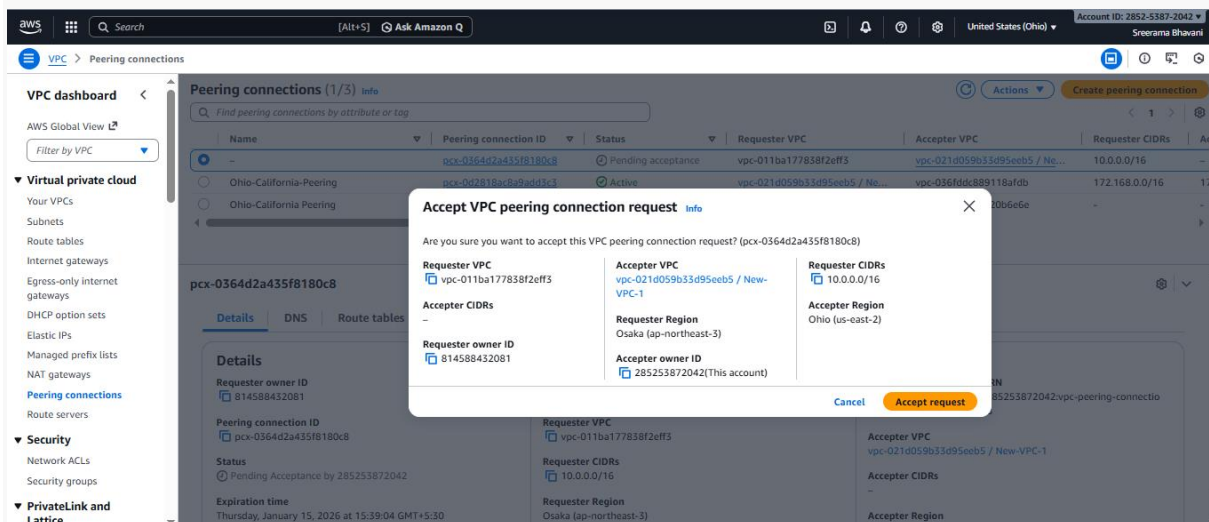
☒ Another Region

- Select a local VPC to peer with VPC ID (requester).
- Select another VPC to peer with account as another account
- Fill account Id
- Select Region as another region.

VPC-TASK2



- Click on Create peering connection which is send to acceptor.



- From other account this shows for accept request

VPC-TASK2

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
172.168.0.0/16	Peering Connection	-	No	CreateRoute
172.168.0.0/16	pcx-0364d2a435f8180c8			

- Click on Route tables and edit route tables and edit routes
- Add friend CIDR and peering connection
- Click on Save changes

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

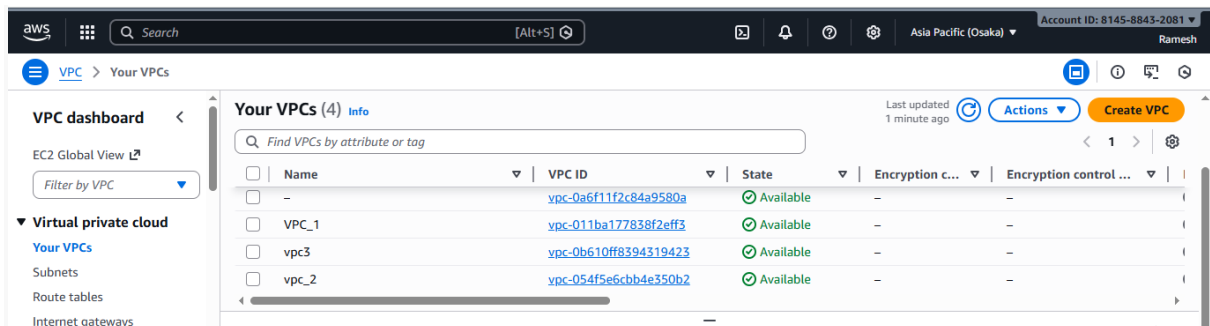
last login: Thu Jan  8 06:18:14 2026 from 15.168.105.162
[ec2-user@ip-10-0-232-74 ~]$ ping 172.168.0.4
PING 172.168.0.4 (172.168.0.4) 56(84) bytes of data:
64 bytes from 172.168.0.4: icmp_seq=1 ttl=44 time=273 ms
64 bytes from 172.168.0.4: icmp_seq=2 ttl=44 time=273 ms
64 bytes from 172.168.0.4: icmp_seq=3 ttl=44 time=273 ms
64 bytes from 172.168.0.4: icmp_seq=4 ttl=44 time=272 ms
64 bytes from 172.168.0.4: icmp_seq=5 ttl=44 time=273 ms
64 bytes from 172.168.0.4: icmp_seq=6 ttl=44 time=272 ms
64 bytes from 172.168.0.4: icmp_seq=7 ttl=44 time=273 ms
64 bytes from 172.168.0.4: icmp_seq=8 ttl=44 time=273 ms
```

- Check ping ip address with friend ip and ping is connected.

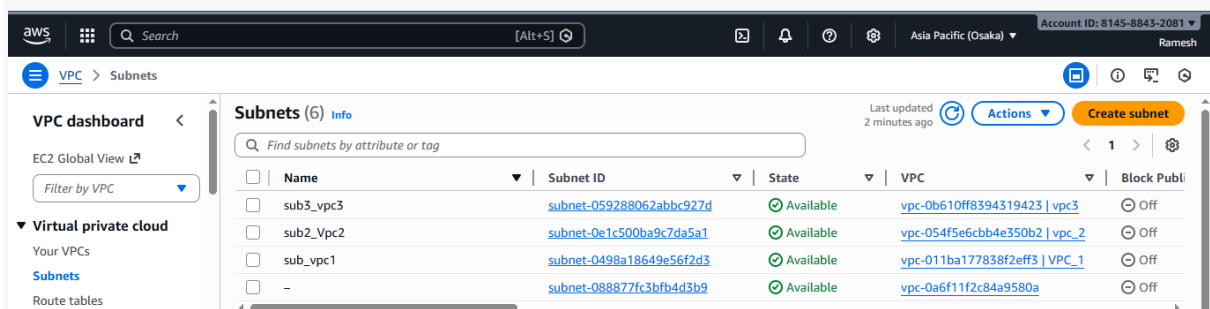
VPC-TASK2

4. Set up a VPC Transit Gateway.

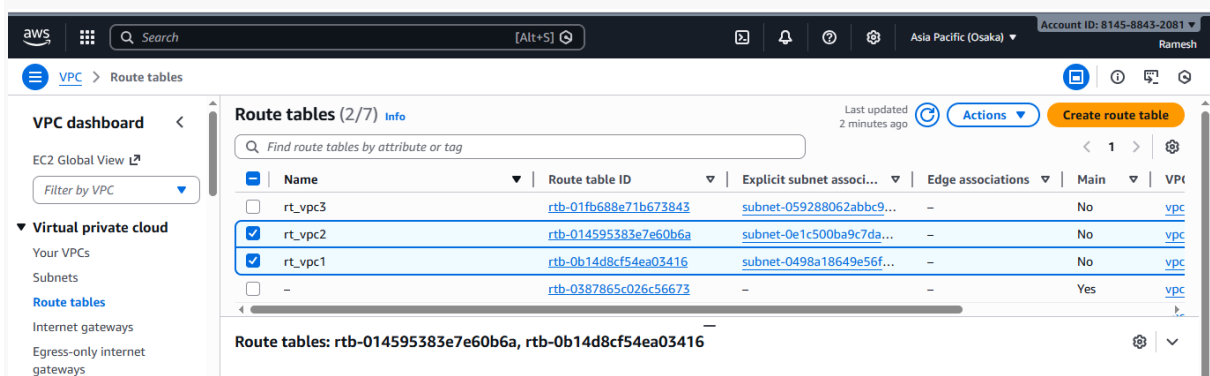
- Transit Gateway allows you to connect many VPCs and on-prem networks through a single gateway instead of managing many VPC peering connections.



- Click on VPC and create VPC as per our requirement with CIDR range
- Click on your VPC and it shows VPCs present in it.



- Click on subnet and create subnet with in VPC CIDR as per our requirement.
- For that subnet we should add corresponding VPC



- Click on create on route table and add VPC to them.

VPC-TASK2

Internet gateways (4) Info

Find internet gateways by attribute or tag

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	VPC1-IGW	igw-045b0b61ad73347c9	Attached	vpc-011ba177838f2eff3 VPC_1
<input type="checkbox"/>	vpc3_igw	igw-066fe3da44bcb6e6e	Attached	vpc-0b610ff8394319423 vpc3
<input type="checkbox"/>	vpc2_igw	igw-0c54a4ce357c3260c	Attached	vpc-054f5e6cbb4e350b2 vpc_2
<input type="checkbox"/>	-	igw-0e105d7d902b484a3	Attached	vpc-0a6f11f2c84a9580a

- Click on create Internet gateway for VPC present in our region.

Instances (3) Info

Find Instance by attribute or tag (case-sensitive)

Instance state = running

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	ec2_vpc3	i-089140accbeb0664f	Running	t2.micro	2/2 checks passed	View alarms +	ap-northeast-1
<input type="checkbox"/>	ec2_vpc1	i-0a5486ac4cf7bb459	Running	t2.micro	2/2 checks passed	View alarms +	ap-northeast-1
<input type="checkbox"/>	ec2_vpc2	i-0f5b23712455b1baf	Running	t3.micro	3/3 checks passed	View alarms +	ap-northeast-1

- Click on EC2 and click on instance and launch Instances as required.

Transit gateways (1/1) Info

Find transit gateway by attribute or tag

<input checked="" type="checkbox"/>	Name	Transit gateway ID	Owner ID	State
<input checked="" type="checkbox"/>	transit_gateway	tgw-0792864d88e9f1dea	814588432081	Available

Transit gateway: tgw-0792864d88e9f1dea / transit_gateway

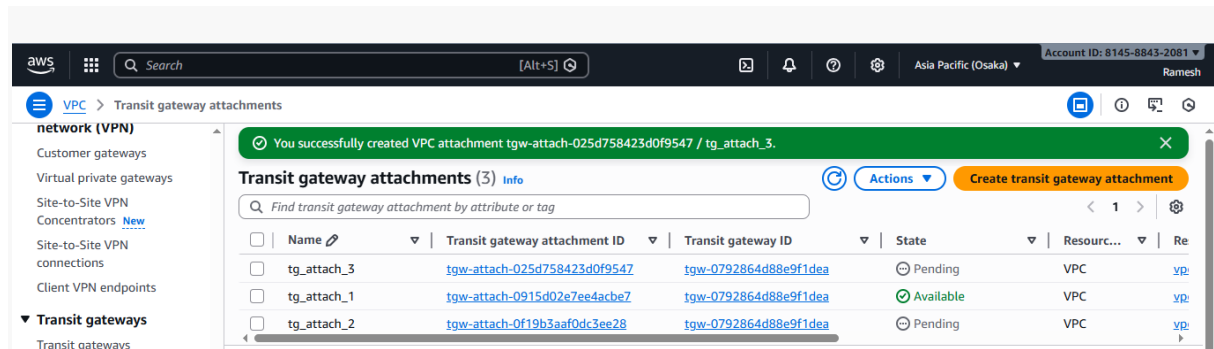
Details | Flow logs | Sharing | Tags

Details

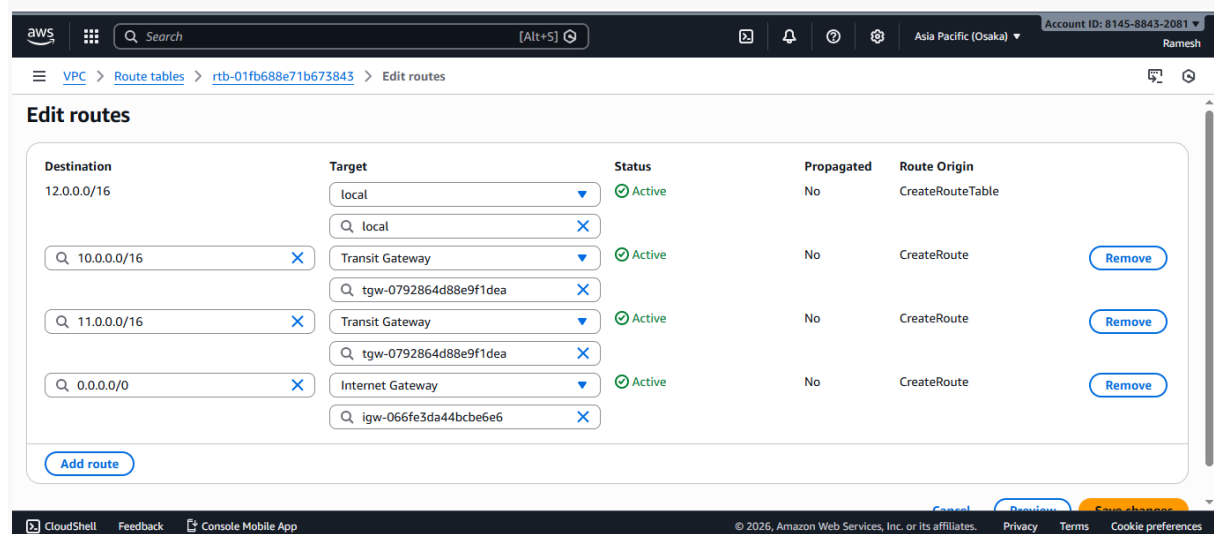
Transit gateway ID	State	Amazon ASN	DNS support
tgw-0792864d88e9f1dea	Available	64512	Enable

- Search for Transit gateways and create transit gateway

VPC-TASK2



- Click on transit gateway attachments and create transit gateway attachment.



- In VPC and select Route tables and edit routes
- Add transit gateways CIDR and add internet gateway.
- Click on save changes.

VPC-TASK2

[illegible]

- Above image shows VPC transit gateway among all EC2.

VPC-TASK2

5. Set up a VPC Endpoint.

- An endpoint is a specific entry or exit point used to communicate with a service, application, or network.
Think of it as an address where requests are sent and responses are received.

The screenshot shows the 'Create endpoint' page in the AWS Management Console. The breadcrumb navigation is 'VPC > Endpoints > Create endpoint'. The page title is 'Create endpoint' with an 'Info' link. Below the title, it says 'Create the type of VPC endpoint that supports the service, service network or resource to which you want to connect.' The 'Endpoint settings' section has a 'Name tag - optional' field with the value 'ep_Neelima'. The 'Type' section has a 'Select a category' dropdown. The 'AWS services' option is selected, with a description: 'Connect to services provided by Amazon with an Interface endpoint, or a Gateway endpoint'. Other options include 'PrivateLink Ready partner services', 'AWS Marketplace services', 'EC2 Instance Connect Endpoint', 'Resources', and 'Service networks'. The footer shows '© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

- In VPC select Endpoints and
- Click on create on endpoint.
- Select type as AWS services.

The screenshot shows the 'Create endpoint' page in the AWS Management Console, specifically the 'Service Region' section. The breadcrumb navigation is 'VPC > Endpoints > Create endpoint'. The 'Service Region' section has a 'Enable Cross Region endpoint' checkbox checked and a dropdown menu showing 'Asia Pacific (Osaka) (ap-northeast-3)'. Below this, a message says 'Showing services available in service region: Asia Pacific (Osaka) (ap-northeast-3)'. The 'Services (1/2)' section has a search bar and a table of services. The table has columns for 'Service Name', 'Owner', and 'Type'. The first row is 'com.amazonaws.ap-northeast-3.s3' with owner 'amazon' and type 'Interface'. The second row is 'com.amazonaws.ap-northeast-3.s3' with owner 'amazon' and type 'Gateway'. The footer shows '© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

Service Name	Owner	Type
com.amazonaws.ap-northeast-3.s3	amazon	Interface
com.amazonaws.ap-northeast-3.s3	amazon	Gateway

- Select Service Region
- In services select for service which is associate with the region.

VPC-TASK2

The screenshot shows the AWS console 'Create endpoint' page. The 'Network settings' section is active, showing a dropdown for 'VPC' with the value 'vpc-006e2888d698c709e (Endpoint_VPC)'. Below it, the 'Additional settings' section is collapsed. The 'Route tables (2)' section is expanded, showing a table with two route tables: 'rtb-092127b36b118bfe3' (Main: Yes) and 'rtb-0cc7e9a7e6343e4dc (EP_rt)' (Main: No).

Name	Route Table ID	Main	Associated Id
-	rtb-092127b36b118bfe3	Yes	-
EP_rt	rtb-0cc7e9a7e6343e4dc (EP_rt)	No	-

- In Networking setting Select VPC which is created for VPC endpoints.
- Select Route tables which are created for endpoints.

The screenshot shows the AWS console 'Create endpoint' page. The 'Route tables (1/2)' section is expanded, showing a table with two route tables: 'rtb-092127b36b118bfe3' (Main: Yes) and 'rtb-0cc7e9a7e6343e4dc (EP_rt)' (Main: No). The 'EP_rt' row is selected. Below the table, a warning message states: '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.' Below the warning, the route table ID 'rtb-0cc7e9a7e6343e4dc' is entered. The 'Policy' section is expanded, showing a radio button for 'Full access' selected.

Name	Route Table ID	Main	Associated Id
-	rtb-092127b36b118bfe3	Yes	-
<input checked="" type="checkbox"/> EP_rt	rtb-0cc7e9a7e6343e4dc (EP_rt)	No	-

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.

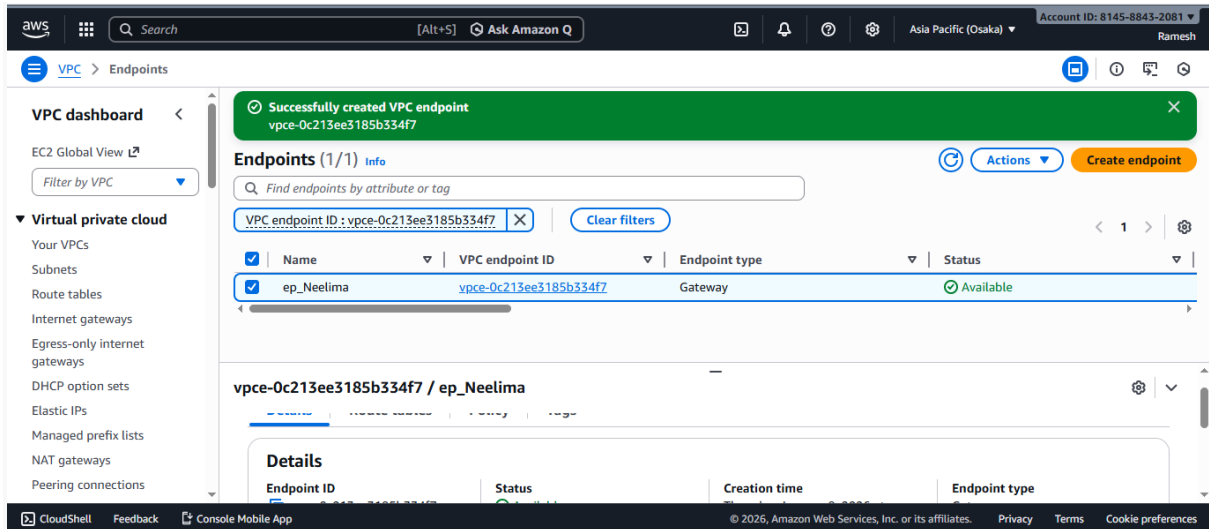
rtb-0cc7e9a7e6343e4dc

Policy Info
VPC endpoint policy controls access to the service.

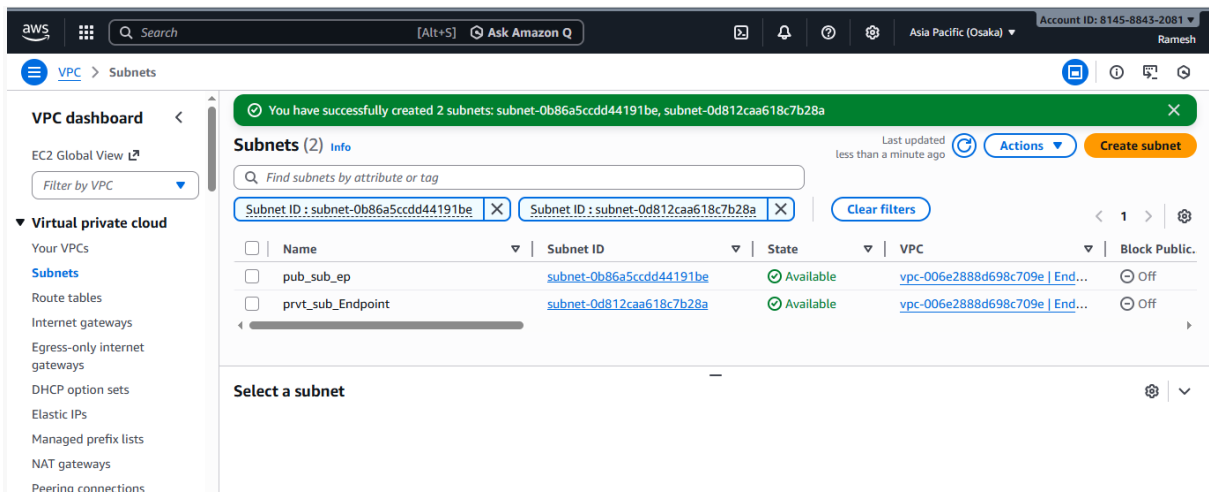
☒ Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket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

- Click on policy and select full access.
- Save it.

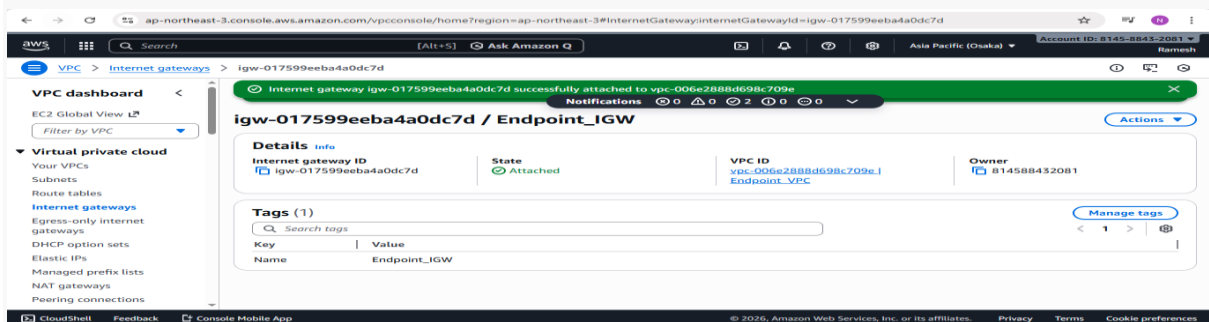
VPC-TASK2



- Above image shows endpoints created successfully



- Click on subnet and create subnets with VPC which is associate with it



- Click on Internet gateway and create IGW and route edit route and internet gateway to public subnet.

VPC-TASK2

[illegible]

- Connect to ec2 instance which created for endpoints.

```
root@ip-14-0-1-11:~  
[ec2-user@ip-14-0-1-11 ~]$ sudo su -  
[root@ip-14-0-1-11 ~]# ping 14.0.1.11  
PING 14.0.1.11 (14.0.1.11) 56(84) bytes of data.  
64 bytes from 14.0.1.11: icmp_seq=1 ttl=127 time=0.015 ms  
64 bytes from 14.0.1.11: icmp_seq=2 ttl=127 time=0.027 ms  
64 bytes from 14.0.1.11: icmp_seq=3 ttl=127 time=0.025 ms  
64 bytes from 14.0.1.11: icmp_seq=4 ttl=127 time=0.026 ms  
^C  
--- 14.0.1.11 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3128ms  
rtt min/avg/max/mdev = 0.015/0.023/0.027/0.004 ms  
[root@ip-14-0-1-11 ~]# ping 14.0.2.4  
PING 14.0.2.4 (14.0.2.4) 56(84) bytes of data.  
64 bytes from 14.0.2.4: icmp_seq=1 ttl=127 time=0.865 ms  
64 bytes from 14.0.2.4: icmp_seq=2 ttl=127 time=0.890 ms  
64 bytes from 14.0.2.4: icmp_seq=3 ttl=127 time=1.38 ms  
64 bytes from 14.0.2.4: icmp_seq=4 ttl=127 time=1.04 ms  
64 bytes from 14.0.2.4: icmp_seq=5 ttl=127 time=1.47 ms  
^C  
--- 14.0.2.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4079ms  
rtt min/avg/max/mdev = 0.865/1.128/1.469/0.249 ms  
[root@ip-14-0-1-11 ~]# |
```

VPC-TASK2

- Check ping connection for private ip with public subnet ip.

```
[root@ip-14-0-1-11 ~]# aws configure
AWS Access Key ID [*****KPRI]: AKIA33KKBB3I7ZCCKPRI
AWS Secret Access Key [*****H6Ph]: 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
Default region name [text]: ap-south-1
Default output format [text]: text
[root@ip-14-0-1-11 ~]# aws s3 ls
2025-10-15 05:45:47 aws-athena-query-results-814588432081-us-east-2-0pf98ayv
2025-09-10 18:25:51 aws-cloudtrail-logs-814588432081-0a7db287
2025-08-15 15:11:11 demo-wrerwe
2025-11-03 03:45:13 dummy-buck516
2025-08-14 10:18:05 josh-1-2
2025-08-11 14:43:06 kavya54321
2025-08-12 16:54:23 kvk24
2025-10-15 04:08:25 nam-etl-516
2025-11-10 05:46:40 nfs-data12345
2025-08-13 14:49:28 s3-life-cycle1
2026-01-06 19:09:30 s3neelima
2025-11-03 03:41:53 venkat-516
2025-10-10 19:38:28 venkey-s3-516
[root@ip-14-0-1-11 ~]#
```

To access AWS first we have to configure through IAM

- \$aws configure
- AWS access key ID:
- AWS Secret Access ID:
- Default region name:
- Default output format:
- Access one of the service like S3 service through it
- AWS s3 ls it shows all files present it.