Gautham Srinivasan

IT Analyst - DTCC

04 Nov 2024

AWS Multi-Region VPC Peering Setup with Private and Public Subnet Instances

Project Overview

The objective of this documentation is to guide through the process of setting up a multi-region AWS Virtual Private Cloud (VPC) architecture with peering connections between two regions. This includes creating and configuring VPCs, subnets, internet gateways, NAT gateways, security groups, and EC2 instances in both Ohio (Zone A) and Mumbai (Zone B) regions. The configuration ensures that instances in the private subnets across regions can securely communicate with each other, simulating a private, interconnected network between geographically separated VPCs.

Prerequisites

AWS Account:

- You must have an active AWS account with permissions to create and manage VPCs, subnets, route tables, internet gateways, NAT gateways, security groups, and EC2 instances.

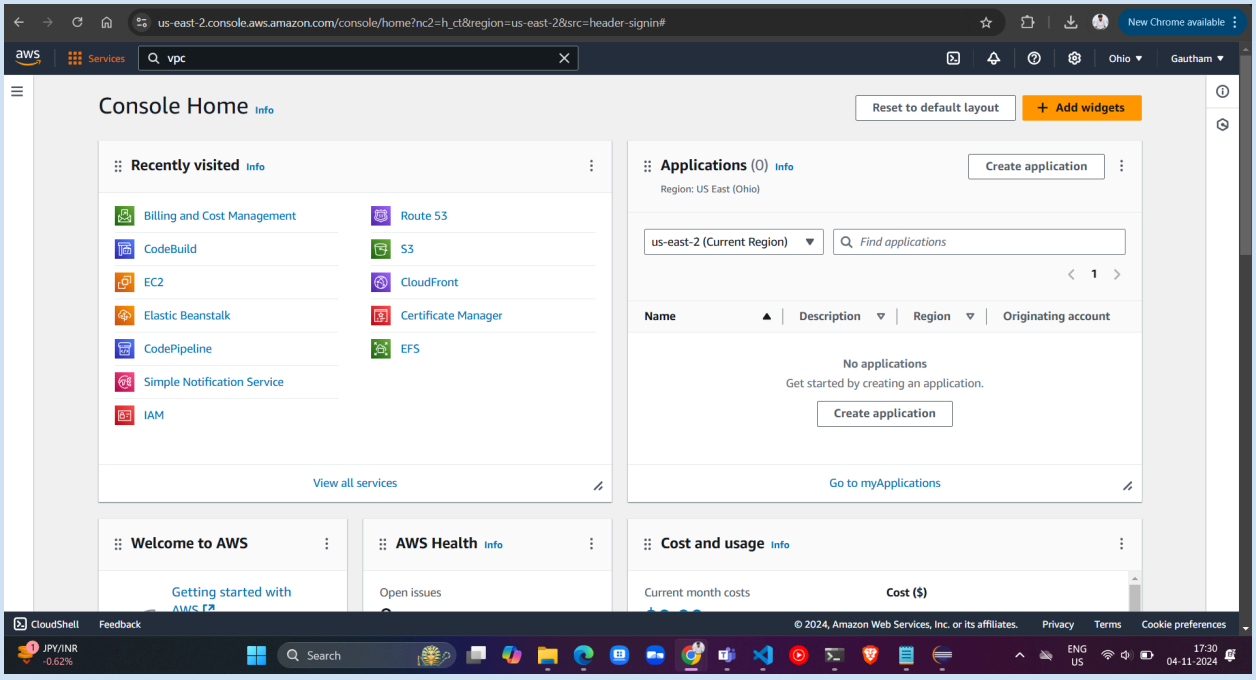
IAM User Permissions:

- The user performing this setup should have permissions for the following AWS services:
    - VPC, Subnet, Route Table, Internet Gateway, NAT Gateway, Peering Connections, Security Group, and EC2.

Procedures

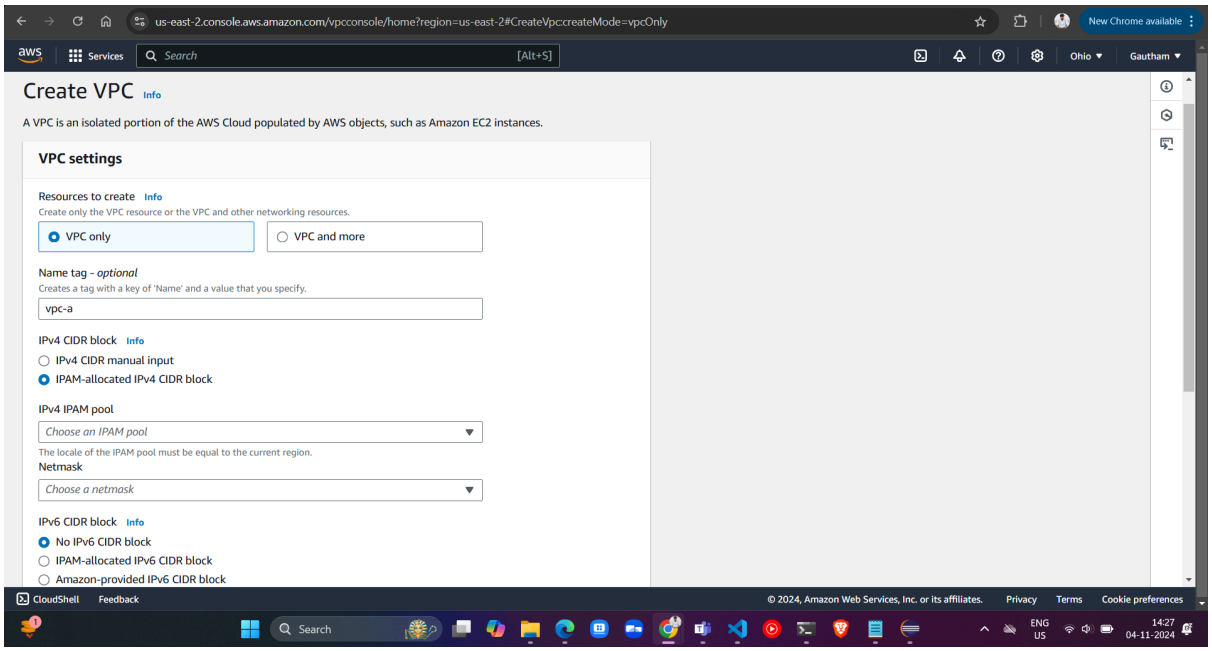
Step 1: Login to AWS Account

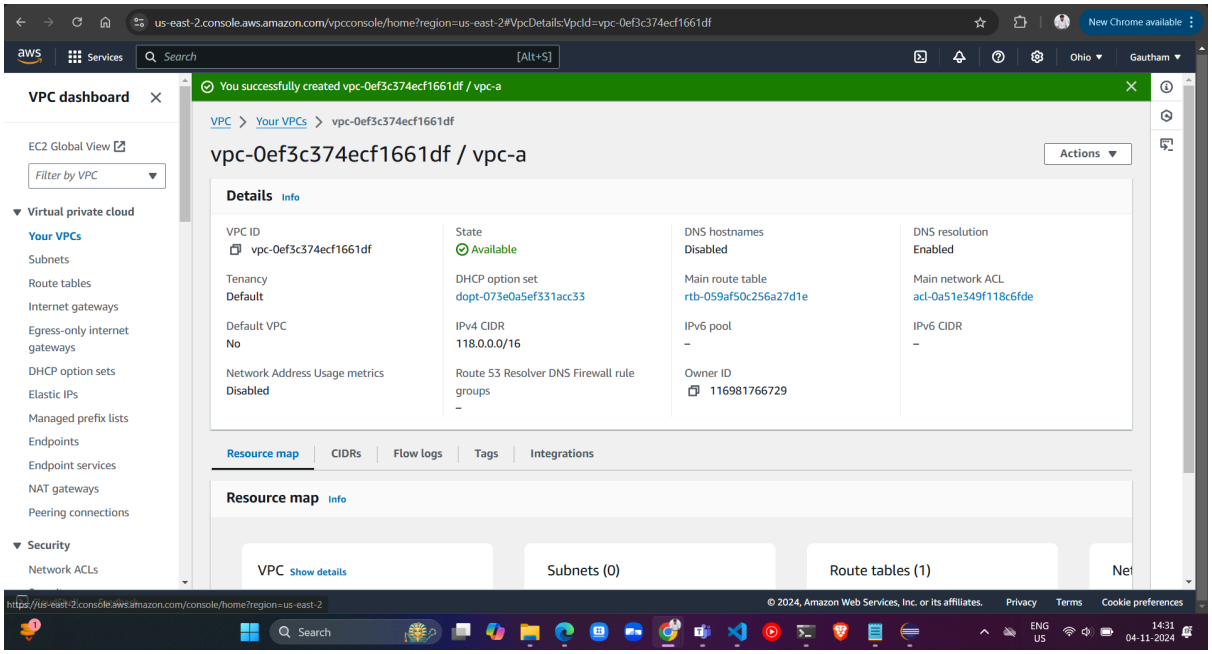
- Log in to your AWS Management Console.



Step 2: Create a VPC in Zone A (Ohio)

- **Navigate to VPC Service**:
  - Go to **VPC** service dashboard and click **Create VPC**.
- **VPC Settings**:
  - Select **VPC Only**.
  - **Name Tag**: Enter `vpc-a`.
  - **IPv4 CIDR Manual Input**: Enter `118.0.0.0/16`.
  - Click **Create VPC**.





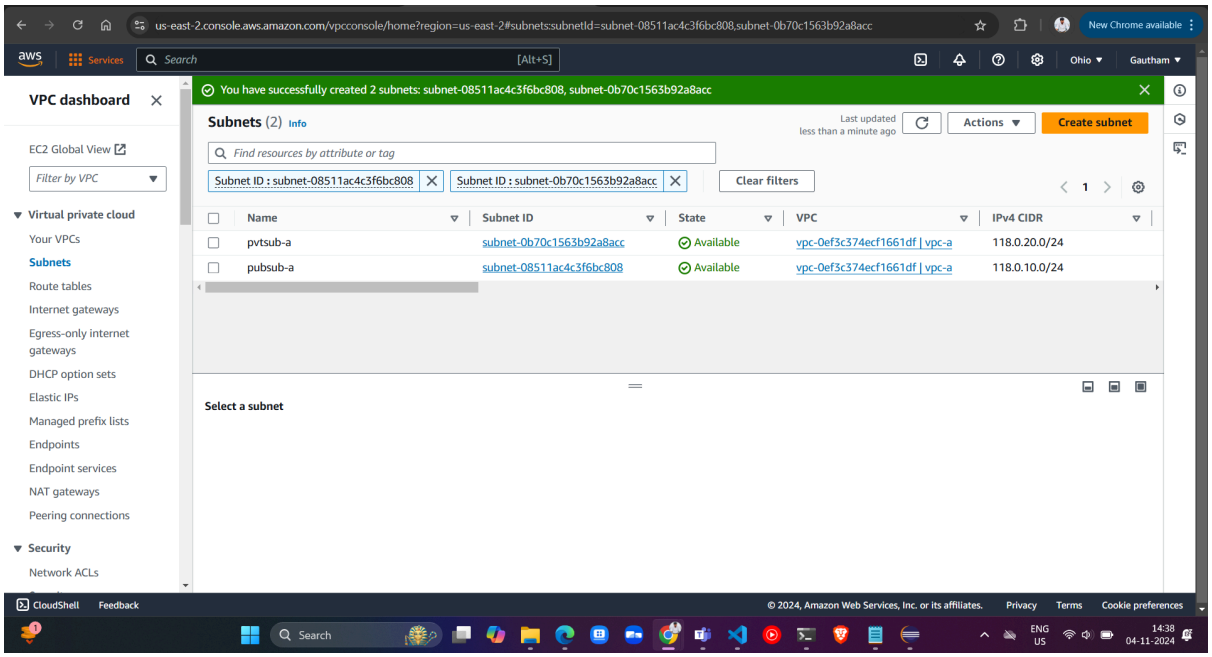
Step 3: Create Subnets in VPC-A

Public Subnet:

- Go to **Subnets** and click **Create subnet**.
- **VPC ID**: Choose `vpc-a`.
- **Subnet Name**: Enter `pubsub-a`.
- **Availability Zone**: Select `us-east-2a`.
- **IPv4 CIDR Block**: Enter `118.0.10.0/24`.

Private Subnet:

- Add another subnet.
- **Subnet Name**: Enter `pvtsub-a`.
- **Availability Zone**: Select `us-east-2b`.
- **IPv4 CIDR Block**: Enter `118.0.20.0/24`.
- Click **Create subnet**.

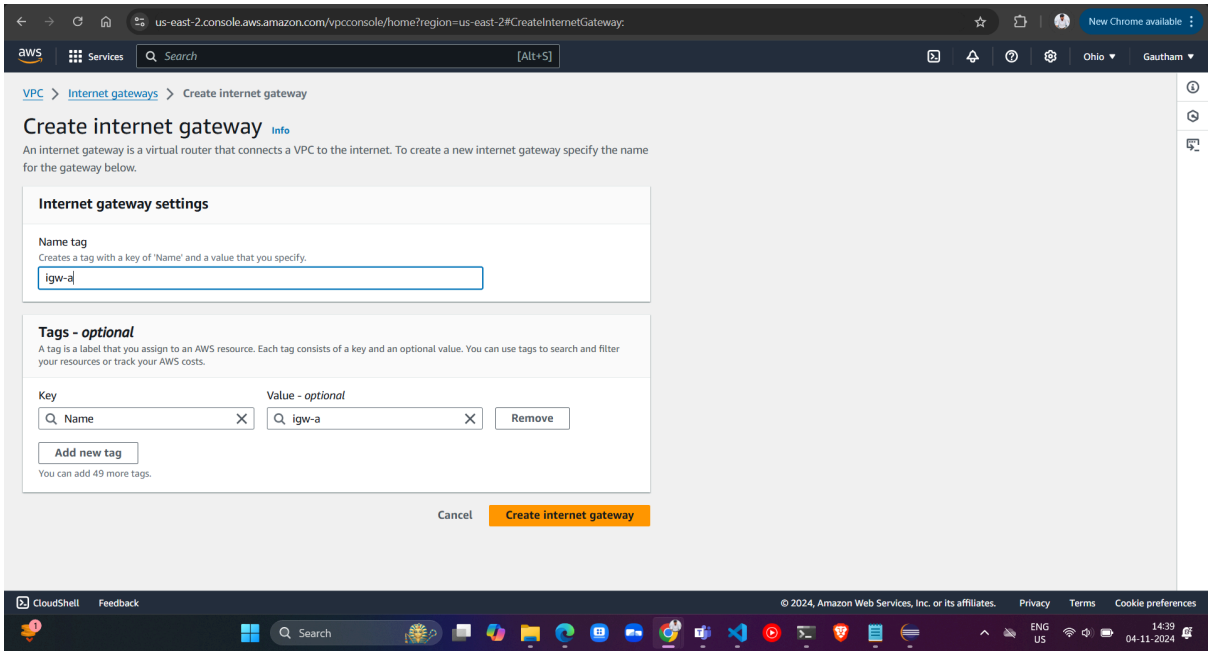


Step 4: Create and Attach Internet Gateway

Public Subnet:

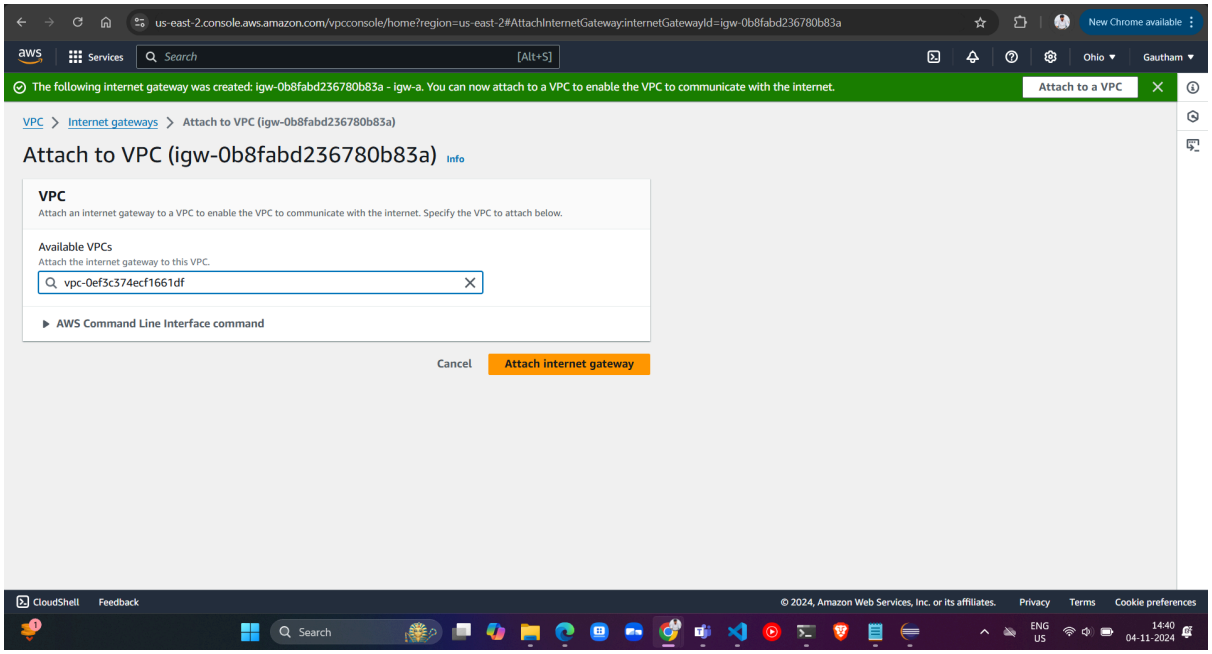
Navigate to Internet Gateway:

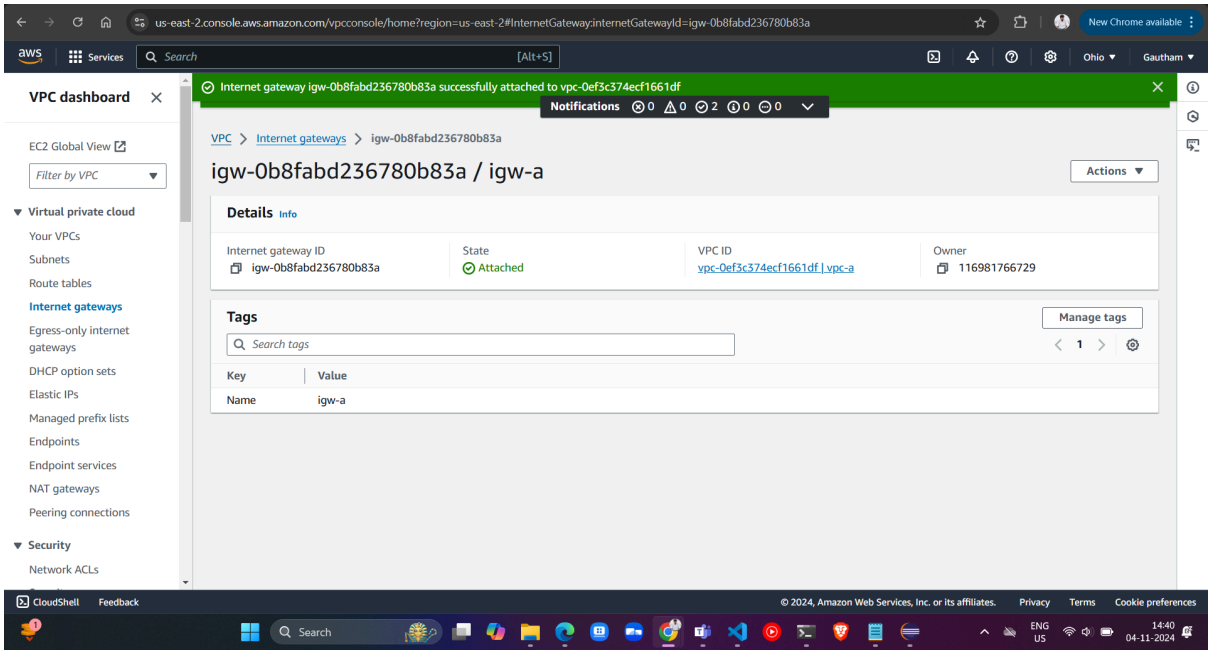
- Go to **Internet Gateways** and click **Create Internet Gateway**.
- **Name Tag**: Enter `igw-a`.



Attach to VPC:

- Select the created internet gateway and click **Attach to VPC**.
- Choose `vpc-a` and click **Attach Internet Gateway**.



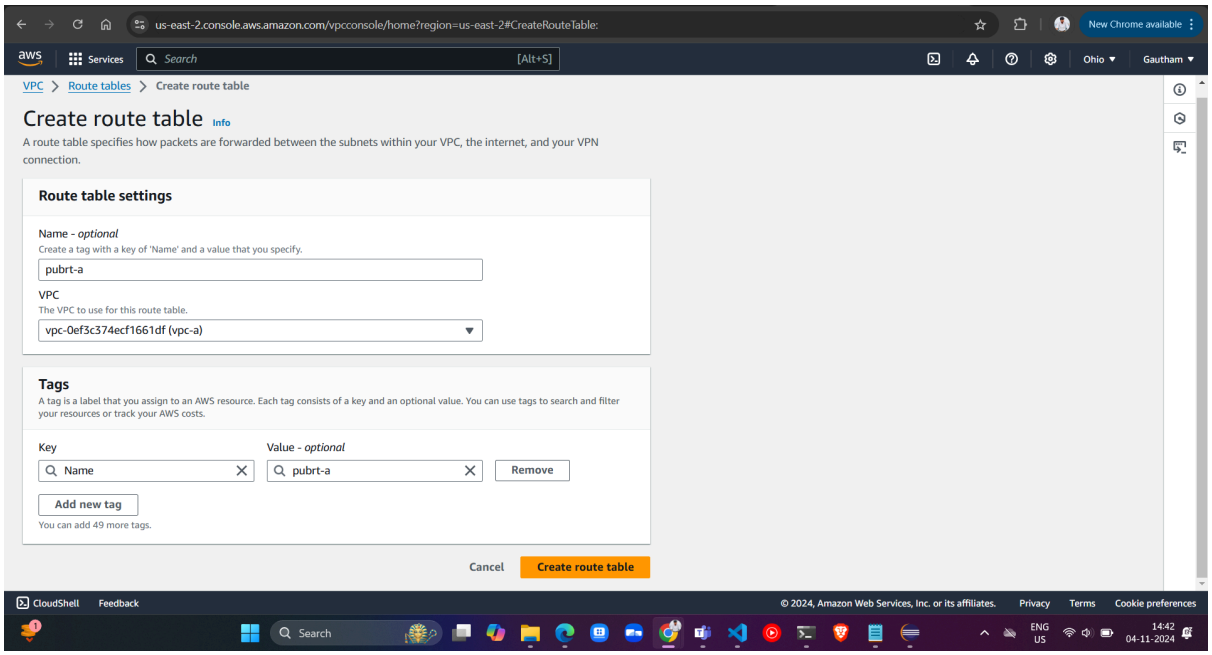


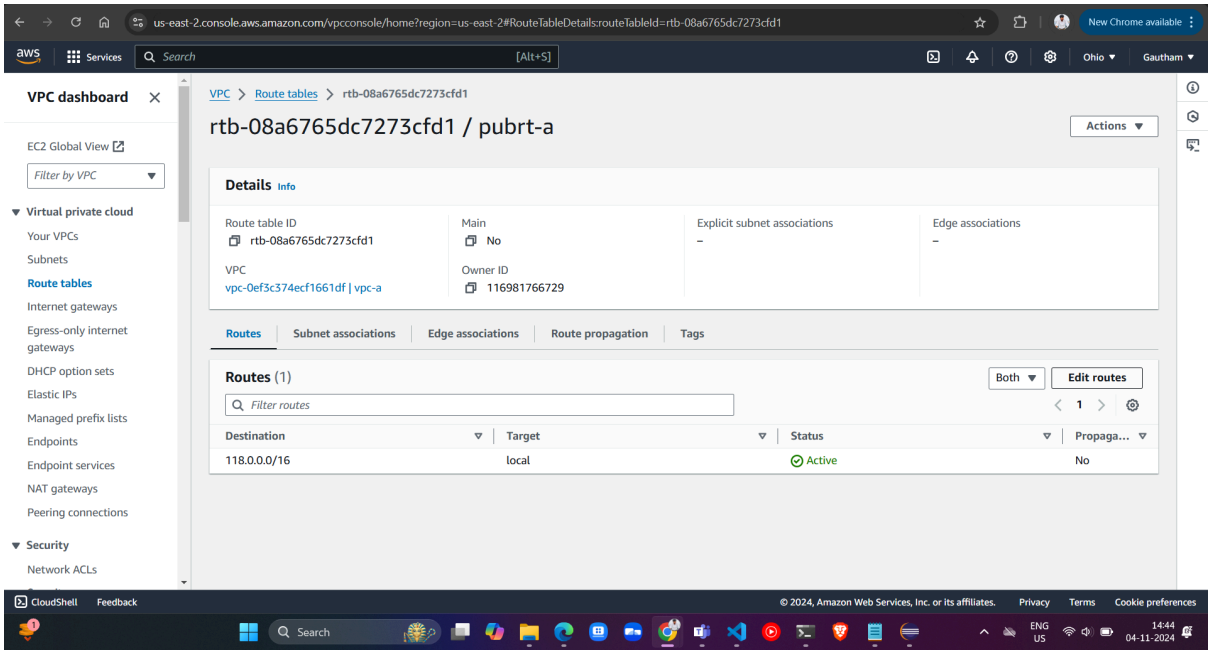
Step 5: Create and Configure Route Tables

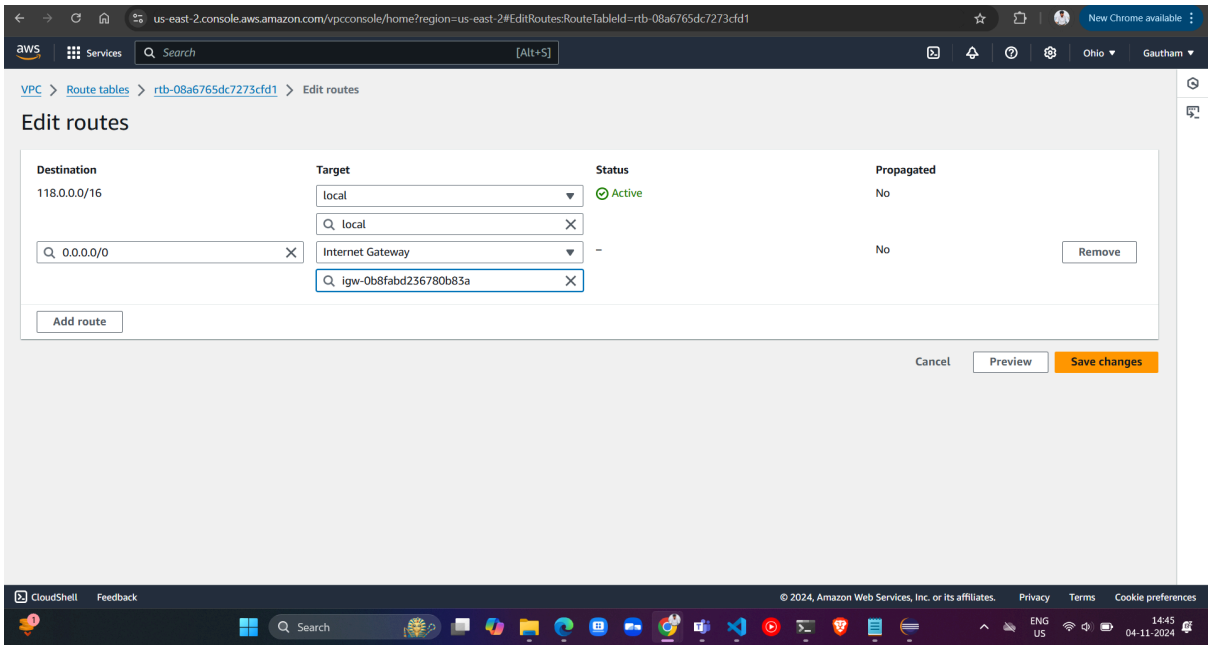
Public Route Table:

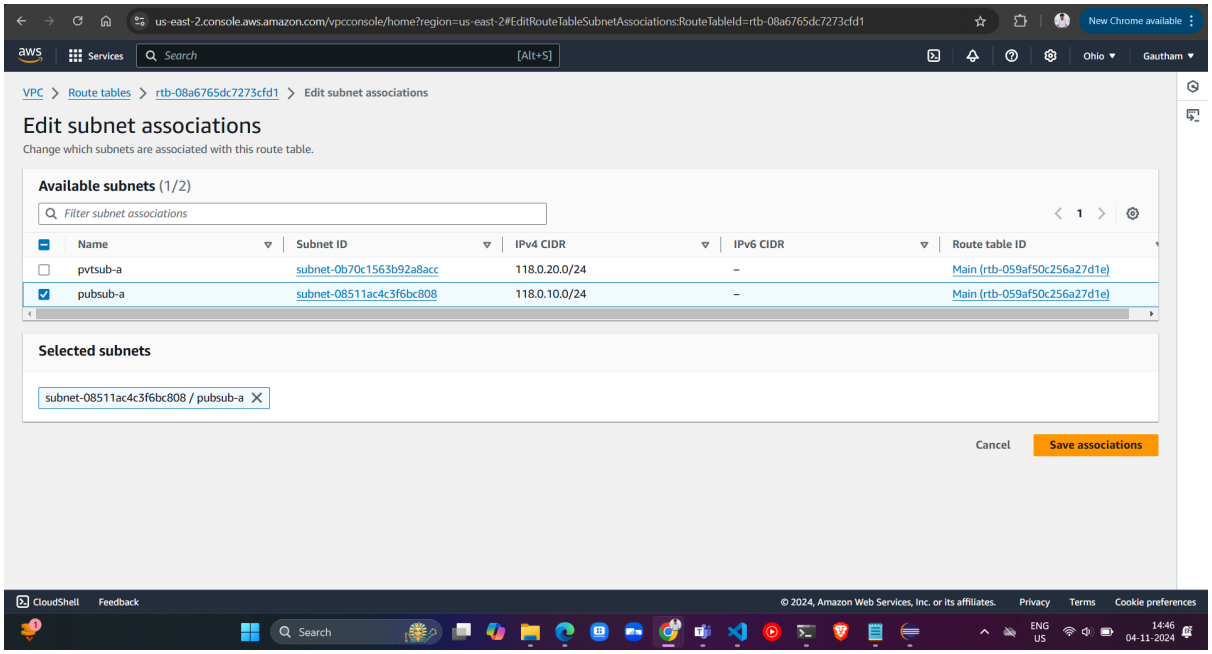
- Go to **Route Tables** and click **Create Route Table**.
- **Name**: Enter `pubrt-a`.
- **Routes**: Edit routes and add `0.0.0.0/0` as the destination with the internet gateway (`igw-a`) as the target.

- **Subnet Associations**: Associate with pubsub-a.



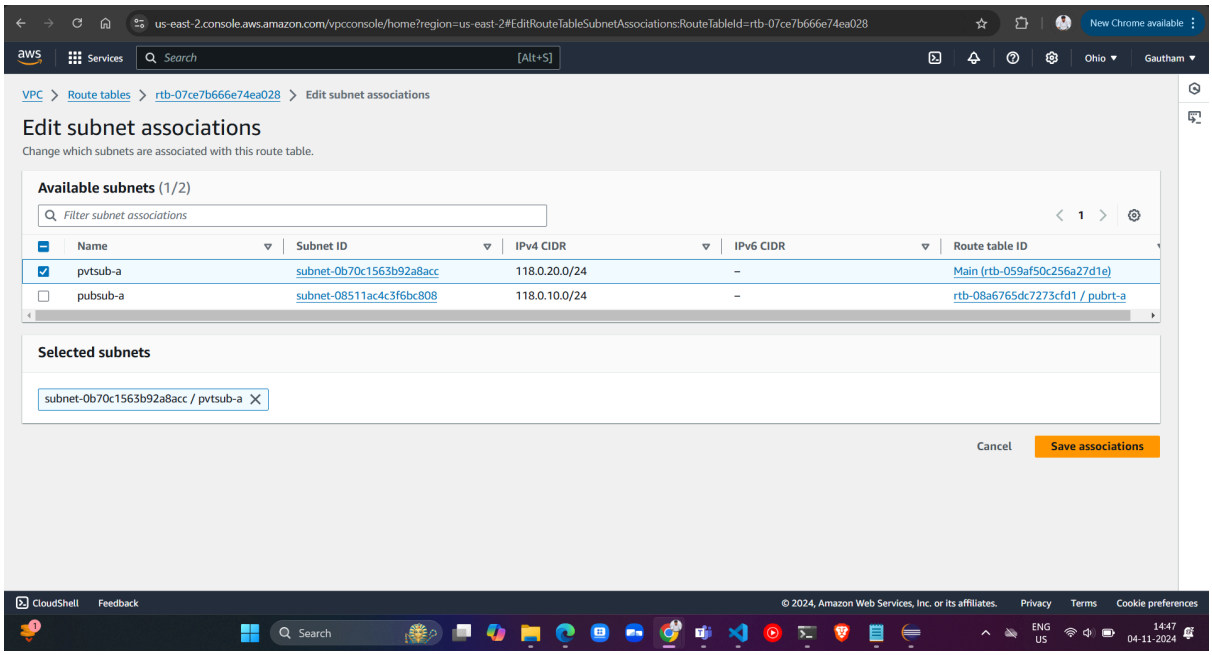


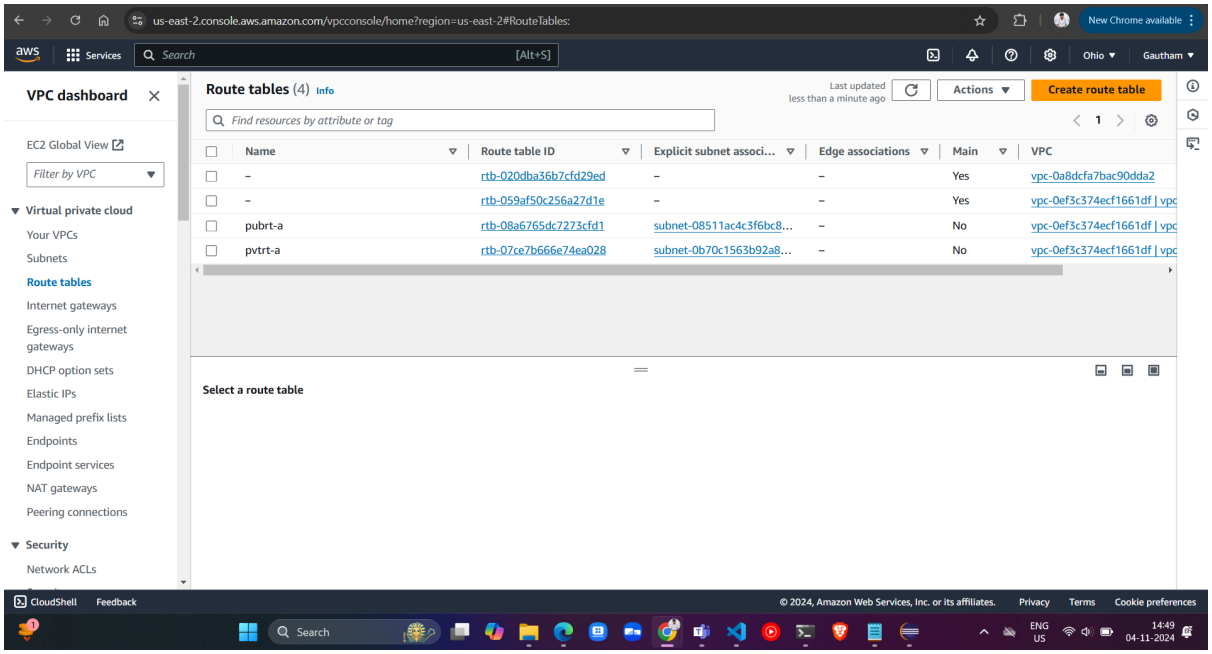




Private Route Table:

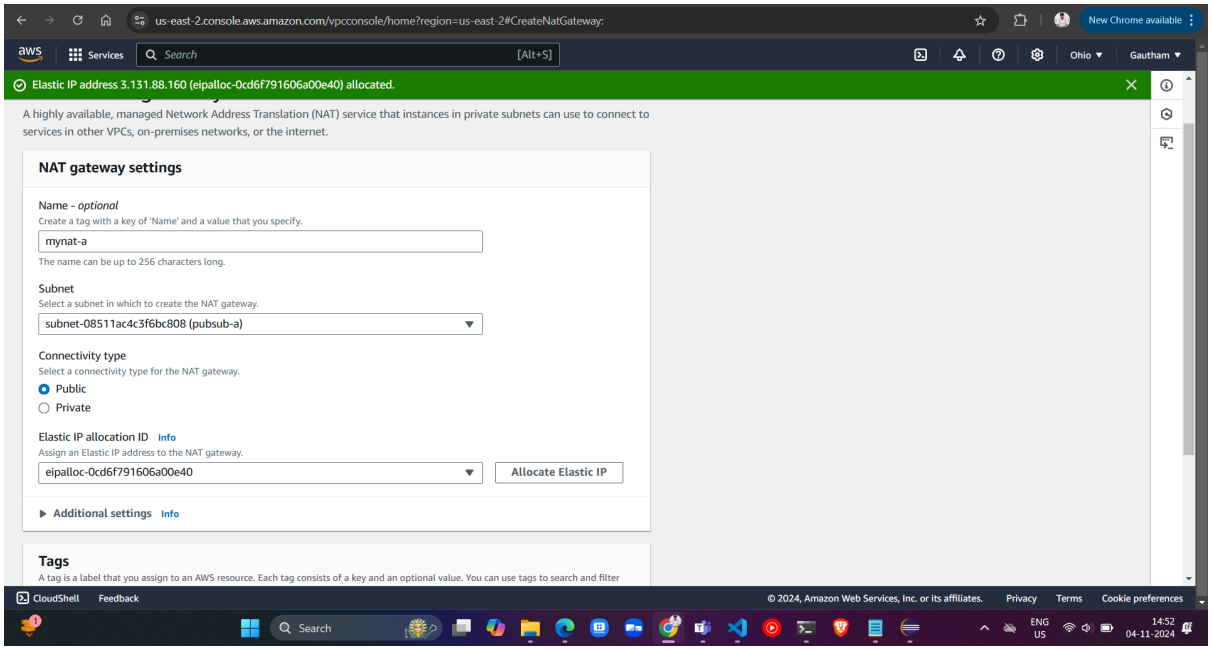
- Create another route table and name it `pvtrt-a`.
- Associate it with `pvtsub-a` under **Subnet Associations**.



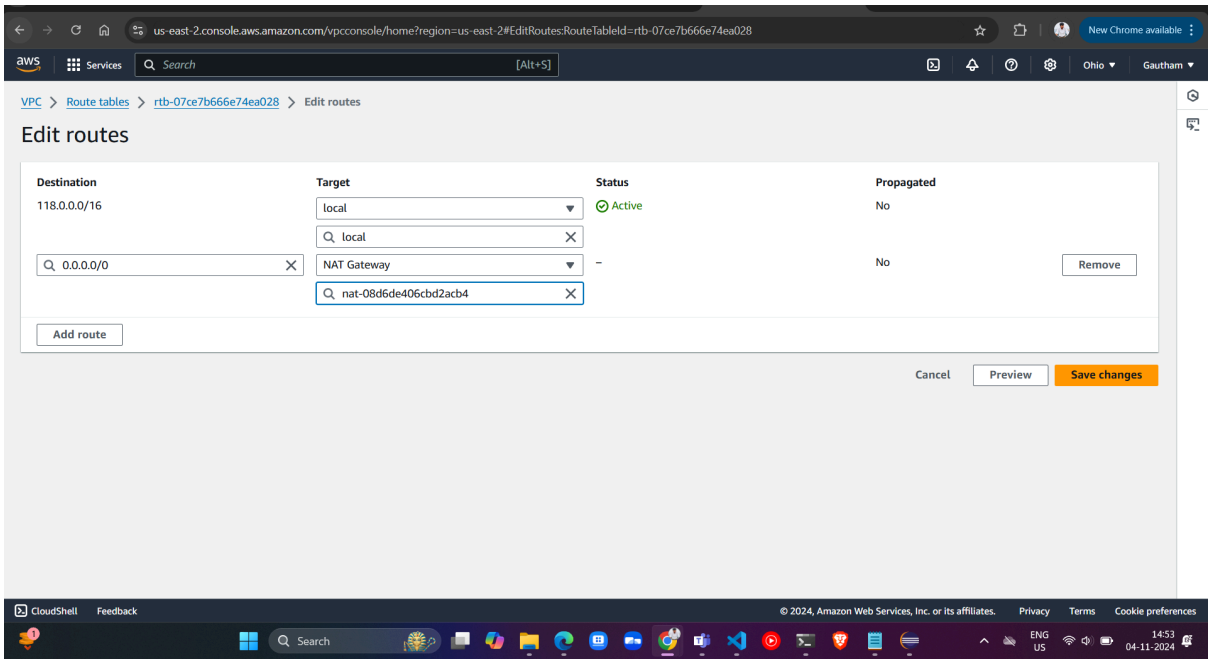


Step 6: Create a NAT Gateway

- **Navigate to NAT Gateways**:
  - Go to **NAT Gateway** and click **Create NAT Gateway**.
  - **Name**: Enter `mynat-a`.
  - **Subnet**: Choose the public subnet (`pubsub-a`).
  - **Elastic IP**: Allocate a new elastic IP.
  - Click **Create NAT Gateway**.



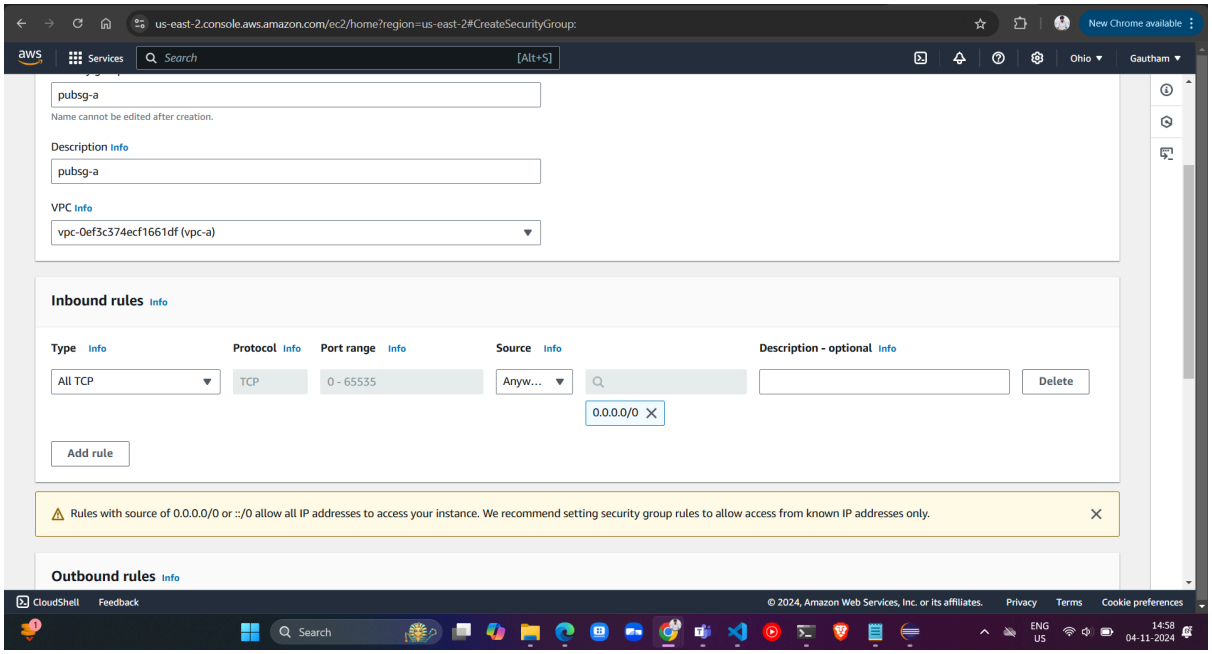
- **Add Route for Private Route Table**:
  - Go to `pvtrt-a` and edit routes.
  - **Destination**: Enter `0.0.0.0/0` and select the created NAT Gateway (`mynat-a`) as the target.



Step 7: Create Security Groups

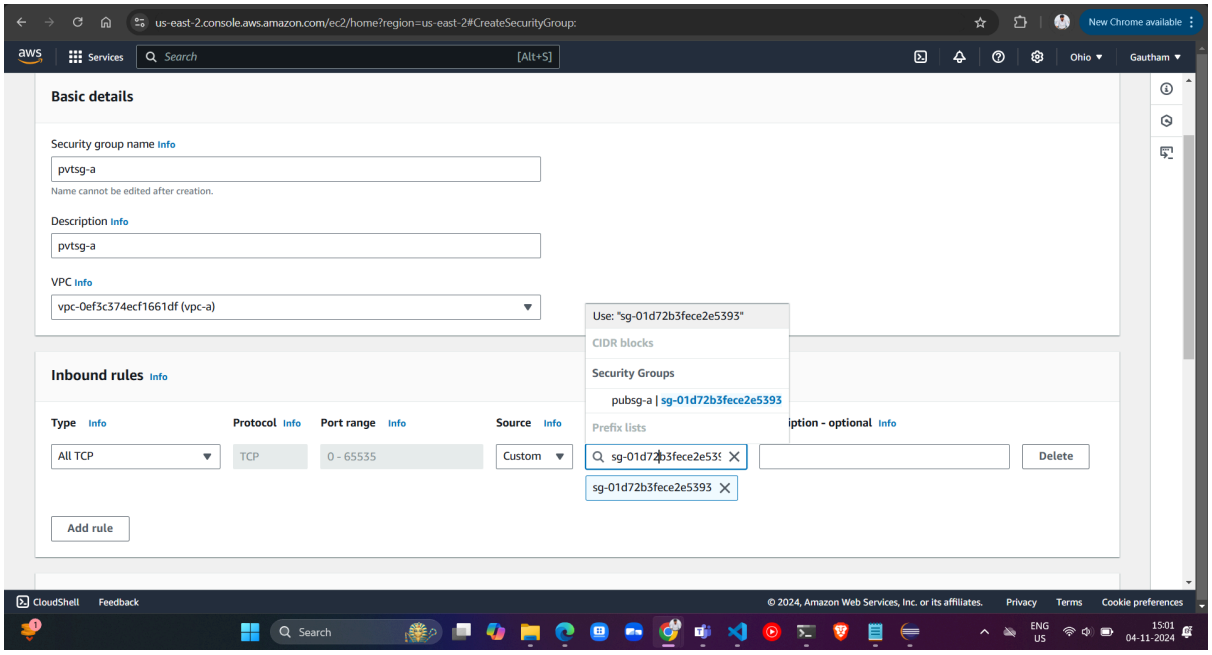
Public Security Group (pubsg-a):

- Go to **Security Groups** and click **Create Security Group**.
- **Name**: Enter `pubsg-a`.
- **VPC**: Select `vpc-a`.
- **Inbound Rule**: Allow **All TCP** with `0.0.0.0/0`.



Private Security Group (pvtsg-a):

- Create another security group named `pvtsg-a` in `vpc-a`.
- **Inbound Rule**: Allow connections from the public security group (`pubsg-a`).



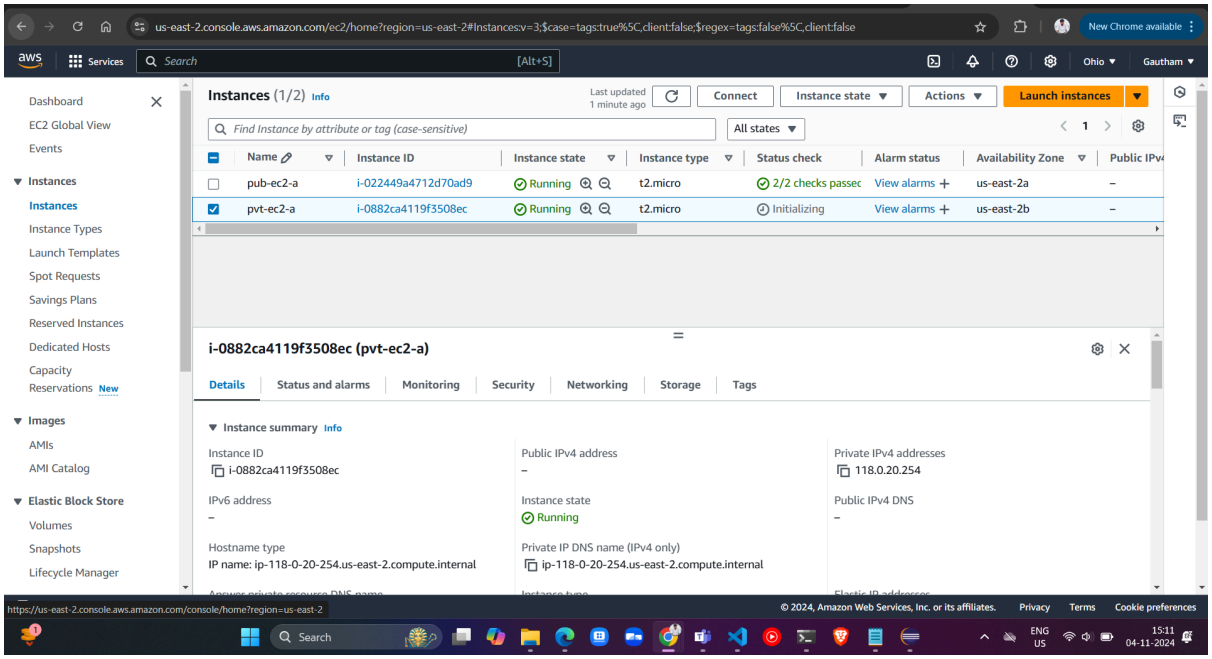
Step 8: Launch EC2 Instances in VPC-A

Public EC2 Instance:

- Go to **EC2 Instances** and click **Launch Instances**.
- **Name**: Enter `pub-ec2-a`.
- **AMI**: Choose Windows Server 2022.
- **Network Settings**: Select `vpc-a`, `pubsub-a`, and enable **Auto-assign Public IP**.
- **Security Group**: Choose `pubsg-a`.

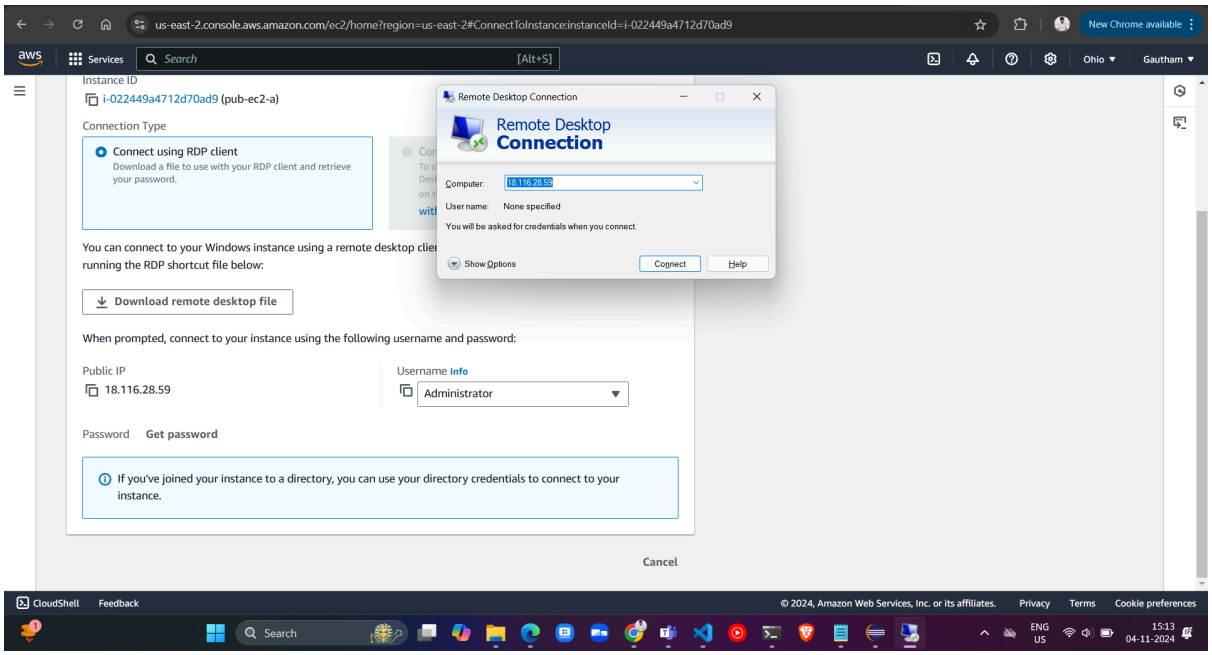
Private EC2 Instance:

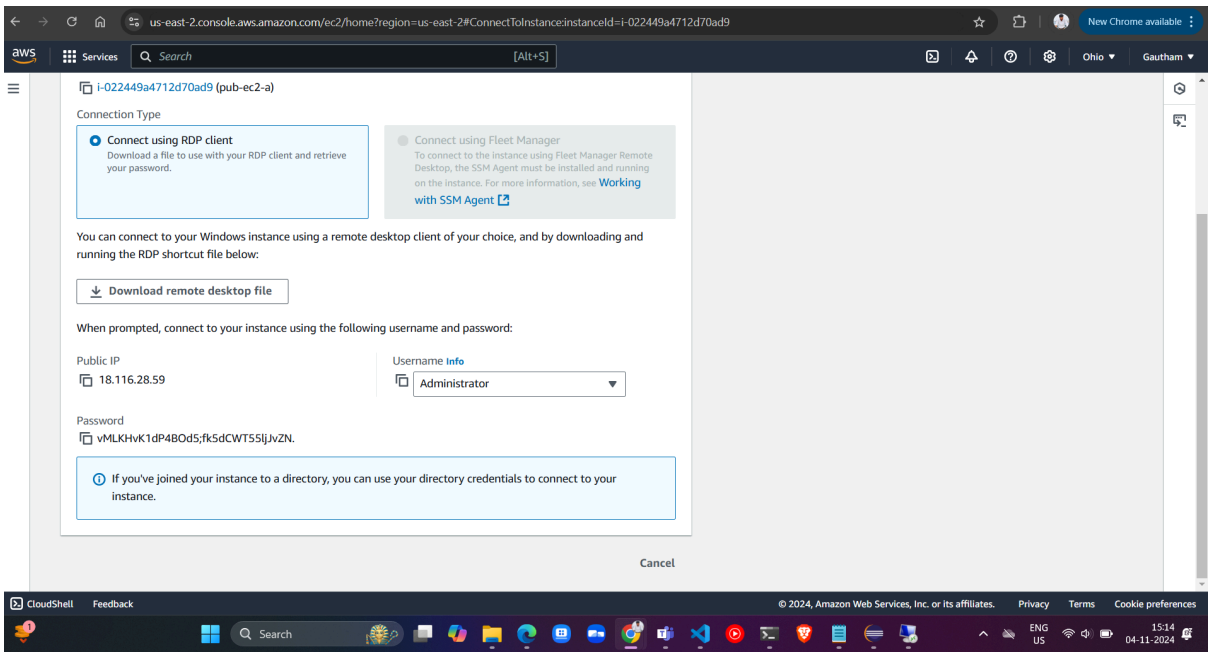
- Launch another instance with **Name** `pvt-ec2-a`.
- **Subnet**: Select `pvtsub-a`, disable **Auto-assign Public IP**, and choose `pvtsg-a` as the security group.

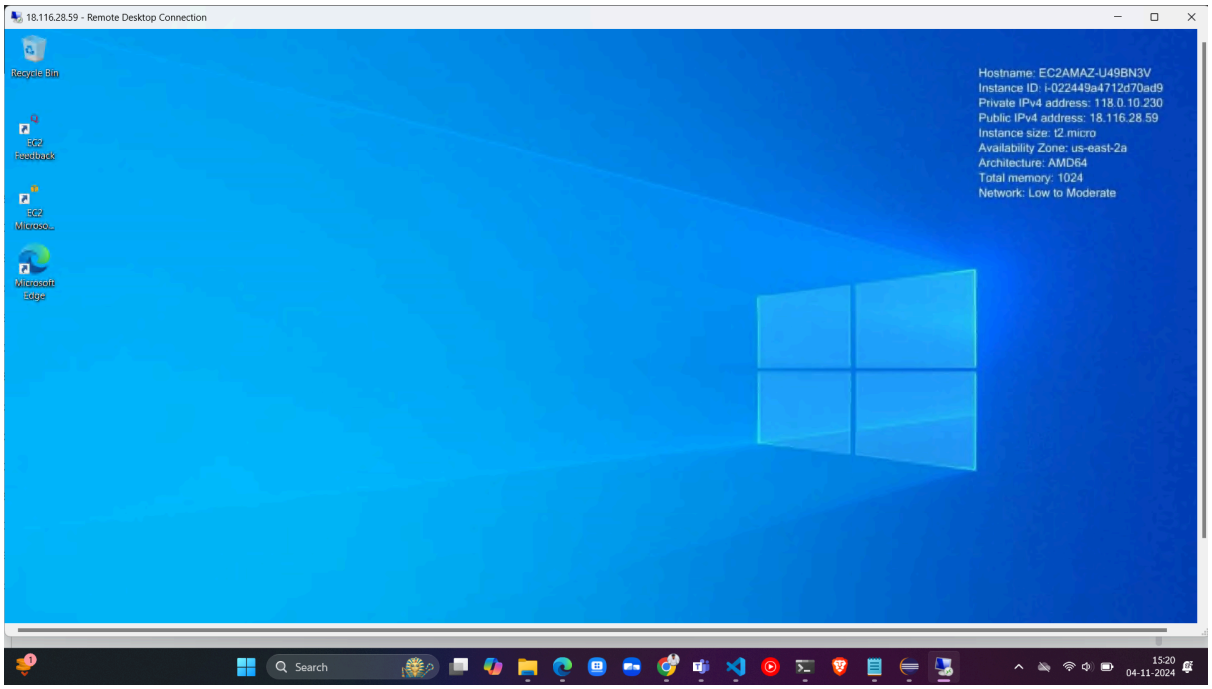


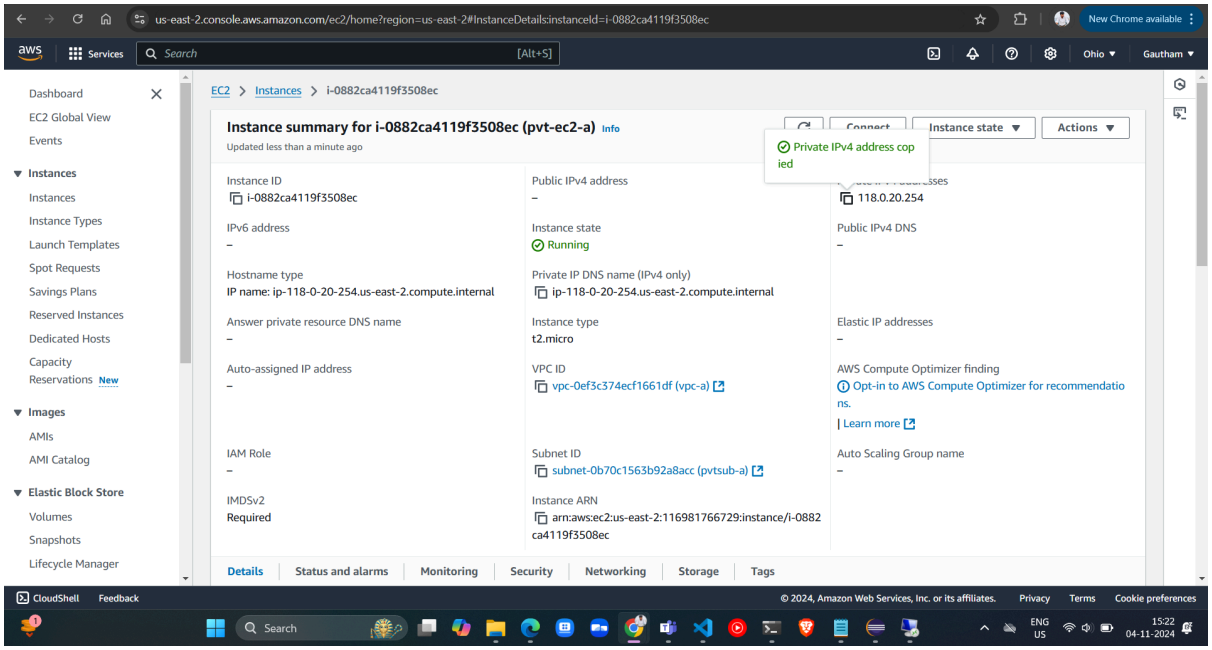
Step 9: Test Connectivity

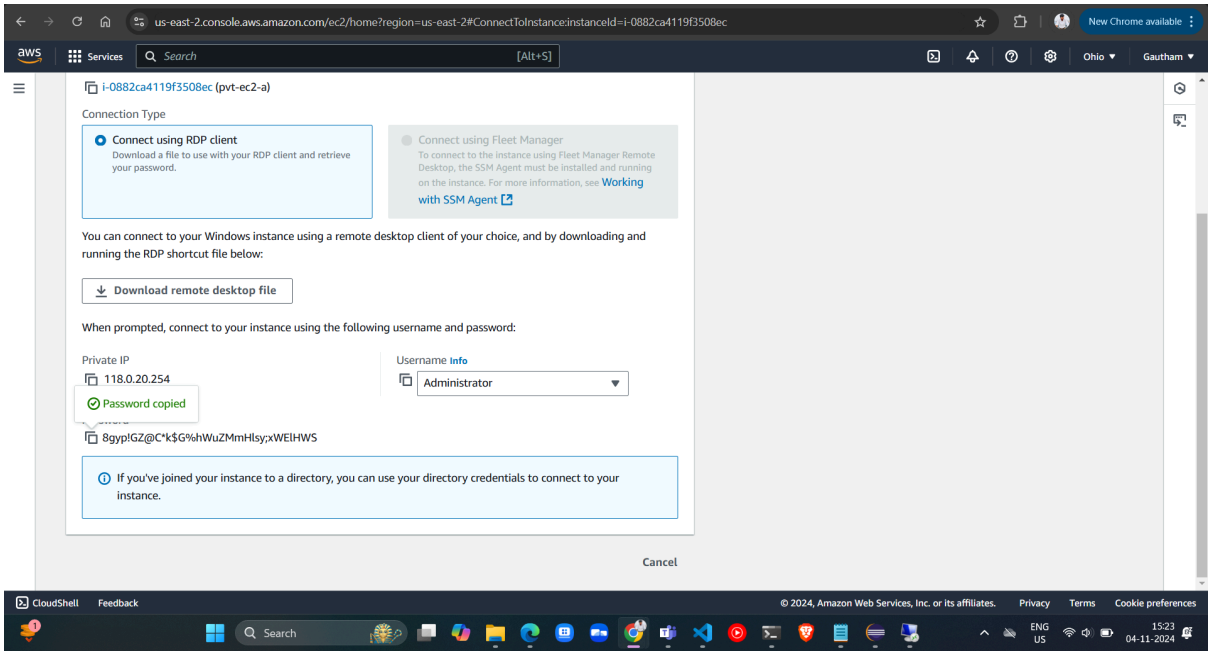
- **Public EC2 to Private EC2 Connection**:
  - Use **Remote Desktop Connection** to connect `pub-ec2-a` to `pvt-ec2-a` via private IP.
  - Verify network connectivity using `ping` commands.

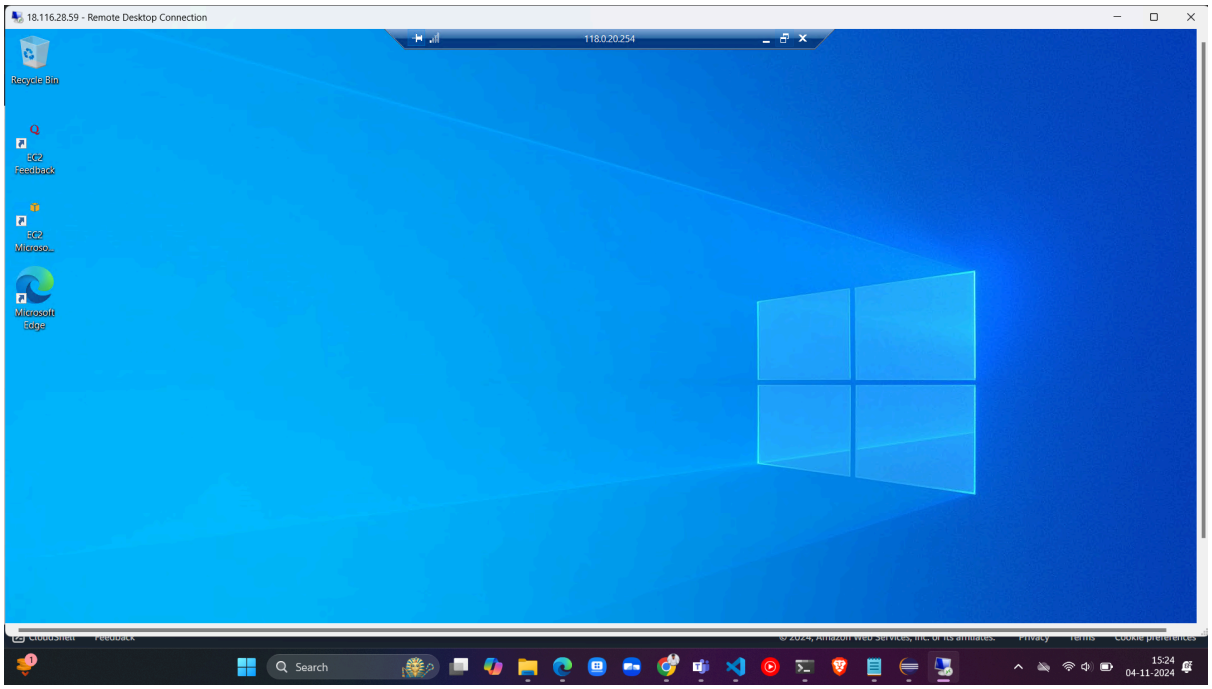

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-022449a4712d70ad9
New Chrome available
aws
Services
Search
[Alt+S]
Ohio
Gautham
Instance ID
i-022449a4712d70ad9 (pub-ec2-a)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
You can connect to your Windows instance using a remote desktop clie
running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Public IP
18.116.28.59
Username Info
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Remote Desktop Connection
Remote Desktop Connection
Computer:
18.116.28.59
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:13
04-11-2024

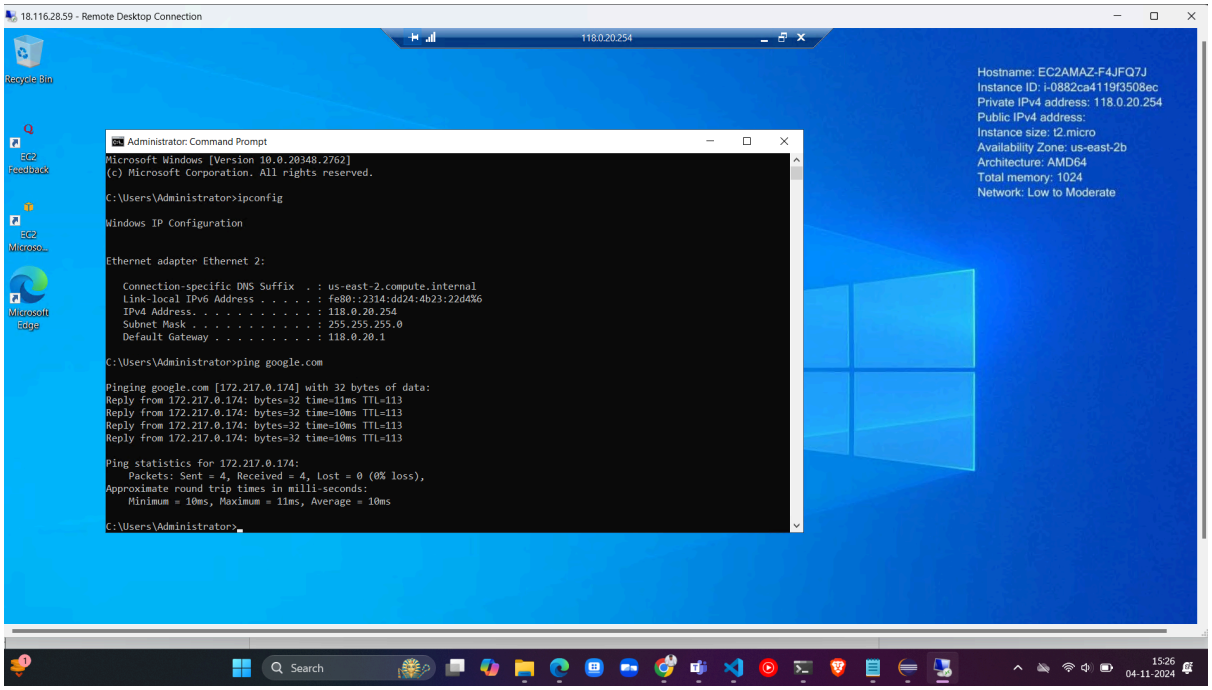

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-022449a4712d70ad9
New Chrome available
aws
Services
Search
[Alt+S]
Ohio
Gautham
i-022449a4712d70ad9 (pub-ec2-a)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your 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:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Public IP
18.116.28.59
Username Info
Administrator
Password
vMLKHvK1dP4BOd5;fk5dCWT55ljJvZN.
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:14
04-11-2024


18.116.28.59 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Microso...
Microsoft Edge
Hostname: EC2AMAZ-U49BN3V
Instance ID: i-022449a4712d70ad9
Private IPv4 address: 118.0.10.230
Public IPv4 address: 18.116.28.59
Instance size: t2.micro
Availability Zone: us-east-2a
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate
Search
15:20
04-11-2024


us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#InstanceDetails:instanceId=i-0882ca4119f3508ec
New Chrome available
aws
Services
Search
[Alt+S]
Ohio
Gautham
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
EC2 > Instances > i-0882ca4119f3508ec
Instance summary for i-0882ca4119f3508ec (pvt-ec2-a) Info
Updated less than a minute ago
Connect
Instance state
Actions
Private IPv4 address copied
Instance ID
i-0882ca4119f3508ec
IPv6 address
–
Hostname type
IP name: ip-118-0-20-254.us-east-2.compute.internal
Answer private resource DNS name
–
Auto-assigned IP address
–
IAM Role
–
IMDSv2
Required
Public IPv4 address
–
Instance state
Running
Private IP DNS name (IPv4 only)
ip-118-0-20-254.us-east-2.compute.internal
Instance type
t2.micro
VPC ID
vpc-0ef3c374ecf1661df (vpc-a)
Subnet ID
subnet-0b70c1563b92a8acc (pvtsub-a)
Instance ARN
arn:aws:ec2:us-east-2:116981766729:instance/i-0882ca4119f3508ec
118.0.20.254
Public IPv4 DNS
–
Elastic IP addresses
–
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
Auto Scaling Group name
–
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:22
04-11-2024


us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-0882ca4119f3508ec
New Chrome available
aws
Services
Search
[Alt+S]
Ohio
Gautham
i-0882ca4119f3508ec (pvt-ec2-a)
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:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Private IP
118.0.20.254
Username Info
Administrator
Password copied
8gyp!GZ@C*k$G%hWuZMmHlsy;xWElHWS
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:23
04-11-2024

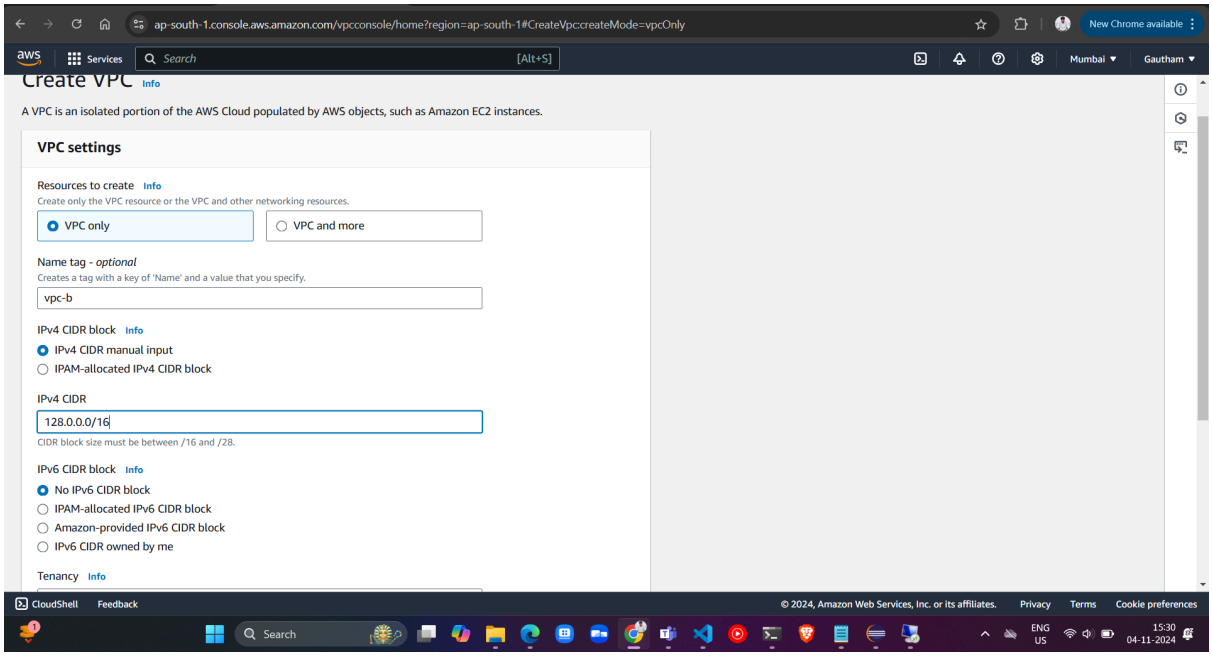


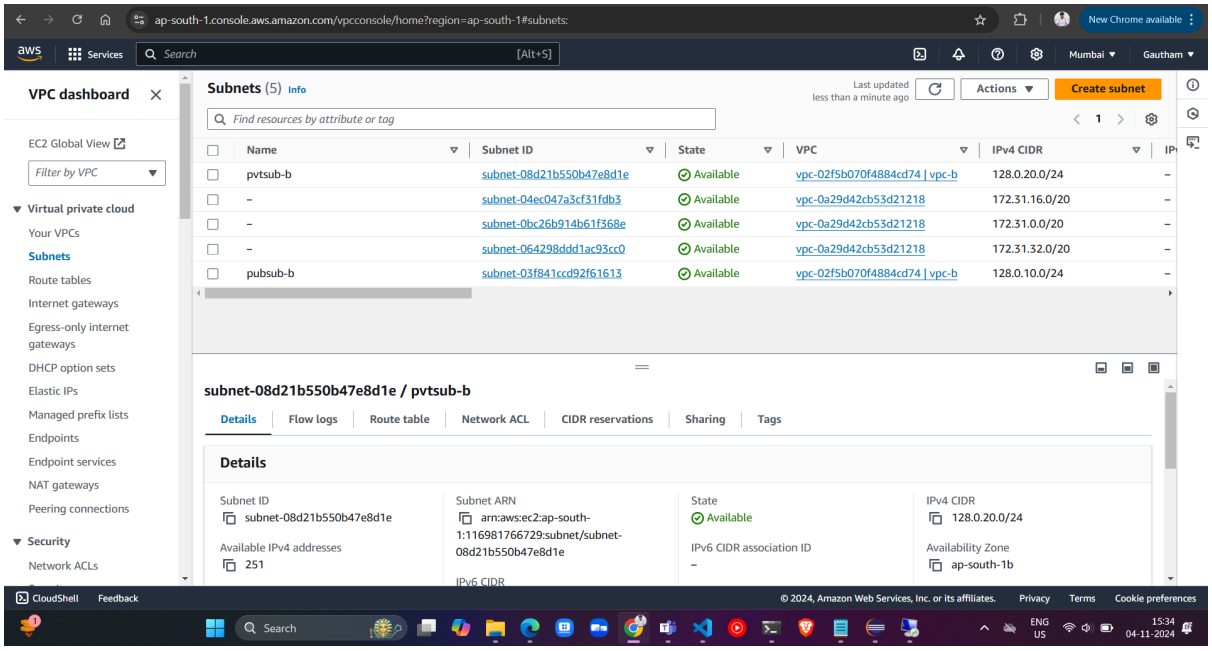


Step 10-16: Repeat Setup in Zone B (Mumbai)

Create VPC-B and Subnets:

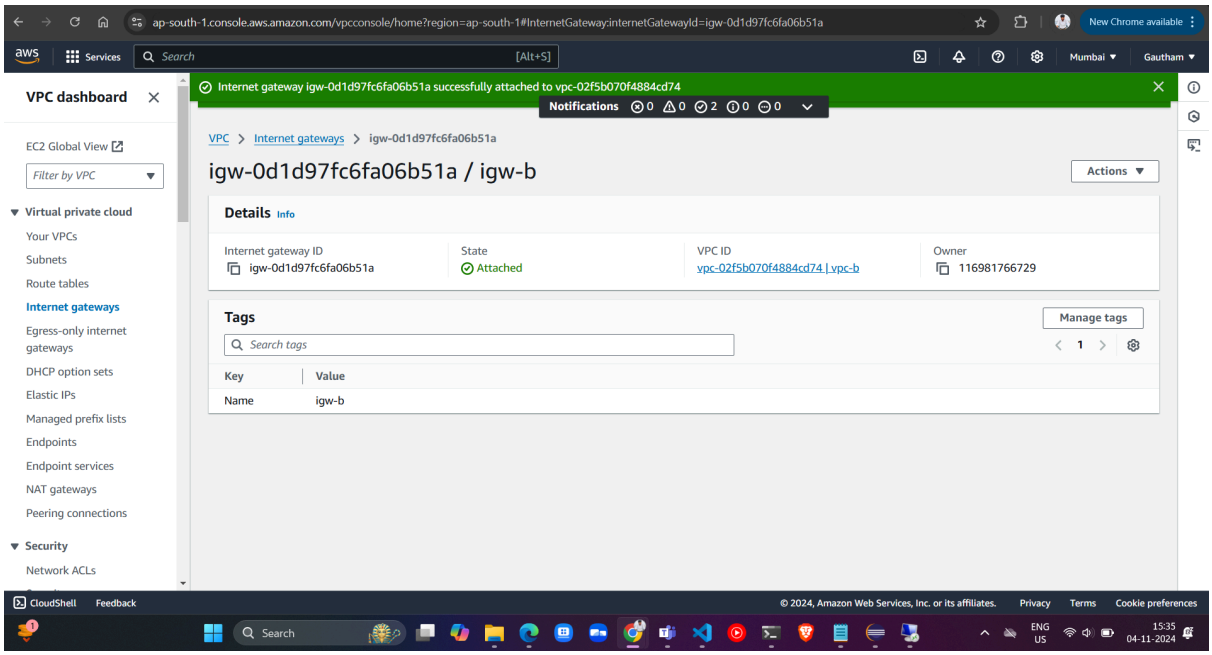
- VPC name: `vpc-b`, CIDR: `128.0.0.0/16`.
- Public Subnet: `pubsub-b`, CIDR: `128.0.10.0/24`.
- Private Subnet: `pvtsub-b`, CIDR: `128.0.20.0/24`.

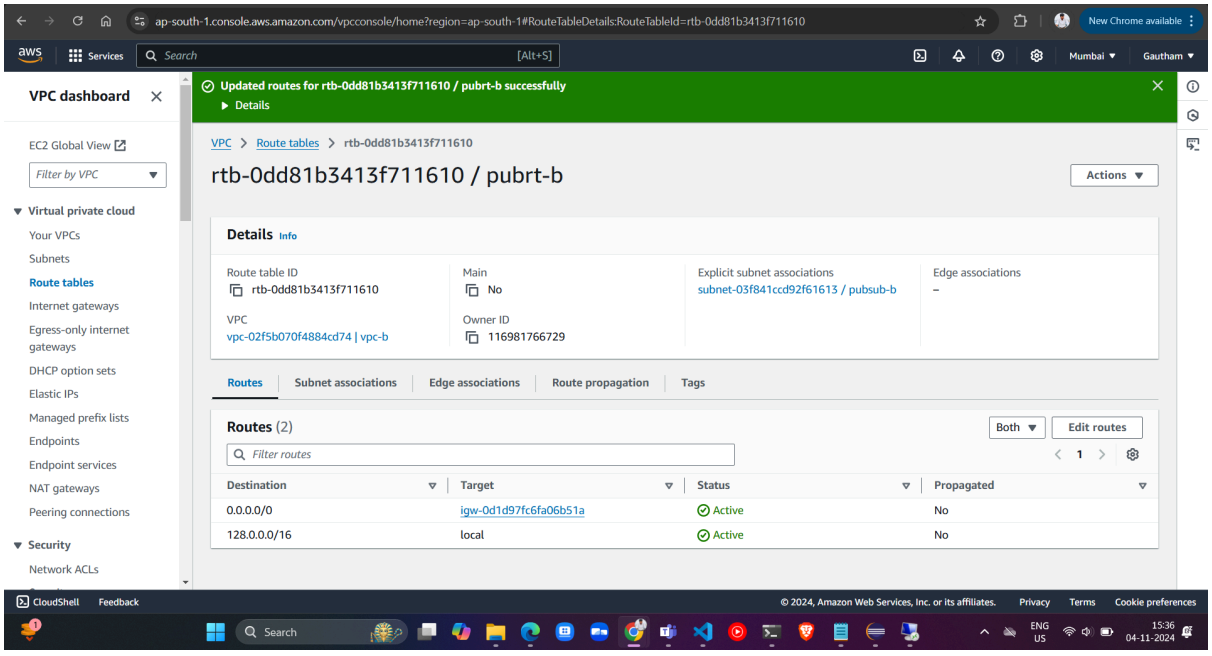


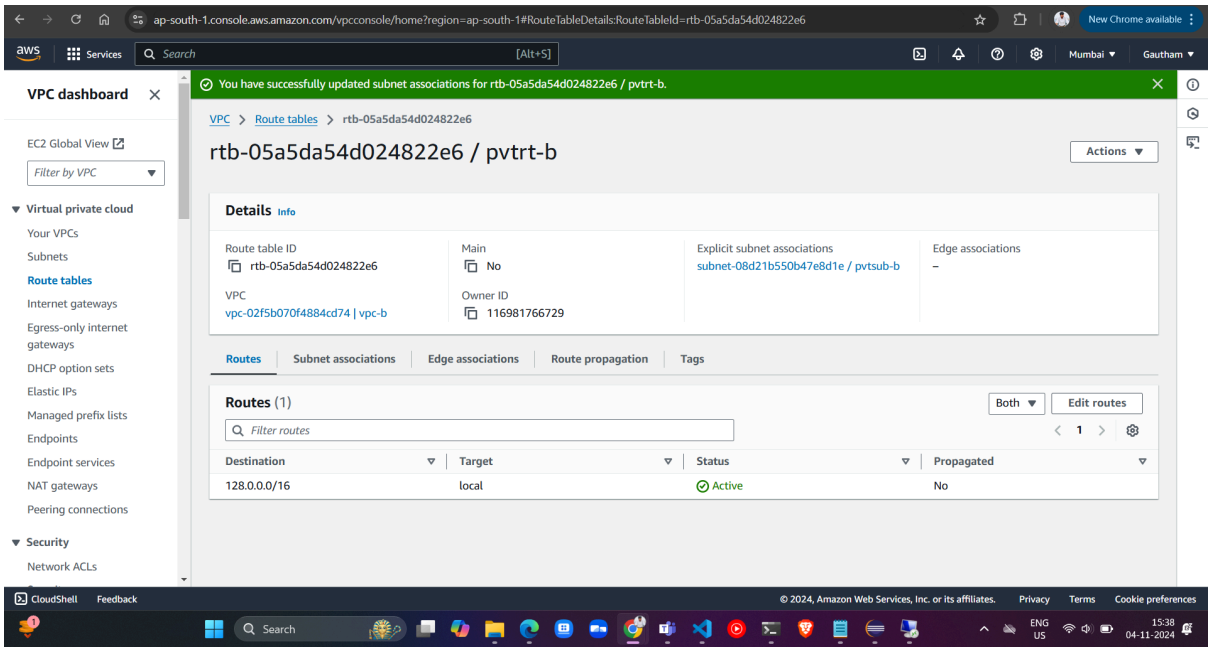


Internet Gateway and Route Tables:

- Create `igw-b`, attach to `vpc-b`.
- Public route (`pubrt-b`) routes internet traffic; `pvtrt-b` routes to NAT.

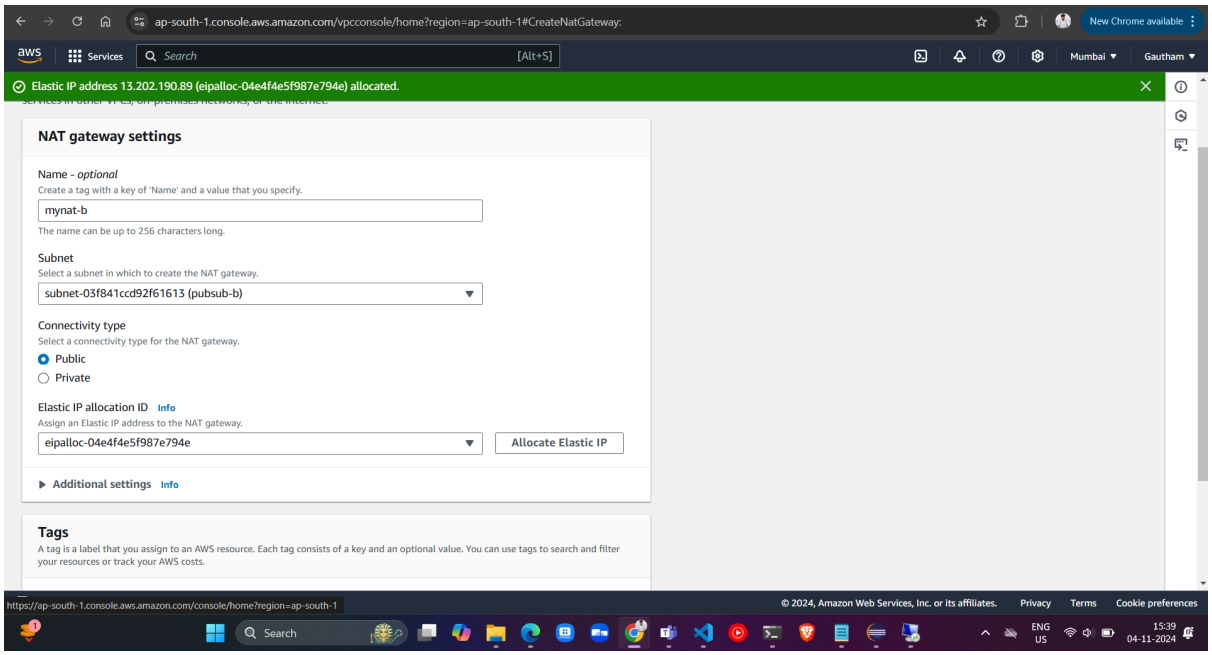

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#InternetGateway:internetGatewayId=igw-0d1d97fc6fa06b51a
New Chrome available
Services
Search
[Alt+S]
Mumbai
Gautham
VPC dashboard
Internet gateway igw-0d1d97fc6fa06b51a successfully attached to vpc-02f5b070f4884cd74
Notifications
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
VPC > Internet gateways > igw-0d1d97fc6fa06b51a
igw-0d1d97fc6fa06b51a / igw-b
Actions
Details Info
Internet gateway ID
igw-0d1d97fc6fa06b51a
State
Attached
VPC ID
vpc-02f5b070f4884cd74 | vpc-b
Owner
116981766729
Tags
Manage tags
Search tags
Key
Value
Name
igw-b
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
US
15:35
04-11-2024

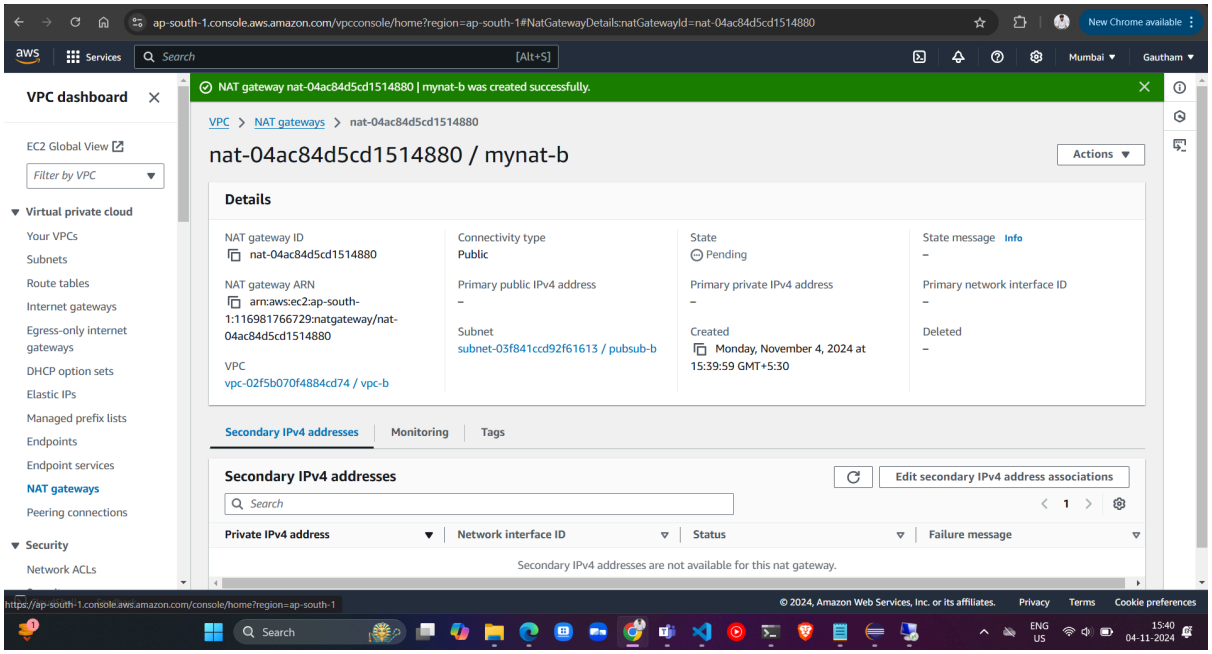

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0dd81b3413f711610
New Chrome available
Services
Search
[Alt+S]
Mumbai
Gautham
VPC dashboard
Updated routes for rtb-0dd81b3413f711610 / pubrt-b successfully
Details
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
VPC > Route tables > rtb-0dd81b3413f711610
rtb-0dd81b3413f711610 / pubrt-b
Actions
Details Info
Route table ID
rtb-0dd81b3413f711610
Main
No
Explicit subnet associations
subnet-03f841ccd92f61613 / pubsub-b
Edge associations
–
VPC
vpc-02f5b070f4884cd74 | vpc-b
Owner ID
116981766729
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-0d1d97fc6fa06b51a
Active
No
128.0.0.0/16
local
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
US
15:36
04-11-2024

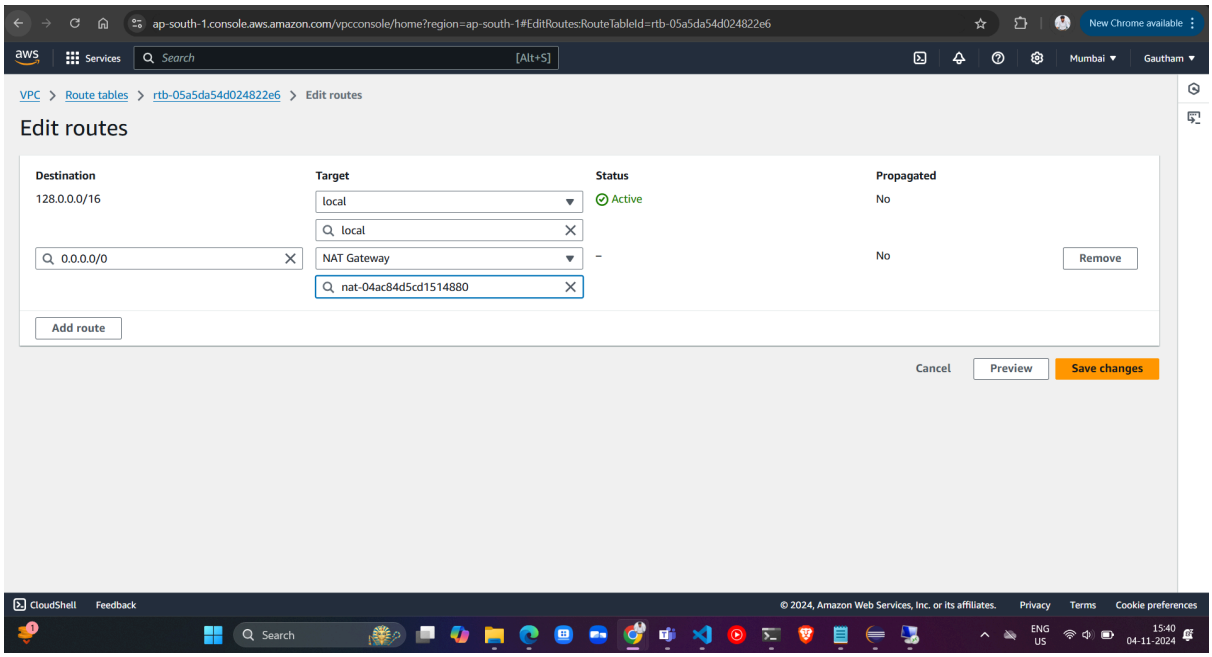


NAT Gateway:

- Name: `mynat-b`, use `pubsub-b` and allocate Elastic IP.

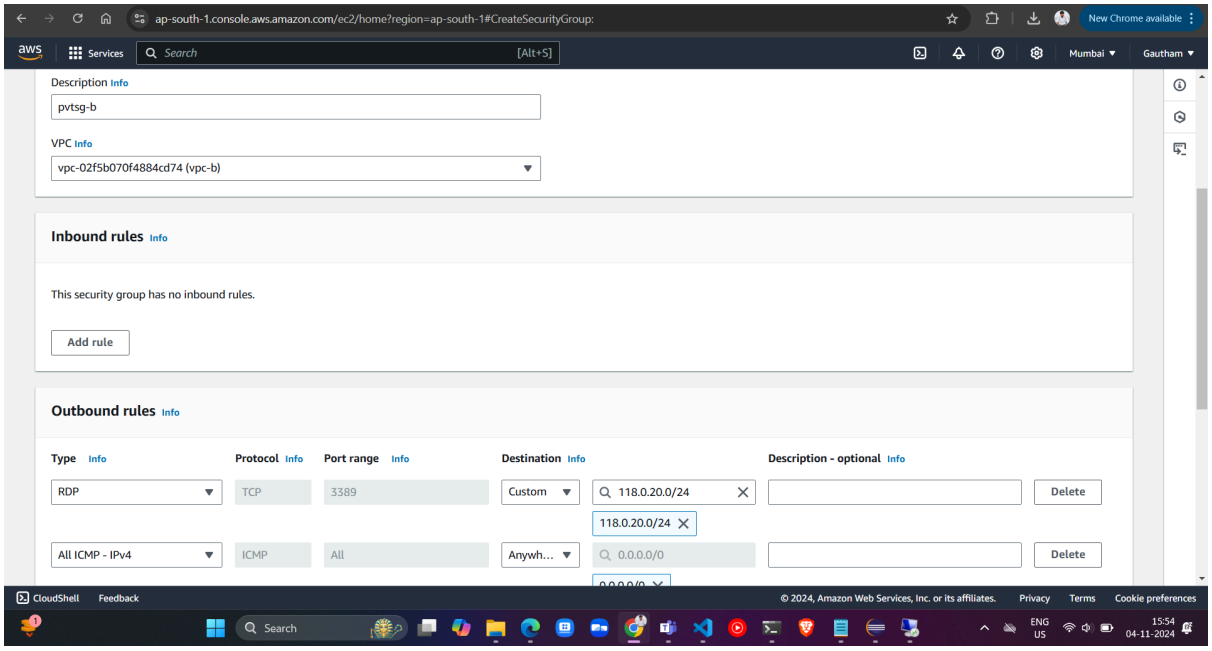

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateNatGateway:
New Chrome available
Services
Search
[Alt+S]
Mumbai
Gautham
Elastic IP address 13.202.190.89 (eipalloc-04e4f4e5f987e794e) allocated.
NAT gateway settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
mynat-b
The name can be up to 256 characters long.
Subnet
Select a subnet in which to create the NAT gateway.
subnet-03f841ccd92f61613 (pubsub-b)
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-04e4f4e5f987e794e
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.
https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:39
04-11-2024


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGatewayDetails:natGatewayId=nat-04ac84d5cd1514880
New Chrome available
Services
Search
[Alt+S]
Mumbai
Gautham
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
NAT gateway nat-04ac84d5cd1514880 | mynat-b was created successfully.
VPC > NAT gateways > nat-04ac84d5cd1514880
nat-04ac84d5cd1514880 / mynat-b
Actions
Details
NAT gateway ID
nat-04ac84d5cd1514880
Connectivity type
Public
State
Pending
State message Info
–
NAT gateway ARN
arn:aws:ec2:ap-south-1:116981766729:natgateway/nat-04ac84d5cd1514880
Primary public IPv4 address
–
Primary private IPv4 address
–
Primary network interface ID
–
VPC
vpc-02f5b070f4884cd74 / vpc-b
Subnet
subnet-03f841ccd92f61613 / pubsub-b
Created
Monday, November 4, 2024 at 15:39:59 GMT+5:30
Deleted
–
Secondary IPv4 addresses
Monitoring
Tags
Secondary IPv4 addresses
Edit secondary IPv4 address associations
Search
Private IPv4 address
Network interface ID
Status
Failure message
Secondary IPv4 addresses are not available for this nat gateway.
https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
15:40
04-11-2024



Security Group (pvtsg-b):

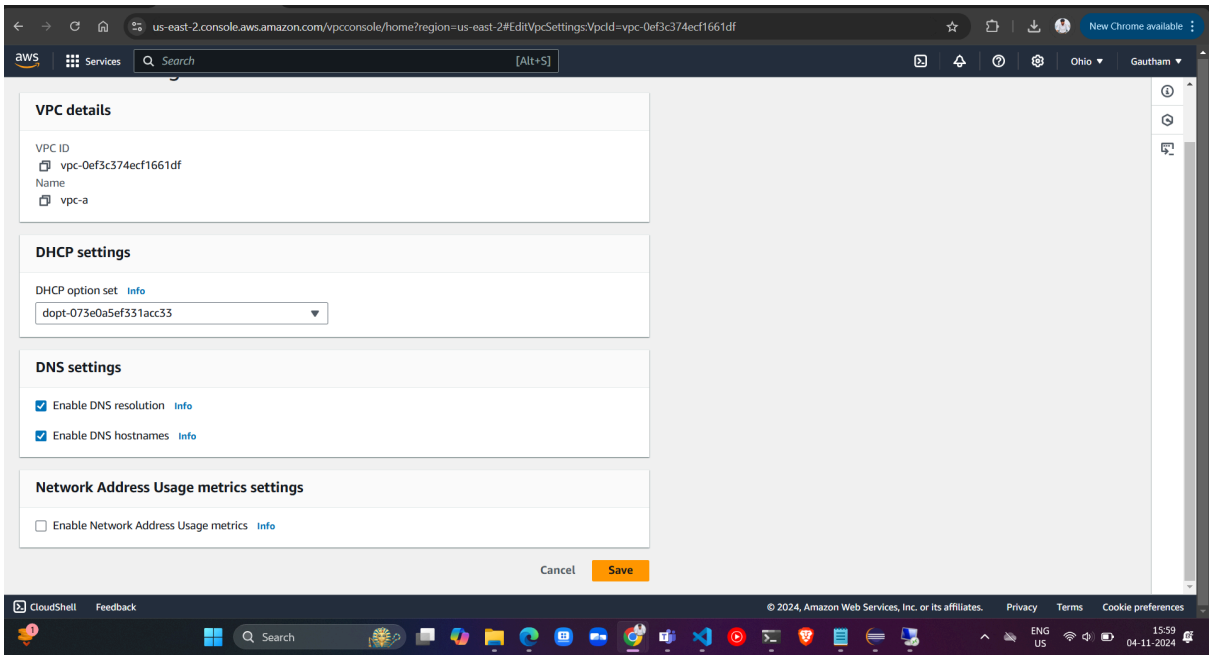
- Inbound rules for **RDP** (from vpc-a private IP) and **All ICMP - IPv4**.



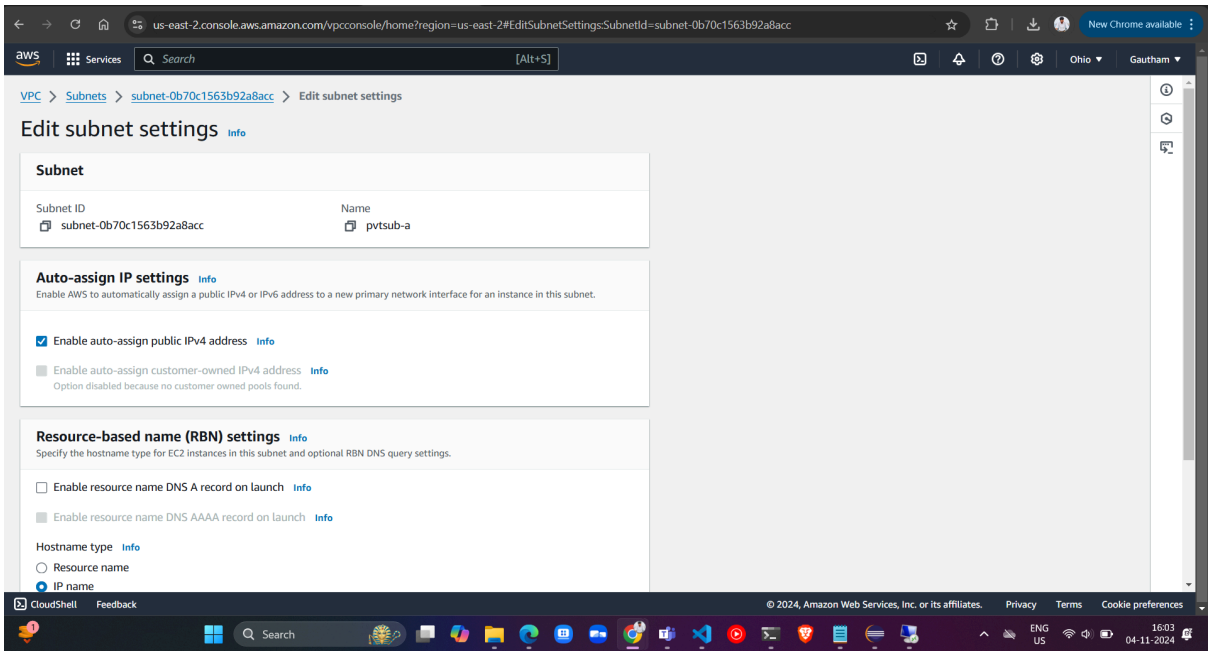
Connect the Private machine from Zone-A (Ohio) to the Private machine in Zone- B (Mumbai)

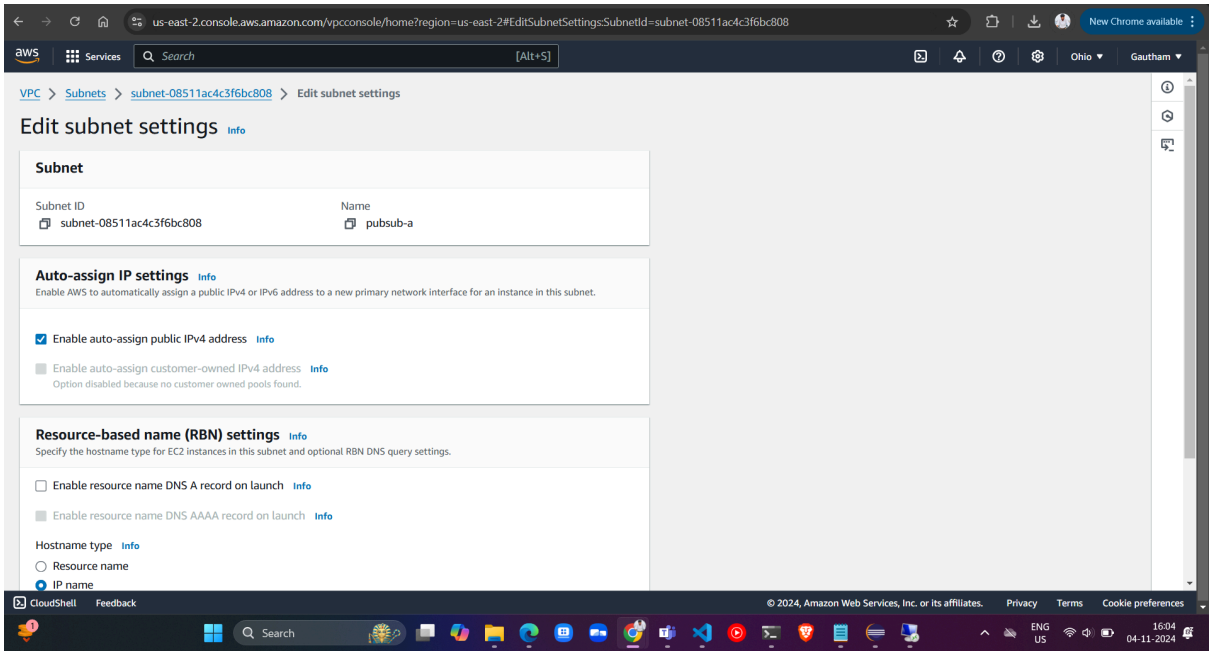
Make the following configuration changes in the zone a

In the vpc-a edit the vpc settings
Enable the DNS Hostnames



Goto subnets and edit actions
Enable the auto assign ip addresses

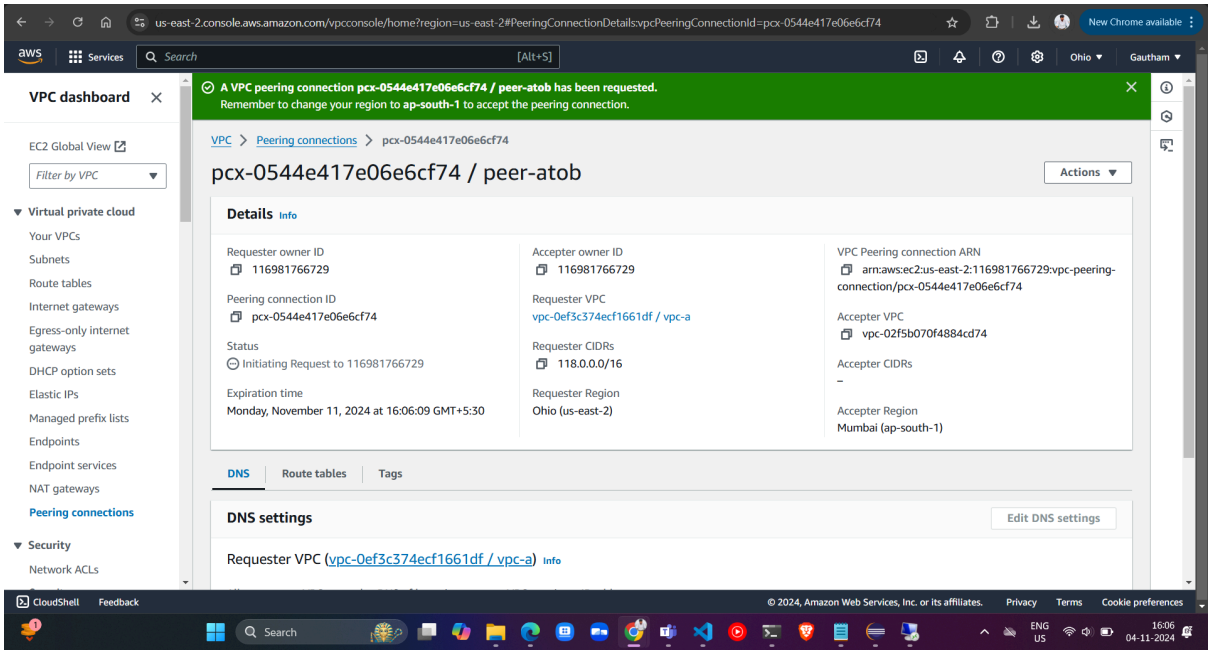




Step 17: Create VPC Peering Connection

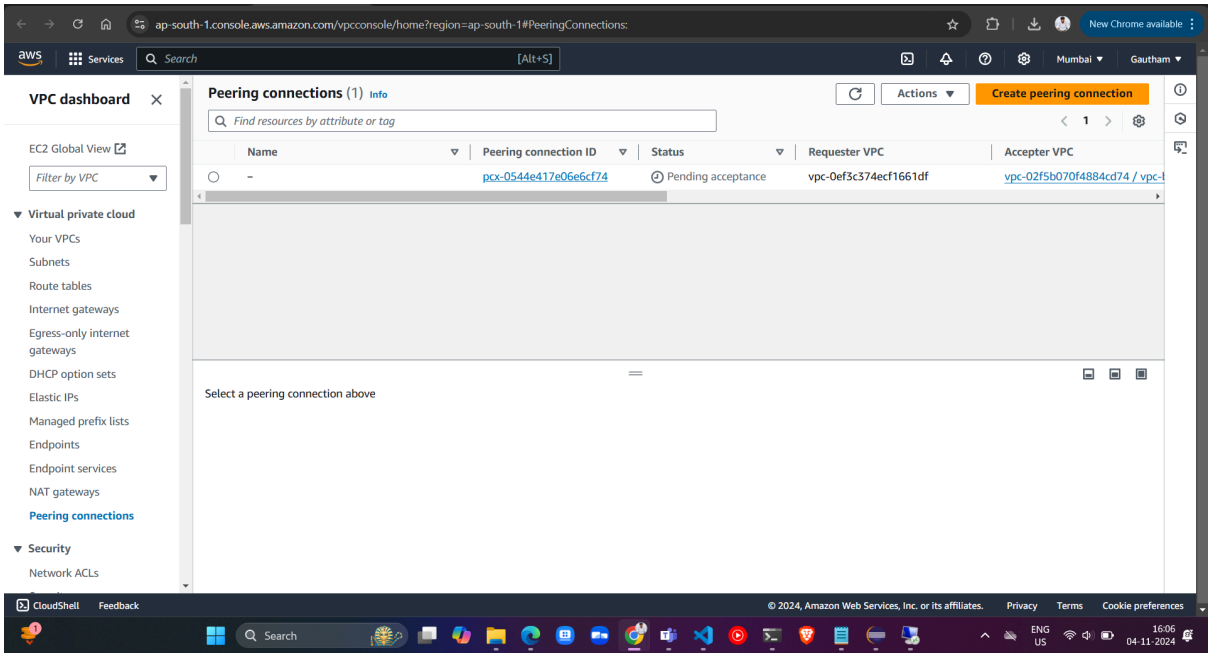
Peering from VPC-A to VPC-B:

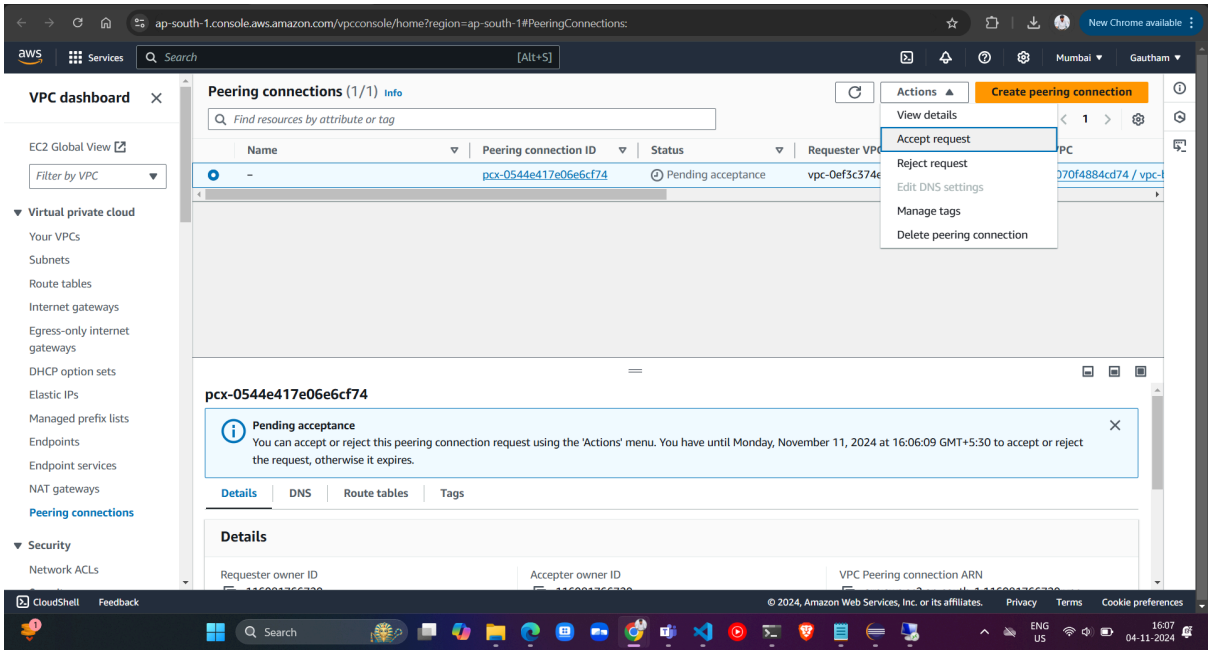
- Name: `peer-atob`, with `vpc-a` as requester, `vpc-b` as accepter.

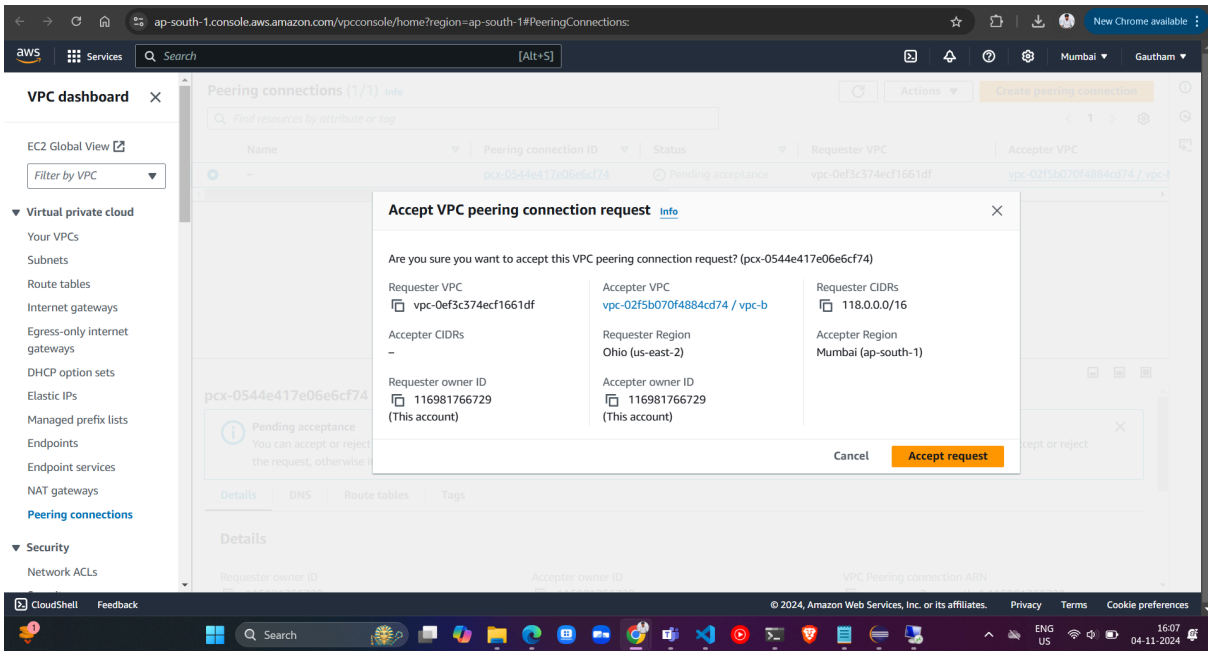


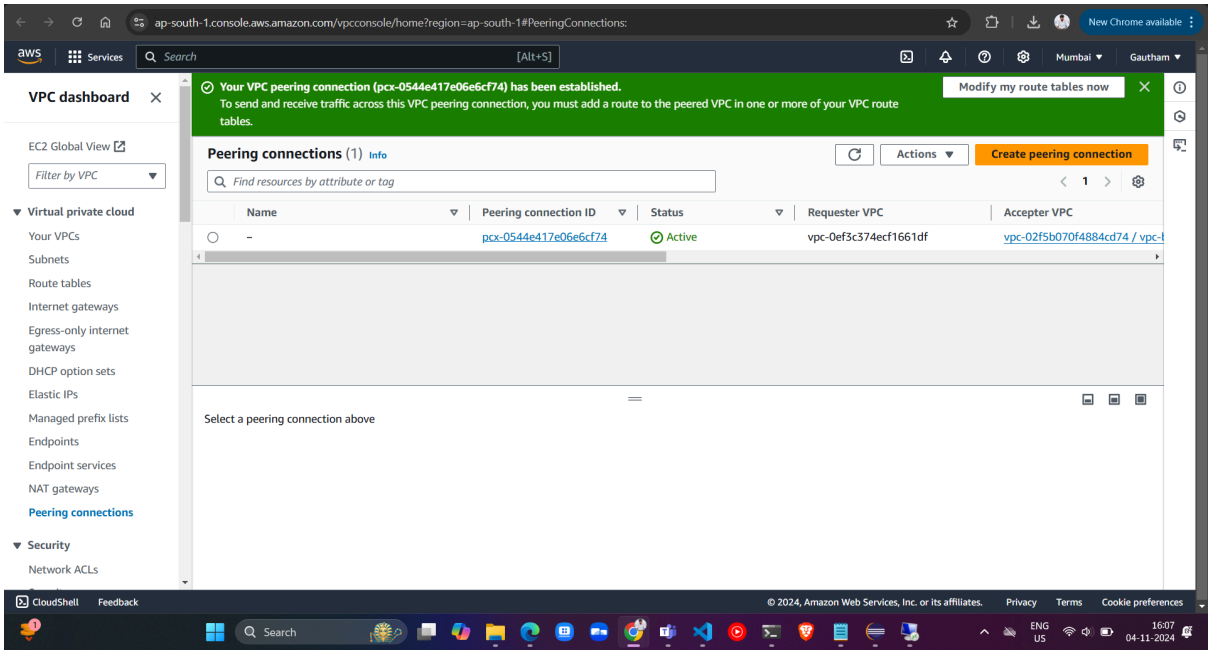
Accept Request in Zone B:

- Accept the request in Mumbai region.



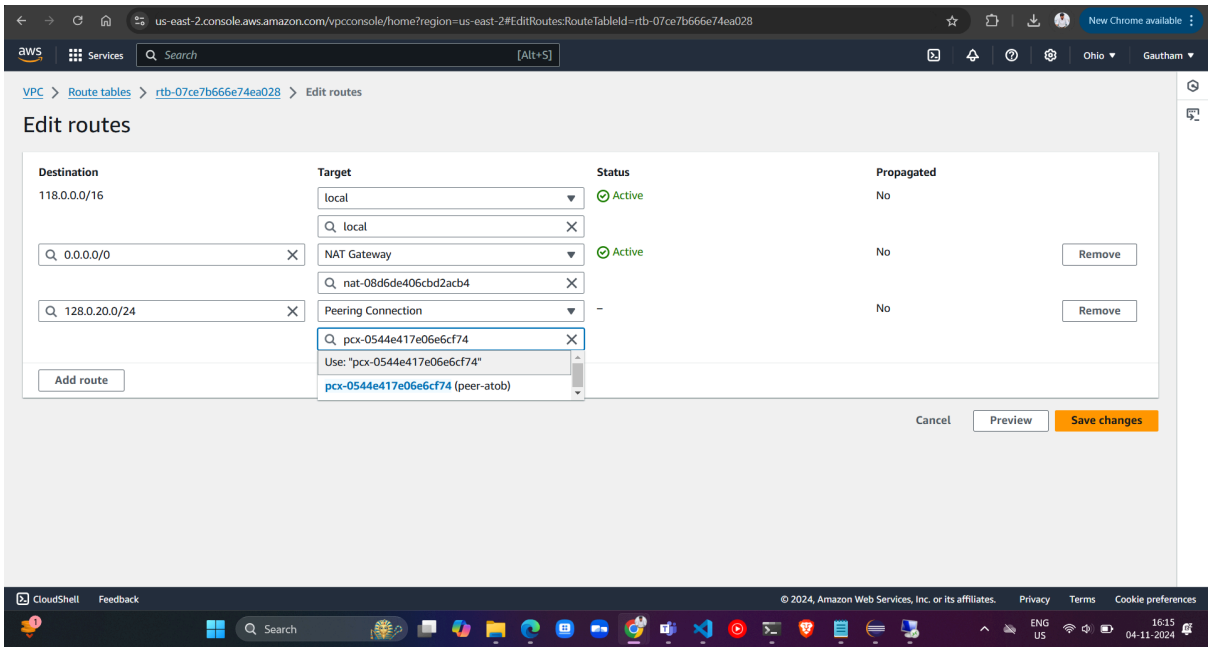




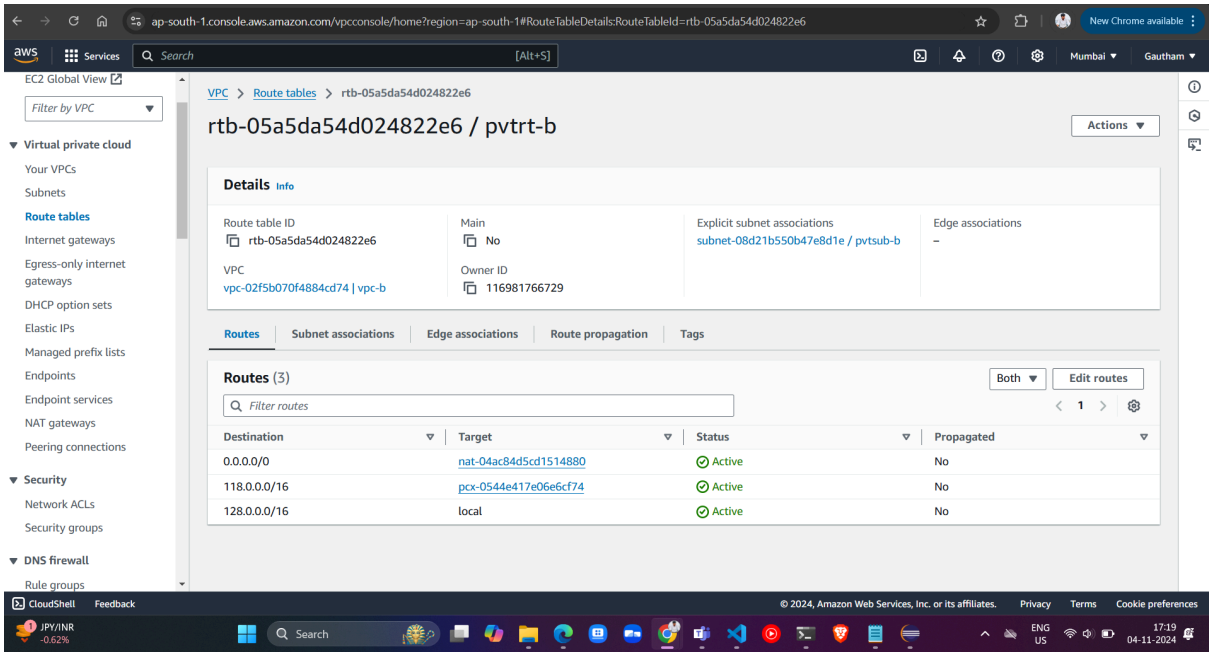


Route Configuration:

- Update `pvtrt-a` to route `128.0.20.0/24` through the peering connection.



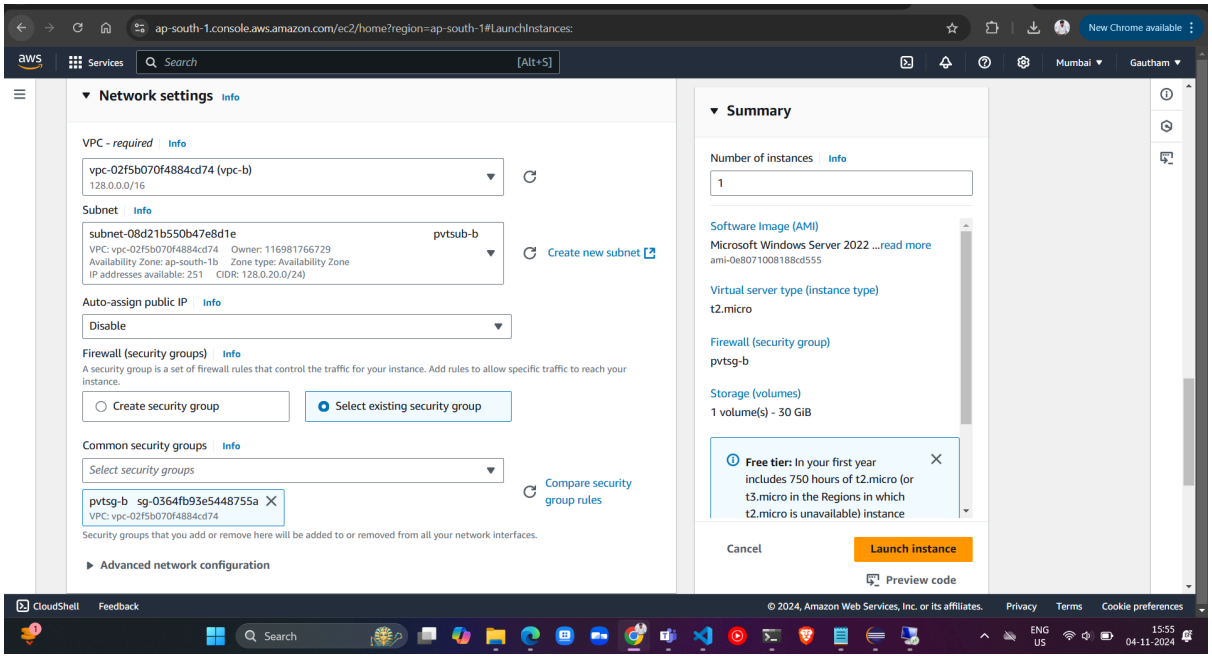
- Update `pvtrt-b` to route `118.0.20.0/24` through the peering connection.

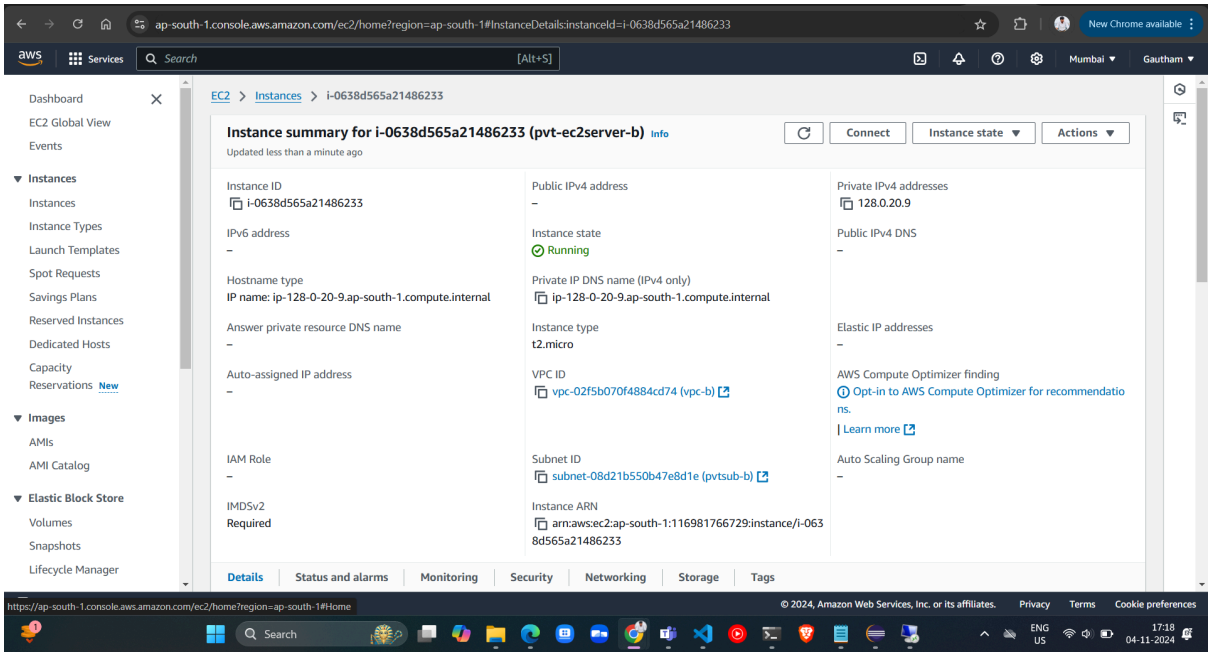


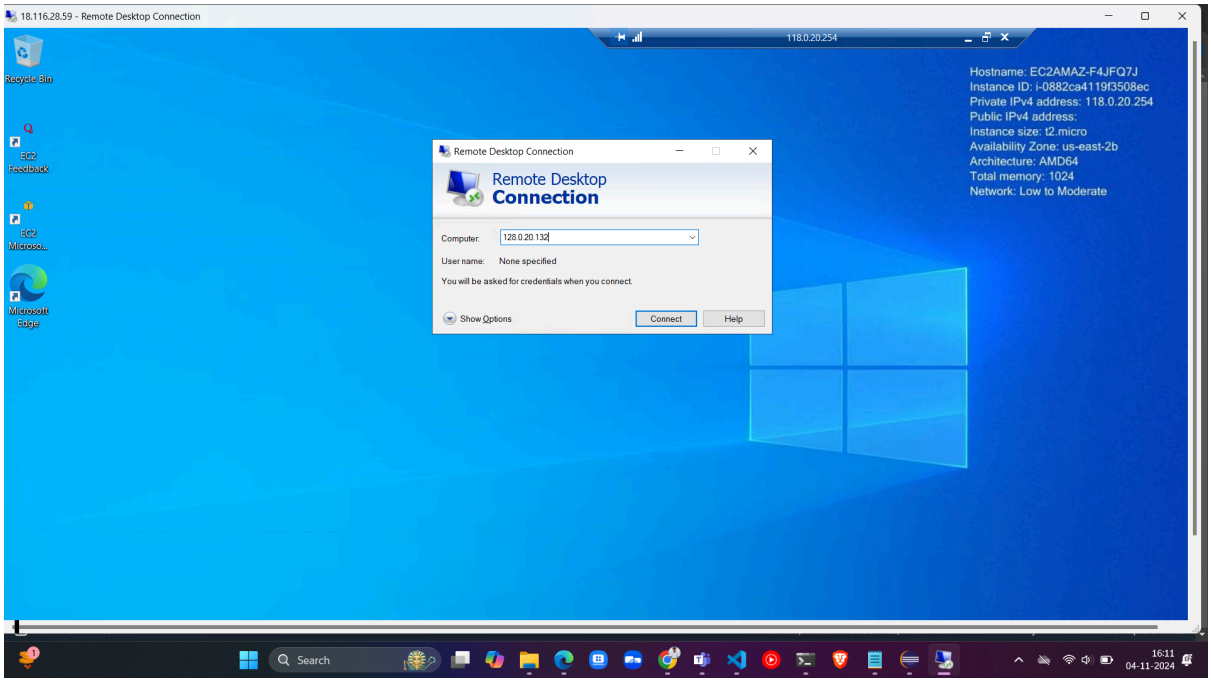
Step 18: Launch EC2 Instances in VPC-A

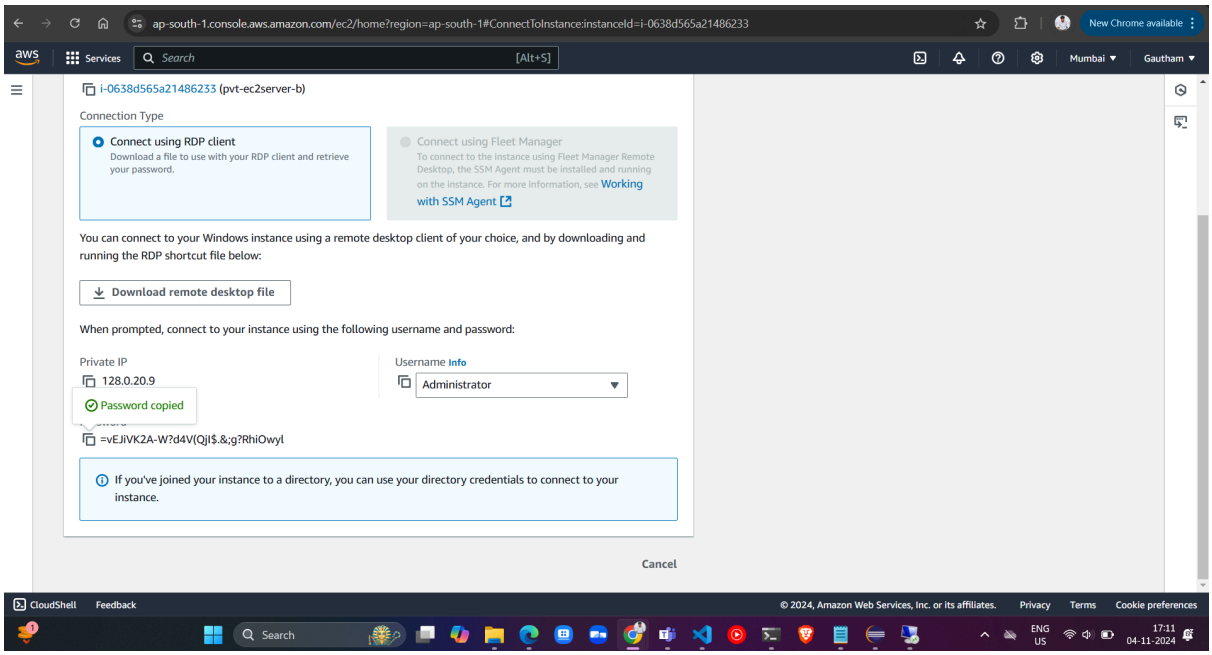
Private EC2 Connection:

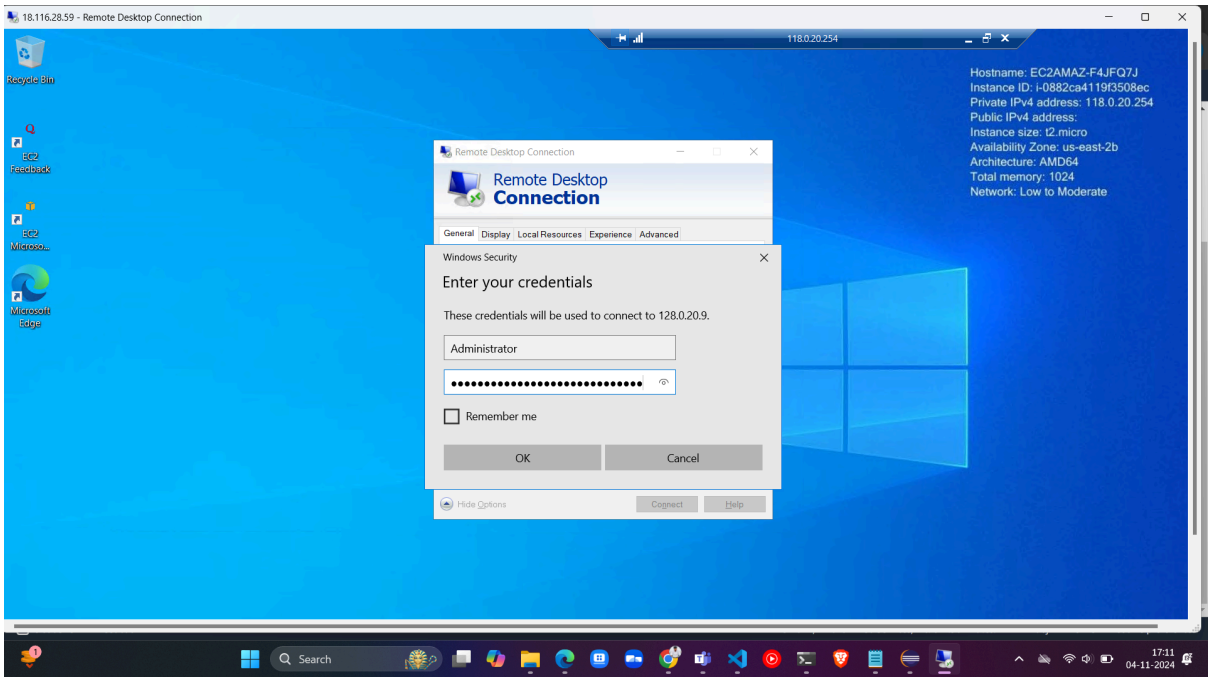
- Connect `pvt-ec2-a` (Ohio) to `pvt-ec2-b` (Mumbai) using **Remote Desktop Connection**.
- Ensure successful connectivity by verifying the private IP address response.

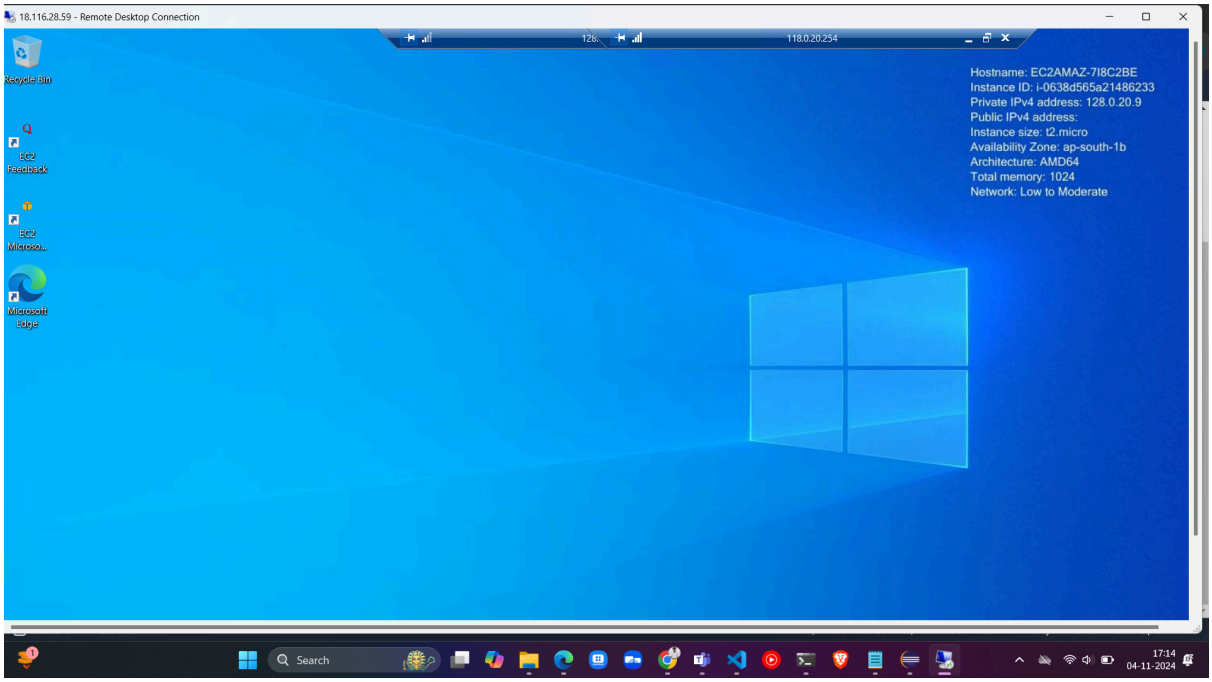



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0638d565a21486233
New Chrome available
aws
Services
Search
[Alt+S]
Mumbai
Gautham
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
EC2 > Instances > i-0638d565a21486233
Instance summary for i-0638d565a21486233 (pvt-ec2server-b) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-0638d565a21486233
Public IPv4 address
–
Private IPv4 addresses
128.0.20.9
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-128-0-20-9.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-128-0-20-9.ap-south-1.compute.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
–
VPC ID
vpc-02f5b070f4884cd74 (vpc-b)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
IAM Role
–
Subnet ID
subnet-08d21b550b47e8d1e (pvtsub-b)
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:ap-south-1:116981766729:instance/i-0638d565a21486233
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG US
17:18
04-11-2024


18.116.28.59 - Remote Desktop Connection
118.0.20.254
Recycle Bin
EC2 Feedback
EC2 Microso...
Microsoft Edge
Hostname: EC2AMAZ-F4JFQ7J
Instance ID: i-0882ca4119f3508ec
Private IPv4 address: 118.0.20.254
Public IPv4 address:
Instance size: t2.micro
Availability Zone: us-east-2b
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate
Remote Desktop Connection
Remote Desktop Connection
Computer:
128.0.20.132
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
Search
16:11
04-11-2024


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-0638d565a21486233
New Chrome available
aws
Services
Search
[Alt+S]
Mumbai
Gautham
i-0638d565a21486233 (pvt-ec2server-b)
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:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Private IP
128.0.20.9
Password copied
Username Info
Administrator
=vEJiVK2A-W?d4V(QjI$.&;g?RhiOwyl
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
US
17:11
04-11-2024





Conclusion

By following this guide, users have successfully configured a secure, interconnected AWS environment with VPC peering between Ohio and Mumbai regions, enabling secure communication between private instances across regions. The multi-region setup ensures high availability and network segmentation for application workloads.