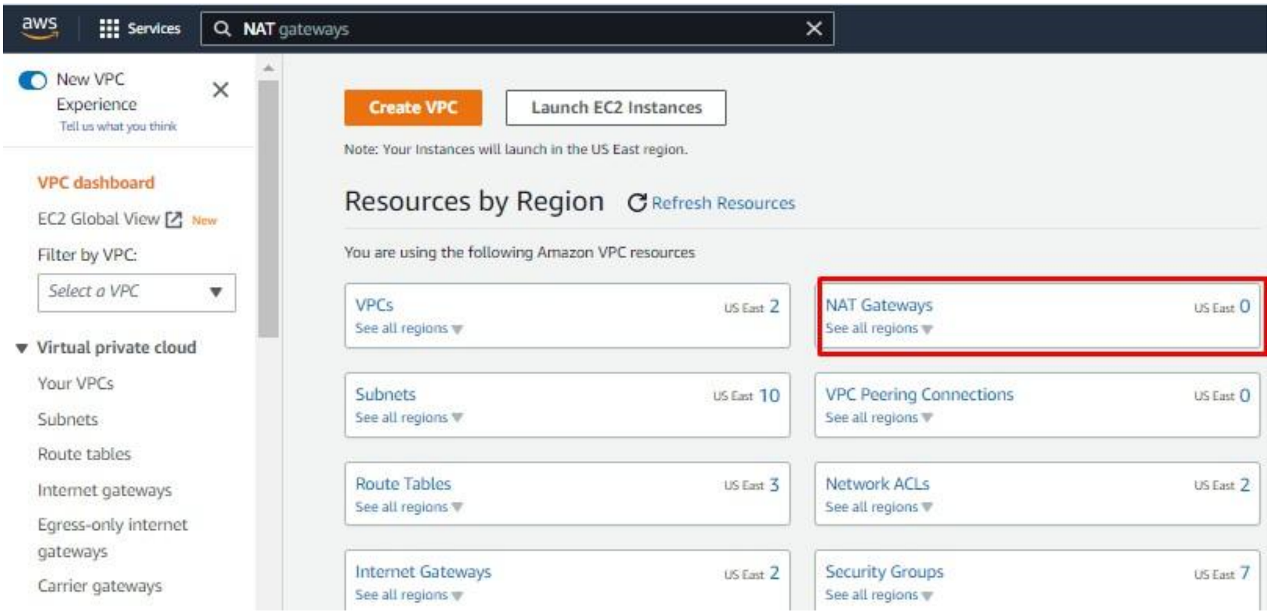
Module 5: Networking using AWS

Demo Document 2

Access Internet Inside Private Subnet Using NAT Gateway

Step 1: Create a Nat Gateway

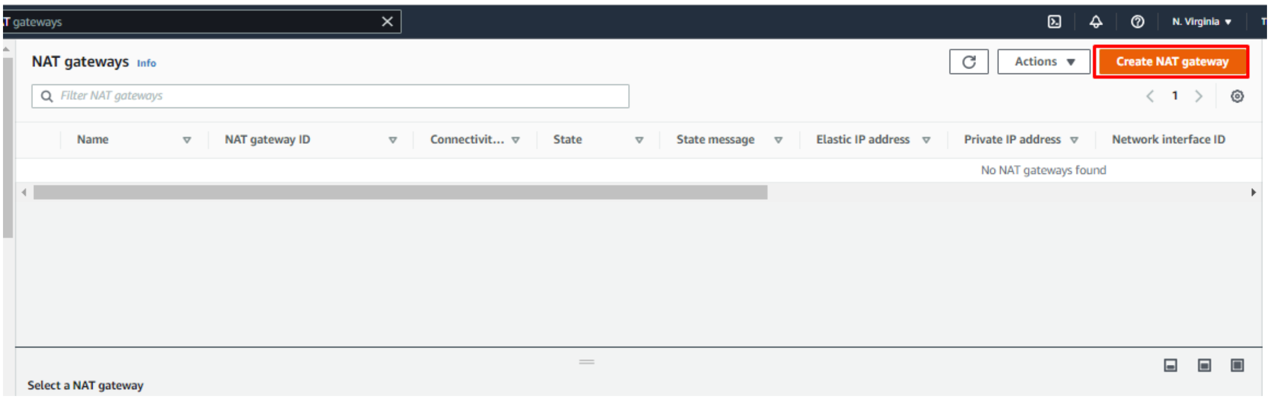
- In VPC dashboard, click on **NAT Gateways**


aws
Services
NAT gateways
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
Create VPC
Launch EC2 Instances
Resources by Region
Refresh Resources
VPCs US East 2 See all regions
NAT Gateways US East 0 See all regions
Subnets US East 10 See all regions
VPC Peering Connections US East 0 See all regions
Route Tables US East 3 See all regions
Network ACLs US East 2 See all regions
Internet Gateways US East 2 See all regions
Security Groups US East 7 See all regions

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

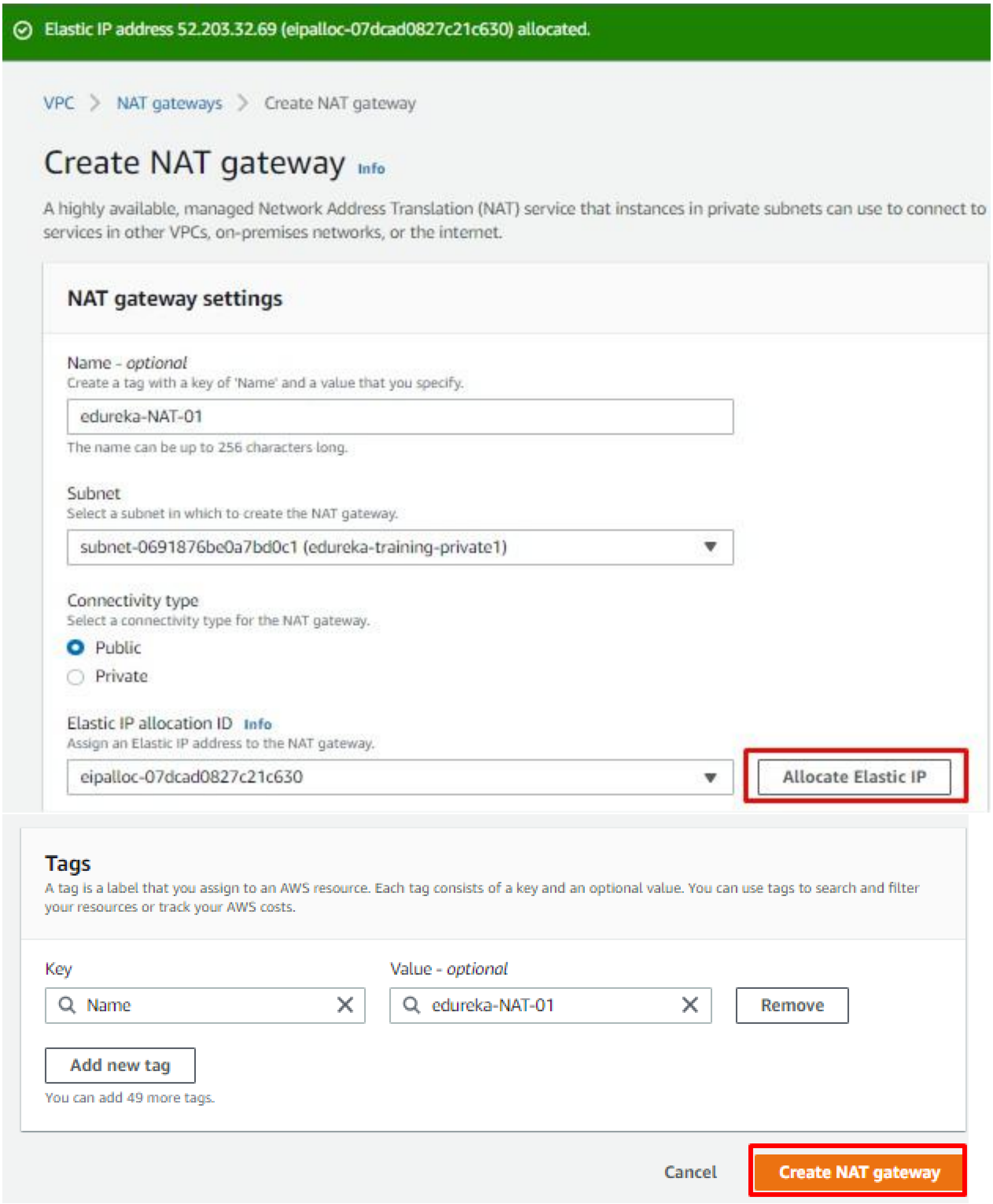
You are using the following Amazon VPC resources

- Click on **Create NAT Gateway**



Name	NAT gateway ID	Connectivit...	State	State message	Elastic IP address	Private IP address	Network interface ID
					No NAT gateways found		

- Choose the private subnet that you wish to have as the internet connectivity
- Create an elastic IP if you don’t have any or allocate the elastic IP if you already have any



Elastic IP address 52.203.32.69 (eipalloc-07dcad0827c21c630) 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.
edureka-NAT-01
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0691876be0a7bd0c1 (edureka-training-private1) ▼

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-07dcad0827c21c630 ▼ Allocate Elastic IP

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.

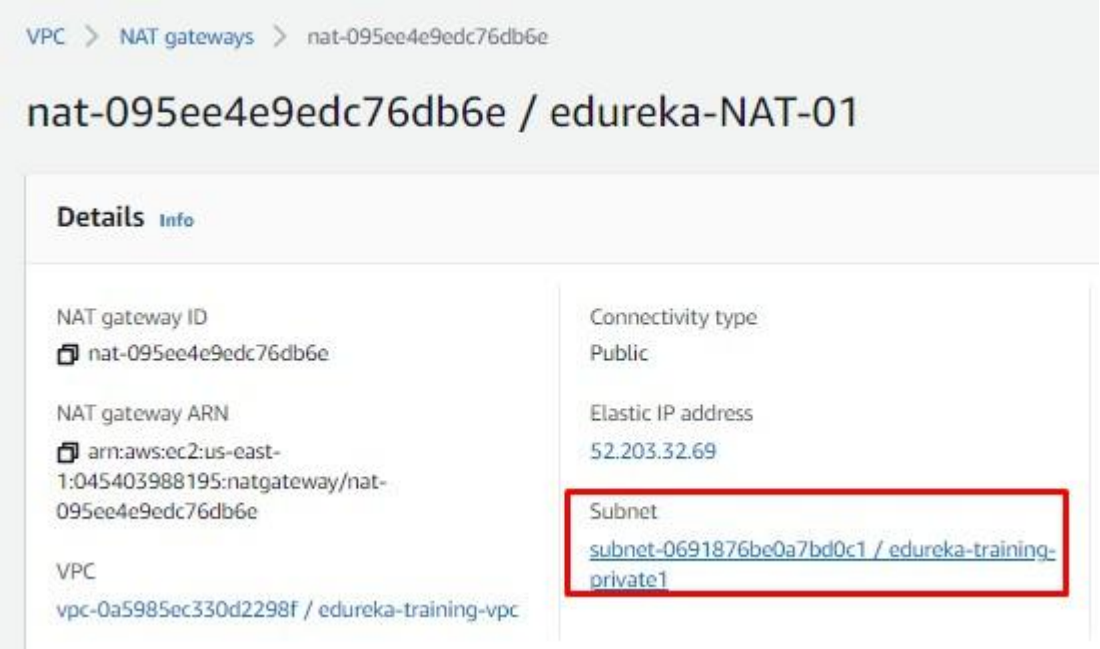
Key	Value - *optional*	
Name	edureka-NAT-01	Remove

Add new tag
You can add 49 more tags.

Cancel Create NAT gateway

Step 2: Update your private route table

- Route all the traffic in the private subnet to the NAT gateway



nat-095ee4e9edc76db6e / edureka-NAT-01

Details Info

NAT gateway ID
nat-095ee4e9edc76db6e

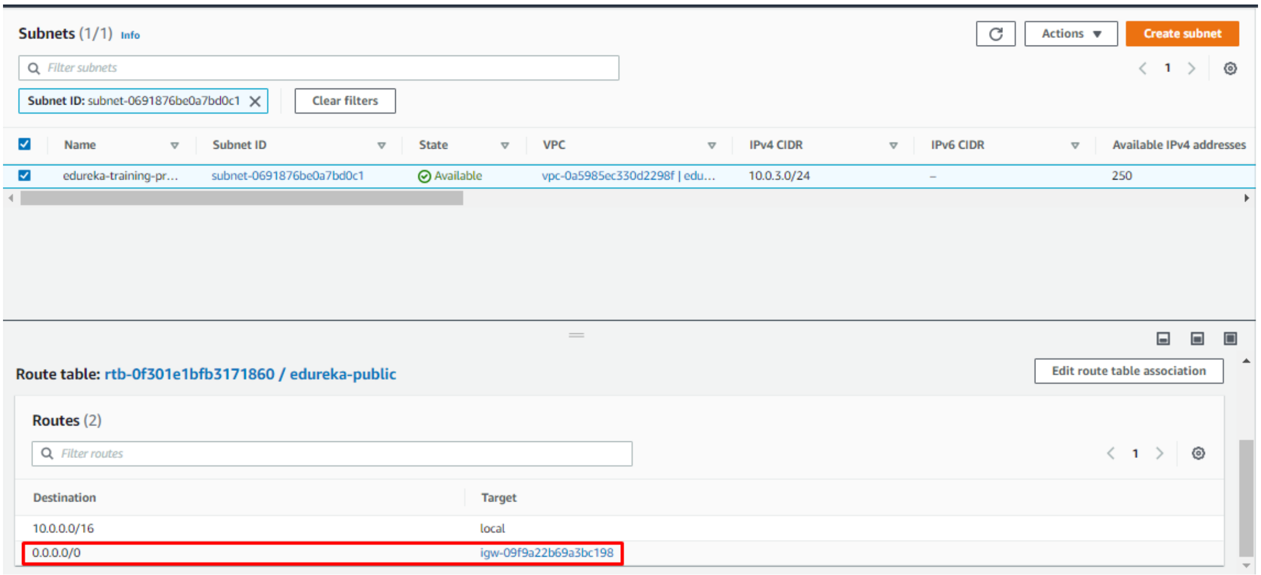
NAT gateway ARN
arn:aws:ec2:us-east-1:045403988195:natgateway/nat-095ee4e9edc76db6e

VPC
vpc-0a5985ec330d2298f / edureka-training-vpc

Connectivity type
Public

Elastic IP address
52.203.32.69

Subnet
subnet-0691876be0a7bd0c1 / edureka-training-private1



Subnets (1/1) Info

Subnet ID: subnet-0691876be0a7bd0c1

☑	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
☑	edureka-training-pr...	subnet-0691876be0a7bd0c1	Available	vpc-0a5985ec330d2298f | edu...	10.0.3.0/24	–	250

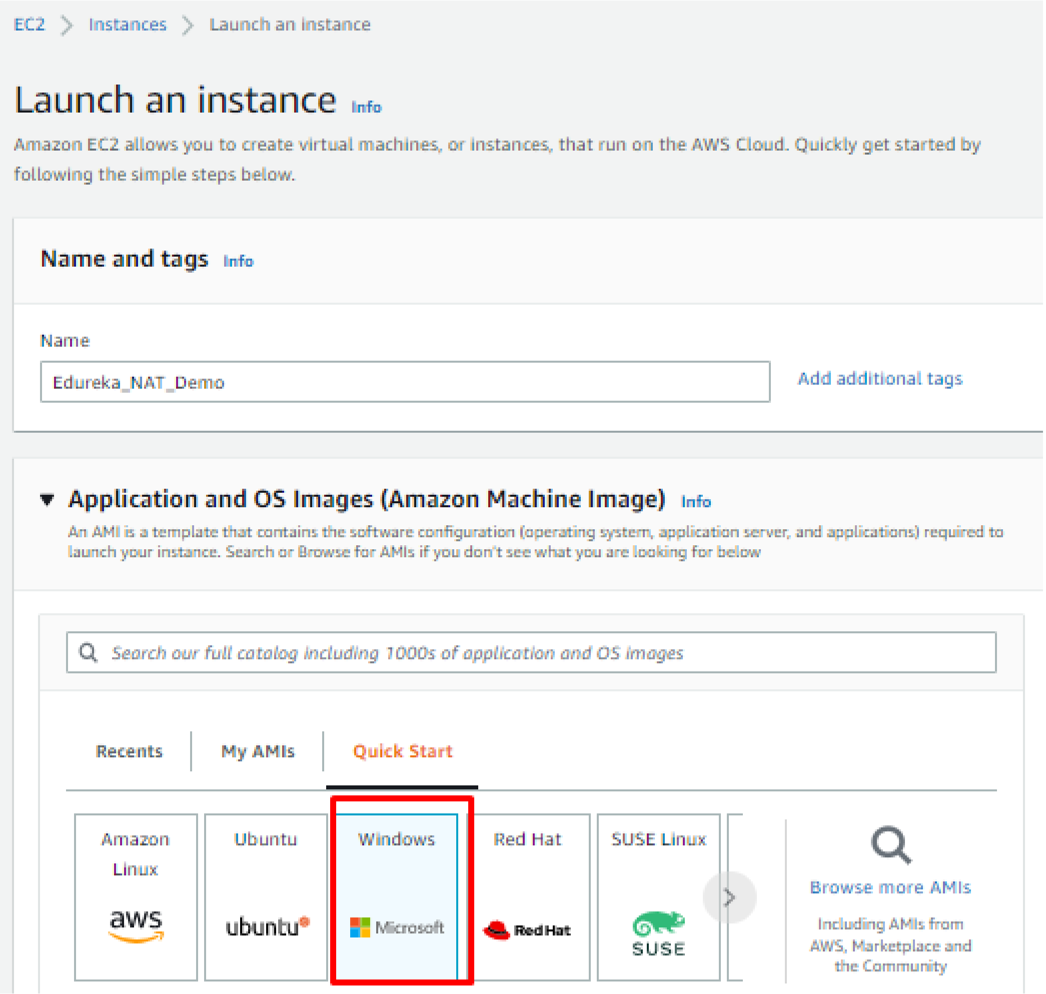
Route table: rtb-0f301e1bfb3171860 / edureka-public

Routes (2)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-09f9a22b69a3bc198

Step 3: Create and connect a windows instance in the private subnet to the internet

- Create a windows instance
- Connect to it through the desktop manager
- Connect it to the internet



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

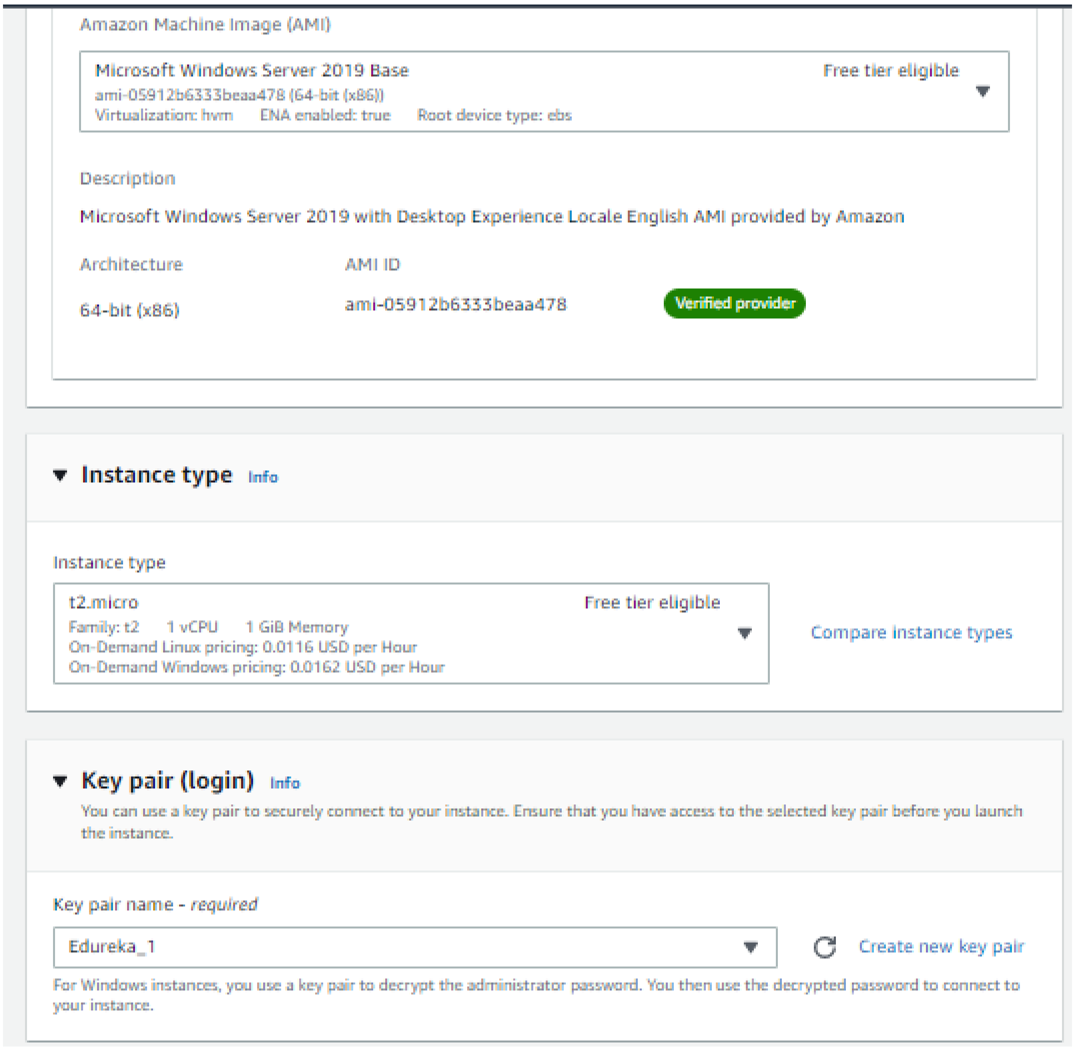
Name and tags Info

Name: Edureka_NAT_Demo

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
My AMIs
Quick Start
Amazon Linux
aws
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Linux
SUSE
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community



Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base — Free tier eligible
ami-05912b6333beaa478 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows Server 2019 with Desktop Experience Locale English AMI provided by Amazon

Architecture: 64-bit (x86)

AMI ID: ami-05912b6333beaa478

Verified provider

▼ Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Compare instance types

▼ Key pair (login) Info

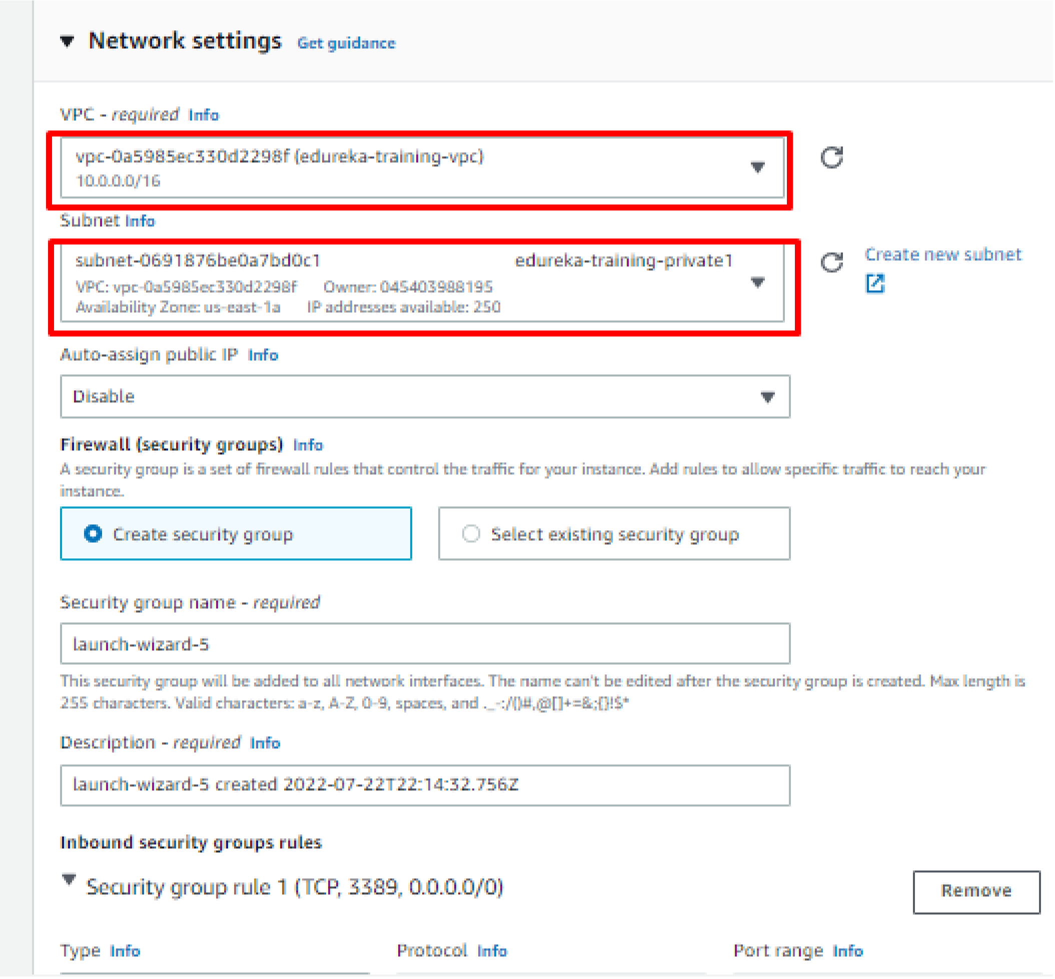
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Edureka_1

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.



▼ Network settings Get guidance

VPC - *required* Info

vpc-0a5985ec330d2298f (edureka-training-vpc)
10.0.0.0/16

Subnet Info

subnet-0691876be0a7bd0c1 edureka-training-private1
VPC: vpc-0a5985ec330d2298f Owner: 045403988195
Availability Zone: us-east-1a IP addresses available: 250

Create new subnet

Auto-assign public IP Info

Disable

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-5

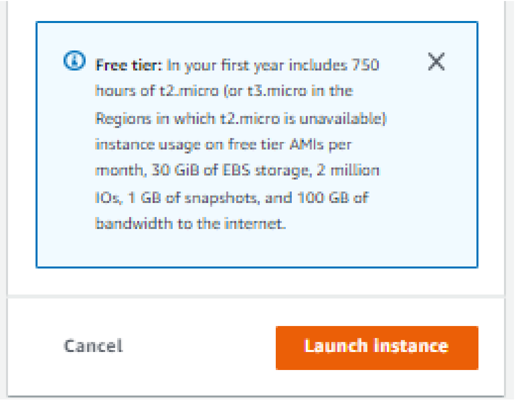
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

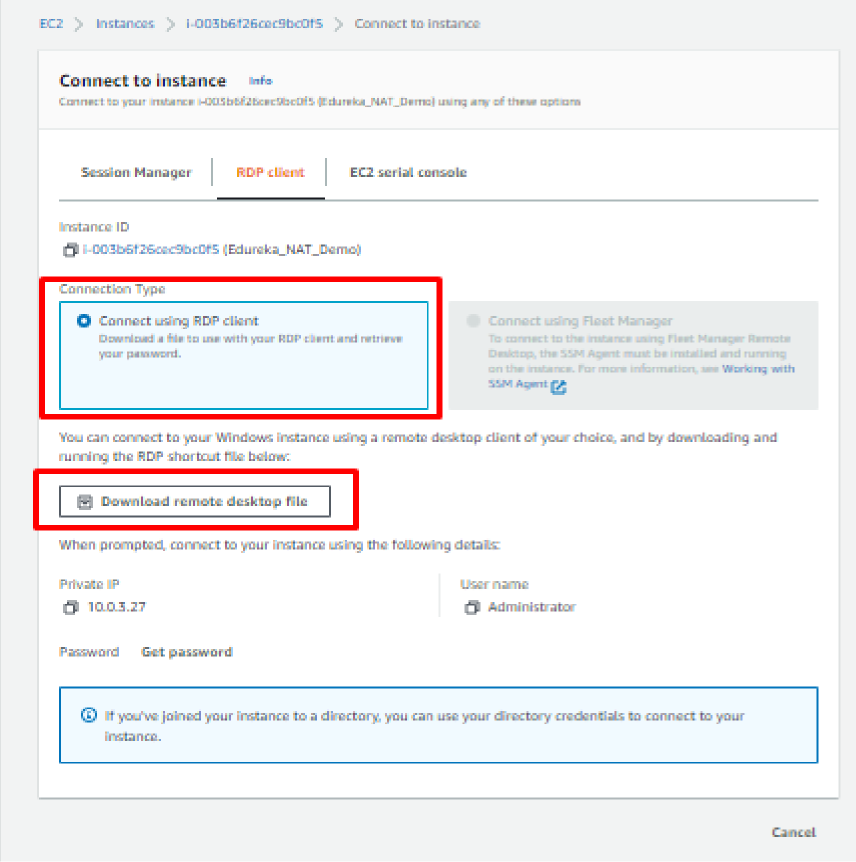
launch-wizard-5 created 2022-07-22T22:14:32.756Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0)



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



EC2 > Instances > i-003b6f26cec9bc0f5 > Connect to instance

Connect to instance Info

Connect to your instance i-003b6f26cec9bc0f5 (Edureka_NAT_Demo) using any of these options

Instance ID

i-003b6f26cec9bc0f5 (Edureka_NAT_Demo)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Private IP
10.0.3.27

User name
Administrator

Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Conclusion: We have successfully accessed Internet Inside Private Subnet Using NAT Gateway

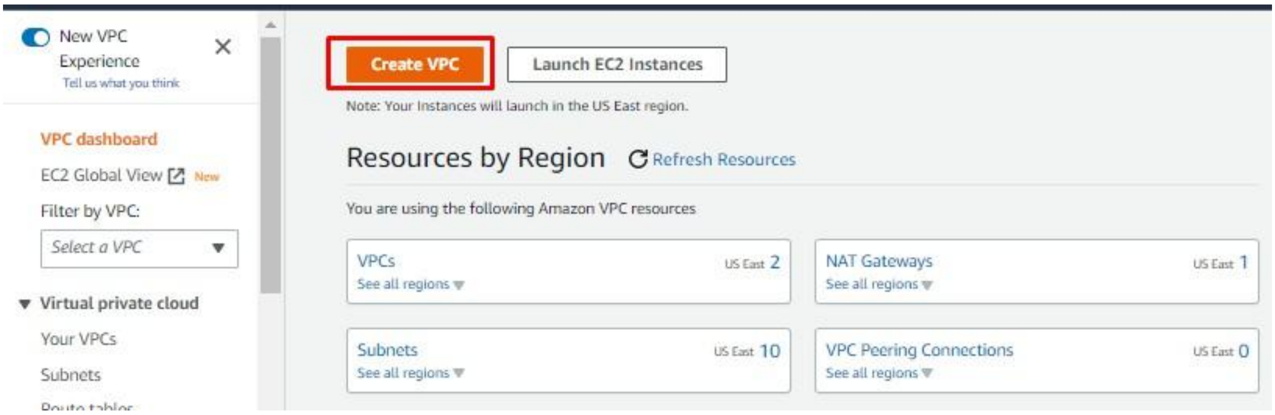
Module 5: Networking using AWS

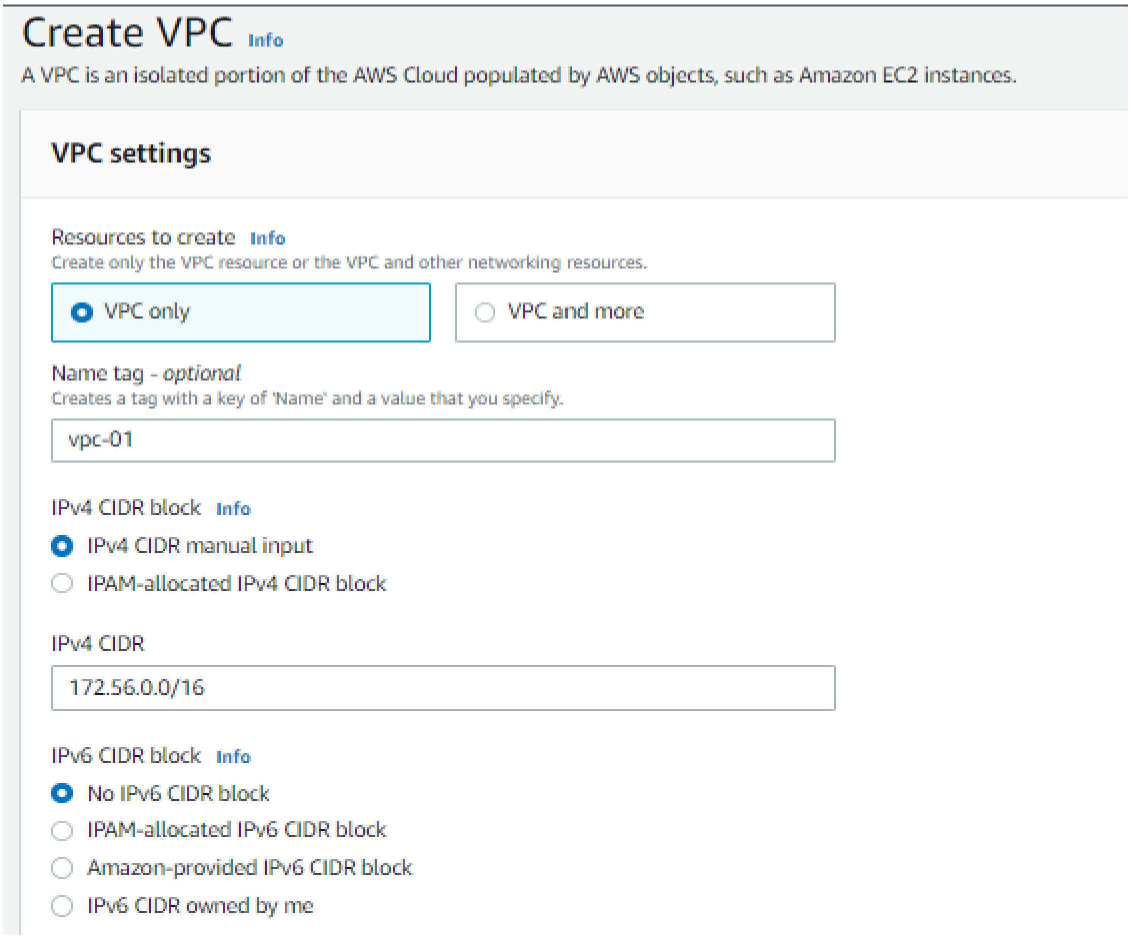
Demo Document 3

Using VPC Peering to Communicate between Two Instances

Step 1: Create two VPCs in your AWS Account

- Create two VPCs in your AWS account which can be connected using VPC peering





Create VPC Info

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

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

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

vpc-01

IPv4 CIDR block Info

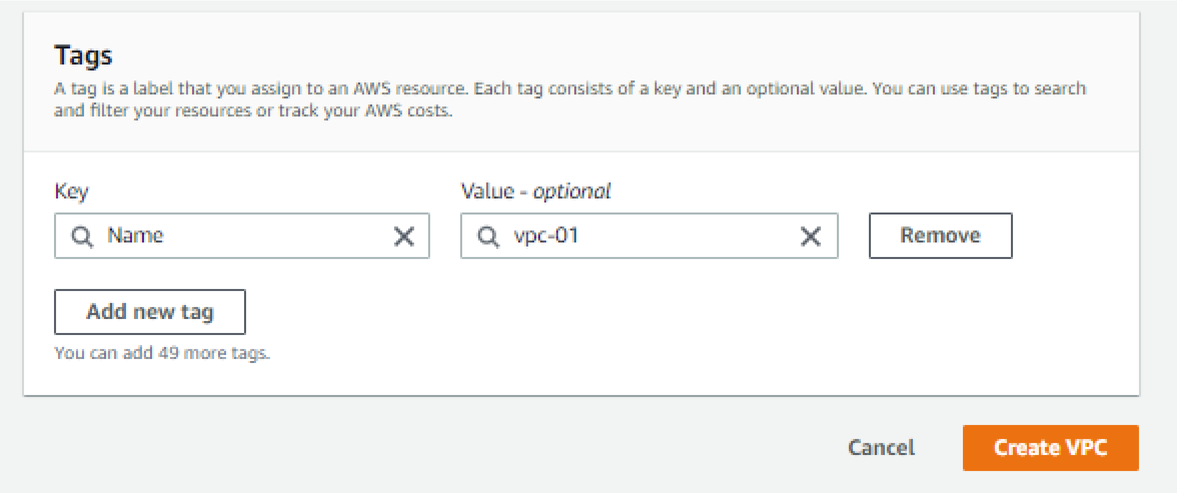
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

172.56.0.0/16

IPv6 CIDR block Info

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

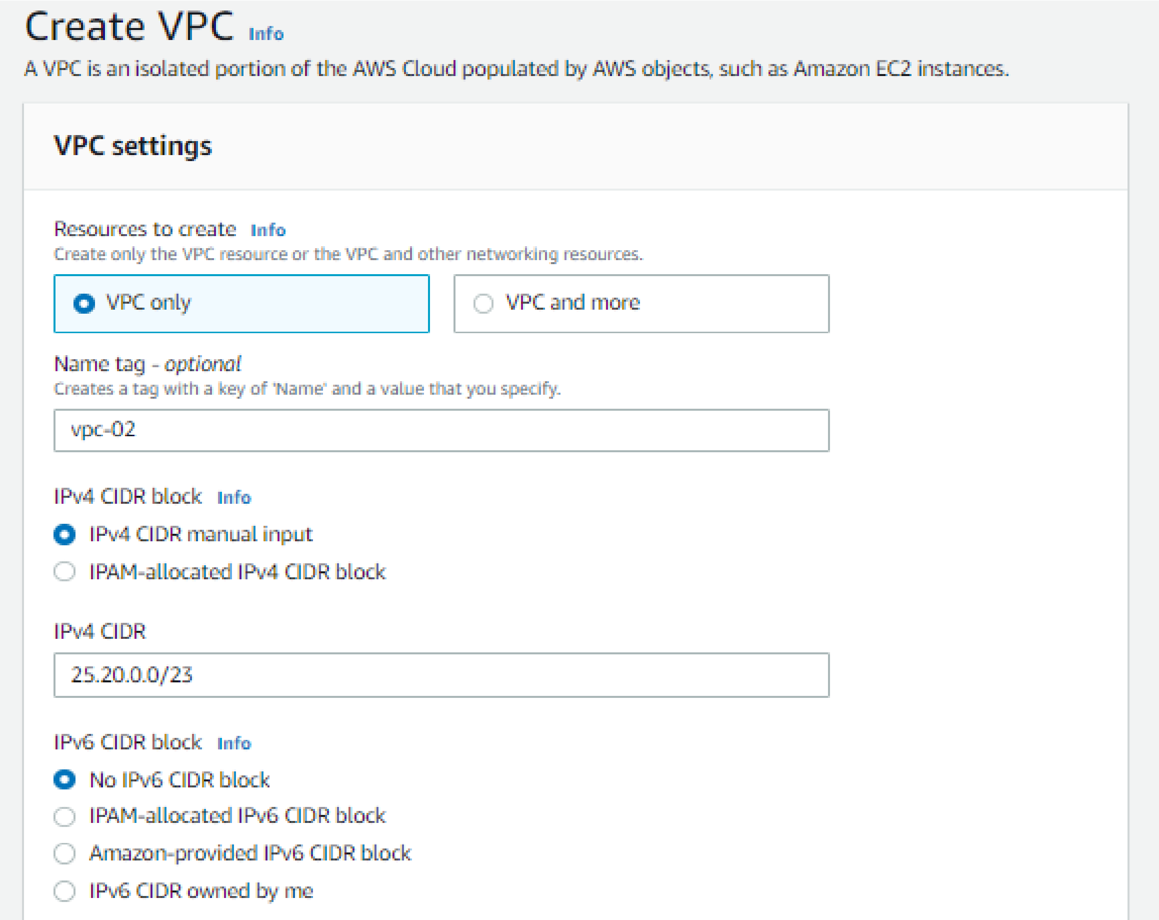


Tags

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*
Name	vpc-01

Create another VPC



Create VPC

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

VPC settings

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.

vpc-02

IPv4 CIDR block

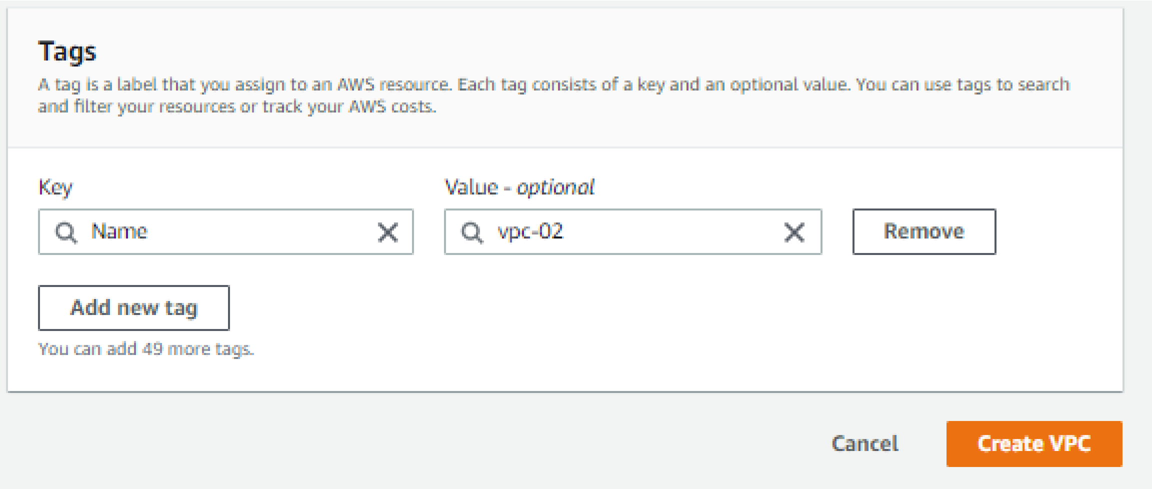
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

25.20.0.0/23

IPv6 CIDR block

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



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.

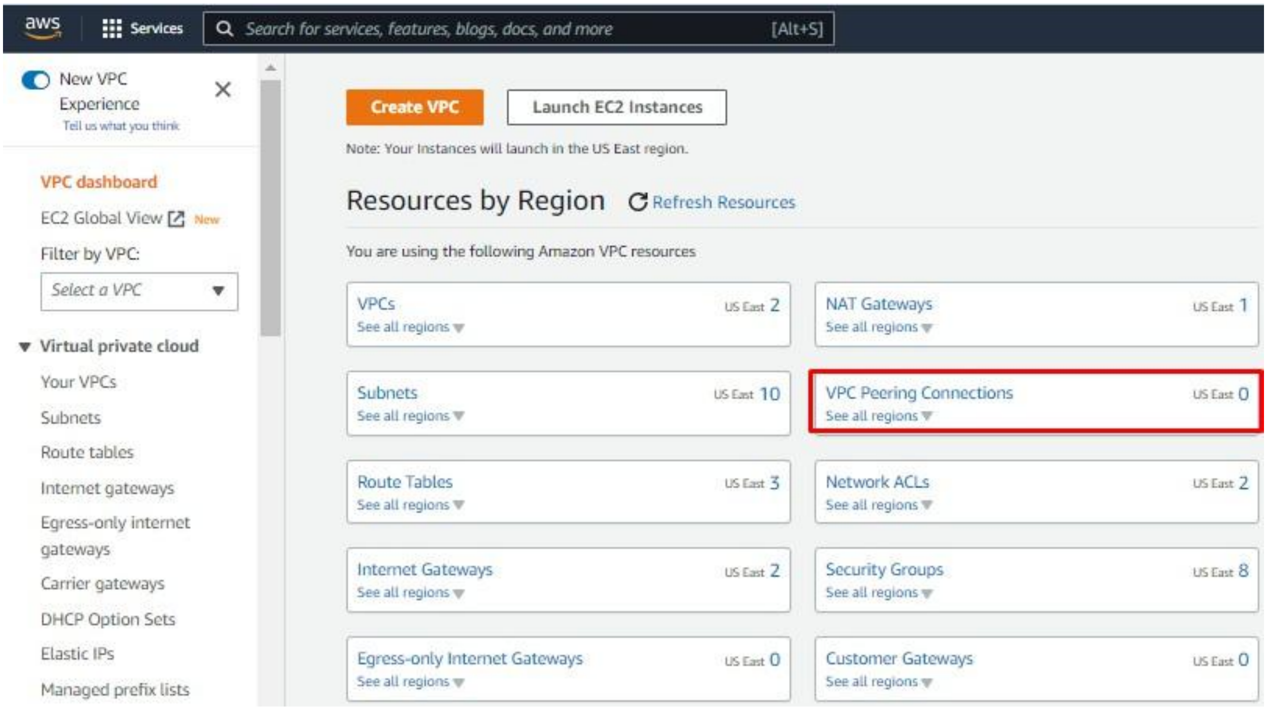
Key: Name

Value - *optional*: vpc-02

You can add 49 more tags.

Step 2: Create a VPC Peering

- In your VPC dashboard, select the **Peering Connection**
- Click on **VPC Peering Connection**



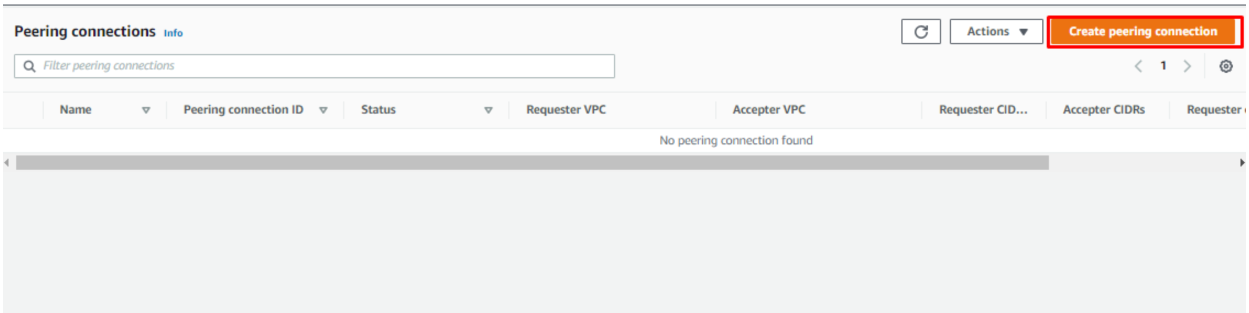
Note: Your Instances will launch in the US East region.

Resources by Region

You are using the following Amazon VPC resources

VPCs	US East 2	NAT Gateways	US East 1
Subnets	US East 10	VPC Peering Connections	US East 0
Route Tables	US East 3	Network ACLs	US East 2
Internet Gateways	US East 2	Security Groups	US East 8
Egress-only Internet Gateways	US East 0	Customer Gateways	US East 0

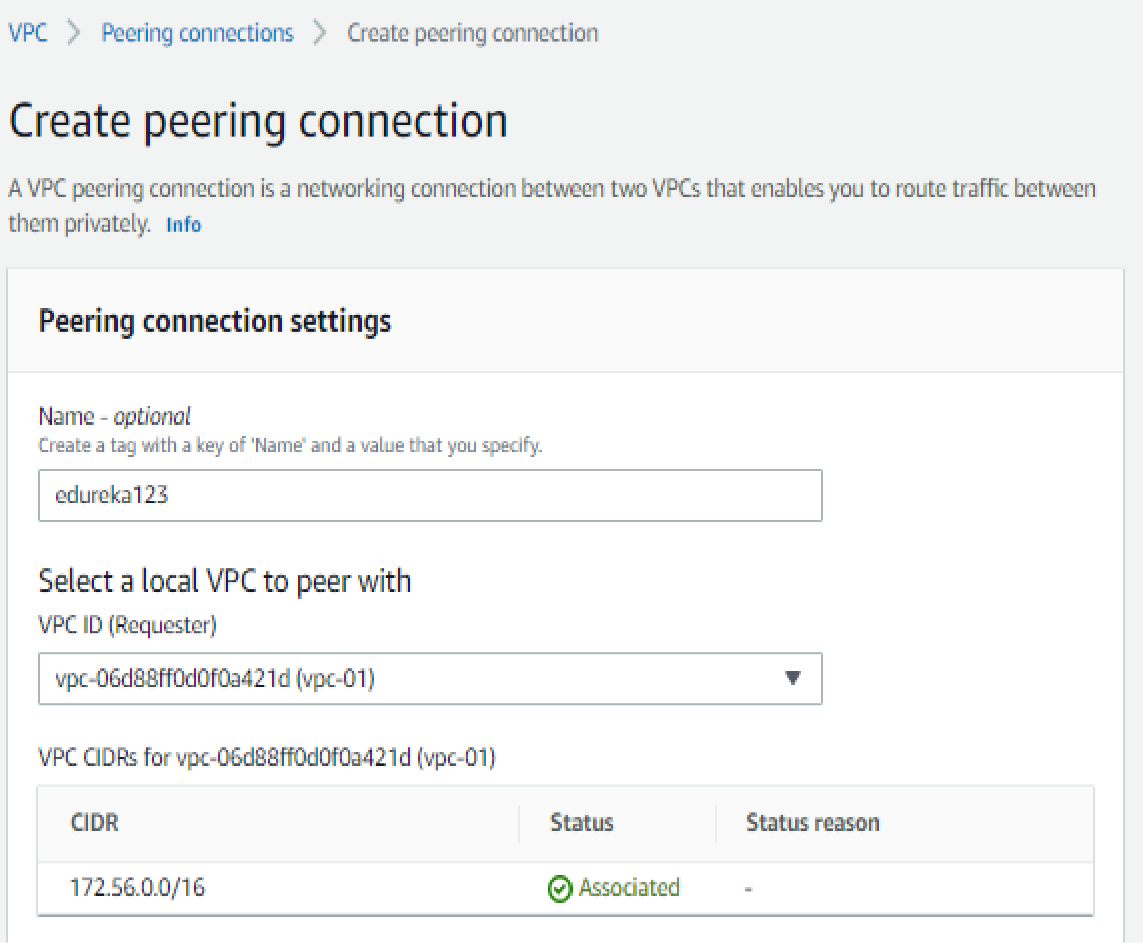
Click on **Create peering connection**



Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CID...	Accepter CIDRs	Requester

No peering connection found

- Give the name for the peering
- Select a VPC, which acts as a requester of the peering connection



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.

edureka123

Select a local VPC to peer with

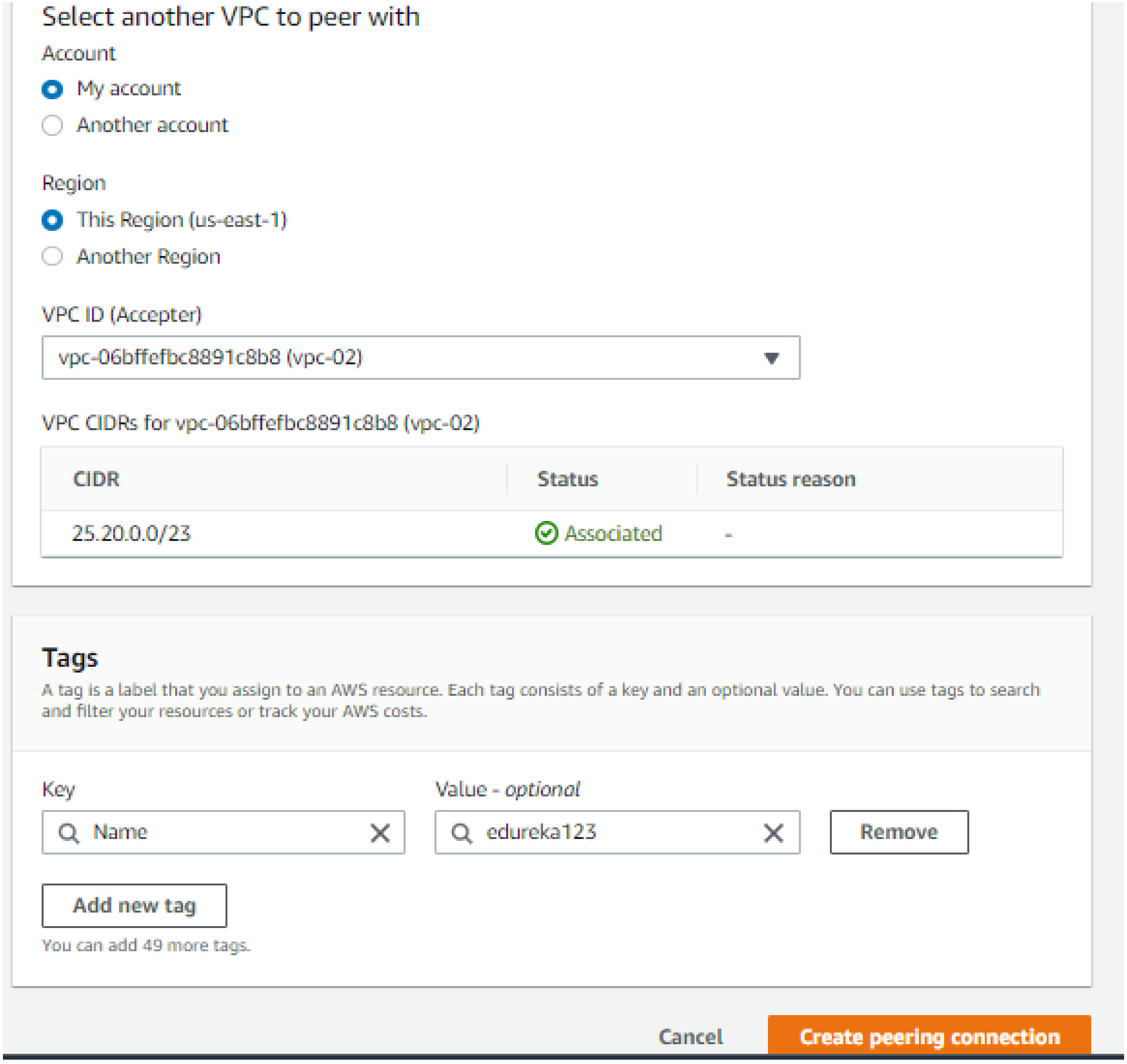
VPC ID (Requester)

vpc-06d88ff0d0f0a421d (vpc-01) ▼

VPC CIDRs for vpc-06d88ff0d0f0a421d (vpc-01)

CIDR	Status	Status reason
172.56.0.0/16	✓ Associated	-

- Select another VPC to peer with
- Select My Account, in accounts and the region where you have created the VPC



Select another VPC to peer with

Account

● My account

○ Another account

Region

● This Region (us-east-1)

○ Another Region

VPC ID (Accepter)

vpc-06bffefbc8891c8b8 (vpc-02)

VPC CIDRs for vpc-06bffefbc8891c8b8 (vpc-02)

CIDR	Status	Status reason
25.20.0.0/23	✓ Associated	-

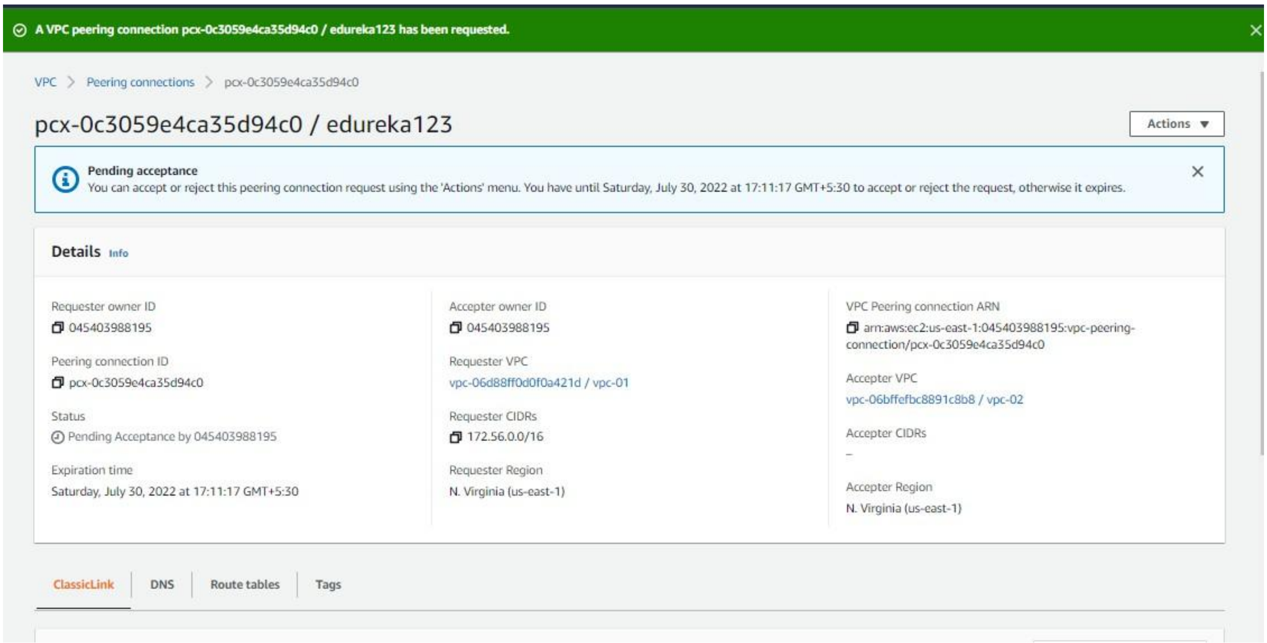
Tags

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*	
Name	edureka123	Remove

You can add 49 more tags.

Click on **Create peering connection**



A VPC peering connection pcx-0c3059e4ca35d94c0 / edureka123 has been requested.

pcx-0c3059e4ca35d94c0 / edureka123

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Saturday, July 30, 2022 at 17:11:17 GMT+5:30 to accept or reject the request, otherwise it expires.

Details Info

Requester owner ID
045403988195

Peering connection ID
pcx-0c3059e4ca35d94c0

Status
Pending Acceptance by 045403988195

Expiration time
Saturday, July 30, 2022 at 17:11:17 GMT+5:30

Accepter owner ID
045403988195

Requester VPC
vpc-06d88ff0d0f0a421d / vpc-01

Requester CIDRs
172.56.0.0/16

Requester Region
N. Virginia (us-east-1)

VPC Peering connection ARN
arn:aws:ec2:us-east-1:045403988195:vpc-peering-connection/pcx-0c3059e4ca35d94c0

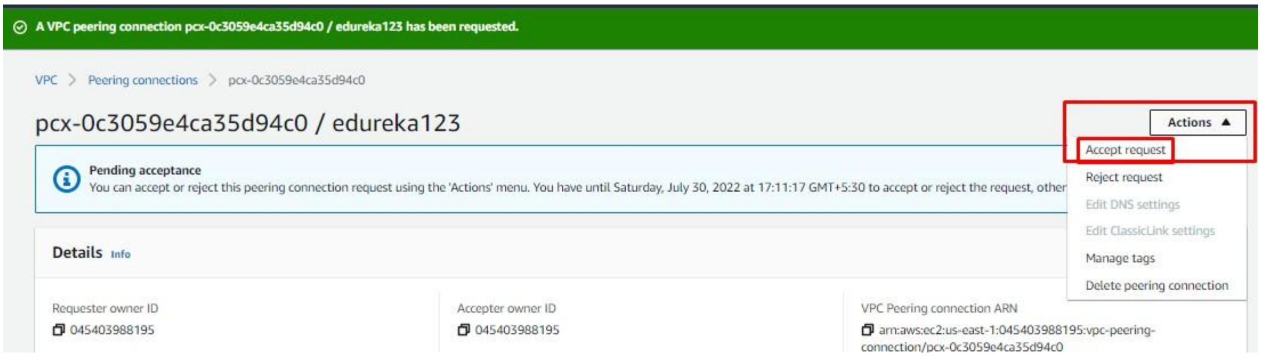
Accepter VPC
vpc-06bffefbc8891c8b8 / vpc-02

Accepter CIDRs
–

Accepter Region
N. Virginia (us-east-1)

Our VPC peering has been created

Now click on **Actions -> Accept request**



A VPC peering connection pcx-0c3059e4ca35d94c0 / edureka123 has been requested.

VPC > Peering connections > pcx-0c3059e4ca35d94c0

pcx-0c3059e4ca35d94c0 / edureka123

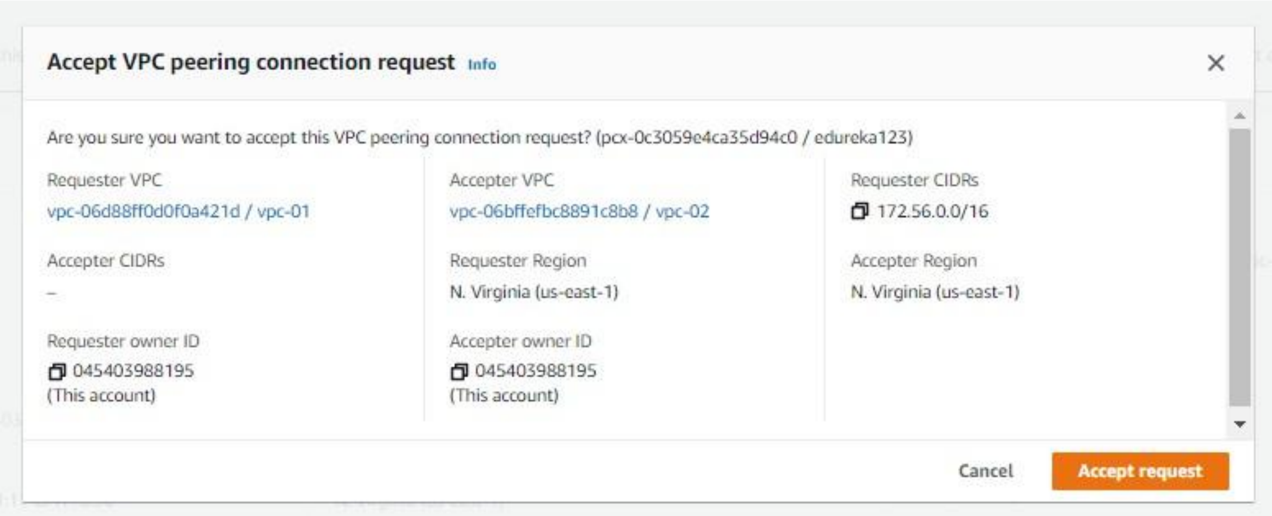
Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Saturday, July 30, 2022 at 17:11:17 GMT+5:30 to accept or reject the request, other

Details Info

Requester owner ID
045403988195

Accepter owner ID
045403988195

VPC Peering connection ARN
arn:aws:ec2:us-east-1:045403988195:vpc-peering-connection/pcx-0c3059e4ca35d94c0



Accept VPC peering connection request Info

Are you sure you want to accept this VPC peering connection request? (pcx-0c3059e4ca35d94c0 / edureka123)

Requester VPC
vpc-06d88ff0d0f0a421d / vpc-01

Accepter VPC
vpc-06bffefbc8891c8b8 / vpc-02

Requester CIDRs
172.56.0.0/16

Accepter CIDRs
–

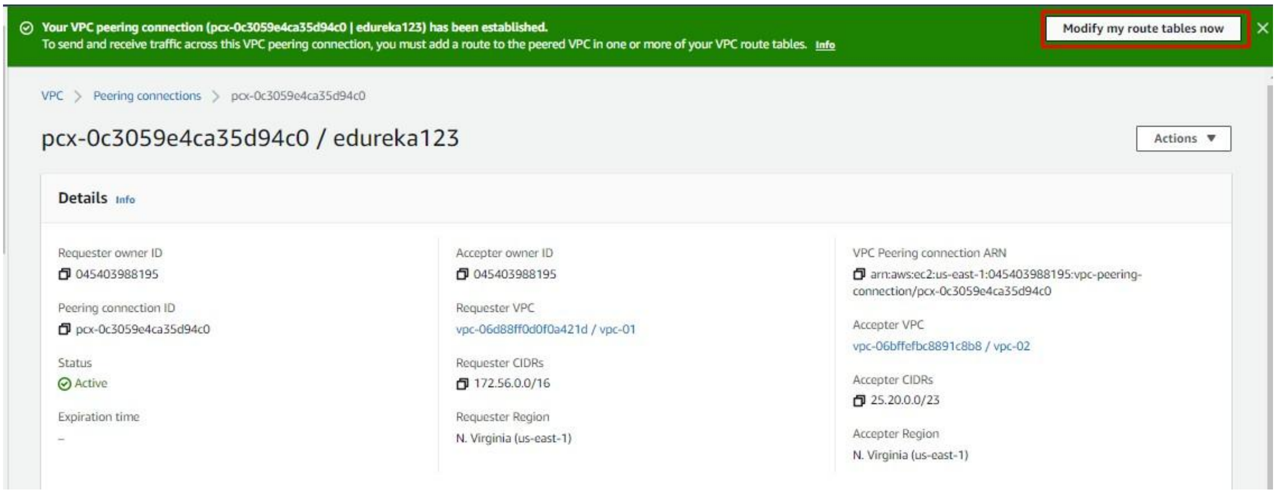
Requester Region
N. Virginia (us-east-1)

Accepter Region
N. Virginia (us-east-1)

Requester owner ID
045403988195
(This account)

Accepter owner ID
045403988195
(This account)

Step 3: Update the route table



Your VPC peering connection (pcx-0c3059e4ca35d94c0 | edureka123) 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

VPC > Peering connections > pcx-0c3059e4ca35d94c0

pcx-0c3059e4ca35d94c0 / edureka123

Details Info

Requester owner ID
045403988195

Peering connection ID
pcx-0c3059e4ca35d94c0

Status
Active

Expiration time
–

Accepter owner ID
045403988195

Requester VPC
vpc-06d88ff0d0f0a421d / vpc-01

Requester CIDRs
172.56.0.0/16

Requester Region
N. Virginia (us-east-1)

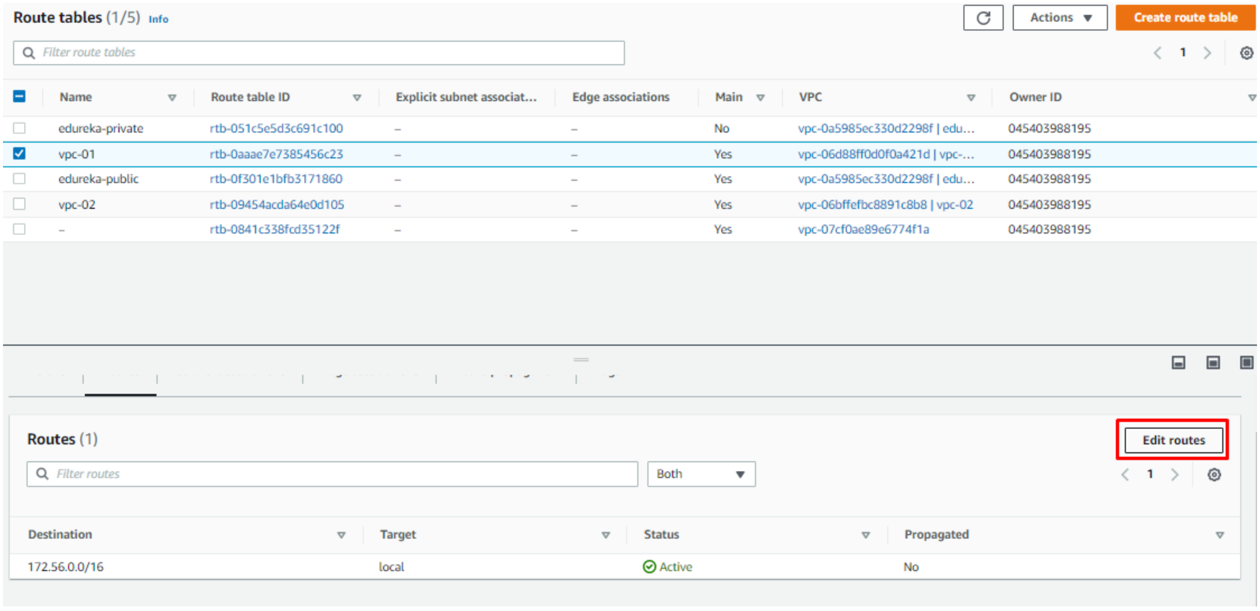
VPC Peering connection ARN
arn:aws:ec2:us-east-1:045403988195:vpc-peering-connection/pcx-0c3059e4ca35d94c0

Accepter VPC
vpc-06bffefbc8891c8b8 / vpc-02

Accepter CIDRs
25.20.0.0/23

Accepter Region
N. Virginia (us-east-1)

- Update the public and private route table in the first VPC
- Such that the traffic of the other VPC is always directed towards the VPC peering



Route tables (1/5) Info

Filter route tables

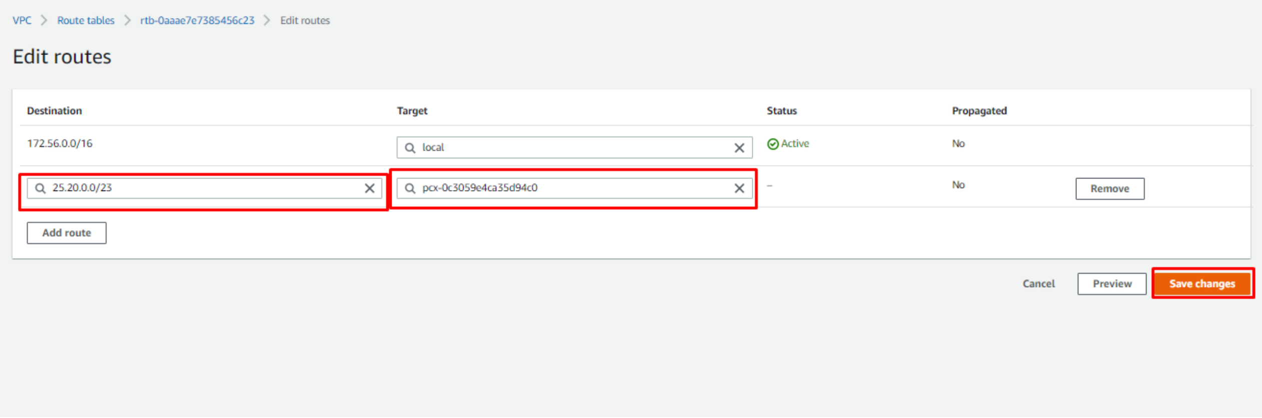
	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	edureka-private	rtb-051c5e5d3c691c100	–	–	No	vpc-0a5985ec330d2298f | edu...	045403988195
☑	vpc-01	rtb-0aaae7e7385456c23	–	–	Yes	vpc-06d88ff0d0f0a421d | vpc-...	045403988195
□	edureka-public	rtb-0f301e1bfb3171860	–	–	Yes	vpc-0a5985ec330d2298f | edu...	045403988195
□	vpc-02	rtb-09454acda64e0d105	–	–	Yes	vpc-06bffefbc8891c8b8 | vpc-02	045403988195
□	–	rtb-0841c338fcd35122f	–	–	Yes	vpc-07cf0ae89e6774f1a	045403988195

Routes (1)

Filter routes | Both

Destination	Target	Status	Propagated
172.56.0.0/16	local	✓ Active	No

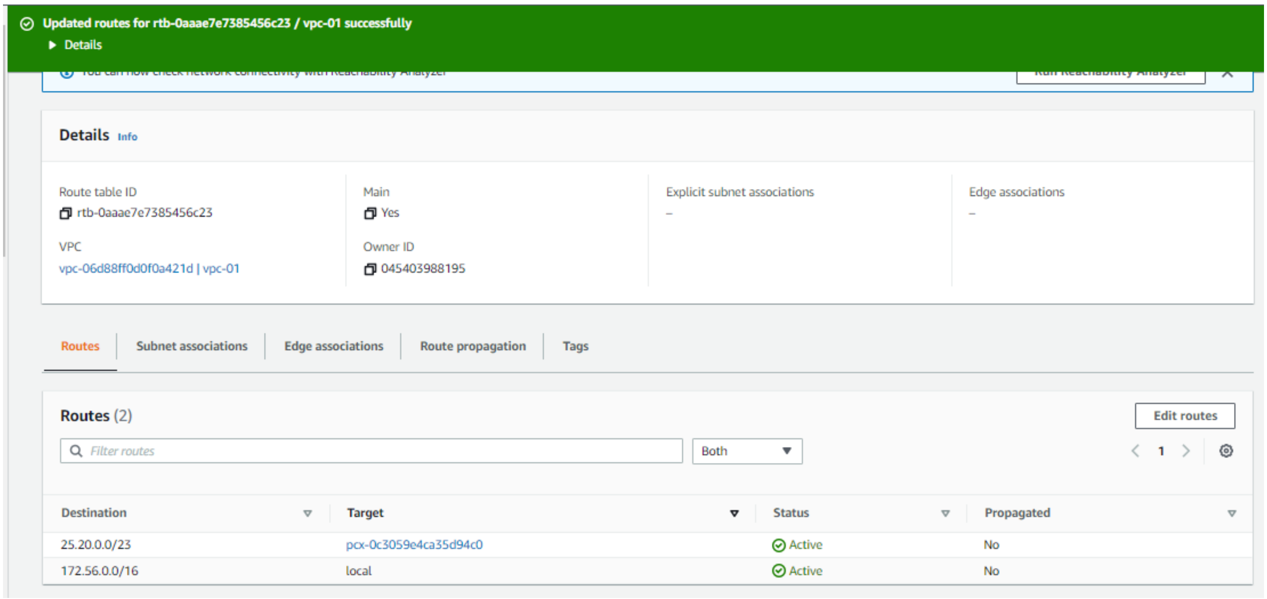
While selecting Target, select **peering connection**



Edit routes

Destination	Target	Status	Propagated
172.56.0.0/16	local	✓ Active	No
25.20.0.0/23	pcx-0c3059e4ca35d94c0	–	No

Our route has been updated as shown below



Updated routes for rtb-0aaae7e7385456c23 / vpc-01 successfully

▶ Details

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-0aaae7e7385456c23

Main: Yes

Explicit subnet associations: –

Edge associations: –

VPC: vpc-06d88ff0d0f0a421d | vpc-01

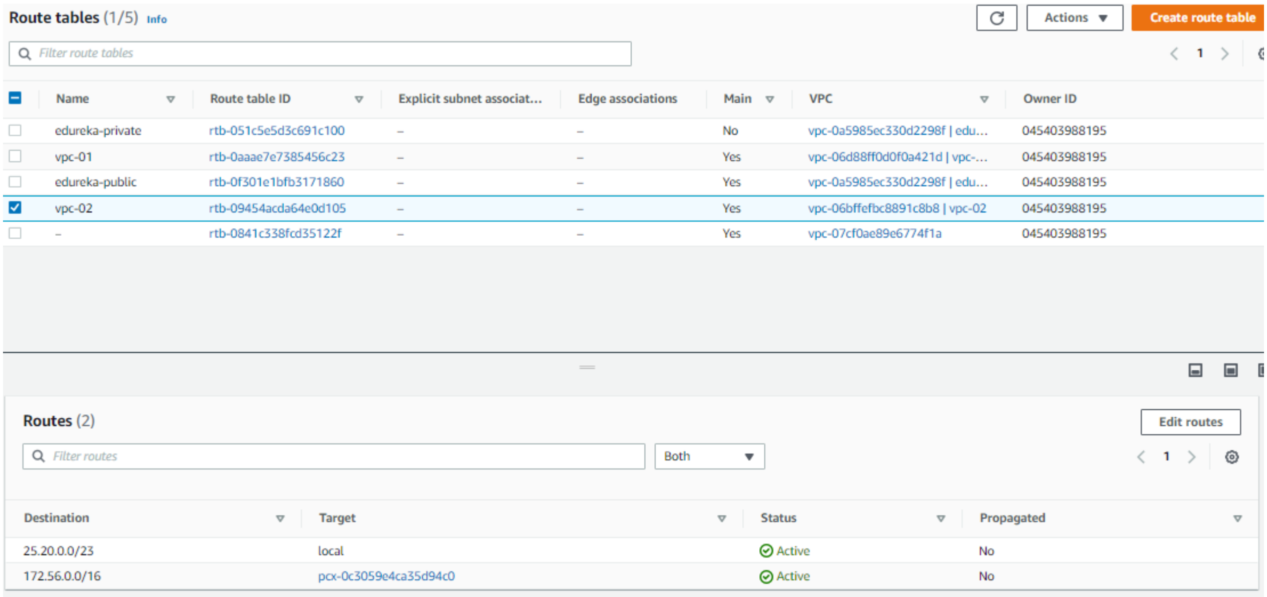
Owner ID: 045403988195

Routes (2)

Filter routes | Both

Destination	Target	Status	Propagated
25.20.0.0/23	pcx-0c3059e4ca35d94c0	✓ Active	No
172.56.0.0/16	local	✓ Active	No

- Similarly, update the route tables of the another VPC



Route tables (1/5)

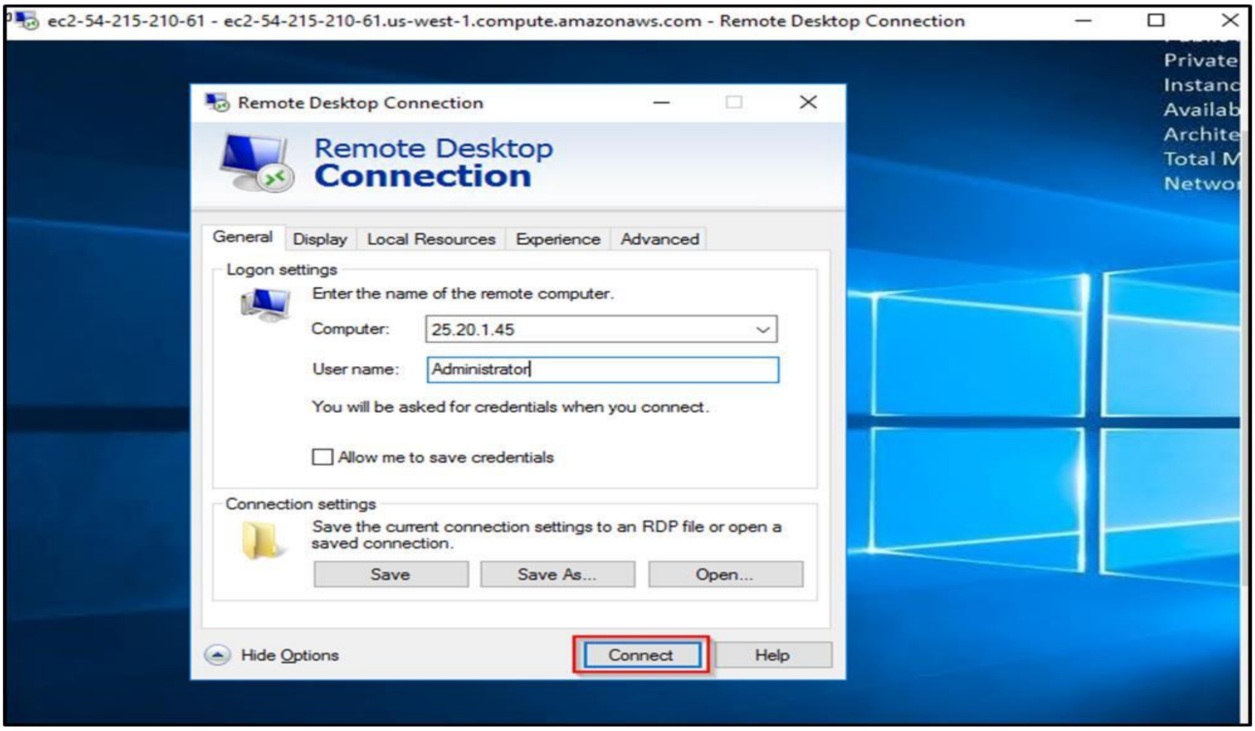
☐	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
☐	edureka-private	rtb-051c5e5d3c691c100	–	–	No	vpc-0a5985ec330d2298f | edu...	045403988195
☐	vpc-01	rtb-0aaae7e7385456c23	–	–	Yes	vpc-06d88ff0d0f0a421d | vpc-...	045403988195
☐	edureka-public	rtb-0f301e1bfb3171860	–	–	Yes	vpc-0a5985ec330d2298f | edu...	045403988195
☑	vpc-02	rtb-09454acda64e0d105	–	–	Yes	vpc-06bffefbc8891c8b8 | vpc-02	045403988195
☐	–	rtb-0841c338fcd35122f	–	–	Yes	vpc-07cf0ae89e6774f1a	045403988195

Routes (2)

Destination	Target	Status	Propagated
25.20.0.0/23	local	✓ Active	No
172.56.0.0/16	pcx-0c3059e4ca35d94c0	✓ Active	No

Step 4: Create a windows instance in each VPC

- Create a Windows instance in each VPC
- Connect a Windows instance in the first VPC to your localhost through **Remote manager**
- Once it gets connected, search for the remote manager in your Windows instance
- In computer, type the private IP of the windows instance in the other VPC
- Give the user name as the **Administrator**



ec2-54-215-210-61 - ec2-54-215-210-61.us-west-1.compute.amazonaws.com - Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: 25.20.1.45

User name: Administrator

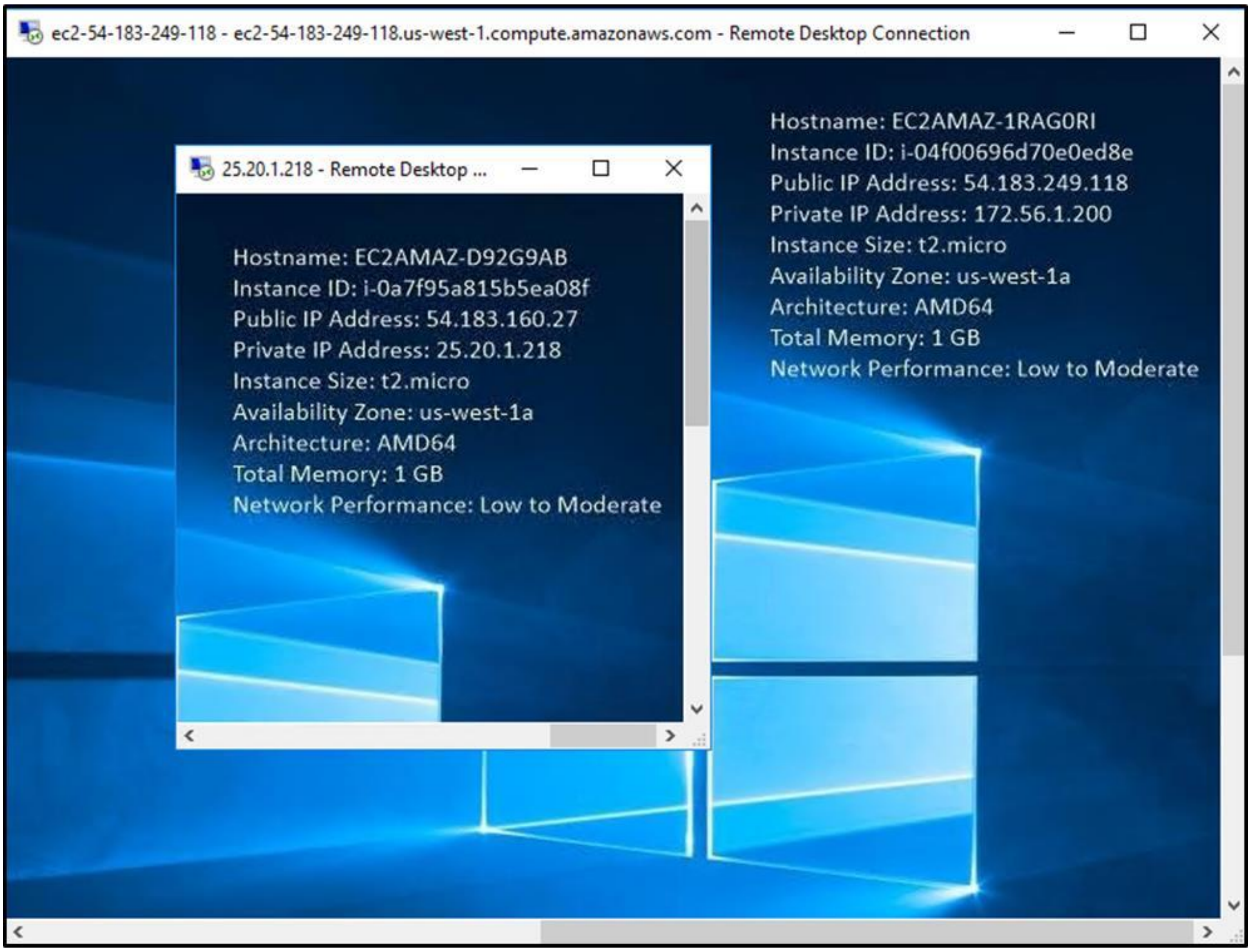
You will be asked for credentials when you connect.

☐ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

- Give the password that was allotted to you while decrypting your **.pem** file
- Now, the instance in different VPCs can communicate with each other through VPC peering


ec2-54-183-249-118 - ec2-54-183-249-118.us-west-1.compute.amazonaws.com - Remote Desktop Connection
25.20.1.218 - Remote Desktop ...

Hostname: EC2AMAZ-D92G9AB
Instance ID: i-0a7f95a815b5ea08f
Public IP Address: 54.183.160.27
Private IP Address: 25.20.1.218
Instance Size: t2.micro
Availability Zone: us-west-1a
Architecture: AMD64
Total Memory: 1 GB
Network Performance: Low to Moderate

Hostname: EC2AMAZ-1RAG0RI
Instance ID: i-04f00696d70e0ed8e
Public IP Address: 54.183.249.118
Private IP Address: 172.56.1.200
Instance Size: t2.micro
Availability Zone: us-west-1a
Architecture: AMD64
Total Memory: 1 GB
Network Performance: Low to Moderate

Conclusion: We have successfully used VPC Peering to Communicate between Two Instances