“A massive industry relevant skill enhancement initiative for the youth of Tamil Nadu.”

Jointly with Veranda edureka!

CLOUD ESSENTIALS PROJECT REPORT

“VIRTUAL PRIVATE CLOUD IN AWS”

Submitted by

SHRUTHI B K - 513120106078

Date

31-10-2022 TO 11-11-2022

THANTHAI PERIYAR

GOVERNMENT INSTITUTE OF TECHNOLOGY

VELLORE – 02.

ACKNOWLEDGEMENT

I feel glad to take this opportunity to cordially thank **Honourable Chief Minister of Tamil Nādu Thiru M K Stalin**, for the implementation of the Naan Mudhalvan Upskilling Platform which benefited the students on a large scale.

I express my sincere thanks to **Tmt.G.LaxmiPriya IAS, Commissioner of Technical Education**, for the execution of this Naan Mudhalvan Upskilling Platform that paved a way for enhancement of the students.

I would like to express my deep sense of gratitude to **respected Principal Dr. M. Arularasu, M.E., Ph.D.,** who bestowed his kind grace and affection on us in completing this course.

I would like to express sincere thanks to **Vice Principal Dr.J.Sreerambabu, M.E., Ph.D., PDF.,** who has provided the great help and support throughout the course.

I would like to express my profound gratitude to our **Head of the Department Dr.Rahila Bilal, M.E., Ph.D.,** for her support and guidance to complete this project.

I would like to express my gratitude to **Institute SPOC Dr.N.Kalaivasan, M.Sc., Ph.D.,** who have been supportive of our career goals and who worked actively to provide me with the protected academic time to pursue those goals.

I extend my gratitude to the **Course Co-Ordinators Mr.K.Thirunavukkarsu, M.E.,** and **Dr.B.Senthil Murugan,M.E.,Ph.D.,** for their continuous support and understanding when undertaking my project.

I sincerely thank all the faculty members for providing necessary support for the course.

Index Page

INTRODUCTION

As a part of the Cloud Essentials course that I was enrolled, this project is done on the topic of Virtual Private Cloud (VPCs). Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet).Cloud Computing provides an alternative to the on-premises datacentre. With an on-premises datacentre, we have to manage everything, such as purchasing and installing hardware, virtualization, installing the operating system, and any other required applications, setting up the network, configuring the firewall, and setting up storage for data. After doing all the set-up, we become responsible for maintaining it through its entire lifecycle. But if we choose Cloud Computing, a cloud vendor is responsible for the hardware purchase and maintenance. They also provide a wide variety of software and platform as a service. We can take any required services on rent. The cloud computing services will be charged based on usage. In this project, a VPC is created in order to have flexible control over the cloud resources. A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider. (Not all private clouds are hosted in this fashion.) VPCs combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing. Imagine a public cloud as a crowded restaurant, and a virtual private cloud as a reserved table in that crowded restaurant. Even though the restaurant is full of people, a table with a "Reserved" sign on it can only be accessed by the party who made the reservation. Similarly, a public cloud is crowded with various cloud customers accessing computing resources – but a VPC reserves some of those resources for use by only one customer.

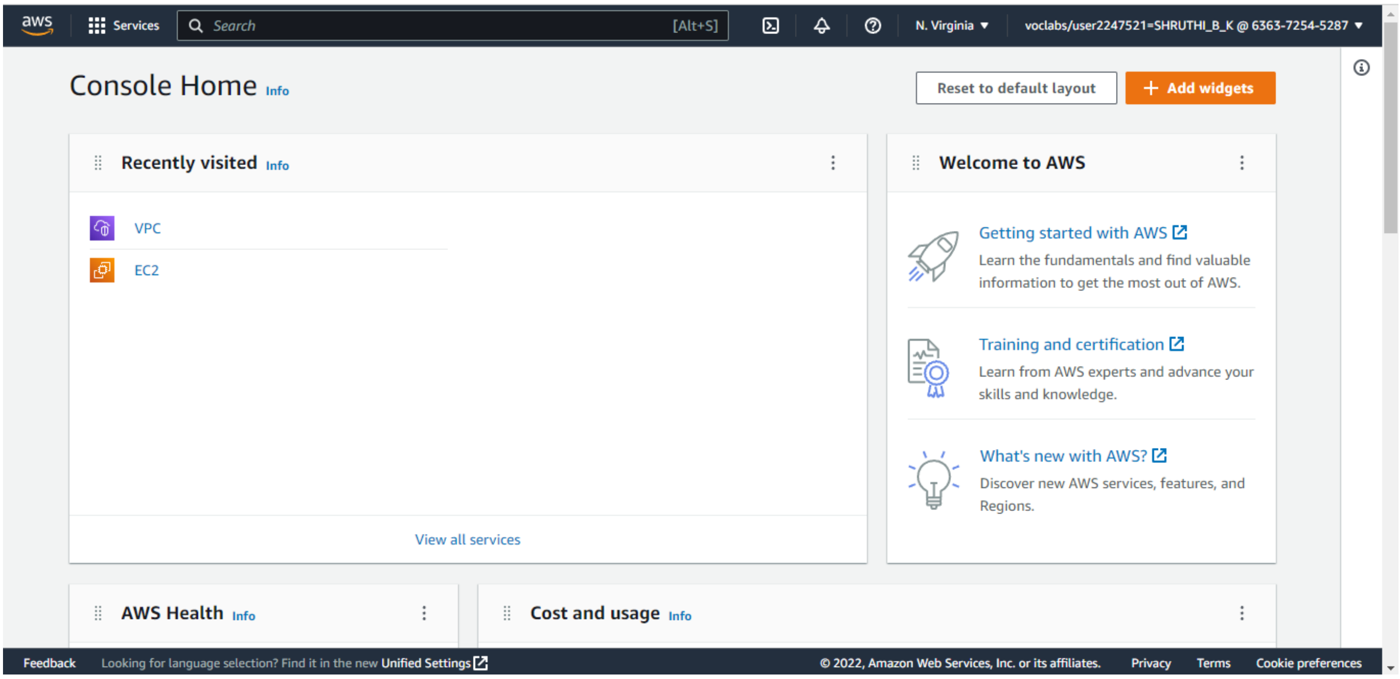
Problem Statement:

John is a newbie to the cloud computing domain; he is exploring AWS and is comfortable with creating most of the AWS services. However, he struggles in creating a Virtual Private Cloud (VPC) using the console in the AWS platform. He would need you to assist him in creating a Virtual Private Cloud. While creating a VPC make sure that you:

- Create an Amazon VPC using the VPC wizard, and it should be displayed on the dashboard
- Associate an Elastic IP address with it
- Explore various resources of VPC such as Internet Gateway, NAT Gateway, Subnets, Security Groups
- Launch a NAT Gateway so that internet access is provided to private resources
- Introduce a Public subnet for resources facing the internet such as a web server and a private subnet for resources at the back end such as database server
- Define security groups with appropriate inbound rules
- Ensure proper routes and corresponding Route tables entries specifying the traffic moving out of the subnet
- Make use of Network ACLs for controlling inbound and outbound traffic in the VPC

1. Creating an Amazon VPC using the VPC wizard:

- Login to the AWS Management Console and navigate to VPC from Services menu.



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

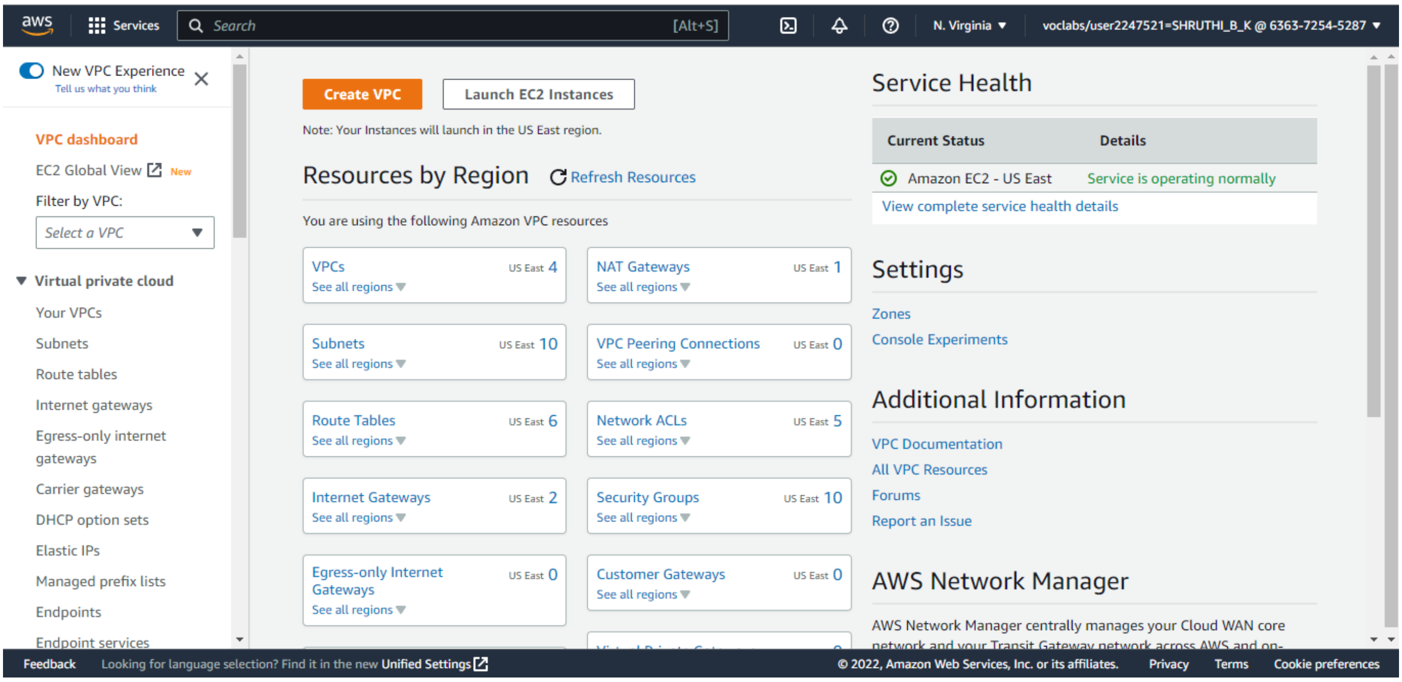
Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

- On the VPC Dashboard, choose Launch VPC Wizard.



Note: Your Instances will launch in the US East region.

You are using the following Amazon VPC resources

VPCs See all regions	US East 4	NAT Gateways See all regions	US East 1
Subnets See all regions	US East 10	VPC Peering Connections See all regions	US East 0
Route Tables See all regions	US East 6	Network ACLs See all regions	US East 5
Internet Gateways See all regions	US East 2	Security Groups See all regions	US East 10
Egress-only Internet Gateways See all regions	US East 0	Customer Gateways See all regions	US East 0

Current Status	Details
Amazon EC2 - US East	Service is operating normally

View complete service health details

AWS Network Manager centrally manages your Cloud WAN core network and your Transit Gateway network across AWS and on-

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

- Under Step 1: Select a VPC Configuration, on VPC with a Single Public Subnet, choose Select.

- Enter the following information into the wizard and choose Create VPC.

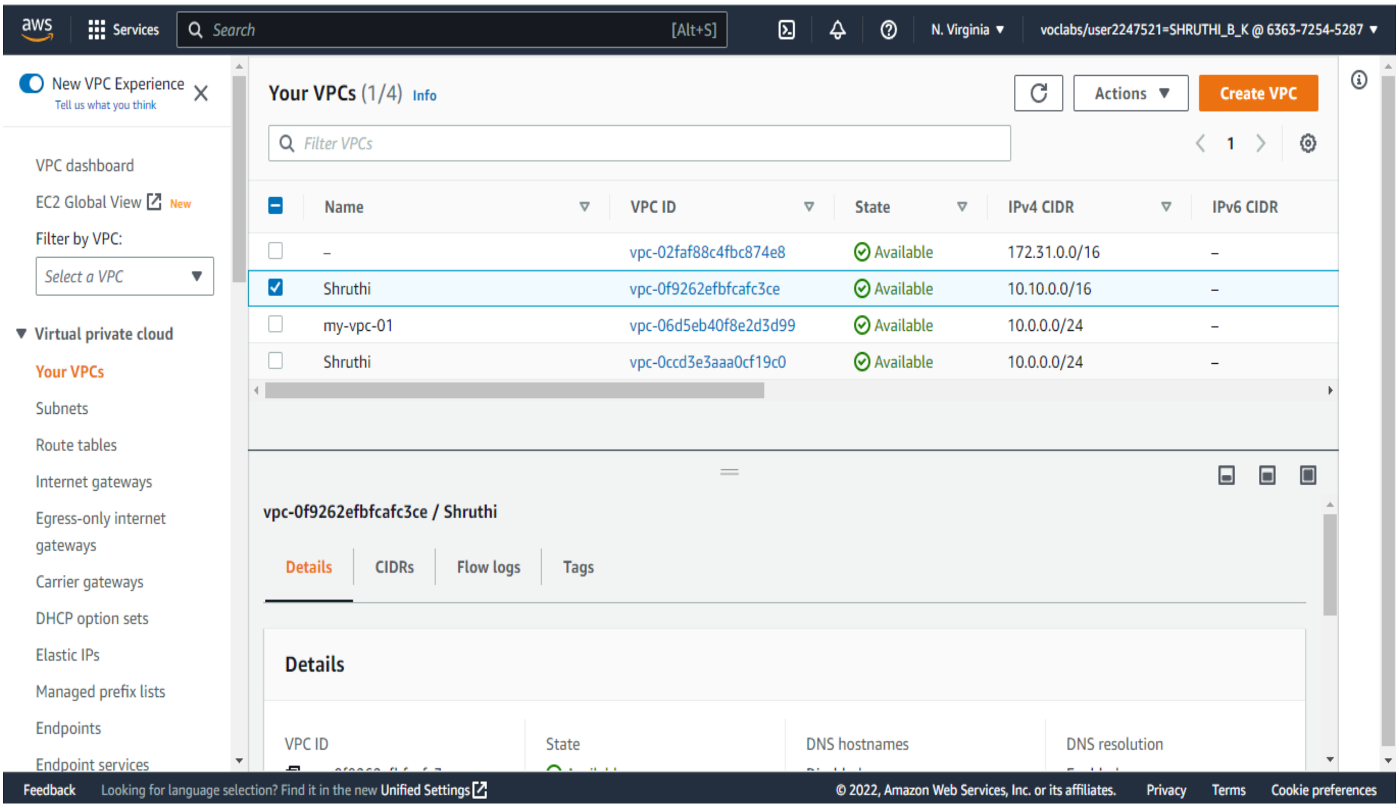
  IP CIDR block - 10.10.0.0/16

  VPC name – Shruthi

  Public subnet - 10.10.0.0/24

  Hardware tenancy – Default

- Now, a VPC is created and it is visible in the dashboard.



Your VPCs (1/4) Info

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
□	–	vpc-02faf88c4fbc874e8	✓ Available	172.31.0.0/16	–
☑	Shruthi	vpc-0f9262efbfcafc3ce	✓ Available	10.10.0.0/16	–
□	my-vpc-01	vpc-06d5eb40f8e2d3d99	✓ Available	10.0.0.0/24	–
□	Shruthi	vpc-0ccd3e3aaa0cf19c0	✓ Available	10.0.0.0/24	–

vpc-0f9262efbfcafc3ce / Shruthi

Details

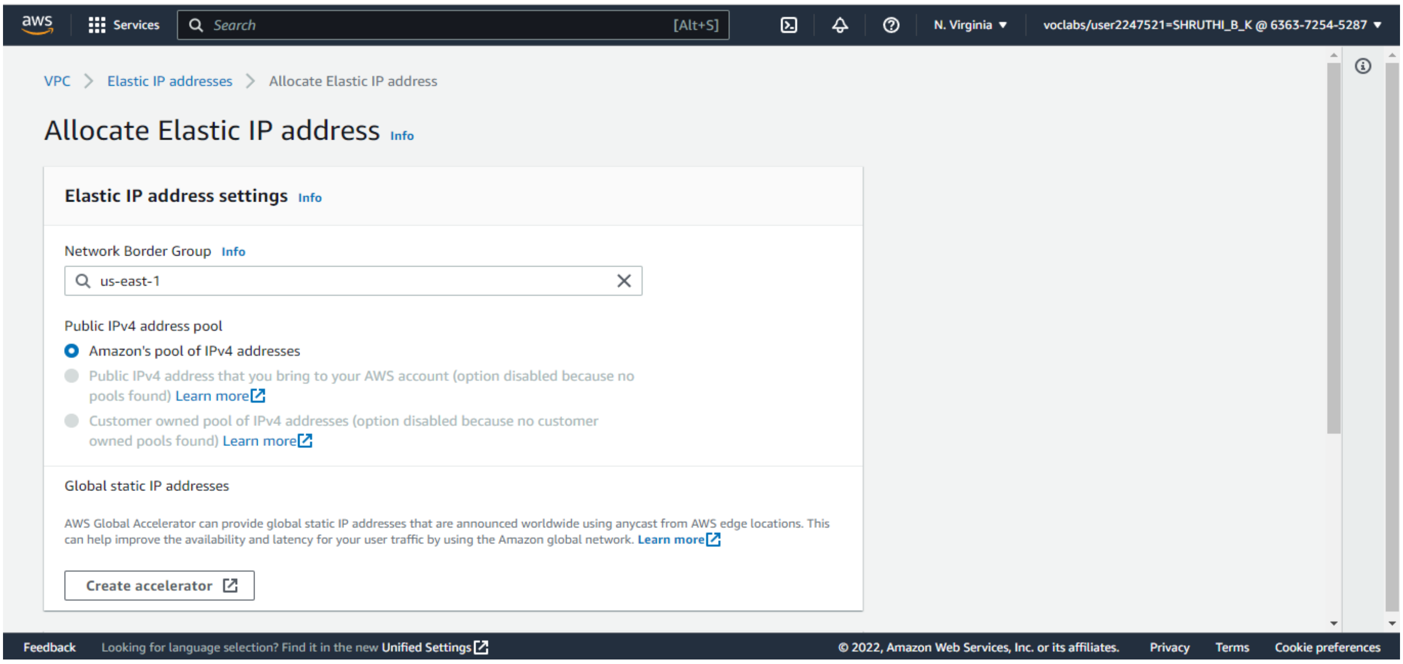
VPC ID | State | DNS hostnames | DNS resolution

2. Associate an Elastic IP address with it:

Before allocating and associating an elastic IP, An Internet Gateway should be created and attached with the VPC. An Internet Gateway can be simply created by Internet Gateway section and can be associated with the created VPC.

Step 1: Allocate an Elastic IP.

- In the Elastic IP section, choose allocate Elastic IP.
- Select network border group and amazon's pool of ipv4.


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2247521=SHRUTHI_B_K @ 6363-7254-5287
VPC > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address Info

Elastic IP address settings Info

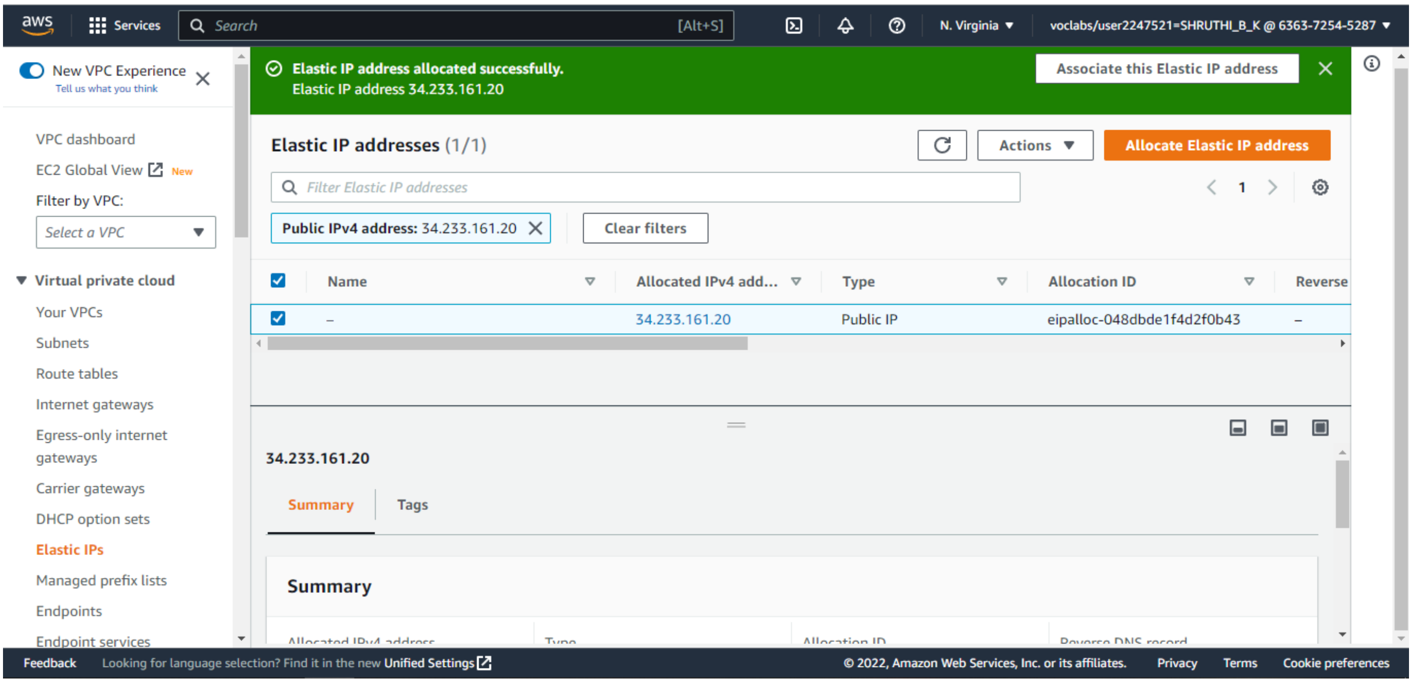
Network Border Group Info: us-east-1

Public IPv4 address pool
- ● Amazon's pool of IPv4 addresses
- ○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more
- ○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Create accelerator
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Elastic IP address allocated successfully.
Elastic IP address 34.233.161.20

Elastic IP addresses (1/1)

Public IPv4 address: 34.233.161.20

☑	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse
☑	–	34.233.161.20	Public IP	eipalloc-048dbde1f4d2f0b43	–

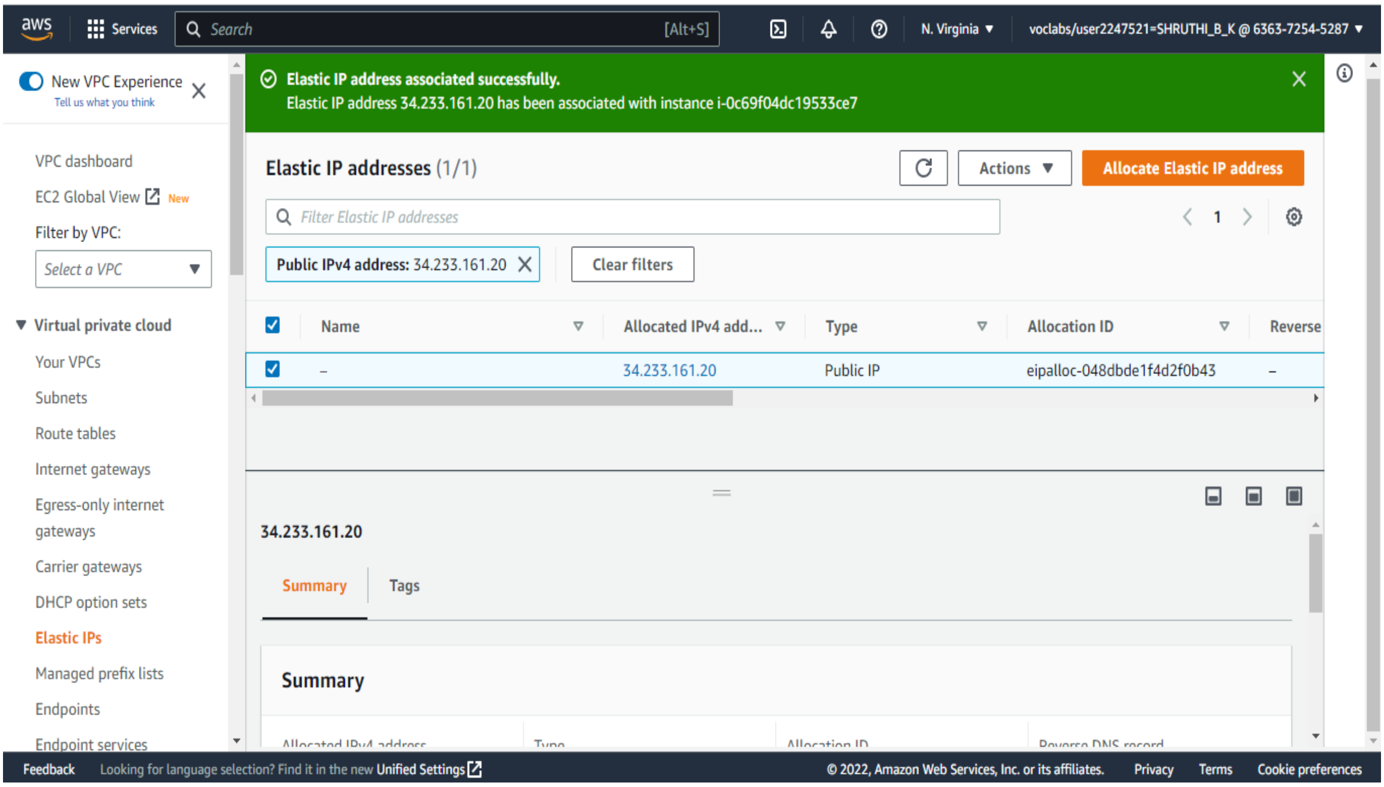
34.233.161.20

Summary

Allocated IPv4 address | Type | Allocation ID | Reverse DNS record

Step 2: Associate the elastic IP with the VPC

- ➢ Create an instance within the VPC.
- ➢ Now select the allocated Elastic IP and Actions> Associate Elastic IP and select the newly created instance.



Elastic IP address associated successfully.
Elastic IP address 34.233.161.20 has been associated with instance i-0c69f04dc19533ce7

Elastic IP addresses (1/1)

Public IPv4 address: 34.233.161.20

☑	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse
☑	–	34.233.161.20	Public IP	eipalloc-048dbde1f4d2f0b43	–

34.233.161.20

Summary

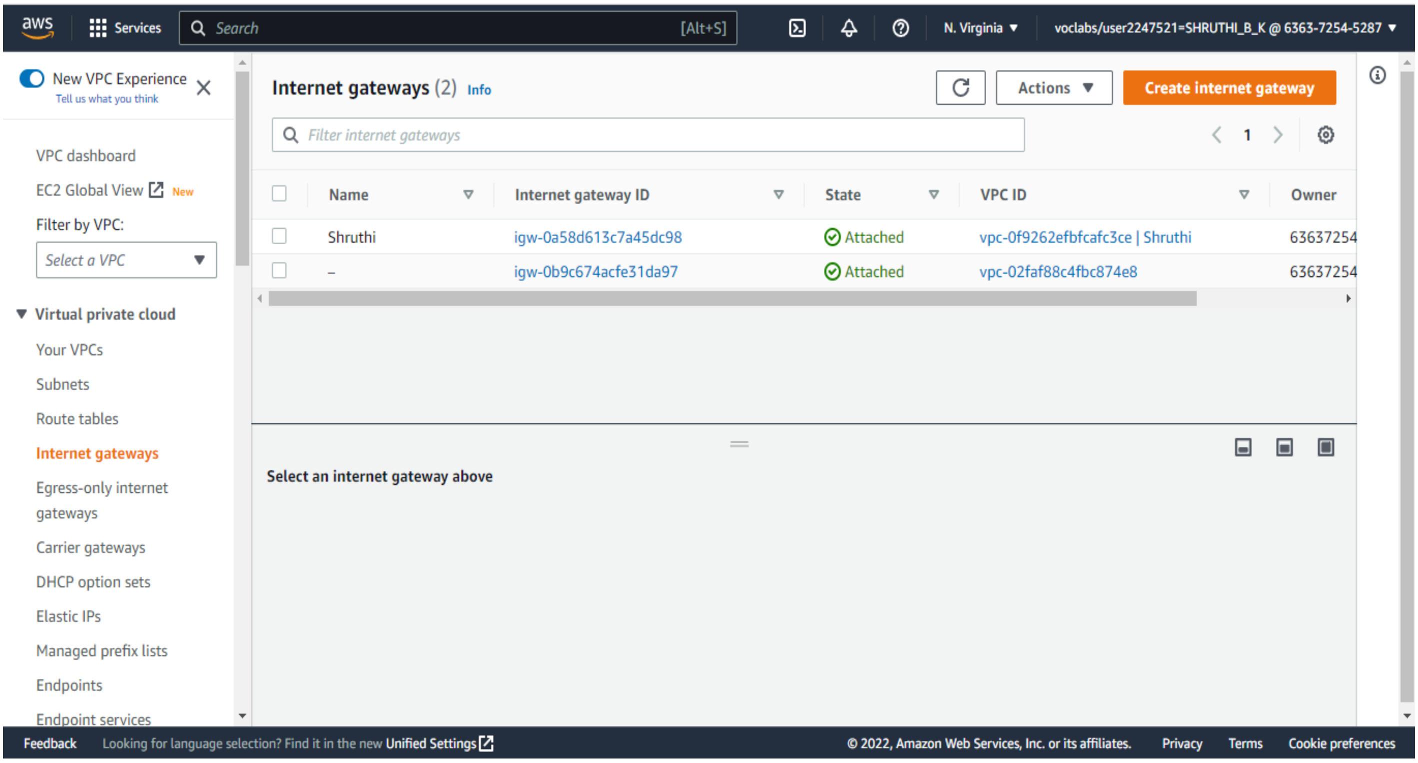
Allocated IPv4 address | Type | Allocation ID | Reverse DNS record

Now, we have successfully created a VPC, an Internet Gateway, an Instance within the VPC and Associated an Elastic IP with the Instance.

3. Explore various resources of VPC such as Internet Gateway, NAT Gateway, Subnets, Security Groups:

1. Internet gateways:

- ➢ In the navigation panel, choose Internet Gateways.
- ➢ Choose “Create Internet Gateways”.
- ➢ Optionally name your internet gateway.
- ➢ Optionally add or remove a tag.
- ➢ [Add a tag] Choose Add tag and do the following:
- ➢ For Key, enter the key name.
- ➢ For Value, enter the key value.
- ➢ [Remove a tag] Choose Remove to the right of the tag’s Key and Value.
- ➢ Choose Create internet gateway.
- ➢ Select the internet gateway that you just created, and then choose Actions, Attach to VPC.



Internet gateways (2) Info

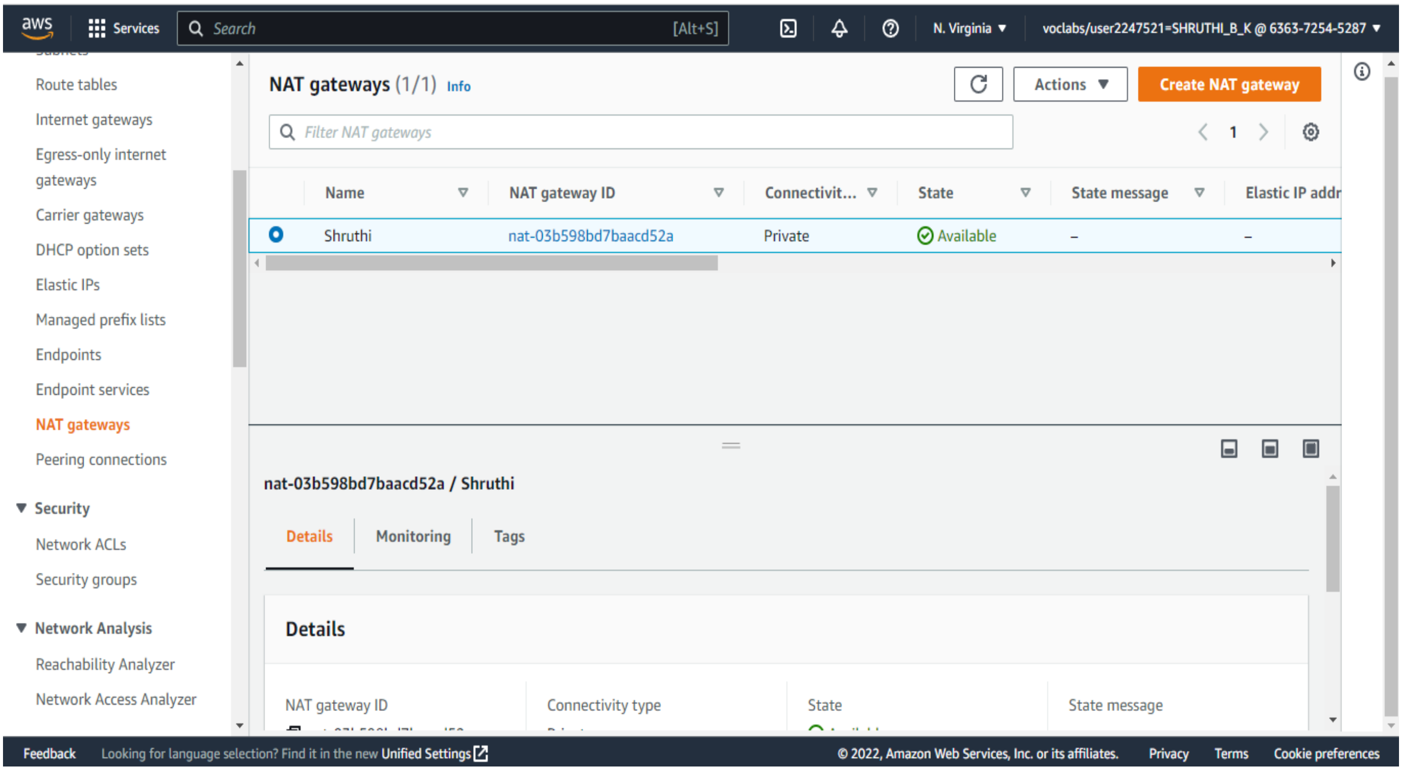
□	Name	Internet gateway ID	State	VPC ID	Owner
□	Shruthi	igw-0a58d613c7a45dc98	✓ Attached	vpc-0f9262efbfcafc3ce | Shruthi	63637254
□	–	igw-0b9c674acfe31da97	✓ Attached	vpc-02faf88c4fbc874e8	63637254

Select an internet gateway above

2. NAT Gateway:

- ➢ In the navigation panel, choose NAT Gateways.
- ➢ Choose Create NAT Gateway and do the following:
  - (Optional) Specify a name for the NAT gateway. This creates a tag where the key is Name and the value is the name that you specify.
  - Select the subnet in which to create the NAT gateway.
  - For Connectivity type, select Private to create a private NAT gateway or Public (the default) to create a public NAT gateway.
  - (Public NAT gateway only) For Elastic IP allocation ID, select an Elastic IP address to associate with the NAT gateway.
  - (Optional) For each tag, choose Add new tag and enter the key name and value.
  - Choose Create a NAT Gateway.

- The initial status of the NAT gateway is Pending. After the status changes to Available, the NAT gateway is ready for you to use. Be sure to update your route tables as needed.



NAT gateways (1/1)

	Name	NAT gateway ID	Connectivit...	State	State message	Elastic IP addr
●	Shruthi	nat-03b598bd7baacd52a	Private	Available	–	–

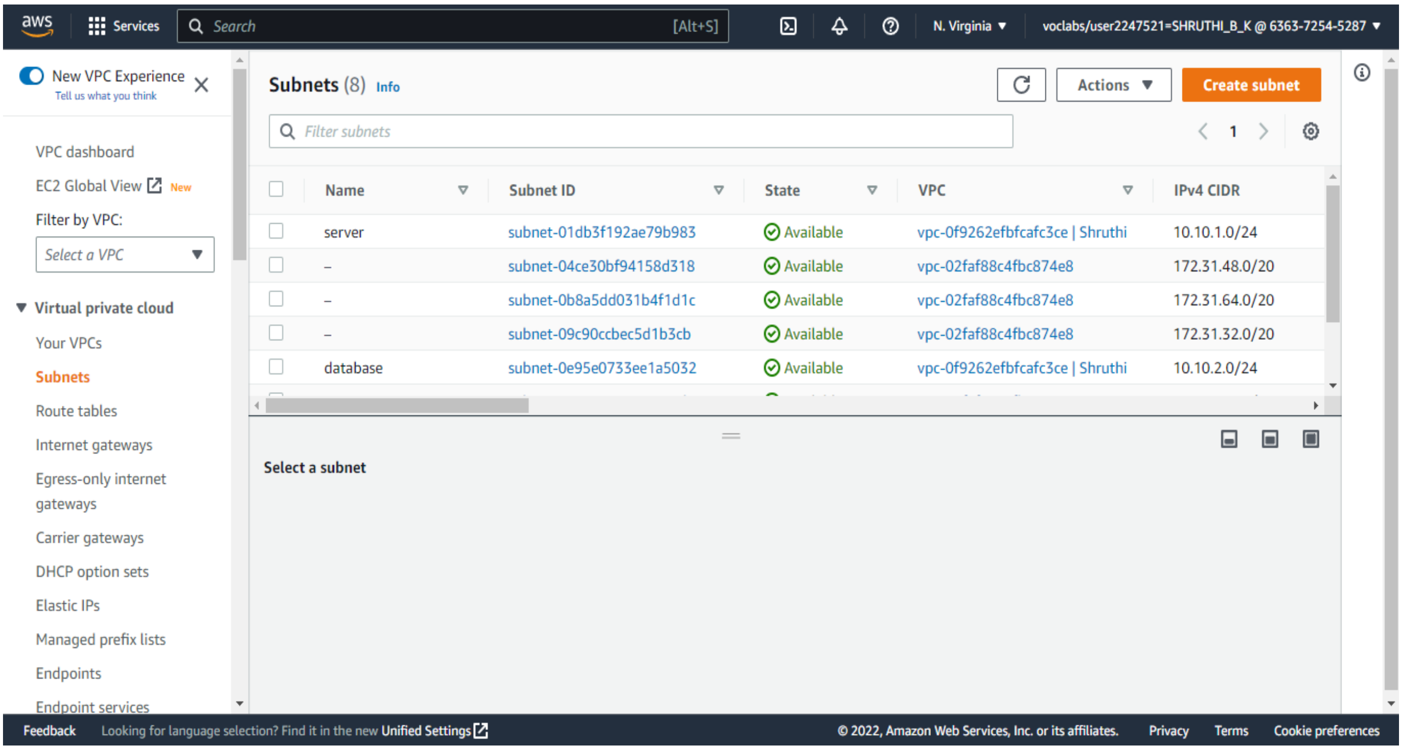
nat-03b598bd7baacd52a / Shruthi

Details

NAT gateway ID	Connectivity type	State	State message

3. Subnets:

- In the navigation panel, choose Subnets.
- Choose ‘Create Subnet’.
- Enter the information in VPC and subnet settings.
- Then at last click “Create Subnet”.
- By above steps create two subnets for server and database separately.



Subnets (8)

Name	Subnet ID	State	VPC	IPv4 CIDR
server	subnet-01db3f192ae79b983	Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.1.0/24
–	subnet-04ce30bf94158d318	Available	vpc-02faf88c4fbc874e8	172.31.48.0/20
–	subnet-0b8a5dd031b4f1d1c	Available	vpc-02faf88c4fbc874e8	172.31.64.0/20
–	subnet-09c90ccbec5d1b3cb	Available	vpc-02faf88c4fbc874e8	172.31.32.0/20
database	subnet-0e95e0733ee1a5032	Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.2.0/24

Select a subnet

4. Security groups:

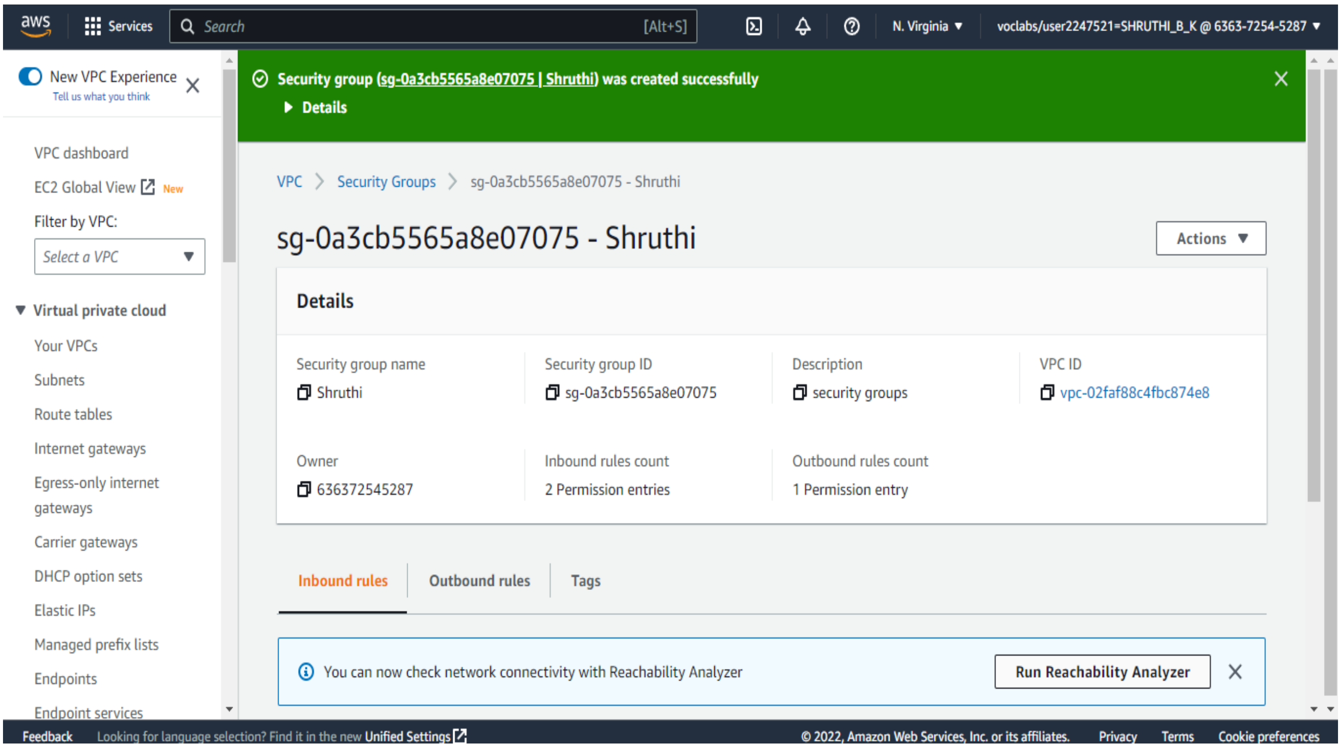
- ➢ In the navigation panel, choose Security group from Security.
- ➢ Choose “Create security group”.
- ➢ Give Basic Details and add inbound and outbound rules.

  Basic Details:

  Security group name- Shruthi

  Description- Security groups

  VPC- vpc-02faf88c4fbc874e8
- ➢ Now click on Create Security groups.


Security group (sg-0a3cb5565a8e07075 | Shruthi) was created successfully

VPC > Security Groups > sg-0a3cb5565a8e07075 - Shruthi

sg-0a3cb5565a8e07075 - Shruthi

Details

Security group name	Security group ID	Description	VPC ID
Shruthi	sg-0a3cb5565a8e07075	security groups	vpc-02faf88c4fbc874e8

Owner	Inbound rules count	Outbound rules count
636372545287	2 Permission entries	1 Permission entry

You can now check network connectivity with Reachability Analyzer

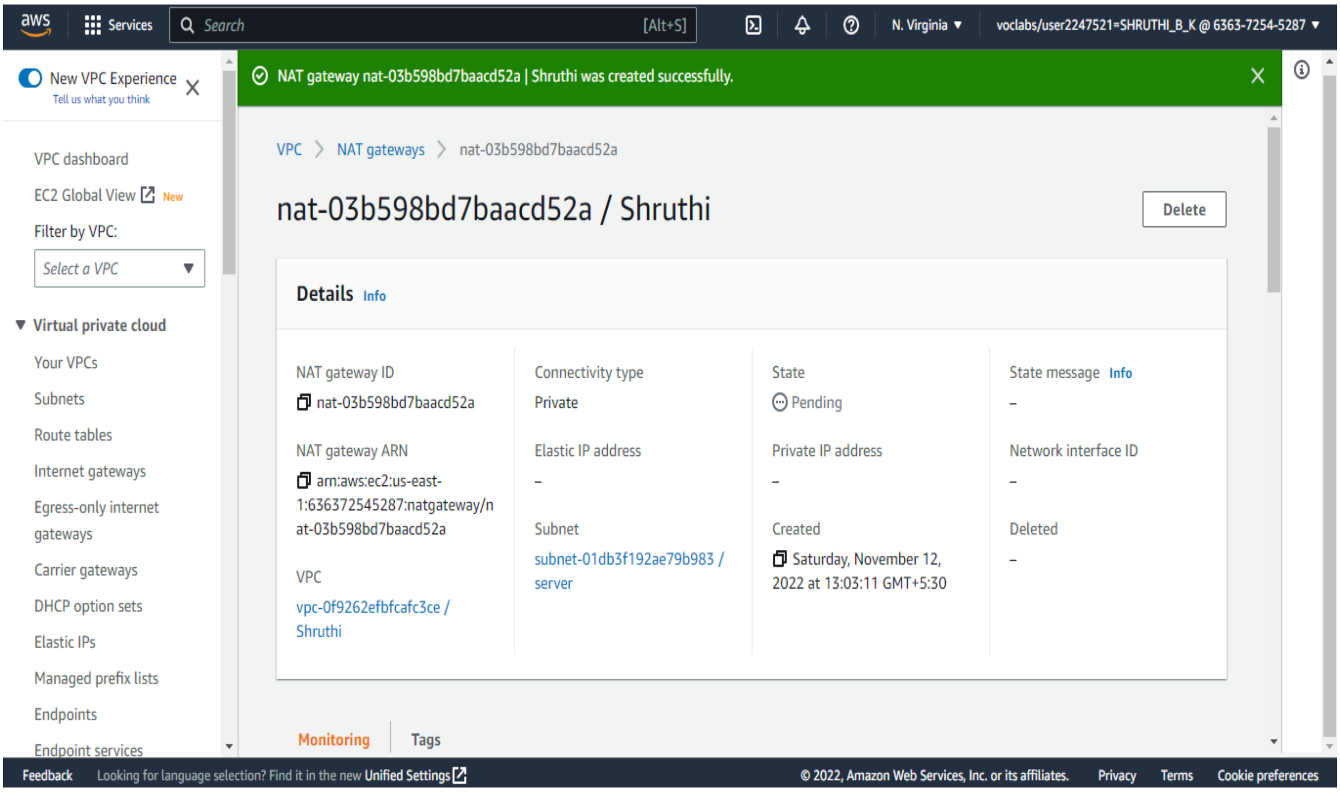
4. NAT Gateway is launched so that internet access is provided to private resources:

- Choose NAT Gateway from the navigation panel.
- Click on “Create NAT Gateway”.
- Give the appropriate information in the settings:

  Name- Shruthi

  Subnet- server

  Connectivity type- Public
- Select the appropriate elastic Ip and allocate it.
- Now, the NAT Gateway is successfully created.



NAT gateway nat-03b598bd7baacd52a | Shruthi was created successfully.

VPC > NAT gateways > nat-03b598bd7baacd52a

nat-03b598bd7baacd52a / Shruthi

Details Info

NAT gateway ID: nat-03b598bd7baacd52a

NAT gateway ARN: arn:aws:ec2:us-east-1:636372545287:natgateway/nat-03b598bd7baacd52a

VPC: vpc-0f9262efbfcafc3ce / Shruthi

Connectivity type: Private

Elastic IP address: -

Subnet: subnet-01db3f192ae79b983 / server

State: Pending

Private IP address: -

Created: Saturday, November 12, 2022 at 13:03:11 GMT+5:30

State message Info: -

Network interface ID: -

Deleted: -

5. Public subnet for resources facing the internet such as web server and a private subnet for resources at the back end such as database server:

- Choose Subnet from navigation panel.
- Click on “Create subnet”.

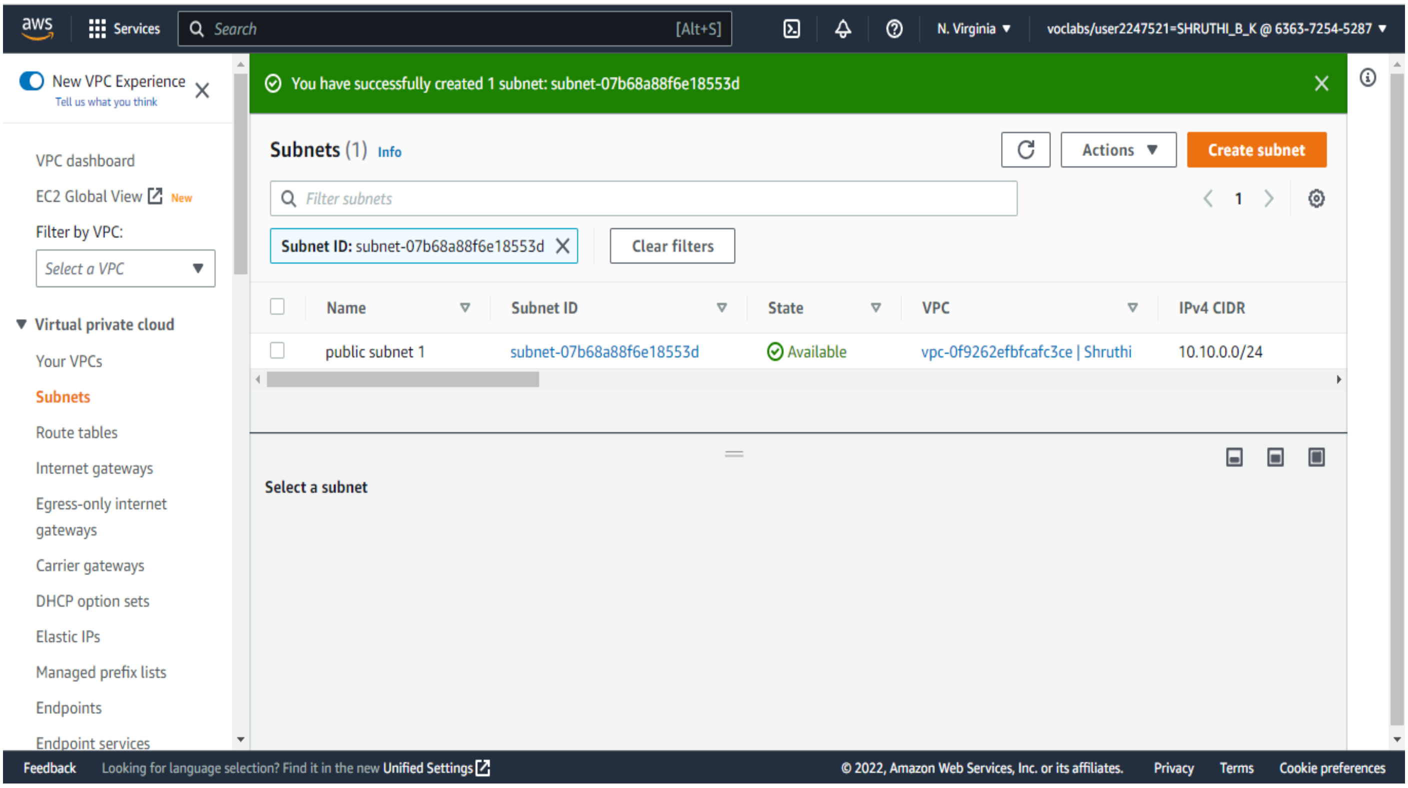
- ➢ Choose the appropriate VPC id, that was already created.
- ➢ Then give the following information:

  Subnet name- Public Subnet

  Availability zone- 1st option

  Ipv4 CIDR id-10.10.0.0/24

- ➢ Click on “Create subnet”.



You have successfully created 1 subnet: subnet-07b68a88f6e18553d

Subnets (1) Info

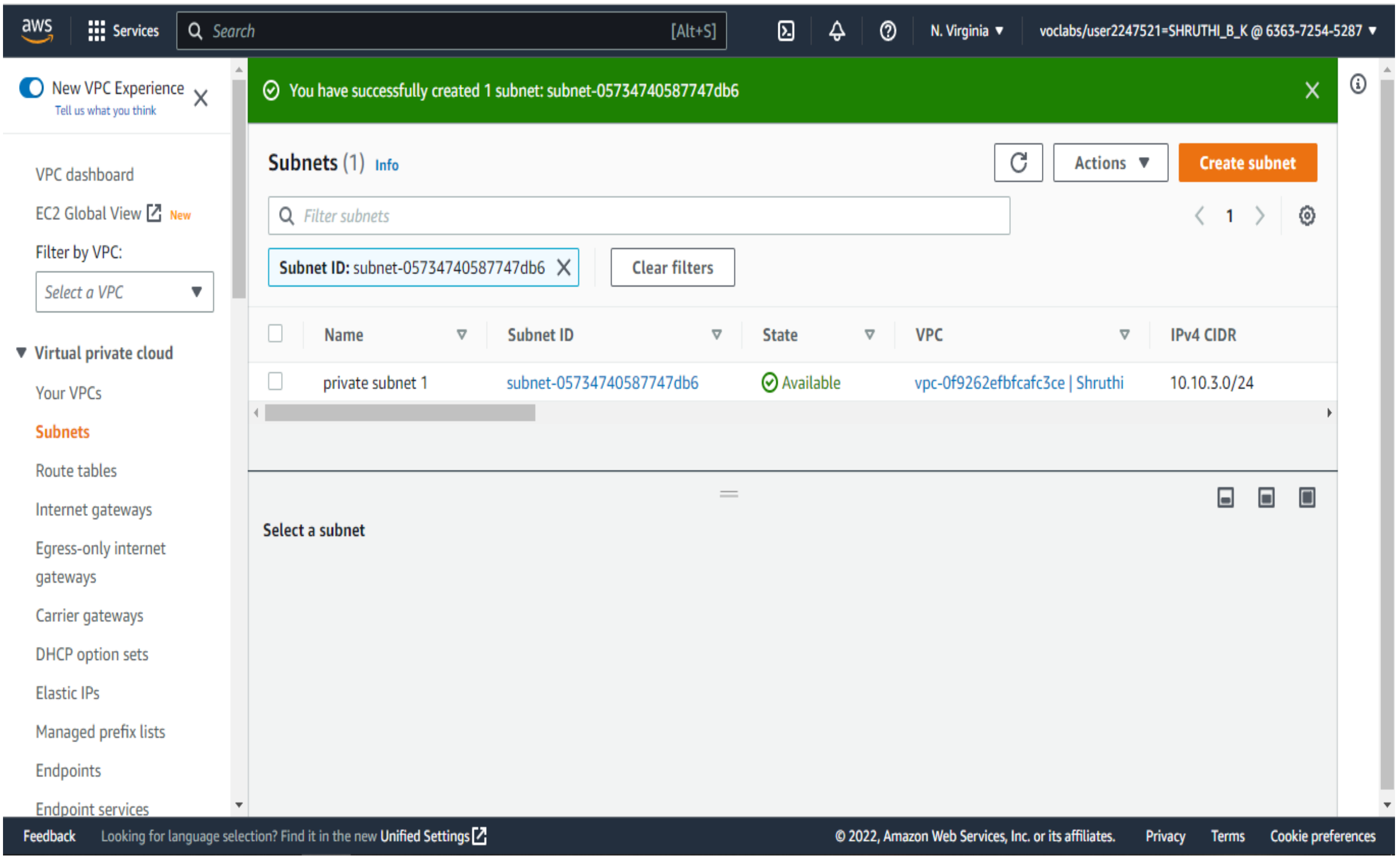
Subnet ID: subnet-07b68a88f6e18553d

	Name	Subnet ID	State	VPC	IPv4 CIDR
□	public subnet 1	subnet-07b68a88f6e18553d	Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.0.0/24

- ➢ Similarly, follow the same steps for creating Public subnet.

  Here, Availability zone- 2nd option

  Ipv4 CIDR id- 10.10.3.0/24



You have successfully created 1 subnet: subnet-05734740587747db6

Subnets (1) Info

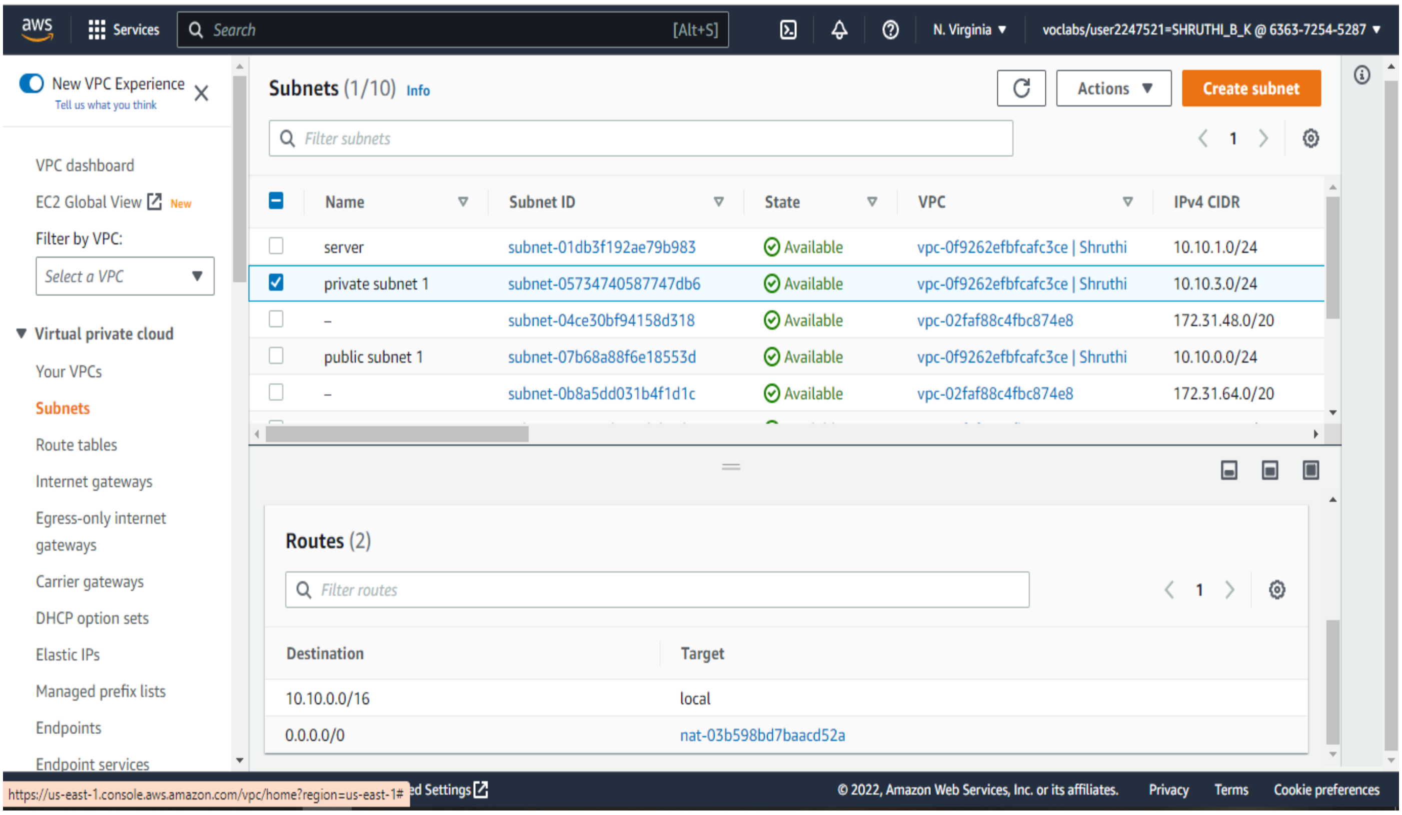
Filter subnets

Subnet ID: subnet-05734740587747db6

□	Name	Subnet ID	State	VPC	IPv4 CIDR
□	private subnet 1	subnet-05734740587747db6	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.3.0/24

Select a subnet

The difference between the public and private subnet is the target, for private subnet it is NAT Gateway and for public it is Internet Gateway.



Subnets (1/10) Info

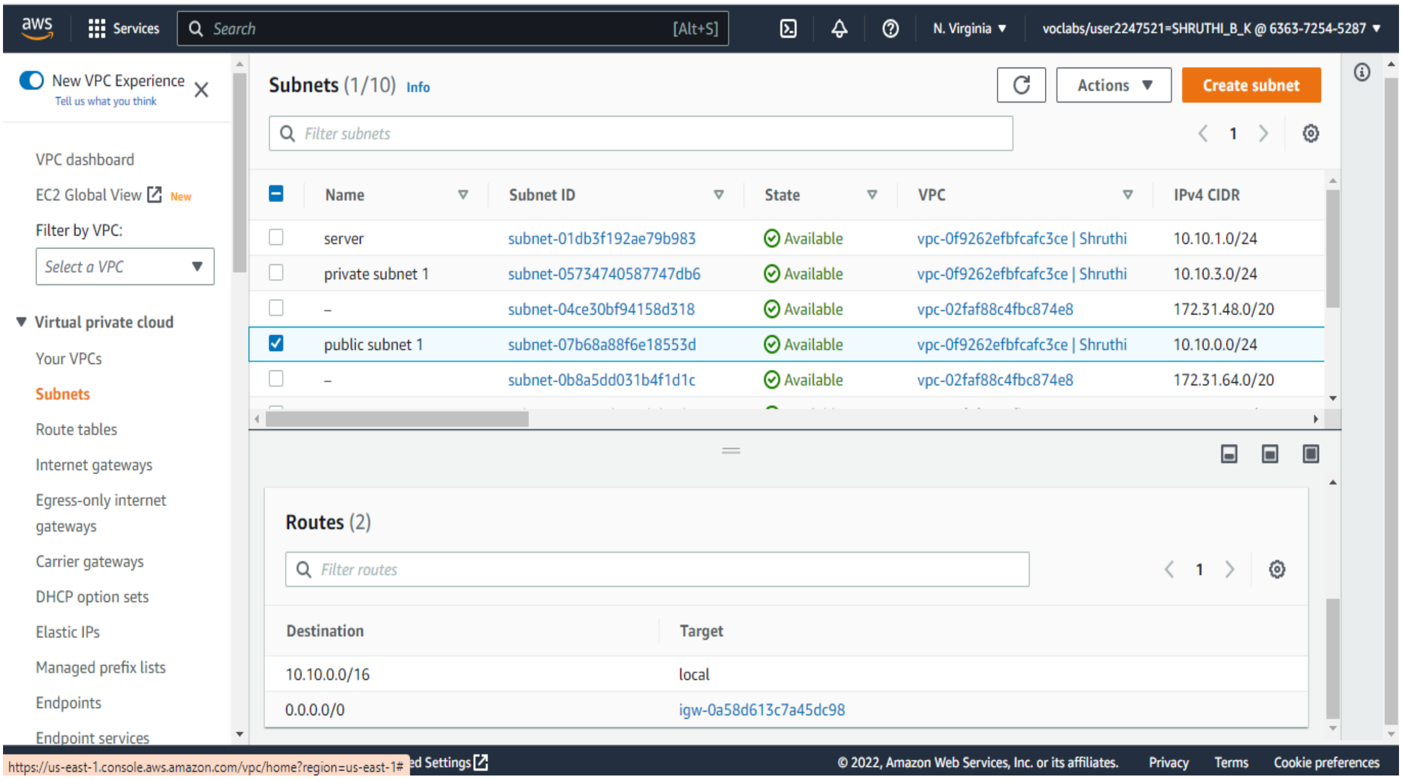
Filter subnets

☐	Name	Subnet ID	State	VPC	IPv4 CIDR
□	server	subnet-01db3f192ae79b983	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.1.0/24
☑	private subnet 1	subnet-05734740587747db6	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.3.0/24
□	–	subnet-04ce30bf94158d318	✓ Available	vpc-02faf88c4fbc874e8	172.31.48.0/20
□	public subnet 1	subnet-07b68a88f6e18553d	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.0.0/24
□	–	subnet-0b8a5dd031b4f1d1c	✓ Available	vpc-02faf88c4fbc874e8	172.31.64.0/20

Routes (2)

Filter routes

Destination	Target
10.10.0.0/16	local
0.0.0.0/0	nat-03b598bd7baacd52a



Subnets (1/10) Info

	Name	Subnet ID	State	VPC	IPv4 CIDR
□	server	subnet-01db3f192ae79b983	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.1.0/24
□	private subnet 1	subnet-05734740587747db6	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.3.0/24
□	–	subnet-04ce30bf94158d318	✓ Available	vpc-02faf88c4fbc874e8	172.31.48.0/20
☑	public subnet 1	subnet-07b68a88f6e18553d	✓ Available	vpc-0f9262efbfcafc3ce | Shruthi	10.10.0.0/24
□	–	subnet-0b8a5dd031b4f1d1c	✓ Available	vpc-02faf88c4fbc874e8	172.31.64.0/20

Routes (2)

Destination	Target
10.10.0.0/16	local
0.0.0.0/0	igw-0a58d613c7a45dc98

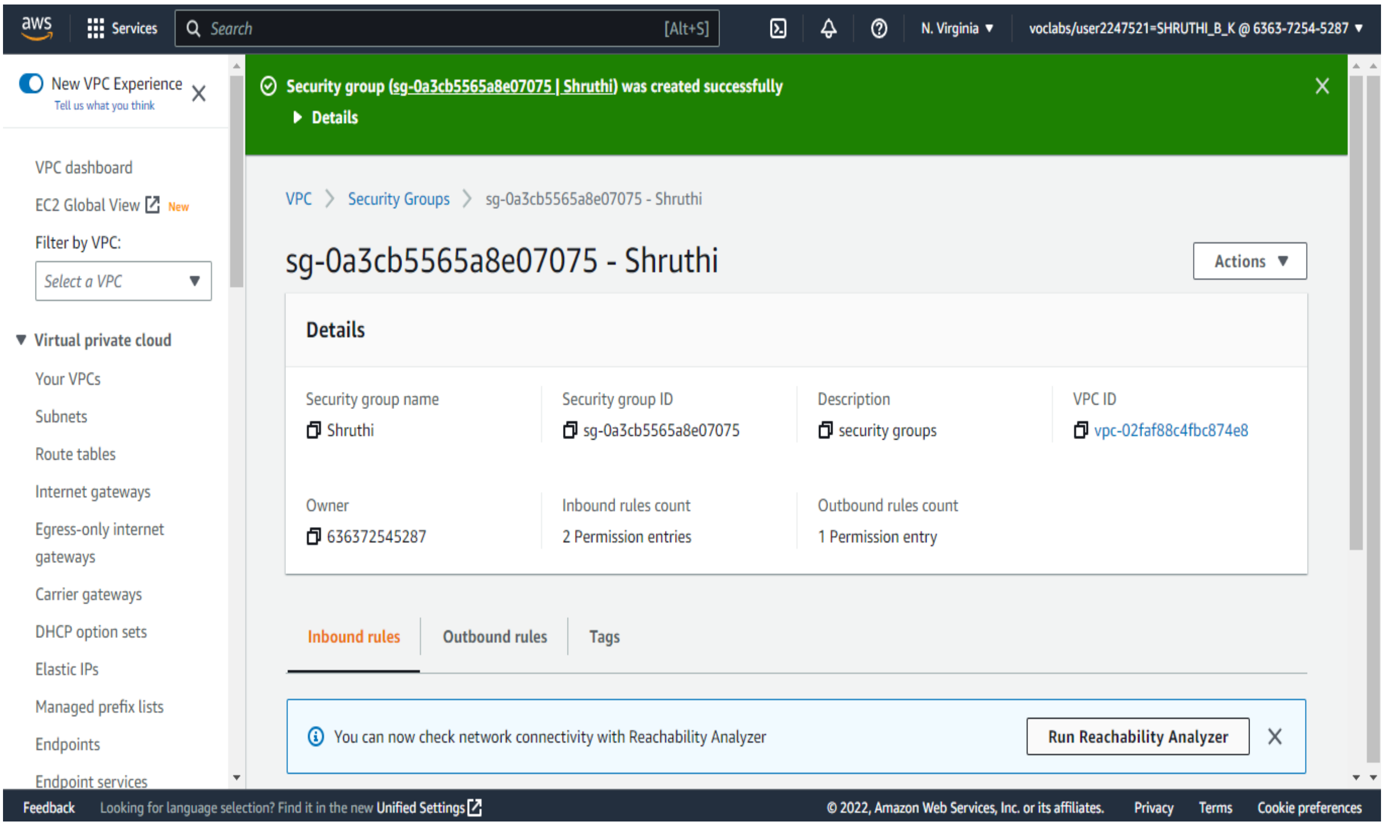
6. Security groups with appropriate inbound rules:

- In the navigation panel, choose Security group from Security.
- Choose "Create security group".
- Basic Details:

  Security group name- Shruthi

  Description- Security groups

  VPC- vpc-02faf88c4fbc874e8
- In the Inbound rules section, click on add rule and choose type as SSH, for source choose "Anywhere-Ipv4", and leave other options as default.
- Now click on Create Security groups.



Security group (sg-0a3cb5565a8e07075 | Shruthi) was created successfully

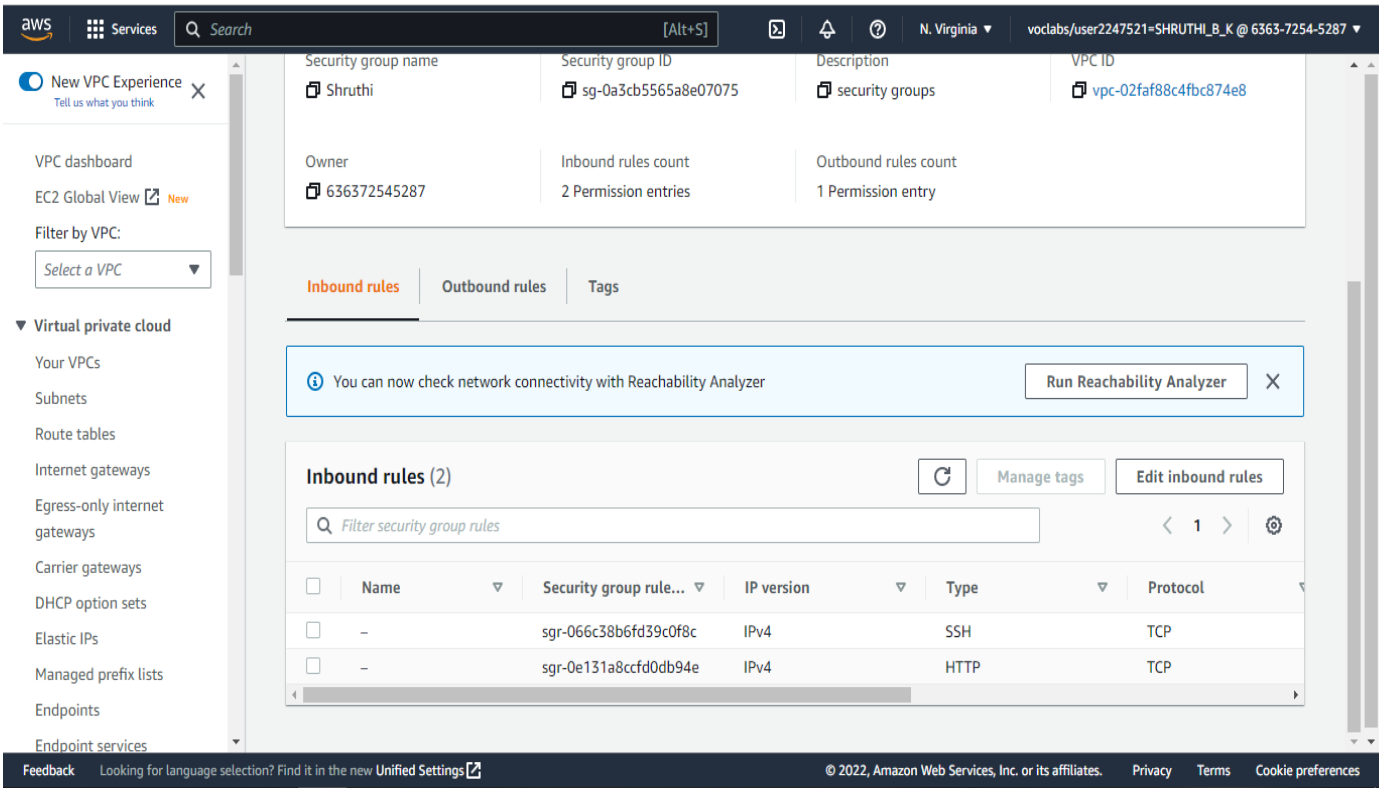
VPC > Security Groups > sg-0a3cb5565a8e07075 - Shruthi

sg-0a3cb5565a8e07075 - Shruthi

Details

Security group name	Security group ID	Description	VPC ID
Shruthi	sg-0a3cb5565a8e07075	security groups	vpc-02faf88c4fbc874e8
Owner	**Inbound rules count**	**Outbound rules count**	
636372545287	2 Permission entries	1 Permission entry	

You can now check network connectivity with Reachability Analyzer



Security group name	Security group ID	Description	VPC ID
Shruthi	sg-0a3cb5565a8e07075	security groups	vpc-02faf88c4fbc874e8

Owner	Inbound rules count	Outbound rules count
636372545287	2 Permission entries	1 Permission entry

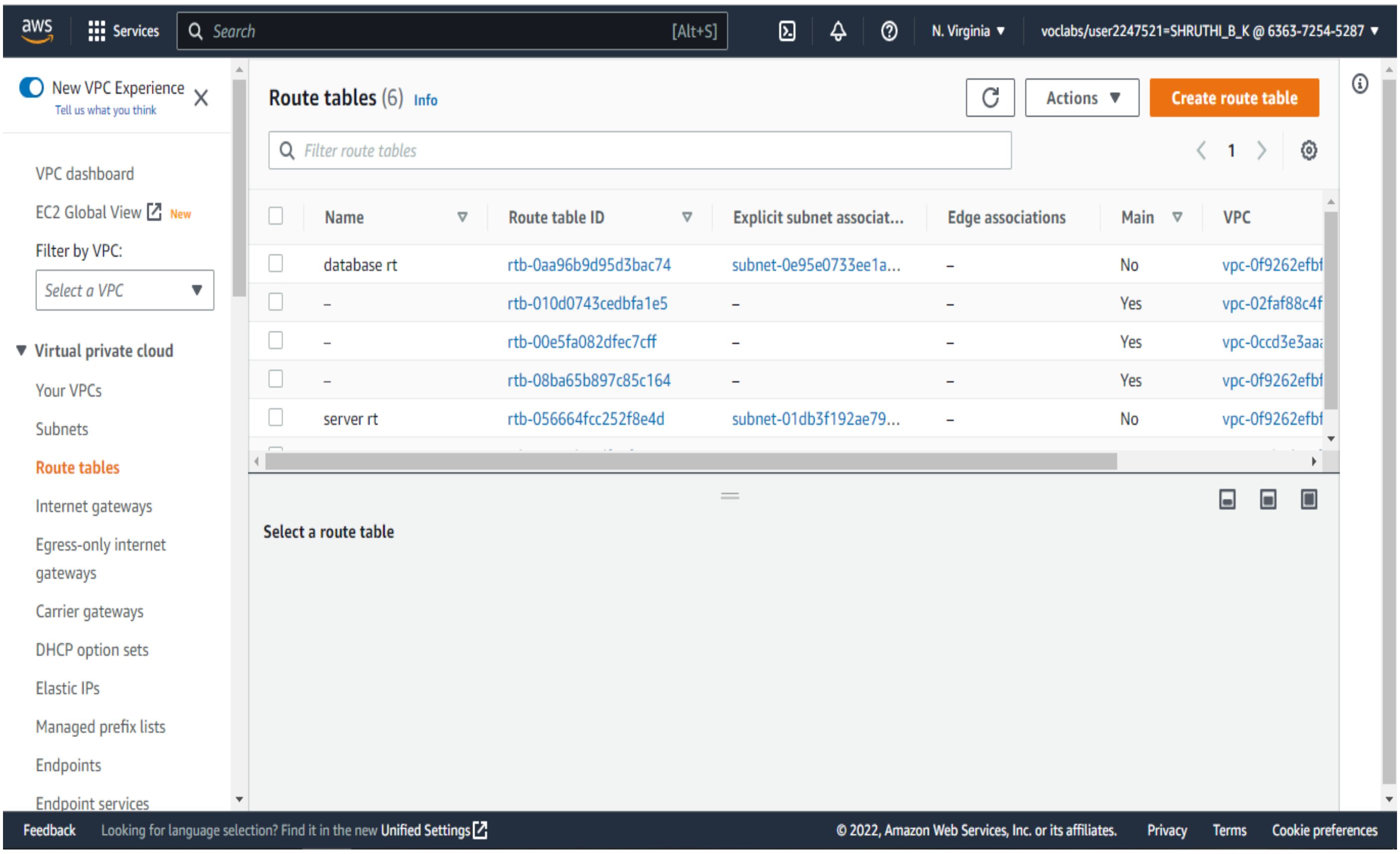
You can now check network connectivity with Reachability Analyzer

Inbound rules (2)

□	Name	Security group rule...	IP version	Type	Protocol
□	–	sgr-066c38b6fd39c0f8c	IPv4	SSH	TCP
□	–	sgr-0e131a8ccfd0db94e	IPv4	HTTP	TCP

7. Routing table:

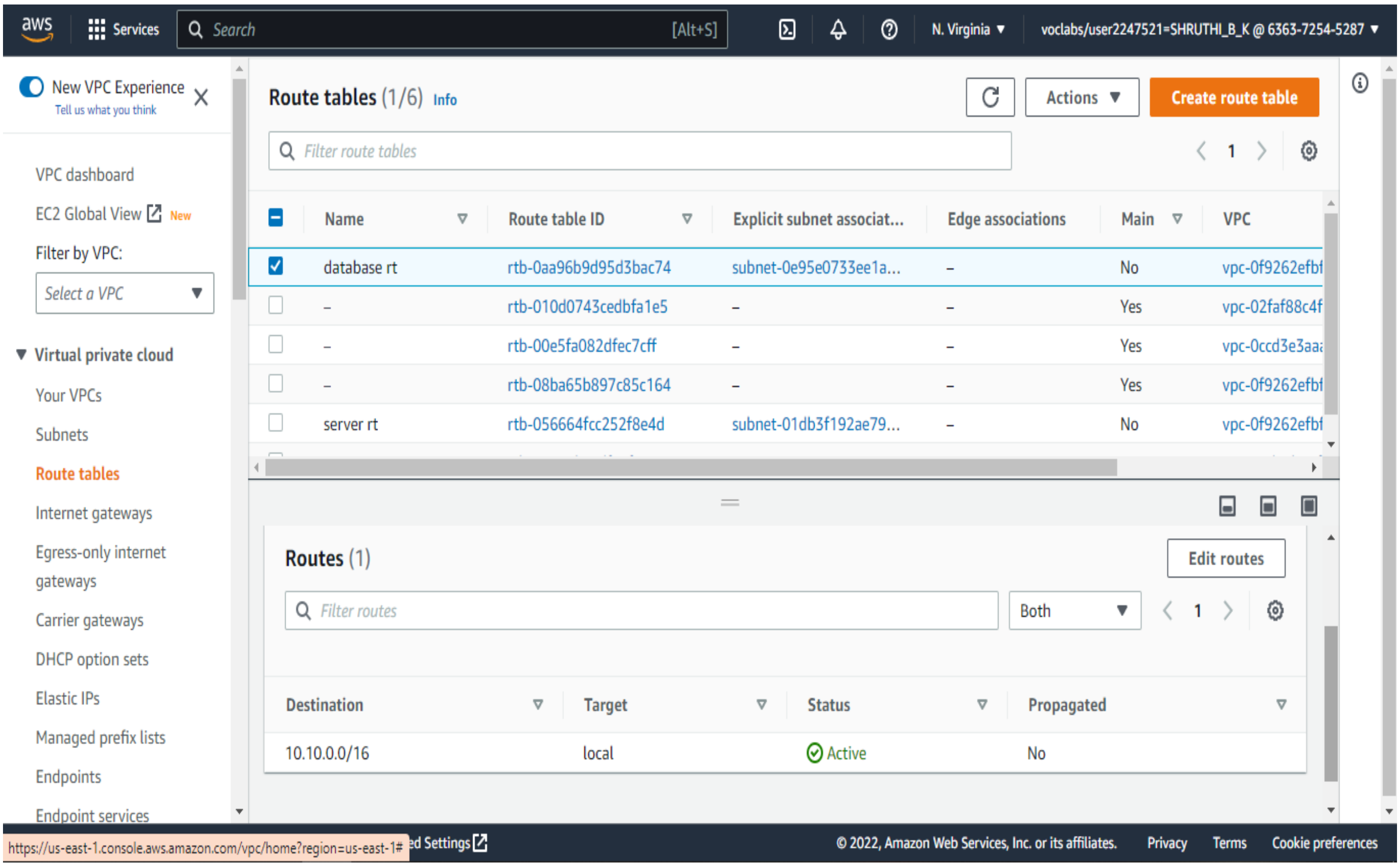
- In the navigation panel, choose Route Tables, and then choose Create route table.
- In the Create route table dialog box, optionally name your route table, then select your VPC, and then choose Create route table.
- Select the custom route table that you just created. The details pane displays tabs for working with its routes, associations, and route propagation.
- On the Routes tab, choose Edit routes, add route, and add the following routes as necessary. Choose Save changes when you're done.
- For IPv4 traffic, specify 0.0.0.0/0 in the Destination box, and select the internet gateway ID in the Target list.
- On the Subnet associations tab, choose Edit subnet associations, select the check box for the subnet, and then choose save associations.



Route tables (6) Info

□	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
□	database rt	rtb-0aa96b9d95d3bac74	subnet-0e95e0733ee1a...	–	No	vpc-0f9262efbf
□	–	rtb-010d0743cedbfa1e5	–	–	Yes	vpc-02faf88c4f
□	–	rtb-00e5fa082dfec7cff	–	–	Yes	vpc-0ccd3e3aa
□	–	rtb-08ba65b897c85c164	–	–	Yes	vpc-0f9262efbf
□	server rt	rtb-056664fcc252f8e4d	subnet-01db3f192ae79...	–	No	vpc-0f9262efbf

Select a route table

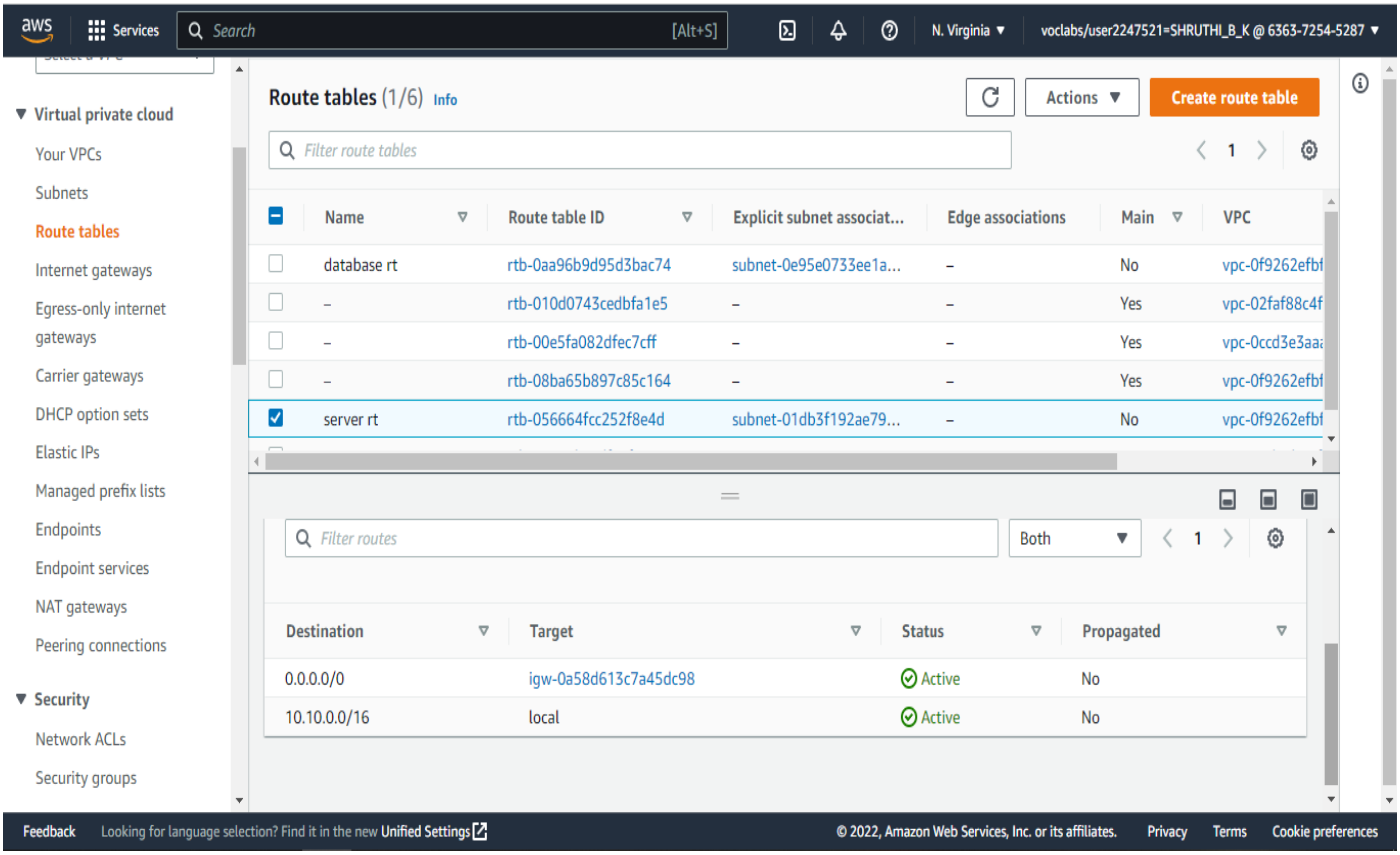


Route tables (1/6) Info

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
☑	database rt	rtb-0aa96b9d95d3bac74	subnet-0e95e0733ee1a...	–	No	vpc-0f9262efbf
□	–	rtb-010d0743cedbfa1e5	–	–	Yes	vpc-02faf88c4f
□	–	rtb-00e5fa082dfec7cff	–	–	Yes	vpc-0ccd3e3aa
□	–	rtb-08ba65b897c85c164	–	–	Yes	vpc-0f9262efbf
□	server rt	rtb-056664fcc252f8e4d	subnet-01db3f192ae79...	–	No	vpc-0f9262efbf

Routes (1)

Destination	Target	Status	Propagated
10.10.0.0/16	local	✓ Active	No



Route tables (1/6) Info

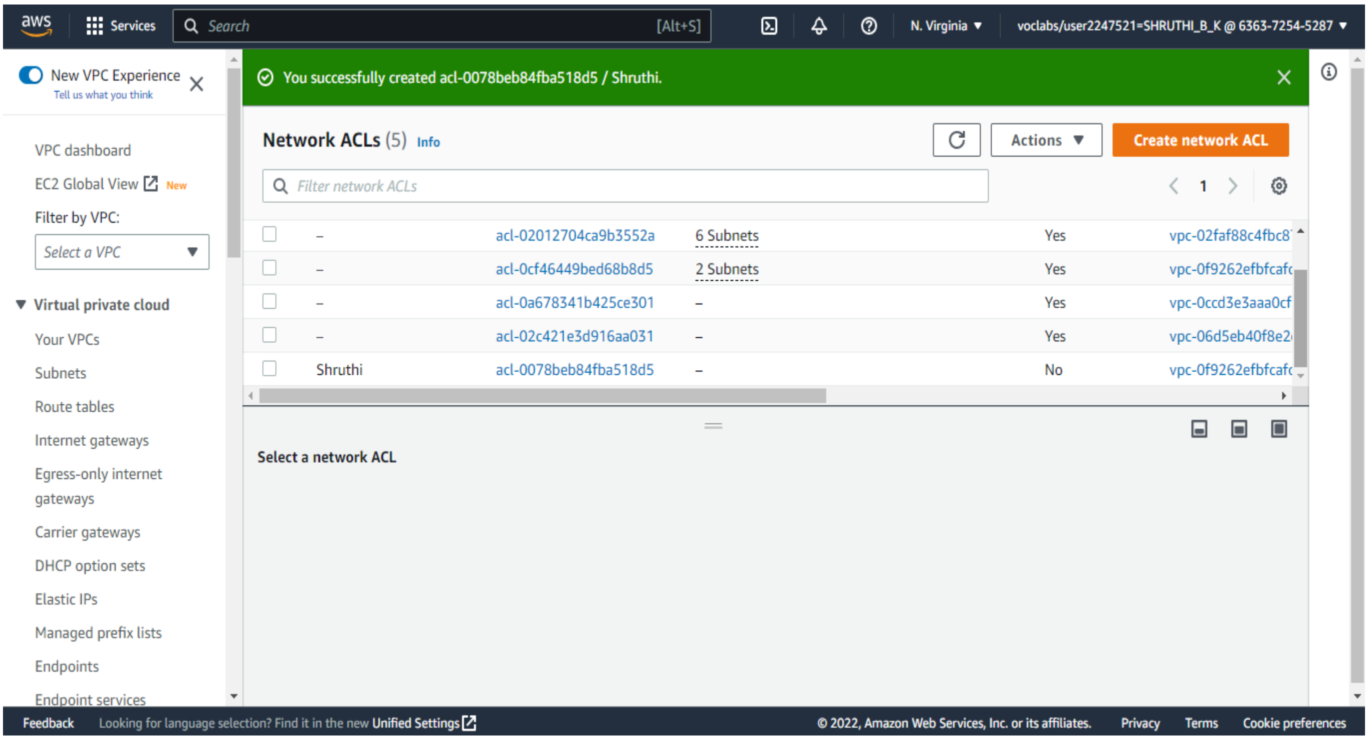
	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
□	database rt	rtb-0aa96b9d95d3bac74	subnet-0e95e0733ee1a...	–	No	vpc-0f9262efbf
□	–	rtb-010d0743cedbfa1e5	–	–	Yes	vpc-02faf88c4f
□	–	rtb-00e5fa082dfec7cff	–	–	Yes	vpc-0ccd3e3aa
□	–	rtb-08ba65b897c85c164	–	–	Yes	vpc-0f9262efbf
☑	server rt	rtb-056664fcc252f8e4d	subnet-01db3f192ae79...	–	No	vpc-0f9262efbf

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a58d613c7a45dc98	✓ Active	No
10.10.0.0/16	local	✓ Active	No

8. Network ACLs for controlling inbound and outbound traffic in the VPC:

An optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You can associate multiple subnets with a single network ACL, but a subnet can be associated with only one network ACL at a time.

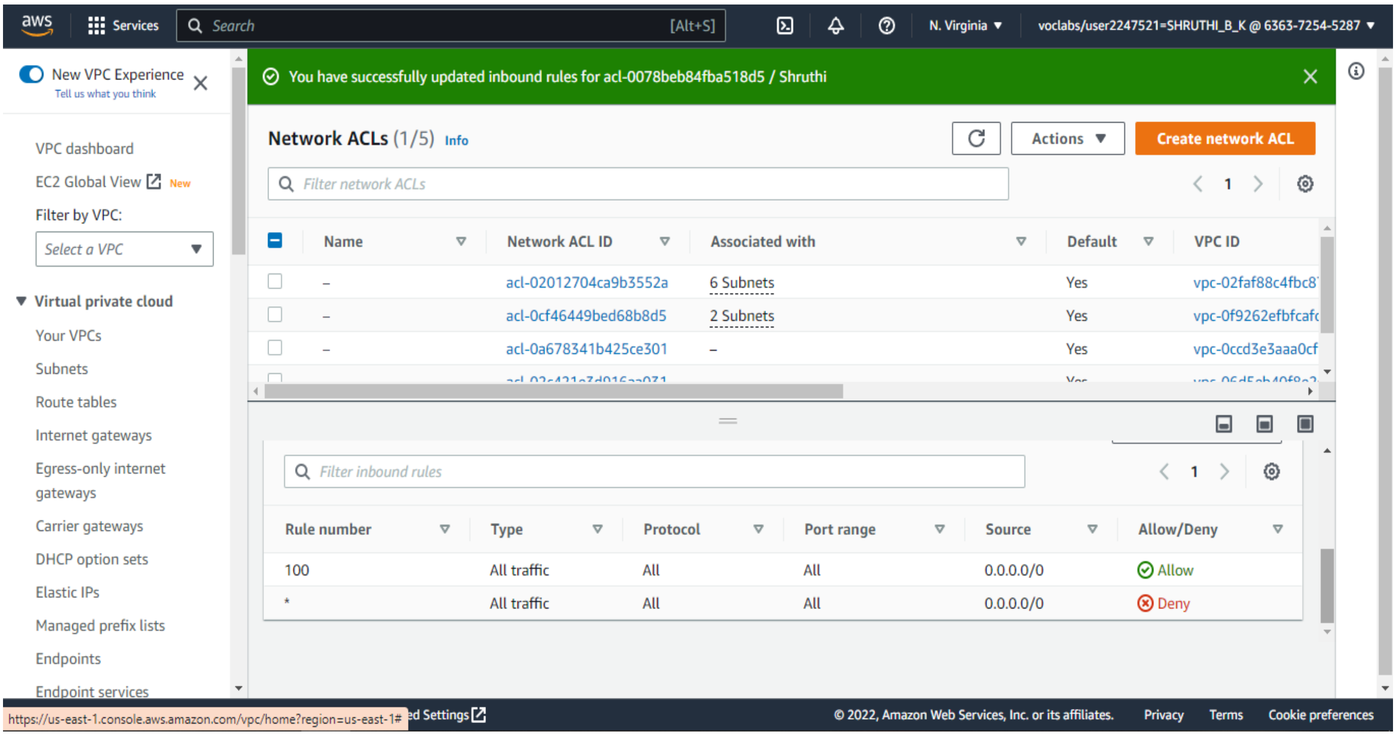
➢ Create a Network ACL through VPC > Network ACLs > Create network ACL. Select the VPC.



You successfully created acl-0078beb84fba518d5 / Shruthi.

□	–	acl-02012704ca9b3552a	6 Subnets	Yes	vpc-02faf88c4fbc8
□	–	acl-0cf46449bed68b8d5	2 Subnets	Yes	vpc-0f9262efbfcafc
□	–	acl-0a678341b425ce301	–	Yes	vpc-0ccd3e3aaa0cf
□	–	acl-02c421e3d916aa031	–	Yes	vpc-06d5eb40f8e2
□	Shruthi	acl-0078beb84fba518d5	–	No	vpc-0f9262efbfcafc

➢ Associate Network ACL with the subnets created. Edit the inbound to allow/deny traffic from the internet to the VPC and use outbound rules to allow/deny the traffic from the VPC to the internet.

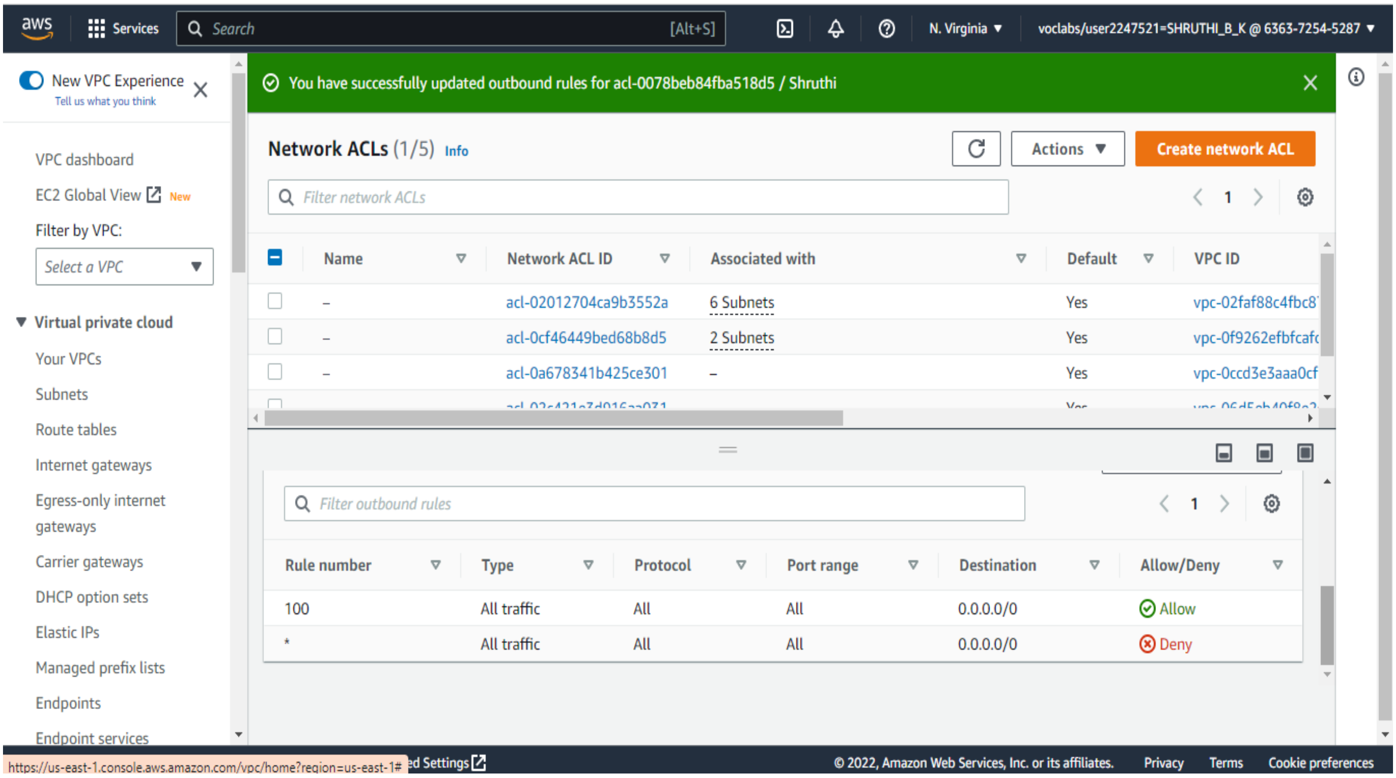


You have successfully updated inbound rules for acl-0078beb84fba518d5 / Shruthi

Network ACLs (1/5) Info

Name	Network ACL ID	Associated with	Default	VPC ID
–	acl-02012704ca9b3552a	6 Subnets	Yes	vpc-02faf88c4fbc8
–	acl-0cf46449bed68b8d5	2 Subnets	Yes	vpc-0f9262efbfcaf
–	acl-0a678341b425ce301	–	Yes	vpc-0ccd3e3aaa0cf

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny



You have successfully updated outbound rules for acl-0078beb84fba518d5 / Shruthi

Network ACLs (1/5) Info

Name	Network ACL ID	Associated with	Default	VPC ID
–	acl-02012704ca9b3552a	6 Subnets	Yes	vpc-02faf88c4fbc8
–	acl-0cf46449bed68b8d5	2 Subnets	Yes	vpc-0f9262efbfcaf
–	acl-0a678341b425ce301	–	Yes	vpc-0ccd3e3aaa0cf

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Network ACL is another layer of protection that can completely allow/deny all the traffic from the internet and to the internet.

CONCLUSION

A virtual private cloud (VPC) is an on-demand configurable pool of shared resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources. The isolation between one VPC user and all other users of the same cloud (other VPC users as well as other public cloud users) is achieved normally through allocation of a private IP subnet and a virtual communication construct (such as a VLAN or a set of encrypted communication channels) per user. In a VPC, the previously described mechanism, providing isolation within the cloud, is accompanied with a virtual private network (VPN) function (again, allocated per VPC user) that secures, by means of authentication and encryption, the remote access of the organization to its VPC resources. With the introduction of the described isolation levels, an organization using this service is in effect working on a 'virtually private' cloud (that is, as if the cloud infrastructure is not shared with other users), and hence the name VPC.VPC is most commonly used in the context of cloud infrastructure as a service. In this context, the infrastructure provider, providing the underlying public cloud infrastructure, and the provider realizing the VPC service over this infrastructure, may be different vendors.

Amazon Web Services launched Amazon Virtual Private Cloud on 26 August 2009, which allows the Amazon Elastic Compute Cloud service to be connected to legacy infrastructure over an IPsec VPN. In AWS, VPC is free to use, however users will be charged for any VPN they use. EC2 and RDS instances running in a VPC can also be purchased using Reserved Instances however, will have a limitation on resources being guaranteed.