Creating peering connection between two VPCs

A **peering connection** is a networking connection between two Virtual Private Clouds (VPCs) that enables them to communicate with each other using private IP addresses. It allows resources within the connected VPCs to communicate as if they were within the same network.

VPC peering enables direct communication between VPCs in the same or different AWS accounts, within the same AWS region or across different regions. It does not require internet gateways, VPN connections, or NAT devices. It privately connects using **private IP** addresses.

The IP ranges of the VPCs being peered **must not overlap**. This ensures that the IP addressing remains unique and does not conflict between the connected VPCs.

Peering connections do not provide any **network security** or routing control mechanisms. Security groups and network ACLs should be configured appropriately to control inbound and outbound traffic between the peered VPCs. (Stateless)

There are a few limitations to be aware of when working with VPC peering.

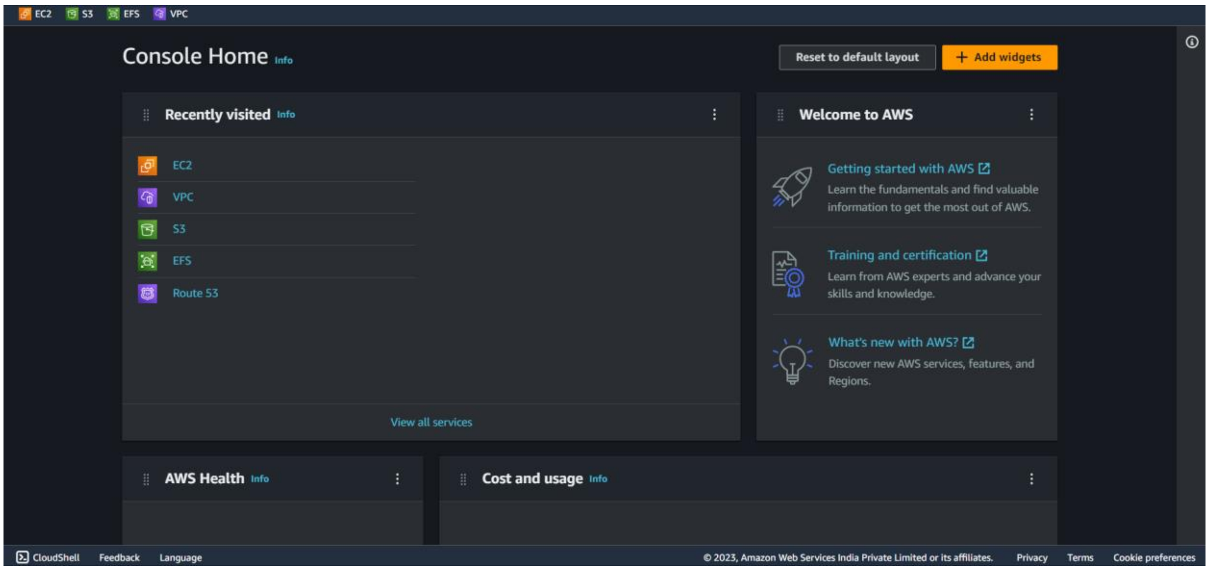
- VPC peering is not transitive across more than two VPCs
- Communication between VPCs in different AWS accounts requires appropriate routing and security configurations.

AWS also supports VPC peering across different AWS regions.

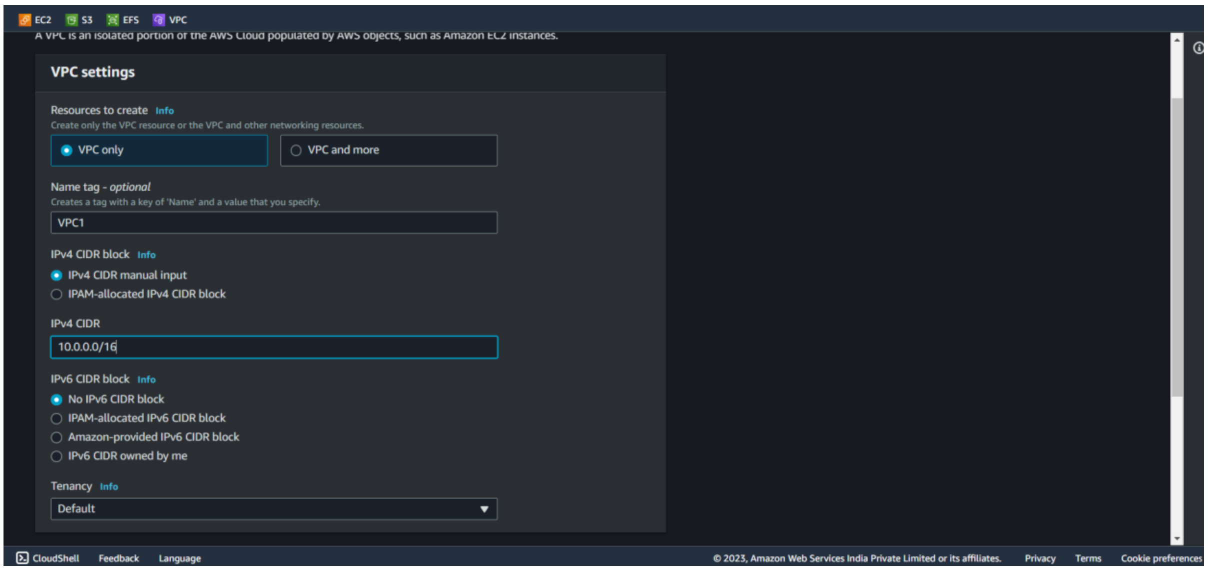
- This enables communication between VPCs in different geographic regions while maintaining the benefits of private connectivity.
- All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck.

There is no charge to create a VPC peering connection. All data transfer over a VPC Peering connection that stays within an Availability Zone (AZ) is free. Charges apply for data transfer over a VPC Peering connections that cross Availability Zones and Regions

1. Firstly Login to your AWS account open Console Home and select VPC.


EC2
S3
EFS
VPC
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
EC2
VPC
S3
EFS
Route 53
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health Info
Cost and usage Info
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

2. Go to your VPCs and select Create VPC to create a Custom VPC.
   Now name your custom VPC as VPC1 and set the respective CIDR to your VPC here I’ve set it to 10.0.0.0/16 i.e., 256*256 hosts can be configured.
   We cannot change the CIDR of an allotted VPC hence AWS suggest to overprovision as they do not charge for allocation.


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.
VPC1

IPv4 CIDR block Info
[✓ IPv4 CIDR manual input]
IPAM-allocated IPv4 CIDR block

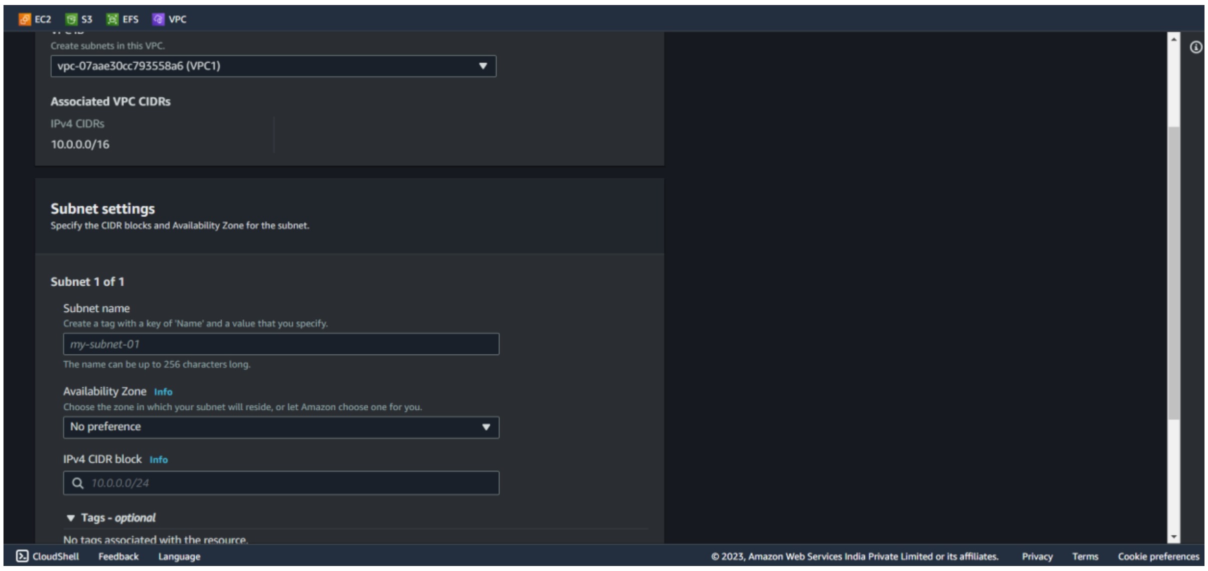
IPv4 CIDR
10.0.0.0/16

IPv6 CIDR block Info
[✓ No IPv6 CIDR block]
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me

Tenancy Info
Default

EC2
S3
EFS
VPC
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

3. Now create a subnet for your VPC for that go to subnets and click on create subnets and set the respective subnet settings in you custom VPC i.e., (VPC1 here)
   Name the subnet and set the availability zone and set the respective CIDR here I’ve set it as 10.0.1.0/24 i.e., (255 hosts)



Create subnets in this VPC.
vpc-07aae30cc793558a6 (VPC1)

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.
my-subnet-01
The name can be up to 256 characters long.

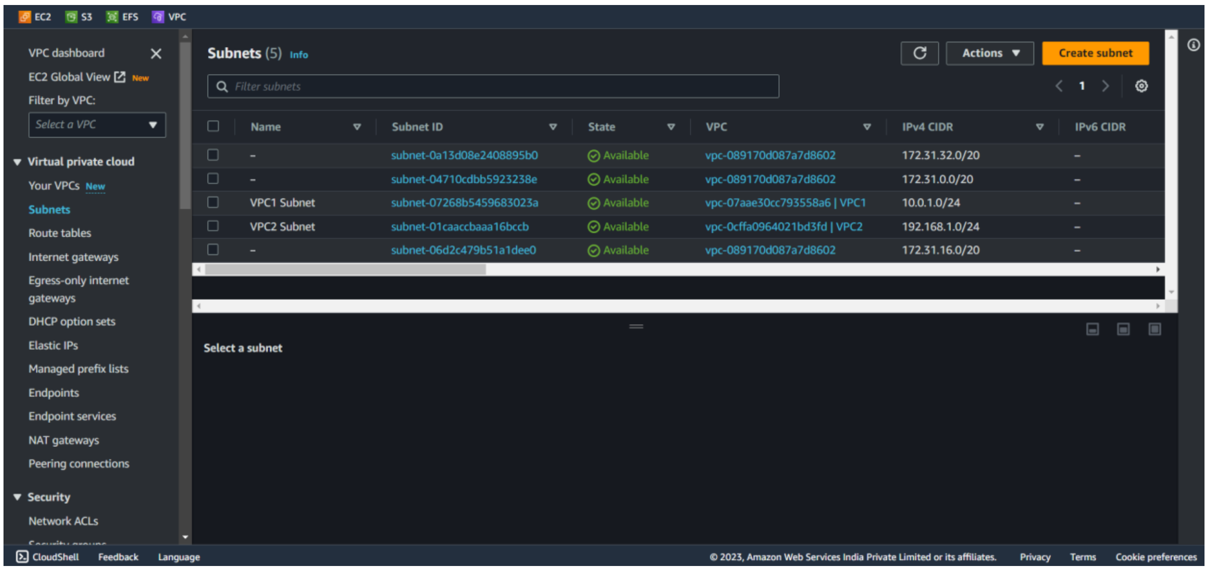
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
10.0.0.0/24

▼ Tags - *optional*
No tags associated with the resource.

© 2023, Amazon Web Services India Private Limited or its affiliates.

4. Similarly create a VPC and subnet in same availability zone naming VPC2 and Subnet2 in another availability zone but in same region since inter region data transfer is not free in AWS free tier



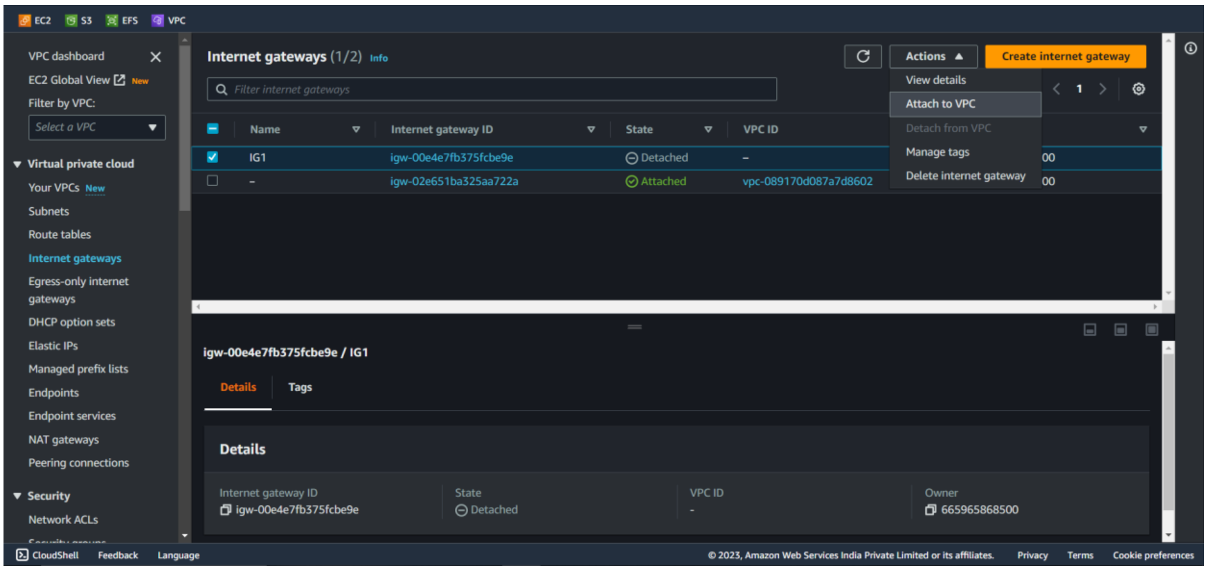
Subnets (5) Info

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
–	subnet-0a13d08e2408895b0	Available	vpc-089170d087a7d8602	172.31.32.0/20	–
–	subnet-04710cdbb5923238e	Available	vpc-089170d087a7d8602	172.31.0.0/20	–
VPC1 Subnet	subnet-07268b5459683023a	Available	vpc-07aae30cc793558a6 | VPC1	10.0.1.0/24	–
VPC2 Subnet	subnet-01caaccbaaa16bccb	Available	vpc-0cffa0964021bd3fd | VPC2	192.168.1.0/24	–
–	subnet-06d2c479b51a1dee0	Available	vpc-089170d087a7d8602	172.31.16.0/20	–

Select a subnet

© 2023, Amazon Web Services India Private Limited or its affiliates.

5. Now Create internet gateways for both the VPCs for that go to internet gateways and click on create internet gateways and attach the IG to respective VPC.



Internet gateways (1/2) Info

Name	Internet gateway ID	State	VPC ID	
IG1	igw-00e4e7fb375fcbe9e	Detached	–	00
–	igw-02e651ba325aa722a	Attached	vpc-089170d087a7d8602	00

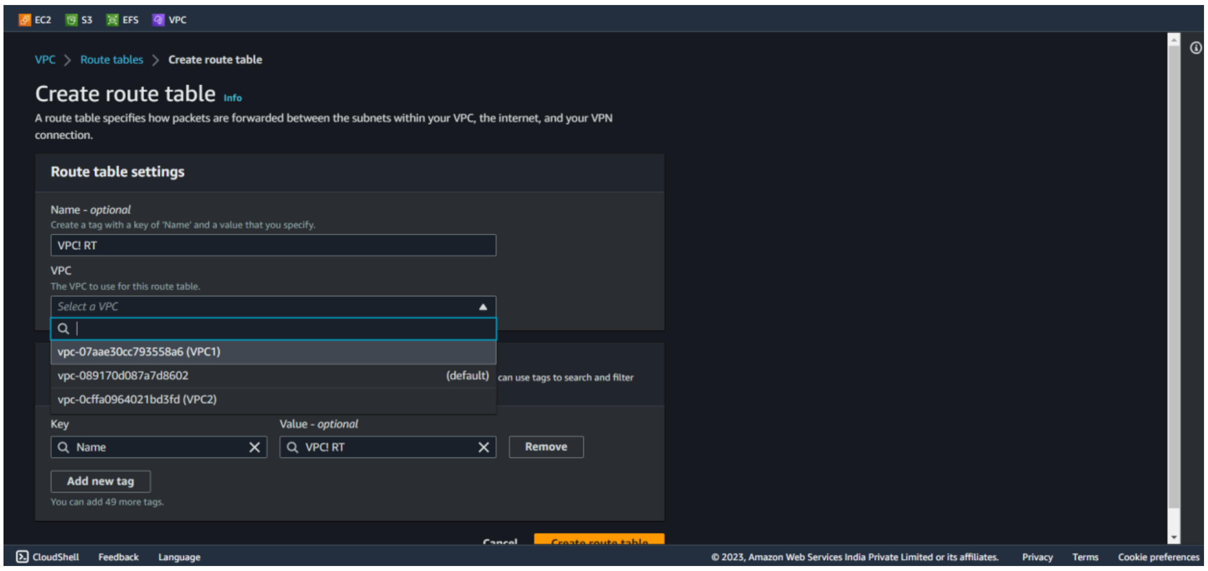
igw-00e4e7fb375fcbe9e / IG1

Details

Internet gateway ID	State	VPC ID	Owner
igw-00e4e7fb375fcbe9e	Detached	-	665965868500

© 2023, Amazon Web Services India Private Limited or its affiliates.

6. Now create a route table for both VPCs to route the traffic for that go to Route tables and click on create route table and select the respective VPC and click on create route table.



Create route table Info

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.
VPC! RT

VPC
The VPC to use for this route table.
Select a VPC
vpc-07aae30cc793558a6 (VPC1)
vpc-089170d087a7d8602 (default)
vpc-0cffa0964021bd3fd (VPC2)

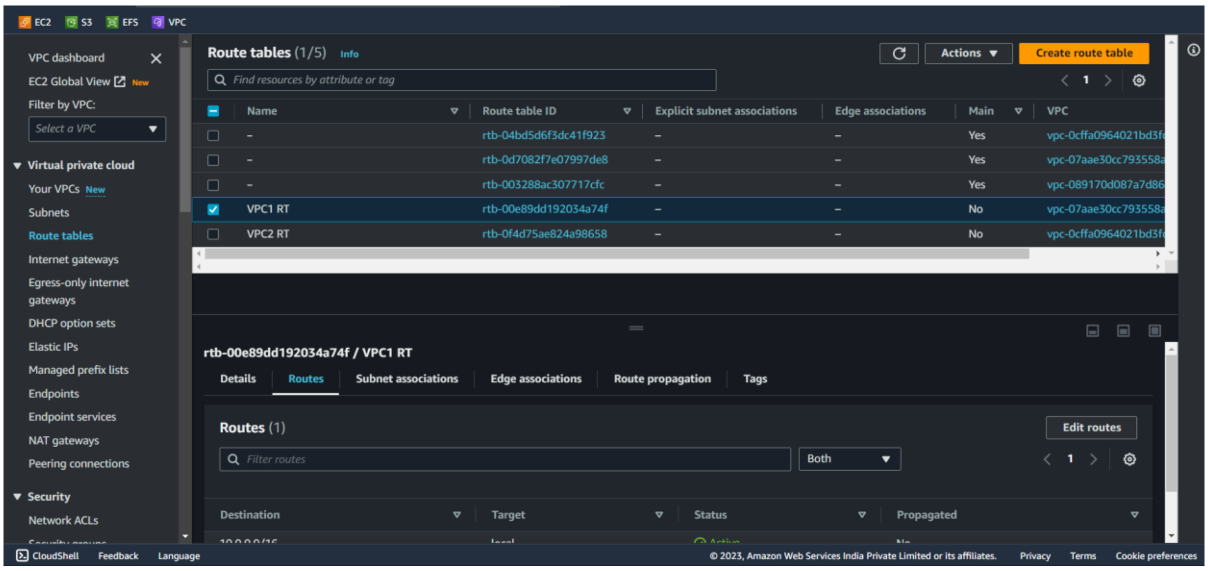
can use tags to search and filter

Key	Value - *optional*
Name	VPC! RT

You can add 49 more tags.

© 2023, Amazon Web Services India Private Limited or its affiliates.

7. Now select the Route table and select on routes and click on edit routes and set the internet gateway as a route.


Route tables (1/5) Info

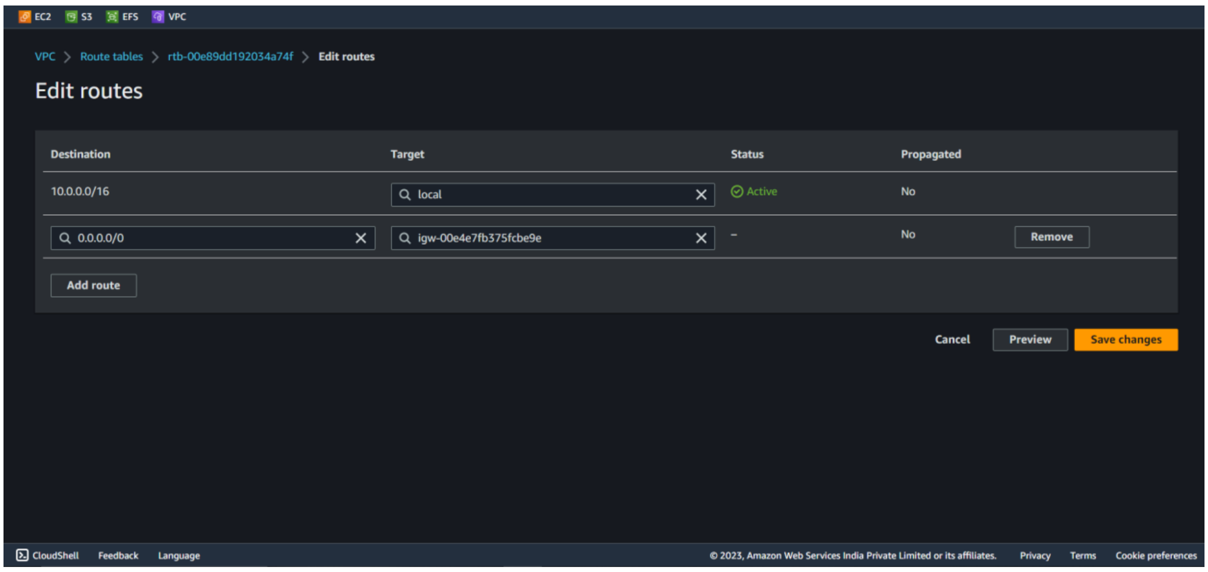
Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
–	rtb-04bd5d6f3dc41f923	–	–	Yes	vpc-0cffa0964021bd3f
–	rtb-0d7082f7e07997de8	–	–	Yes	vpc-07aae30cc793558a
–	rtb-003288ac307717cfc	–	–	Yes	vpc-089170d087a7d86
✓ VPC1 RT	rtb-00e89dd192034a74f	–	–	No	vpc-07aae30cc793558a
VPC2 RT	rtb-0f4d75ae824a98658	–	–	No	vpc-0cffa0964021bd3f

rtb-00e89dd192034a74f / VPC1 RT

Routes (1)

Destination	Target	Status	Propagated

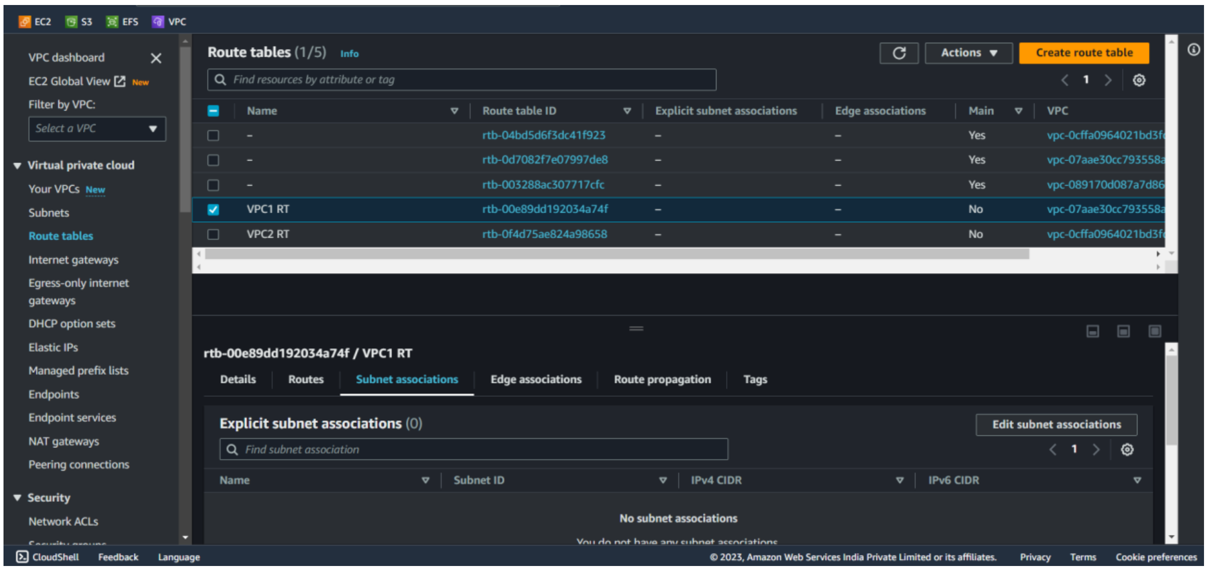
By adding an internet gateway as a route in the route table, you enable resources within the VPC to communicate with the internet. This allows instances in the VPC to access resources outside of the VPC, such as websites, external APIs, and other internet-based services.


VPC > Route tables > rtb-00e89dd192034a74f > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-00e4e7fb375fcbe9e	-	No

8. Now associate the respective subnet to the VPC to route the traffic to end devices in the subnet. For that click on subnet associations in the route table and click on edit subnet associations.



Route tables (1/5) Info

	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
☐	–	rtb-04bd5d6f3dc41f923	–	–	Yes	vpc-0cffa0964021bd3f
☐	–	rtb-0d7082f7e07997de8	–	–	Yes	vpc-07aae30cc793558a
☐	–	rtb-003288ac307717cfc	–	–	Yes	vpc-089170d087a7d86
☑	VPC1 RT	rtb-00e89dd192034a74f	–	–	No	vpc-07aae30cc793558a
☐	VPC2 RT	rtb-0f4d75ae824a98658	–	–	No	vpc-0cffa0964021bd3f

rtb-00e89dd192034a74f / VPC1 RT

Explicit subnet associations (0)

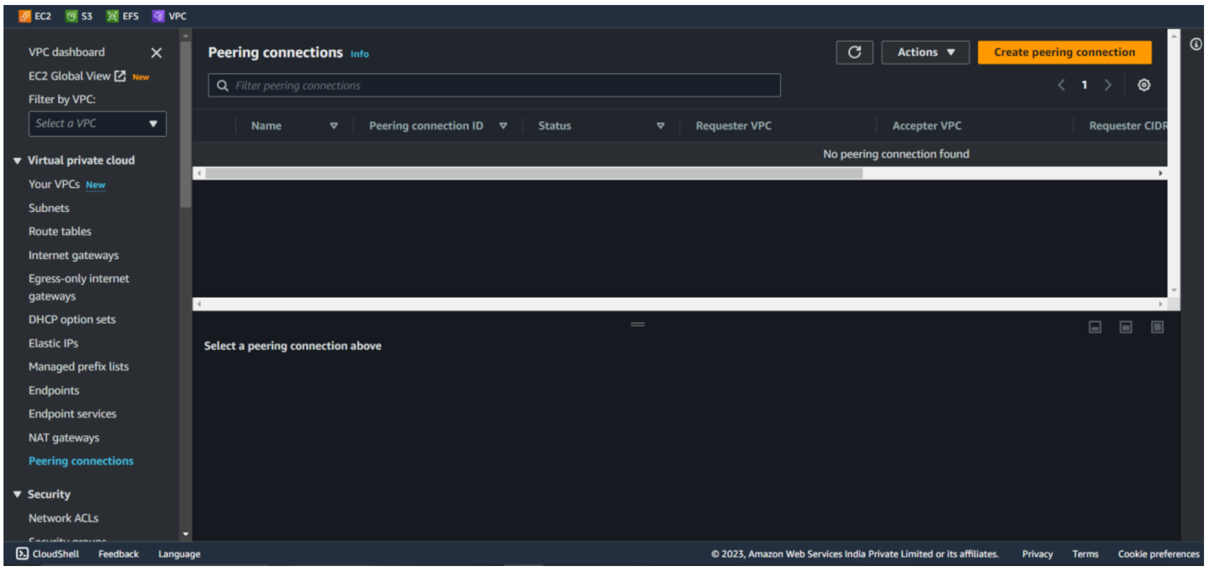
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR

No subnet associations

You do not have any subnet associations

Repeat similarly for VPC2

9. Now create a peering connection to both the VPCs for that go to peering connections and click on create peering connection.



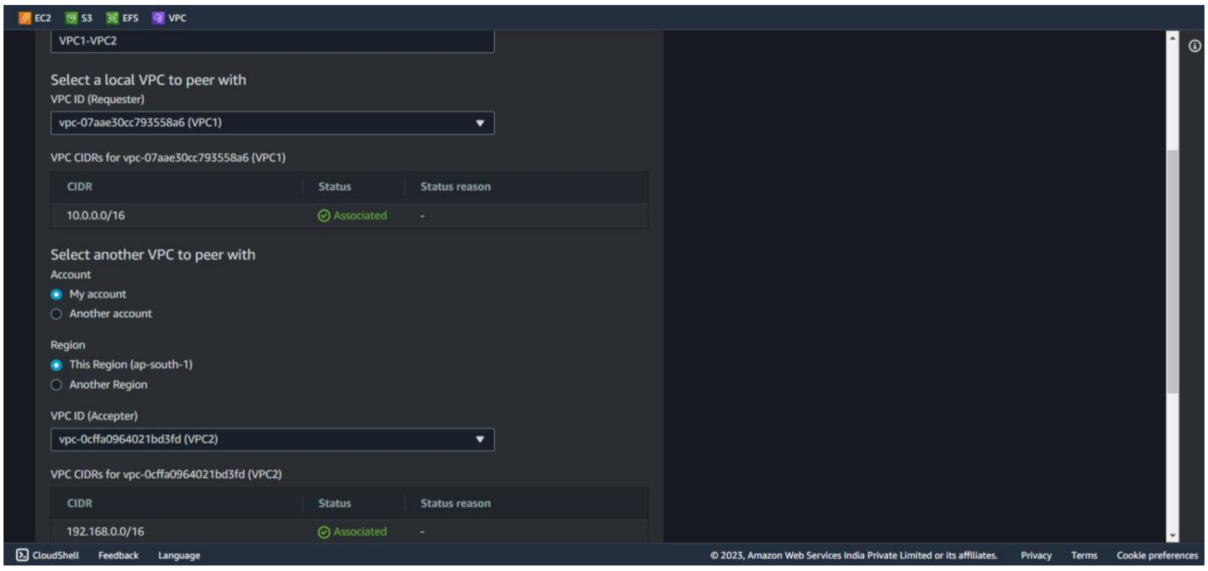
Peering connections Info

Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDR

No peering connection found

Select a peering connection above

10. Name a peering connection name and select the Requestor VPC and Acceptor VPC and click on create peering connection.


EC2
S3
EFS
VPC
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

VPC1-VPC2

Select a local VPC to peer with

VPC ID (Requester)

vpc-07aae30cc793558a6 (VPC1)

VPC CIDRs for vpc-07aae30cc793558a6 (VPC1)

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

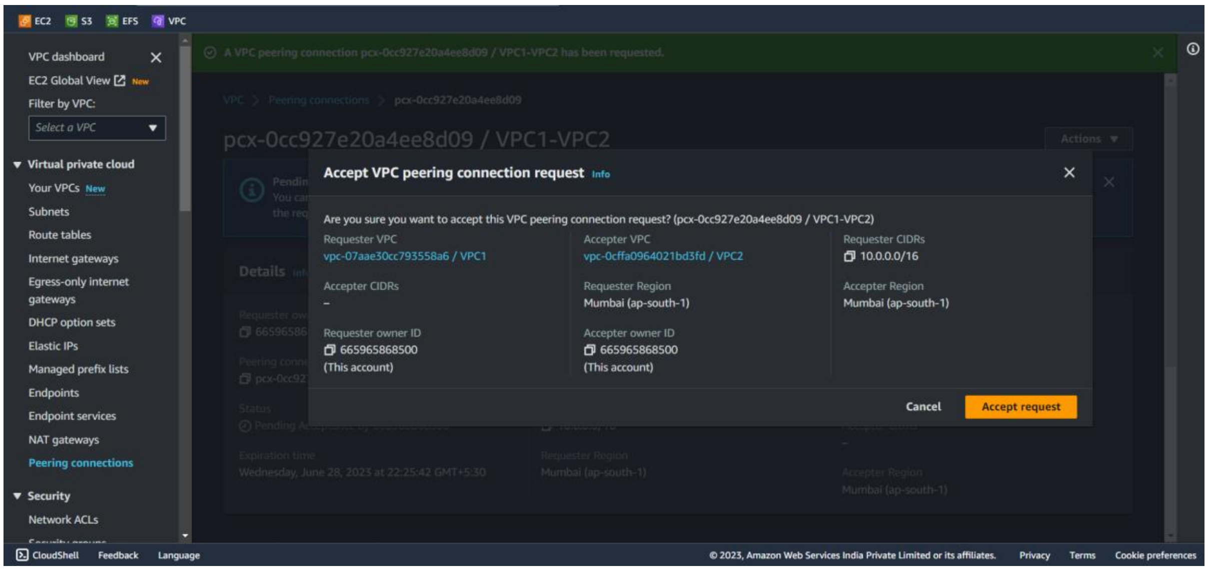
VPC ID (Accepter)

vpc-0cffa0964021bd3fd (VPC2)

VPC CIDRs for vpc-0cffa0964021bd3fd (VPC2)

CIDR	Status	Status reason
192.168.0.0/16	Associated	-

11. After creating a peering connection you must always accept VPC peering connection for that select the peering connection and click on actions and click on accept request.



A VPC peering connection pcx-0cc927e20a4ee8d09 / VPC1-VPC2 has been requested.

VPC > Peering connections > pcx-0cc927e20a4ee8d09

pcx-0cc927e20a4ee8d09 / VPC1-VPC2

Accept VPC peering connection request

Are you sure you want to accept this VPC peering connection request? (pcx-0cc927e20a4ee8d09 / VPC1-VPC2)

Requester VPC	Accepter VPC	Requester CIDRs
vpc-07aae30cc793558a6 / VPC1	vpc-0cffa0964021bd3fd / VPC2	10.0.0.0/16
Accepter CIDRs	**Requester Region**	**Accepter Region**
–	Mumbai (ap-south-1)	Mumbai (ap-south-1)
Requester owner ID	**Accepter owner ID**	
665965868500 (This account)	665965868500 (This account)	

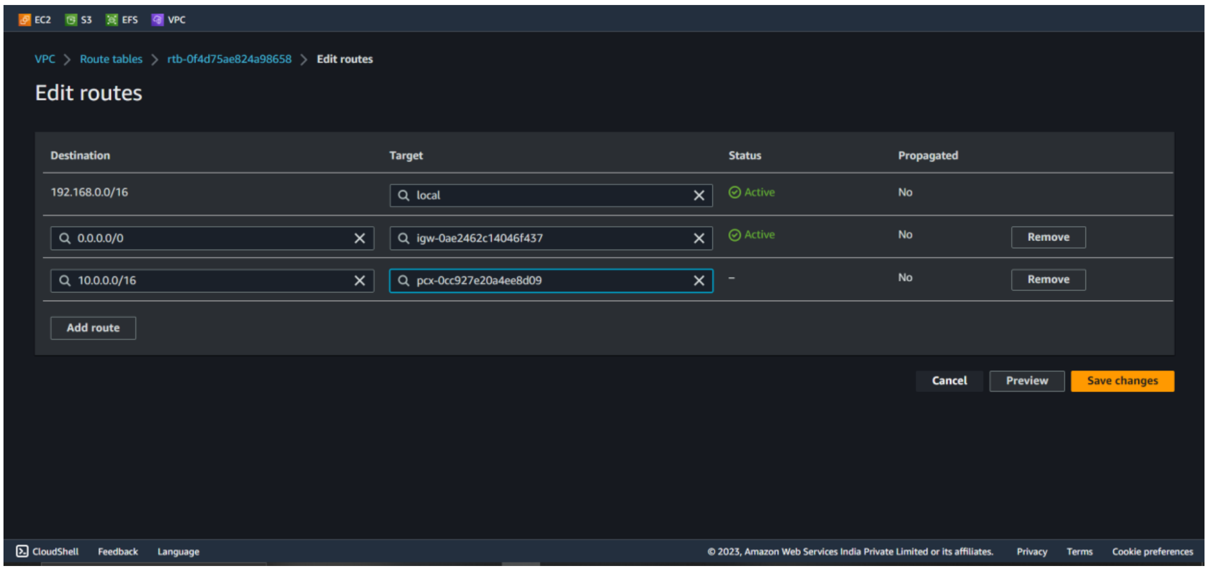
Expiration time

Wednesday, June 28, 2023 at 22:25:42 GMT+5:30

12. Now edit the peering connection route in route table for that go to route tables and click on edit routes and add the peering connection target and set the destination and the opposite VPC CIDR i.e.,

    172.16.0.0/16 for VPC1

    10.0.0.0/16 for VPC2

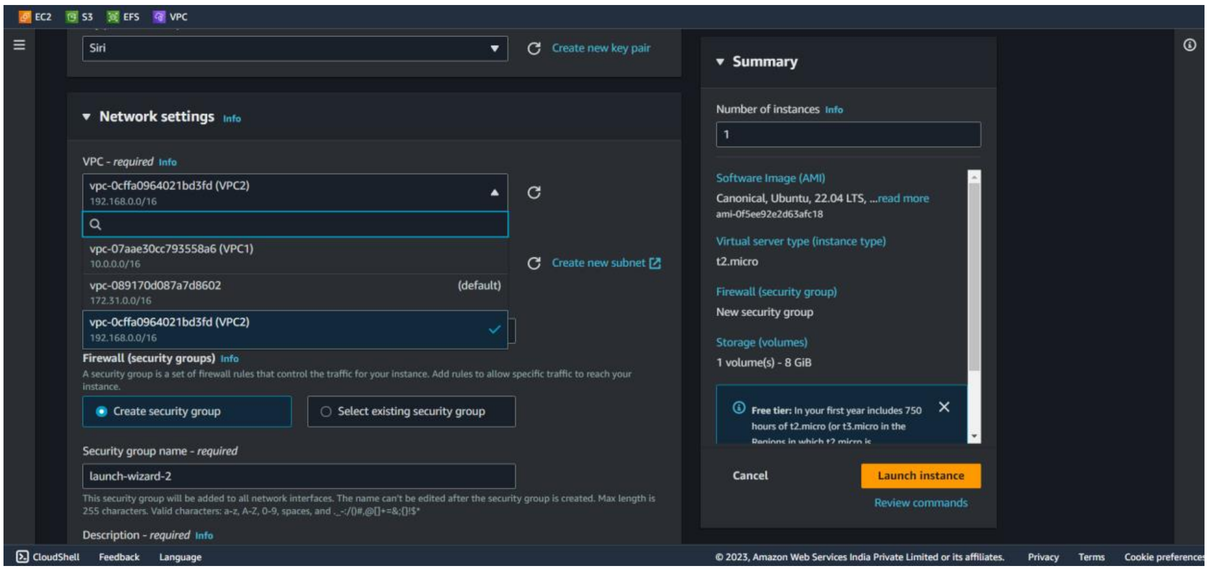


VPC > Route tables > rtb-0f4d75ae824a98658 > Edit routes

Edit routes

Destination	Target	Status	Propagated	
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-0ae2462c14046f437	Active	No	Remove
10.0.0.0/16	pcx-0cc927e20a4ee8d09	-	No	Remove

13. Now create instances in respective custom VPCs to verify the connectivity



Siri

Network settings

VPC - *required*

vpc-0cffa0964021bd3fd (VPC2)
192.168.0.0/16

vpc-07aae30cc793558a6 (VPC1)
10.0.0.0/16

vpc-089170d087a7d8602 (default)
172.31.0.0/16

vpc-0cffa0964021bd3fd (VPC2) ✓
192.168.0.0/16

Firewall (security groups)

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*

launch-wizard-2

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*

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0f5ee92e2d63afc18

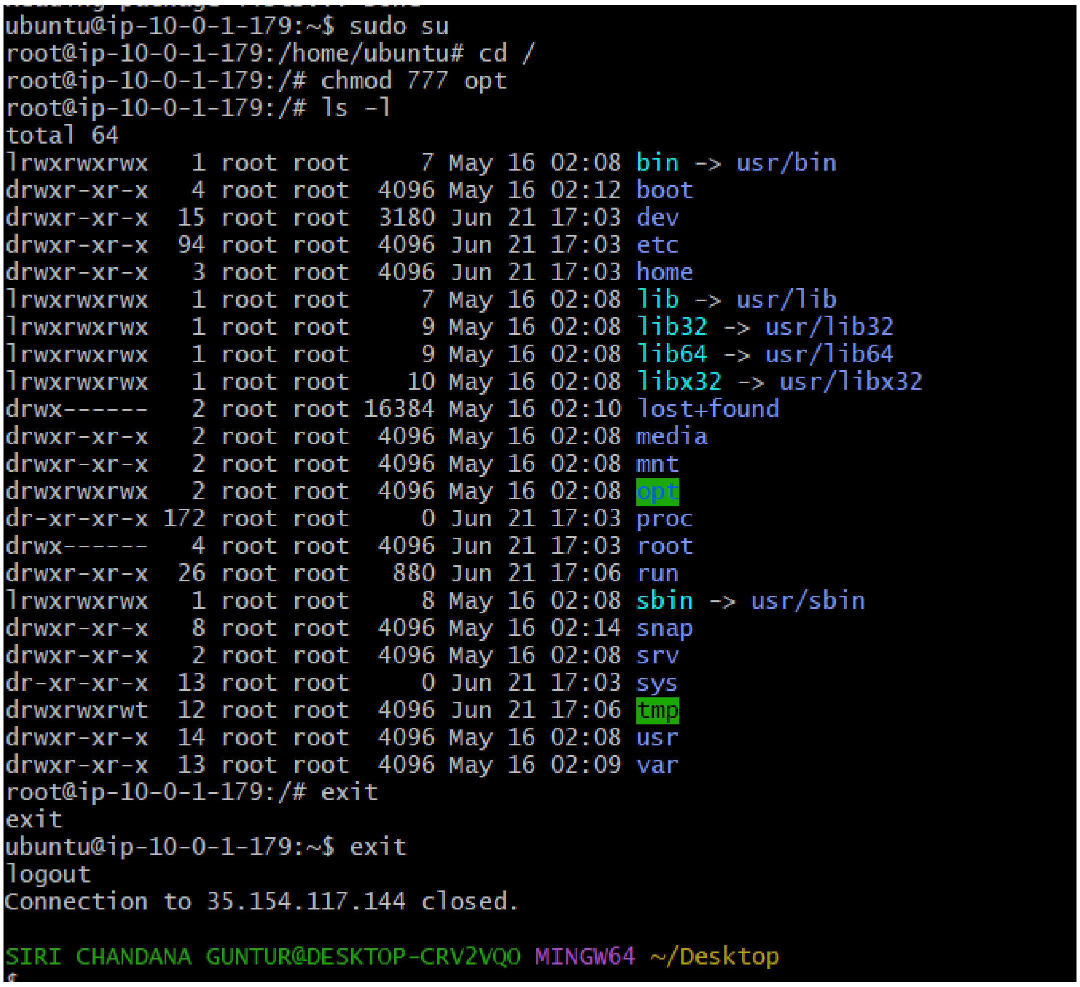
Virtual server type (instance type): t2.micro

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

14. Now connect to instance in VPC 1 using public IP address of that instance and switch to super user mode and change the RWX settings to 777 to any folder to copy key pair of second instance from our local machine to Instance.



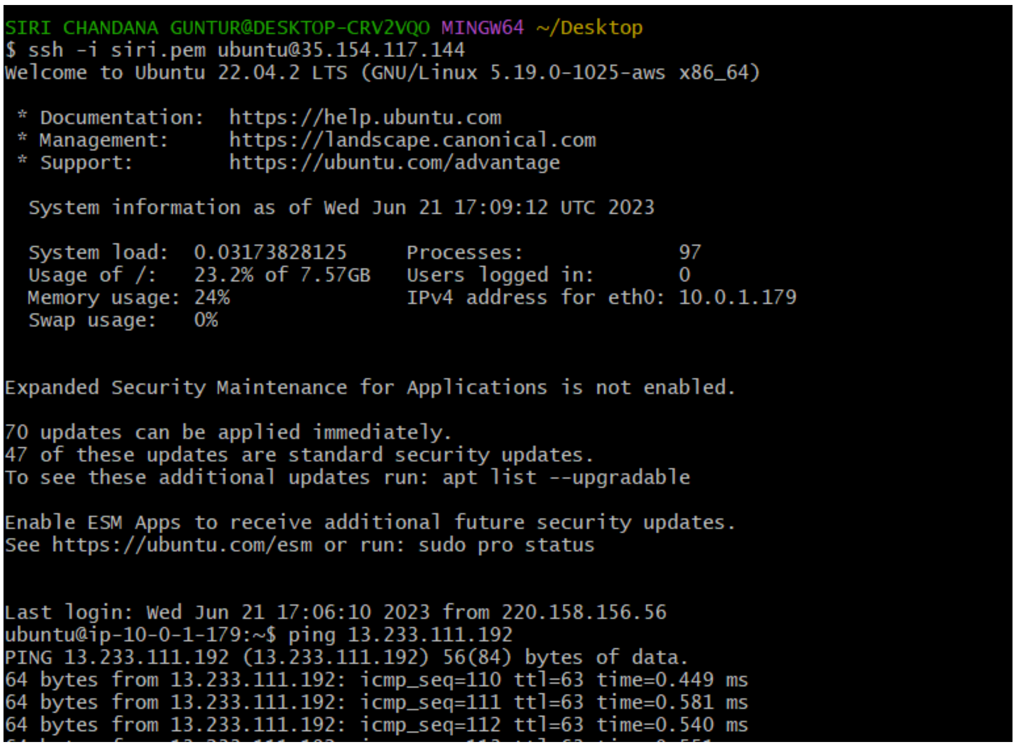
```
ubuntu@ip-10-0-1-179:~$ sudo su
root@ip-10-0-1-179:/home/ubuntu# cd /
root@ip-10-0-1-179:/# chmod 777 opt
root@ip-10-0-1-179:/# ls -l
total 64
lrwxrwxrwx   1 root root     7 May 16 02:08 bin -> usr/bin
drwxr-xr-x   4 root root  4096 May 16 02:12 boot
drwxr-xr-x  15 root root  3180 Jun 21 17:03 dev
drwxr-xr-x  94 root root  4096 Jun 21 17:03 etc
drwxr-xr-x   3 root root  4096 Jun 21 17:03 home
lrwxrwxrwx   1 root root     7 May 16 02:08 lib -> usr/lib
lrwxrwxrwx   1 root root     9 May 16 02:08 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 May 16 02:08 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 May 16 02:08 libx32 -> usr/libx32
drwx------   2 root root 16384 May 16 02:10 lost+found
drwxr-xr-x   2 root root  4096 May 16 02:08 media
drwxr-xr-x   2 root root  4096 May 16 02:08 mnt
drwxrwxrwx   2 root root  4096 May 16 02:08 opt
dr-xr-xr-x 172 root root     0 Jun 21 17:03 proc
drwx------   4 root root  4096 Jun 21 17:03 root
drwxr-xr-x  26 root root   880 Jun 21 17:06 run
lrwxrwxrwx   1 root root     8 May 16 02:08 sbin -> usr/sbin
drwxr-xr-x   8 root root  4096 May 16 02:14 snap
drwxr-xr-x   2 root root  4096 May 16 02:08 srv
dr-xr-xr-x  13 root root     0 Jun 21 17:03 sys
drwxrwxrwt  12 root root  4096 Jun 21 17:06 tmp
drwxr-xr-x  14 root root  4096 May 16 02:08 usr
drwxr-xr-x  13 root root  4096 May 16 02:09 var
root@ip-10-0-1-179:/# exit
exit
ubuntu@ip-10-0-1-179:~$ exit
logout
Connection to 35.154.117.144 closed.

SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$
```

Now exit and come to local machine and click the following command to copy the file from local machine to Instance 1 VM

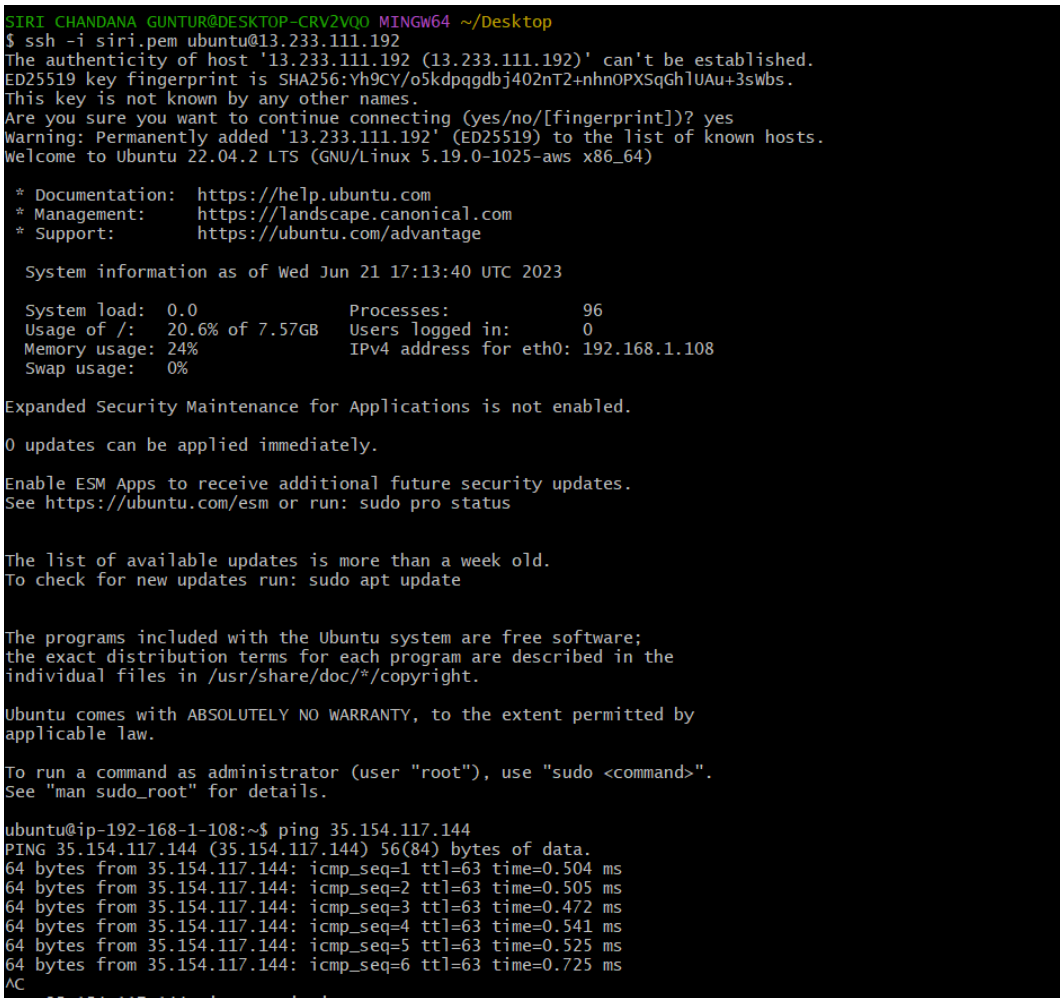
scp -i vpc1Instance.pem ./vpc2Instance.pem ubuntu@publicip:/opt

Now log in back to your instance and try to ping second instance in VPC2

Now connect to your second instance using first instance and try to ping the first instance in VPC1



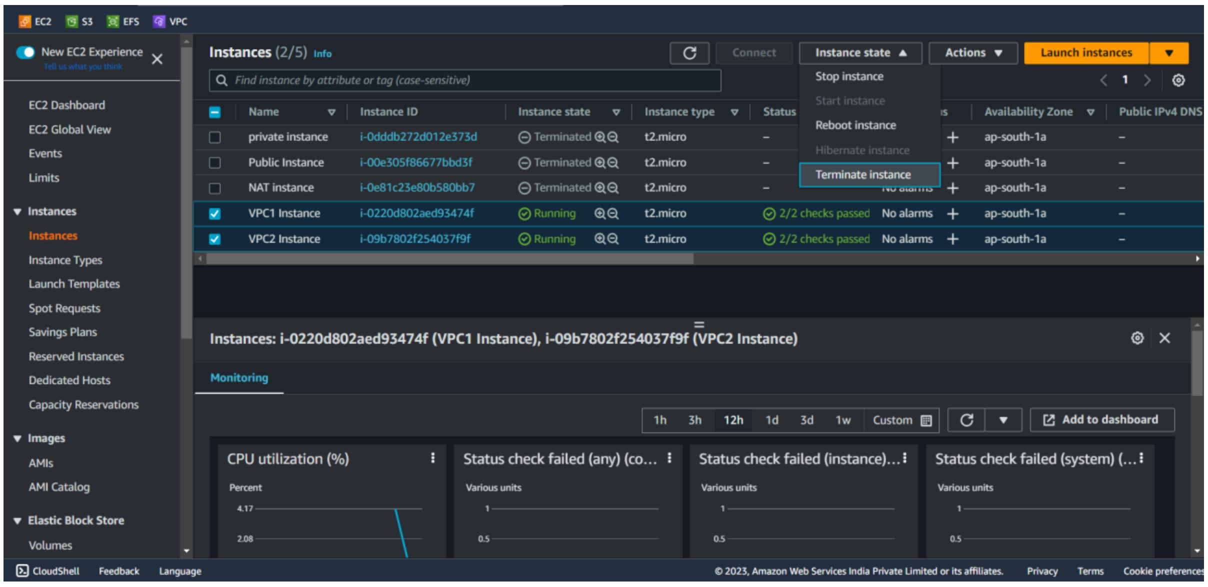
```
SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$ ssh -i siri.pem ubuntu@35.154.117.144
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jun 21 17:09:12 UTC 2023

  System load:  0.03173828125     Processes:             97
  Usage of /:   23.2% of 7.57GB   Users logged in:       0
  Memory usage: 24%               IPv4 address for eth0: 10.0.1.179
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

70 updates can be applied immediately.
47 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Wed Jun 21 17:06:10 2023 from 220.158.156.56
ubuntu@ip-10-0-1-179:~$ ping 13.233.111.192
PING 13.233.111.192 (13.233.111.192) 56(84) bytes of data.
64 bytes from 13.233.111.192: icmp_seq=110 ttl=63 time=0.449 ms
64 bytes from 13.233.111.192: icmp_seq=111 ttl=63 time=0.581 ms
64 bytes from 13.233.111.192: icmp_seq=112 ttl=63 time=0.540 ms
```



```
SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$ ssh -i siri.pem ubuntu@13.233.111.192
The authenticity of host '13.233.111.192 (13.233.111.192)' can't be established.
ED25519 key fingerprint is SHA256:Yh9CY/o5kdpqgdbj402nT2+nhnOPXSqGhlUAu+3sWbs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.233.111.192' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jun 21 17:13:40 UTC 2023

  System load:  0.0               Processes:             96
  Usage of /:   20.6% of 7.57GB   Users logged in:       0
  Memory usage: 24%               IPv4 address for eth0: 192.168.1.108
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-192-168-1-108:~$ ping 35.154.117.144
PING 35.154.117.144 (35.154.117.144) 56(84) bytes of data.
64 bytes from 35.154.117.144: icmp_seq=1 ttl=63 time=0.504 ms
64 bytes from 35.154.117.144: icmp_seq=2 ttl=63 time=0.505 ms
64 bytes from 35.154.117.144: icmp_seq=3 ttl=63 time=0.472 ms
64 bytes from 35.154.117.144: icmp_seq=4 ttl=63 time=0.541 ms
64 bytes from 35.154.117.144: icmp_seq=5 ttl=63 time=0.525 ms
64 bytes from 35.154.117.144: icmp_seq=6 ttl=63 time=0.725 ms
^C
```

Cleaning up workspace

1. Firstly terminate all your instances in EC2 instances.



Instances (2/5)

Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status		Availability Zone	Public IPv4 DNS
☐	private instance	i-0dddb272d012e373d	Terminated	t2.micro	–		ap-south-1a	–
☐	Public Instance	i-00e305f86677bbd3f	Terminated	t2.micro	–		ap-south-1a	–
☐	NAT instance	i-0e81c23e80b580bb7	Terminated	t2.micro	–		ap-south-1a	–
✓	VPC1 Instance	i-0220d802aed93474f	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–
✓	VPC2 Instance	i-09b7802f254037f9f	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–

Instances: i-0220d802aed93474f (VPC1 Instance), i-09b7802f254037f9f (VPC2 Instance)

1h 3h 12h 1d 3d 1w Custom

CPU utilization (%) — Percent — 4.17, 2.08

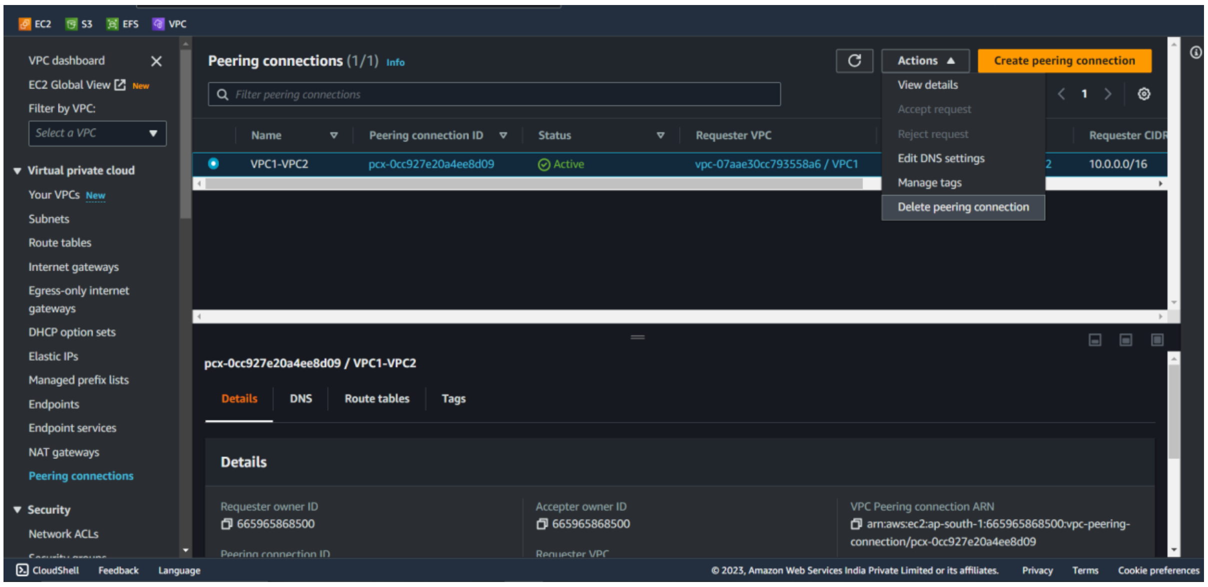
Status check failed (any) (co... — Various units — 1, 0.5

Status check failed (instance)... — Various units — 1, 0.5

Status check failed (system) (... — Various units — 1, 0.5

© 2023, Amazon Web Services India Private Limited or its affiliates.

2. Then delete your peering connection in VPC dashboard -> peering connections select the peering connection and click on actions and click on delete the peering connection.



Peering connections (1/1)

Filter peering connections

	Name	Peering connection ID	Status	Requester VPC		Requester CIDR
●	VPC1-VPC2	pcx-0cc927e20a4ee8d09	Active	vpc-07aae30cc793558a6 / VPC1	2	10.0.0.0/16

pcx-0cc927e20a4ee8d09 / VPC1-VPC2

Details

Requester owner ID: 665965868500

Accepter owner ID: 665965868500

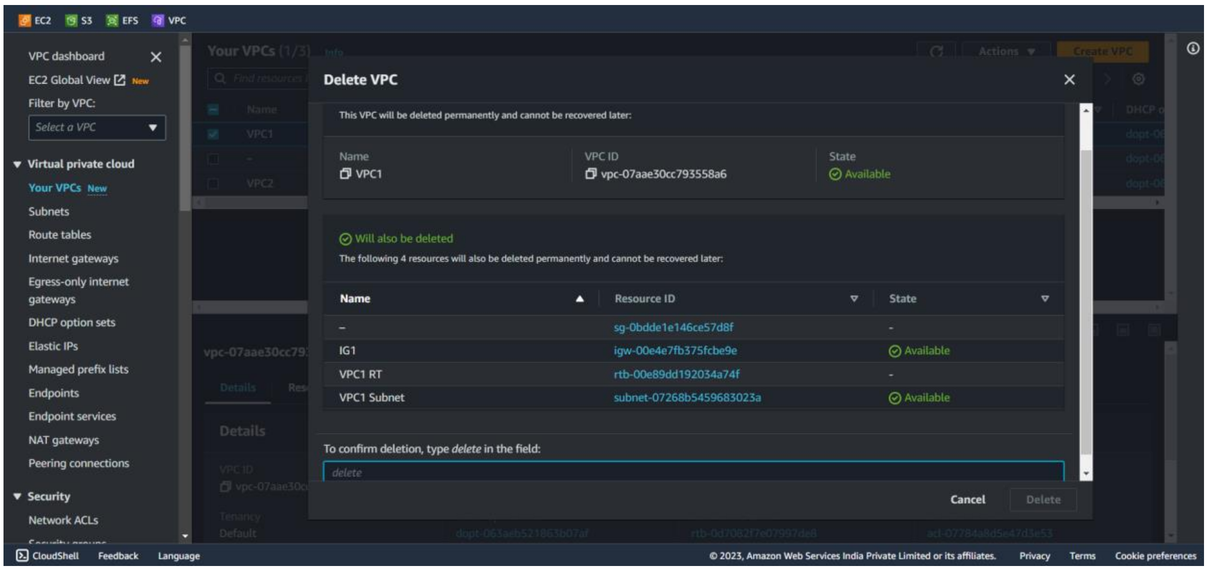
VPC Peering connection ARN: arn:aws:ec2:ap-south-1:665965868500:vpc-peering-connection/pcx-0cc927e20a4ee8d09

Peering connection ID

Requester VPC

© 2023, Amazon Web Services India Private Limited or its affiliates.

3. Now go to VPCs and select the VPC and click on action and click on delete VPC.



Delete VPC

This VPC will be deleted permanently and cannot be recovered later:

Name	VPC ID	State
VPC1	vpc-07aae30cc793558a6	Available

Will also be deleted

The following 4 resources will also be deleted permanently and cannot be recovered later:

Name	Resource ID	State
–	sg-0bdde1e146ce57d8f	-
IG1	igw-00e4e7fb375fcbe9e	Available
VPC1 RT	rtb-00e89dd192034a74f	-
VPC1 Subnet	subnet-07268b5459683023a	Available

To confirm deletion, type *delete* in the field:

delete

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences