# Creating a Custom Virtual Private Cloud

## Virtual Private Cloud (VPC)

It is a **virtual network** within the Amazon Web Services (AWS) cloud infrastructure. It allows you to create your **own private network** environment with separate IP address ranges, subnets, route tables, and security groups. This enables you to isolate your resources and control network traffic flow.

VPC allows you to create **subnets** within your virtual network. Subnets are logical divisions of the VPC IP address range that you can use to organize and isolate resources.

VPC enables internet connectivity for your resources. You can configure an **Internet Gateway** to allow outbound internet access from your VPC and set up **public** subnets for resources that need to be accessible from the internet.

**Network Address Translation** (NAT) gateways or instances can be used to enable internet access for **private** subnets.

There are two types of NAT available in AWS VPC:

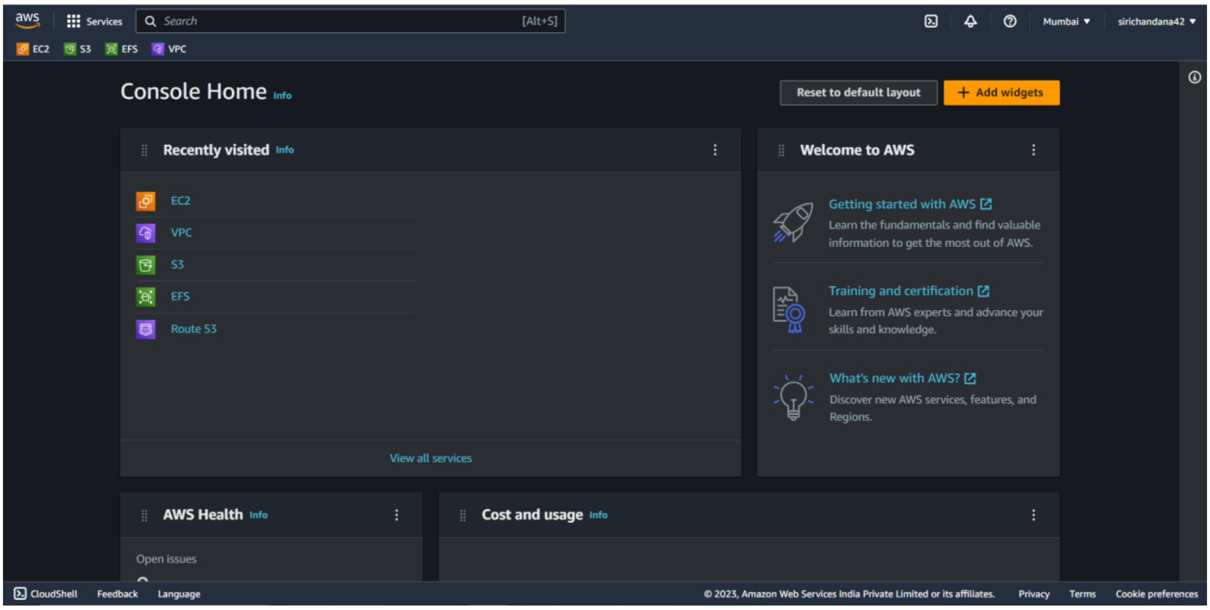
1. **NAT Gateway:**
   - A NAT Gateway is a managed service provided by AWS.
   - It is deployed in a public subnet and requires an Elastic IP address.
2. **NAT Instance:**
   - A NAT Instance is a regular EC2 instance that is deployed in a public subnet And configured to perform NAT.
   - Source and destination check should be disabled whenever we create an NAT using instance

VPC supports integration with AWS **VPN** and AWS **Direct Connect**. This allows you to securely connect your VPC to your on-premises network or other networks through encrypted VPN tunnels or dedicated network connections.

## Network Access Control List

Network Access Control Lists (NACLs) are a type of security control that you can use to filter and control inbound and outbound traffic at the subnet level in your Virtual Private Cloud.

1. First Log in to your AWS free tier account and open your AWS management console and click on services and **select VPC**



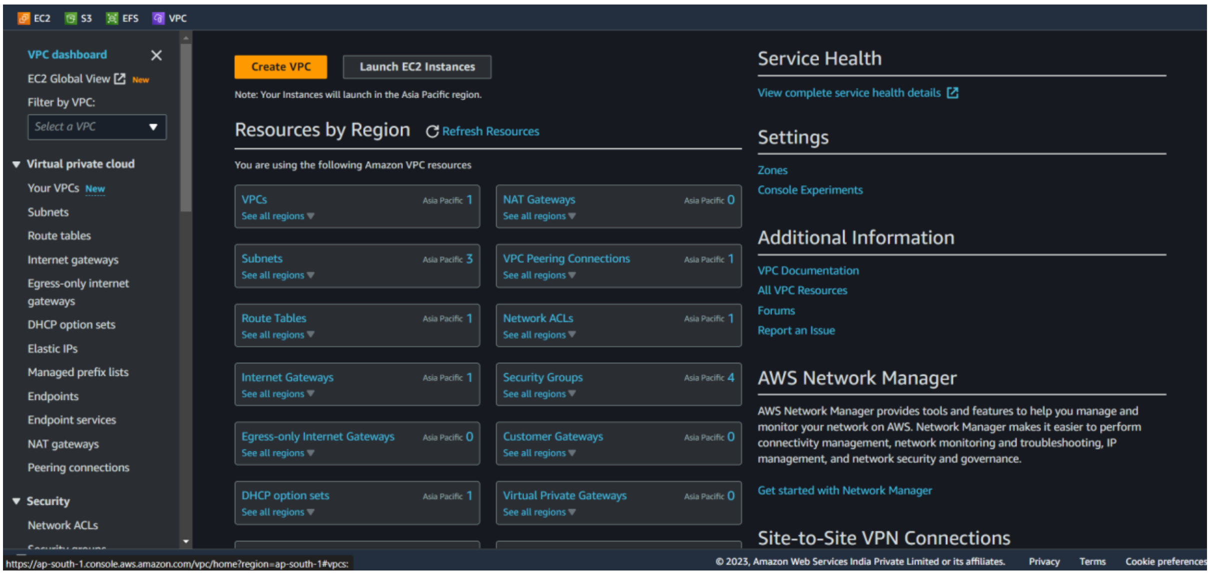
Learn the fundamentals and find valuable information to get the most out of AWS.

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

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

2. Now you will be redirected to VPC dashboard then click on your VPCs to **create a custom** virtual private cloud



Note: Your Instances will launch in the Asia Pacific region.

You are using the following Amazon VPC resources

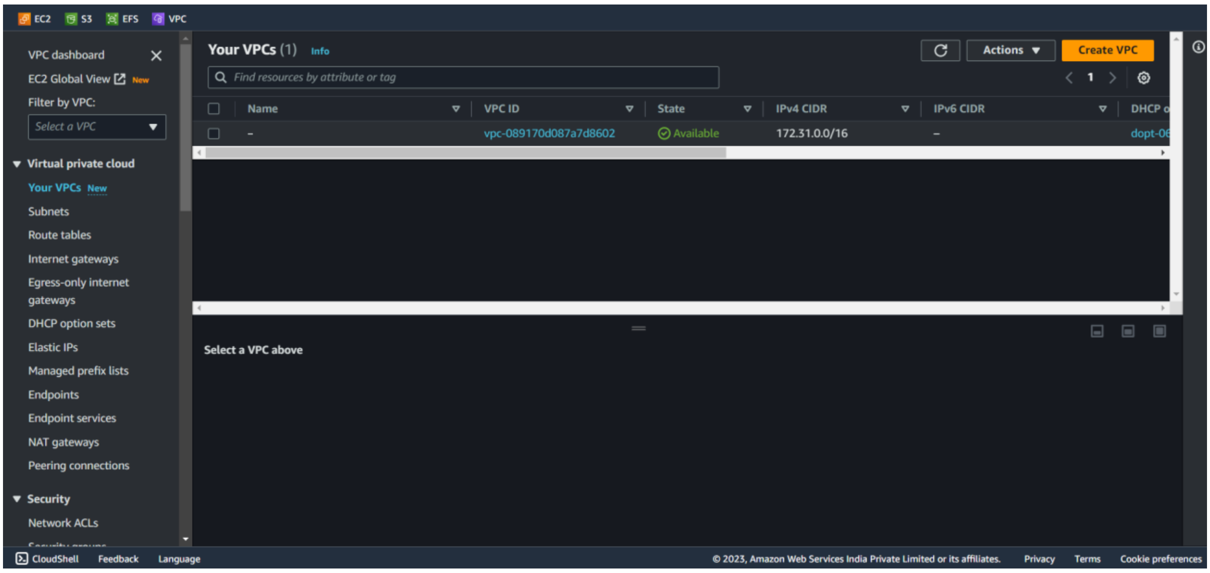
| | | | |
|---|---|---|---|
| VPCs<br>See all regions ▼ | Asia Pacific 1 | NAT Gateways<br>See all regions ▼ | Asia Pacific 0 |
| Subnets<br>See all regions ▼ | Asia Pacific 3 | VPC Peering Connections<br>See all regions ▼ | Asia Pacific 1 |
| Route Tables<br>See all regions ▼ | Asia Pacific 1 | Network ACLs<br>See all regions ▼ | Asia Pacific 1 |
| Internet Gateways<br>See all regions ▼ | Asia Pacific 1 | Security Groups<br>See all regions ▼ | Asia Pacific 4 |
| Egress-only Internet Gateways<br>See all regions ▼ | Asia Pacific 0 | Customer Gateways<br>See all regions ▼ | Asia Pacific 0 |
| DHCP option sets<br>See all regions ▼ | Asia Pacific 1 | Virtual Private Gateways<br>See all regions ▼ | Asia Pacific 0 |

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#vpcs:

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

3. Now click on **create VPC** to create a new custom VPC.

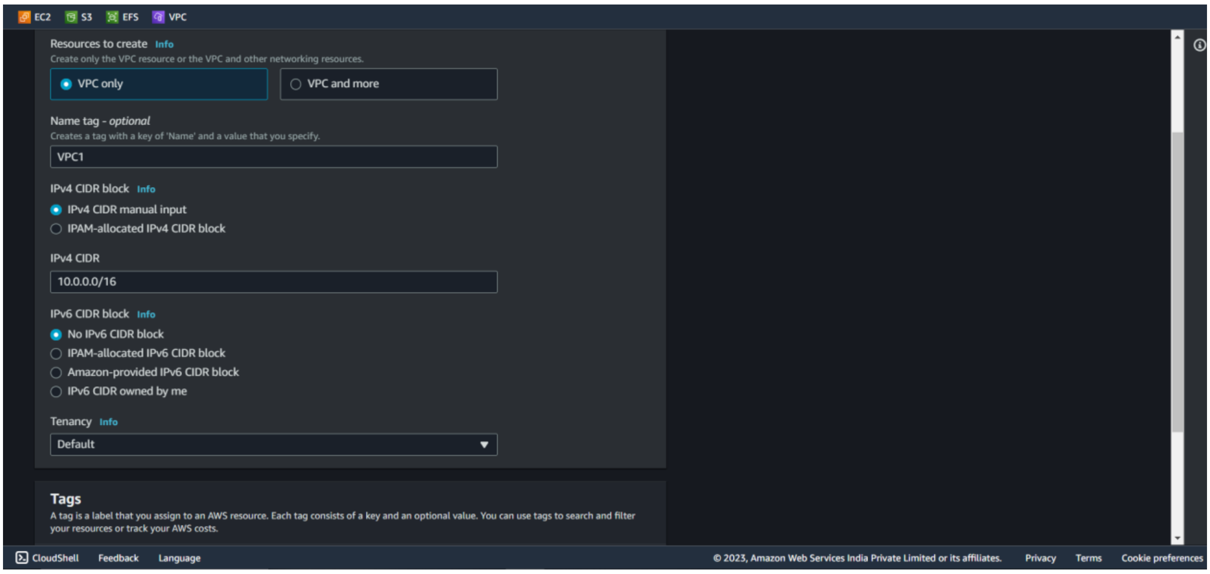


Your VPCs (1)

| Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | DHCP o |
|---|---|---|---|---|---|
| - | vpc-089170d087a7d8602 | ✓ Available | 172.31.0.0/16 | - | dopt-06 |

Select a VPC above

4. Now set a **name** for your VPC and assign **a valid CIDR** and click on create VPC.



Resources to create

Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*

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

VPC1

IPv4 CIDR block

● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block

● No IPv6 CIDR block

○ IPAM-allocated IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

○ IPv6 CIDR owned by me

Tenancy

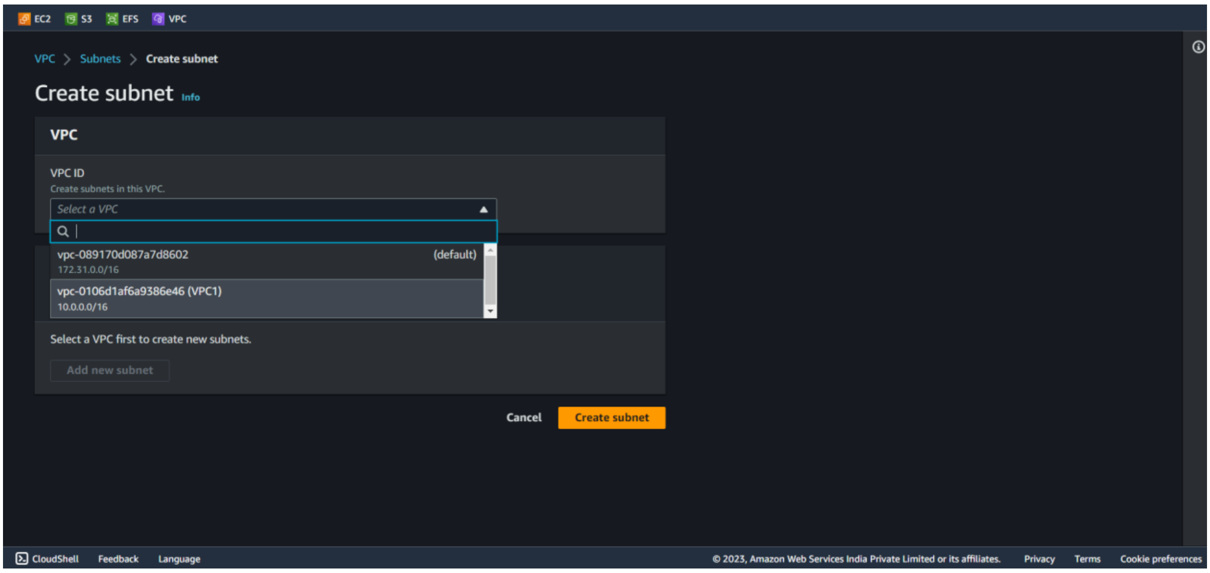
Default

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.

**Classless Inter-Domain Routing** (CIDR) notation is commonly used to represent subnets. It combines the network IP address and the subnet mask, represented as a slash followed by the number of network bits. For example, a subnet with a CIDR notation of /24 means that the first 24 bits of the IP address represent the network, while the remaining 8 bits represent the host portion. AWS allows from **/16 to /28** only

5. Now go to subnets and click on **create subnet** and create 2 subnets in custom VPC



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
Select a VPC

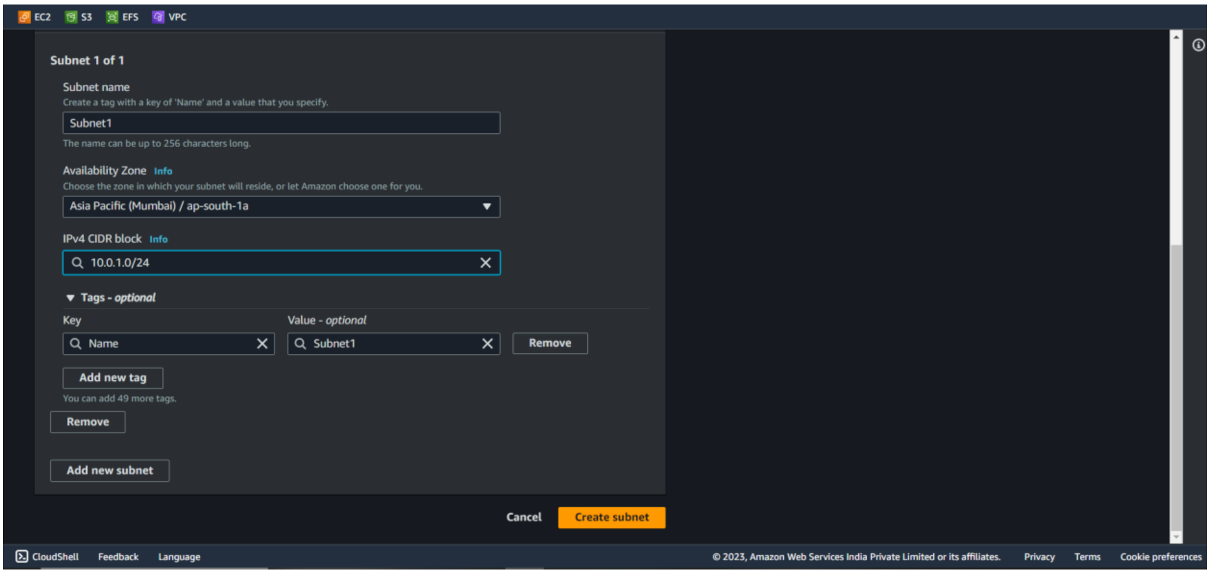
vpc-089170d087a7d8602 (default)
172.31.0.0/16

vpc-0106d1af6a9386e46 (VPC1)
10.0.0.0/16

Select a VPC first to create new subnets.

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

6. Give the subnet name. Select the availability zone in which we want to create a subnet, give the CIDR of the subnet within the CIDR of VPC.



Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Subnet1
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
10.0.1.0/24

Tags - *optional*

Key: Name
Value - *optional*: Subnet1

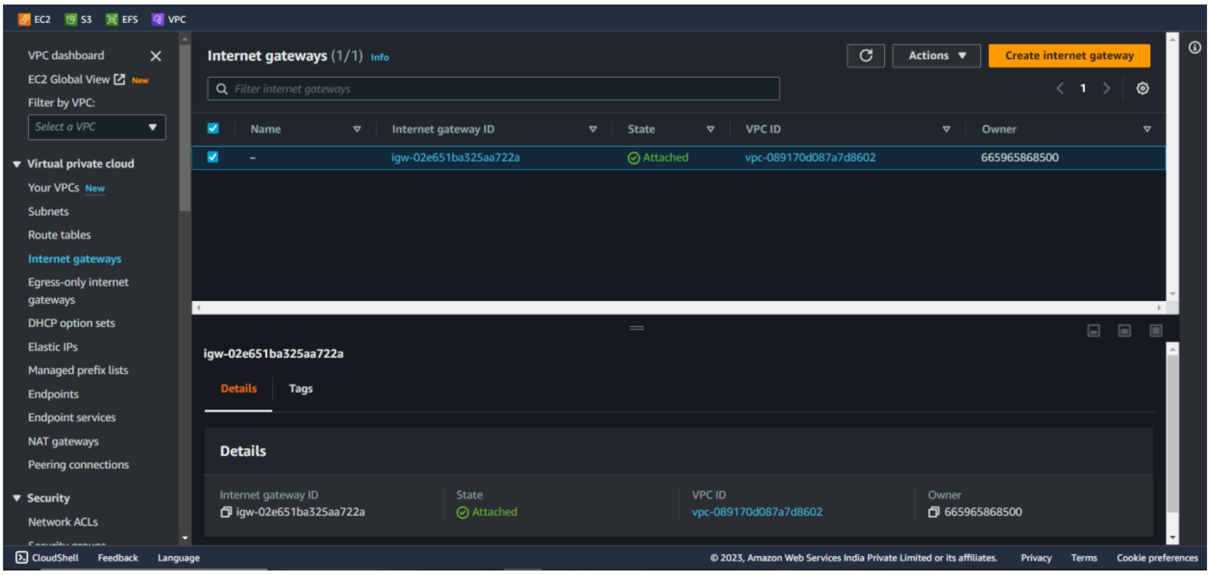
You can add 49 more tags.

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

Similarly create another subnet with CIDR **10.0.2.0/24** so that 2 subnets will be created in same VPC.

Rename them as Public and private for your convenience.

7. Now for internet access for your public subnet create an **Internet gateway**. For that go to internet gateways and click on create Internet Gateway.



Internet gateways (1/1) Info

| | Name | Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|---|---|
| ☑ | – | igw-02e651ba325aa722a | Attached | vpc-089170d087a7d8602 | 665965868500 |

igw-02e651ba325aa722a

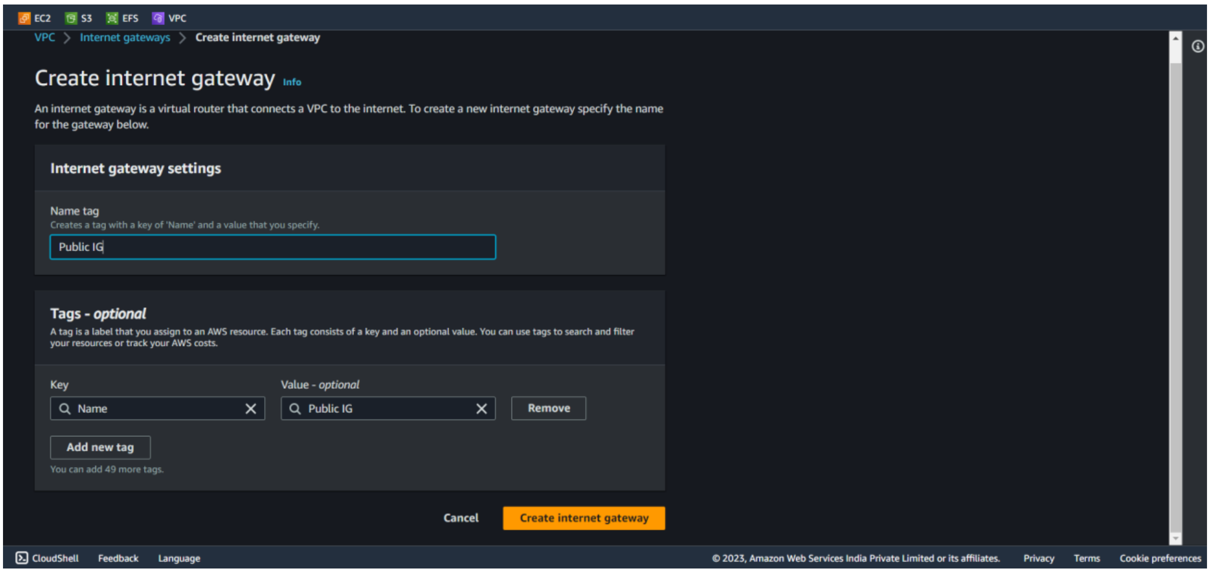
Details | Tags

Details

| Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|
| igw-02e651ba325aa722a | Attached | vpc-089170d087a7d8602 | 665965868500 |

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

8. Now name your Internet gateway and click on create 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.
Public IG

Tags - *optional*

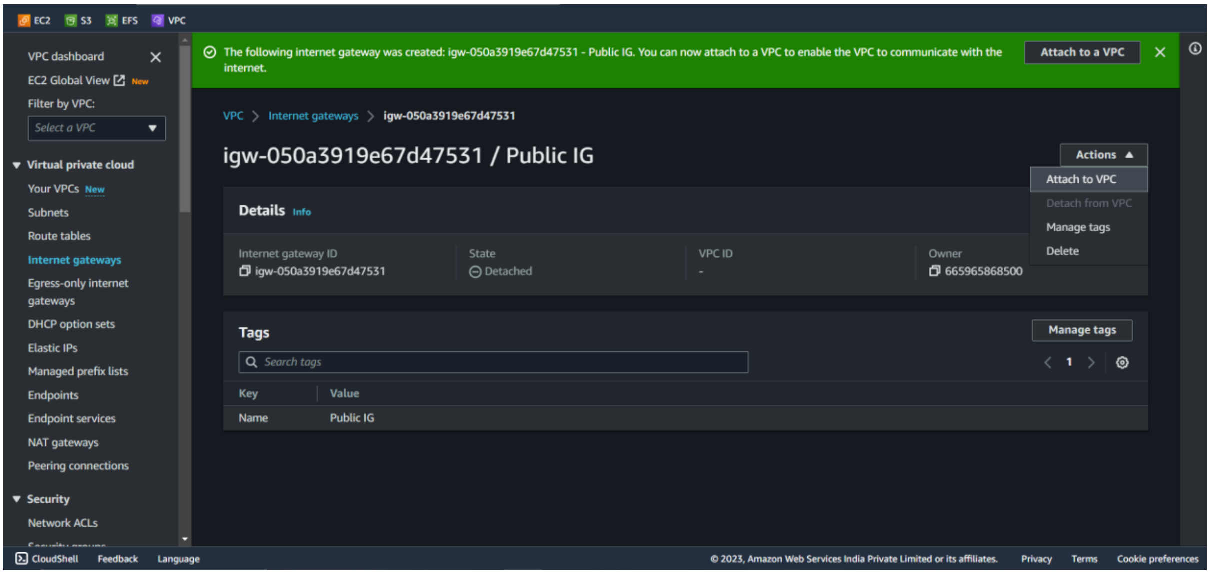
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* |
|---|---|
| Name | Public IG |

You can add 49 more tags.

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

9. Now select the VPC and click on actions and click on attach to VPC to **attach the internet gateway** to the custom VPC.



The following internet gateway was created: igw-050a3919e67d47531 - Public IG. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-050a3919e67d47531 / Public IG

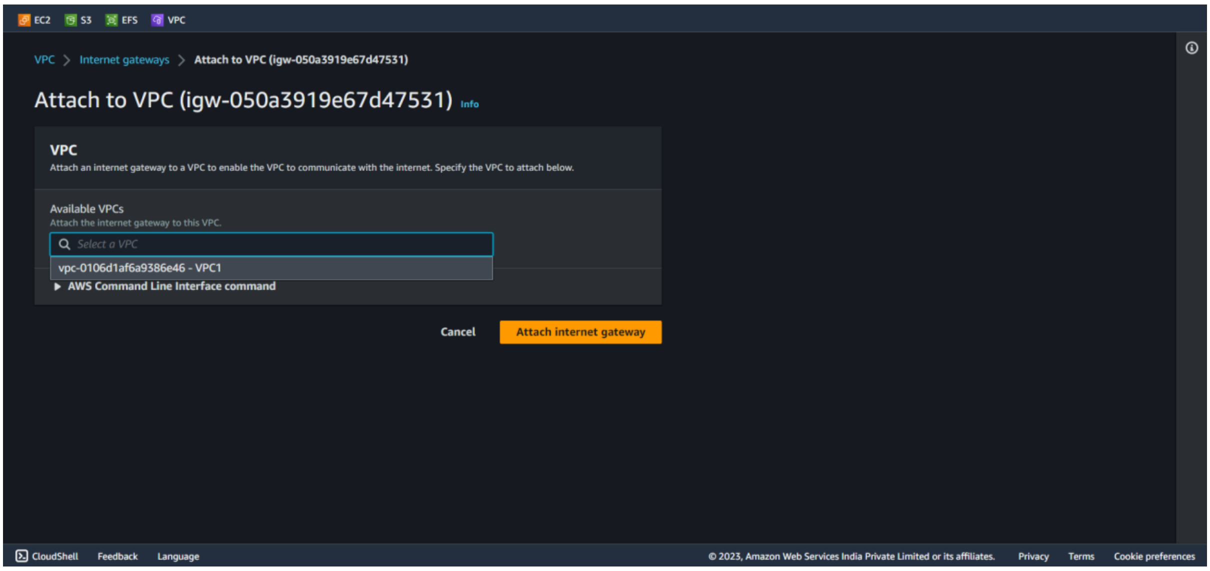
Details

| Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|
| igw-050a3919e67d47531 | Detached | - | 665965868500 |

Tags

| Key | Value |
|---|---|
| Name | Public IG |

10. Now select the custom VPC from the available VPCs and attach the IG to the VPC



EC2
S3
EFS
VPC
VPC
Internet gateways
Attach to VPC (igw-050a3919e67d47531)
Info
Select a VPC
AWS Command Line Interface command
Cancel
Attach internet gateway
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Attach to VPC (igw-050a3919e67d47531)

VPC

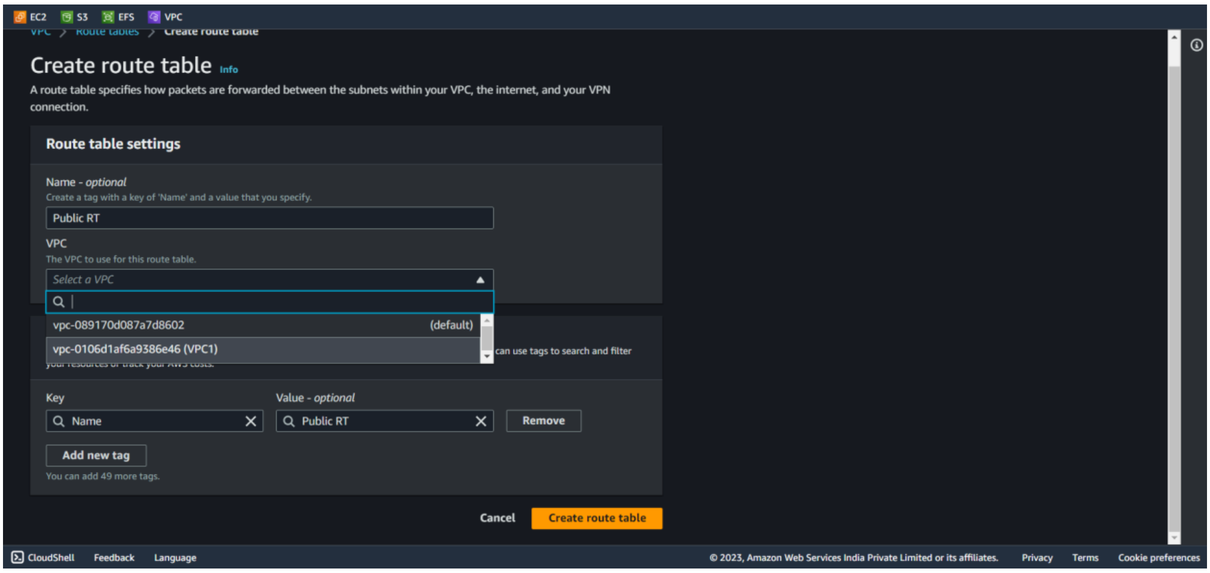
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0106d1af6a9386e46 - VPC1

11. Now to create **route tables** for both public and private subnets click on Route tables and click on create route table name the RT and select the VPC and 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.
Public RT

VPC
The VPC to use for this route table.
*Select a VPC*

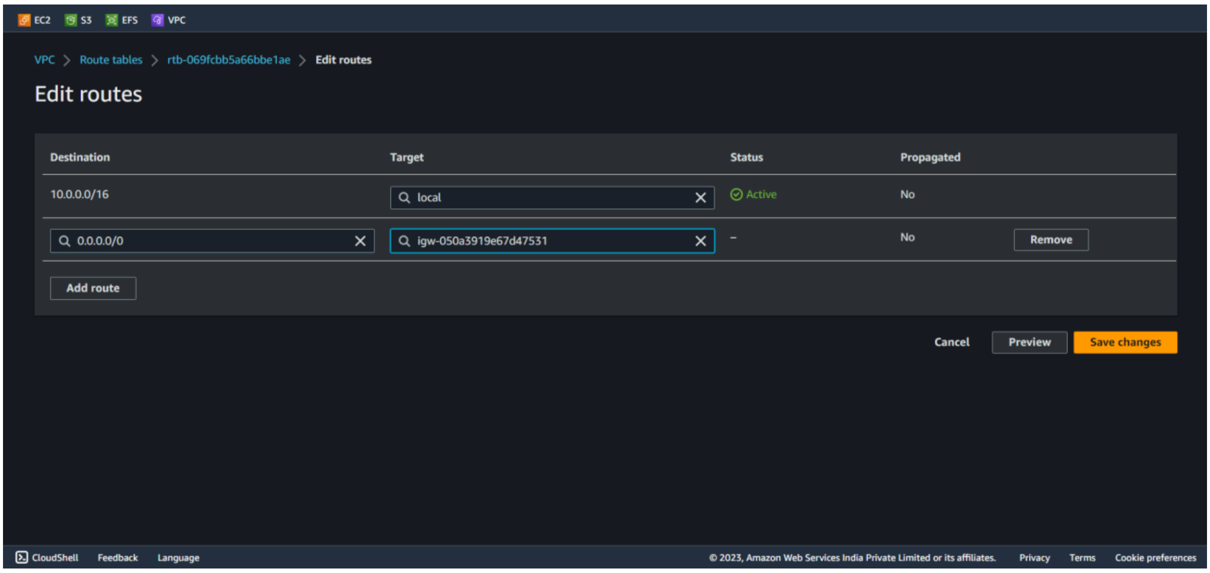
vpc-089170d087a7d8602 (default)
vpc-0106d1af6a9386e46 (VPC1)

...can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* |
|---|---|
| Name | Public RT |

You can add 49 more tags.

12. Now edit the route settings and add Internet gateway as a route to it and click on save changes.



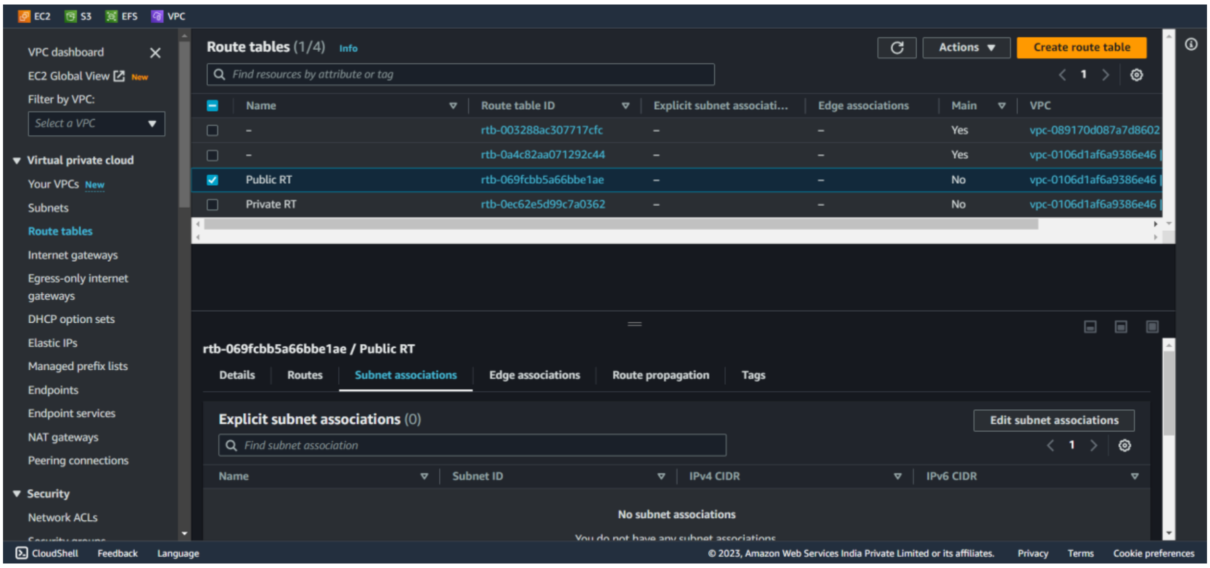
VPC > Route tables > rtb-069fcbb5a66bbe1ae > Edit routes

## Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |
| 0.0.0.0/0 | igw-050a3919e67d47531 | - | No |

Similarly create another route table but don't add IG as private subnet shouldn't have access to the internet

13. Now select the route table and select subnet associations, click on edit subnet associations and associate the public subnet to public and private subnet to private RT.



Route tables (1/4) Info

| | Name | Route table ID | Explicit subnet associati... | Edge associations | Main | VPC |
|---|---|---|---|---|---|---|
| □ | – | rtb-003288ac307717cfc | – | – | Yes | vpc-089170d087a7d8602 |
| □ | – | rtb-0a4c82aa071292c44 | – | – | Yes | vpc-0106d1af6a9386e46 |
| ☑ | Public RT | rtb-069fcbb5a66bbe1ae | – | – | No | vpc-0106d1af6a9386e46 |
| □ | Private RT | rtb-0ec62e5d99c7a0362 | – | – | No | vpc-0106d1af6a9386e46 |

rtb-069fcbb5a66bbe1ae / Public RT

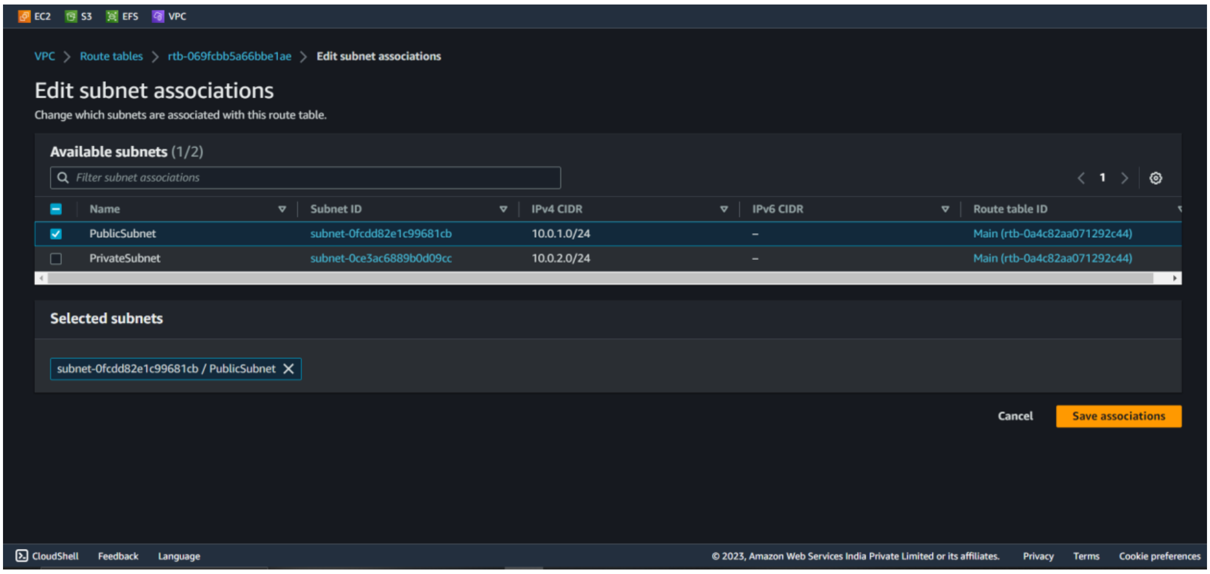
Explicit subnet associations (0)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|

No subnet associations

You do not have any subnet associations

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



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

| | Name | Subnet ID | IPv4 CIDR | IPv6 CIDR | Route table ID |
|---|---|---|---|---|---|
| ☑ | PublicSubnet | subnet-0fcdd82e1c99681cb | 10.0.1.0/24 | – | Main (rtb-0a4c82aa071292c44) |
| □ | PrivateSubnet | subnet-0ce3ac6889b0d09cc | 10.0.2.0/24 | – | Main (rtb-0a4c82aa071292c44) |

Selected subnets

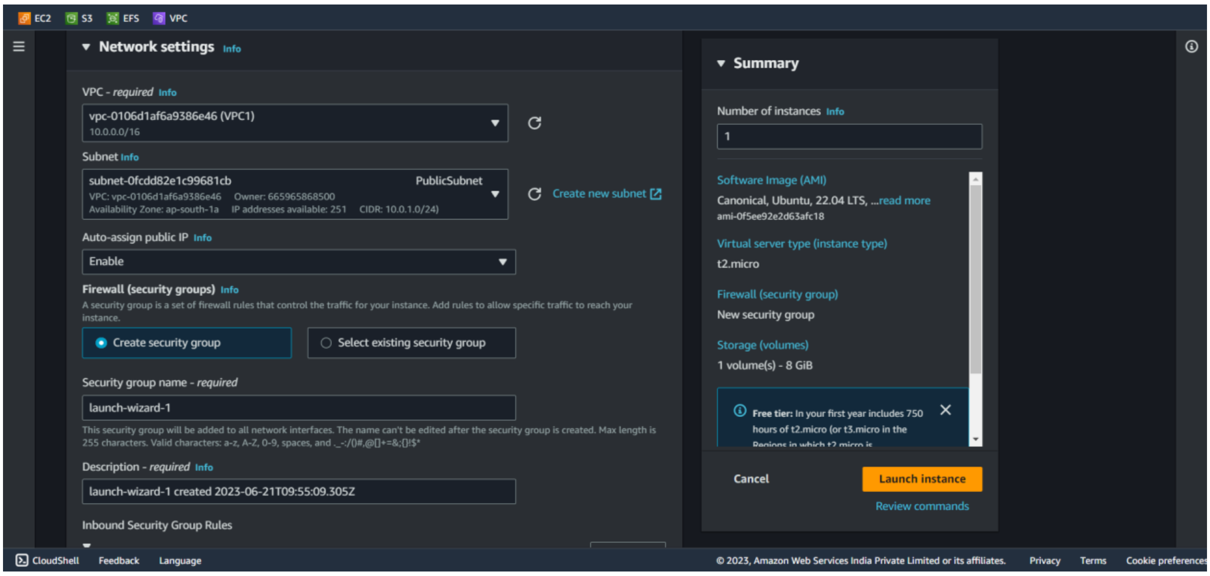
subnet-0fcdd82e1c99681cb / PublicSubnet

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

Now your VPC has been completely set up now create 2 instances in two different subnets in your custom VPC.

## Creating Instances in two different subnets

1. While creating ensure that your network settings are on Custom VPC and subnet in a public subnet for Public instance and enable **auto assign public IP** and Private Subnet for private instance.



▼ Network settings Info

VPC - *required* Info

vpc-0106d1af6a9386e46 (VPC1)
10.0.0.0/16

Subnet Info

subnet-0fcdd82e1c99681cb PublicSubnet
VPC: vpc-0106d1af6a9386e46 Owner: 665965868500
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.1.0/24)

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*

launch-wizard-1

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-1 created 2023-06-21T09:55:09.305Z

Inbound Security Group Rules

▼ Summary

Number of instances Info

1

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

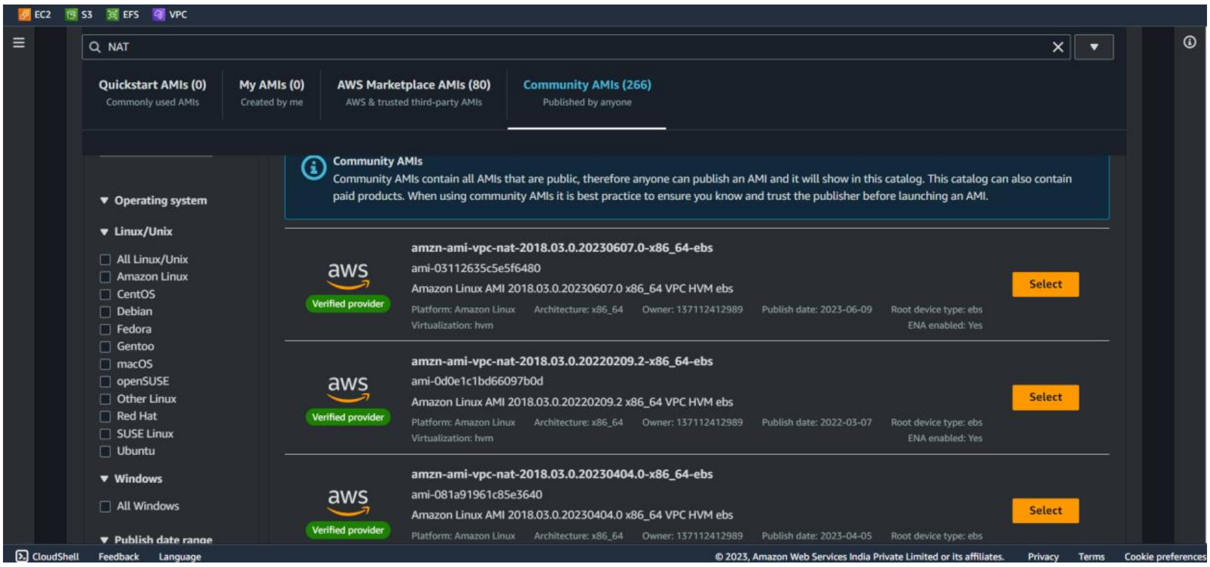
Virtual server type (instance type)
t2.micro

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 Regions in which t2.micro is

2. Create a NAT instance by selecting AMI containing NAT in the community AMIs



NAT

Quickstart AMIs (0) — Commonly used AMIs
My AMIs (0) — Created by me
AWS Marketplace AMIs (80) — AWS & trusted third-party AMIs
Community AMIs (266) — Published by anyone

**Community AMIs**
Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.

▼ Operating system

▼ Linux/Unix

□ All Linux/Unix
□ Amazon Linux
□ CentOS
□ Debian
□ Fedora
□ Gentoo
□ macOS
□ openSUSE
□ Other Linux
□ Red Hat
□ SUSE Linux
□ Ubuntu

▼ Windows

□ All Windows

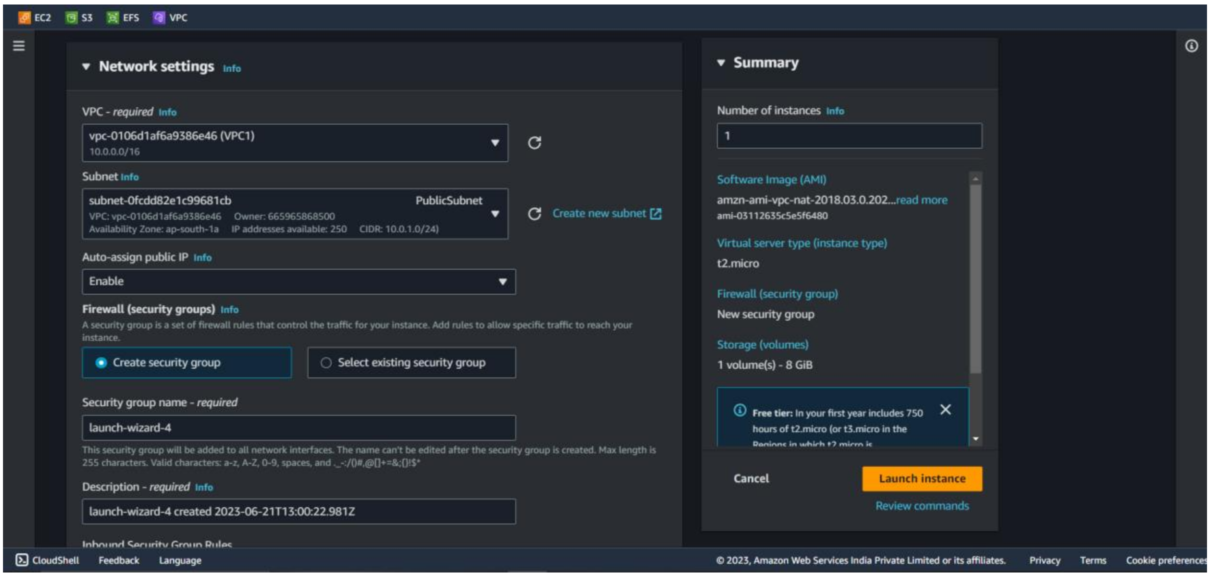
▼ Publish date range

**amzn-ami-vpc-nat-2018.03.0.20230607.0-x86_64-ebs**
ami-03112635c5e5f6480
Amazon Linux AMI 2018.03.0.20230607.0 x86_64 VPC HVM ebs
Platform: Amazon Linux Architecture: x86_64 Owner: 137112412989 Publish date: 2023-06-09 Root device type: ebs
Virtualization: hvm ENA enabled: Yes

**amzn-ami-vpc-nat-2018.03.0.20220209.2-x86_64-ebs**
ami-0d0e1c1bd66097b0d
Amazon Linux AMI 2018.03.0.20220209.2 x86_64 VPC HVM ebs
Platform: Amazon Linux Architecture: x86_64 Owner: 137112412989 Publish date: 2022-03-07 Root device type: ebs
Virtualization: hvm ENA enabled: Yes

**amzn-ami-vpc-nat-2018.03.0.20230404.0-x86_64-ebs**
ami-081a91961c85e3640
Amazon Linux AMI 2018.03.0.20230404.0 x86_64 VPC HVM ebs
Platform: Amazon Linux Architecture: x86_64 Owner: 137112412989 Publish date: 2023-04-05 Root device type: ebs

3. Since NAT requires internet connection to work it is placed in Public subnet



Network settings Info

VPC - *required* Info
vpc-0106d1af6a9386e46 (VPC1)
10.0.0.0/16

Subnet Info
subnet-0fcdd82e1c99681cb PublicSubnet
VPC: vpc-0106d1af6a9386e46 Owner: 665965868500
Availability Zone: ap-south-1a IP addresses available: 250 CIDR: 10.0.1.0/24)

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*
launch-wizard-4
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-4 created 2023-06-21T13:00:22.981Z

Inbound Security Group Rules

Number of instances Info
1

Software Image (AMI)
amzn-ami-vpc-nat-2018.03.0.202...read more
ami-03112635c5e5f6480

Virtual server type (instance type)
t2.micro

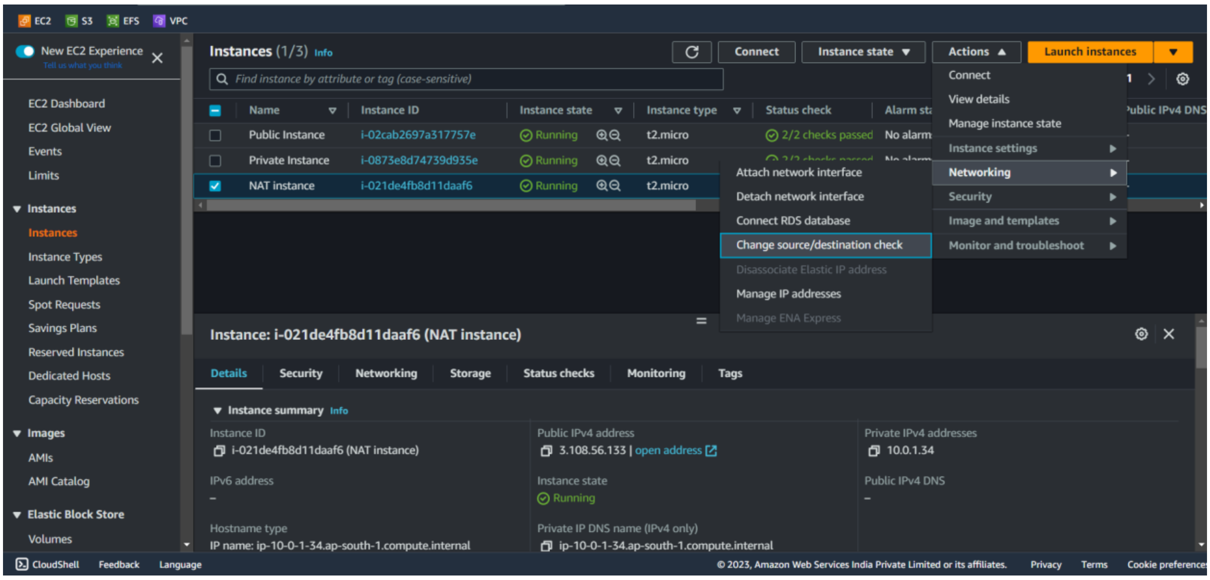
Firewall (security group)
New security group

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

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

4. Now select the instance and stop the source and destination check for the NAT instance



Instances (1/3) Info

Find instance by attribute or tag (case-sensitive)

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm sta | Public IPv4 DNS |
|---|---|---|---|---|---|---|---|
| □ | Public Instance | i-02cab2697a317757e | Running | t2.micro | 2/2 checks passed | No alarm | |
| □ | Private Instance | i-0873e8d74739d935e | Running | t2.micro | 2/2 checks passed | No alarm | |
| ☑ | NAT instance | i-021de4fb8d11daaf6 | Running | t2.micro | | | |

Instance: i-021de4fb8d11daaf6 (NAT instance)

Instance summary Info

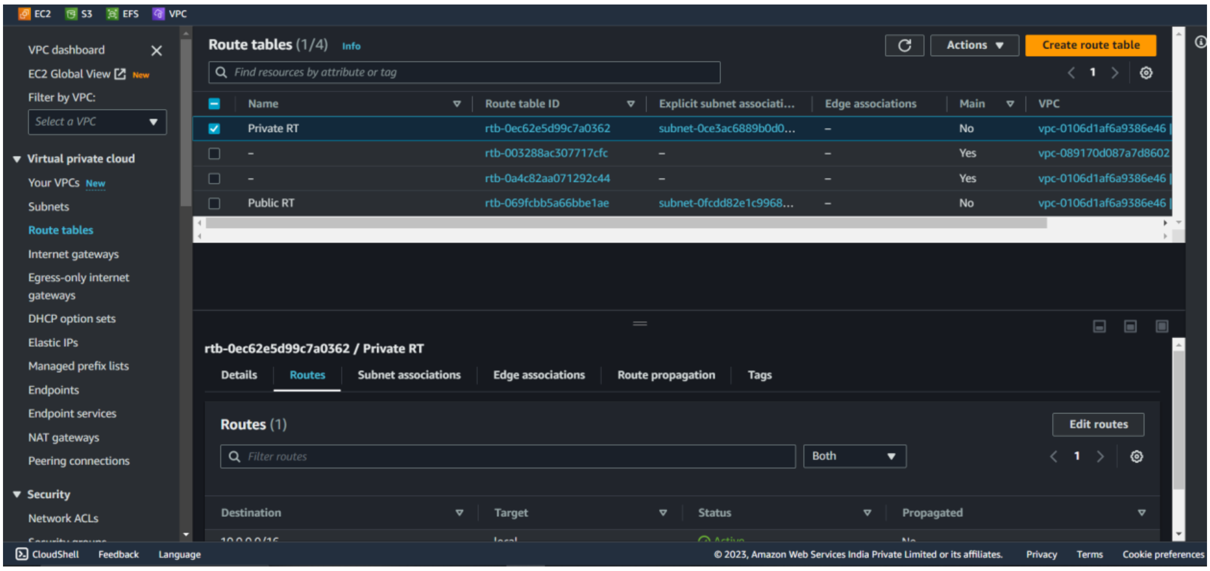
| Instance ID | Public IPv4 address | Private IPv4 addresses |
|---|---|---|
| i-021de4fb8d11daaf6 (NAT instance) | 3.108.56.133 \| open address | 10.0.1.34 |

| IPv6 address | Instance state | Public IPv4 DNS |
|---|---|---|
| – | Running | – |

| Hostname type | Private IP DNS name (IPv4 only) |
|---|---|
| IP name: ip-10-0-1-34.ap-south-1.compute.internal | ip-10-0-1-34.ap-south-1.compute.internal |

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

5. Now add NAT instance as a route in private routes



Route tables (1/4) Info

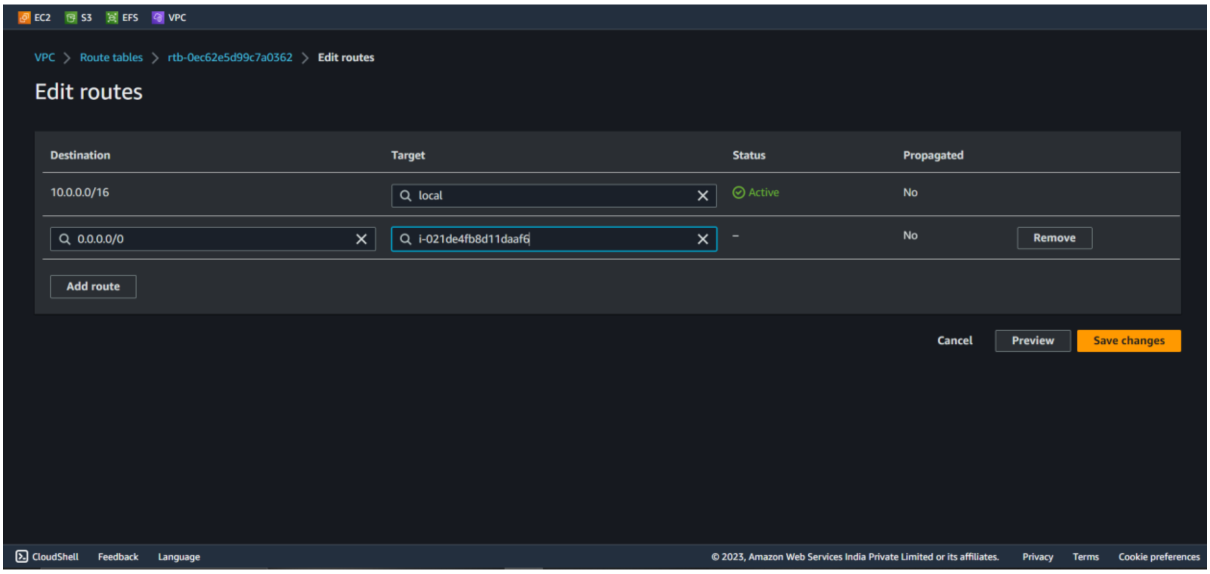
| | Name | Route table ID | Explicit subnet associati... | Edge associations | Main | VPC |
|---|---|---|---|---|---|---|
| ☑ | Private RT | rtb-0ec62e5d99c7a0362 | subnet-0ce3ac6889b0d0... | – | No | vpc-0106d1af6a9386e46 |
| □ | - | rtb-003288ac307717cfc | – | – | Yes | vpc-089170d087a7d8602 |
| □ | - | rtb-0a4c82aa071292c44 | – | – | Yes | vpc-0106d1af6a9386e46 |
| □ | Public RT | rtb-069fcbb5a66bbe1ae | subnet-0fcdd82e1c9968... | – | No | vpc-0106d1af6a9386e46 |

rtb-0ec62e5d99c7a0362 / Private RT

Routes (1)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |

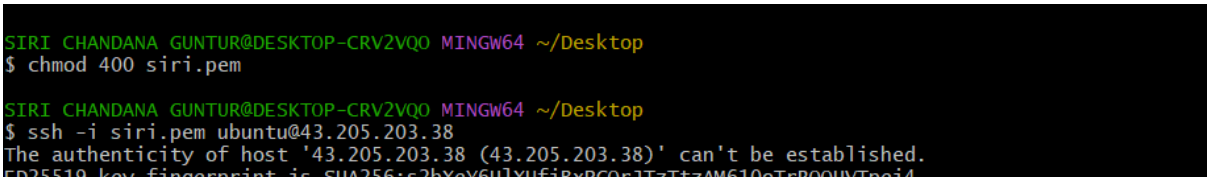
6. Add CIDR  0.0.0.0/0 as destination to NAT instance in route table.



Edit routes

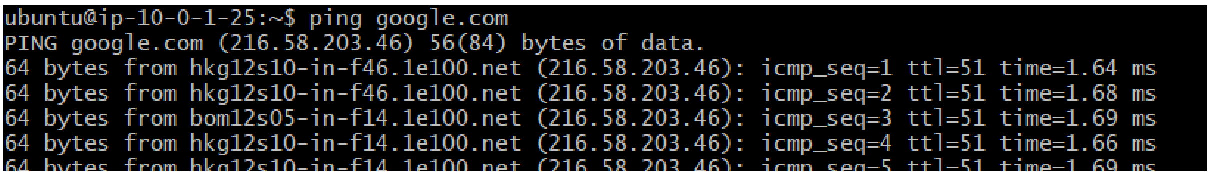
| Destination | Target | Status | Propagated |
|---|---|---|---|
| 10.0.0.0/16 | local | Active | No |
| 0.0.0.0/0 | i-021de4fb8d11daaf6 | - | No |

7. Now firstly connect to public instance using GIT Bash using SSH



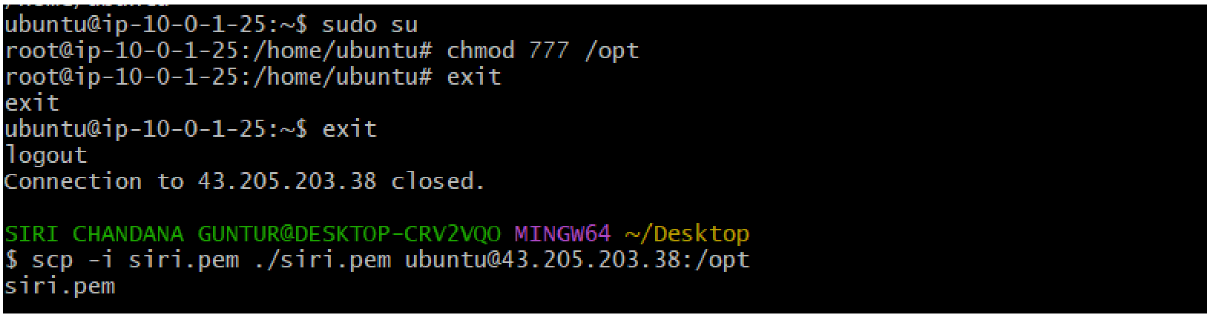
```
SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$ chmod 400 siri.pem

SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$ ssh -i siri.pem ubuntu@43.205.203.38
The authenticity of host '43.205.203.38 (43.205.203.38)' can't be established.
```

Now try to ping any website for ex Google.com to verify internet connectivity.



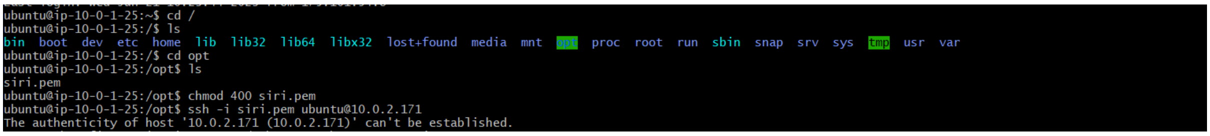
```
ubuntu@ip-10-0-1-25:~$ ping google.com
PING google.com (216.58.203.46) 56(84) bytes of data.
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=1 ttl=51 time=1.64 ms
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=2 ttl=51 time=1.68 ms
64 bytes from bom12s05-in-f14.1e100.net (216.58.203.46): icmp_seq=3 ttl=51 time=1.69 ms
64 bytes from hkg12s10-in-f14.1e100.net (216.58.203.46): icmp_seq=4 ttl=51 time=1.66 ms
64 bytes from hkg12s10-in-f14.1e100.net (216.58.203.46): icmp_seq=5 ttl=51 time=1.69 ms
```

Now enable rwx permissions to a directory in public instance and copy the key pair file onto public instance to connect to Private instance.



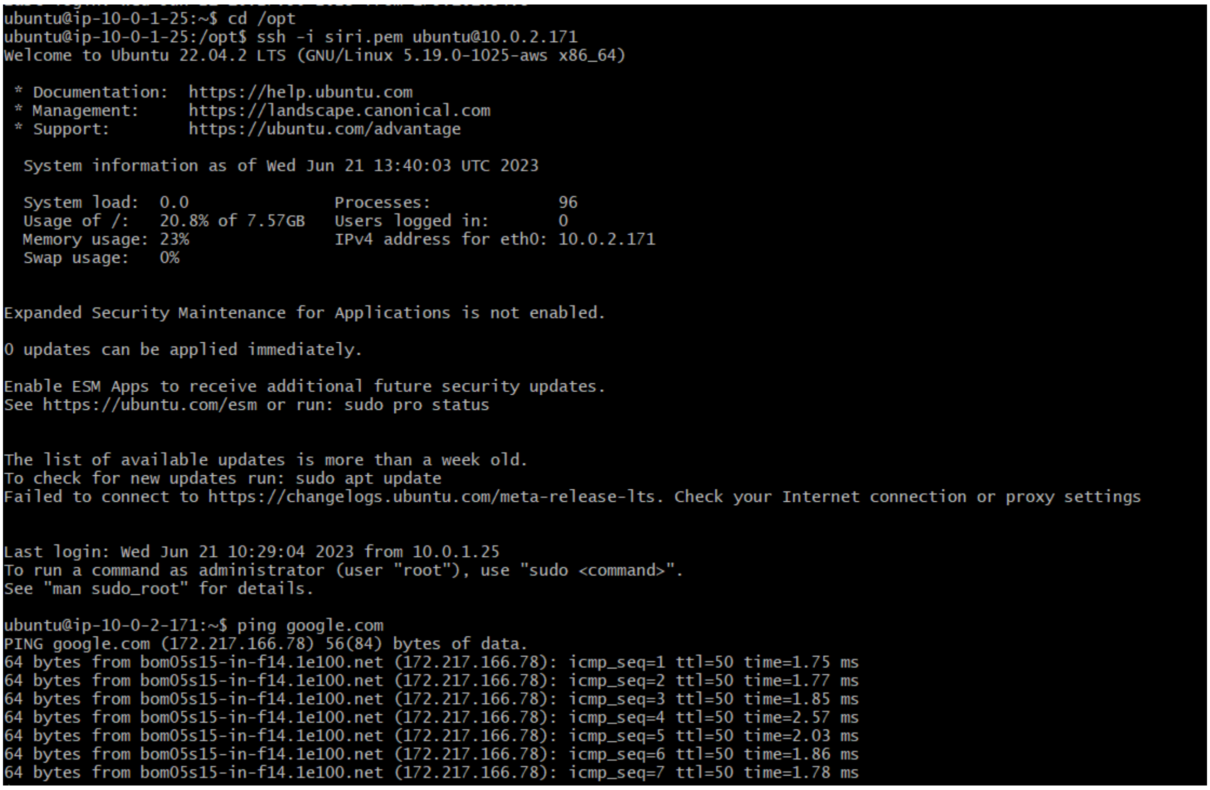
```
ubuntu@ip-10-0-1-25:~$ sudo su
root@ip-10-0-1-25:/home/ubuntu# chmod 777 /opt
root@ip-10-0-1-25:/home/ubuntu# exit
exit
ubuntu@ip-10-0-1-25:~$ exit
logout
Connection to 43.205.203.38 closed.

SIRI CHANDANA GUNTUR@DESKTOP-CRV2VQO MINGW64 ~/Desktop
$ scp -i siri.pem ./siri.pem ubuntu@43.205.203.38:/opt
siri.pem
```

8. Now connect back to public instance and connect to private instance from /opt directory since it has private key file



```
ubuntu@ip-10-0-1-25:~$ cd /
ubuntu@ip-10-0-1-25:/$ ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  snap  srv  sys  tmp  usr  var
ubuntu@ip-10-0-1-25:/$ cd opt
ubuntu@ip-10-0-1-25:/opt$ ls
siri.pem
ubuntu@ip-10-0-1-25:/opt$ chmod 400 siri.pem
ubuntu@ip-10-0-1-25:/opt$ ssh -i siri.pem ubuntu@10.0.2.171
The authenticity of host '10.0.2.171 (10.0.2.171)' can't be established.
```

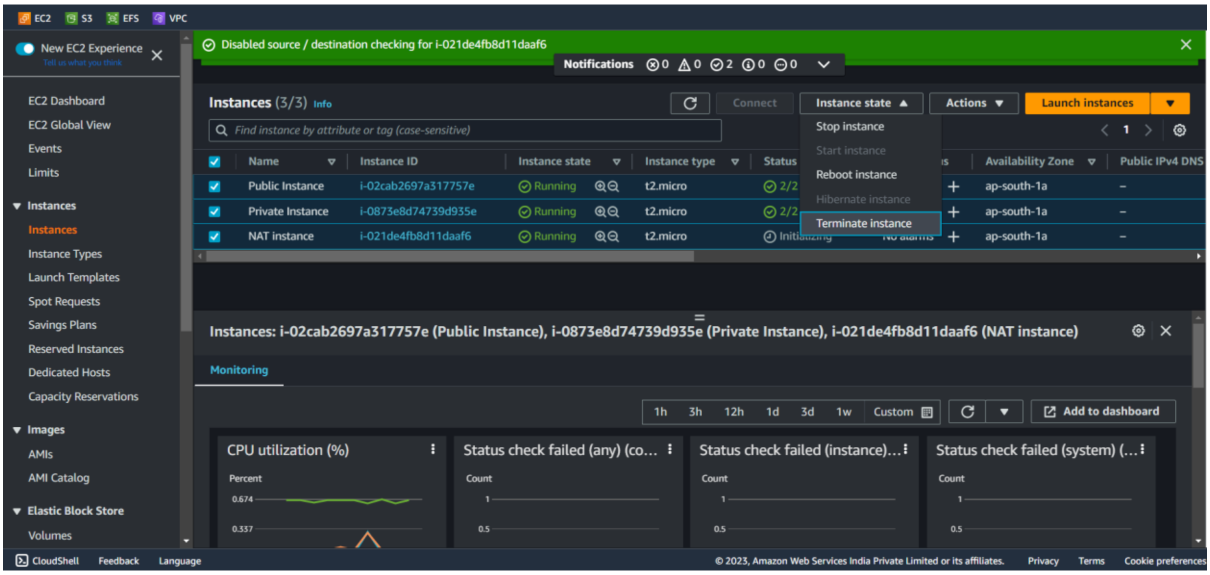
9. Now try to ping google.com from private internet



```
ubuntu@ip-10-0-1-25:~$ cd /opt
ubuntu@ip-10-0-1-25:/opt$ ssh -i siri.pem ubuntu@10.0.2.171
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 13:40:03 UTC 2023

  System load:  0.0               Processes:             96
  Usage of /:   20.8% of 7.57GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for eth0: 10.0.2.171
  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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Jun 21 10:29:04 2023 from 10.0.1.25
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-171:~$ ping google.com
PING google.com (172.217.166.78) 56(84) bytes of data.
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=1 ttl=50 time=1.75 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=2 ttl=50 time=1.77 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=3 ttl=50 time=1.85 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=4 ttl=50 time=2.57 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=5 ttl=50 time=2.03 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=6 ttl=50 time=1.86 ms
64 bytes from bom05s15-in-f14.1e100.net (172.217.166.78): icmp_seq=7 ttl=50 time=1.78 ms
```

## Cleaning up workspace

1. Terminate all the EC2 instances



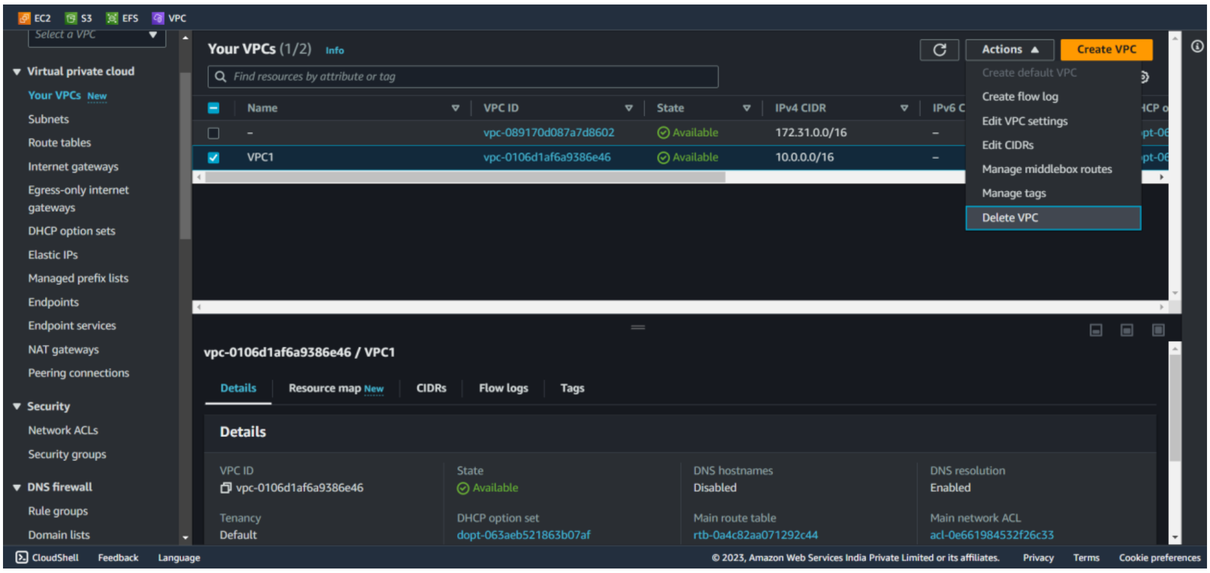
Disabled source / destination checking for i-021de4fb8d11daaf6

Instances (3/3)

| ☑ | Name | Instance ID | Instance state | Instance type | Status | Availability Zone | Public IPv4 DNS |
|---|---|---|---|---|---|---|---|
| ☑ | Public Instance | i-02cab2697a317757e | Running | t2.micro | 2/2 | ap-south-1a | – |
| ☑ | Private Instance | i-0873e8d74739d935e | Running | t2.micro | 2/2 | ap-south-1a | – |
| ☑ | NAT instance | i-021de4fb8d11daaf6 | Running | t2.micro | Initializing | ap-south-1a | – |

Instances: i-02cab2697a317757e (Public Instance), i-0873e8d74739d935e (Private Instance), i-021de4fb8d11daaf6 (NAT instance)

2. Delete the VPC so that all the components regarding the VPC will be deleted.



Your VPCs (1/2) Info

|  | Name | VPC ID | State | IPv4 CIDR | IPv6 C | HCP o |
|---|---|---|---|---|---|---|
| □ | – | vpc-089170d087a7d8602 | Available | 172.31.0.0/16 | – | pt-06 |
| ☑ | VPC1 | vpc-0106d1af6a9386e46 | Available | 10.0.0.0/16 | – | pt-06 |

vpc-0106d1af6a9386e46 / VPC1

Details

VPC ID: vpc-0106d1af6a9386e46

State: Available

DNS hostnames: Disabled

DNS resolution: Enabled

Tenancy: Default

DHCP option set: dopt-063aeb521863b07af

Main route table: rtb-0a4c82aa071292c44

Main network ACL: acl-0e661984532f26c33

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