Cloud Security and Management Assignment-1

Name :- Maanav Singh

Batch :- 3 (CCVT)

SAP ID :- 500108304

Enrollment no. :-R2142220977

Faculty :- Dr. Avita Katal

Objective:- This assignment focuses on understanding and configuring a Virtual Private Cloud (VPC) in a cloud environment, with both theoretical concepts and practical implementation using a cloud platform like AWS.

Part 1: Theoretical Assignment

Questions:

1. Define VPC and explain its concept in detail.

2. Discuss the benefits of using VPCs in cloud computing.

3. Describe the key components of a VPC. Include Subnets, Route Tables, Internet Gateway, NAT Gateway, and Security Groups.

4. Compare VPC with traditional on-premises networking.

5. Explain how VPC differs from traditional LANs and VPNs.

6. What is the significance of subnets in a VPC?

7. Discuss the difference between public and private subnets.

8. Explain the role of Security Groups and Network Access Control Lists (NACLs) in securing a VPC. Compare and contrast Security Groups and NACLs.

9. Explain why a NAT Gateway is necessary and where it is typically used in a VPC architecture. How does a NAT Gateway work in a VPC?

10. Describe the process of peering two VPCs, its use cases, and potential challenges?

Name → Maanav Singh
SAP ID → 500108304

Page No.
Date:
YOUVA

Q-1 Define VPC and explain its concept in detail.

→ A Virtual Private Cloud (VPC) is a logically isolated section of the cloud, such as AWS, where you can launch ~~instance~~ resources like EC2 instances in a virtual network. You have complete control over your VPC, including IP address ranges, subnets, route tables, and internet gateways. VPCs allow organizations to simulate the experience of having a private, on-premises network while utilizing cloud infrastructure. This concept enables users to securely connect their cloud resources to the internet, other VPCs, or on-premises data centers.

Q-2 Discuss the benefits of using VPCs in cloud computing.

→ The key benefits of using VPCs include :-

- Isolation → Logical separation from other virtual networks ensures data privacy.
- Security → Users can configure security measures like security groups and NACLs.
- Flexibility → VPC allows users to customize IP ranges, subnets and routing rules.
- Scalability → Cloud-based VPCs can scale on demand without physical hardware limits.
- Hybrid connectivity → VPCs can connect with on-premises data centers through VPNs or Direct Connect.

Q-3 Describe the key components of a VPC.

→ Key components of a VPC include :-

- Subnets → Logical subdivisions of the VPC network. Subnets can be public or private, with resources deployed in different subnets based on accessibility.

- Route Tables → Define rules that control how traffic is directed within the VPC. Each subnet is associated with a route table.
- Internet Gateway → Enables communication between instances in the VPC and the internet.
- NAT Gateway → Allows instances in a private subnet to access the internet without exposing them to inbound traffic.
- Security Groups → Stateful firewalls that control inbound and outbound traffic to and from resources like EC2 instances.

Q-4 Compare VPC with traditional on-premises networking.

→ VPCs are similar to on-premises networks but hosted in the cloud. In traditional on-premises networks :-

- Infrastructure Management → you manage all physical devices, such as routers and switches, whereas in a VPC, this infrastructure is ~~vital~~ virtual and managed by cloud provider.
- Scalability → On-premises networks have limited scalability based on hardware, while VPCs can easily scale in the cloud.
- Cost → On-premises requires up-front capital investment, while VPCs are more cost-effective with a pay-as-you-go model.

Q-5 Explain how VPC differs from traditional LANs and VPNs.

→ • VPC v/s LANs → While both provide network segmentation, VPCs are virtual networks within the cloud, whereas LANs are physical networks confined to a specific location.

- VPC v/s VPNs → VPNs are secure, encrypted connections between two networks (eg. a corporate LAN and the cloud). VPCs are complete cloud-based virtual networks with their own components like subnets and route tables.

Q-6 What is the significance of subnets in a VPC?
→ Subnets divide the VPC's IP address range into smaller segments, allowing you to group resources based on security or accessibility needs. Subnets enable logical separation of resources (eg. web servers in public subnets and databases in private subnets) and control traffic flow.

Q-7 Discuss the difference between public and private subnets.
→ • Public Subnets → Resources in public subnets have direct access to the internet via an Internet Gateway. Typically used for public-facing resources like web servers.

- Private Subnets → Resources in private subnets do not have direct internet access. They use a NAT Gateway for outbound communication while remaining inaccessible from the internet.

Q-8 Explain the role of Security Groups and Network Access Control Lists (NACLs) in securing a VPC. Compare and contrast Security Groups and NACLs.
→ • Security Groups → Act as stateful firewalls controlling inbound and outbound traffic to instances. They remember outgoing requests, allowing return traffic automatically.
- NACLs → Stateless firewalls that control traffic at the subnet level. They check every request individually for both inbound and outbound rules.

Comparison

- Scope → Security groups are applied at the instance level, while NACLs operate at the subnet level.
- Statefulness → Security groups are stateful, while NACLs are stateless.
- Rules → Security groups only allow "allow" rules, whereas NACLs allow both "allow" and "deny" rules.

Q-9 Explain why a NAT gateway is necessary and where it is typically used in a VPC architecture. How does NAT gateway work in VPC?

→ A NAT gateway is necessary to allow instances in private subnets to access the internet (e.g. for software updates) while preventing inbound internet traffic. It works by translating private IP addresses to public IP addresses for outbound traffic and then translating the responses back. NAT gateways are usually placed in public subnets, and private subnets route internet-bound traffic through them.

Q-10 Describe the process of peering two VPCs, its use cases, and potential challenges.

→ VPC peering allows two VPCs to communicate privately without routing traffic through the internet.
The process involves:-

1) Creating a VPC peering connection request from one VPC to another.
2) Accepting the peering request in the target VPC.
3) Updating the route tables in both VPCs to enable communication.

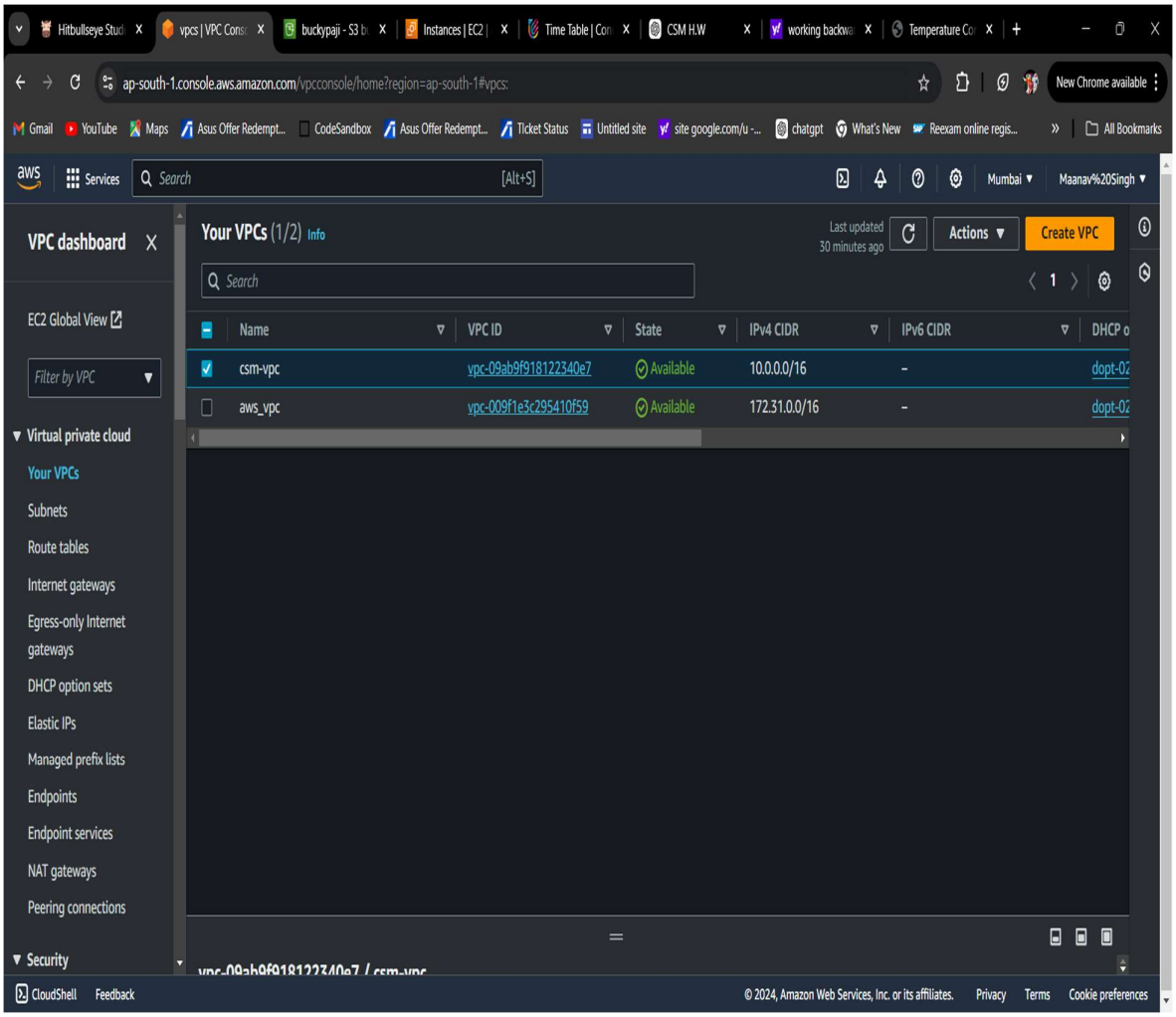
Use cases include inter-region data transfer, multi-VPC architectures, and microservices.
Challenges include managing route tables and ensuring IP address ranges do not overlap, as overlapping IP ranges prevent successful peering.

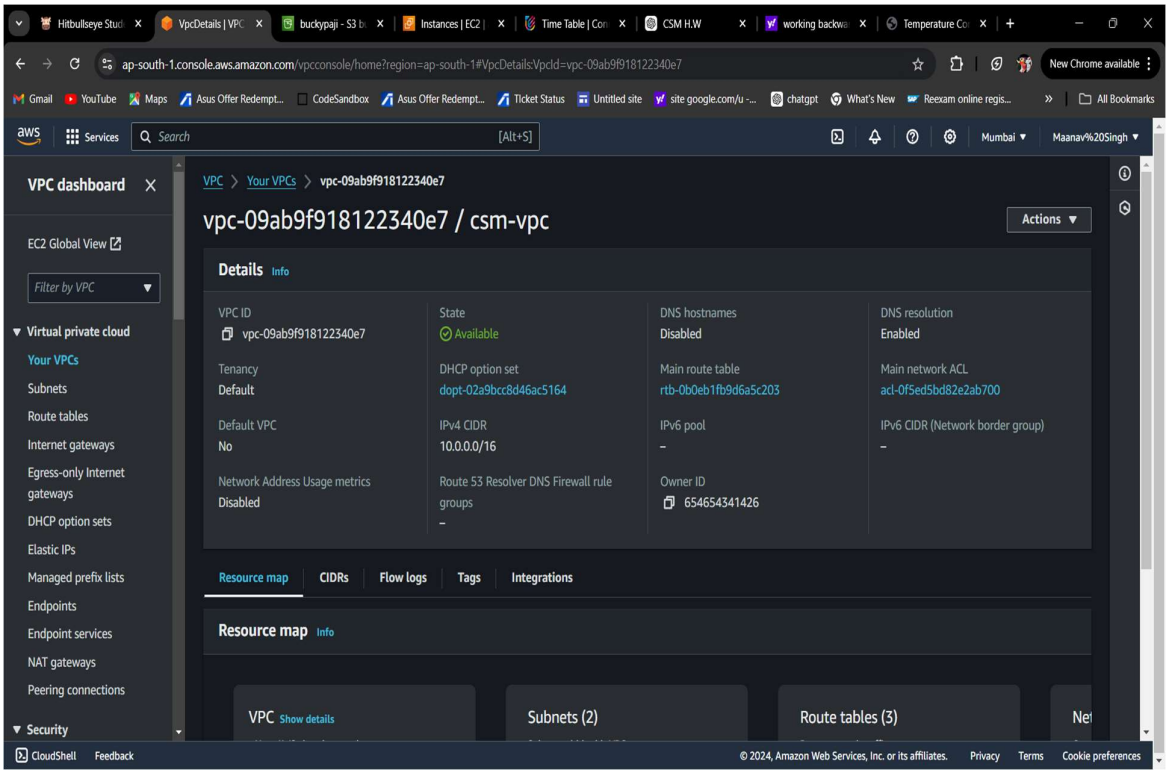
Part 2: Practical Assignment

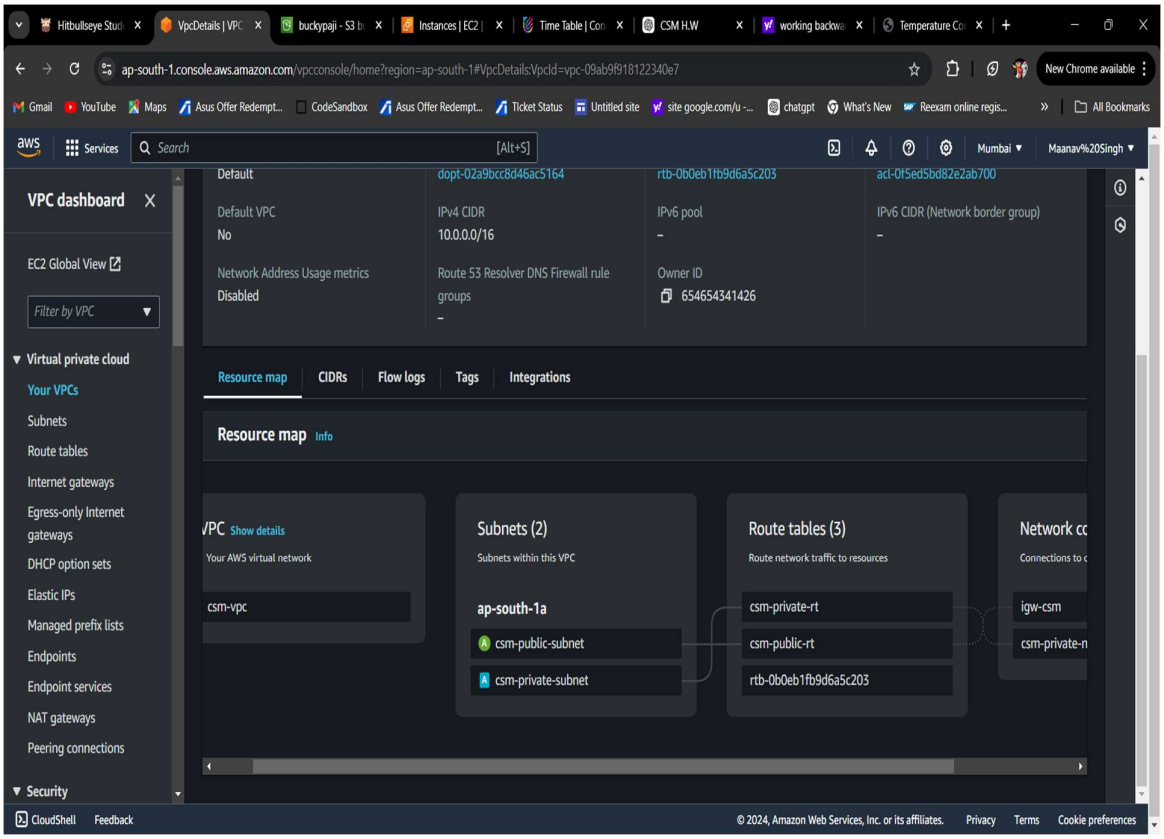
Objective: To provide hands-on experience in setting up and configuring a Virtual Private Cloud (VPC) on a cloud platform (AWS)

Task: 1. You will create and configure a VPC with the following specifications:

- **Create a VPC with a custom IP address range.**
- **Use the CIDR block: 10.0.0.0/16.**

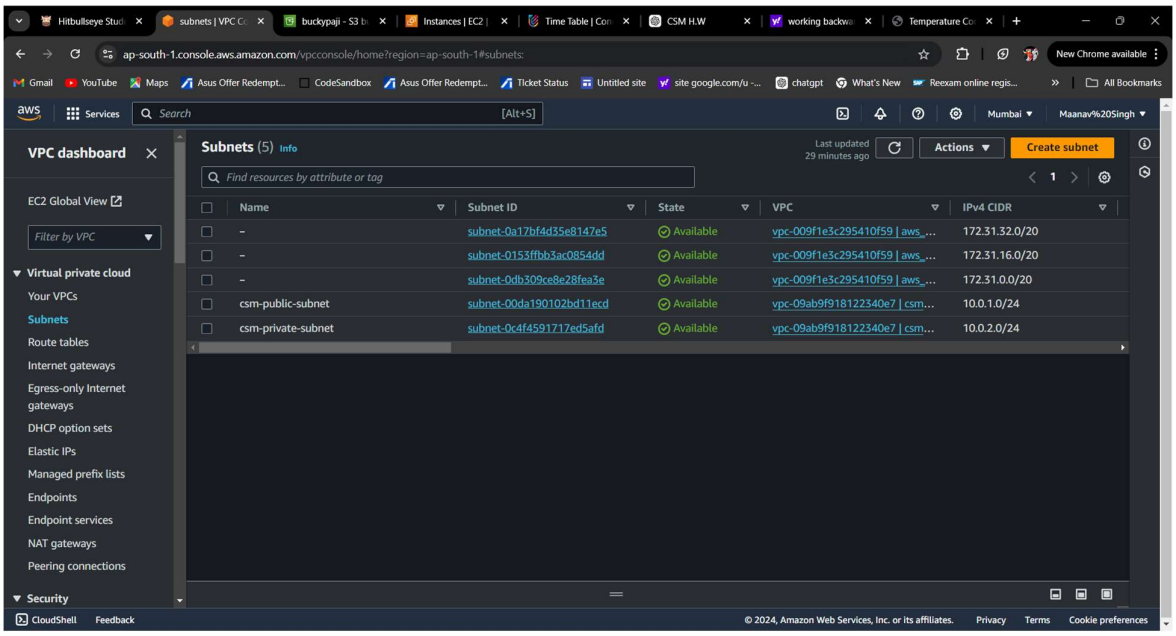


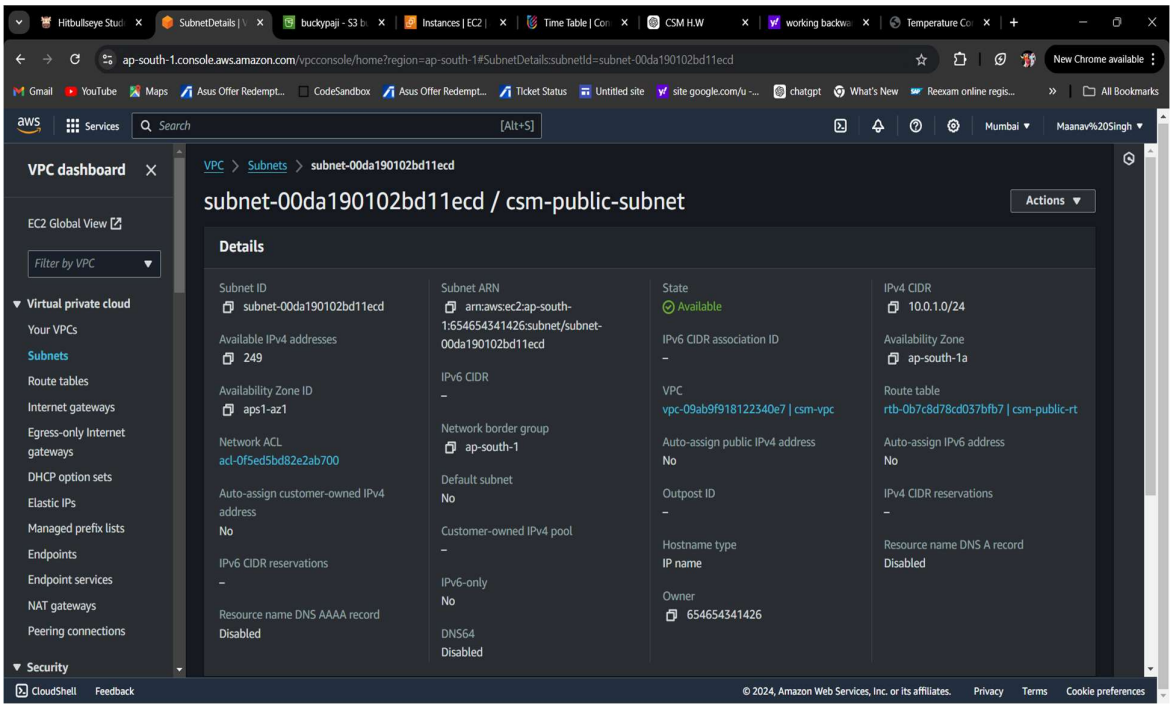

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-09ab9f918122340e7
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Your VPCs > vpc-09ab9f918122340e7
vpc-09ab9f918122340e7 / csm-vpc
Actions
Details Info
VPC ID
vpc-09ab9f918122340e7
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-02a9bcc8d46ac5164
Main route table
rtb-0b0eb1fb9d6a5c203
Main network ACL
acl-0f5ed5bd82e2ab700
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
-
IPv6 CIDR (Network border group)
-
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
-
Owner ID
654654341426
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Subnets (2)
Route tables (3)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

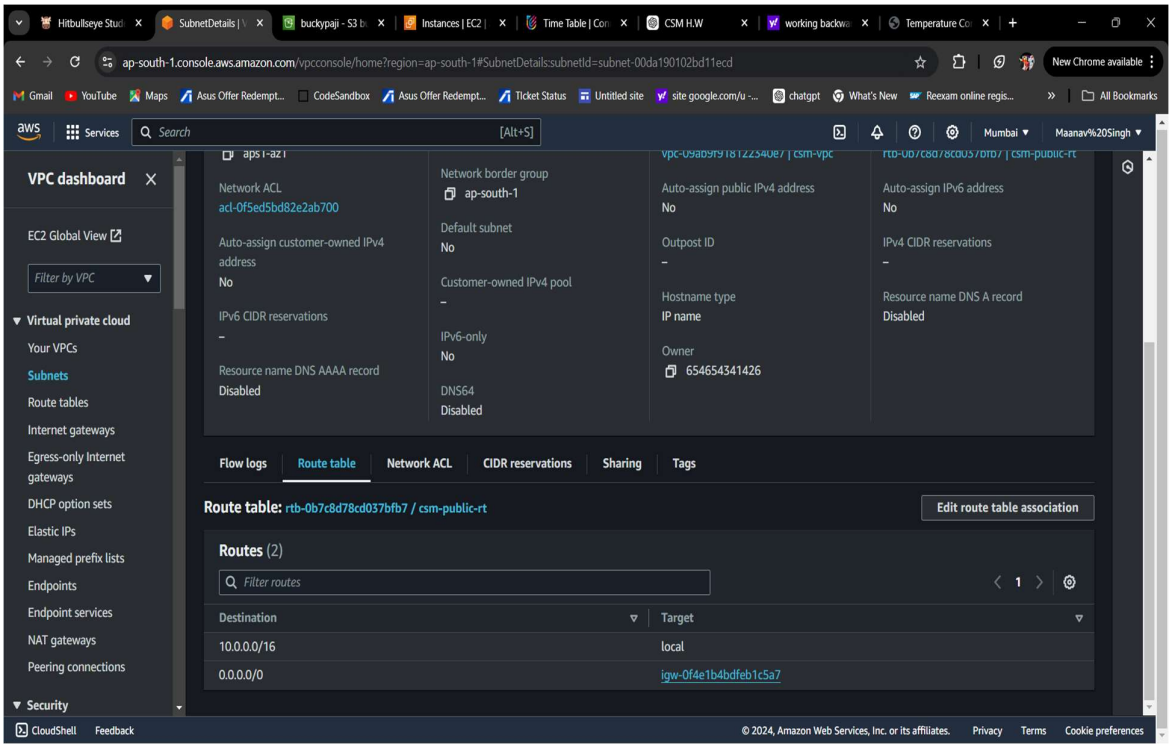

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-09ab9f918122340e7
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Default
dopt-02a9bcc8d46ac5164
rtb-0b0eb1fb9d6a5c203
acl-0f5ed5bd82e2ab700
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
-
IPv6 CIDR (Network border group)
-
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
-
Owner ID
654654341426
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
/PC Show details
Your AWS virtual network
csm-vpc
Subnets (2)
Subnets within this VPC
ap-south-1a
csm-public-subnet
csm-private-subnet
Route tables (3)
Route network traffic to resources
csm-private-rt
csm-public-rt
rtb-0b0eb1fb9d6a5c203
Network cc
Connections to c
igw-csm
csm-private-n
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

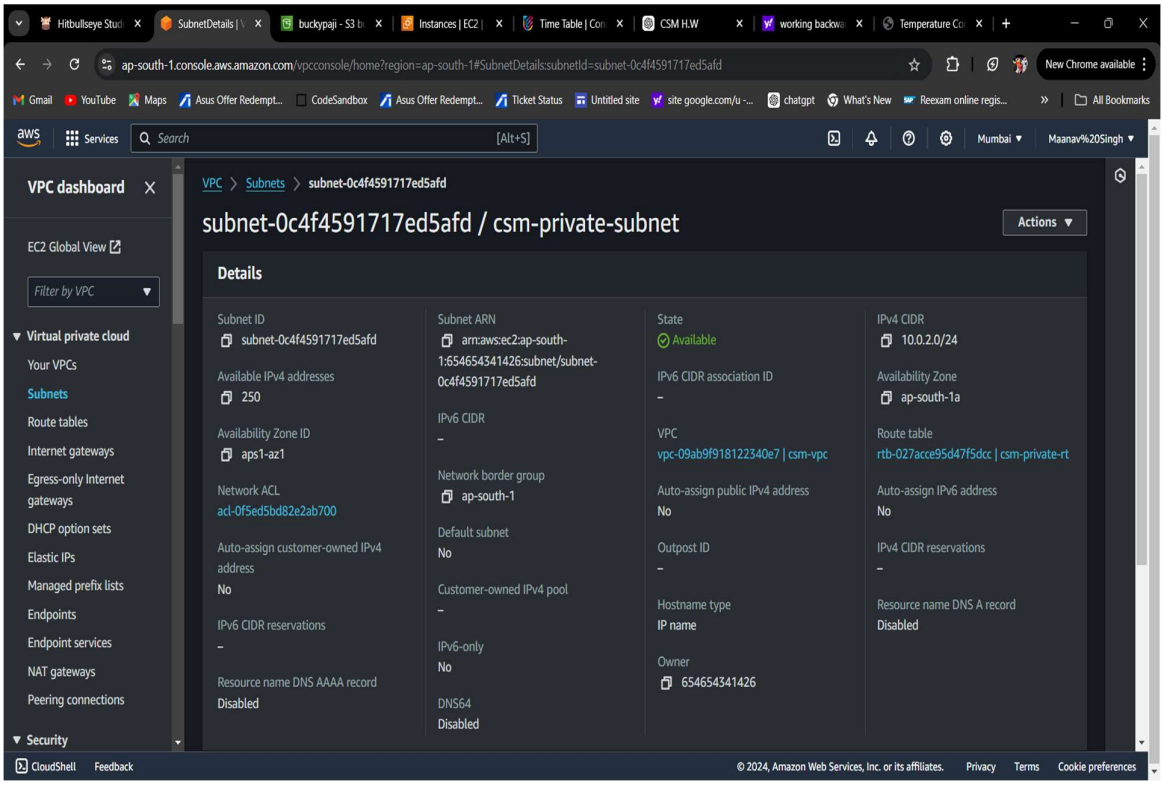
2. Create subnets:

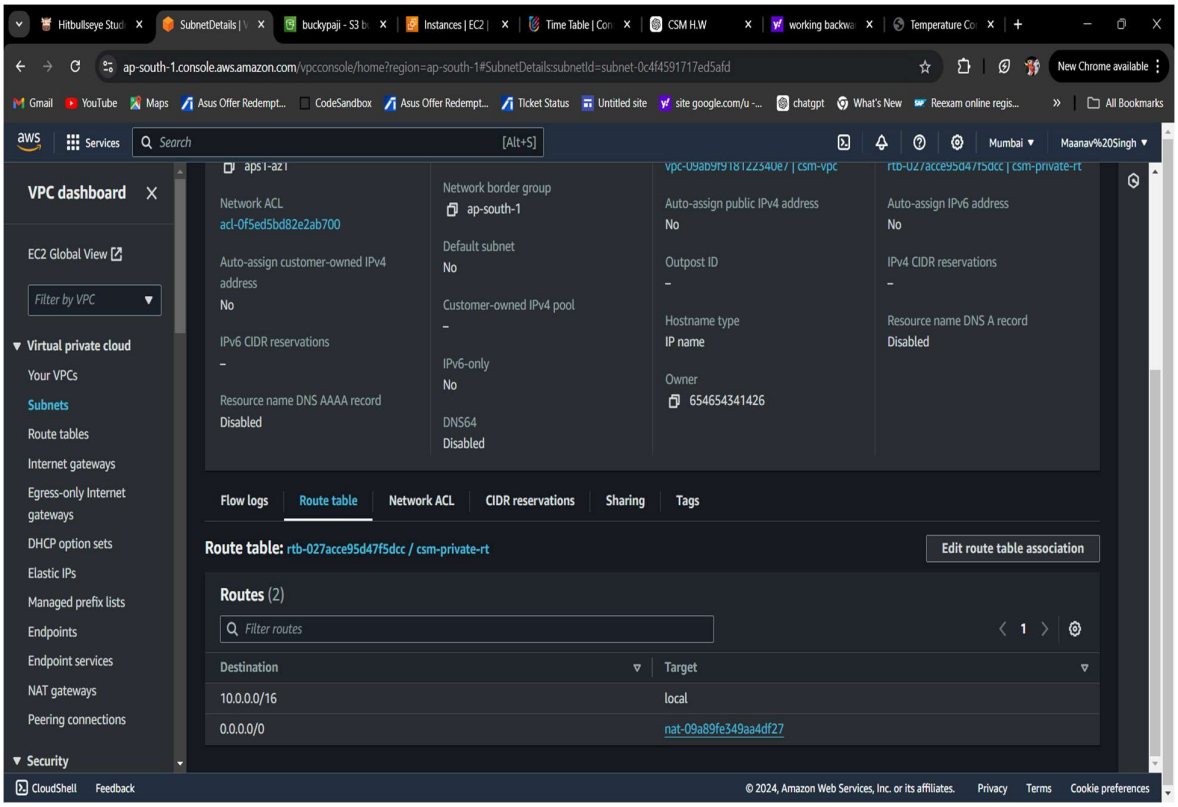
- **Create one public subnet in Availability Zone A with CIDR 10.0.1.0/24.**
- **Create one private subnet in Availability Zone A with CIDR 10.0.2.0/24.**



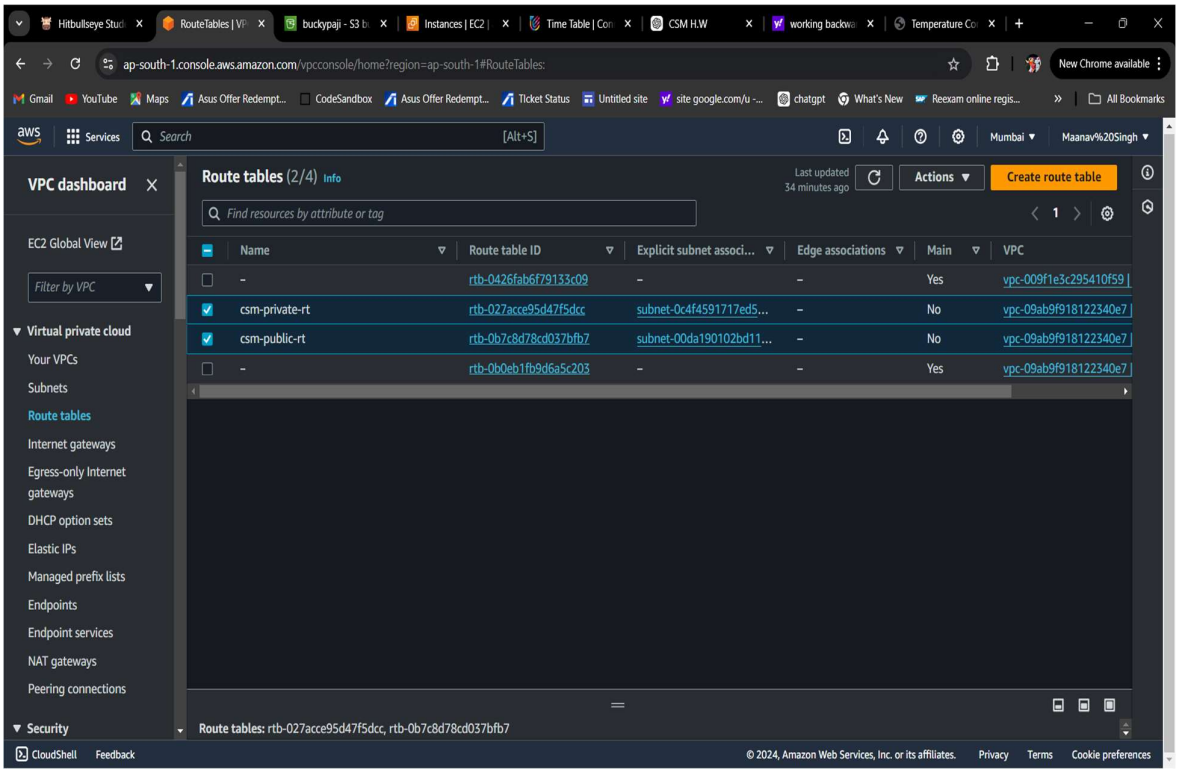


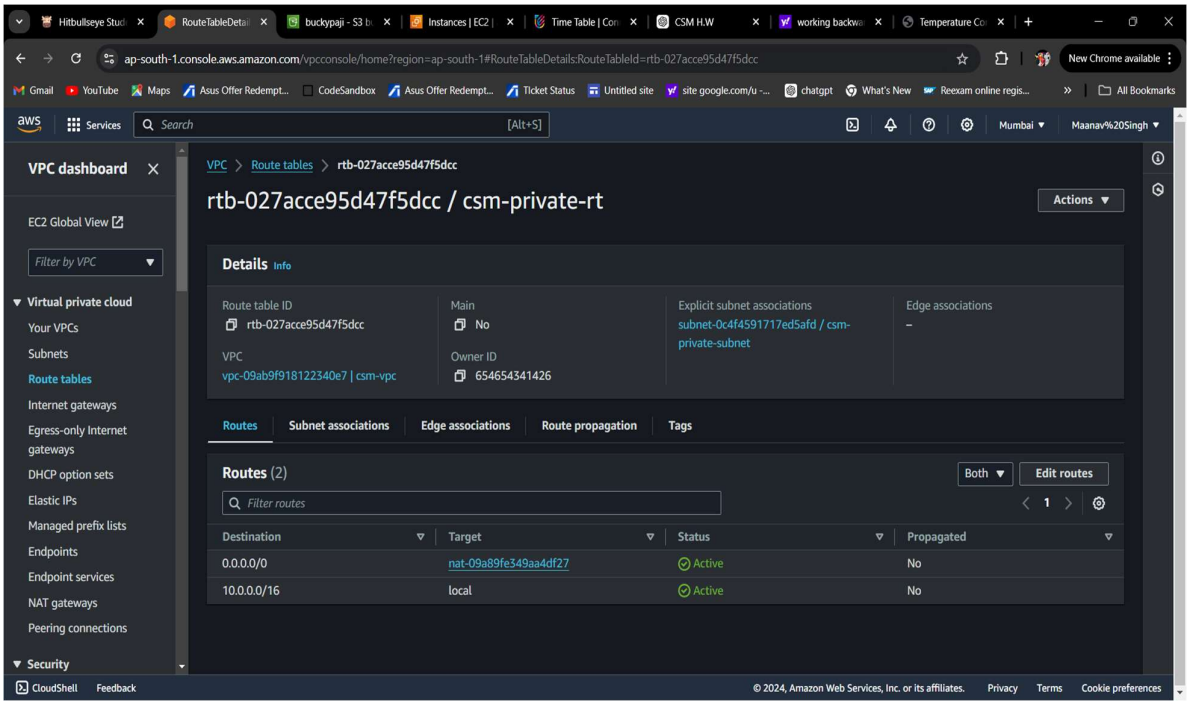

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SubnetDetails:subnetId=subnet-00da190102bd11ecd
VPC dashboard
Network ACL
acl-0f5ed5bd82e2ab700
Auto-assign customer-owned IPv4 address
No
IPv6 CIDR reservations
-
Resource name DNS AAAA record
Disabled
Network border group
ap-south-1
Default subnet
No
Customer-owned IPv4 pool
-
IPv6-only
No
DNS64
Disabled
Auto-assign public IPv4 address
No
Outpost ID
-
Hostname type
IP name
Owner
654654341426
Auto-assign IPv6 address
No
IPv4 CIDR reservations
-
Resource name DNS A record
Disabled
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Route table: rtb-0b7c8d78cd037bfb7 / csm-public-rt
Edit route table association
Routes (2)
Filter routes
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-0f4e1b4bdfeb1c5a7

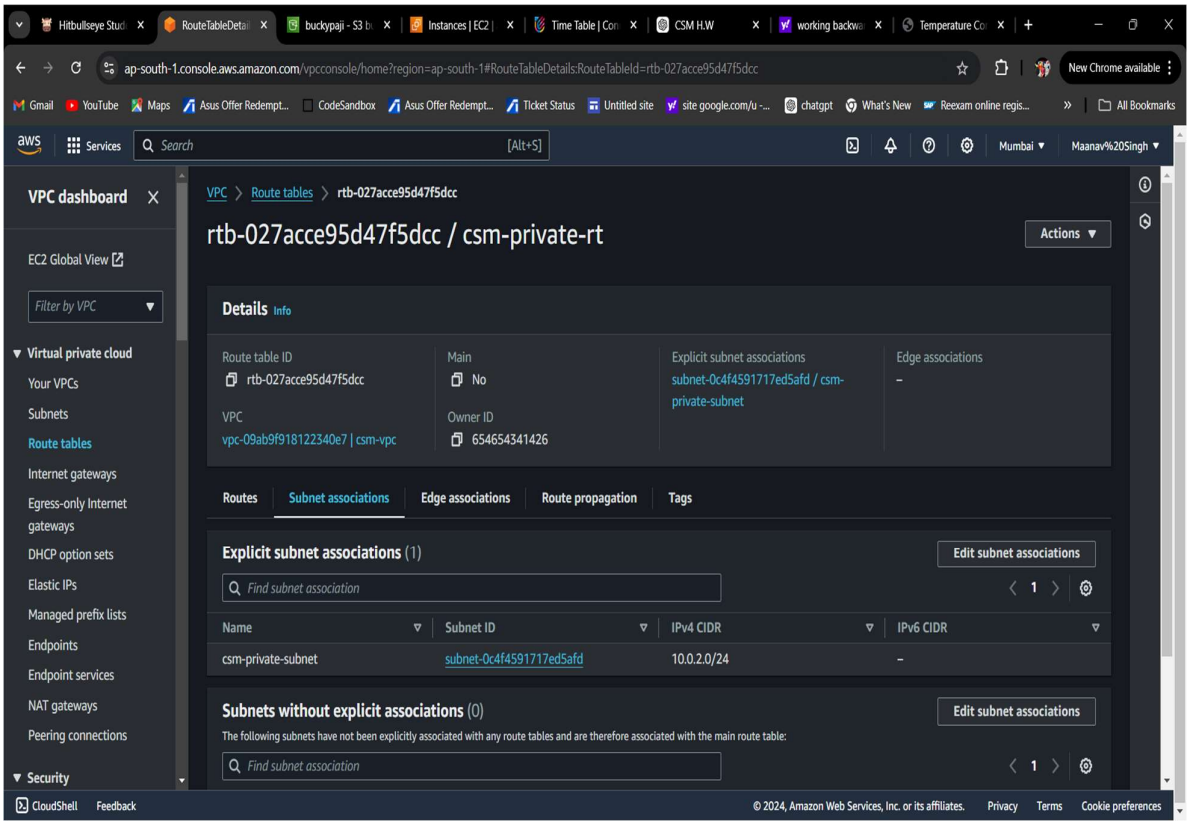

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c4f4591717ed5afd
VPC dashboard
VPC > Subnets > subnet-0c4f4591717ed5afd
subnet-0c4f4591717ed5afd / csm-private-subnet
Actions
Details
Subnet ID
subnet-0c4f4591717ed5afd
Available IPv4 addresses
250
Availability Zone ID
aps1-az1
Network ACL
acl-0f5ed5bd82e2ab700
Auto-assign customer-owned IPv4 address
No
IPv6 CIDR reservations
-
Resource name DNS AAAA record
Disabled
Subnet ARN
arn:aws:ec2:ap-south-1:654654341426:subnet/subnet-0c4f4591717ed5afd
IPv6 CIDR
-
Network border group
ap-south-1
Default subnet
No
Customer-owned IPv4 pool
-
IPv6-only
No
DNS64
Disabled
State
Available
IPv6 CIDR association ID
-
VPC
vpc-09ab9f918122340e7 | csm-vpc
Auto-assign public IPv4 address
No
Outpost ID
-
Hostname type
IP name
Owner
654654341426
IPv4 CIDR
10.0.2.0/24
Availability Zone
ap-south-1a
Route table
rtb-027acce95d47f5dcc | csm-private-rt
Auto-assign IPv6 address
No
IPv4 CIDR reservations
-
Resource name DNS A record
Disabled

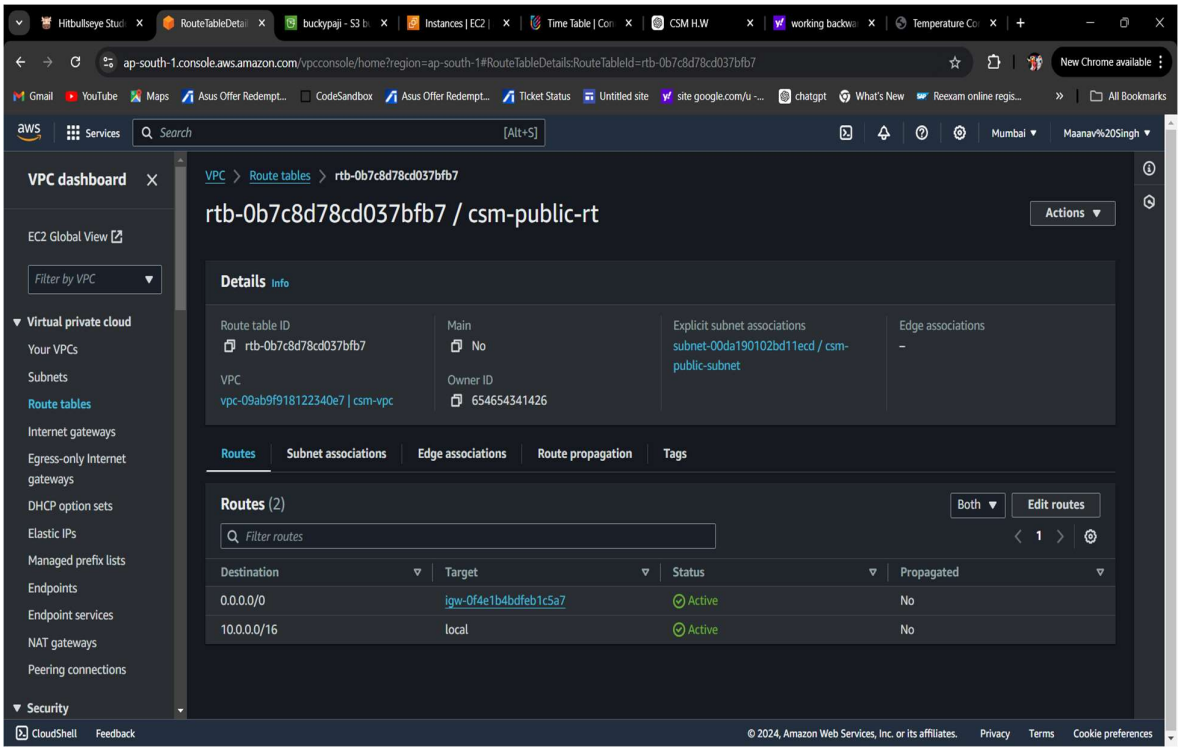


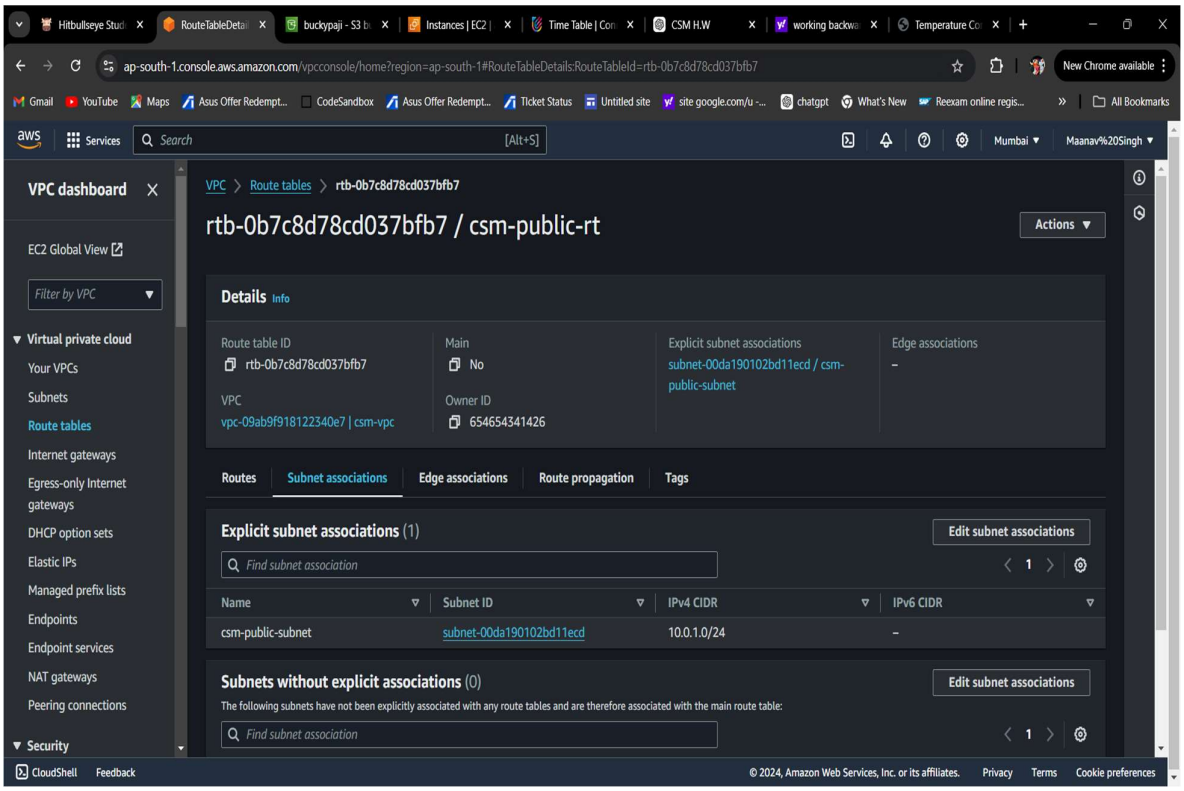
Creating Route Tables for both subnets.




ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-027acce95d47f5dcc
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
VPC > Route tables > rtb-027acce95d47f5dcc
rtb-027acce95d47f5dcc / csm-private-rt
Actions
Details Info
Route table ID
rtb-027acce95d47f5dcc
Main
No
Explicit subnet associations
subnet-0c4f4591717ed5afd / csm-private-subnet
Edge associations
-
VPC
vpc-09ab9f918122340e7 | csm-vpc
Owner ID
654654341426
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
nat-09a89fe349aa4df27
Active
No
10.0.0.0/16
local
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

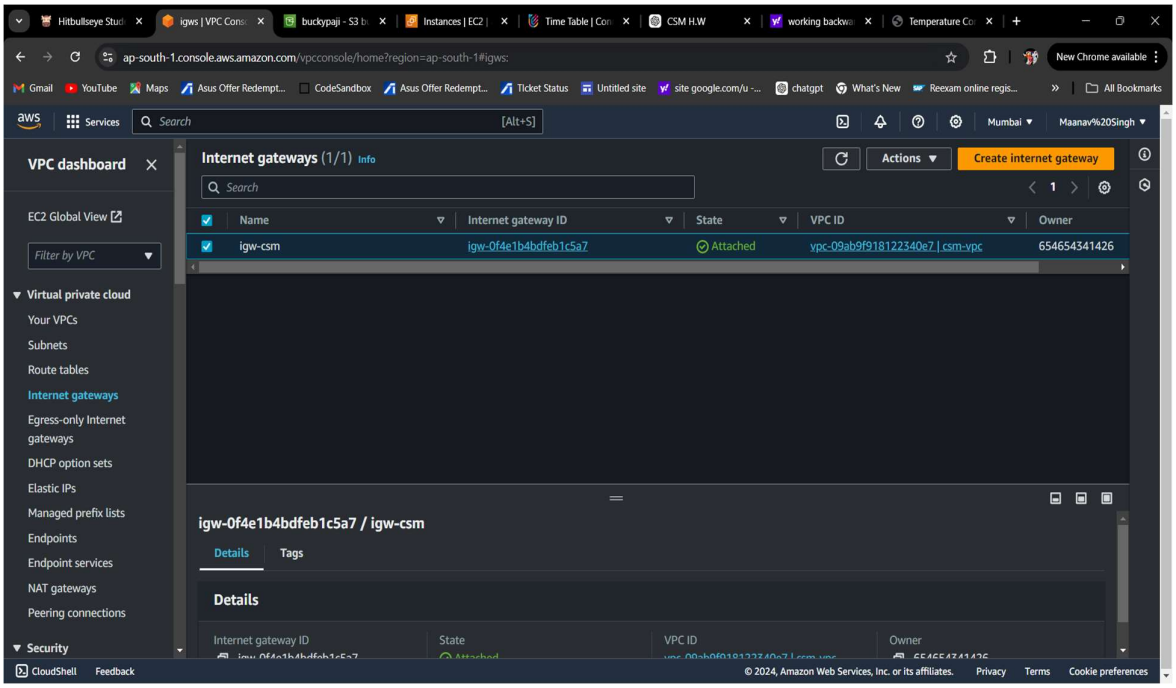

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-027acce95d47f5dcc
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Route tables > rtb-027acce95d47f5dcc
rtb-027acce95d47f5dcc / csm-private-rt
Actions
Details Info
Route table ID
rtb-027acce95d47f5dcc
Main
No
Explicit subnet associations
subnet-0c4f4591717ed5afd / csm-private-subnet
Edge associations
-
VPC
vpc-09ab9f918122340e7 | csm-vpc
Owner ID
654654341426
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
csm-private-subnet
subnet-0c4f4591717ed5afd
10.0.2.0/24
-
Subnets without explicit associations (0)
Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Find subnet association
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

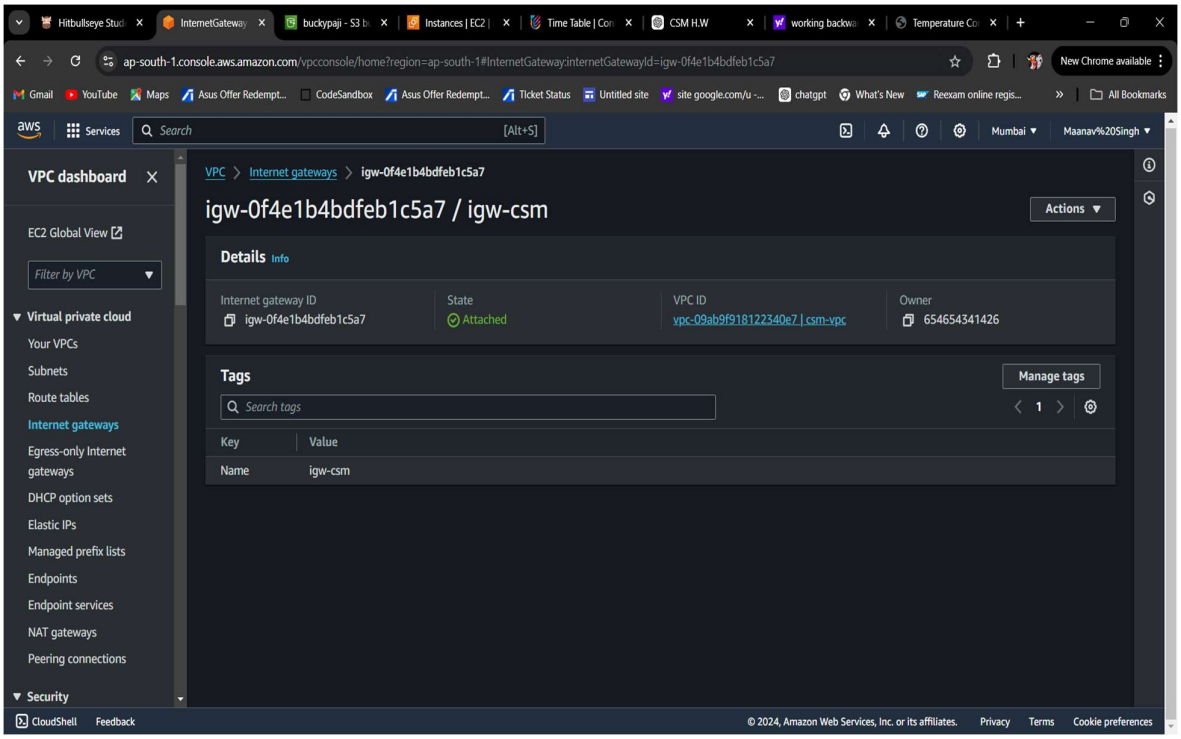

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0b7c8d78cd037bfb7
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Route tables > rtb-0b7c8d78cd037bfb7
rtb-0b7c8d78cd037bfb7 / csm-public-rt
Actions
Details Info
Route table ID
rtb-0b7c8d78cd037bfb7
Main
No
Explicit subnet associations
subnet-00da190102bd11ecd / csm-public-subnet
Edge associations
–
VPC
vpc-09ab9f918122340e7 | csm-vpc
Owner ID
654654341426
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-0f4e1b4bdfeb1c5a7
Active
No
10.0.0.0/16
local
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0b7c8d78cd037bfb7
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
VPC > Route tables > rtb-0b7c8d78cd037bfb7
rtb-0b7c8d78cd037bfb7 / csm-public-rt
Actions
Details Info
Route table ID
rtb-0b7c8d78cd037bfb7
Main
No
Explicit subnet associations
subnet-00da190102bd11ecd / csm-public-subnet
Edge associations
–
VPC
vpc-09ab9f918122340e7 | csm-vpc
Owner ID
654654341426
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
csm-public-subnet
subnet-00da190102bd11ecd
10.0.1.0/24
–
Subnets without explicit associations (0)
Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Find subnet association
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

3. Internet Gateway: Attach an Internet Gateway to the VPC.

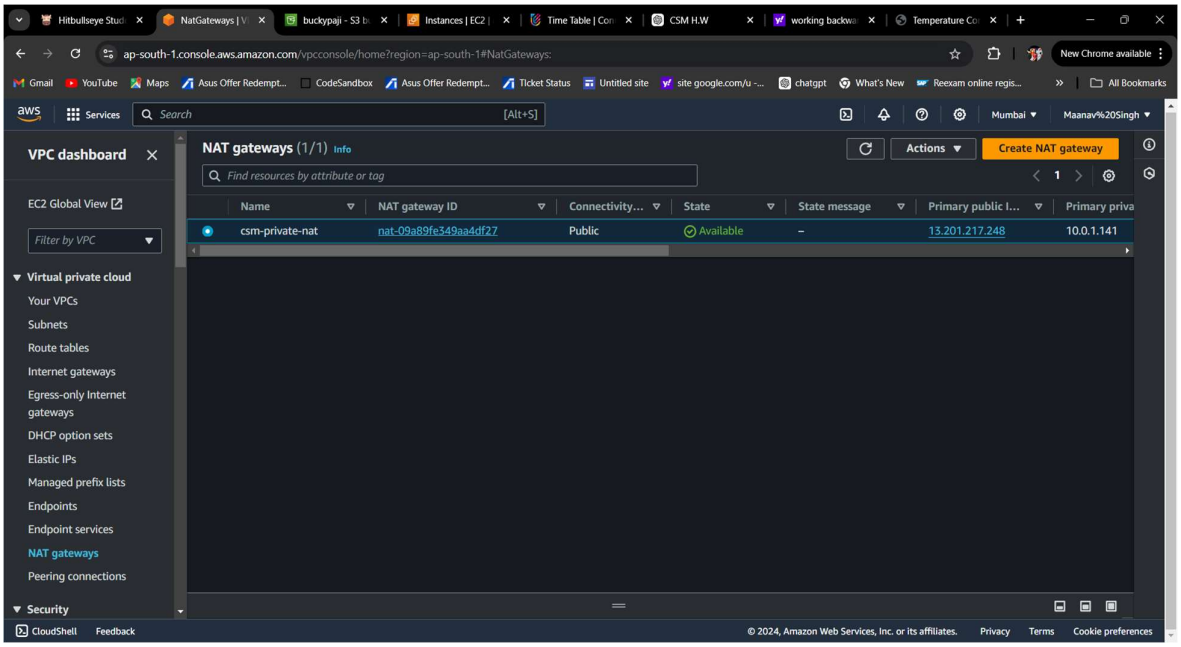
• Configure the public subnet to route traffic to the Internet Gateway.

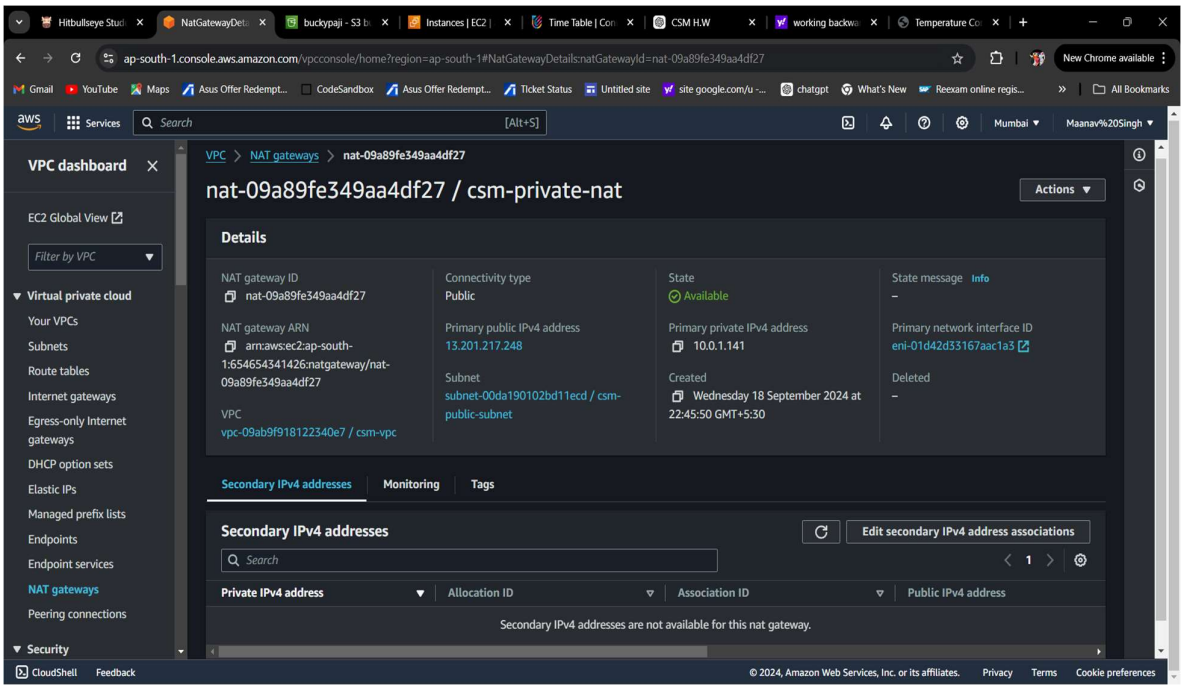




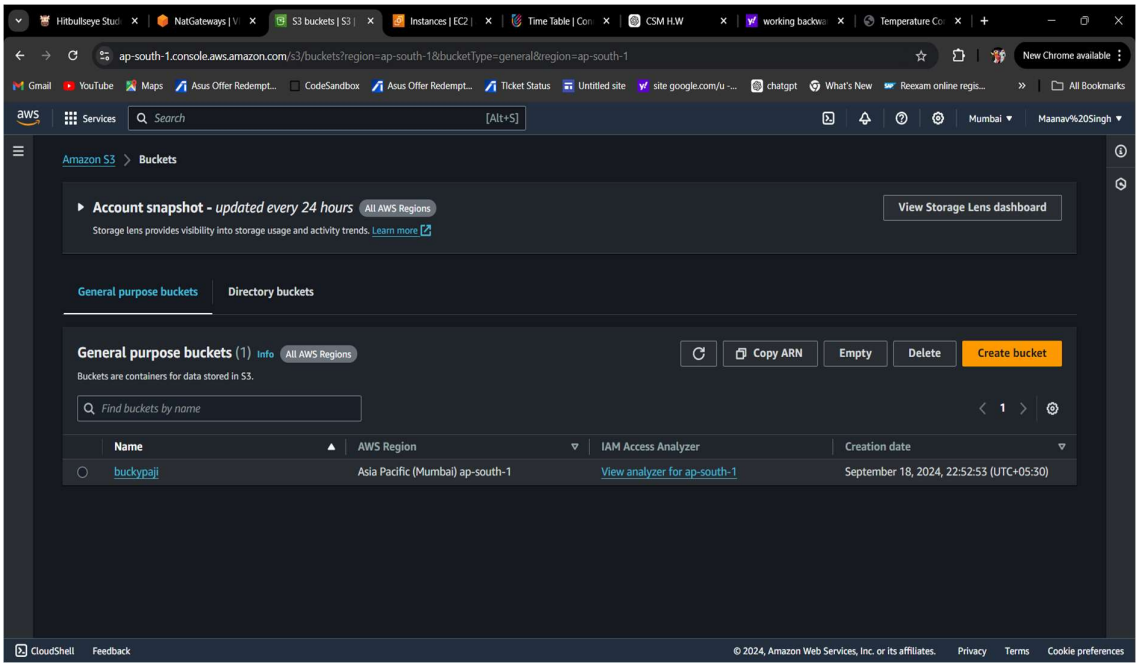
4. NAT Gateway: Set up a NAT Gateway in the public subnet.

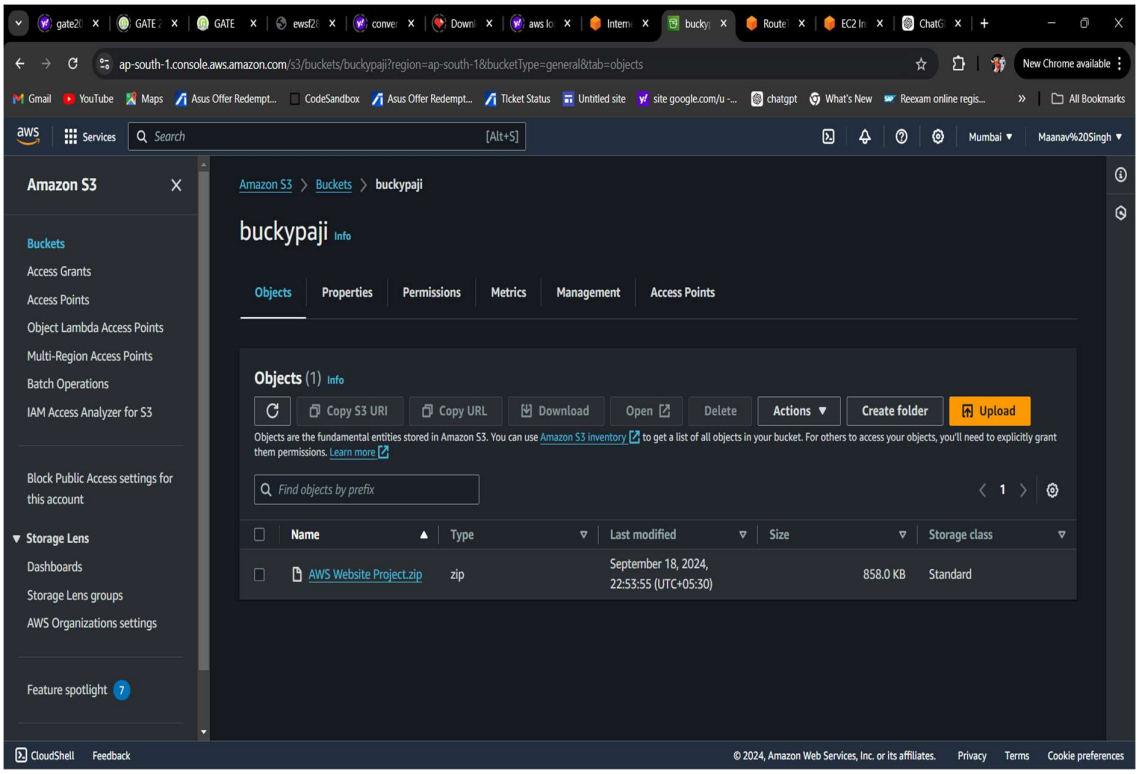
• Modify the route table of the private subnet to allow instances in the private subnet to access the internet via the NAT Gateway.





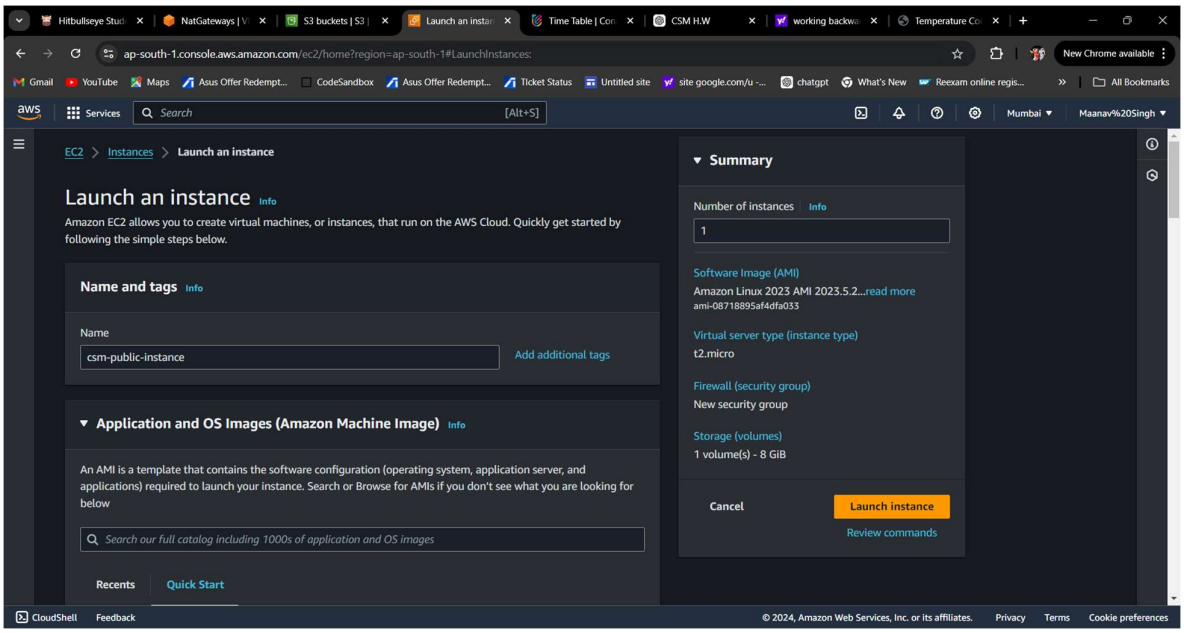
Creating S3 for Testing Connectivity for public instance using SSH

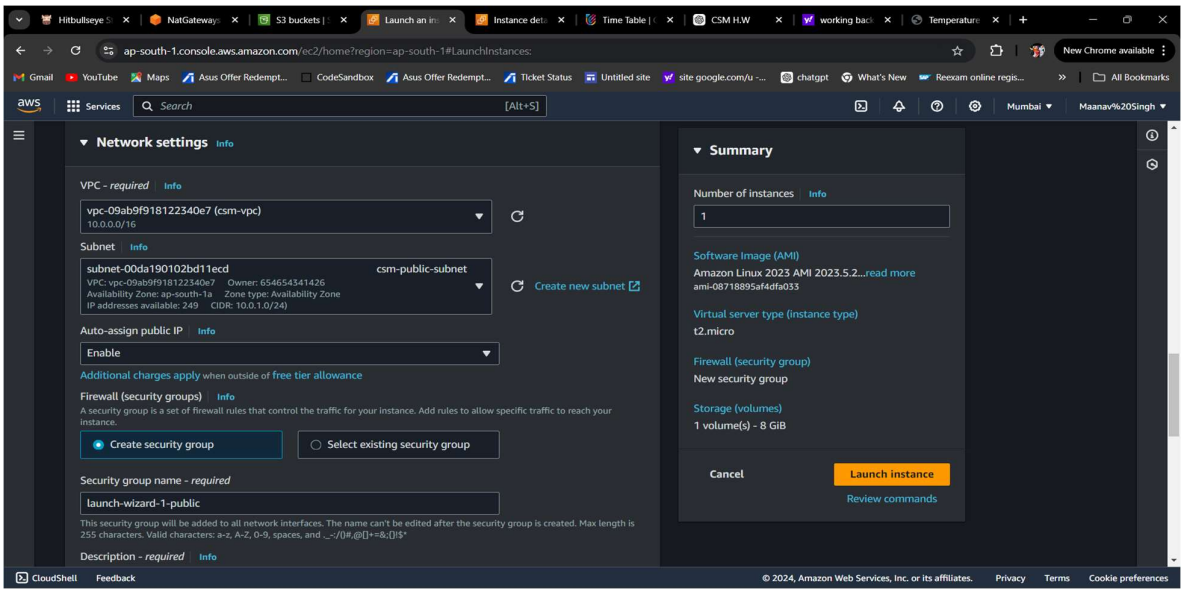


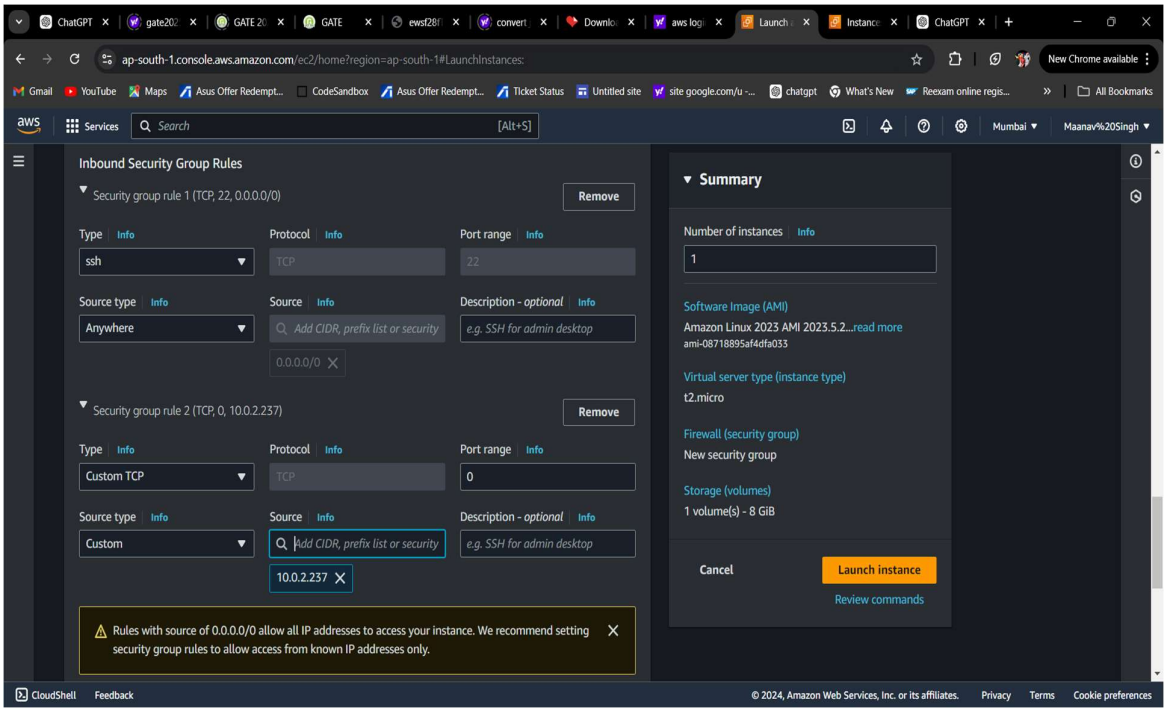


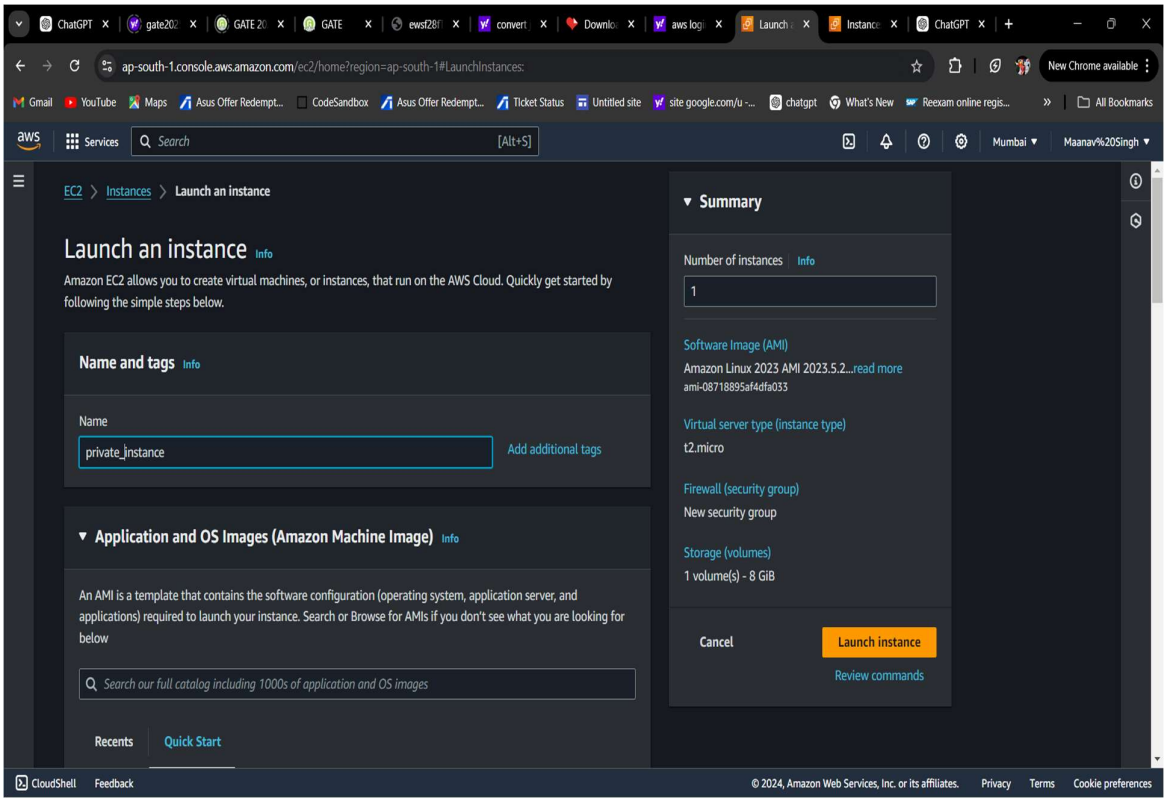
5. Launch EC2 instances (or similar on other platforms):

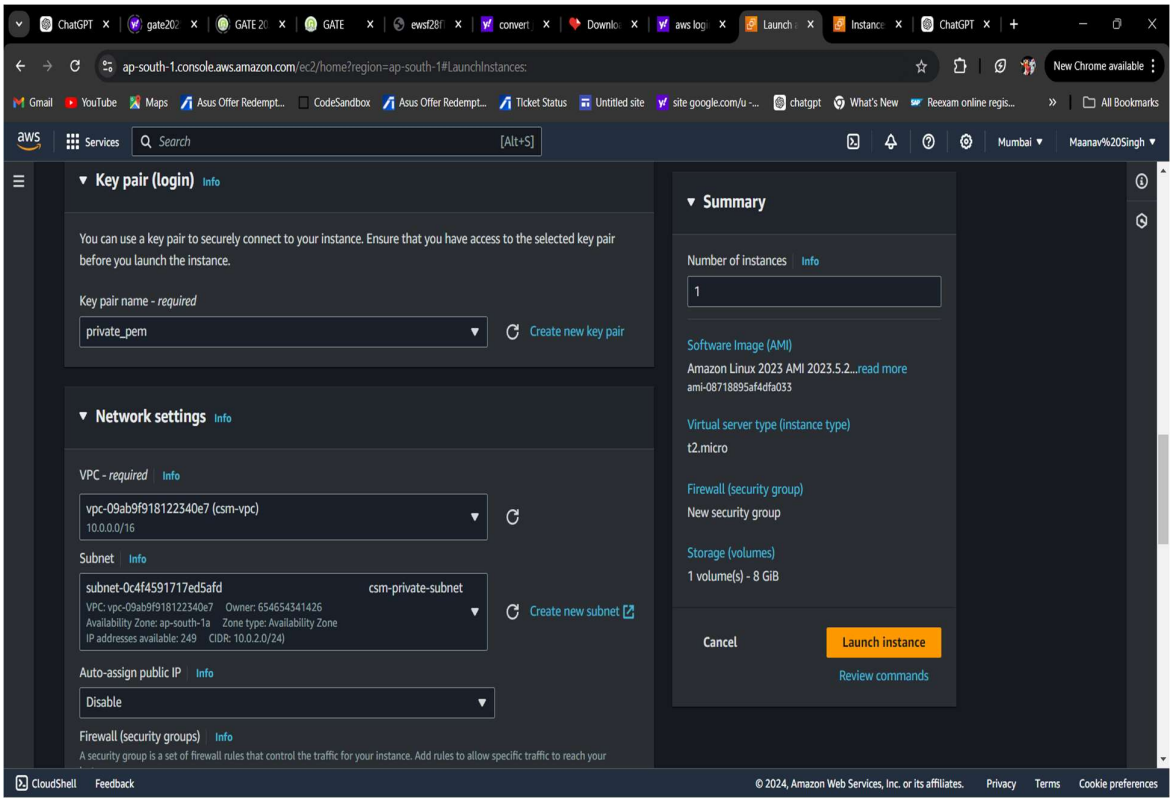
- **Launch one instance in the public subnet and one instance in the private subnet.**
- **Ensure the public instance can be accessed from the internet using an Elastic IP.**
- **Ensure the private instance can access the internet but cannot be accessed directly from the internet.**

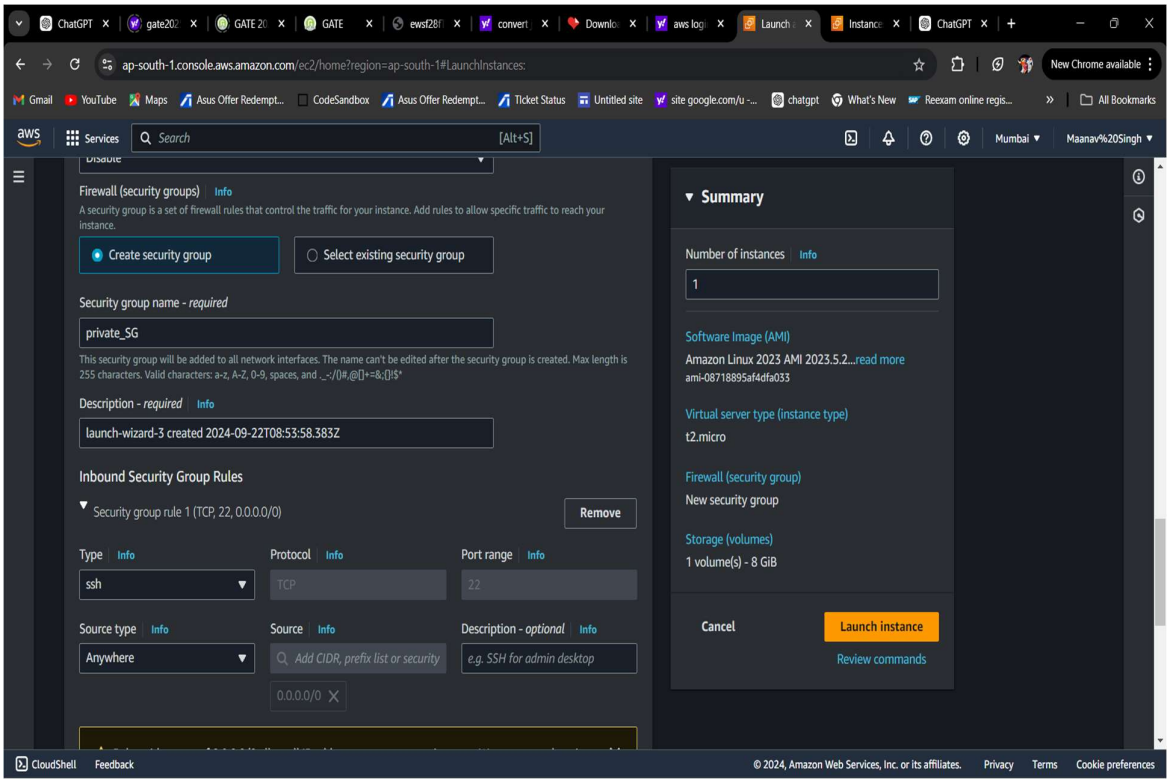


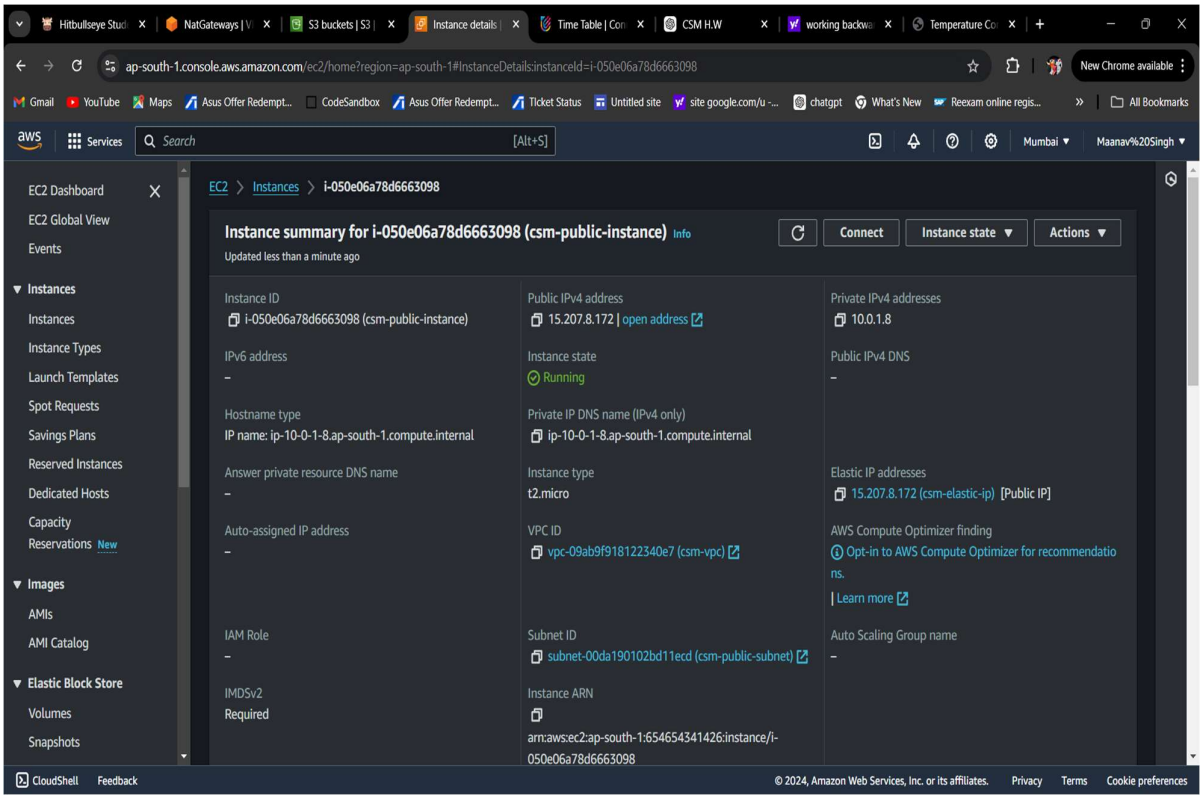


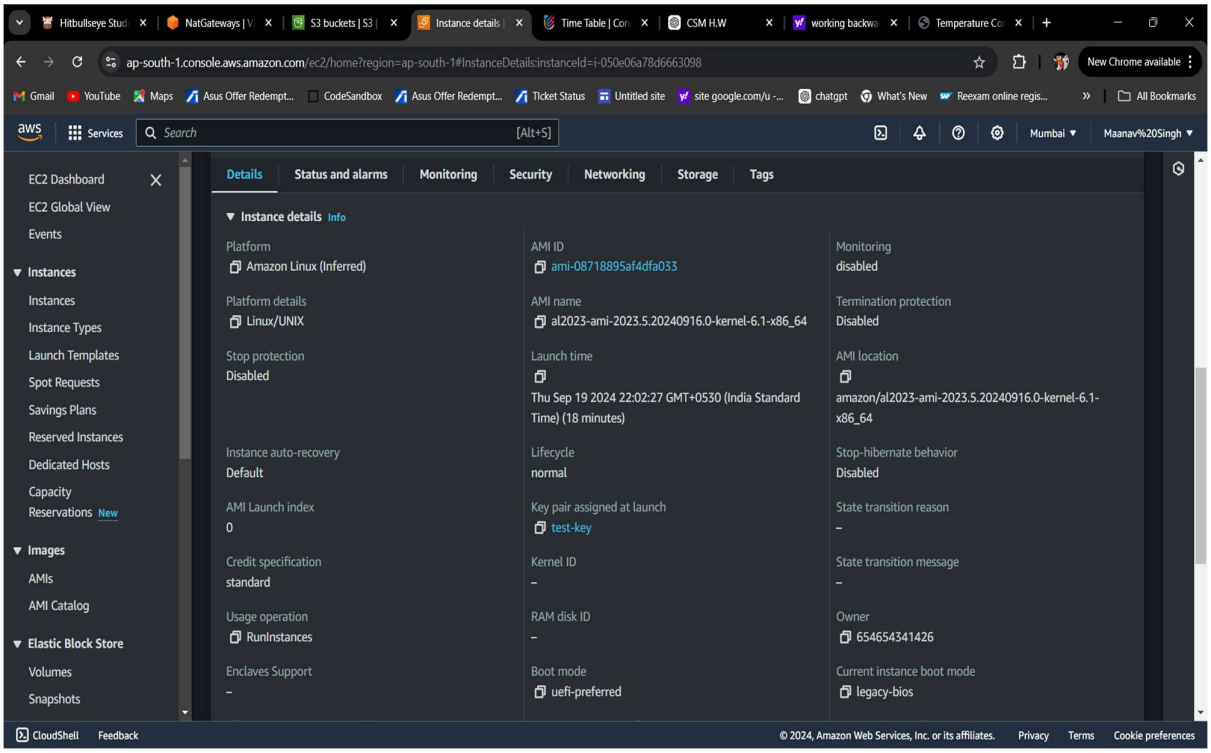

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 0, 10.0.2.237)
Remove
Type Info
Custom TCP
Protocol Info
TCP
Port range Info
0
Source type Info
Custom
Source Info
Add CIDR, prefix list or security
10.0.2.237
Description - optional Info
e.g. SSH for admin desktop
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-08718895af4dfa033
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

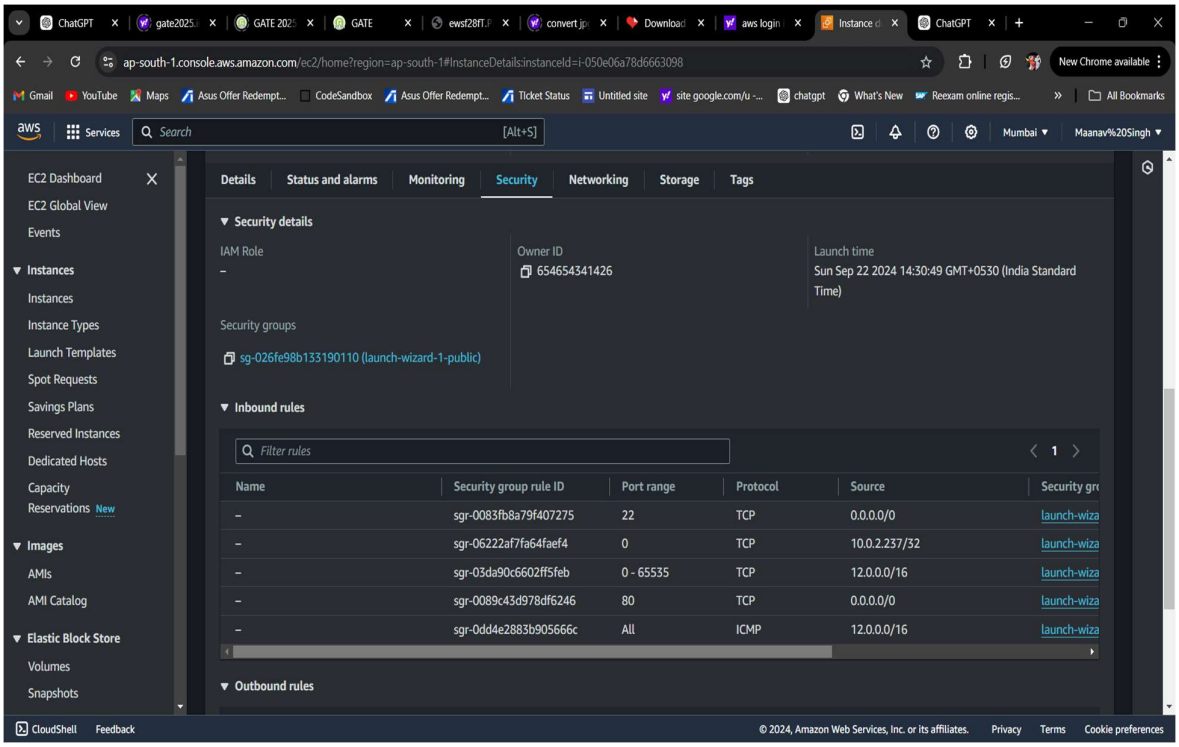

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
private_instance
Add additional tags
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
Quick Start
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-08718895af4dfa033
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

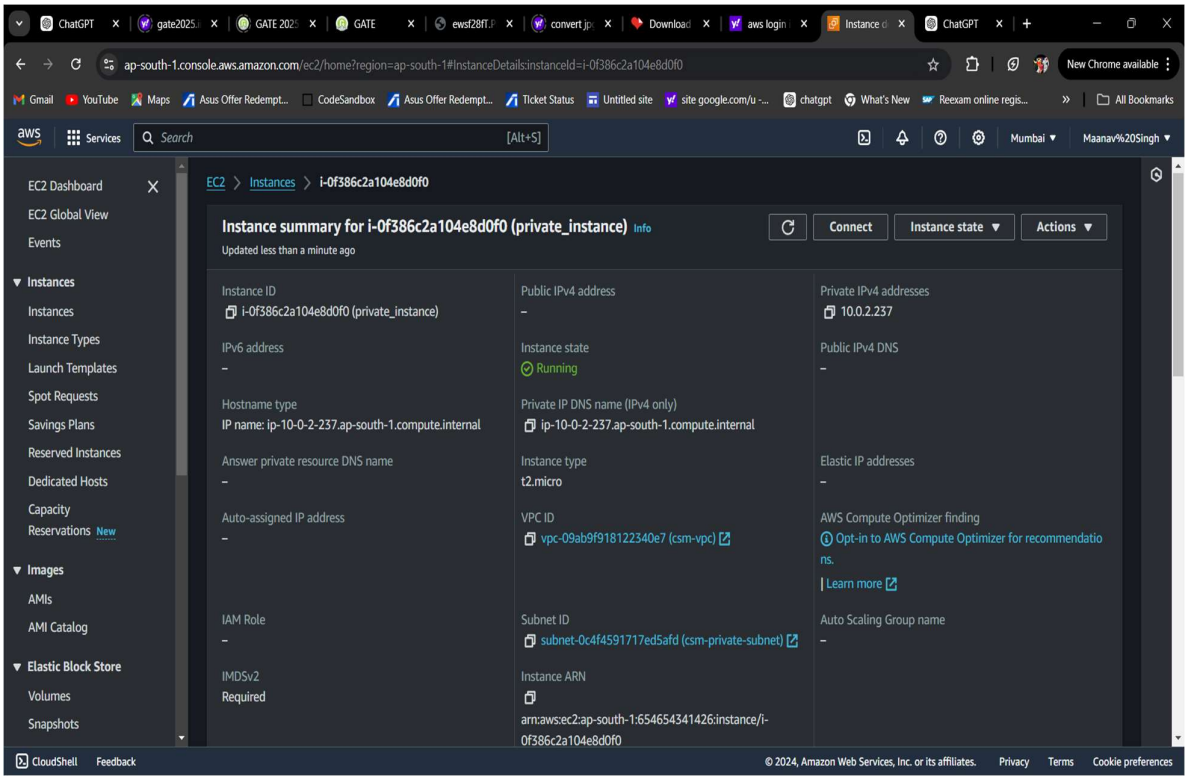

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
Maanav%20Singh
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
private_pem
Create new key pair
Network settings Info
VPC - required Info
vpc-09ab9f918122340e7 (csm-vpc)
10.0.0.0/16
Subnet Info
subnet-0c4f4591717ed5afd
csm-private-subnet
VPC: vpc-09ab9f918122340e7 Owner: 654654341426
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 249 CIDR: 10.0.2.0/24)
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
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-08718895af4dfa033
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

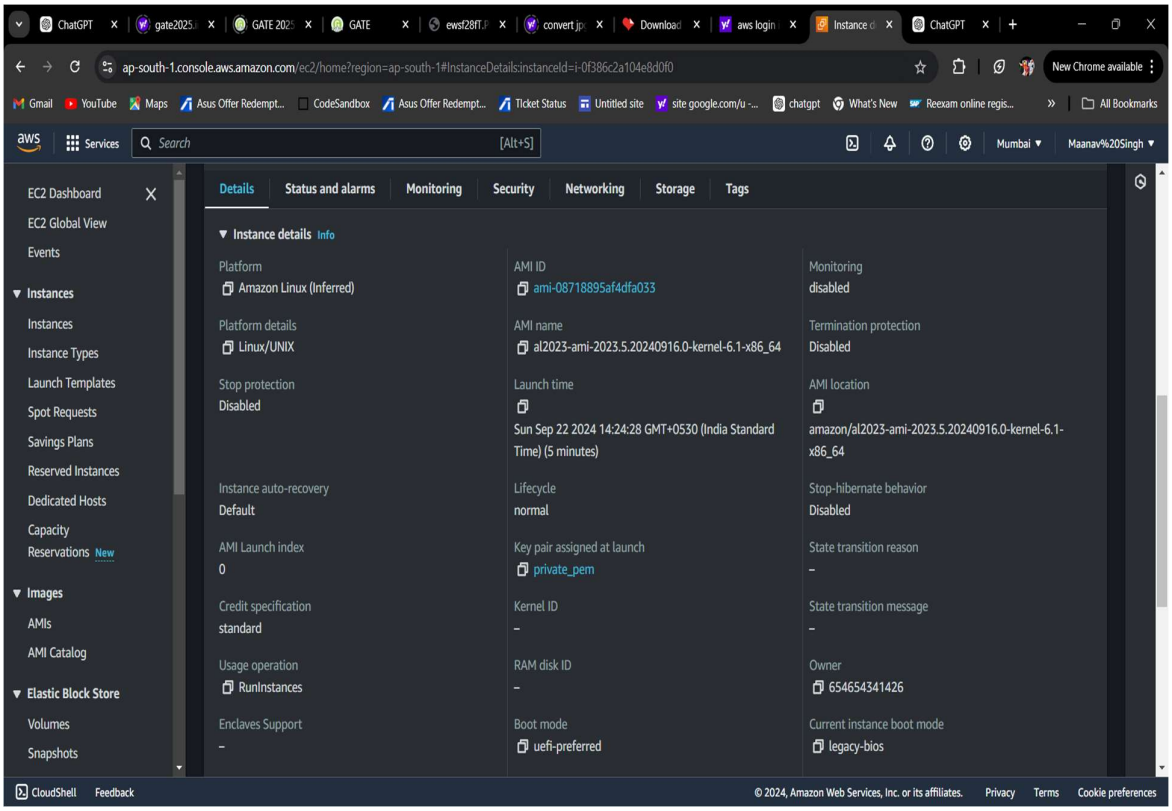

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
Maanav%20Singh
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
private_SG
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-3 created 2024-09-22T08:53:58.383Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-08718895af4dfa033
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

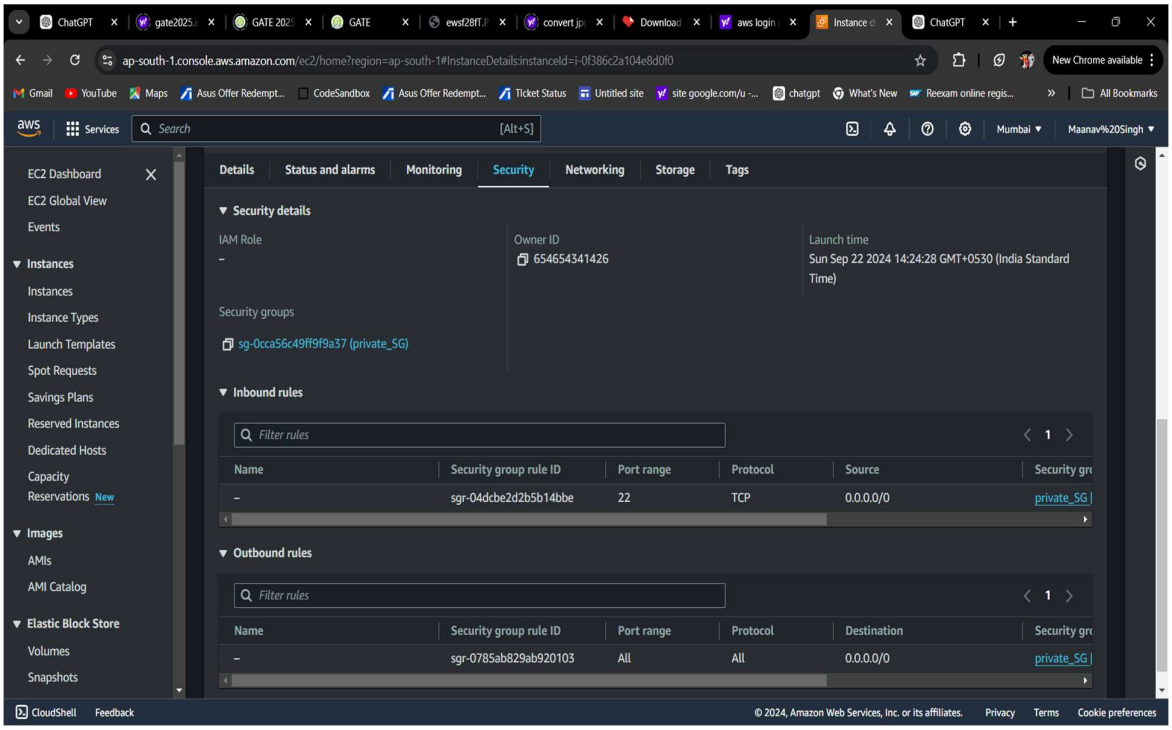

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-050e06a78d6663098
EC2 > Instances > i-050e06a78d6663098
Instance summary for i-050e06a78d6663098 (csm-public-instance) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-050e06a78d6663098 (csm-public-instance)
Public IPv4 address
15.207.8.172 | open address
Private IPv4 addresses
10.0.1.8
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-10-0-1-8.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-1-8.ap-south-1.compute.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
15.207.8.172 (csm-elastic-ip) [Public IP]
Auto-assigned IP address
–
VPC ID
vpc-09ab9f918122340e7 (csm-vpc)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
IAM Role
–
Subnet ID
subnet-00da190102bd11ecd (csm-public-subnet)
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:ap-south-1:654654341426:instance/i-050e06a78d6663098
EC2 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-050e06a78d6663098
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details Info
Platform
Amazon Linux (Inferred)
AMI ID
ami-08718895af4dfa033
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Termination protection
Disabled
Stop protection
Disabled
Launch time
Thu Sep 19 2024 22:02:27 GMT+0530 (India Standard Time) (18 minutes)
AMI location
amazon/al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Instance auto-recovery
Default
Lifecycle
normal
Stop-hibernate behavior
Disabled
AMI Launch index
0
Key pair assigned at launch
test-key
State transition reason
–
Credit specification
standard
Kernel ID
–
State transition message
–
Usage operation
RunInstances
RAM disk ID
–
Owner
654654341426
Enclaves Support
–
Boot mode
uefi-preferred
Current instance boot mode
legacy-bios
EC2 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-050e06a78d6663098
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Security details
IAM Role
-
Owner ID
654654341426
Launch time
Sun Sep 22 2024 14:30:49 GMT+0530 (India Standard Time)
Security groups
sg-026fe98b133190110 (launch-wizard-1-public)
Inbound rules
Filter rules
Name
Security group rule ID
Port range
Protocol
Source
sgr-0083fb8a79f407275
22
TCP
0.0.0.0/0
sgr-06222af7fa64faef4
0
TCP
10.0.2.237/32
sgr-03da90c6602ff5feb
0 - 65535
TCP
12.0.0.0/16
sgr-0089c43d978df6246
80
TCP
0.0.0.0/0
sgr-0dd4e2883b905666c
All
ICMP
12.0.0.0/16
Outbound rules

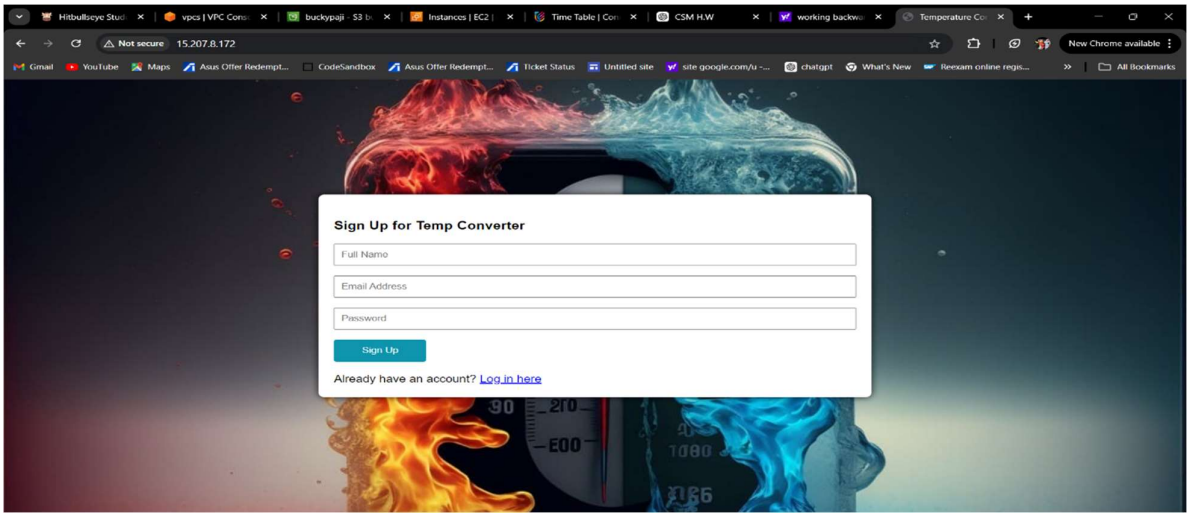

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0f386c2a104e8d0f0
EC2 > Instances > i-0f386c2a104e8d0f0
Instance summary for i-0f386c2a104e8d0f0 (private_instance)
Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-0f386c2a104e8d0f0 (private_instance)
Public IPv4 address
-
Private IPv4 addresses
10.0.2.237
IPv6 address
-
Instance state
Running
Public IPv4 DNS
-
Hostname type
IP name: ip-10-0-2-237.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-2-237.ap-south-1.compute.internal
Answer private resource DNS name
-
Instance type
t2.micro
Elastic IP addresses
-
Auto-assigned IP address
-
VPC ID
vpc-09ab9f918122340e7 (csm-vpc)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
IAM Role
-
Subnet ID
subnet-0c4f4591717ed5afd (csm-private-subnet)
Auto Scaling Group name
-
IMDSv2
Required
Instance ARN
arn:aws:ec2:ap-south-1:654654341426:instance/i-0f386c2a104e8d0f0


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0f386c2a104e8d0f0
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details Info
Platform
Amazon Linux (Inferred)
AMI ID
ami-08718895af4dfa033
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Sep 22 2024 14:24:28 GMT+0530 (India Standard Time) (5 minutes)
AMI location
amazon/al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Instance auto-recovery
Default
Lifecycle
normal
Stop-hibernate behavior
Disabled
AMI Launch index
0
Key pair assigned at launch
private_pem
State transition reason
–
Credit specification
standard
Kernel ID
–
State transition message
–
Usage operation
RunInstances
RAM disk ID
–
Owner
654654341426
Enclaves Support
–
Boot mode
uefi-preferred
Current instance boot mode
legacy-bios

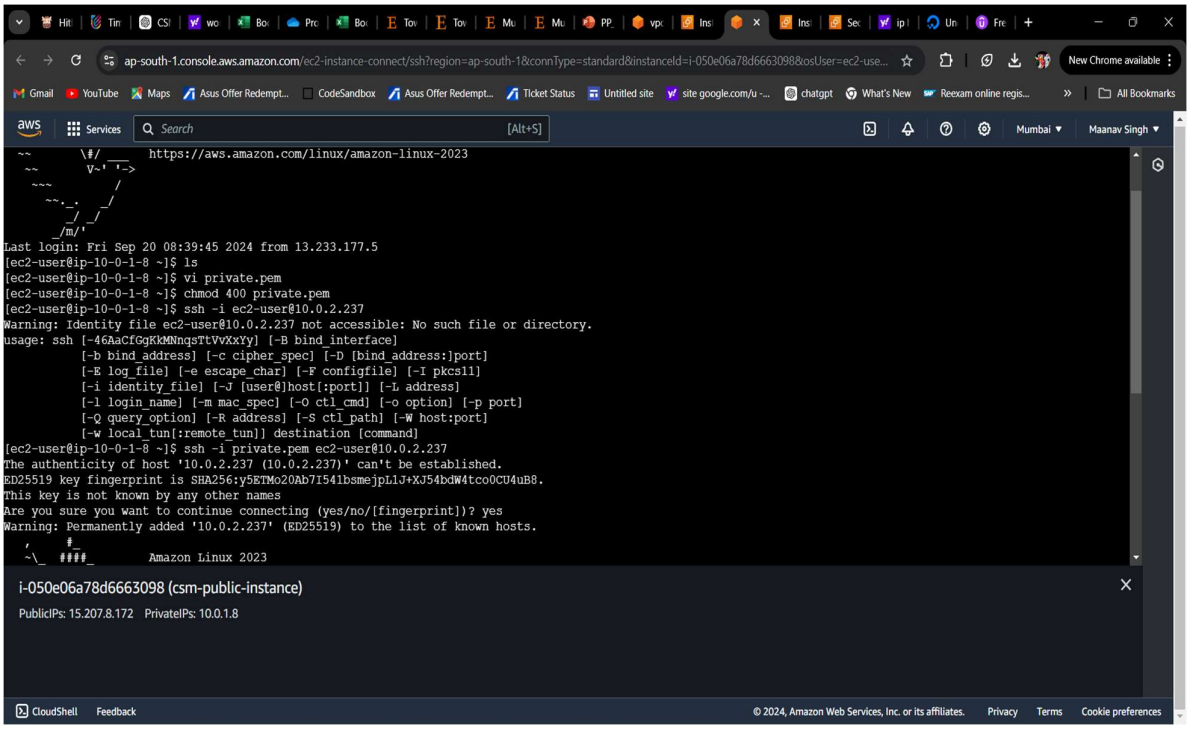

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0f386c2a104e8d0f0
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Security details
IAM Role
–
Owner ID
654654341426
Launch time
Sun Sep 22 2024 14:24:28 GMT+0530 (India Standard Time)
Security groups
sg-0cca56c49ff9f9a37 (private_SG)
Inbound rules
Filter rules
Name
Security group rule ID
Port range
Protocol
Source
Security gr
–
sgr-04dcbe2d2b5b14bbe
22
TCP
0.0.0.0/0
private_SG
Outbound rules
Filter rules
Name
Security group rule ID
Port range
Protocol
Destination
Security gr
–
sgr-0785ab829ab920103
All
All
0.0.0.0/0
private_SG

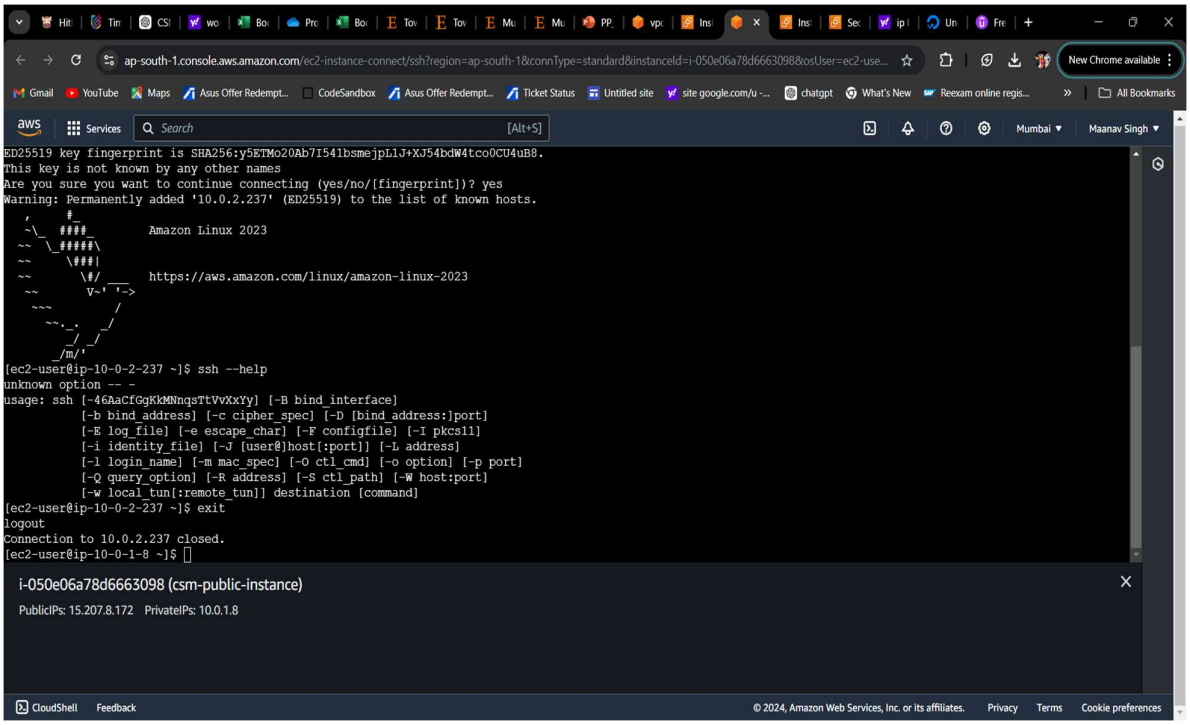
7. Test Connectivity: Connect to the public instance using SSH.

- **From the public instance, SSH into the private instance using its private IP.**



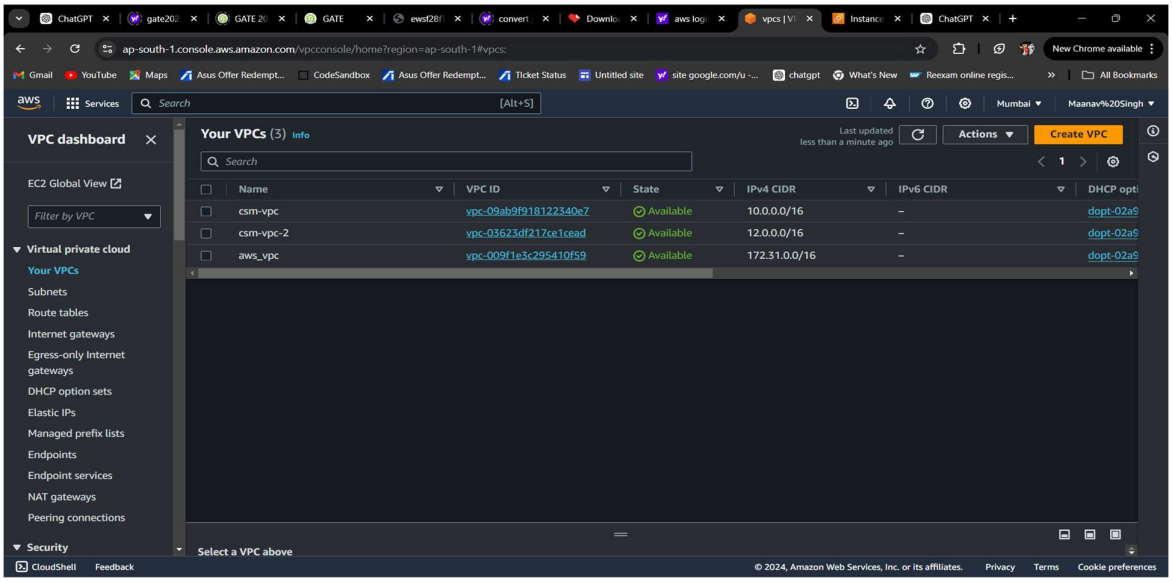
Run commands to check private instance connectivity it is written in screenshot below:

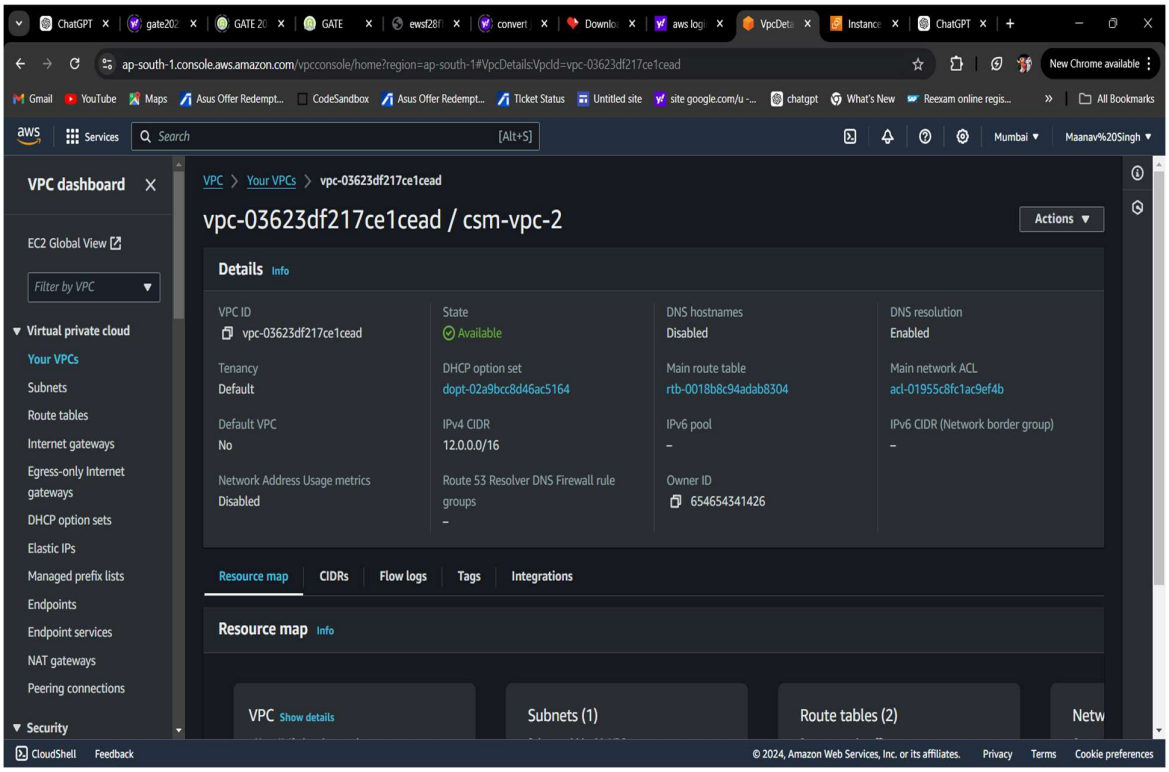


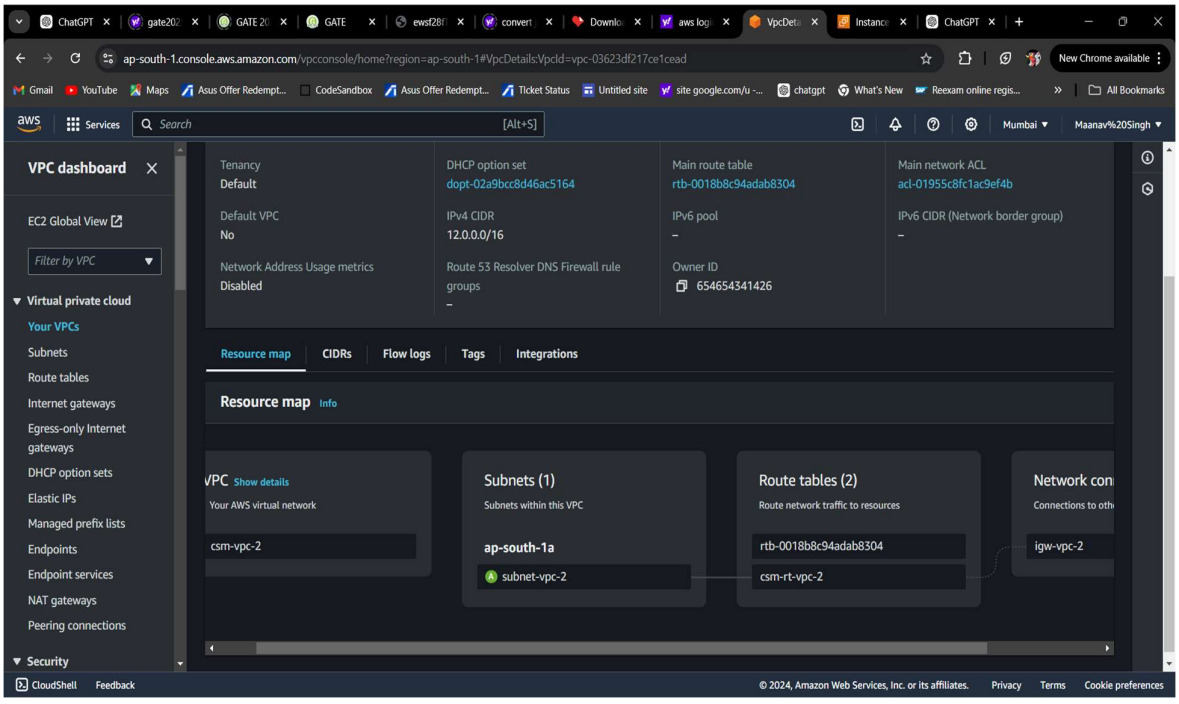


8. VPC Peering (optional advanced task for bonus marks): If you have created two separate VPCs, peer them and configure the route tables to allow instances in both VPCs to communicate.

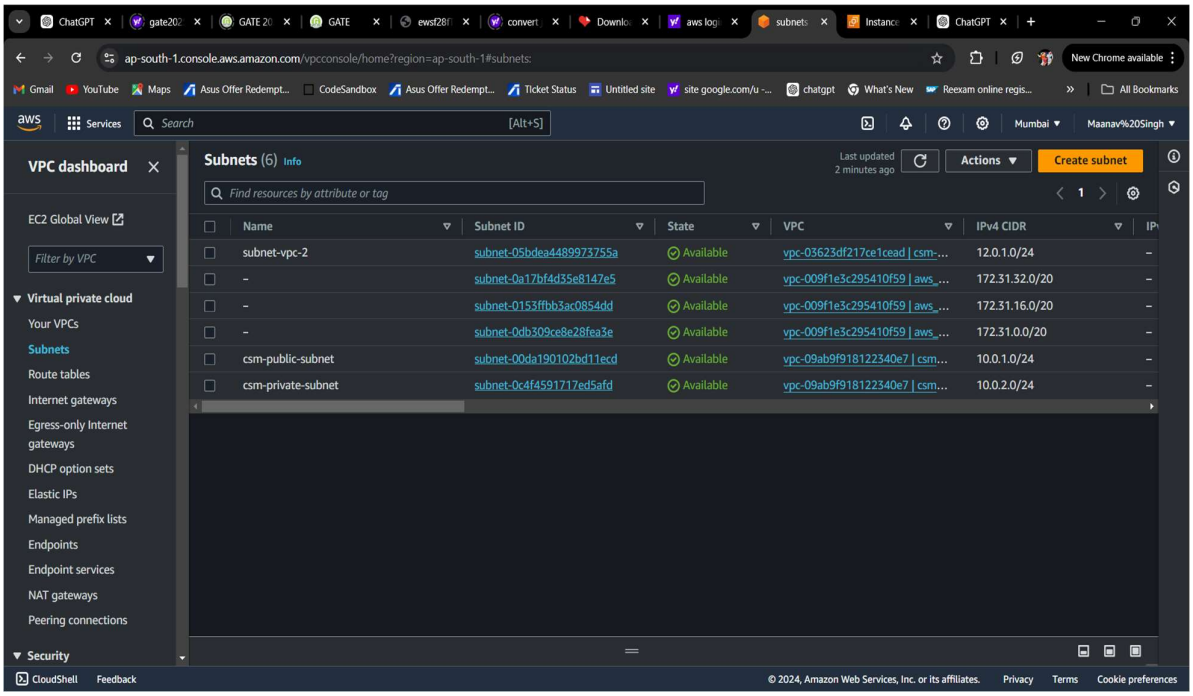
a) Create 2nd VPC.

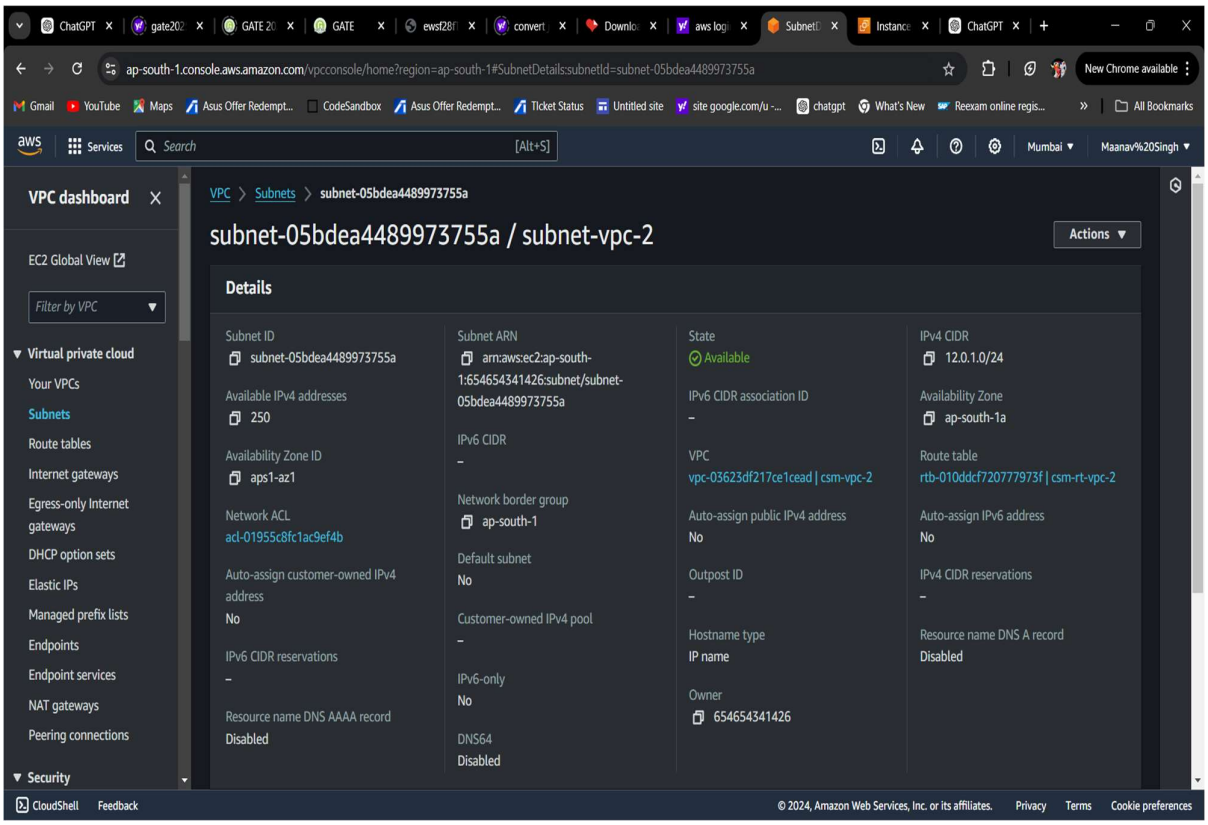


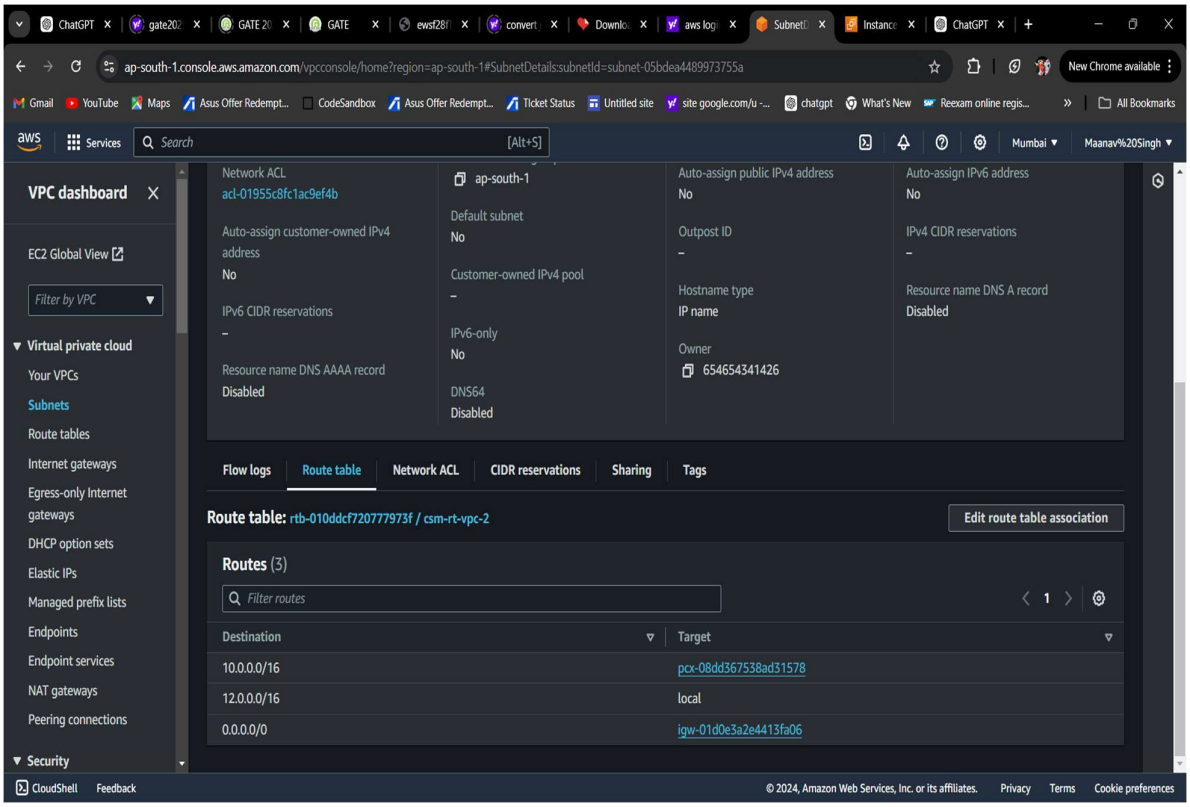

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-03623df217ce1cead
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Your VPCs > vpc-03623df217ce1cead
vpc-03623df217ce1cead / csm-vpc-2
Actions
Details Info
VPC ID
vpc-03623df217ce1cead
State
Available
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-02a9bcc8d46ac5164
Main route table
rtb-0018b8c94adab8304
Main network ACL
acl-01955c8fc1ac9ef4b
Default VPC
No
IPv4 CIDR
12.0.0.0/16
IPv6 pool
-
IPv6 CIDR (Network border group)
-
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
-
Owner ID
654654341426
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Subnets (1)
Route tables (2)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#VpcDetails:VpcId=vpc-03623df217ce1cead
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
Tenancy
Default
DHCP option set
dopt-02a9bcc8d46ac5164
Main route table
rtb-0018b8c94adab8304
Main network ACL
acl-01955c8fc1ac9ef4b
Default VPC
No
IPv4 CIDR
12.0.0.0/16
IPv6 pool
-
IPv6 CIDR (Network border group)
-
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
-
Owner ID
654654341426
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
csm-vpc-2
Subnets (1)
Subnets within this VPC
ap-south-1a
subnet-vpc-2
Route tables (2)
Route network traffic to resources
rtb-0018b8c94adab8304
csm-rt-vpc-2
Network con
Connections to oth
igw-vpc-2
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

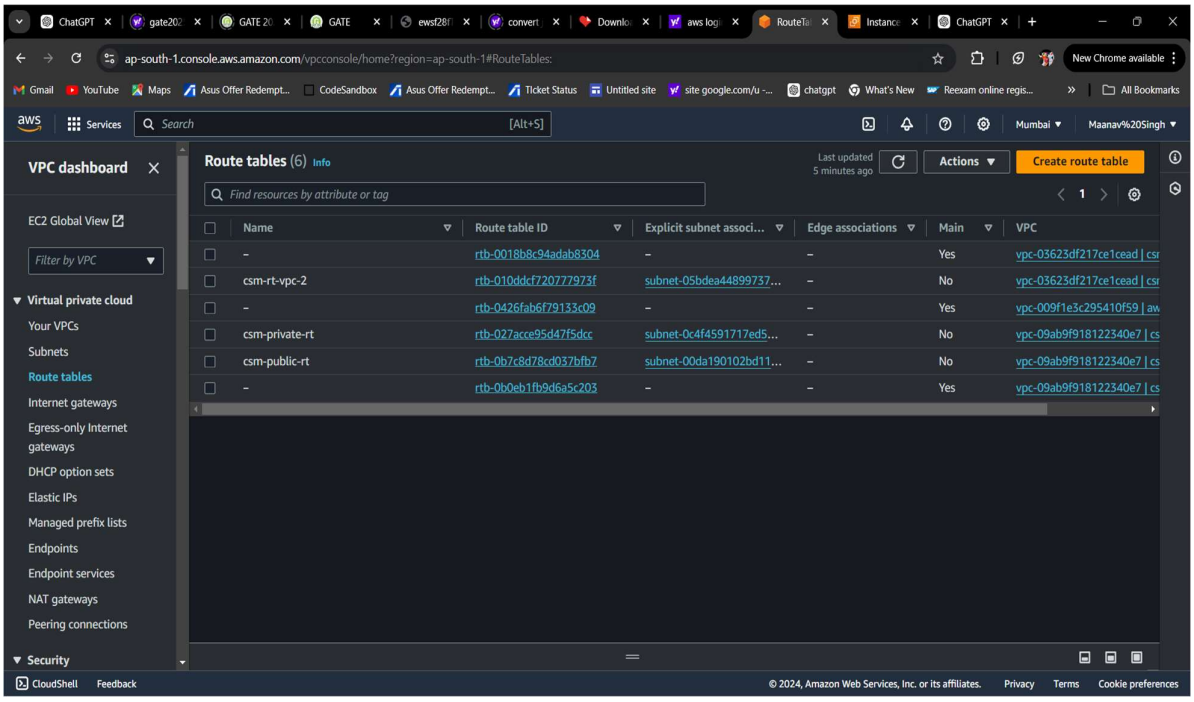
b) create subnet for vpc-2

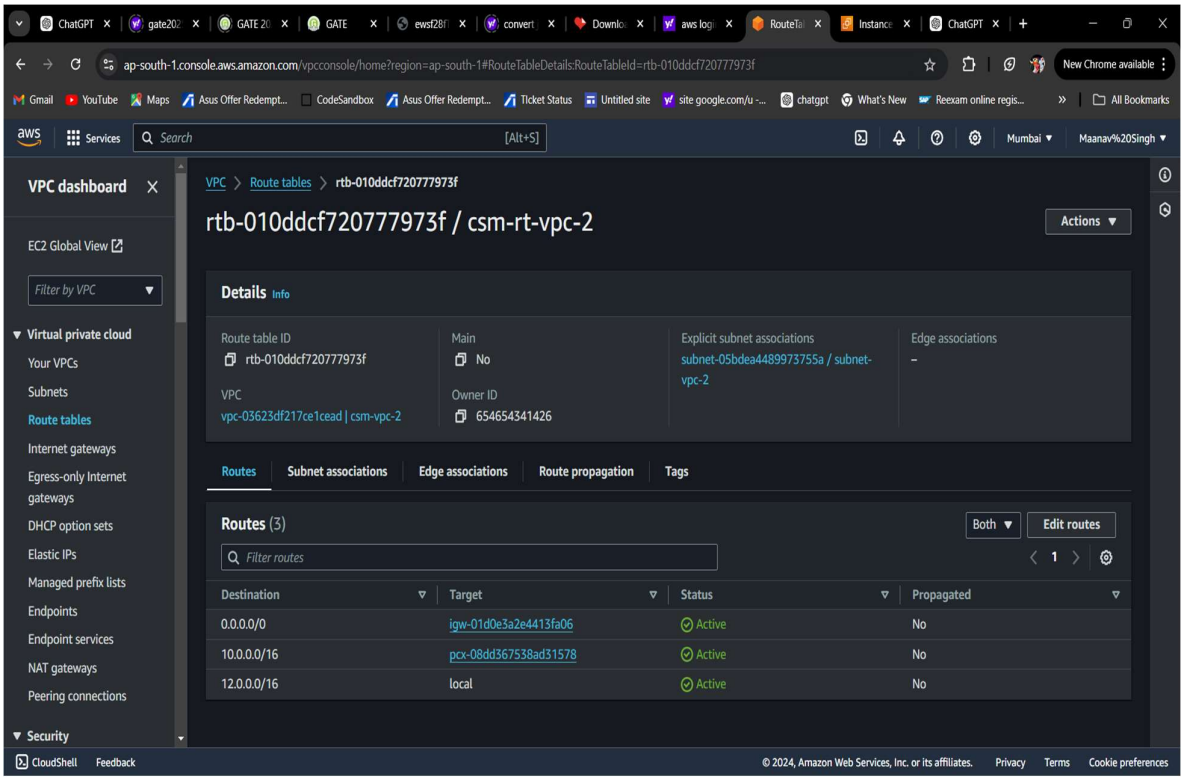


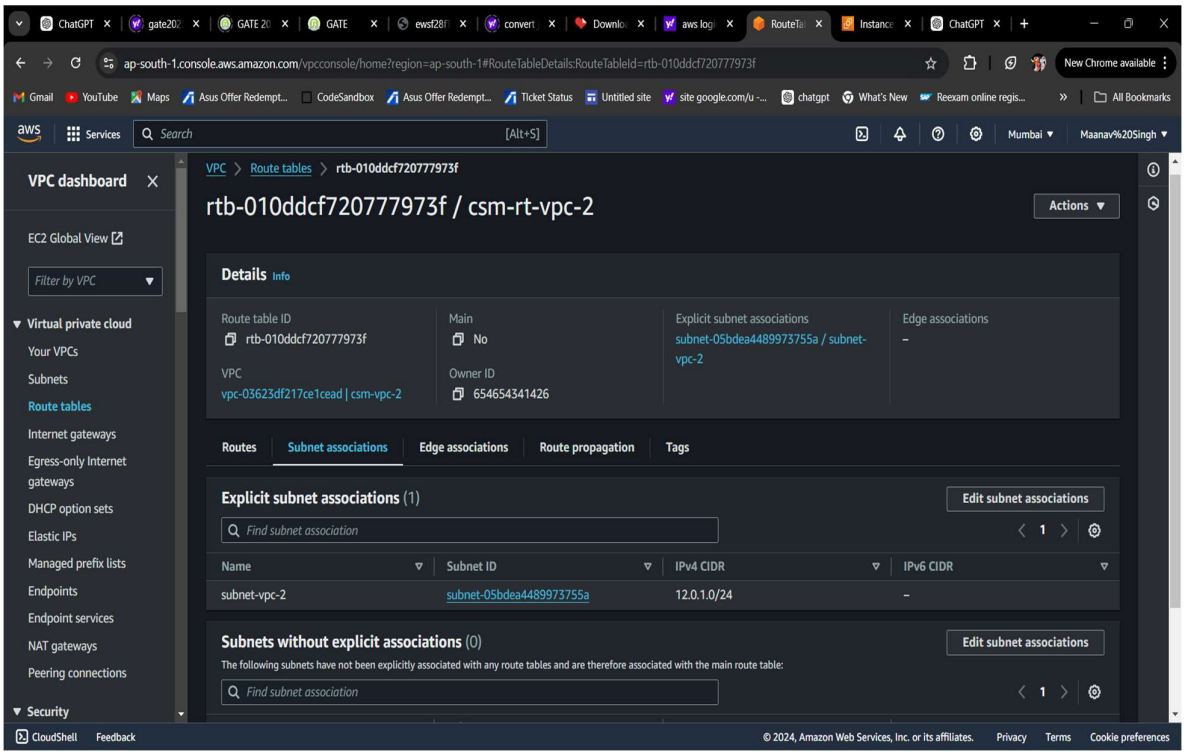




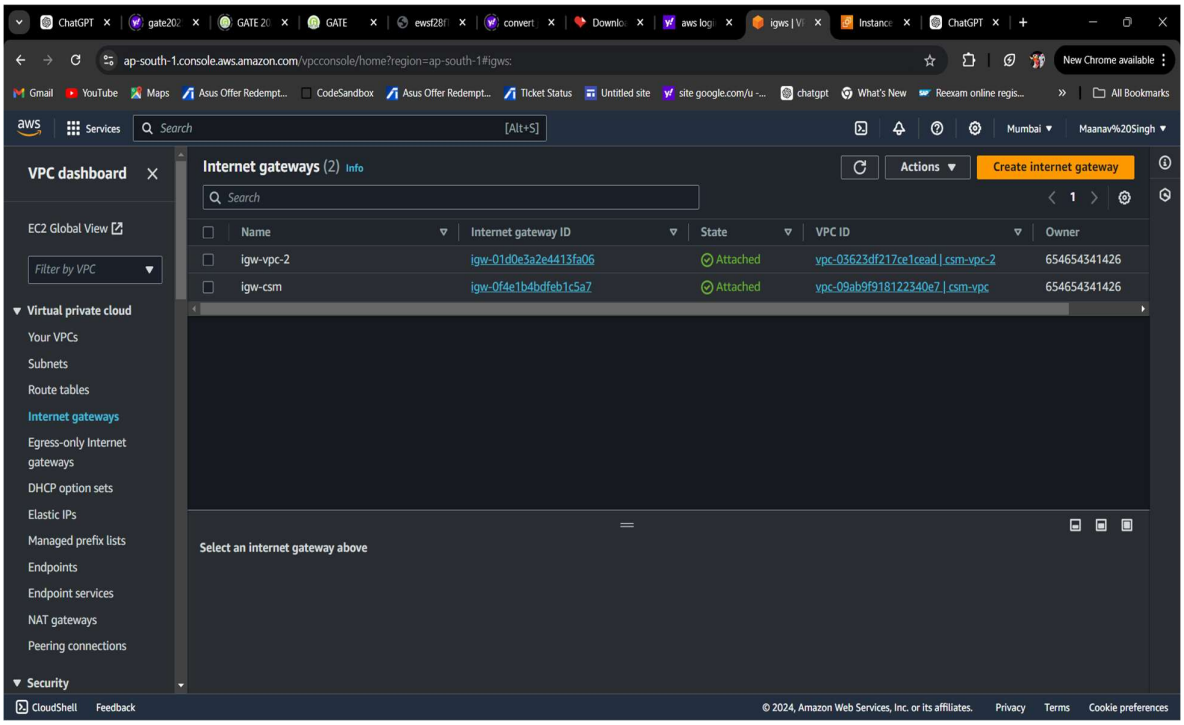
c) create route table for subnet.

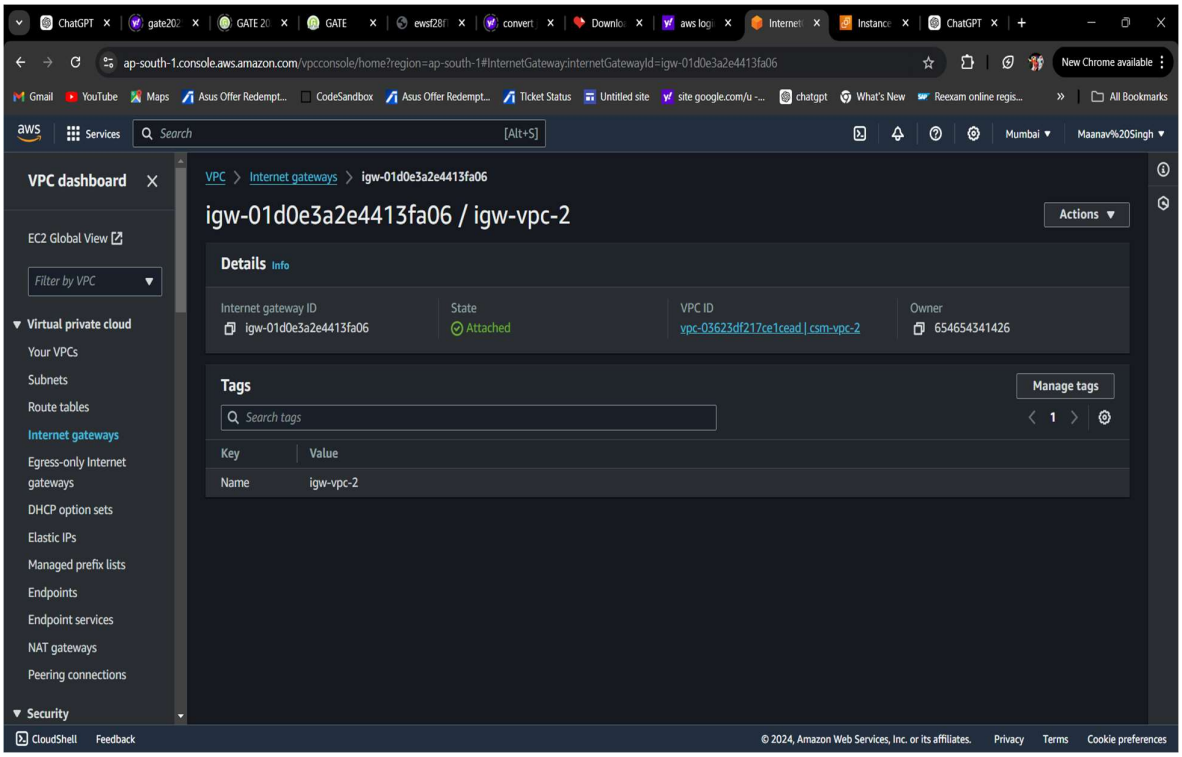



ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-010ddcf720777973f
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Route tables > rtb-010ddcf720777973f
rtb-010ddcf720777973f / csm-rt-vpc-2
Actions
Details Info
Route table ID
rtb-010ddcf720777973f
Main
No
Explicit subnet associations
subnet-05bdea4489973755a / subnet-vpc-2
Edge associations
–
VPC
vpc-03623df217ce1cead | csm-vpc-2
Owner ID
654654341426
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (3)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-01d0e3a2e4413fa06
Active
No
10.0.0.0/16
pcx-08dd367538ad31578
Active
No
12.0.0.0/16
local
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

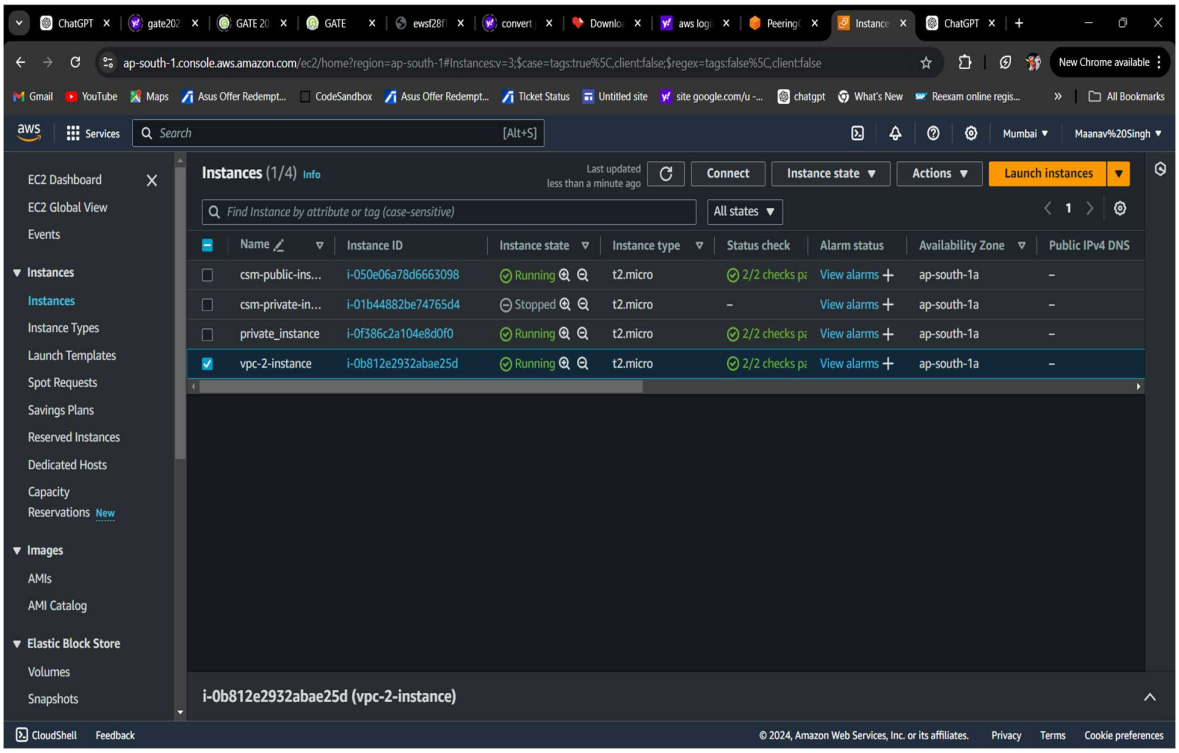

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-010ddcf720777973f
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
VPC > Route tables > rtb-010ddcf720777973f
rtb-010ddcf720777973f / csm-rt-vpc-2
Actions
Details Info
Route table ID
rtb-010ddcf720777973f
Main
No
Explicit subnet associations
subnet-05bdea4489973755a / subnet-vpc-2
Edge associations
–
VPC
vpc-03623df217ce1cead | csm-vpc-2
Owner ID
654654341426
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
subnet-vpc-2
subnet-05bdea4489973755a
12.0.1.0/24
–
Subnets without explicit associations (0)
Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Find subnet association
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

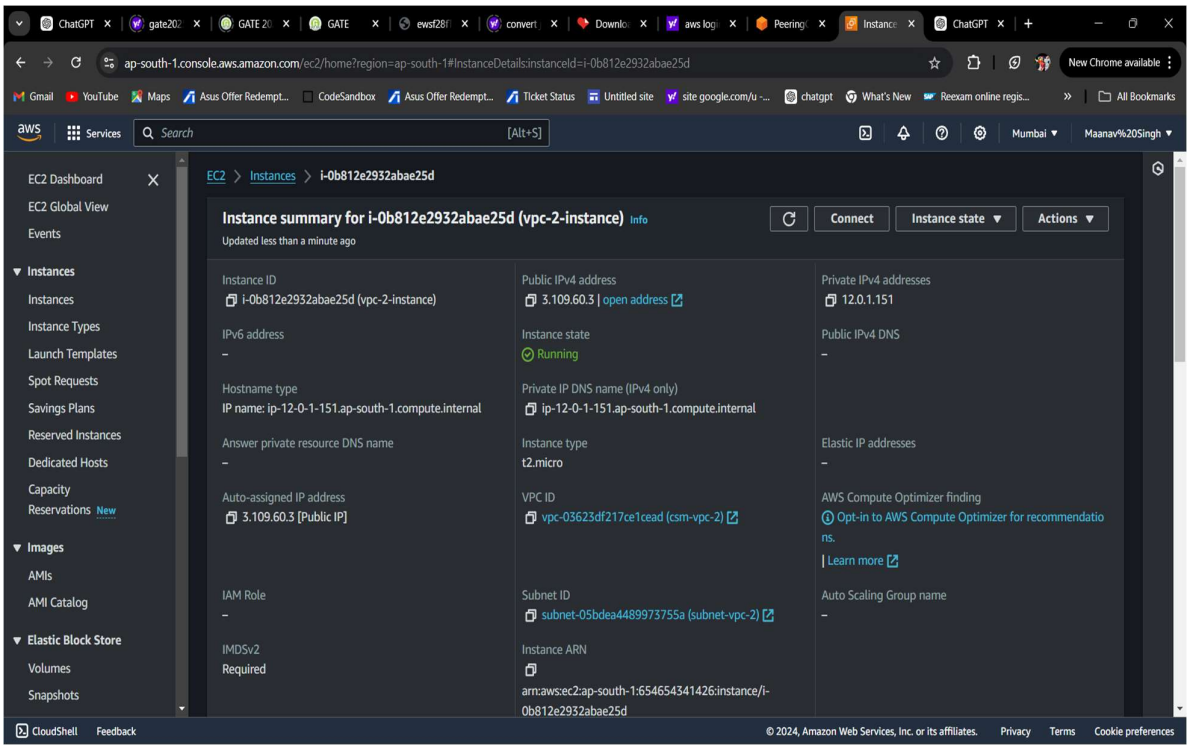
d) create internet gateway for vpc-2.

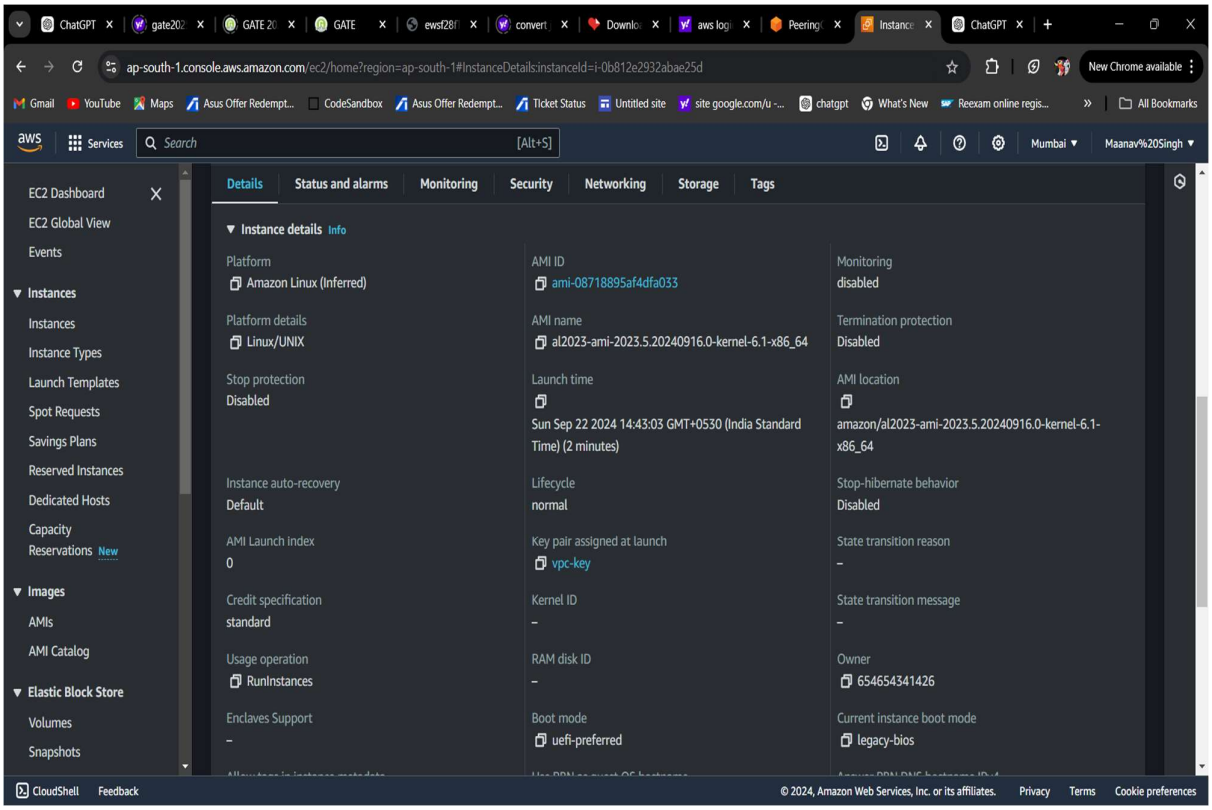


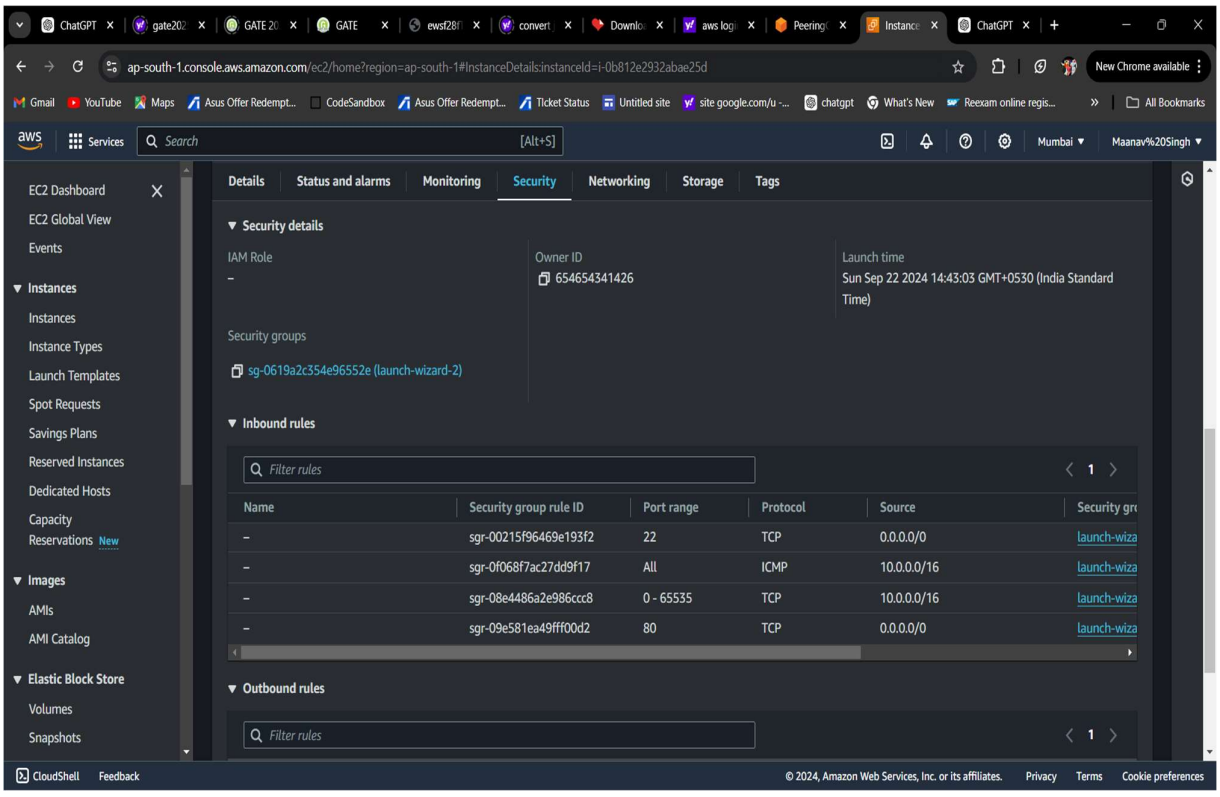


e) create instance for vpc-2.

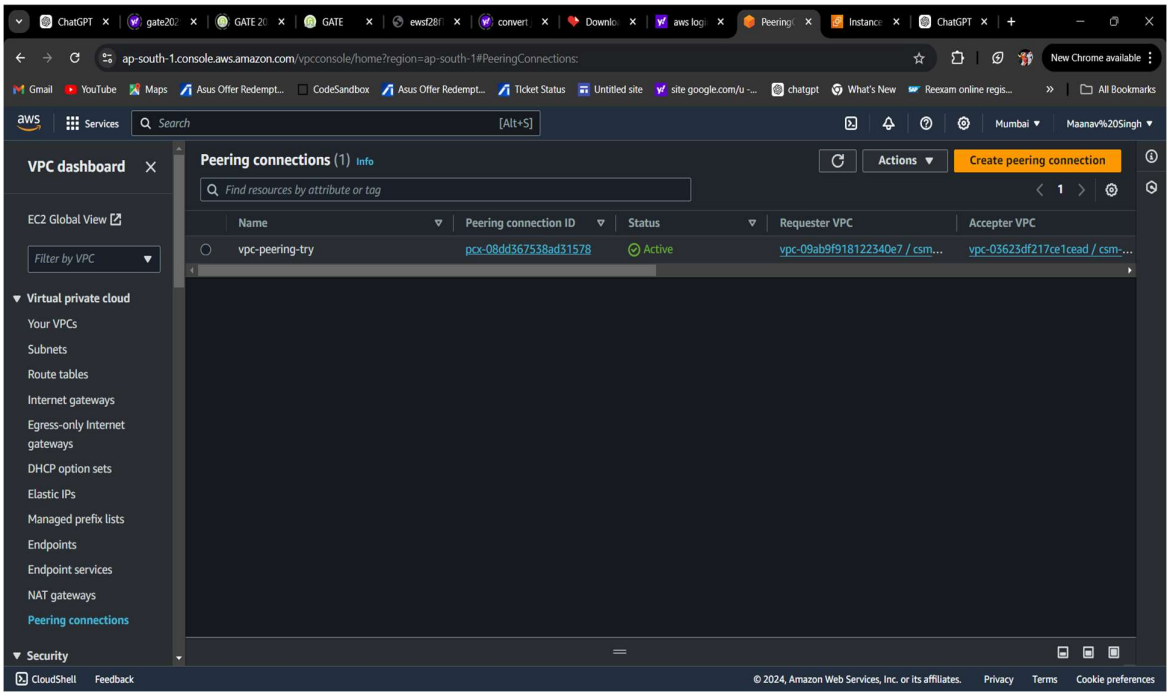


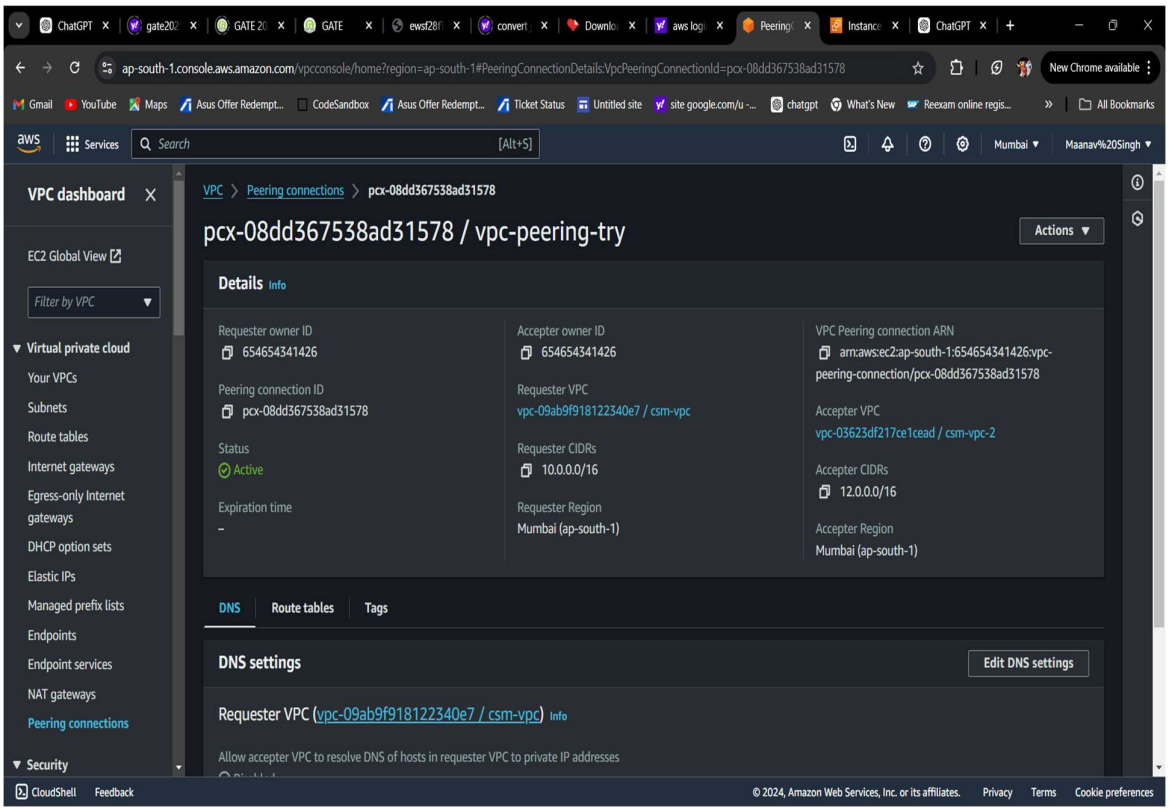


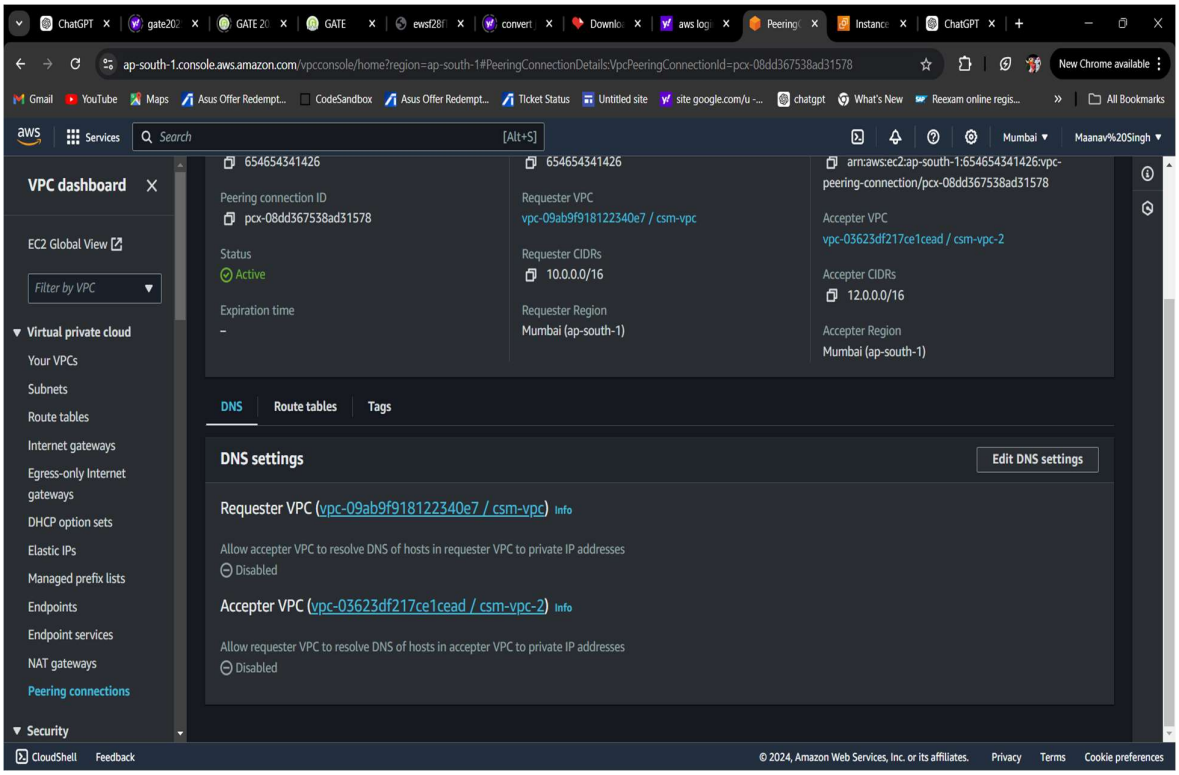

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0b812e2932abae25d
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance details Info
Platform
Amazon Linux (Inferred)
AMI ID
ami-08718895af4dfa033
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Termination protection
Disabled
Stop protection
Disabled
Launch time
Sun Sep 22 2024 14:43:03 GMT+0530 (India Standard Time) (2 minutes)
AMI location
amazon/al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Instance auto-recovery
Default
Lifecycle
normal
Stop-hibernate behavior
Disabled
AMI Launch index
0
Key pair assigned at launch
vpc-key
State transition reason
–
Credit specification
standard
Kernel ID
–
State transition message
–
Usage operation
RunInstances
RAM disk ID
–
Owner
654654341426
Enclaves Support
–
Boot mode
uefi-preferred
Current instance boot mode
legacy-bios
EC2 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

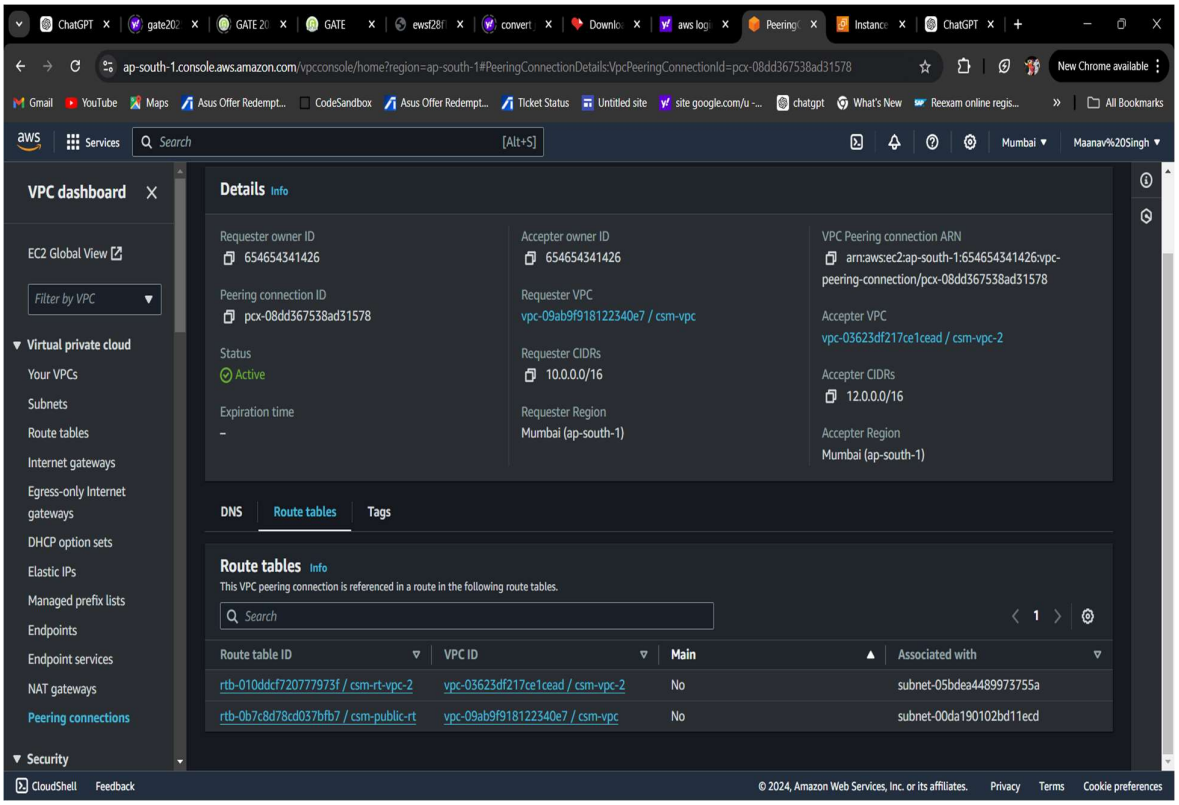

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-0b812e2932abae25d
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Security details
IAM Role
–
Owner ID
654654341426
Launch time
Sun Sep 22 2024 14:43:03 GMT+0530 (India Standard Time)
Security groups
sg-0619a2c354e96552e (launch-wizard-2)
Inbound rules
Filter rules
Name
Security group rule ID
Port range
Protocol
Source
Security gr
– sgr-00215f96469e193f2 22 TCP 0.0.0.0/0 launch-wiza
– sgr-0f068f7ac27dd9f17 All ICMP 10.0.0.0/16 launch-wiza
– sgr-08e4486a2e986ccc8 0 - 65535 TCP 10.0.0.0/16 launch-wiza
– sgr-09e581ea49fff00d2 80 TCP 0.0.0.0/0 launch-wiza
Outbound rules
Filter rules
EC2 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

f) create peering connection for vpc’s.

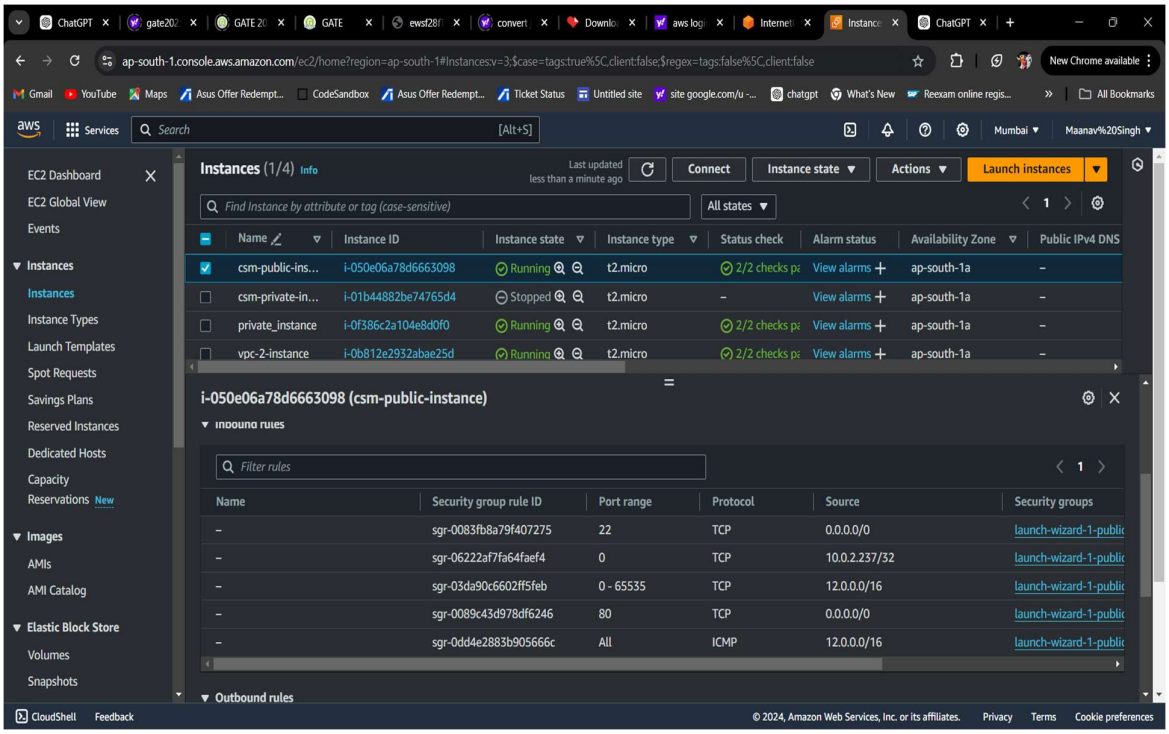


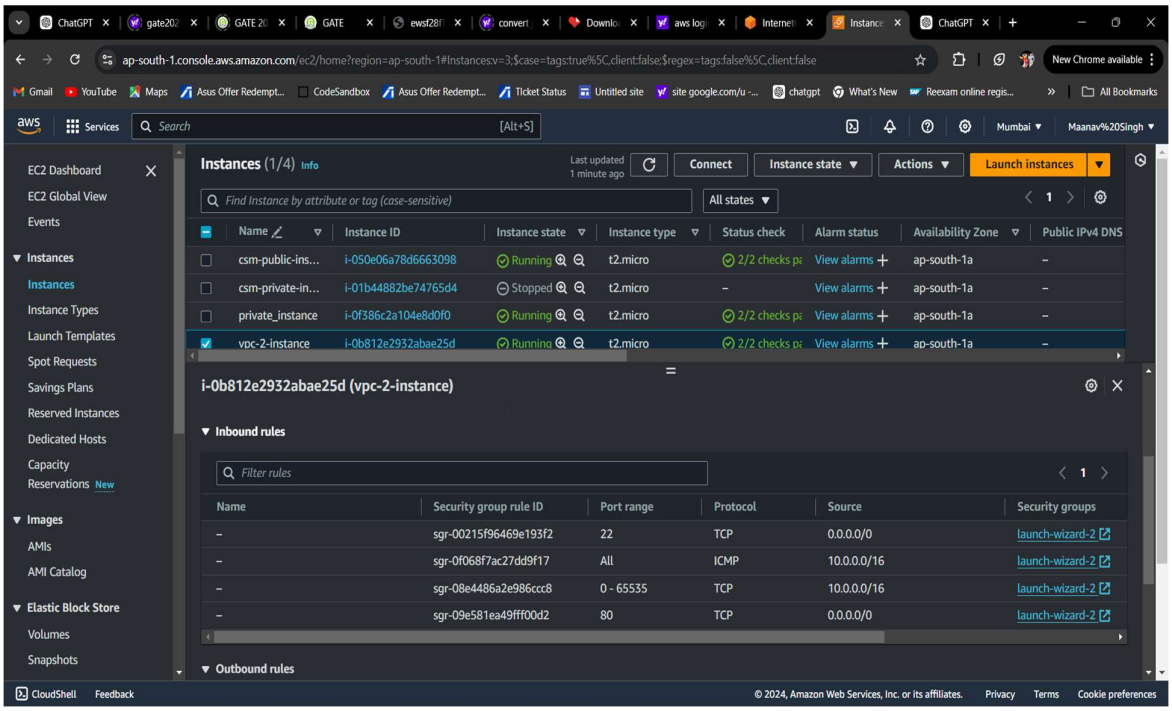



ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnectionDetails:VpcPeeringConnectionId=pcx-08dd367538ad31578
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
654654341426
Peering connection ID
pcx-08dd367538ad31578
Status
Active
Expiration time
-
654654341426
Requester VPC
vpc-09ab9f918122340e7 / csm-vpc
Requester CIDRs
10.0.0.0/16
Requester Region
Mumbai (ap-south-1)
arn:aws:ec2:ap-south-1:654654341426:vpc-peering-connection/pcx-08dd367538ad31578
Accepter VPC
vpc-03623df217ce1cead / csm-vpc-2
Accepter CIDRs
12.0.0.0/16
Accepter Region
Mumbai (ap-south-1)
DNS
Route tables
Tags
DNS settings
Edit DNS settings
Requester VPC (vpc-09ab9f918122340e7 / csm-vpc) Info
Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
Disabled
Accepter VPC (vpc-03623df217ce1cead / csm-vpc-2) Info
Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
Disabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnectionDetails:VpcPeeringConnectionId=pcx-08dd367538ad31578
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
Details Info
Requester owner ID
654654341426
Peering connection ID
pcx-08dd367538ad31578
Status
Active
Expiration time
-
Accepter owner ID
654654341426
Requester VPC
vpc-09ab9f918122340e7 / csm-vpc
Requester CIDRs
10.0.0.0/16
Requester Region
Mumbai (ap-south-1)
VPC Peering connection ARN
arn:aws:ec2:ap-south-1:654654341426:vpc-peering-connection/pcx-08dd367538ad31578
Accepter VPC
vpc-03623df217ce1cead / csm-vpc-2
Accepter CIDRs
12.0.0.0/16
Accepter Region
Mumbai (ap-south-1)
DNS
Route tables
Tags
Route tables Info
This VPC peering connection is referenced in a route in the following route tables.
Search
Route table ID
VPC ID
Main
Associated with
rtb-010ddcf720777973f / csm-rt-vpc-2
vpc-03623df217ce1cead / csm-vpc-2
No
subnet-05bdea4489973755a
rtb-0b7c8d78cd037bfb7 / csm-public-rt
vpc-09ab9f918122340e7 / csm-vpc
No
subnet-00da190102bd11ecd
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

g) Go to instances and choose public instance of vpc-1 and edit the inbound and outbound rules.





h) after editing the inbound and outbound rules connect the public instance of vpc-1 and run the following command:

ping private-ip-of-vpc-2-instance (in my case it is 12.0.1.151).