॥ सिद्धिः भूषयते विद्याम् ॥

avantika
UNIVERSITY

Discipline

Build a custom VPC and Do peering

CS5002

Assignment-16

Sheikh Muhammed Tadeeb (AU19B1014)

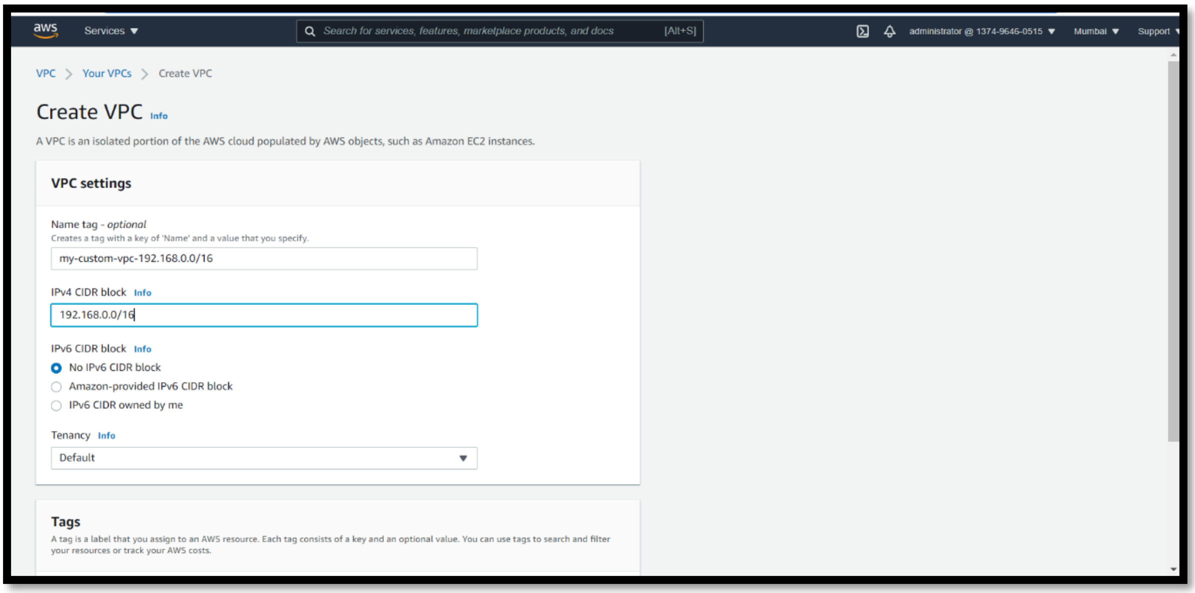
❖ Problem Statement: -

Create a Custom VPC (192.168.0.0/16) and create 2 Subnet (Public Subnet: 192.168.1.0/24), Private subnet: 192.168.2.0). Setup 1 VM in each Subnet. VM in Public should be publicly accessed and VM in private to be Privately Accessed only. Private machine should have internet connectivity.

Create a VPC peering between Default VPC and the New VPC, Check the Ping and SSH on Private Ip address.

❖ Solution:

Step -1: Create a custom VPC with the desired requirements.



VPC > Your VPCs > 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

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
my-custom-vpc-192.168.0.0/16

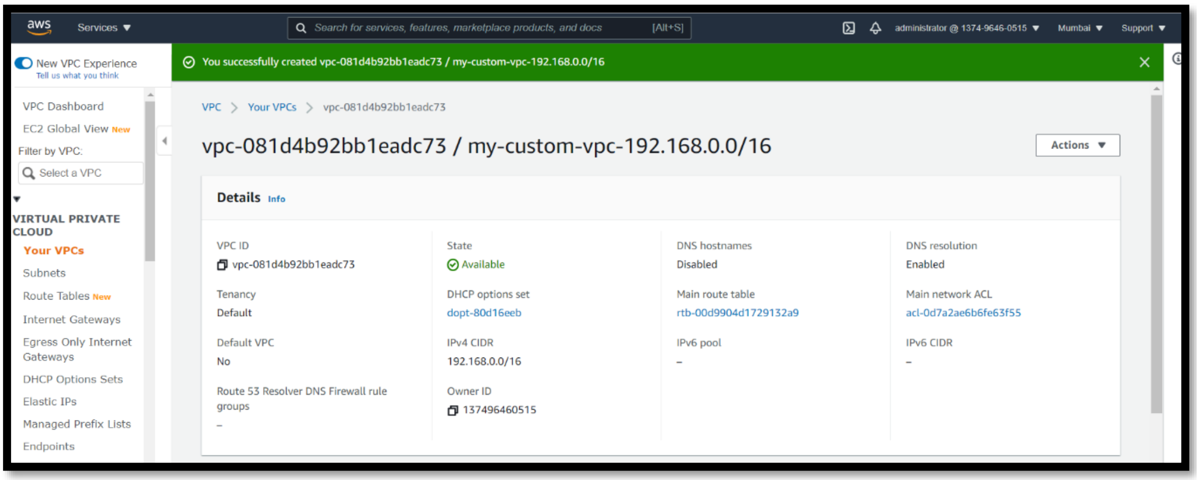
IPv4 CIDR block Info
192.168.0.0/16

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

Tenancy Info
Default

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.

aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼



You successfully created vpc-081d4b92bb1eadc73 / my-custom-vpc-192.168.0.0/16

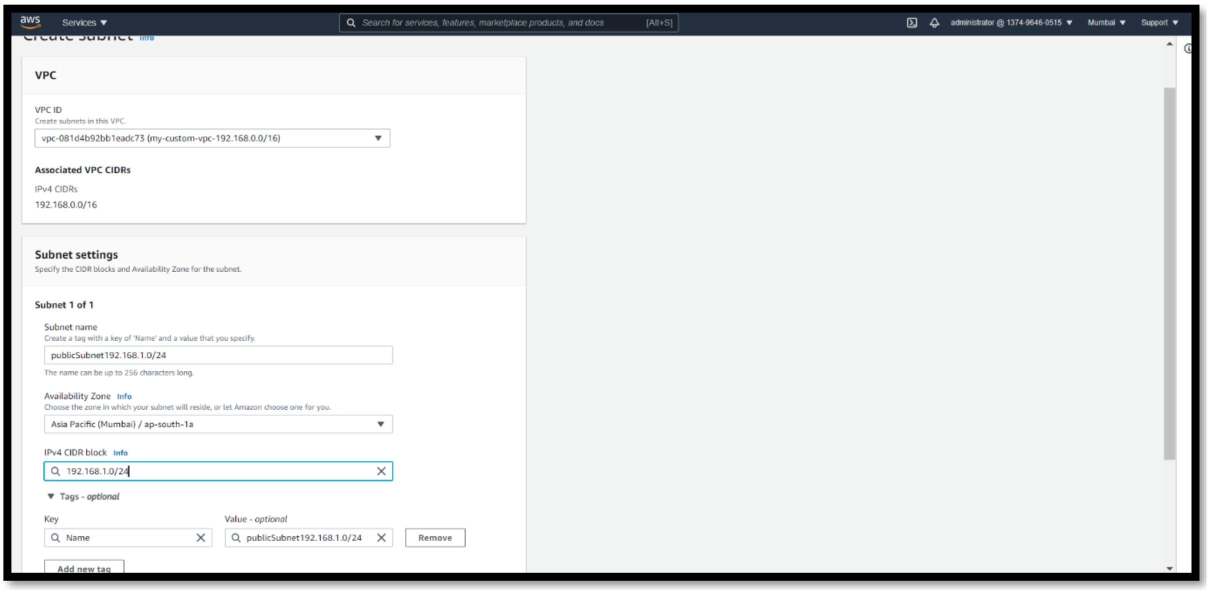
VPC > Your VPCs > vpc-081d4b92bb1eadc73

vpc-081d4b92bb1eadc73 / my-custom-vpc-192.168.0.0/16

Details Info

VPC ID vpc-081d4b92bb1eadc73	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-80d16eeb	Main route table rtb-00d9904d1729132a9	Main network ACL acl-0d7a2ae6b6fe63f55
Default VPC No	IPv4 CIDR 192.168.0.0/16	IPv6 pool –	IPv6 CIDR –
Route 53 Resolver DNS Firewall rule groups –	Owner ID 137496460515		

Step -2: Create the public as well as private subnet as per given IP criteria.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
Info

VPC

VPC ID
Create subnets in this VPC.
vpc-081d4b92bb1eadc73 (my-custom-vpc-192.168.0.0/16) ▼

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

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.
publicSubnet192.168.1.0/24
The name can be up to 256 characters long.

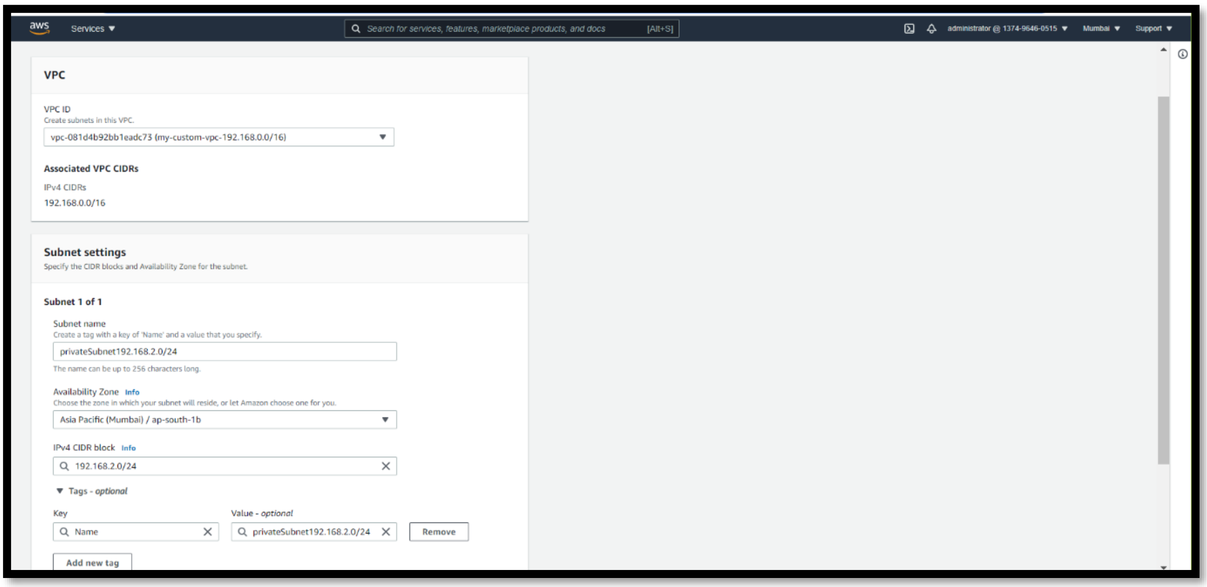
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1a ▼

IPv4 CIDR block Info
192.168.1.0/24

▼ Tags - *optional*

Key	Value - *optional*	
Name	publicSubnet192.168.1.0/24	Remove

Add new tag


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼

VPC

VPC ID
Create subnets in this VPC.
vpc-081d4b92bb1eadc73 (my-custom-vpc-192.168.0.0/16) ▼

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

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.
privateSubnet192.168.2.0/24
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-1b ▼

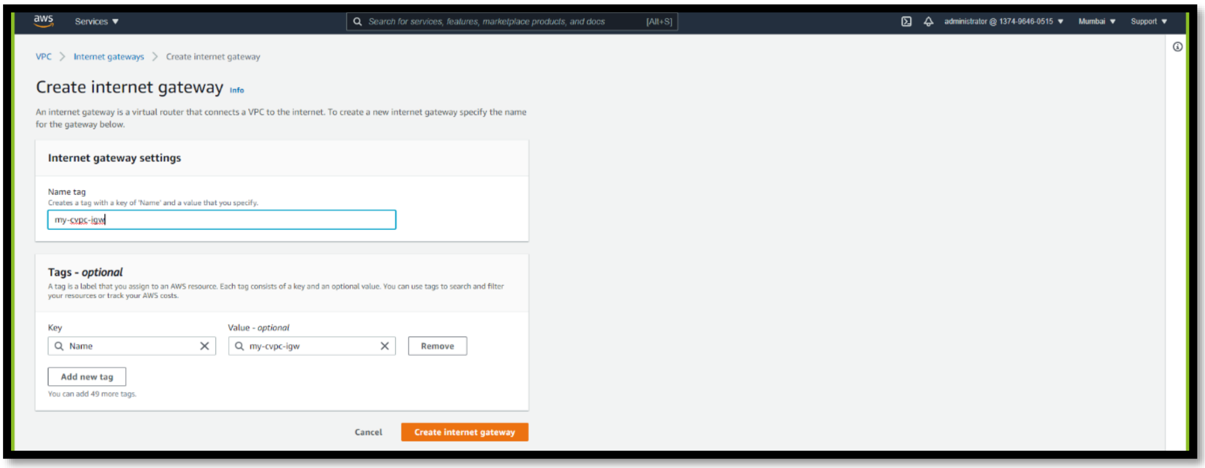
IPv4 CIDR block Info
192.168.2.0/24

▼ Tags - *optional*

Key	Value - *optional*	
Name	privateSubnet192.168.2.0/24	Remove

Add new tag

Step3) Create an Internet Gateway for you VPC.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
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.
my-cvpc-igw

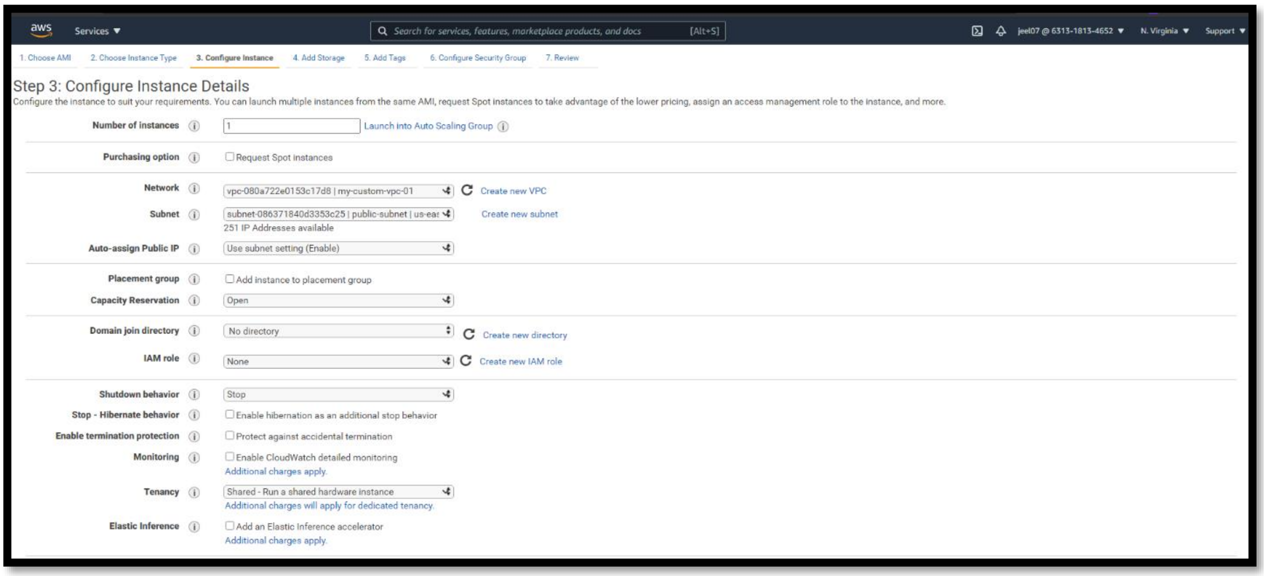
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	my-cvpc-igw	Remove

Add new tag
You can add 49 more tags.

Cancel Create internet gateway

Step -4: Create the public Instance with the custom VPC created and public subnet given and add the script as well.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-080a722e0153c17d8 | my-custom-vpc-01 — Create new VPC

Subnet: subnet-086371840d3353c25 | public-subnet | us-eas — Create new subnet
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory — Create new directory

IAM role: None — Create new IAM role

Shutdown behavior: Stop

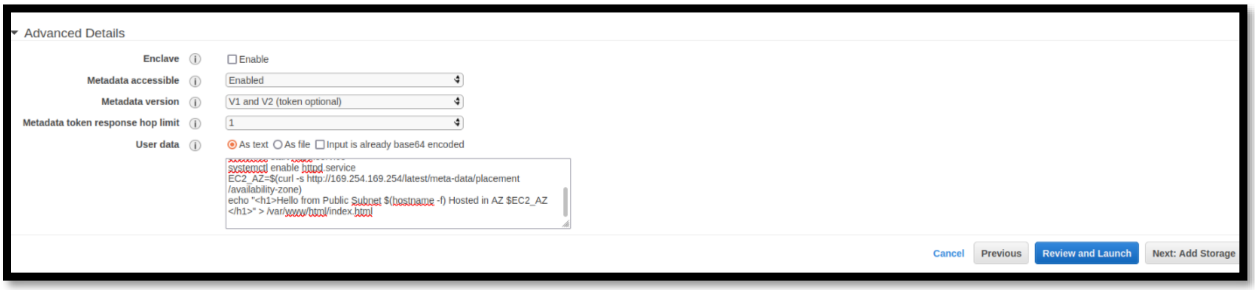
Stop - Hibernate behavior: □ Enable hibernation as an additional stop behavior

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Elastic Inference: □ Add an Elastic Inference accelerator
Additional charges apply.



Advanced Details

Enclave: □ Enable

Metadata accessible: Enabled

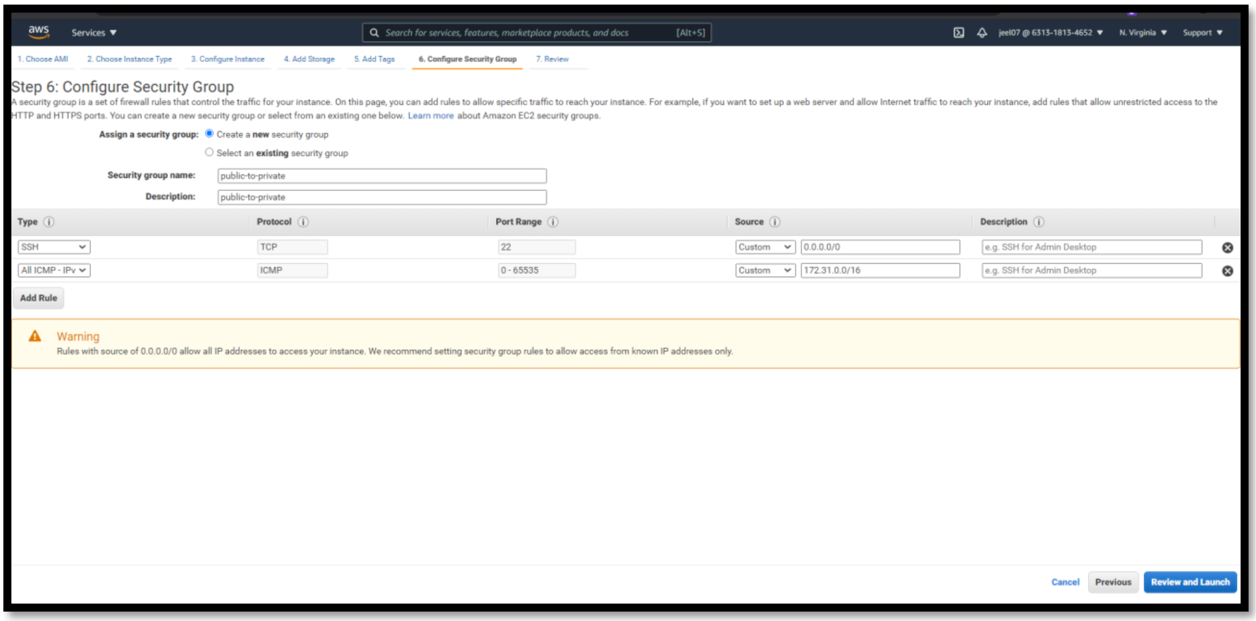
Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data: ● As text ○ As file □ Input is already base64 encoded

```
systemctl enable httpd.service
EC2_AZ=$(curl -s http://169.254.169.254/latest/meta-data/placement
/availability-zone)
echo "<h1>Hello from Public Subnet $(hostname -f) Hosted in AZ $EC2_AZ
</h1>" > /var/www/html/index.html
```

- **Step -3b:** Creating a security group naming public to private and add SSH and ALL ICMP-IPV4.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

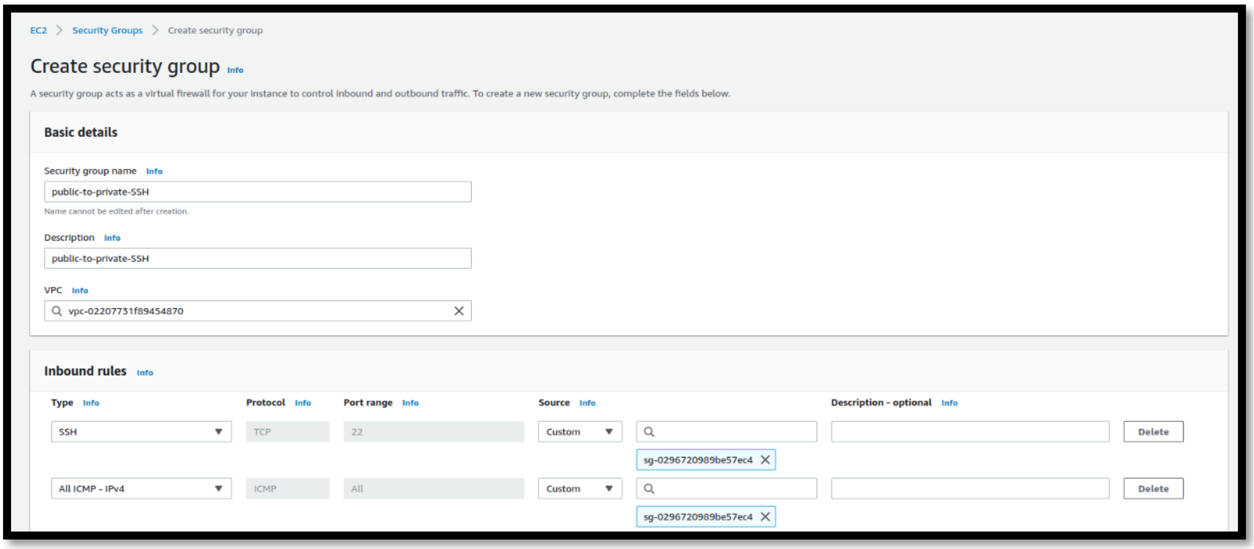
Security group name: public-to-private

Description: public-to-private

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv	ICMP	0 - 65535	Custom	172.31.0.0/16	e.g. SSH for Admin Desktop

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Step -3b: Create a security group naming public to private and add SSH and ALL ICMP-IPV4.



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info: public-to-private-SSH

Name cannot be edited after creation.

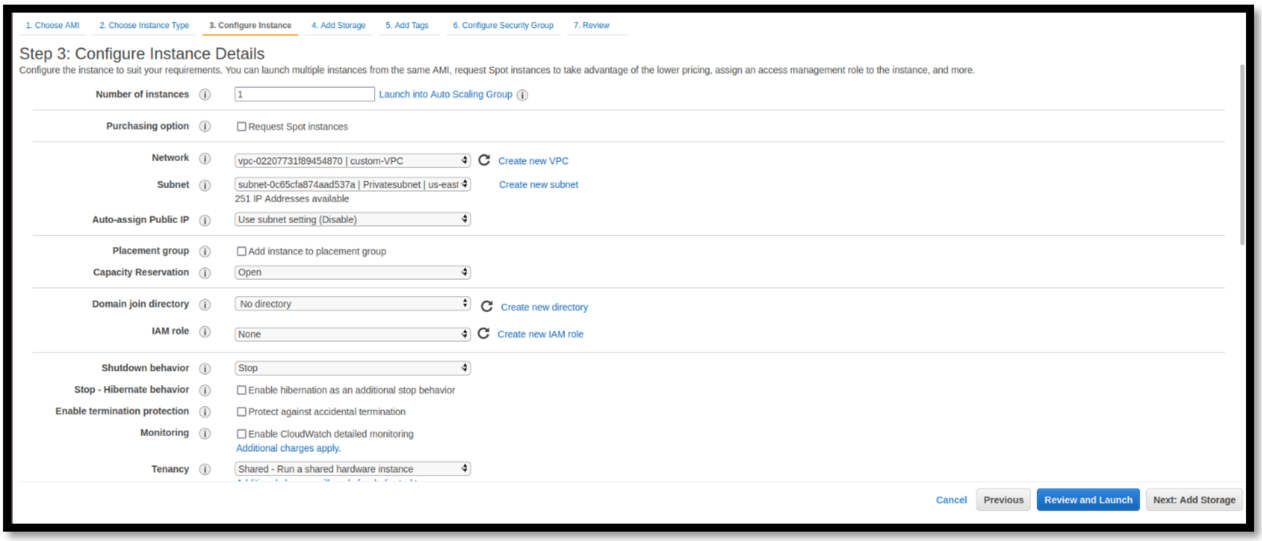
Description Info: public-to-private-SSH

VPC Info: vpc-02207731f89454870

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH	TCP	22	Custom	sg-0296720989be57ec4		Delete
All ICMP - IPv4	ICMP	All	Custom	sg-0296720989be57ec4		Delete

Step -4: Create a EC2 with custom VPC created and private subnet created.

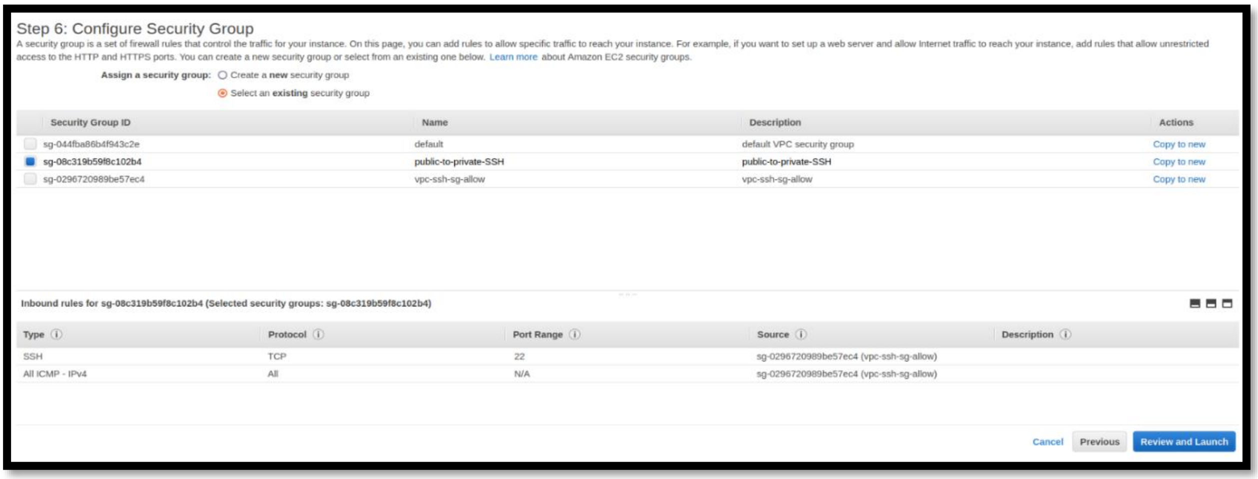


Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-02207731f89454870 | custom-VPC Create new VPC
Subnet	subnet-0c65cfa874aad537a | Privatesubnet | us-east Create new subnet 251 IP Addresses available
Auto-assign Public IP	Use subnet setting (Disable)
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance

Step -4b: Provide the security group created in steb-3b.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

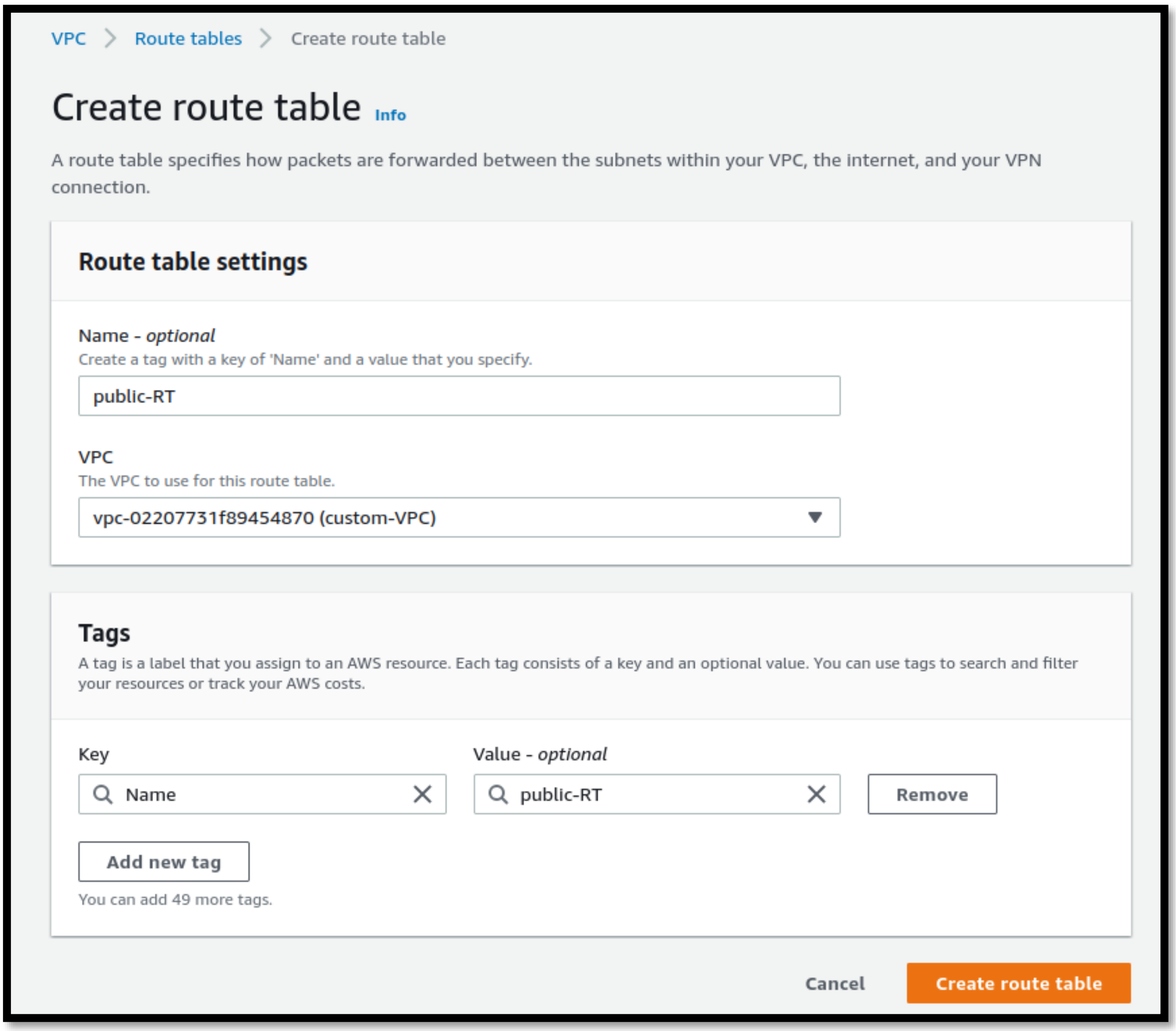
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-044fba86b4f943c2e	default	default VPC security group	Copy to new
☑	sg-08c319b59f8c102b4	public-to-private-SSH	public-to-private-SSH	Copy to new
□	sg-0296720989be57ec4	vpc-ssh-sg-allow	vpc-ssh-sg-allow	Copy to new

Inbound rules for sg-08c319b59f8c102b4 (Selected security groups: sg-08c319b59f8c102b4)

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	sg-0296720989be57ec4 (vpc-ssh-sg-allow)	
All ICMP - IPv4	All	N/A	sg-0296720989be57ec4 (vpc-ssh-sg-allow)	

Step -5: Create Public, Private 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.
public-RT

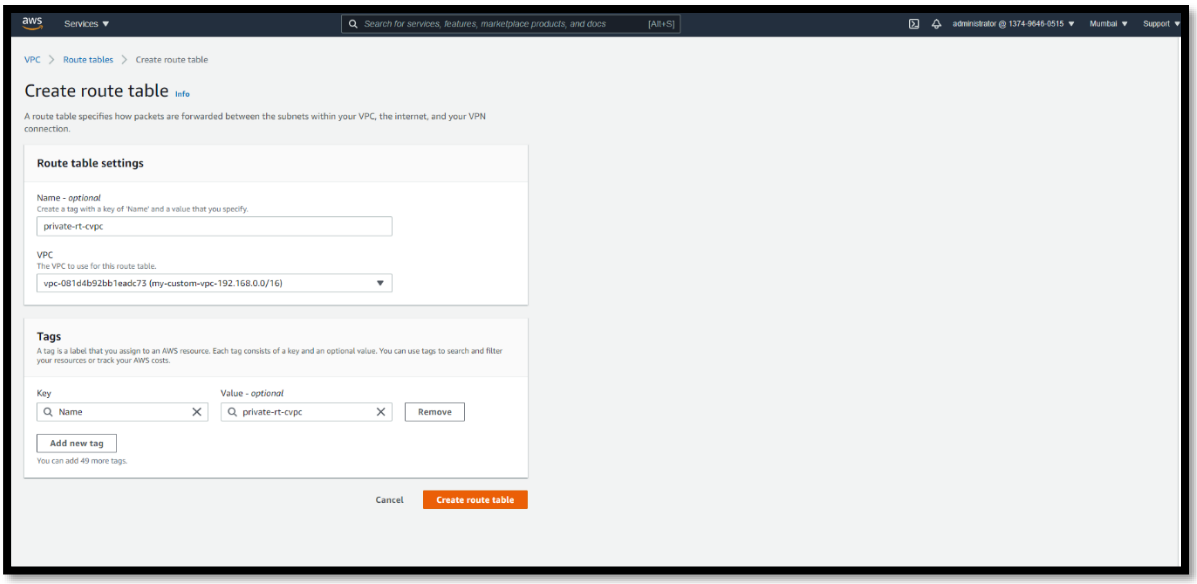
VPC
The VPC to use for this route table.
vpc-02207731f89454870 (custom-VPC)

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*: public-RT

You can add 49 more tags.


aws
Services ▼
Search for services, features, marketplace products, and docs
[Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
VPC > Route tables > Create route table
Info
Remove
Add new tag
Cancel
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.
private-rt-cvpc

VPC
The VPC to use for this route table.
vpc-081d4b92bb1eadc73 (my-custom-vpc-192.168.0.0/16)

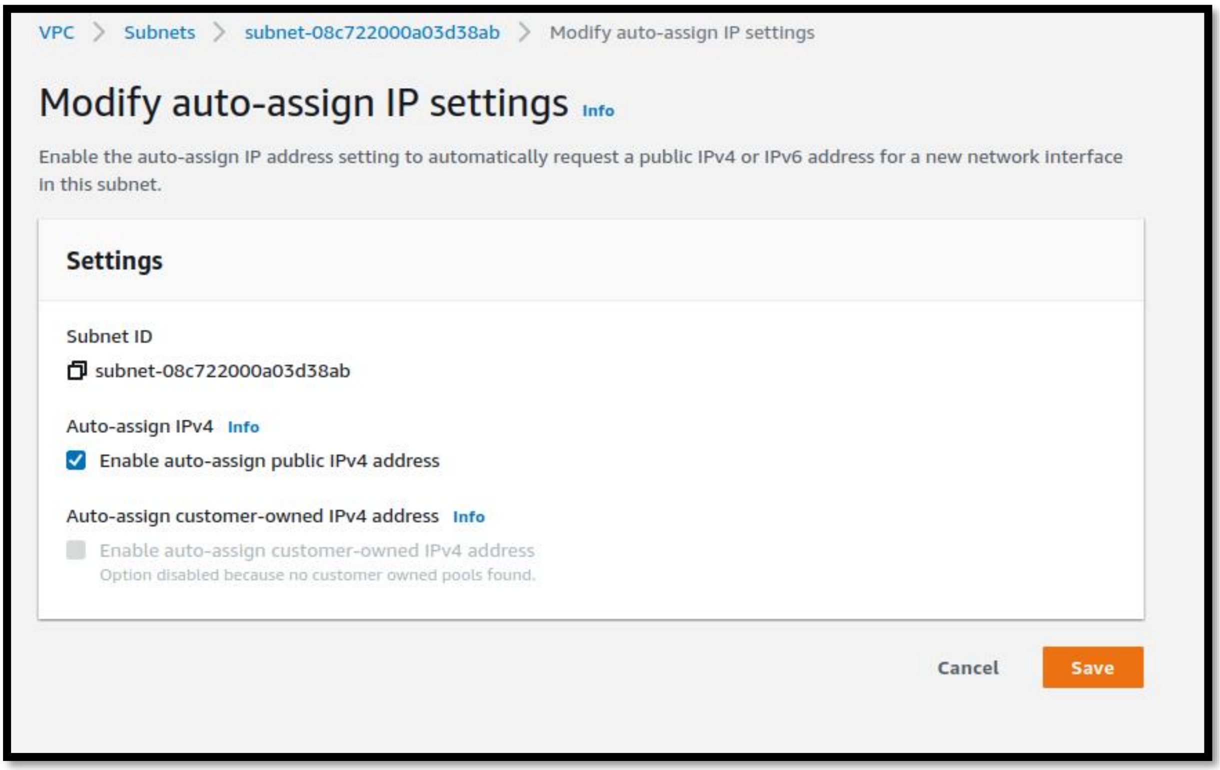
Tags

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*: private-rt-cvpc

You can add 49 more tags.

Step -6: Go to actions of public subnet and enable auto assign public Ipv4.



VPC > Subnets > subnet-08c722000a03d38ab > Modify auto-assign IP settings

Modify auto-assign IP settings Info

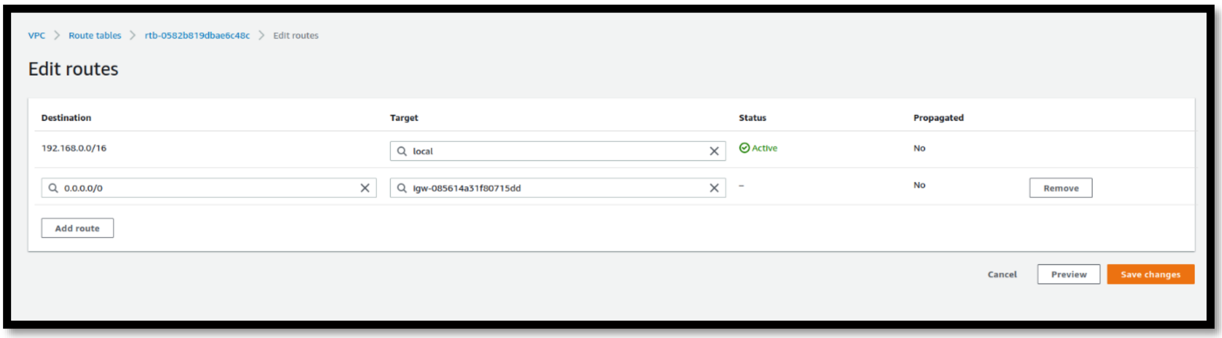
Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Settings

Subnet ID
subnet-08c722000a03d38ab

Auto-assign IPv4 Info
☑ Enable auto-assign public IPv4 address

Auto-assign customer-owned IPv4 address Info
□ Enable auto-assign customer-owned IPv4 address
Option disabled because no customer owned pools found.

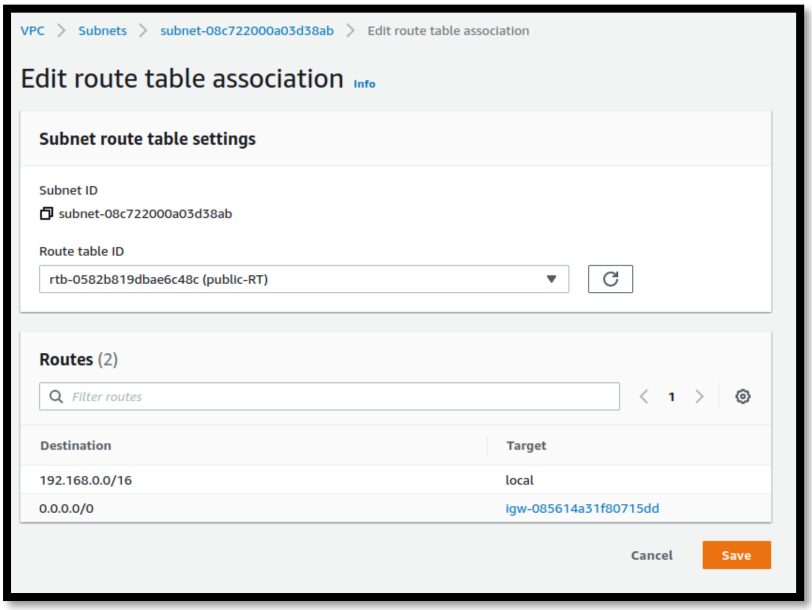


VPC > Route tables > rtb-0582b819dbae6c48c > Edit routes

Edit routes

Destination	Target	Status	Propagated	
192.168.0.0/16	local	Active	No	
0.0.0.0/0	igw-085614a31f80715dd	-	No	Remove

Step -7: Give Route to public subnet so as to add access to internet with the help of gateway.



VPC > Subnets > subnet-08c722000a03d38ab > Edit route table association

Edit route table association Info

Subnet route table settings

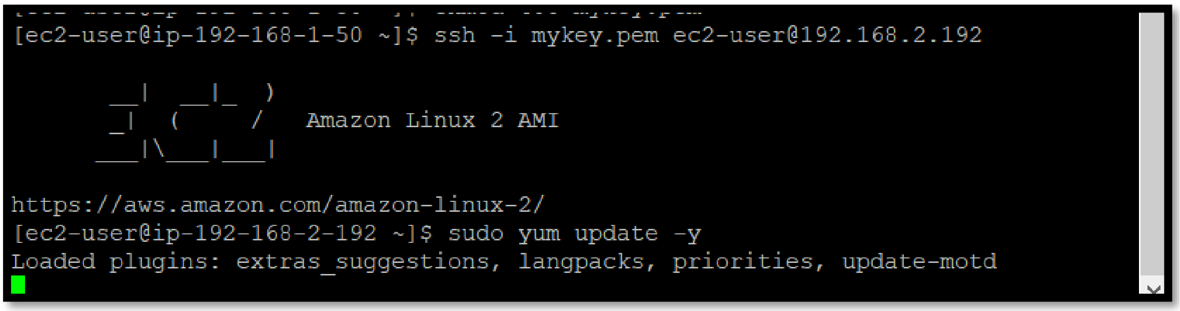
Subnet ID
subnet-08c722000a03d38ab

Route table ID
rtb-0582b819dbae6c48c (public-RT)

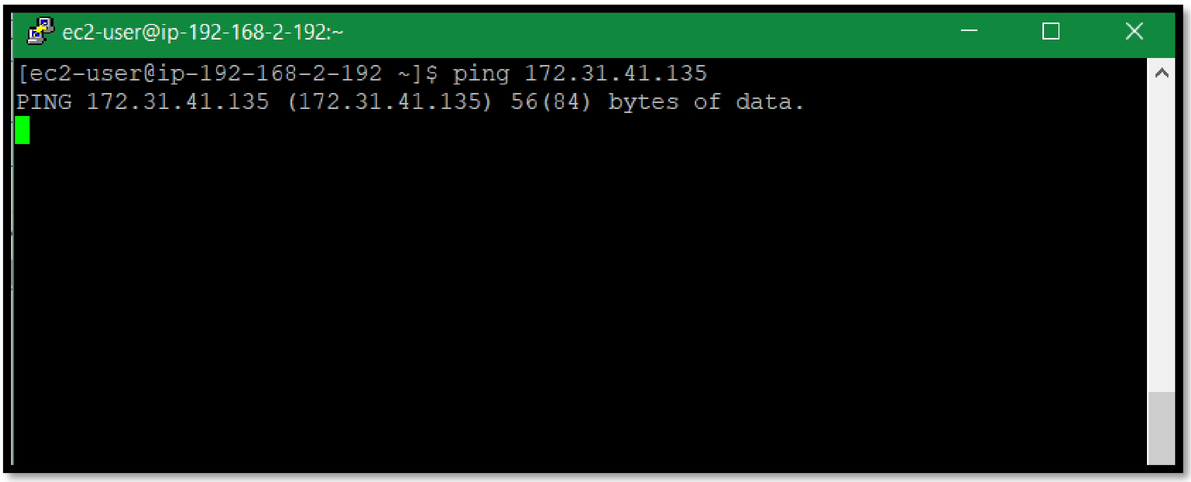
Routes (2)

Destination	Target
192.168.0.0/16	local
0.0.0.0/0	igw-085614a31f80715dd

Step -8: Open Putty and log in to private EC2 machine and check we can’t do sudo yum update -y and also, we can’t ping to another private instance (which is some other VPC).

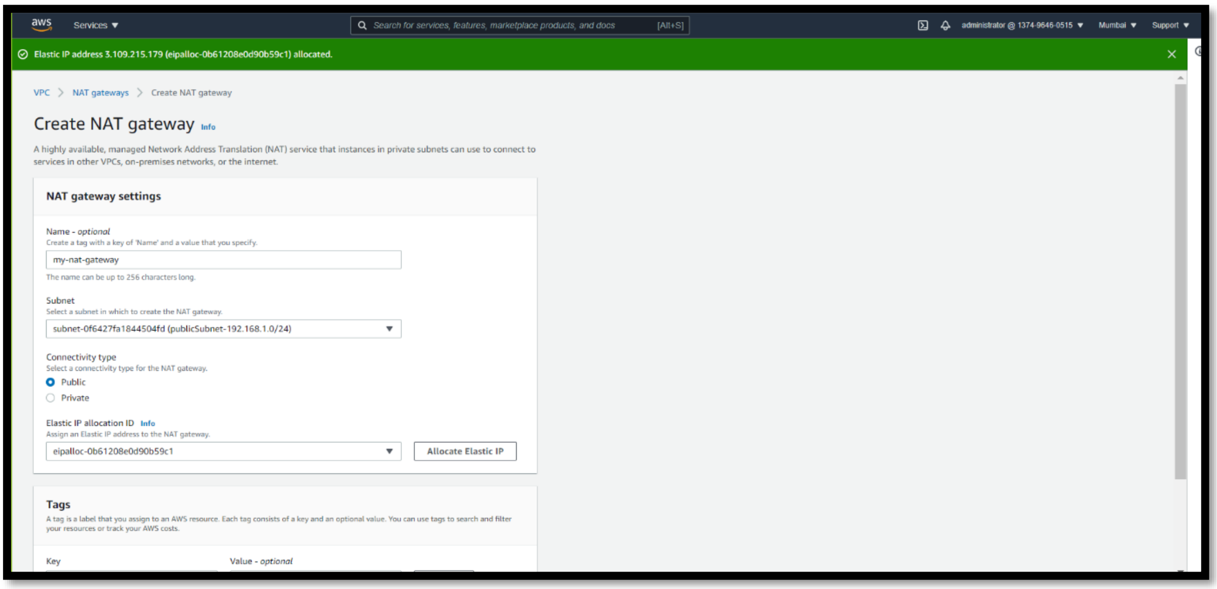


```
[ec2-user@ip-192-168-1-50 ~]$ ssh -i mykey.pem ec2-user@192.168.2.192

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-2-192 ~]$ sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
```



```
[ec2-user@ip-192-168-2-192 ~]$ ping 172.31.41.135
PING 172.31.41.135 (172.31.41.135) 56(84) bytes of data.
```

Step -9: Create public NAT Gateway with public subnet.



aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼

Elastic IP address 3.109.215.179 (eipalloc-0b61208e0d90b59c1) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my-nat-gateway
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0f6427fa1844504fd (publicSubnet-192.168.1.0/24)

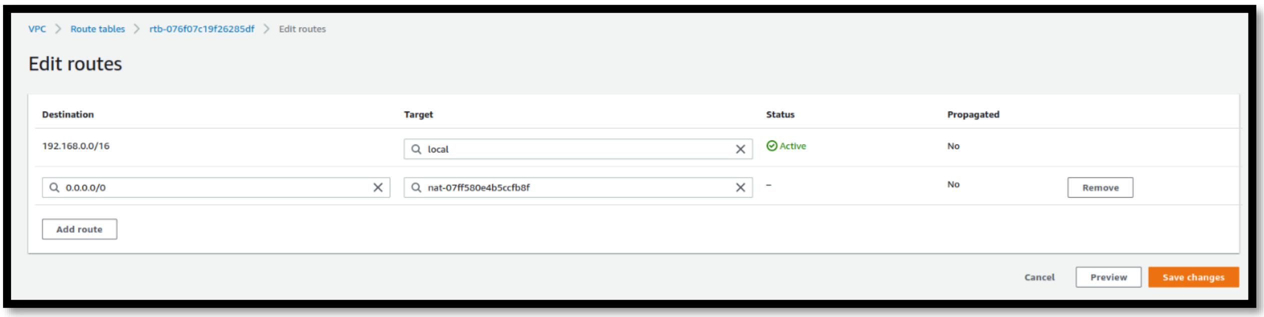
Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-0b61208e0d90b59c1

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*

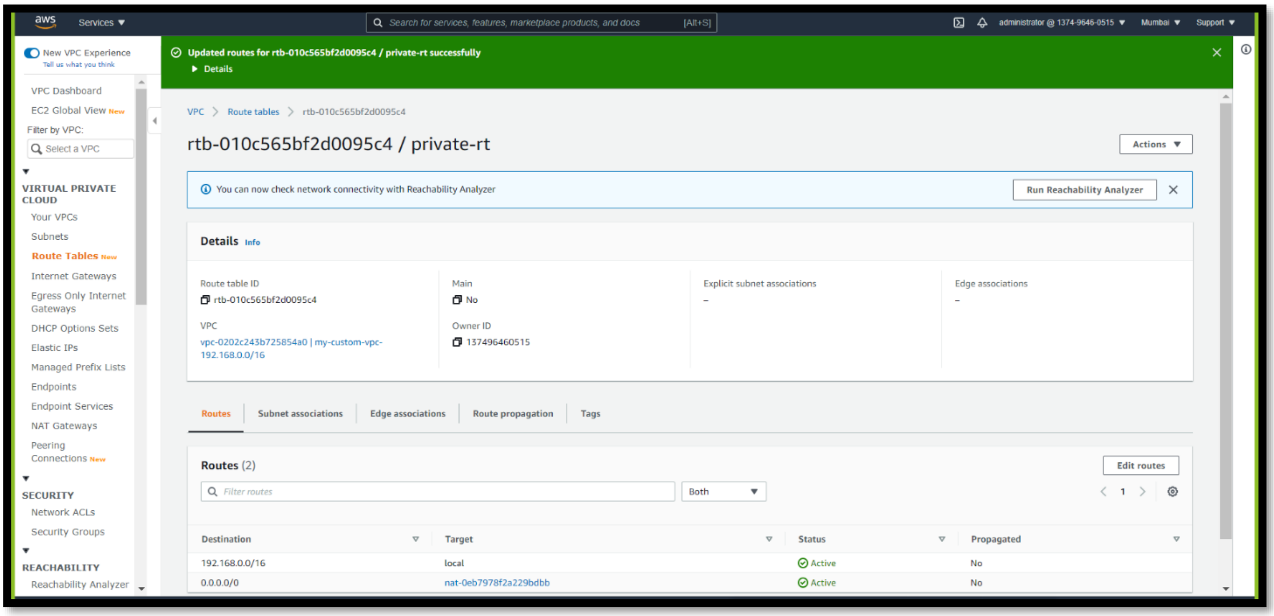
Step -10: Add public access for NAT gateway in private route table.



VPC > Route tables > rtb-076f07c19f26285df > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	nat-07ff580e4b5ccfb8f	-	No



Updated routes for rtb-010c565bf2d0095c4 / private-rt successfully

Details

VPC > Route tables > rtb-010c565bf2d0095c4

rtb-010c565bf2d0095c4 / private-rt

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-010c565bf2d0095c4

Main: No

Explicit subnet associations: –

Edge associations: –

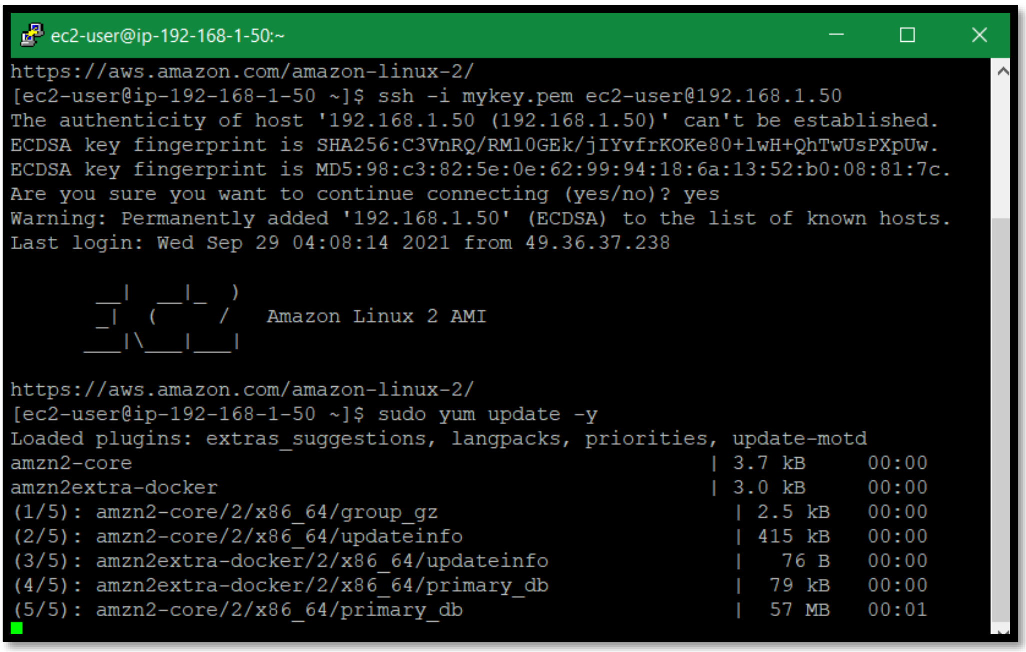
VPC: vpc-0202c243b725854a0 | my-custom-vpc-192.168.0.0/16

Owner ID: 137496460515

Routes (2)

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	nat-0eb7978f2a229bdbb	Active	No

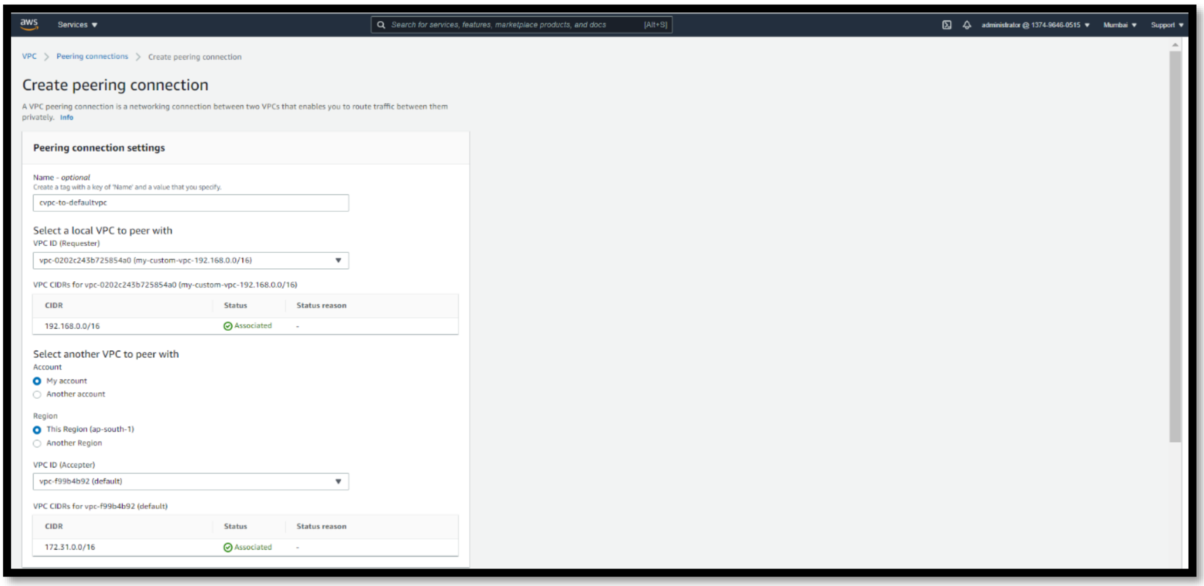
Step -10a: Once the NAT Gateway with public subnet is set-up, we are able to do sudo yum update -y. (As NAT is used to connect private instances to the internet or other AWS services so our private instance has now access to the internet as we setup NAT gateway, an AWS managed NAT service).



ec2-user@ip-192-168-1-50:~

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-1-50 ~]$ ssh -i mykey.pem ec2-user@192.168.1.50
The authenticity of host '192.168.1.50 (192.168.1.50)' can't be established.
ECDSA key fingerprint is SHA256:C3VnRQ/RM10GEk/jIYvfrKOKe80+lwH+QhTwUsPXpUw.
ECDSA key fingerprint is MD5:98:c3:82:5e:0e:62:99:94:18:6a:13:52:b0:08:81:7c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.50' (ECDSA) to the list of known hosts.
Last login: Wed Sep 29 04:08:14 2021 from 49.36.37.238

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-1-50 ~]$ sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                              | 3.7 kB     00:00
amzn2extra-docker                                       | 3.0 kB     00:00
(1/5): amzn2-core/2/x86_64/group_gz                       |  2.5 kB   00:00
(2/5): amzn2-core/2/x86_64/updateinfo                     | 415 kB    00:00
(3/5): amzn2extra-docker/2/x86_64/updateinfo              |   76 B    00:00
(4/5): amzn2extra-docker/2/x86_64/primary_db              |  79 kB    00:00
(5/5): amzn2-core/2/x86_64/primary_db                     |  57 MB    00:01
```

Step -11: Create connecting Peer for our custom VPC.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
VPC > Peering connections > Create peering connection

Create peering connection

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.
cvpc-to-defaultvpc

Select a local VPC to peer with
VPC ID (Requester)
vpc-0202c243b725854a0 (my-custom-vpc-192.168.0.0/16)

VPC CIDRs for vpc-0202c243b725854a0 (my-custom-vpc-192.168.0.0/16)

CIDR	Status	Status reason
192.168.0.0/16	Associated	-

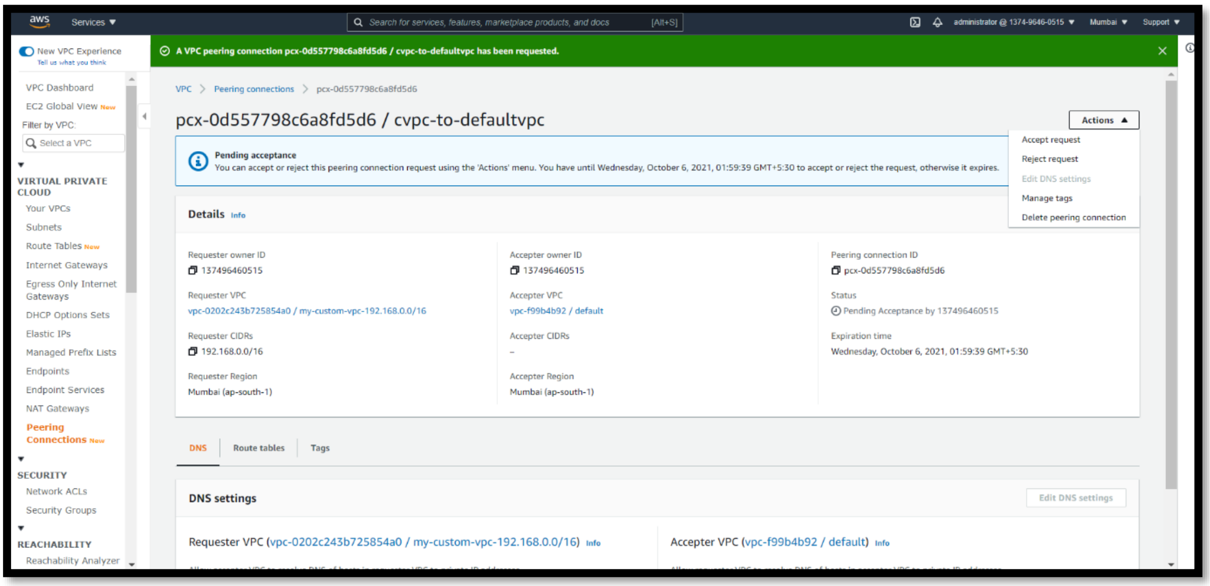
Select another VPC to peer with
Account
● My account
○ Another account

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

VPC ID (Accepter)
vpc-f99b4b92 (default)

VPC CIDRs for vpc-f99b4b92 (default)

CIDR	Status	Status reason
172.31.0.0/16	Associated	-



A VPC peering connection pcx-0d557798c6a8fd5d6 / cvpc-to-defaultvpc has been requested.

pcx-0d557798c6a8fd5d6 / cvpc-to-defaultvpc

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Wednesday, October 6, 2021, 01:59:39 GMT+5:30 to accept or reject the request, otherwise it expires.

Details Info

Requester owner ID
137496460515

Requester VPC
vpc-0202c243b725854a0 / my-custom-vpc-192.168.0.0/16

Requester CIDRs
192.168.0.0/16

Requester Region
Mumbai (ap-south-1)

Accepter owner ID
137496460515

Accepter VPC
vpc-f99b4b92 / default

Accepter CIDRs
–

Accepter Region
Mumbai (ap-south-1)

Peering connection ID
pcx-0d557798c6a8fd5d6

Status
Pending Acceptance by 137496460515

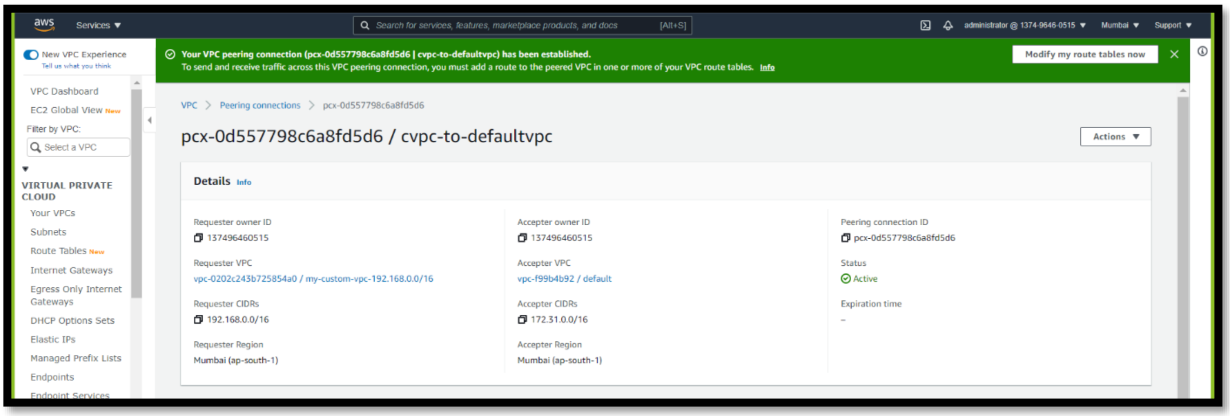
Expiration time
Wednesday, October 6, 2021, 01:59:39 GMT+5:30

DNS settings

Requester VPC (vpc-0202c243b725854a0 / my-custom-vpc-192.168.0.0/16) Info

Accepter VPC (vpc-f99b4b92 / default) Info

NOTE: In above figure as both the machines are in my account, I am getting the option to Accept the request for VPC



Your VPC peering connection (pcx-0d557798c6a8fd5d6 | cvpc-to-defaultvpc) 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. Info

pcx-0d557798c6a8fd5d6 / cvpc-to-defaultvpc

Details Info

Requester owner ID
137496460515

Requester VPC
vpc-0202c243b725854a0 / my-custom-vpc-192.168.0.0/16

Requester CIDRs
192.168.0.0/16

Requester Region
Mumbai (ap-south-1)

Accepter owner ID
137496460515

Accepter VPC
vpc-f99b4b92 / default

Accepter CIDRs
172.31.0.0/16

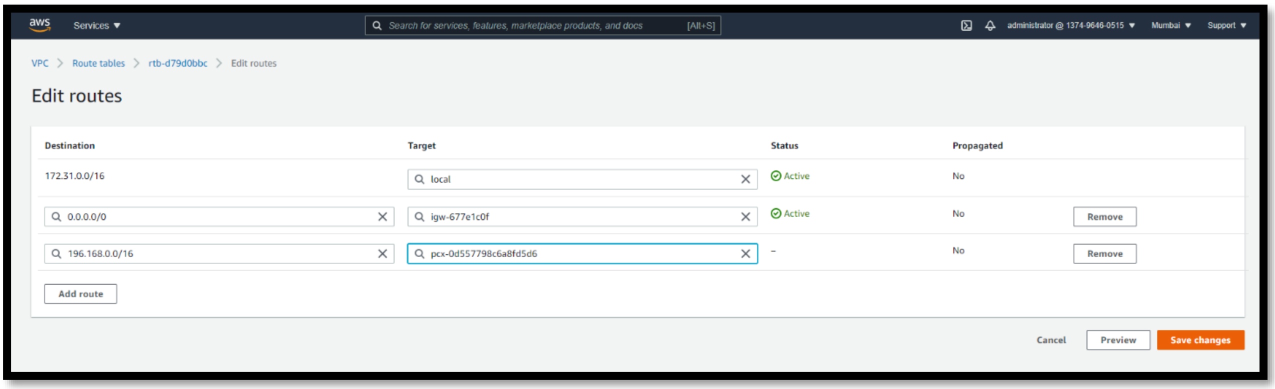
Accepter Region
Mumbai (ap-south-1)

Peering connection ID
pcx-0d557798c6a8fd5d6

Status
Active

Expiration time
–

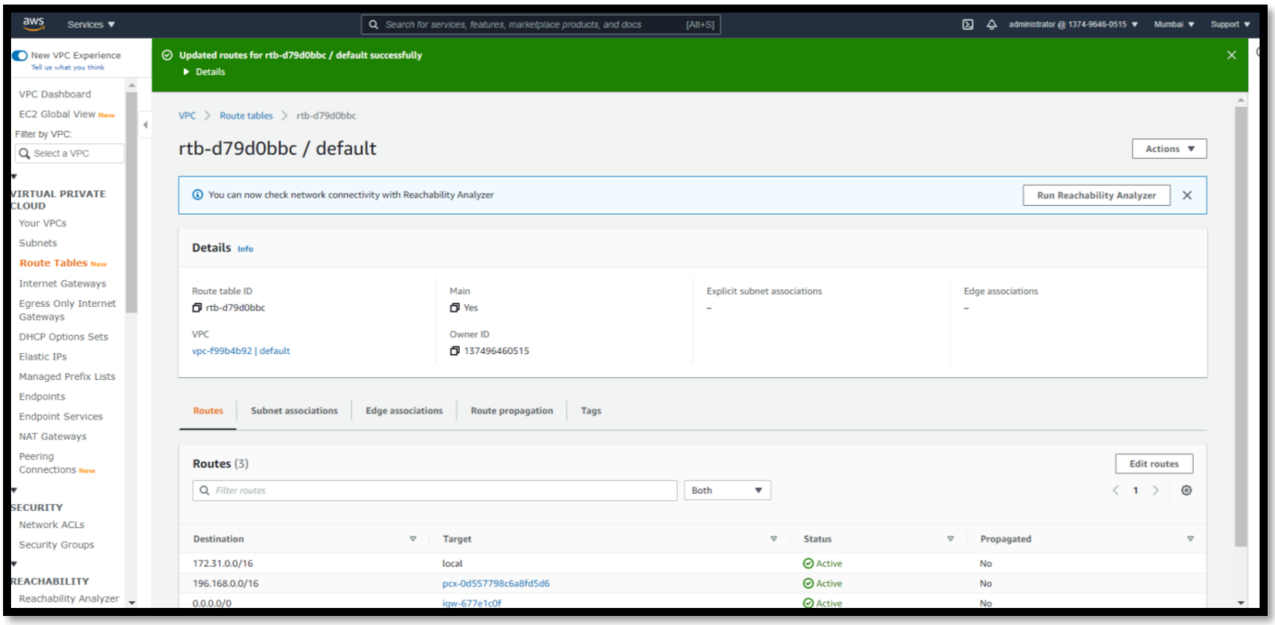
Step -12: Go to default route table and add route to custom VPC from other VPC (i.e., we are setting the peering connection here).


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
Add route
Remove
Cancel
Preview
Save changes

VPC > Route tables > rtb-d79d0bbc > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-677e1c0f	Active	No
196.168.0.0/16	pcx-0d557798c6a8fd5d6	-	No



Updated routes for rtb-d79d0bbc / default successfully

▶ Details

VPC > Route tables > rtb-d79d0bbc

rtb-d79d0bbc / default

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-d79d0bbc

Main: Yes

Explicit subnet associations: –

Edge associations: –

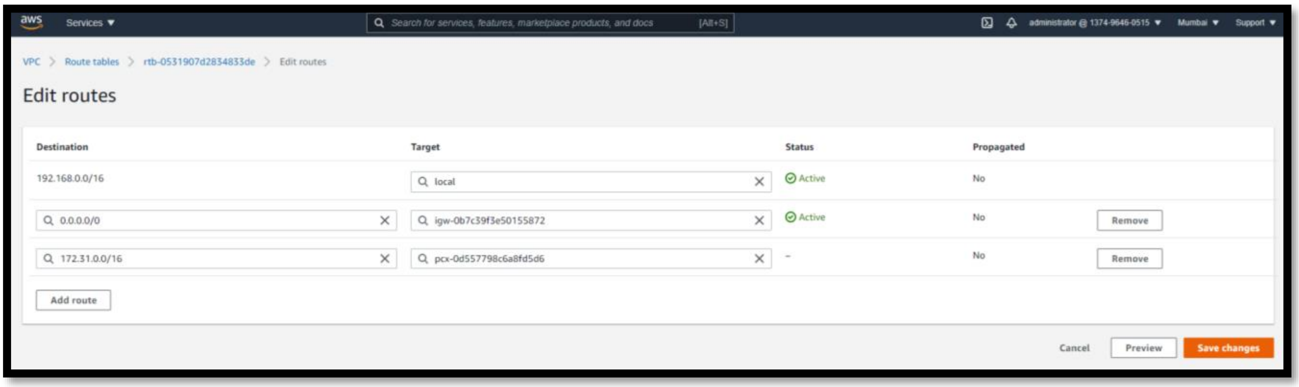
VPC: vpc-f99b4b92 | default

Owner ID: 137496460515

Routes (3)

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
196.168.0.0/16	pcx-0d557798c6a8fd5d6	Active	No
0.0.0.0/0	igw-677e1c0f	Active	No

Step -12a: Similarly, we’ll be adding route to other tables and add route to default VPC from custom VPC (i.e., we are setting the peering connection here).

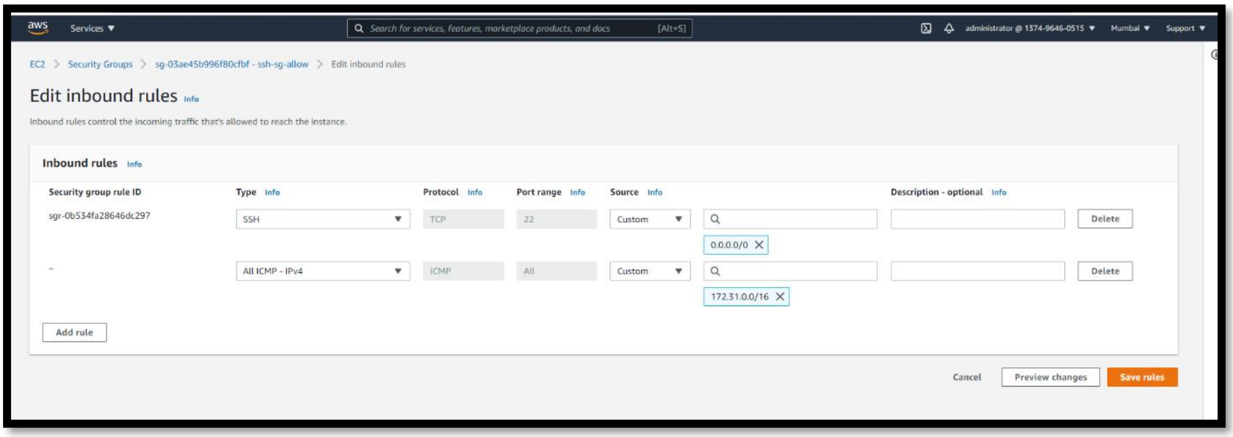

aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515 ▼
Mumbai ▼
Support ▼
Add route
Remove
Cancel
Preview
Save changes

VPC > Route tables > rtb-0531907d2834833de > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-0b7c39f3e50155872	Active	No
172.31.0.0/16	pcx-0d557798c6a8fd5d6	-	No

Step-13) Go to security group of default machine and Add rule (All ICMP). We are doing this to enable ping in security groups of our machine.



EC2 > Security Groups > sg-03ae45b996f80cfbf - ssh-sg-allow > Edit inbound rules

Edit inbound rules

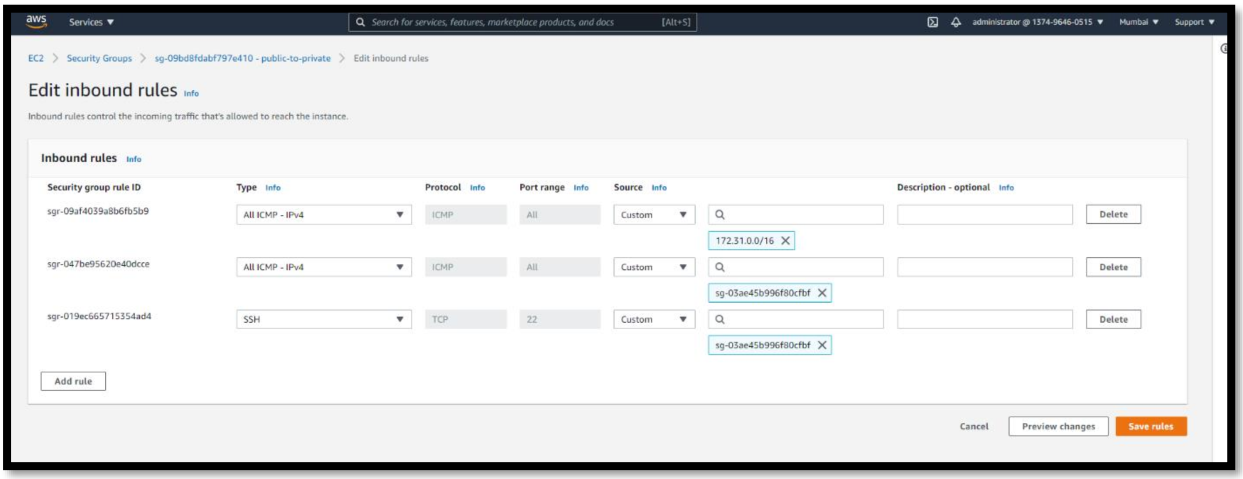
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0b534fa28646dc297	SSH	TCP	22	Custom	0.0.0.0/0	
-	All ICMP - IPv4	ICMP	All	Custom	172.31.0.0/16	

aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515
Mumbai
Support
Info
Delete
Add rule
Cancel
Preview changes
Save rules

Step-13b) Similarly we will enable ping for other machines as well.



EC2 > Security Groups > sg-09bd8fdabf797e410 - public-to-private > Edit inbound rules

Edit inbound rules

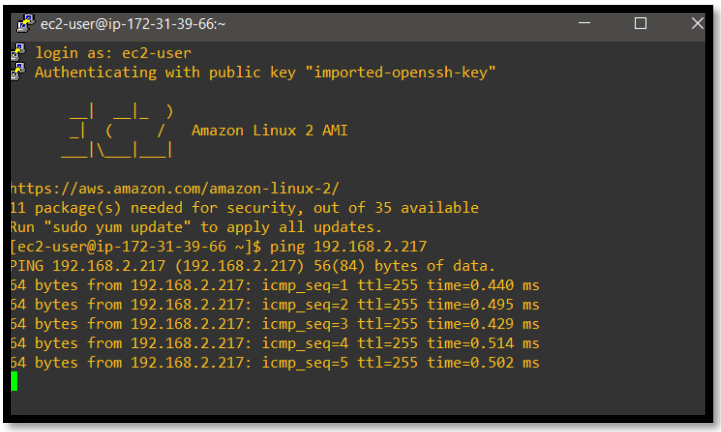
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-09af4039a8b6fb5b9	All ICMP - IPv4	ICMP	All	Custom	172.31.0.0/16	
sgr-047be95620e40dcce	All ICMP - IPv4	ICMP	All	Custom	sg-03ae45b996f80cfbf	
sgr-019ec665715354ad4	SSH	TCP	22	Custom	sg-03ae45b996f80cfbf	

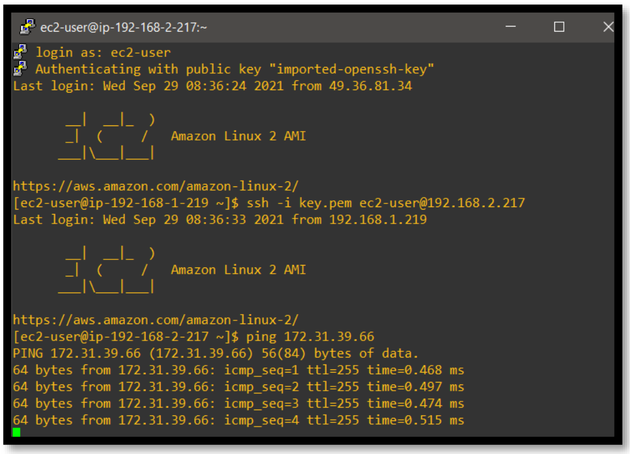
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
administrator @ 1374-9646-0515
Mumbai
Support
Info
Delete
Add rule
Cancel
Preview changes
Save rules

Step -14: Now ping will work hence both the private machines are pinging with each other hence it is verified that we have established a successful VPC peering.



ec2-user@ip-172-31-39-66:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

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

nttps://aws.amazon.com/amazon-linux-2/
11 package(s) needed for security, out of 35 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-39-66 ~]$ ping 192.168.2.217
PING 192.168.2.217 (192.168.2.217) 56(84) bytes of data.
54 bytes from 192.168.2.217: icmp_seq=1 ttl=255 time=0.440 ms
54 bytes from 192.168.2.217: icmp_seq=2 ttl=255 time=0.495 ms
54 bytes from 192.168.2.217: icmp_seq=3 ttl=255 time=0.429 ms
54 bytes from 192.168.2.217: icmp_seq=4 ttl=255 time=0.514 ms
54 bytes from 192.168.2.217: icmp_seq=5 ttl=255 time=0.502 ms
```



ec2-user@ip-192-168-2-217:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Sep 29 08:36:24 2021 from 49.36.81.34

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-1-219 ~]$ ssh -i key.pem ec2-user@192.168.2.217
Last login: Wed Sep 29 08:36:33 2021 from 192.168.1.219

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-2-217 ~]$ ping 172.31.39.66
PING 172.31.39.66 (172.31.39.66) 56(84) bytes of data.
64 bytes from 172.31.39.66: icmp_seq=1 ttl=255 time=0.468 ms
64 bytes from 172.31.39.66: icmp_seq=2 ttl=255 time=0.497 ms
64 bytes from 172.31.39.66: icmp_seq=3 ttl=255 time=0.474 ms
64 bytes from 172.31.39.66: icmp_seq=4 ttl=255 time=0.515 ms
```