

Creating Secure VPC

Amazon Virtual Private Cloud is a commercial cloud computing service that provides a virtual private cloud, by provisioning a logically isolated section of Amazon Web Services Cloud. Enterprise customers can access the Amazon Elastic Compute Cloud over an IPsec based virtual private network.

Step1 : Logging In to the Amazon Web Services Console

login to your AWS account using your credentials.

Step 2: Create VPC

1. In the AWS Management Console search bar, enter VPC, and click the VPC result under Services:
2. To start creating VPC, in the left down side, Click on **Your VPC** to Create VPC:
2. Enter VPC name and IPV4 CIDR Range Click on create VPC

The screenshot shows the AWS Management Console interface for creating a VPC. The breadcrumb navigation is 'VPC > Your VPCs > Create VPC'. The main heading is 'Create VPC' with an 'Info' link. Below this is a descriptive sentence: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' The 'VPC settings' section contains the following fields:

- Resources to create** (Info link): A note says 'Create only the VPC resource or the VPC and other networking resources.' There are two radio buttons: 'VPC only' (selected) and 'VPC and more'.
- Name tag - optional** (Info link): A note says 'Creates a tag with a key of 'Name' and a value that you specify.' The text input field contains 'Demo'.
- IPv4 CIDR block** (Info link): Two radio buttons are present: 'IPv4 CIDR manual input' (selected) and 'IPAM-allocated IPv4 CIDR block'.
- IPv4 CIDR**: A text input field contains '10.0.0.0/16'. Below it, a note states 'CIDR block size must be between /16 and /28'.
- IPv6 CIDR block** (Info link): This section is partially visible at the bottom.

An 'Activate Windows' watermark is visible in the bottom right corner of the console window.

2. Click on below button create VPC

aws Services Search [Alt+S] N. Virginia sonali chetan kur

IPv4 CIDR
10.0.0.0/24
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy Info
Default

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.

No tags associated with the resource
Add tag
You can add 50 more tags

Cancel Create VPC

Activate Windows
Go to Settings to activate Windows.

Step 3 : Create IGW

1. To start creating IGW , in the left down side, click Create Internet Gateway:
2. Give name to internet Gateway and click on create internet gateway

← → ↺ us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#CreateInternetGateway: AWS Services Search [Alt+S] N. Virginia sonali chetan kur

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.
Public 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 | Public IGW | Remove |

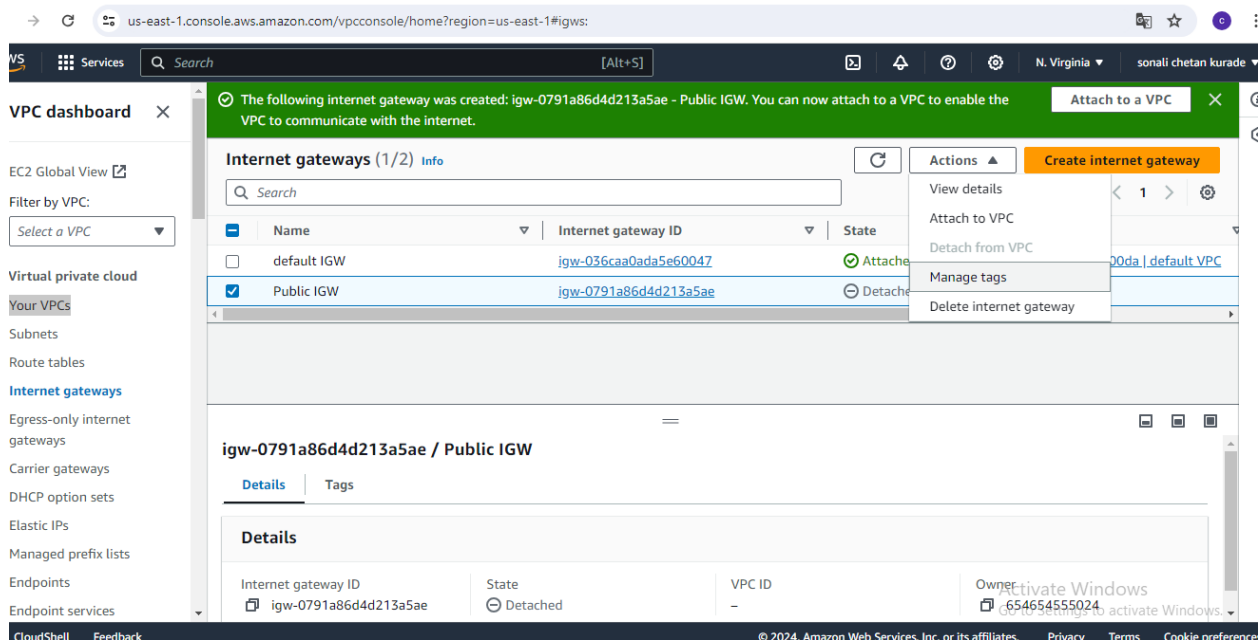
Add new tag
You can add 49 more tags.

Cancel Create internet gateway

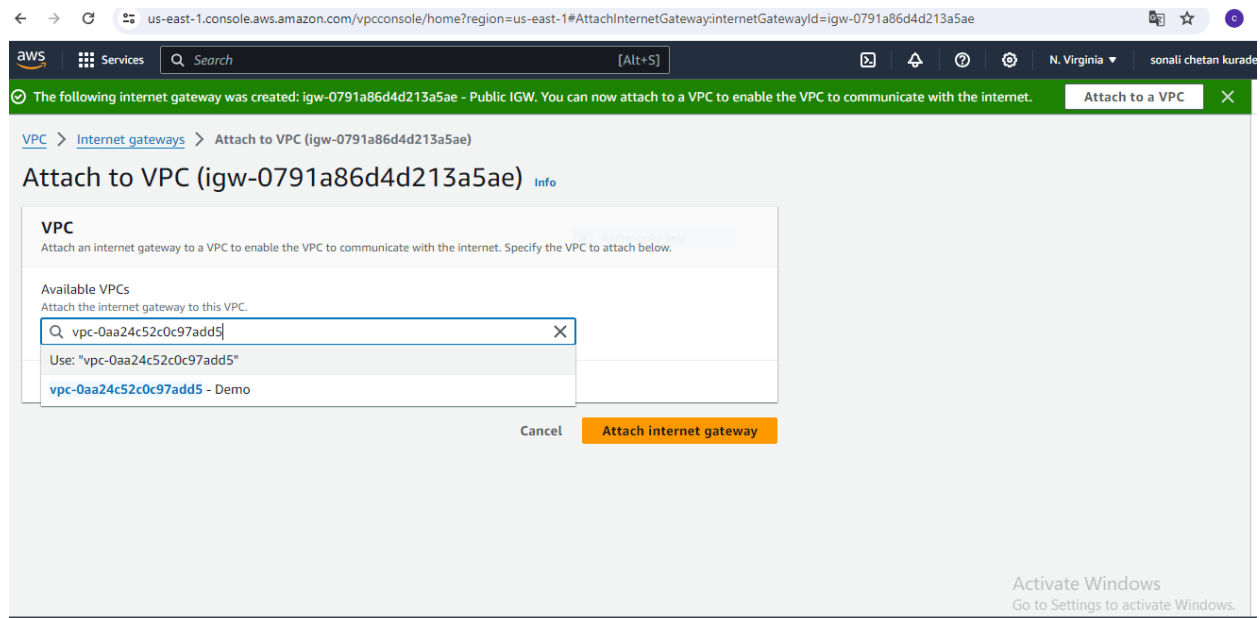
Activate Windows
Go to Settings to activate Windows.

Step 4 : Attach Your IGW to VPC

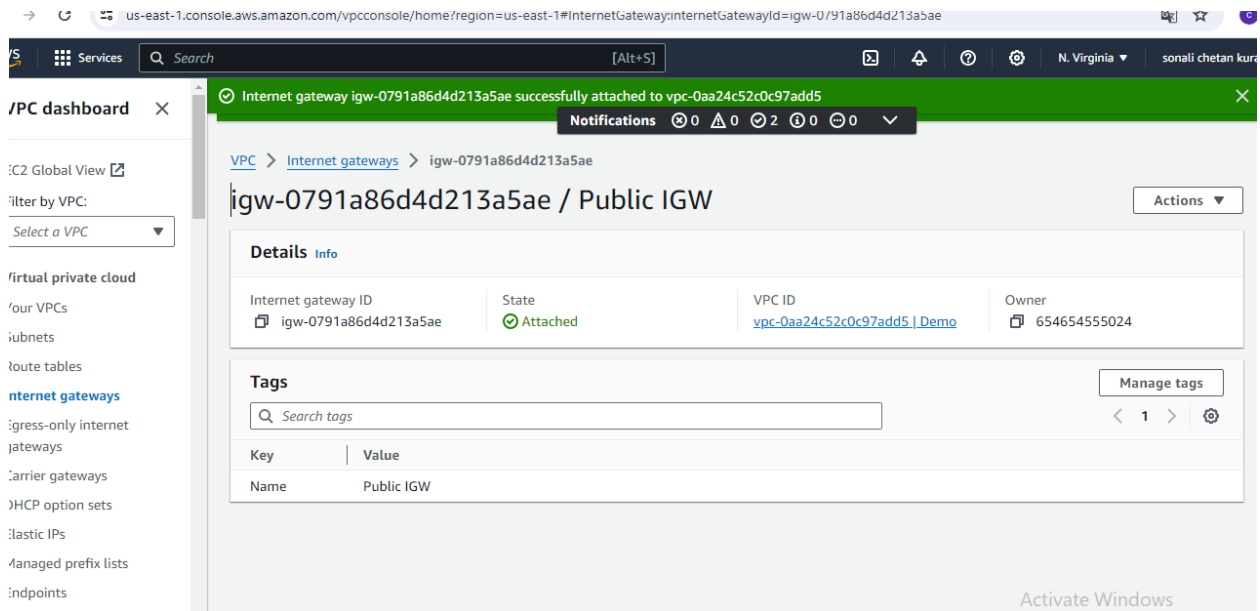
- Select IGW Which you have created recently and Click on **Action** and select option **Attach to VPC**



- Select VPC and click on **Attach internet gateway**

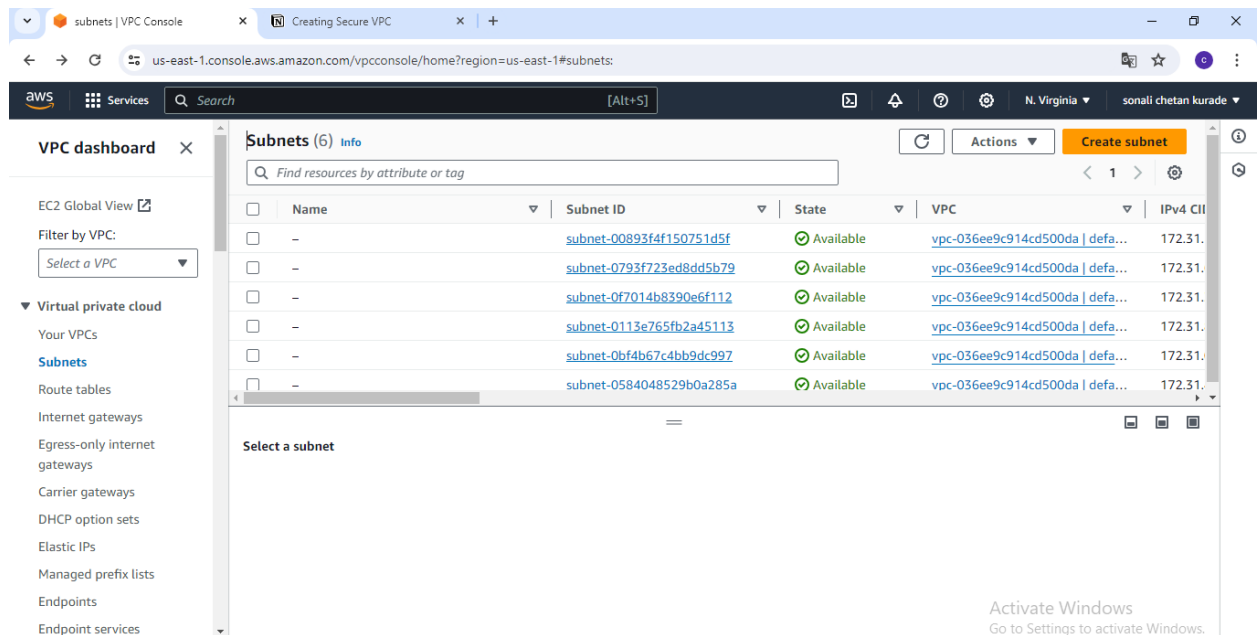


- IGW is attached successfully



Step 4 : Create Subnet

- To start creating subnet , in the left down side, click on **Create subnets**:



- Click on **Create Subnet** and select newly created vpc

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.
vpc-0aa24c52c0c97add5 (Demo)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

- Give name for that subnet and Select availability zone and enter the CIDR range

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

Public subnet

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.
US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.10.0/24 256 IPs

▼ **Tags - optional**

| Key | Value - optional | |
|------|------------------|--------|
| Name | Public subnet | Remove |

Add new tag

You can add 49 more tags.

Remove

- Click on Create subnet

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0/16

IPv4 subnet CIDR block

10.0.10.0/24 256 IPs

▼ Tags - optional

Key Value - optional

Q Name X Q Public subnet X Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

- Create another subnet that is private subnet same like above procedure.
- Finally two subnet is created

VPC dashboard

EC2 Global View

Filter by VPC: Select a VPC

▼ Virtual private cloud

- Your VPCs
- Subnets**
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints

You have successfully created 1 subnet: subnet-063de19e4bb7bd96f

Subnets (8) [Info](#)

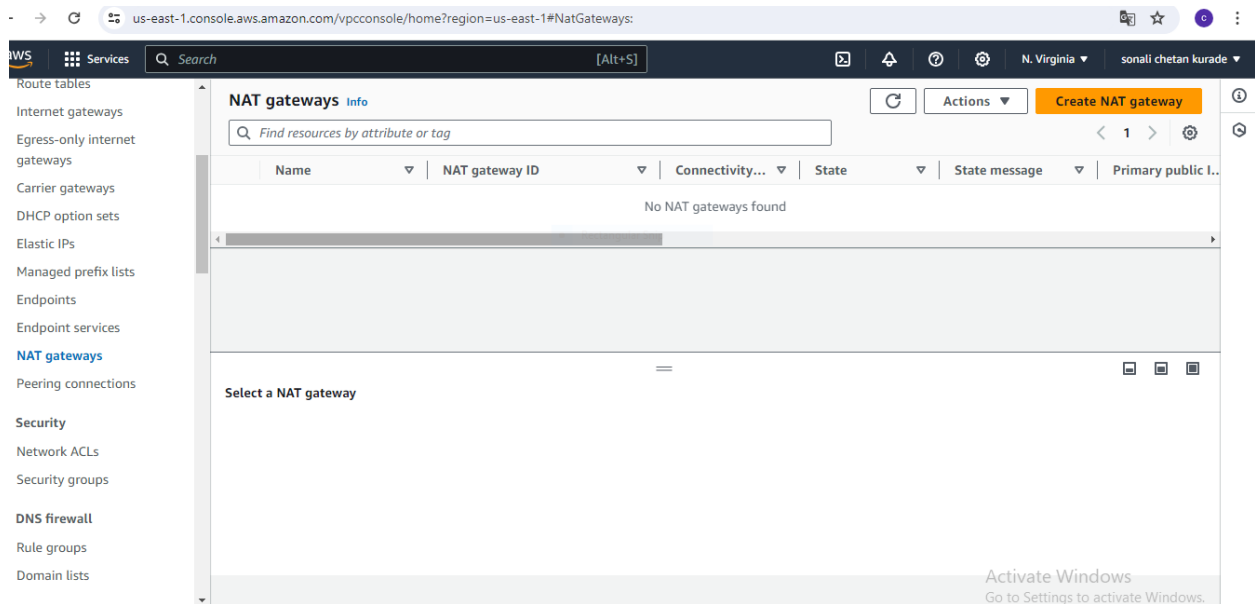
Find resources by attribute or tag

| <input type="checkbox"/> | Name | Subnet ID | State | VPC | IPv4 CII |
|--------------------------|----------------|--|-----------|---|----------|
| <input type="checkbox"/> | Private Subnet | subnet-063de19e4bb7bd96f | Available | vpc-0aa24c52c0c97add5 Demo | 10.0.20 |
| <input type="checkbox"/> | - | subnet-00893f4f150751d5f | Available | vpc-036ee9c914cd500da defa... | 172.31. |
| <input type="checkbox"/> | - | subnet-0793f723ed8dd5b79 | Available | vpc-036ee9c914cd500da defa... | 172.31. |
| <input type="checkbox"/> | Public subnet | subnet-00dded0cc10961eaa | Available | vpc-0aa24c52c0c97add5 Demo | 10.0.10 |
| <input type="checkbox"/> | - | subnet-0f7014b8390e6f112 | Available | vpc-036ee9c914cd500da defa... | 172.31. |

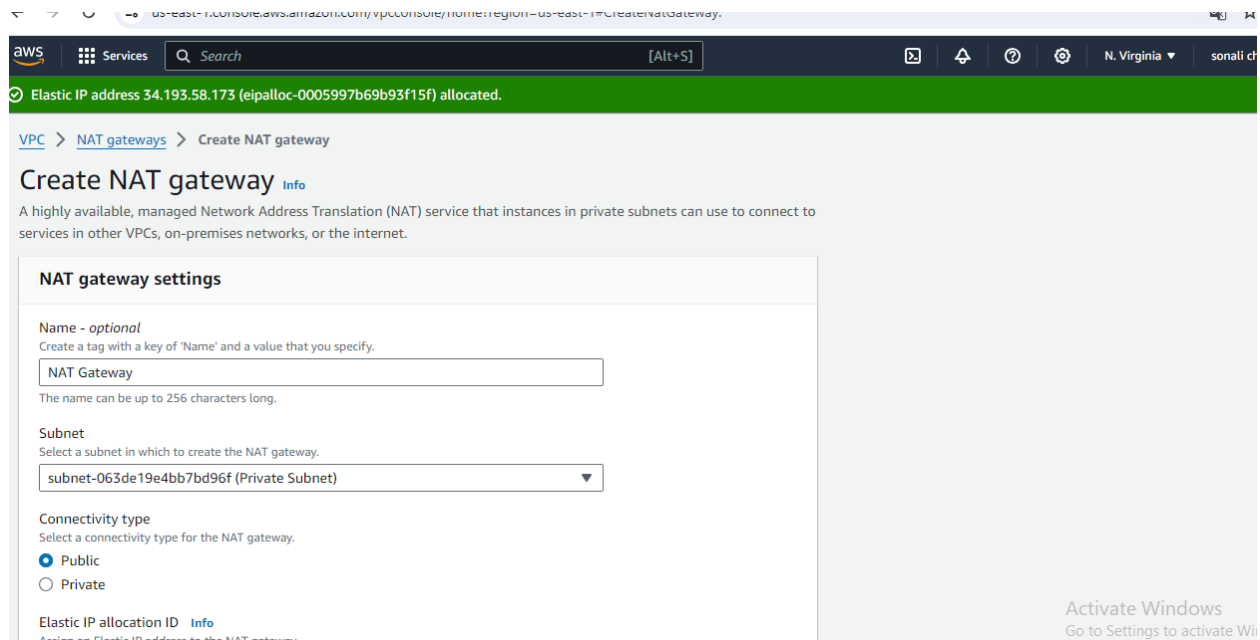
Select a subnet

Step 5: Create NAT Gateway

- To start creating NAT Gateway , in the left down side, click on Create **NAT Gateways**:



- Click on create **NAT Gateway** give name for that and select private subnet



- Allocate Elastic IP and click on create NAT gateway

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateNatGateway:

Elastic IP address 34.193.58.173 (eipalloc-0005997b69b93f15f) allocated.

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.

[Reallocate Elastic IP](#) [Allocate Elastic IP](#)

► **Additional settings** [Info](#)

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

[Remove](#)

[Add new tag](#)
You can add 49 more tags.

[Cancel](#) [Create NAT gateway](#)

Activate Windows
Go to Settings to activate Windows.

Step 6: Create Route table

- To start creating Route table, in the left down side, click on Create **Route Table** :

CreateRouteTable | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateRouteTable:

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings [Reallocate Elastic IP](#)

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

VPC
The VPC to use for this route table.

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

[Remove](#)

[Add new tag](#)

Activate Windows
Go to Settings to activate Windows.

- Select Vpc and Click on **Create route table**

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#CreateRouteTable:

Route table settings

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

VPC
The VPC to use for this route table.
vpc-0aa24c52c0c97add5 (Demo)

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
Remove

Add new tag
You can add 49 more tags.

Cancel Create route table

- Route table is created successfully. Same ways you have to create two route tables and add route to it.

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-0c0c135da373e4490

VPC dashboard

EC2 Global View

Filter by VPC:
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

RouteTableDetails > Route tables > rtb-0c0c135da373e4490

rtb-0c0c135da373e4490 / Private RT

Details info

| | | | |
|---|--------------------------|-----------------------------------|------------------------|
| Route table ID rtb-0c0c135da373e4490 | Main No | Explicit subnet associations - | Edge associations - |
| VPC vpc-0aa24c52c0c97add5 Demo | Owner ID 654654555024 | | |

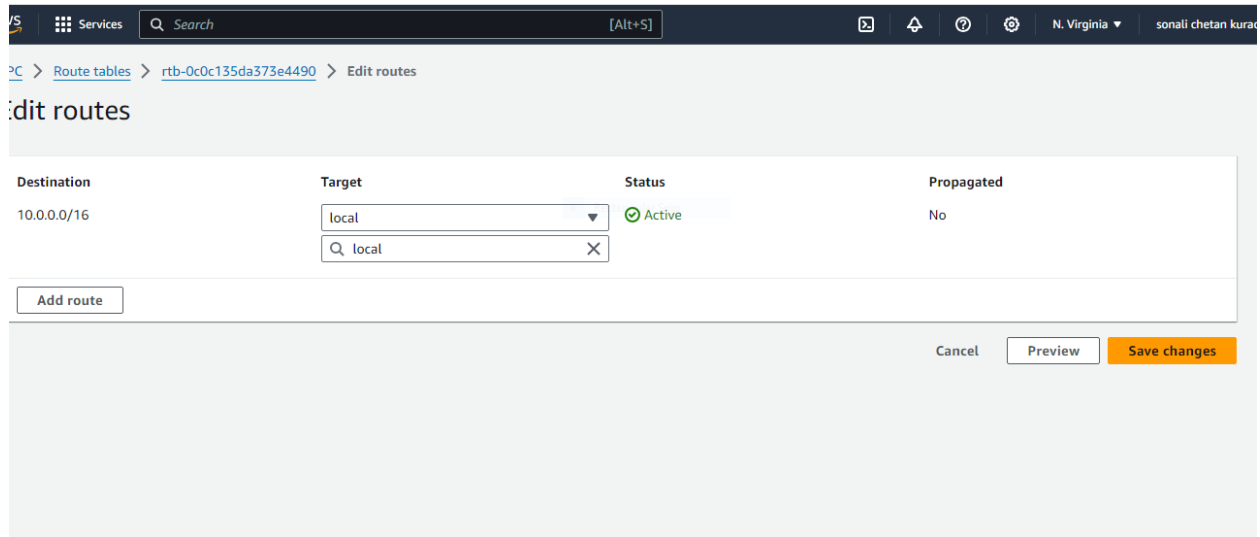
Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

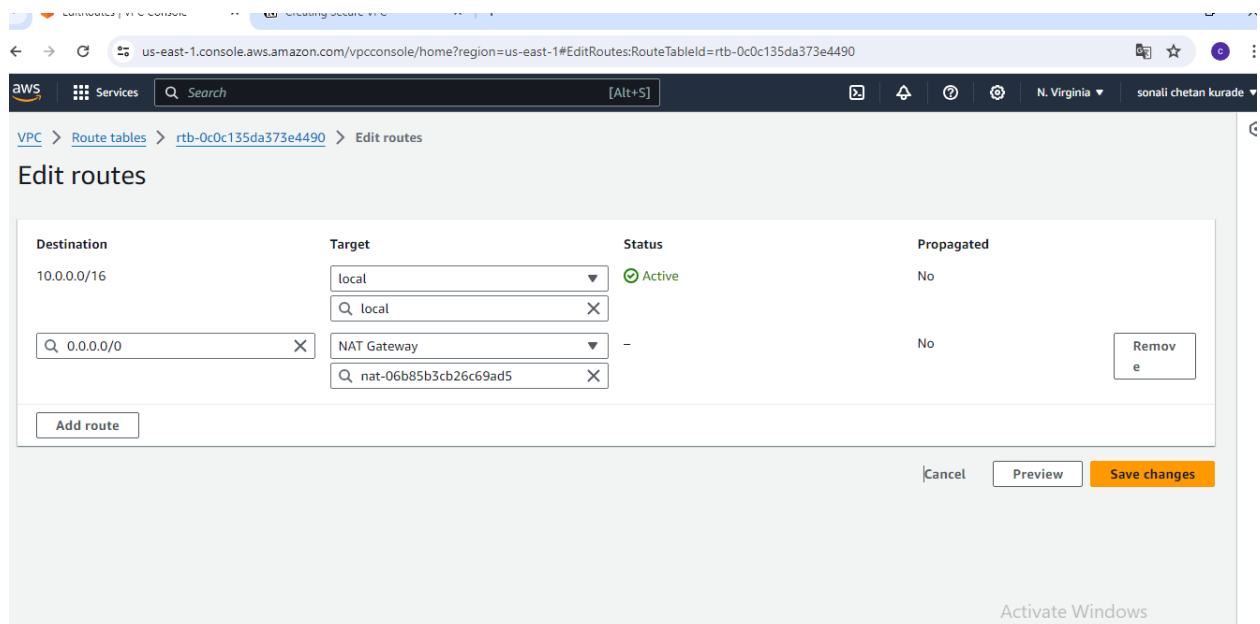
Filter routes

| Destination | Target | Status | Propag... |
|-------------|--------|--------|-----------|
| 10.0.0.0/16 | local | Active | No |

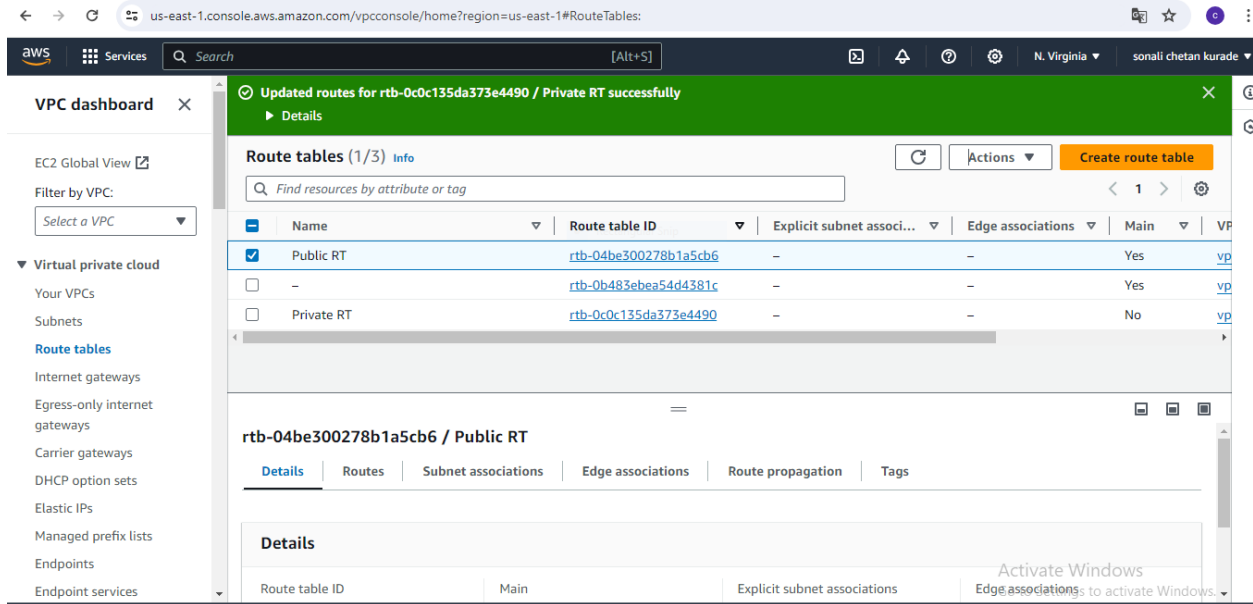
- To add the Route in route table go inside the route table and select option **Edit route**



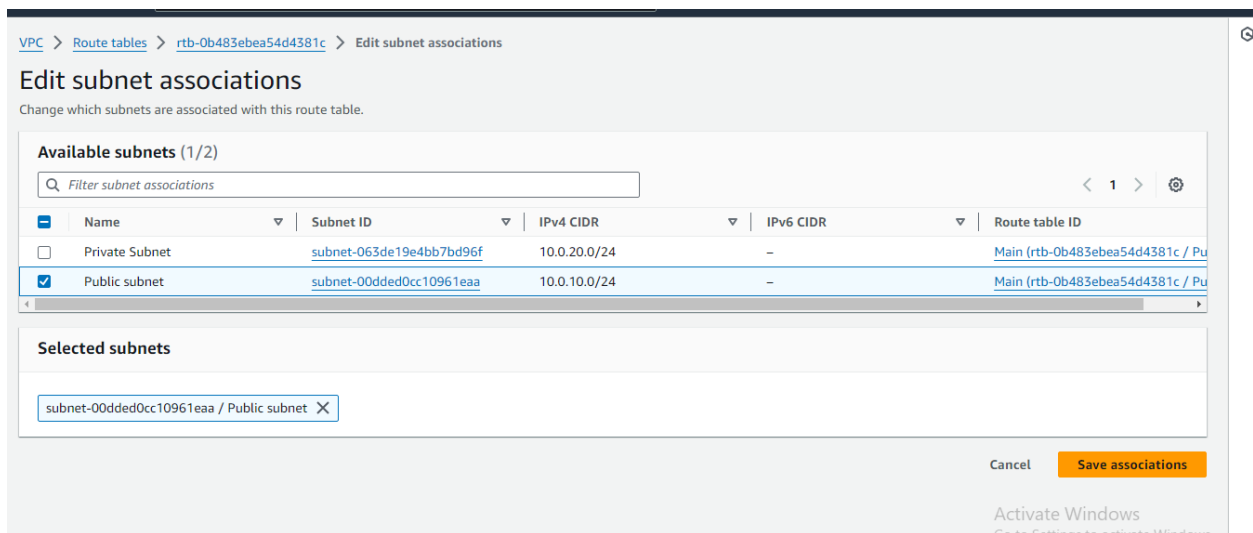
- Click on **Add Route** add route into it.
- select destination 0.0.0.0/0 (anywhere) and target is NAT gateway in private route table
- select destination 0.0.0.0/0 (anywhere) and target is Internet gateway in public route table



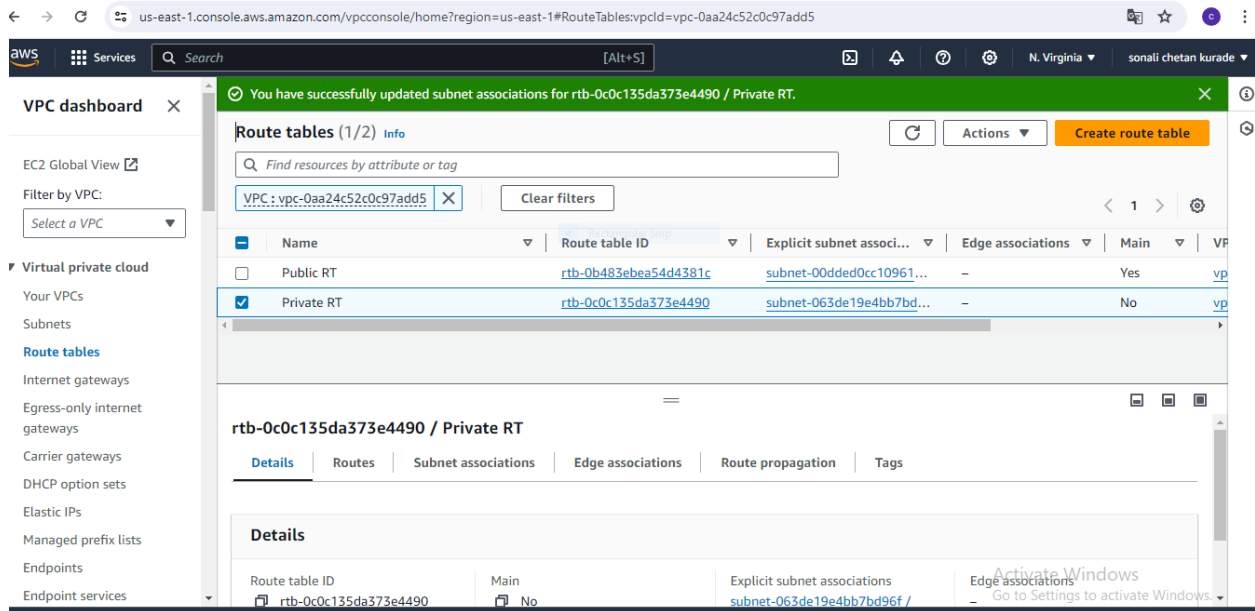
- Attach Route table to Subnet



- Click on Action and select the option **Edit Subnet Association** select the **subnet**

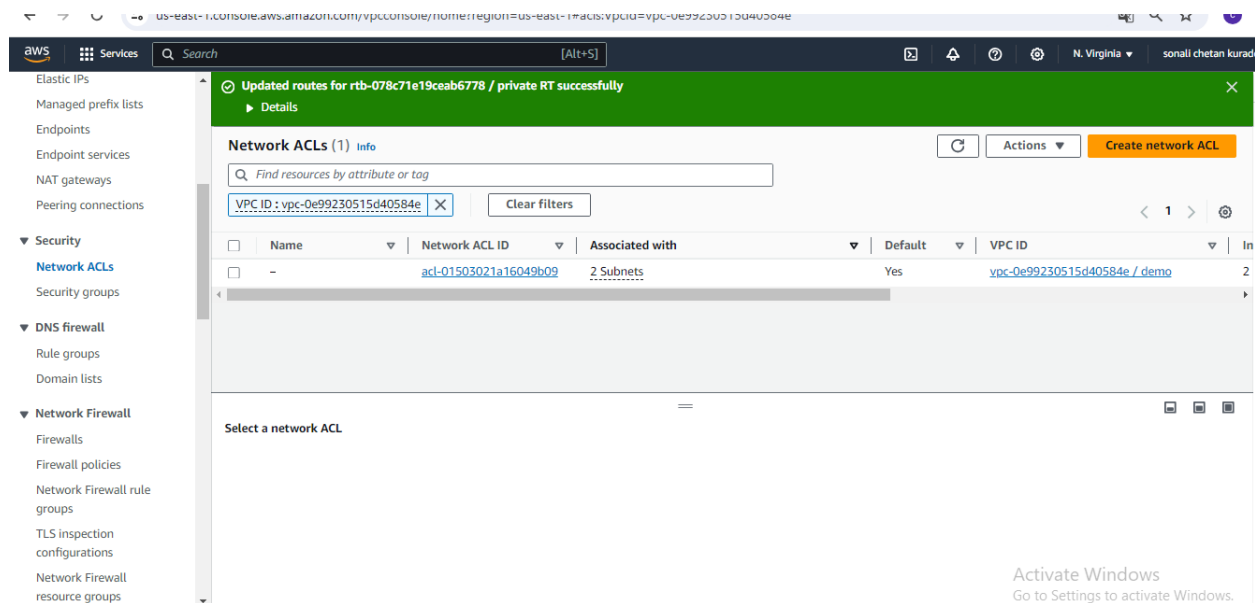


- Attached successfully



Step 7: Creating NACL

- To start creating NACL, in the left down side, click on **Network ACL**. Click on **Create network ACL**



- Enter the details like Name and VPC and click on **Create network ACL**

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#CreateNetworkACL

aws Services Search [Alt+S]

VPC > Network ACLs > Create network ACL

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

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

Demo-NACL

VPC
VPC to use for this network ACL.

vpc-036ee9c914cd500da (default 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 **Value - optional**

Q Name X Q Demo-NACL X Remove tag

Add tag

You can add 49 more tags

Cancel Create network ACL

Activate Windows
Go to Settings to activate Windows.

- Attach this NACL to Private subnet. Select NACL which we have created previously and click on **action**. Select the option **Edit subnet association**.

us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#acIs:VpcId=vpc-0e99230515d40584e

aws Services Search [Alt+S]

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups
- DNS firewall
- Rule groups

Network ACLs (1/2) Info

Find resources by attribute or tag

VPC ID: vpc-0e99230515d40584e X Clear filters

| | Name | Network ACL ID | Associated with | Default | VPC ID | In |
|-------------------------------------|-----------|-----------------------|-----------------|---------|------------------------------|----|
| <input type="checkbox"/> | - | acl-01503021a16049b09 | 2 Subnets | Yes | vpc-0e99230515d40584e / demo | 2 |
| <input checked="" type="checkbox"/> | Demo-NACL | acl-0813c8c319fd13eaf | - | No | vpc-0e99230515d40584e / demo | 1 |

acl-0813c8c319fd13eaf / Demo-NACL

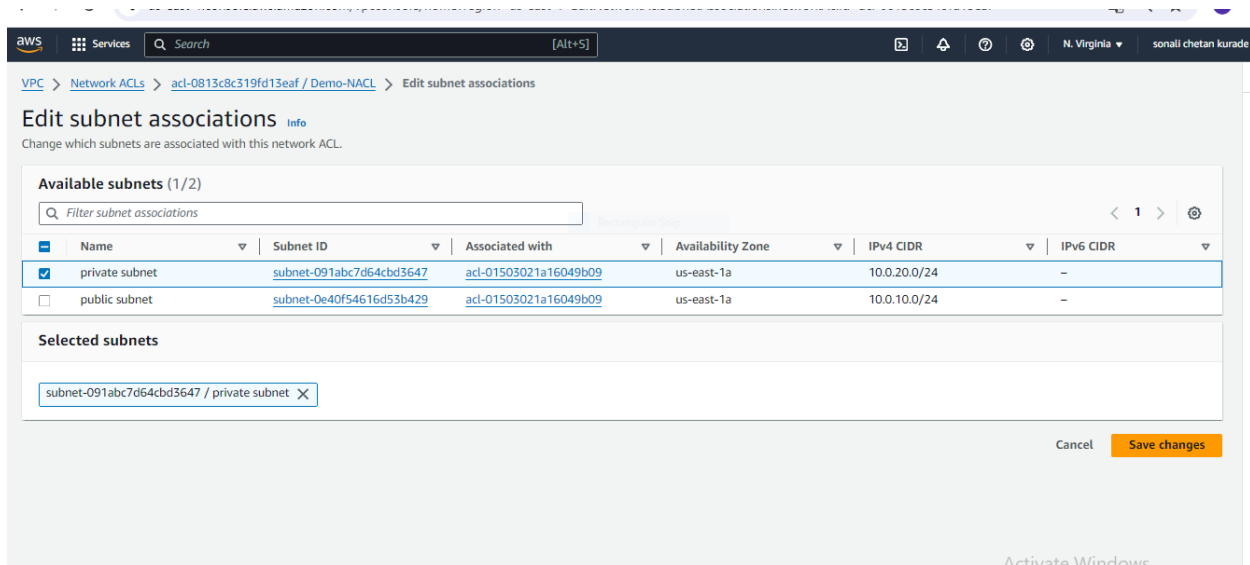
Details Inbound rules Outbound rules Subnet associations Tags

Details

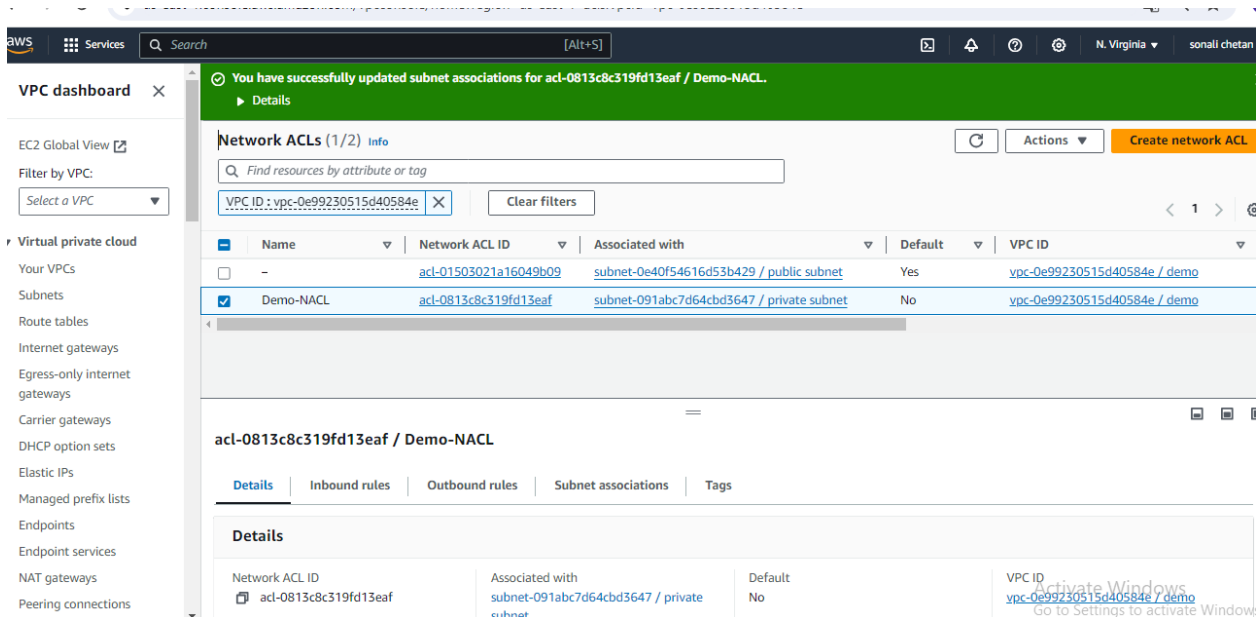
| | | | |
|-----------------------|-----------------|---------|------------------------------|
| Network ACL ID | Associated with | Default | VPC ID |
| acl-0813c8c319fd13eaf | - | No | vpc-0e99230515d40584e / demo |
| Owner | | | |

Activate Windows
Go to Settings to activate Windows.

- Select private subnet and click on **save changes**



- subnet Association is completed successfully



Step 8: Creating Bastion host

- In the AWS Management Console search bar, enter EC2, and click the EC2 result under Services:
- To start creating Bastion host, in the left down side, click on **Instances**. Click on **Launch Instance**
- Give the name **bastion** and select the Image

- Select the key Pair
- Click on Edit Network
- Select the VPC and public Subnet
- Enable the **Auto-assign public IP**
- Create a Security Group. Give name to that security group (bastion-sg) and description

The screenshot shows the AWS Management Console interface for launching instances. The 'Network settings' section is expanded, showing the following configurations:

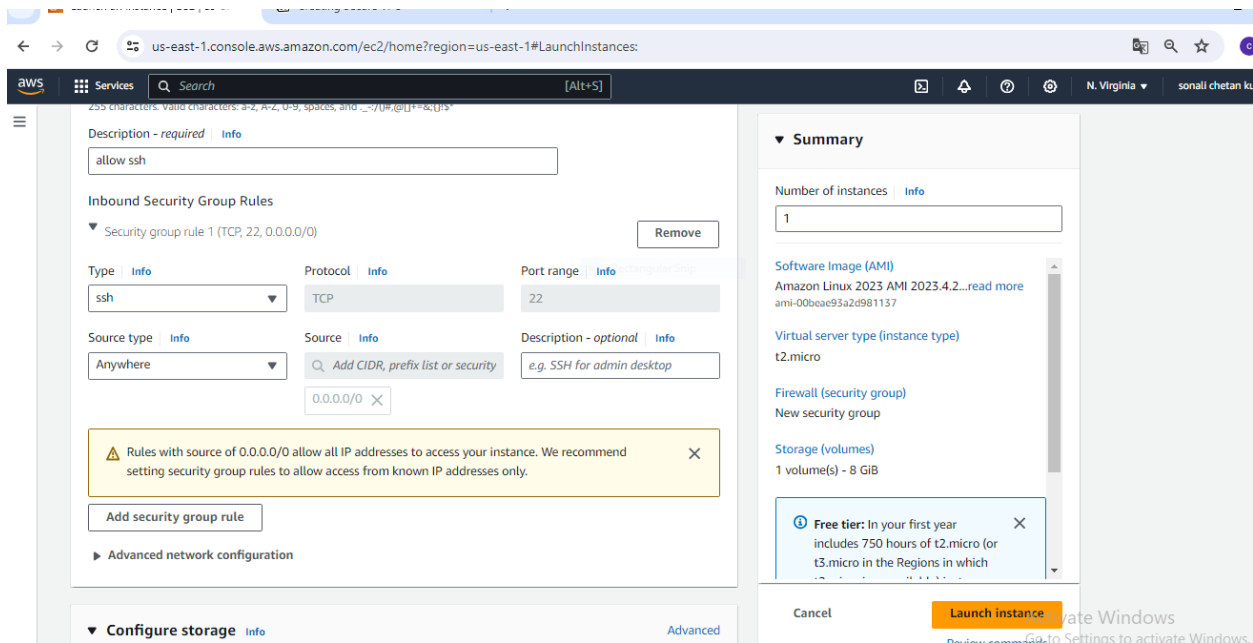
- VPC - required:** vpc-0e99230515d40584e (demo) with CIDR 10.0.0.0/16.
- Subnet:** subnet-0e40f54616d53b429 (public subnet) with CIDR 10.0.10.0/24.
- Auto-assign public IP:** Set to 'Enable'.
- Firewall (security groups):** The 'Create security group' radio button is selected. The security group name is 'Bastion-sg' and the description is 'allow ssh'.

The 'Summary' section on the right shows the following details:

- Number of instances:** 1
- Software Image (AMI):** Amazon Linux 2023 AMI 2023.4.2...
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** New security group
- Storage (volumes):** 1 volume(s) - 8 GiB

At the bottom right, there is a 'Launch instance' button and a 'Free tier' notification stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which...)'.

- Add the inbound rule and click on **launch instance** to launch instance.



Step 9 : Creating Database Server

- In the AWS Management Console search bar, enter EC2, and click the EC2 result under Services:
- To start creating Bastion host, in the left down side, click on **Instances**. Click on **Launch Instance**
- Give the name **Database** and select the Image
- Select the key Pair
- Click on Edit Network
- Select the VPC and private Subnet
- Disable the **Auto-assign public IP**
- Create a Security Group. Give name to that security group(database-sg) and and description

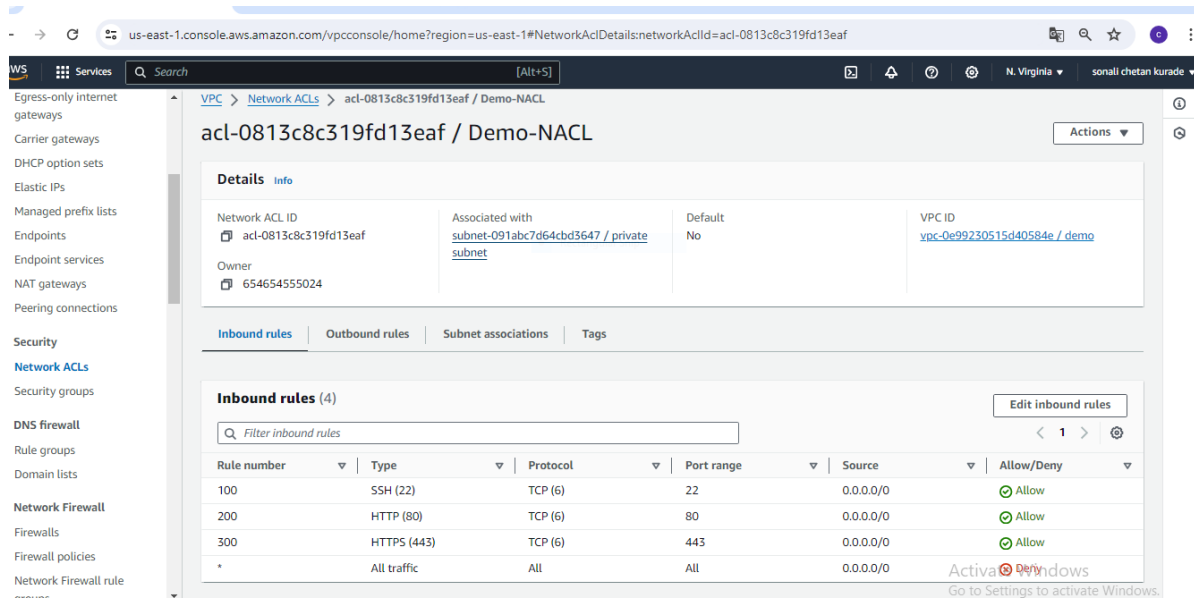
- Add the Inbound rule ssh,http,https and click on **launch instance**

| Security group rule ID | Type | Protocol | Port range | Source | Description - optional |
|------------------------|-------|----------|------------|---------|------------------------|
| sg-0065f1d5e1e90e449 | SSH | TCP | 22 | Custom | sg-0cd9541e5f6349e00 |
| sg-04fafb0192e128e0a | HTTP | TCP | 80 | Anyw... | 0.0.0.0/0 |
| sg-0d8ea09bd4658baee | HTTPS | TCP | 443 | Anyw... | 0.0.0.0/0 |

Step 10 : Add the Inbound and Outbound Rules to in NACL

- In the left down side, click on **Network ACL**. Select the NACL which we have created.

- And add inbound rule and click edit inbound rule after adding the rule click on save changes
 - ssh
 - http
 - https



- And add outbound rule
 - http
 - https

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditOutboundRules:networkAclId=acl-0813c8c319fd13eaf

aws Services Search [Alt+S] N. Virginia sonali.chetan.kurade

VPC > Network ACLs > acl-0813c8c319fd13eaf / Demo-NACL > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

| Rule number <small>Info</small> | Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Destination <small>Info</small> | Allow/Deny <small>Info</small> | |
|---------------------------------|--------------------------|------------------------------|-----------------------------------|---------------------------------|--------------------------------|-------------------------|
| 100 | HTTP (80) | TCP (6) | 80 <small>Port Range Help</small> | 0.0.0.0/0 | Allow | <button>Remove</button> |
| 200 | HTTPS (443) | TCP (6) | 443 | 0.0.0.0/0 | Allow | <button>Remove</button> |
| * | All traffic | All | All | 0.0.0.0/0 | Deny | |

Add new rule Sort by rule number

Cancel Preview changes Save changes

Activate Windows
Go to Settings to activate Windows.