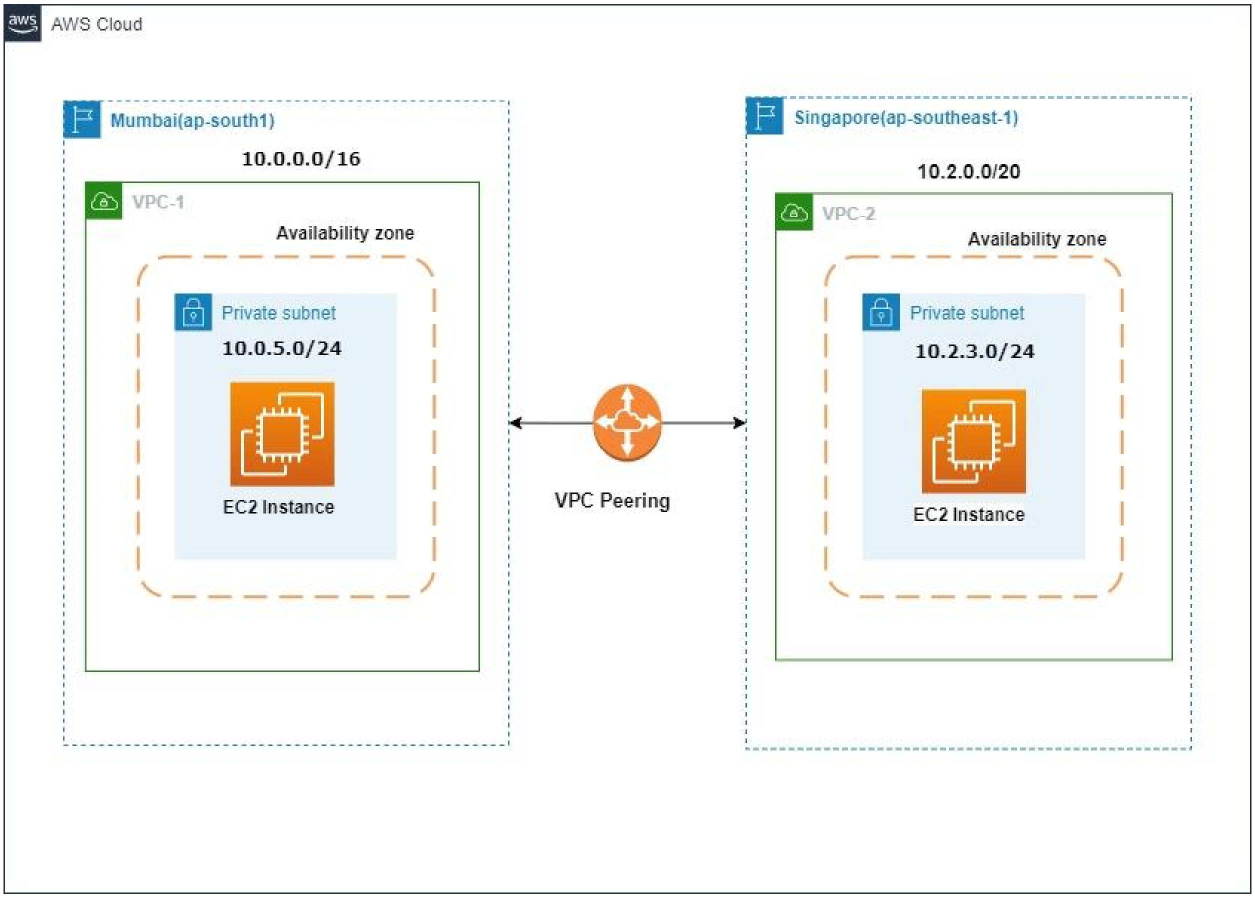
TWO VPC PEERING IN DIFFERENT REGION

➢What is a Virtual Private Cloud Network (VPC)?

- The Virtual Private Network (VPC) is an isolated or private cloud computing environment within a public cloud. VPC provides networking for your cloud-based resources and services that are global, scalable, and flexible.
- Amazon Virtual Private Cloud (Amazon VPC) enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you've defined.
- In AWS The VPC is Created in Regional.

  Refer to the link: https://docs.aws.amazon.com/vpc/index.html

➢ Architecture diagram of two VPC peering connection

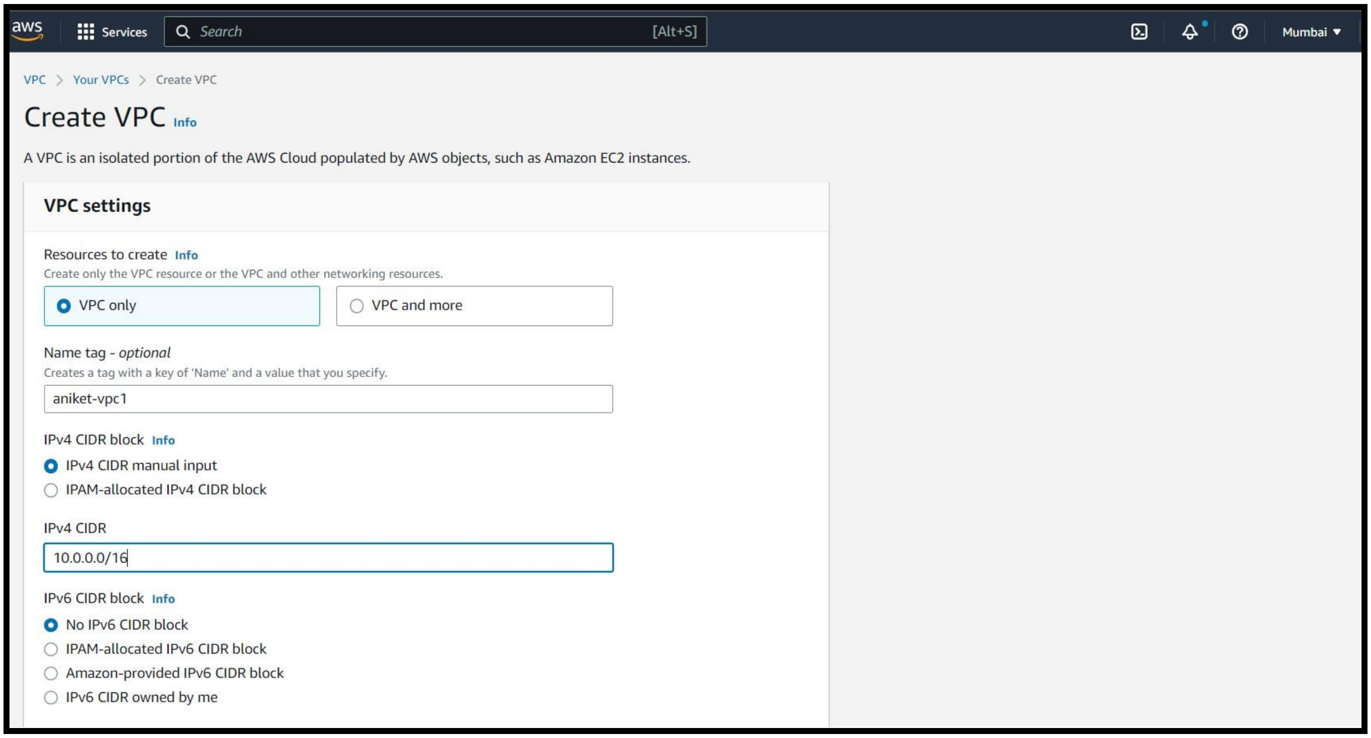


Two VPC Peering Connection

Now, we are working on two VPC peering connections in two different regions to check if they are pinging or not.

Step 1 : Create one VPC network in a **Mumbai region (ap-south-1)**

1. Go to VPC and then click to create VPC
2. Give the name to your VPC then
3. Select CIDR range and give the proper private range (we are making connection two private VPC's)
4. Remain other parameters as default and now create VPC.



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
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.
aniket-vpc1

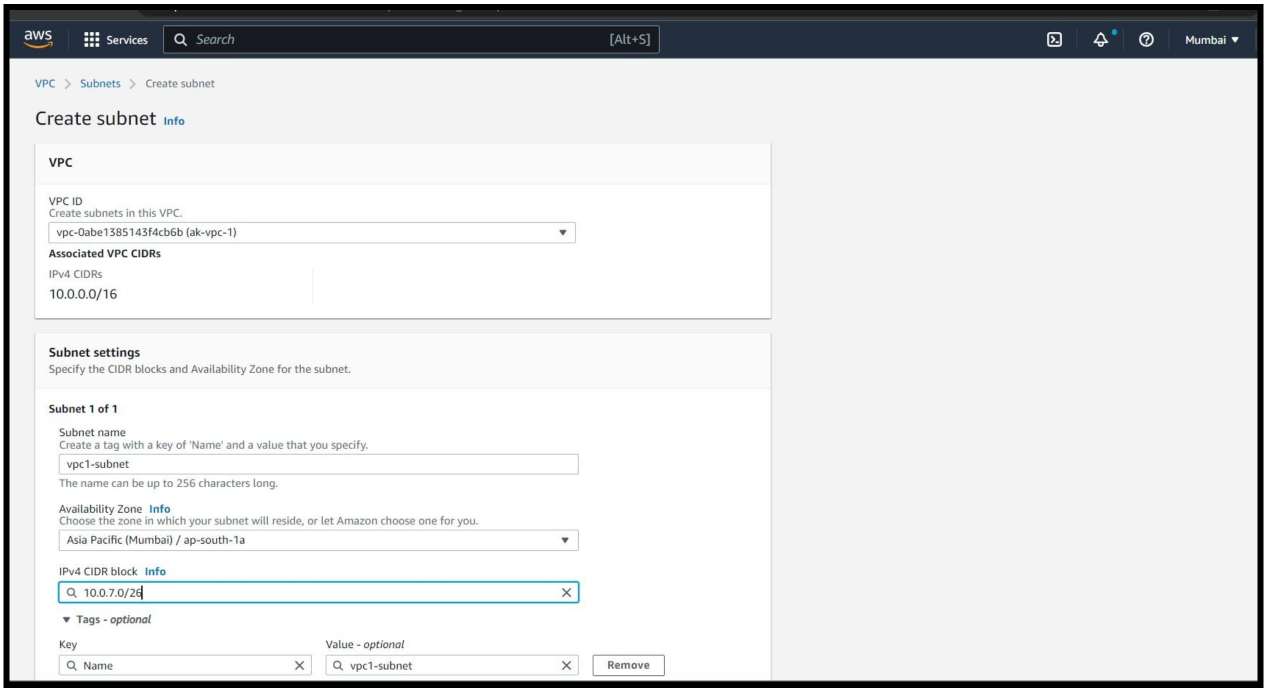
IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16

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

Step 2 : In VPC, create a subnet.

1. Select created VPC ID.
2. Then in subnet setting select availability zone in **Asia pacific mumbai(ap-south 1a)**
3. Give the proper **IPV4 CIDR** block range for vpc-1 subnet
4. Click on create subnet.



VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0abe1385143f4cb6b (ak-vpc-1) ▾

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

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.
vpc1-subnet
The name can be up to 256 characters long.

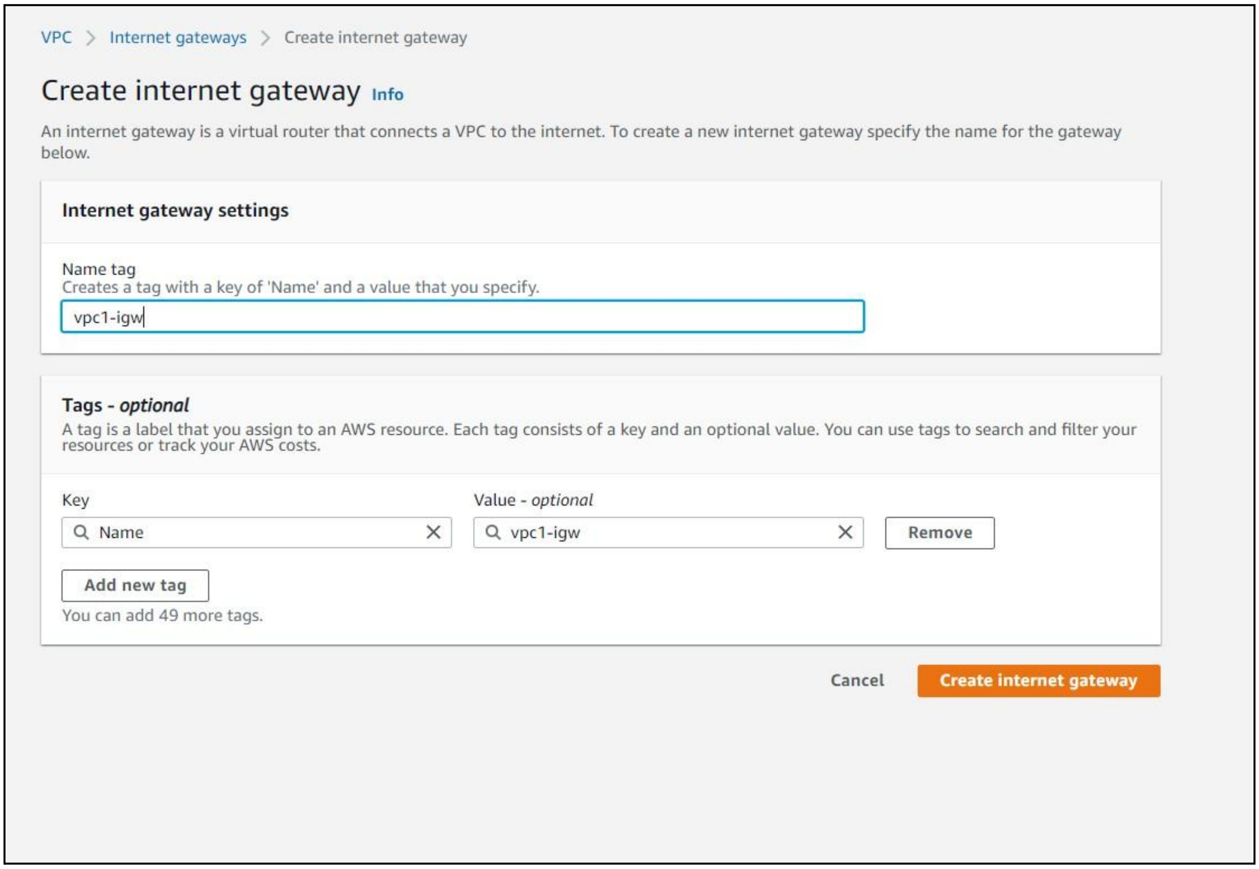
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1a ▾

IPv4 CIDR block Info
10.0.7.0/26

▾ Tags - *optional*

Key	Value - *optional*	
Name	vpc1-subnet	Remove

Step 3: Create an Internet Gateway



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

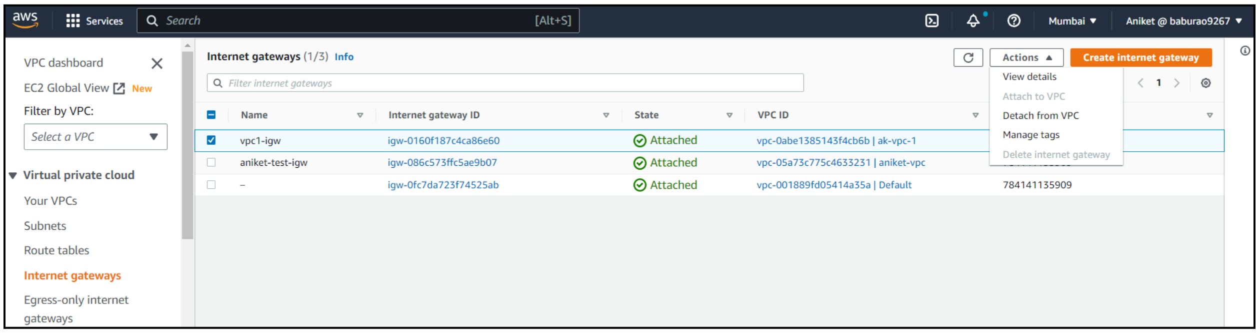
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
vpc1-igw

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	vpc1-igw	Remove

You can add 49 more tags.

1. Name your internet gateway(IGW) and create it.
2. Now, attach an Internet gateway to the VPC.In my case, **vpc1-igw** is already attached.

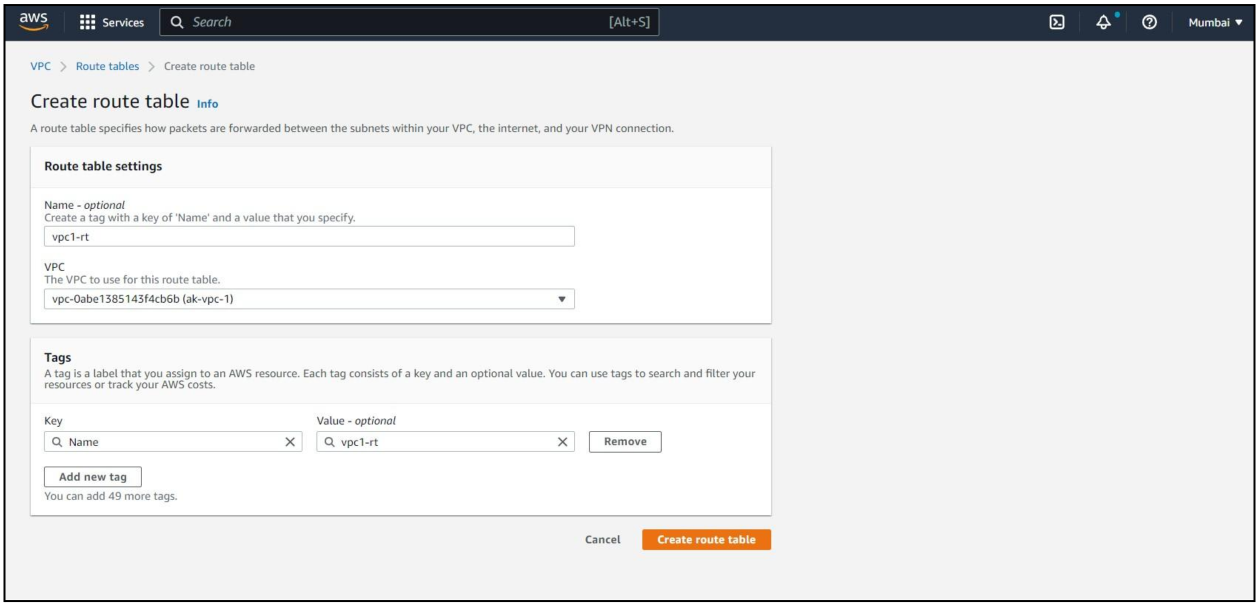


Internet gateways (1/3) Info

	Name	Internet gateway ID	State	VPC ID	
☑	vpc1-igw	igw-0160f187c4ca86e60	Attached	vpc-0abe1385143f4cb6b | ak-vpc-1	
□	aniket-test-igw	igw-086c573ffc5ae9b07	Attached	vpc-05a73c775c4633231 | aniket-vpc	
□	–	igw-0fc7da723f74525ab	Attached	vpc-001889fd05414a35a | Default	784141135909

Step 4 : Create route table

1. Name your route table then select your created VPC.
2. Click on create route table.



Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
vpc1-rt

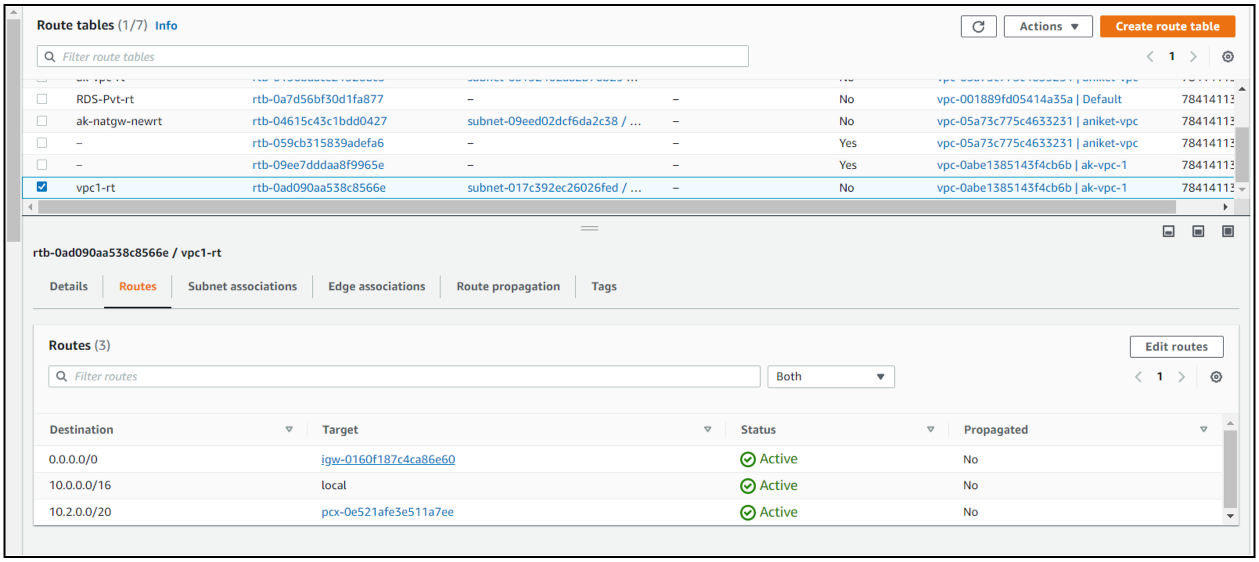
VPC
The VPC to use for this route table.
vpc-0abe1385143f4cb6b (ak-vpc-1)

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: Name
Value - *optional*: vpc1-rt

You can add 49 more tags.

3. Now,in the created route table ,go to routes.
4. Edit the routes, then allow internet IP **0.0.0.0/0** to IGW and save.



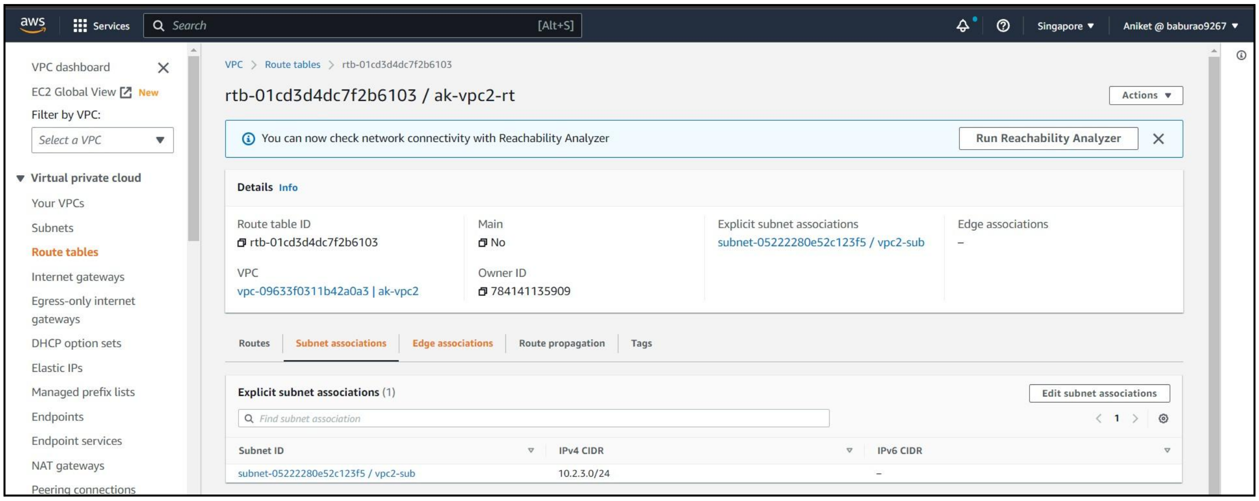
Route tables (1/7) Info

□	RDS-Pvt-rt	rtb-0a7d56bf30d1fa877	–	–	No	vpc-001889fd05414a35a | Default	78414113
□	ak-natgw-newrt	rtb-04615c43c1bdd0427	subnet-09eed02dcf6da2c38 / ...	–	No	vpc-05a73c775c4633231 | aniket-vpc	78414113
□	–	rtb-059cb315839adefa6	–	–	Yes	vpc-05a73c775c4633231 | aniket-vpc	78414113
□	–	rtb-09ee7dddaa8f9965e	–	–	Yes	vpc-0abe1385143f4cb6b | ak-vpc-1	78414113
☑	vpc1-rt	rtb-0ad090aa538c8566e	subnet-017c392ec26026fed / ...	–	No	vpc-0abe1385143f4cb6b | ak-vpc-1	78414113

rtb-0ad090aa538c8566e / vpc1-rt

Routes (3)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0160f187c4ca86e60	Active	No
10.0.0.0/16	local	Active	No
10.2.0.0/20	pcx-0e521afe3e511a7ee	Active	No



VPC > Route tables > rtb-01cd3d4dc7f2b6103

rtb-01cd3d4dc7f2b6103 / ak-vpc2-rt

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-01cd3d4dc7f2b6103

Main: No

Explicit subnet associations: subnet-05222280e52c123f5 / vpc2-sub

Edge associations: –

VPC: vpc-09633f0311b42a0a3 | ak-vpc2

Owner ID: 784141135909

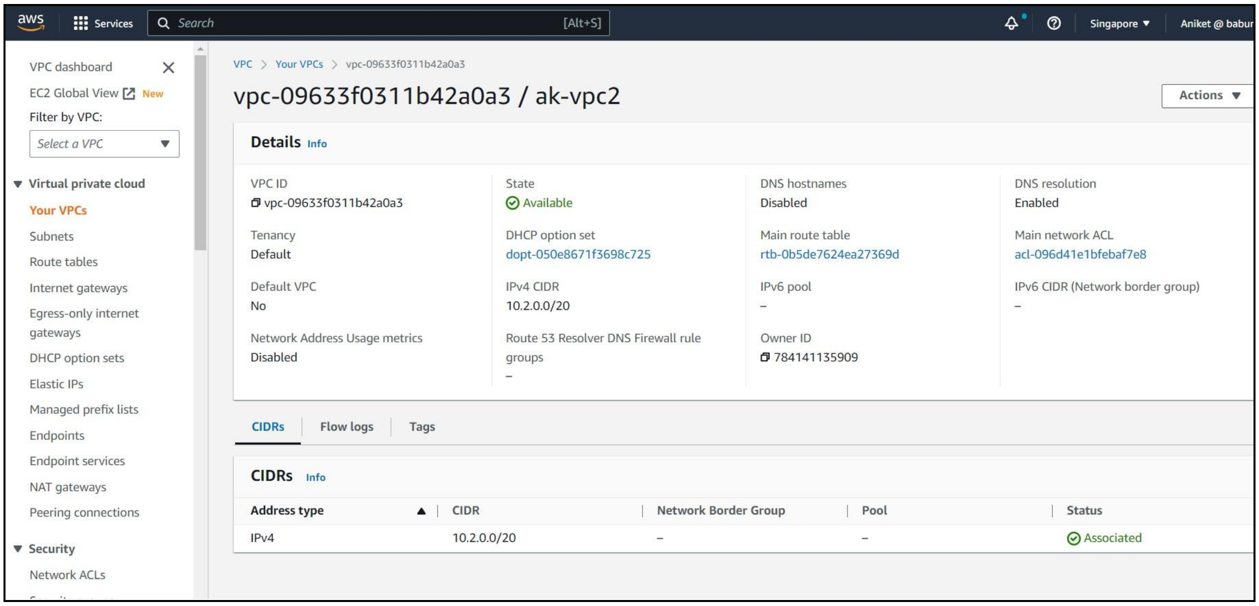
Explicit subnet associations (1)

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-05222280e52c123f5 / vpc2-sub	10.2.3.0/24	–

5. Now go to the subnet association and add the **subnet**.
6. In my case ,already given routes and added subnet.

Step 5: Now, repeat the same process for the second VPC in the **Singapore region(ap-southeast-1).**

1. Name the vpc and give IPV4 CIDR which is different from mumbai region vpc in my case i am assigned **10.2.0.0/20** .
2. Other parameters are set to default.



VPC > Your VPCs > vpc-09633f0311b42a0a3

vpc-09633f0311b42a0a3 / ak-vpc2

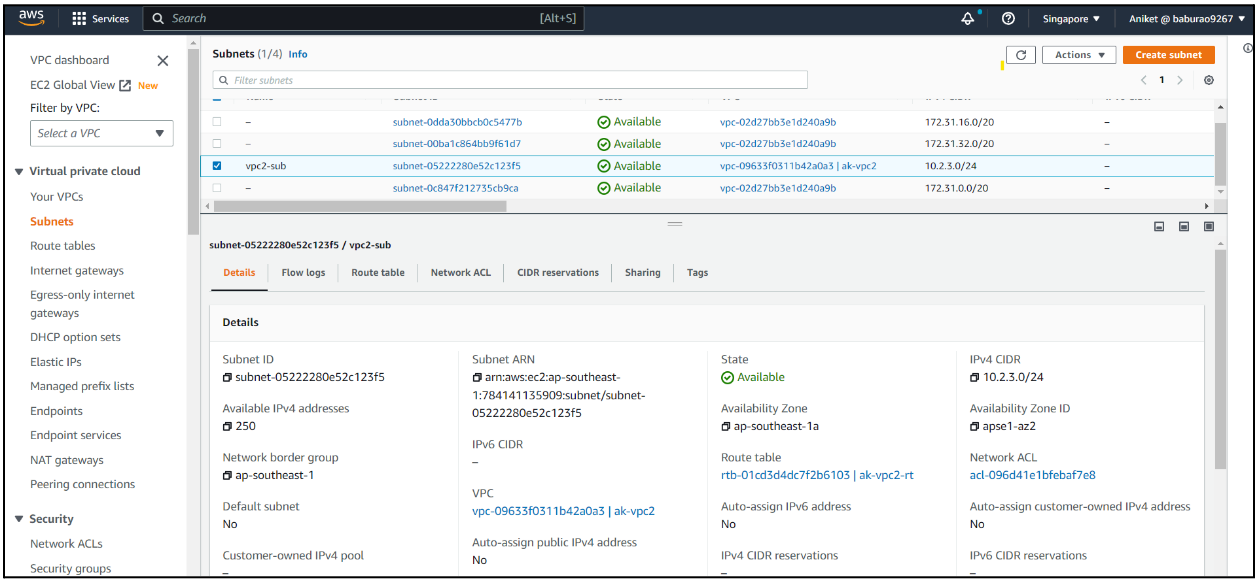
Details

VPC ID vpc-09633f0311b42a0a3	State ✓ Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-050e8671f3698c725	Main route table rtb-0b5de7624ea27369d	Main network ACL acl-096d41e1bfebaf7e8
Default VPC No	IPv4 CIDR 10.2.0.0/20	IPv6 pool –	IPv6 CIDR (Network border group) –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 784141135909	

CIDRs

Address type	CIDR	Network Border Group	Pool	Status
IPv4	10.2.0.0/20	–	–	✓ Associated

3. Now,create subnet with proper IPV4 CIDR.



Subnets (1/4)

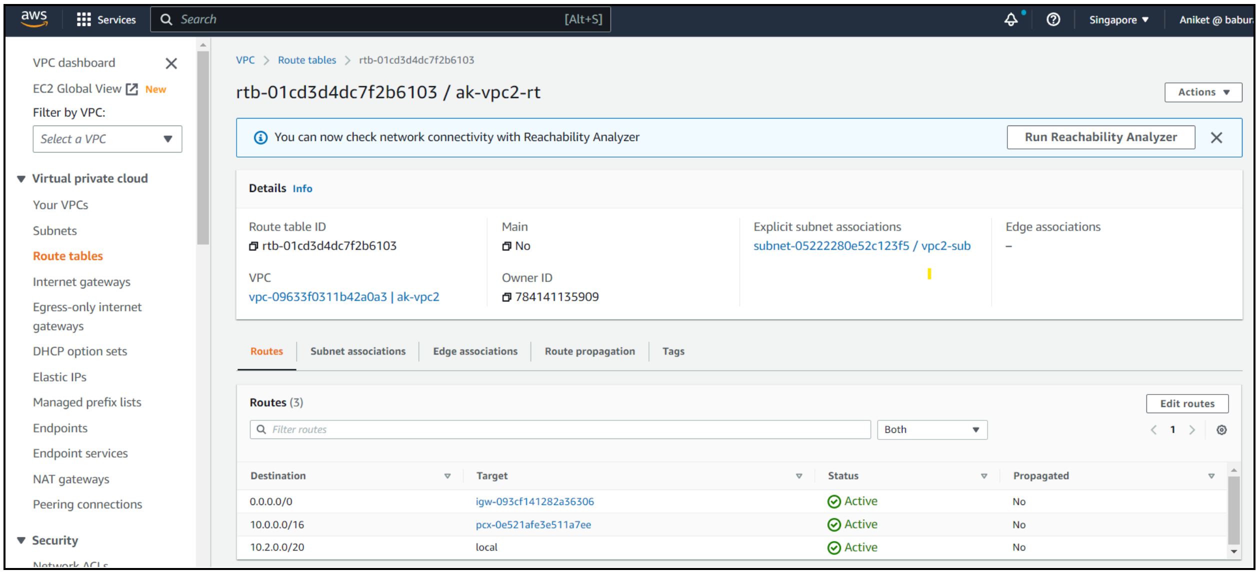
□	–	subnet-0dda30bbcb0c5477b	✓ Available	vpc-02d27bb3e1d240a9b	172.31.16.0/20	–
□	–	subnet-00ba1c864bb9f61d7	✓ Available	vpc-02d27bb3e1d240a9b	172.31.32.0/20	–
☑	vpc2-sub	subnet-05222280e52c123f5	✓ Available	vpc-09633f0311b42a0a3 | ak-vpc2	10.2.3.0/24	–
□	–	subnet-0c847f212735cb9ca	✓ Available	vpc-02d27bb3e1d240a9b	172.31.0.0/20	–

subnet-05222280e52c123f5 / vpc2-sub

Details

Subnet ID subnet-05222280e52c123f5	Subnet ARN arn:aws:ec2:ap-southeast-1:784141135909:subnet/subnet-05222280e52c123f5	State ✓ Available	IPv4 CIDR 10.2.3.0/24
Available IPv4 addresses 250	IPv6 CIDR –	Availability Zone ap-southeast-1a	Availability Zone ID apse1-az2
Network border group ap-southeast-1	VPC vpc-09633f0311b42a0a3 | ak-vpc2	Route table rtb-01cd3d4dc7f2b6103 | ak-vpc2-rt	Network ACL acl-096d41e1bfebaf7e8
Default subnet No	Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool –		IPv4 CIDR reservations –	IPv6 CIDR reservations –

4. Go to the internet gateway and create.
5. Now, attach **vpc2-igw** to the second VPC .



rtb-01cd3d4dc7f2b6103 / ak-vpc2-rt

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-01cd3d4dc7f2b6103

Main: No

Explicit subnet associations: subnet-05222280e52c123f5 / vpc2-sub

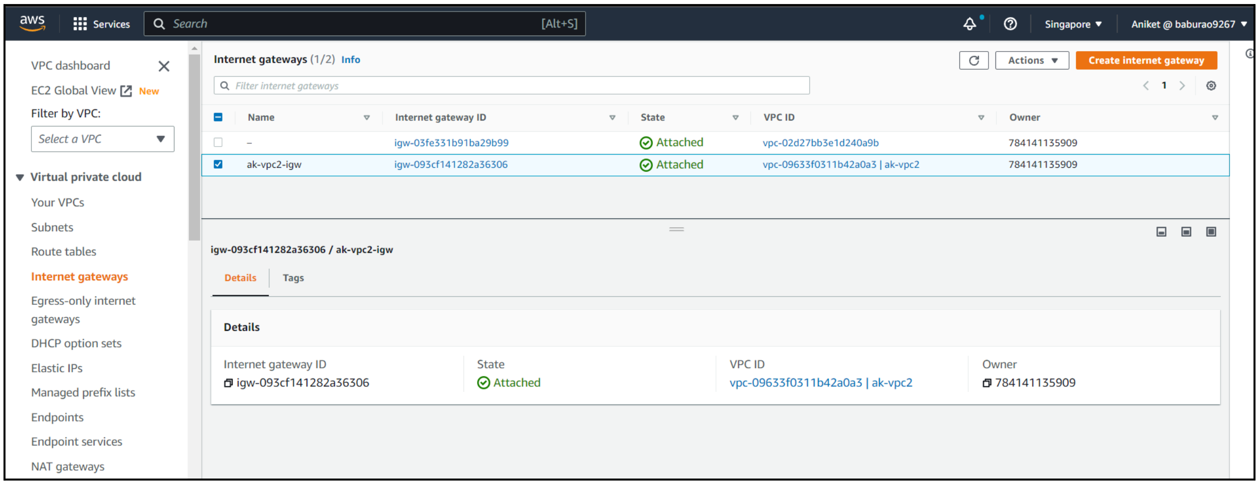
Edge associations: –

VPC: vpc-09633f0311b42a0a3 | ak-vpc2

Owner ID: 784141135909

Routes (3)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-093cf141282a36306	Active	No
10.0.0.0/16	pcx-0e521afe3e511a7ee	Active	No
10.2.0.0/20	local	Active	No



Internet gateways (1/2) Info

	Name	Internet gateway ID	State	VPC ID	Owner
□	–	igw-03fe331b91ba29b99	Attached	vpc-02d27bb3e1d240a9b	784141135909
☑	ak-vpc2-igw	igw-093cf141282a36306	Attached	vpc-09633f0311b42a0a3 | ak-vpc2	784141135909

igw-093cf141282a36306 / ak-vpc2-igw

Details

Internet gateway ID: igw-093cf141282a36306

State: Attached

VPC ID: vpc-09633f0311b42a0a3 | ak-vpc2

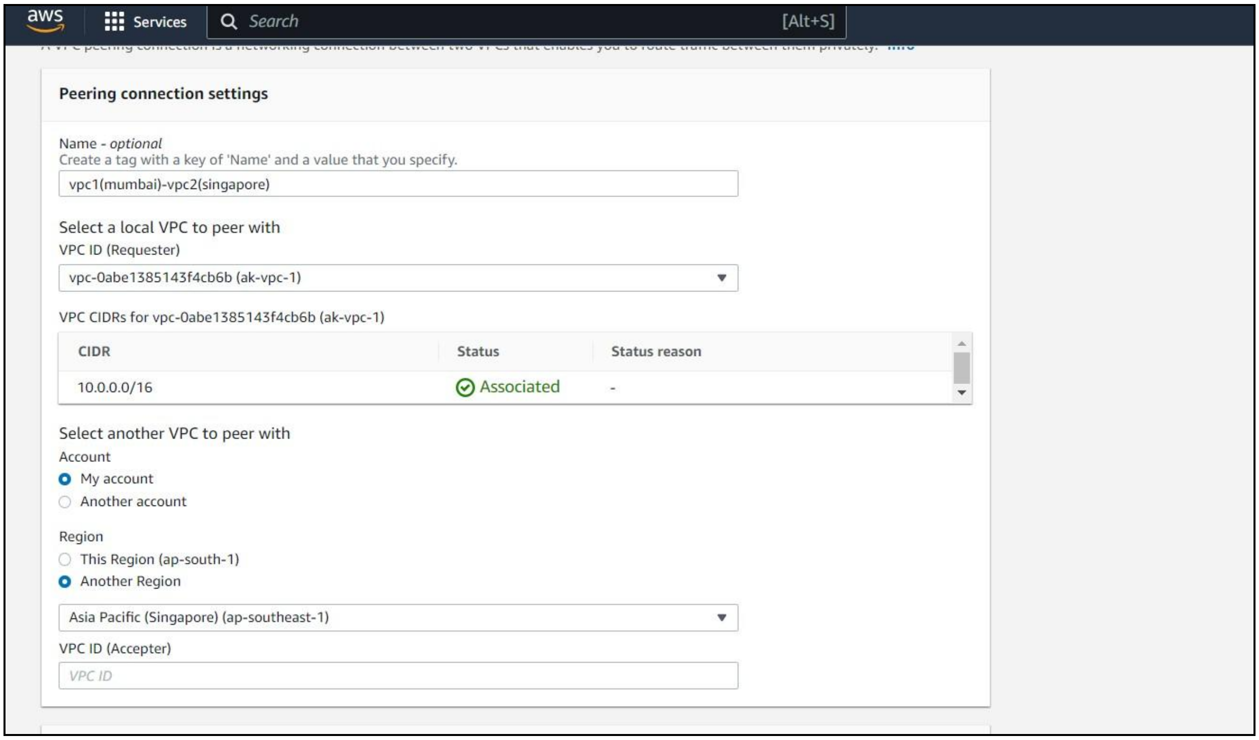
Owner: 784141135909

6. Create a route table and route all ip (**0.0.0.0/0**) to **ak-vpc2-igw**.
7. Go to the subnet association then add the subnet to the **route table.**

We have created two VPC in two different regions. Now, we need to make the connection between them that enables you to route traffic between them using private IPV4 addresses or IPv6 addresses. This connection between two VPC is called a **VPC peering connection**.

Step 6 : Make peering connection between **VPC-1 (Mumbai)** and **VPC-2 (Singapore)**

1. First name for the peering connection
2. From VPC-2(**Mumbai**) is (**requester**) peering the connection with another VPC.
3. The connection will be established with VPC-2(**Singapore**) as the **acceptor**.



A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info

Peering connection settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
vpc1(mumbai)-vpc2(singapore)

Select a local VPC to peer with
VPC ID (Requester)
vpc-0abe1385143f4cb6b (ak-vpc-1)

VPC CIDRs for vpc-0abe1385143f4cb6b (ak-vpc-1)

CIDR	Status	Status reason
10.0.0.0/16	✓ Associated	-

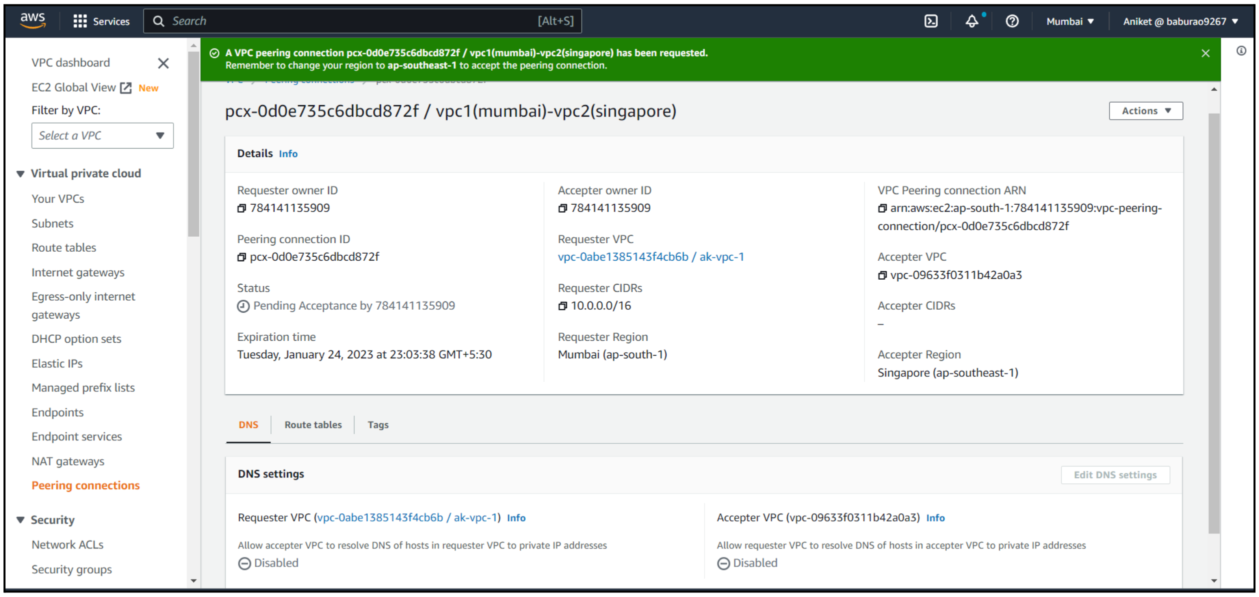
Select another VPC to peer with
Account
● My account
○ Another account

Region
○ This Region (ap-south-1)
● Another Region

Asia Pacific (Singapore) (ap-southeast-1)

VPC ID (Accepter)
VPC ID

4. Select another region in **Asia Pacific (Singapore)(ap-southeast-1).**
5. Give **VPC-2(Singapore**) ID then click create VPC peering connection.



A VPC peering connection pcx-0d0e735c6dbcd872f / vpc1(mumbai)-vpc2(singapore) has been requested.
Remember to change your region to **ap-southeast-1** to accept the peering connection.

pcx-0d0e735c6dbcd872f / vpc1(mumbai)-vpc2(singapore)

Details Info

Requester owner ID
784141135909

Peering connection ID
pcx-0d0e735c6dbcd872f

Status
Pending Acceptance by 784141135909

Expiration time
Tuesday, January 24, 2023 at 23:03:38 GMT+5:30

Accepter owner ID
784141135909

Requester VPC
vpc-0abe1385143f4cb6b / ak-vpc-1

Requester CIDRs
10.0.0.0/16

Requester Region
Mumbai (ap-south-1)

VPC Peering connection ARN
arn:aws:ec2:ap-south-1:784141135909:vpc-peering-connection/pcx-0d0e735c6dbcd872f

Accepter VPC
vpc-09633f0311b42a0a3

Accepter CIDRs
–

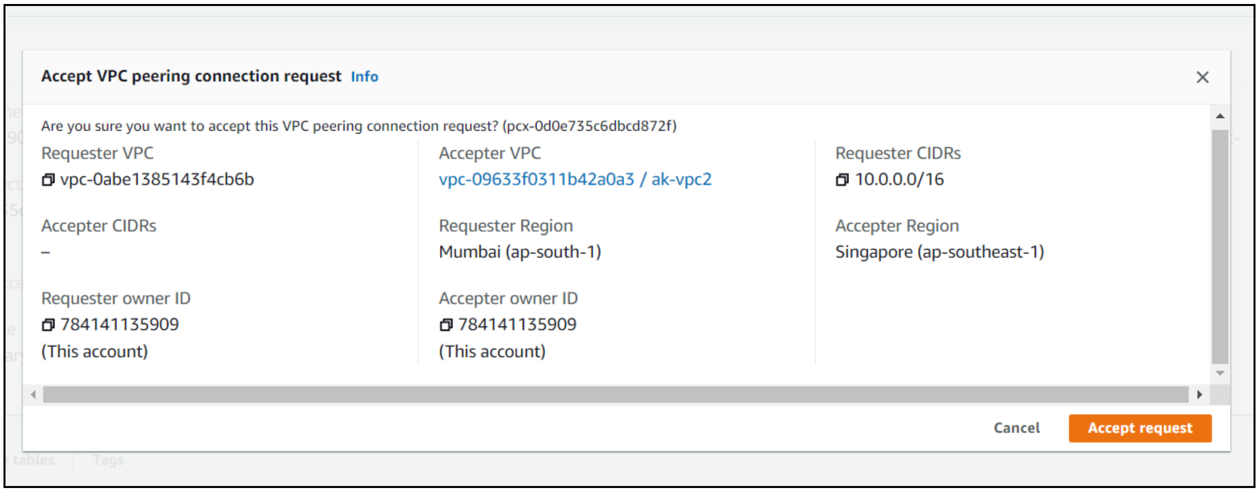
Accepter Region
Singapore (ap-southeast-1)

DNS settings

Requester VPC (vpc-0abe1385143f4cb6b / ak-vpc-1) Info
Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
Disabled

Accepter VPC (vpc-09633f0311b42a0a3) Info
Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
Disabled

6. After creating a connection, status shows pending accept request from **VPC-2(Singapore).**
7. Go to the **Singapore** region VPC and accept a peering connection request.

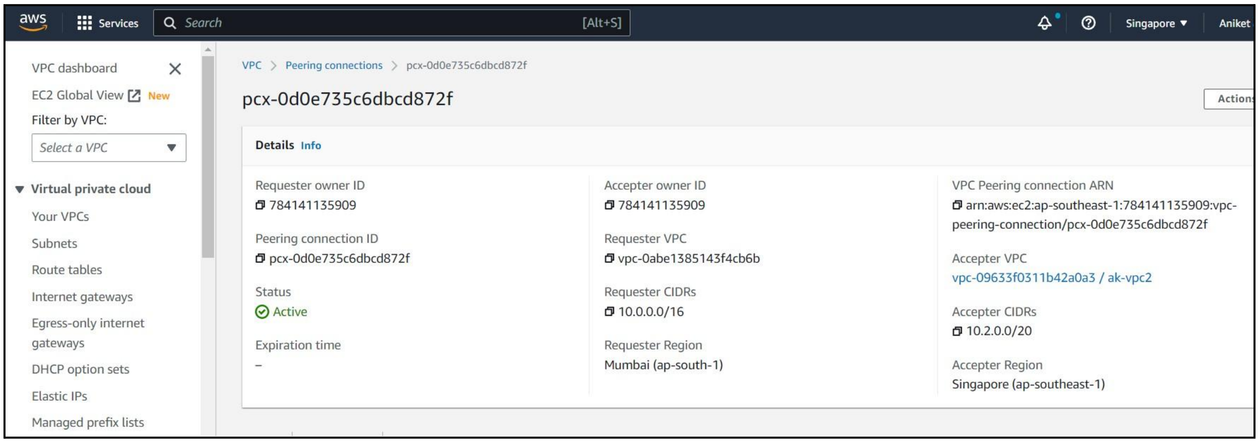


Accept VPC peering connection request Info

Are you sure you want to accept this VPC peering connection request? (pcx-0d0e735c6dbcd872f)

Requester VPC vpc-0abe1385143f4cb6b	Accepter VPC vpc-09633f0311b42a0a3 / ak-vpc2	Requester CIDRs 10.0.0.0/16
Accepter CIDRs –	Requester Region Mumbai (ap-south-1)	Accepter Region Singapore (ap-southeast-1)
Requester owner ID 784141135909 (This account)	Accepter owner ID 784141135909 (This account)	

8. Now the peering connection status is **active**.



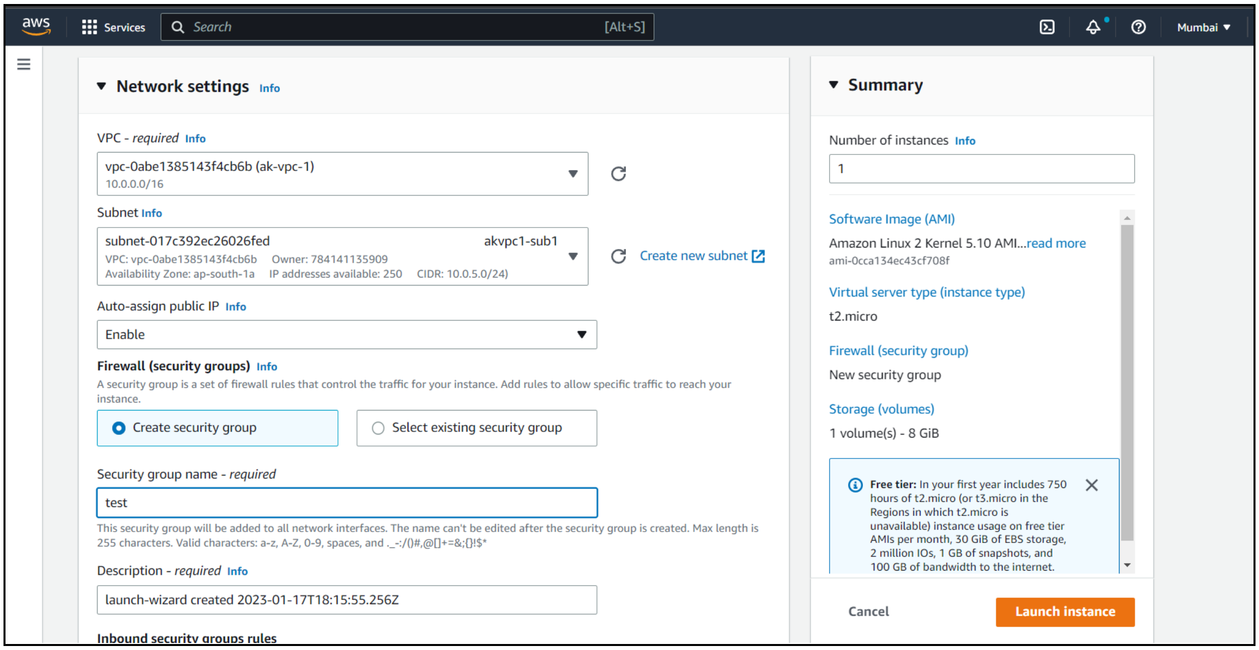
pcx-0d0e735c6dbcd872f

Details Info

Requester owner ID 784141135909	Accepter owner ID 784141135909	VPC Peering connection ARN arn:aws:ec2:ap-southeast-1:784141135909:vpc-peering-connection/pcx-0d0e735c6dbcd872f
Peering connection ID pcx-0d0e735c6dbcd872f	Requester VPC vpc-0abe1385143f4cb6b	Accepter VPC vpc-09633f0311b42a0a3 / ak-vpc2
Status ✓ Active	Requester CIDRs 10.0.0.0/16	Accepter CIDRs 10.2.0.0/20
Expiration time –	Requester Region Mumbai (ap-south-1)	Accepter Region Singapore (ap-southeast-1)

Step 7: Launch EC2 instance in both region with their custom VPC-1(Mumbai) with availability zone subnet in Mumbai(ap-south-1a) and VPC-2(Singapore) with subnet in availability zone Singapore(ap-southeast-1a) respectively.

1. Name the instance, then select Amazon AMI and select the key pair if not, then create a new key pair that you use to securely connect to your instance.



Network settings Info

VPC - *required* Info

vpc-0abe1385143f4cb6b (ak-vpc-1)
10.0.0.0/16

Subnet Info

subnet-017c392ec26026fed akvpc1-sub1
VPC: vpc-0abe1385143f4cb6b Owner: 784141135909
Availability Zone: ap-south-1a IP addresses available: 250 CIDR: 10.0.5.0/24)

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

test

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard created 2023-01-17T18:15:55.256Z

Inbound security groups rules

Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0cca134ec43cf708f

Virtual server type (instance type)
t2.micro

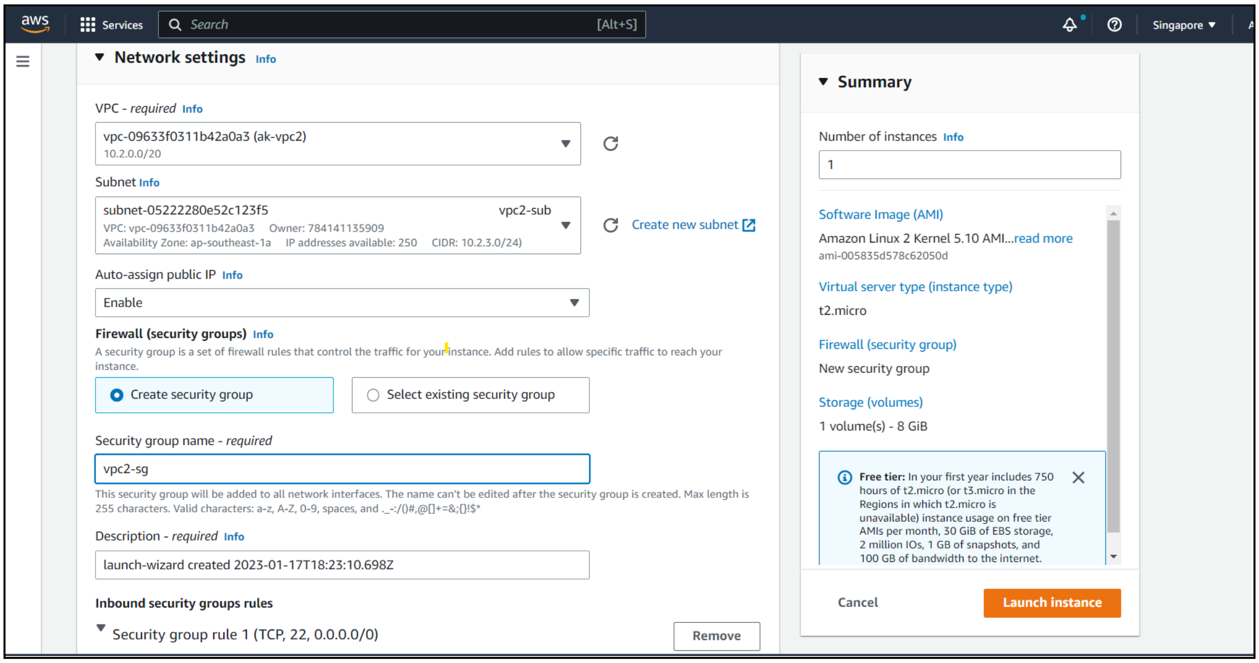
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

2. In the network setting click edit and select custom **VPC-1(Mumbai)** then select the same vpc subnet.
3. Enable auto-assigned public ip.
4. Create a new Firewall(Security group).
5. Launch Instance

Step 8: Launch an EC2 instance in the **Singapore region.**



Network settings Info

VPC - *required* Info

vpc-09633f0311b42a0a3 (ak-vpc2)
10.2.0.0/20

Subnet Info

subnet-05222280e52c123f5 vpc2-sub
VPC: vpc-09633f0311b42a0a3 Owner: 784141135909
Availability Zone: ap-southeast-1a IP addresses available: 250 CIDR: 10.2.3.0/24)

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

vpc2-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard created 2023-01-17T18:23:10.698Z

Inbound security groups rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-005835d578c62050d

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

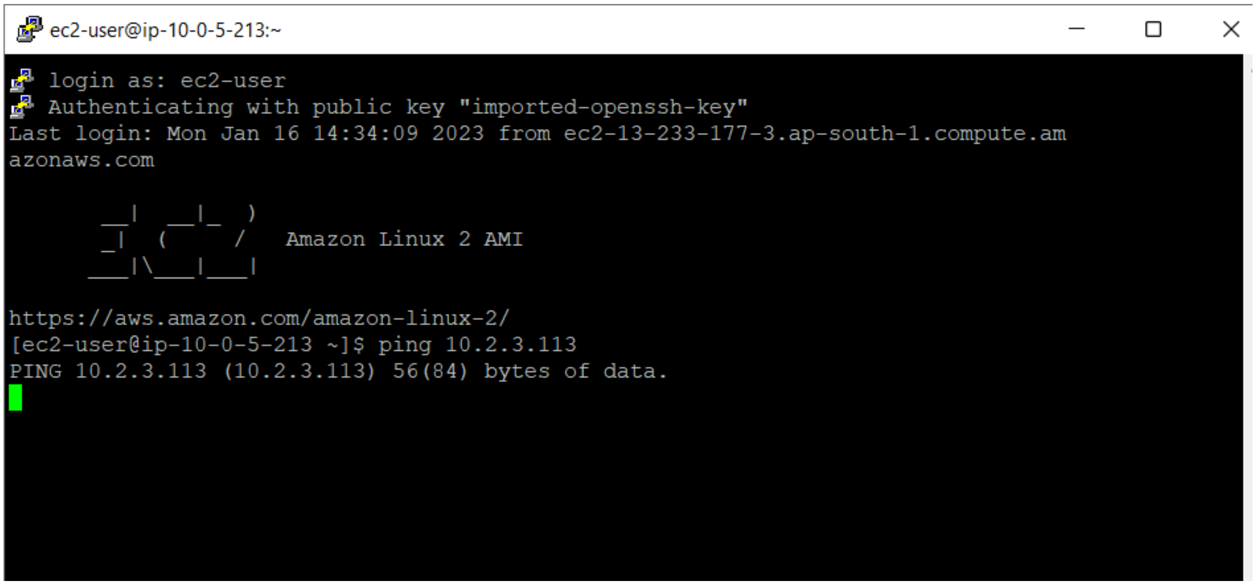
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

1. Name the instance then select the created key pair.
2. In the network setting click edit and select custom **VPC-2(Singapore)** then select the same vpc subnet.
3. Enable auto-assigned public ip.
4. Create a new Firewall(Security group).
5. Launch Instance

Step 9 : Now after EC2 instance created check whether the both vpc instance ping each other or not

1. In my case I use Putty as SSH client and login both instance as **ec2-user**

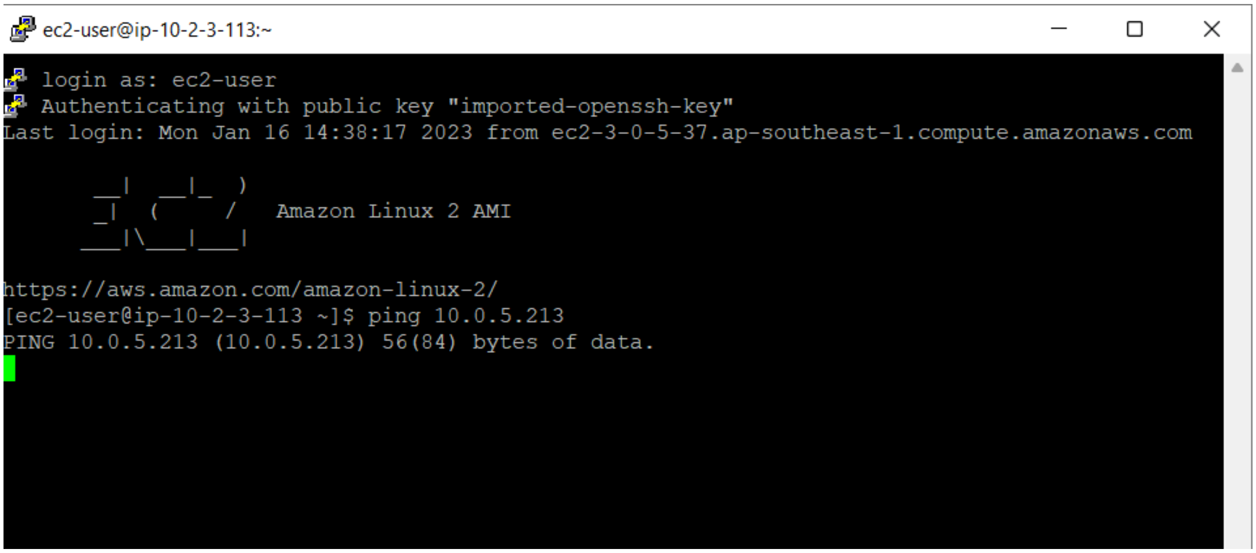


```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon Jan 16 14:34:09 2023 from ec2-13-233-177-3.ap-south-1.compute.am
azonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-5-213 ~]$ ping 10.2.3.113
PING 10.2.3.113 (10.2.3.113) 56(84) bytes of data.
```

Mumbai-server



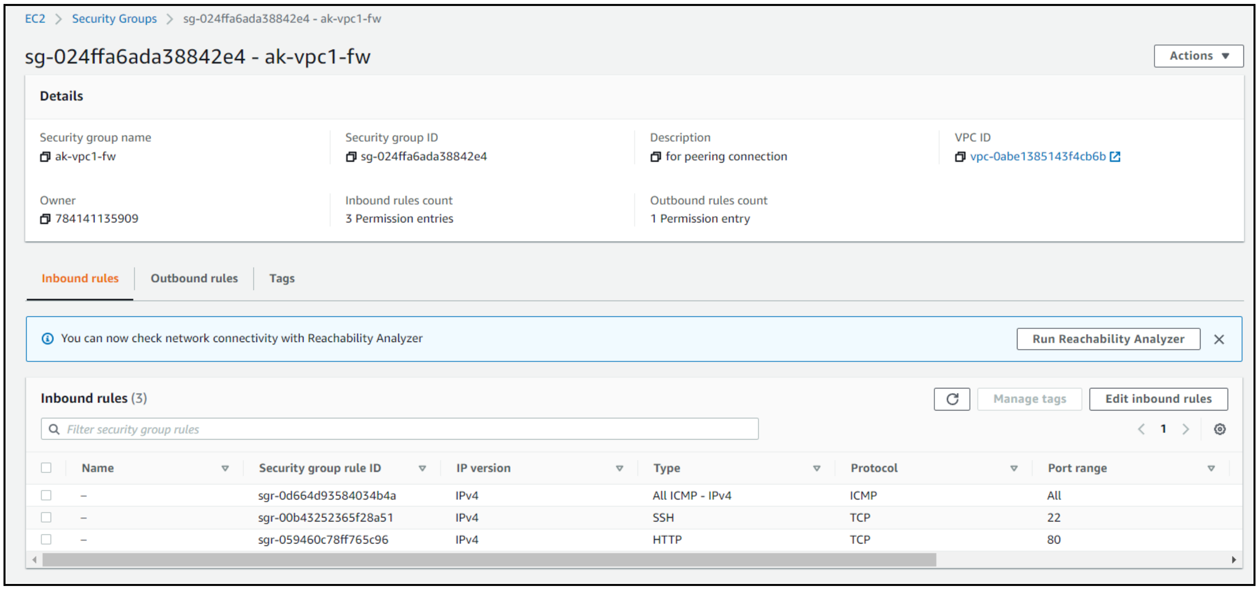
```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon Jan 16 14:38:17 2023 from ec2-3-0-5-37.ap-southeast-1.compute.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-2-3-113 ~]$ ping 10.0.5.213
PING 10.0.5.213 (10.0.5.213) 56(84) bytes of data.
```

Singapore-server

2. To check connection the **ping** command is used but still private ip not ping to each other
3. To ping the connection it required the **ICMP** protocol.
4. In the both instance security group edit inbound rules ,add **ALL ICMP IPV4** protocol routes through internet traffic (**0.0.0.0/0**).



EC2 > Security Groups > sg-024ffa6ada38842e4 - ak-vpc1-fw

sg-024ffa6ada38842e4 - ak-vpc1-fw

Details

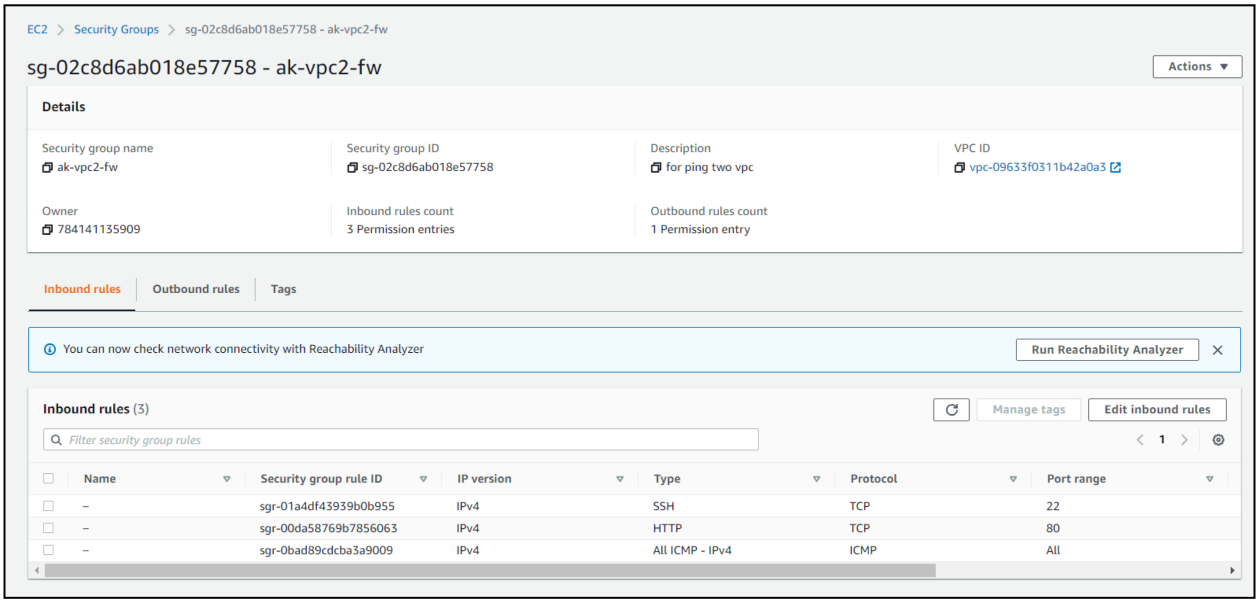
Security group name	Security group ID	Description	VPC ID
ak-vpc1-fw	sg-024ffa6ada38842e4	for peering connection	vpc-0abe1385143f4cb6b
Owner	**Inbound rules count**	**Outbound rules count**	
784141135909	3 Permission entries	1 Permission entry	

You can now check network connectivity with Reachability Analyzer

Inbound rules (3)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-0d664d93584034b4a	IPv4	All ICMP - IPv4	ICMP	All
□	–	sgr-00b43252365f28a51	IPv4	SSH	TCP	22
□	–	sgr-059460c78ff765c96	IPv4	HTTP	TCP	80

Mumbai-server security group



EC2 > Security Groups > sg-02c8d6ab018e57758 - ak-vpc2-fw

sg-02c8d6ab018e57758 - ak-vpc2-fw

Details

Security group name	Security group ID	Description	VPC ID
ak-vpc2-fw	sg-02c8d6ab018e57758	for ping two vpc	vpc-09633f0311b42a0a3
Owner	**Inbound rules count**	**Outbound rules count**	
784141135909	3 Permission entries	1 Permission entry	

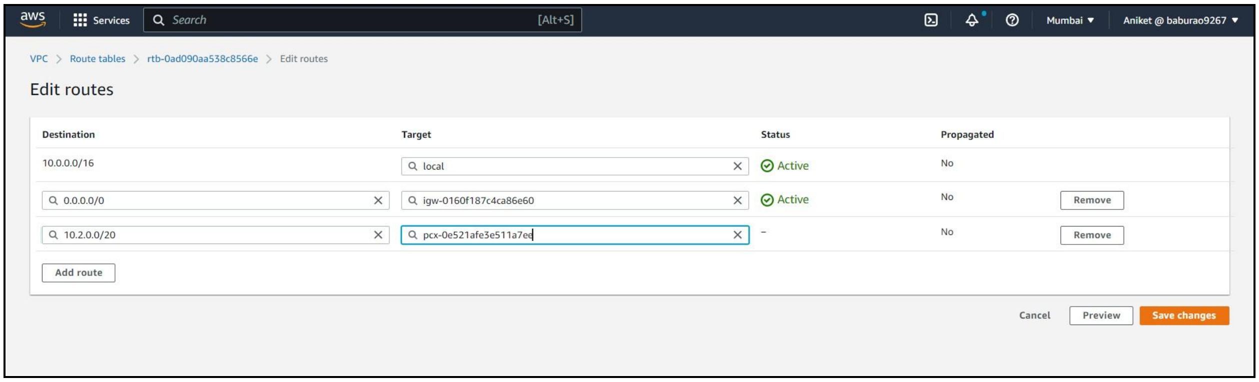
You can now check network connectivity with Reachability Analyzer

Inbound rules (3)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	sgr-01a4df43939b0b955	IPv4	SSH	TCP	22
□	–	sgr-00da58769b7856063	IPv4	HTTP	TCP	80
□	–	sgr-0bad89cdcba3a9009	IPv4	All ICMP - IPv4	ICMP	All

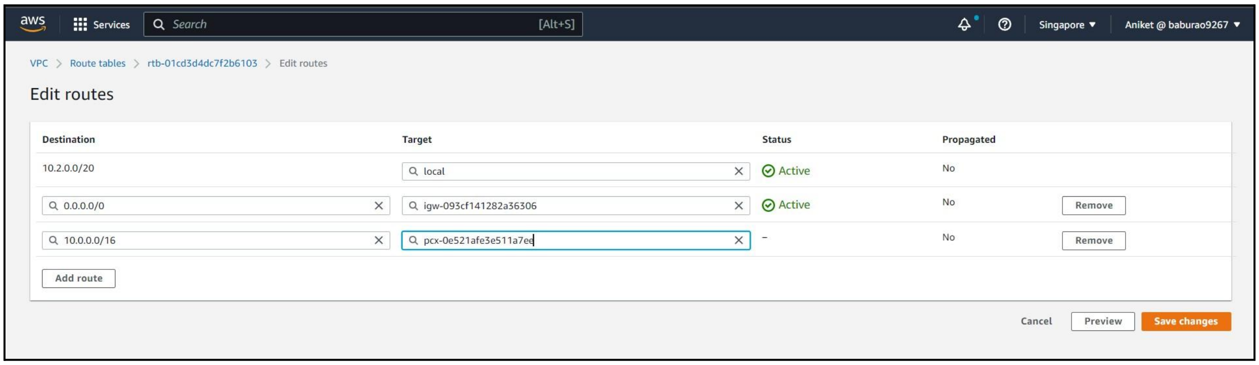
Singapore-server security group

5. Also allow **mumbai-server** and **singapore-server** instance private ip traffic to the VPC-2(singapore) and VPC-1(mumbai) respectively.



Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-0160f187c4ca86e60	Active	No	Remove
10.2.0.0/20	pcx-0e521afe3e511a7ee	-	No	Remove

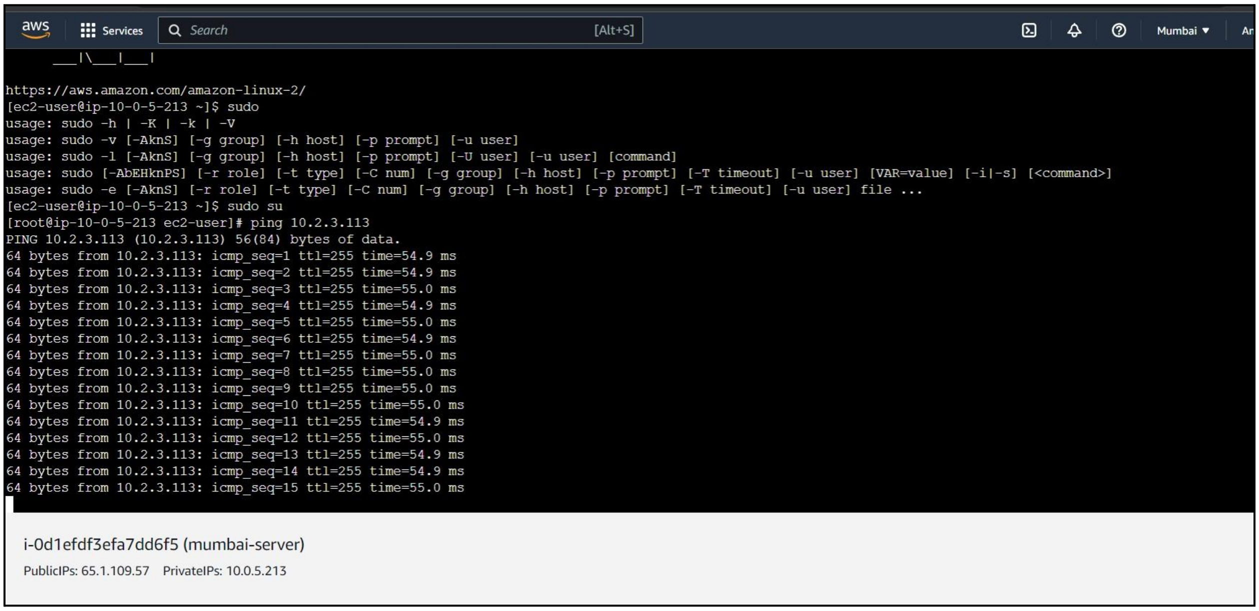
Vpc-1 route table



Destination	Target	Status	Propagated	
10.2.0.0/20	local	Active	No	
0.0.0.0/0	igw-093cf141282a36306	Active	No	Remove
10.0.0.0/16	pcx-0e521afe3e511a7ee	-	No	Remove

Vpc-2 route table

6. Also we have set route traffic of the created peering connection of VPC-1 and VPC-2.
7. In **vpc1-rt** add VPC-2 peering connection IPV4 address route.
8. and in **vpc2-rt** add vpc1 peering connection route.
9. Now check whether **VPC's** are pinging or not.

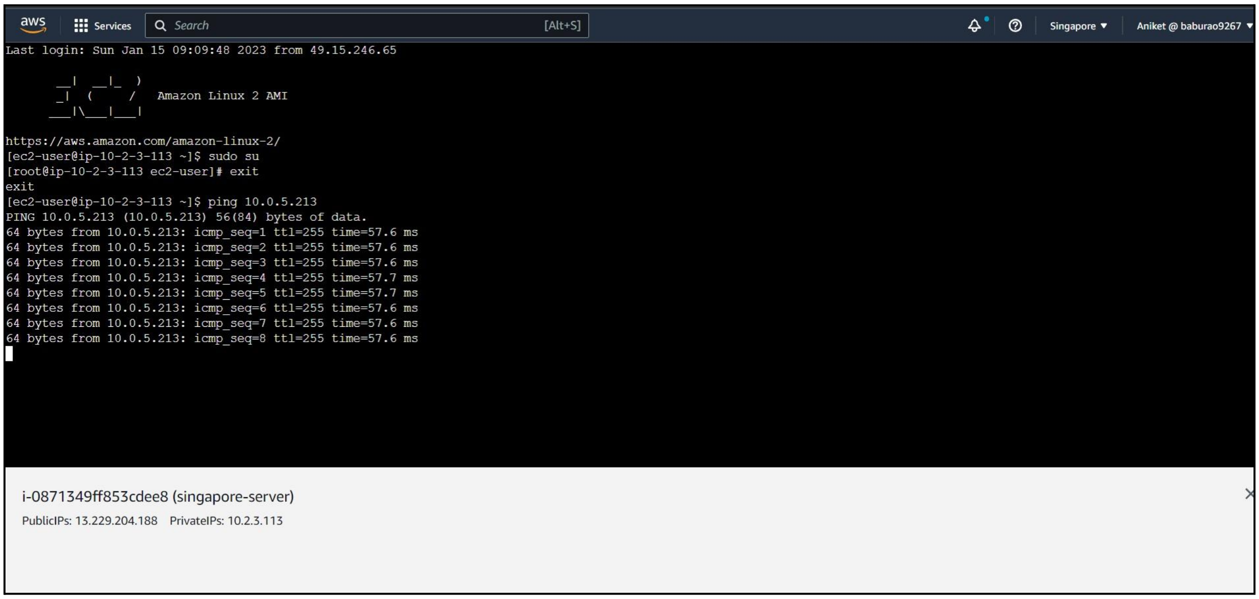


```
     ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-5-213 ~]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
[ec2-user@ip-10-0-5-213 ~]$ sudo su
[root@ip-10-0-5-213 ec2-user]# ping 10.2.3.113
PING 10.2.3.113 (10.2.3.113) 56(84) bytes of data.
64 bytes from 10.2.3.113: icmp_seq=1 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=2 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=3 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=4 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=5 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=6 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=7 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=8 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=9 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=10 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=11 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=12 ttl=255 time=55.0 ms
64 bytes from 10.2.3.113: icmp_seq=13 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=14 ttl=255 time=54.9 ms
64 bytes from 10.2.3.113: icmp_seq=15 ttl=255 time=55.0 ms
```

i-0d1efdf3efa7dd6f5 (mumbai-server)

PublicIPs: 65.1.109.57   PrivateIPs: 10.0.5.213



```
Last login: Sun Jan 15 09:09:48 2023 from 49.15.246.65

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-2-3-113 ~]$ sudo su
[root@ip-10-2-3-113 ec2-user]# exit
exit
[ec2-user@ip-10-2-3-113 ~]$ ping 10.0.5.213
PING 10.0.5.213 (10.0.5.213) 56(84) bytes of data.
64 bytes from 10.0.5.213: icmp_seq=1 ttl=255 time=57.6 ms
64 bytes from 10.0.5.213: icmp_seq=2 ttl=255 time=57.6 ms
64 bytes from 10.0.5.213: icmp_seq=3 ttl=255 time=57.6 ms
64 bytes from 10.0.5.213: icmp_seq=4 ttl=255 time=57.7 ms
64 bytes from 10.0.5.213: icmp_seq=5 ttl=255 time=57.7 ms
64 bytes from 10.0.5.213: icmp_seq=6 ttl=255 time=57.6 ms
64 bytes from 10.0.5.213: icmp_seq=7 ttl=255 time=57.6 ms
64 bytes from 10.0.5.213: icmp_seq=8 ttl=255 time=57.6 ms
```

i-0871349ff853cdee8 (singapore-server)

PublicIPs: 13.229.204.188 PrivateIPs: 10.2.3.113

VPC-1 Mumbai (ap-south1) peering connection is successfully and securely established with **VPC-2 Singapore (ap-southeast-1)** without an internet gateway. Their EC2 instance are pinging each other, as shown in above figure.