cprime

AWS VPC Deployment with Public-Private Subnet Segregation

NAME : T MANOJ

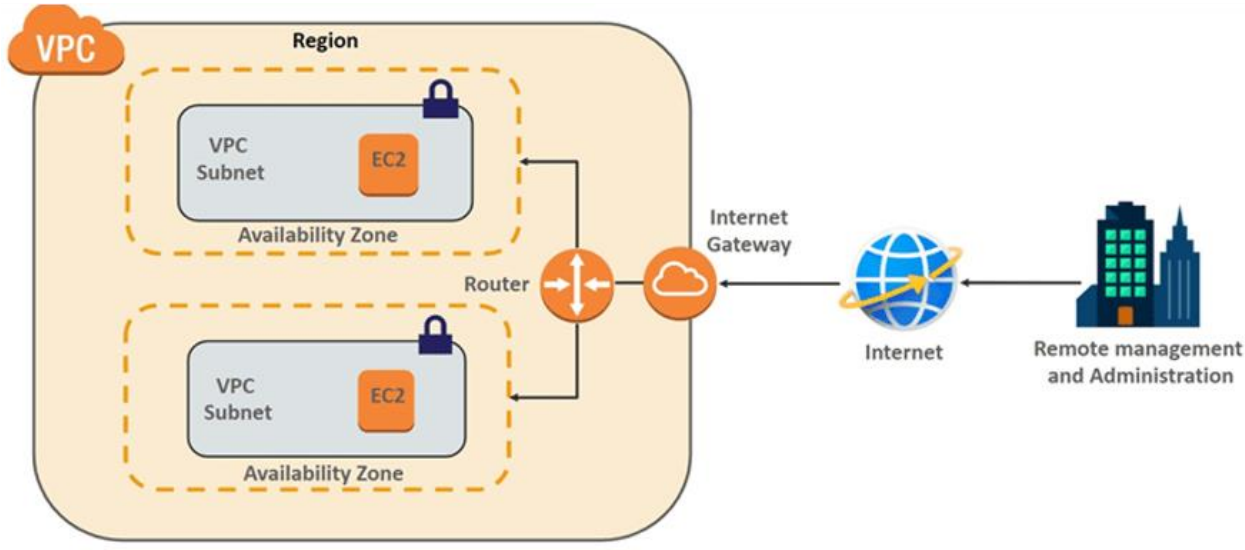
EMP ID : LYAKE2KHS

Overview

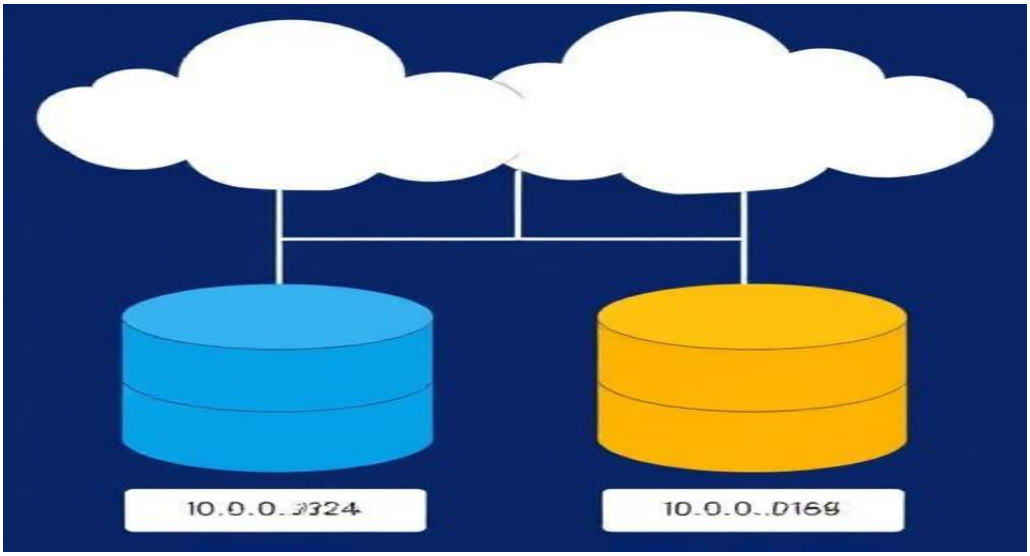
This project demonstrates the complete setup of a Virtual Private Cloud (VPC) in AWS, designed with both public and private subnets to securely deploy web applications. The public subnet hosts a home page EC2 instance with direct internet access, while the private subnet houses a login page EC2 instance without direct internet exposure. The private instance is accessible only through the public instance, ensuring enhanced security. The network is structured using proper CIDR allocations, route tables, an Internet Gateway for the public subnet, and a NAT Gateway for private subnet internet access. The project also integrates Apache HTTPD servers on both instances and uses a reverse proxy mechanism, allowing users to access the login page hosted on the private instance by clicking a button on the home page.

Terminologies :

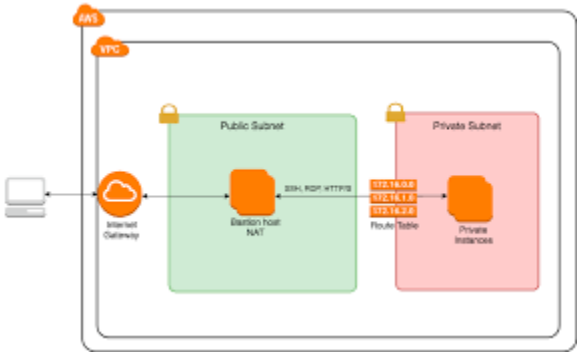
1. **Virtual Private Cloud (VPC):** A logically isolated network in AWS where you can launch resources in a secure environment. It provides full control over networking components, including IP address ranges, subnets, route tables, and gateways.



2. **Subnets:** Subdivisions of a VPC that allow you to group resources based on security and operational needs. Public subnets connect directly to the internet, while private subnets do not and are typically used for backend services.

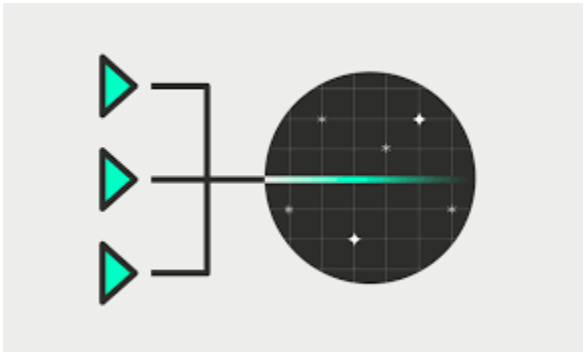


3. **Route Tables:** Define how network traffic is directed within the VPC. Each subnet must be associated with a route table to determine how instances communicate with each other, with gateways, and with the internet.



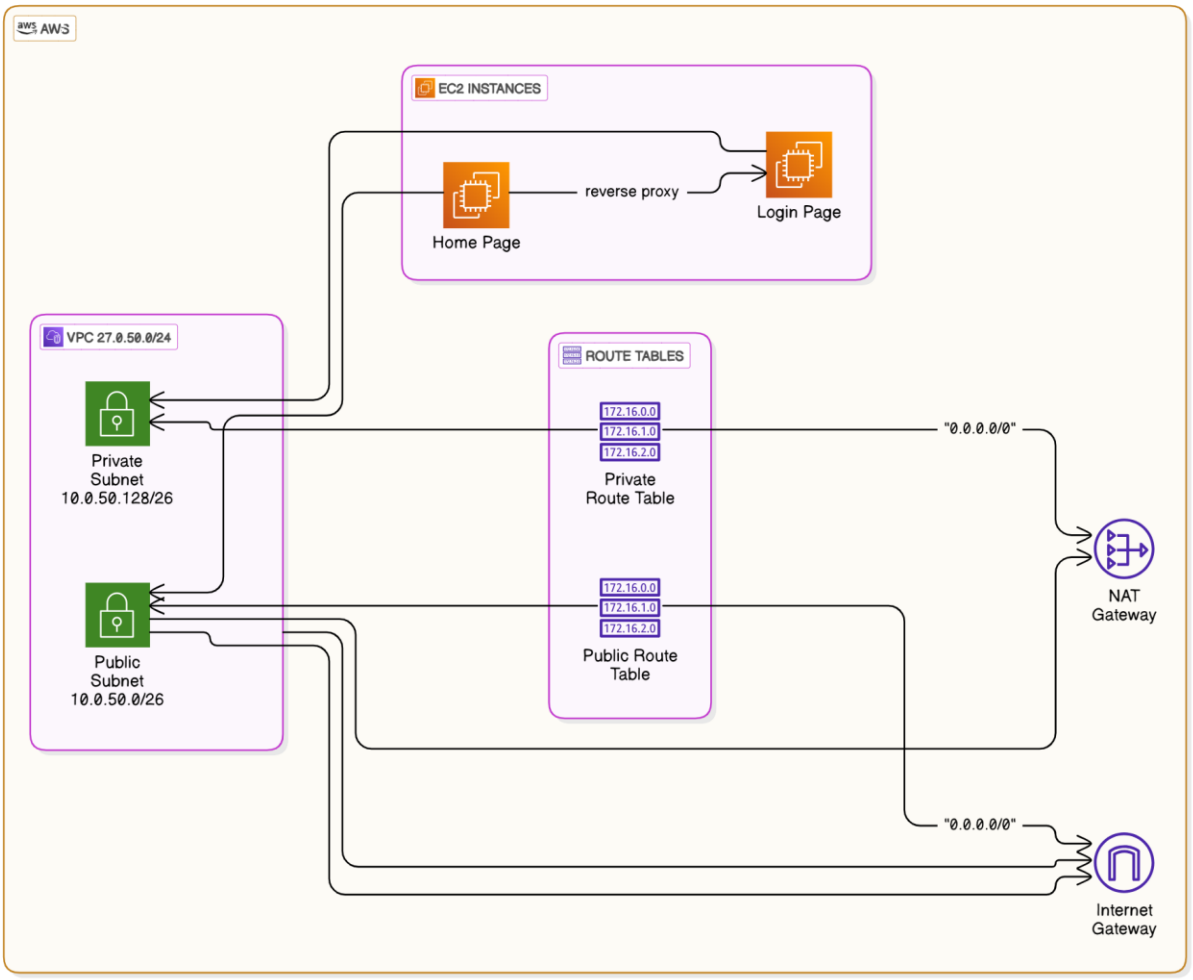
4. **Internet Gateway (IGW):** A VPC component that allows communication between instances in the VPC and the internet. It is attached to the VPC and connected to public subnets through appropriate route table entries.

5. **NAT Gateway:** Enables instances in private subnets to access the internet for software updates or data retrieval while preventing inbound internet traffic, thus enhancing security.



6. **Security Groups:** Virtual firewalls associated with instances to control inbound and outbound traffic. Security groups ensure that only authorized traffic reaches resources in both public and private subnets.

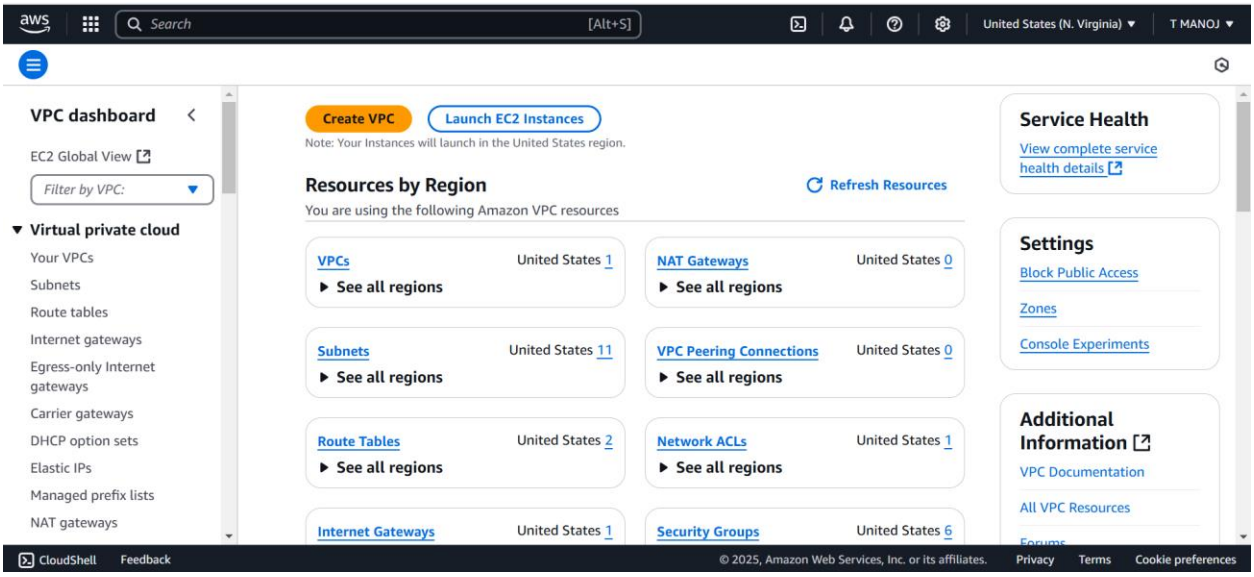
Architecture :

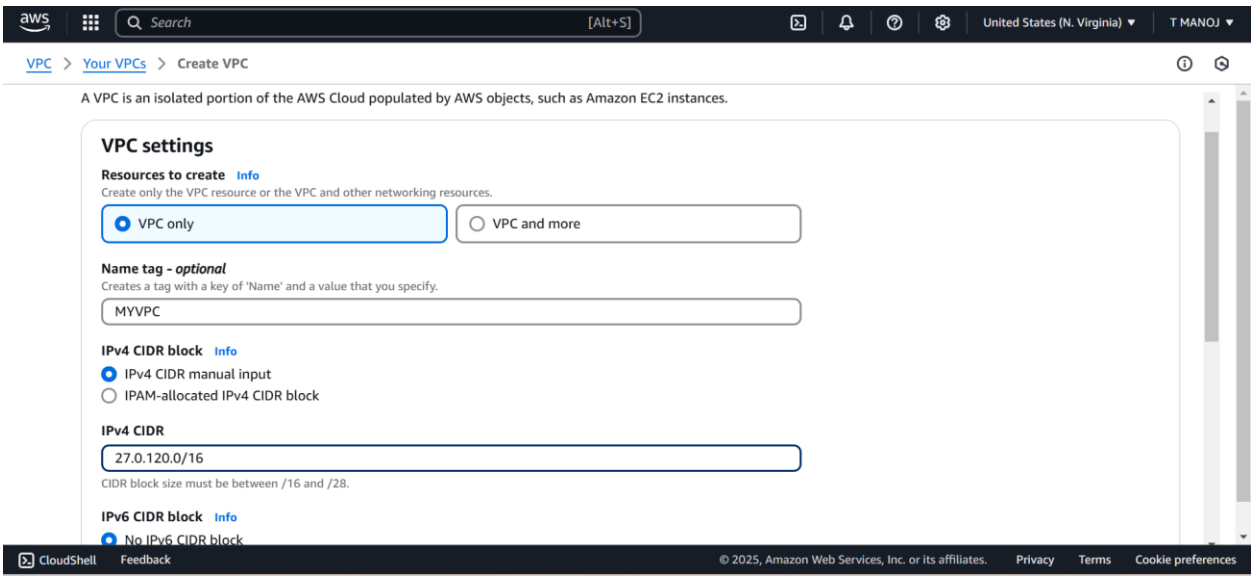


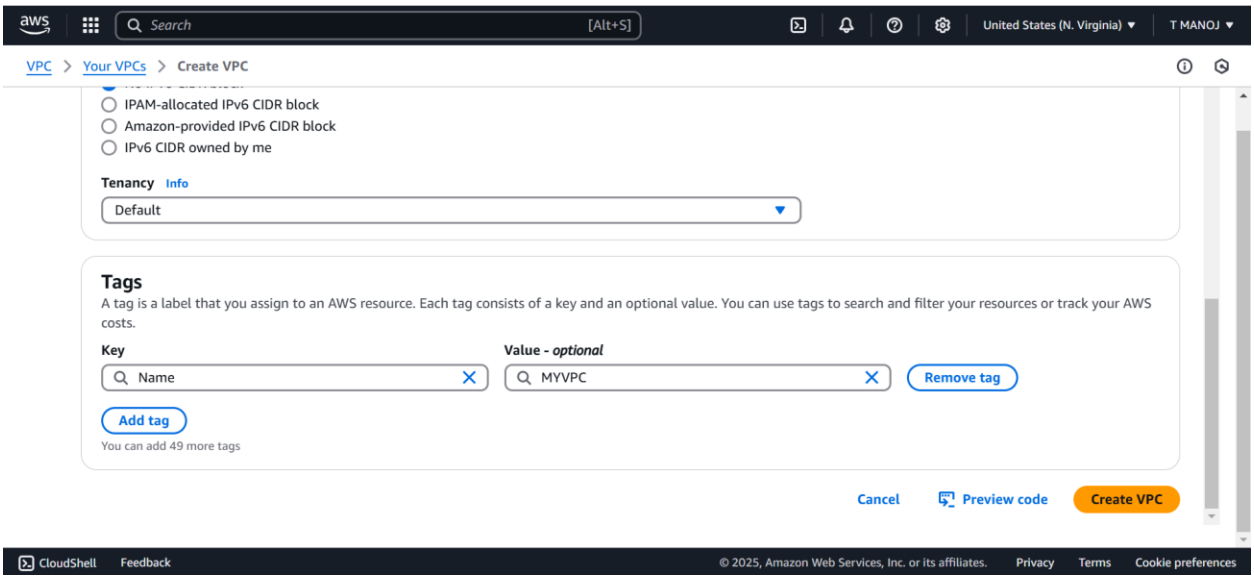
VPC Setup with Public and Private Subnets and EC2 Instances

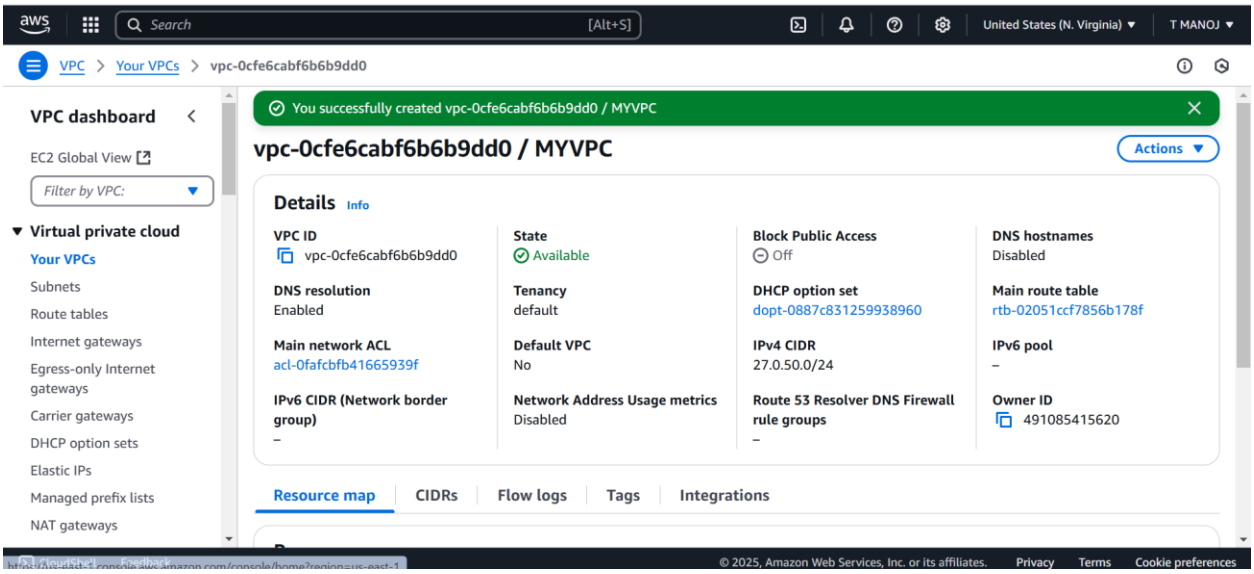
Step 1: Create VPC

1. Go to AWS Console → VPC → Your VPCs → Create VPC.
2. Name tag: MyVPC
3. IPv4 CIDR block: `27.0.50.0/24`
4. Tenancy: Default
5. Click Create VPC.


Search [Alt+S]
United States (N. Virginia)
T MANOJ
VPC dashboard
EC2 Global View
Filter by 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
NAT gateways
Create VPC
Launch EC2 Instances
Note: Your Instances will launch in the United States region.
Resources by Region
Refresh Resources
You are using the following Amazon VPC resources
VPCs United States 1
See all regions
NAT Gateways United States 0
See all regions
Subnets United States 11
See all regions
VPC Peering Connections United States 0
See all regions
Route Tables United States 2
See all regions
Network ACLs United States 1
See all regions
Internet Gateways United States 1
Security Groups United States 6
Service Health
View complete service health details
Settings
Block Public Access
Zones
Console Experiments
Additional Information
VPC Documentation
All VPC Resources
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
T MANOJ
VPC > Your VPCs > Create VPC
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
MYVPC
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
27.0.120.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences





Step 2: Divide the Network into Public and Private Subnets

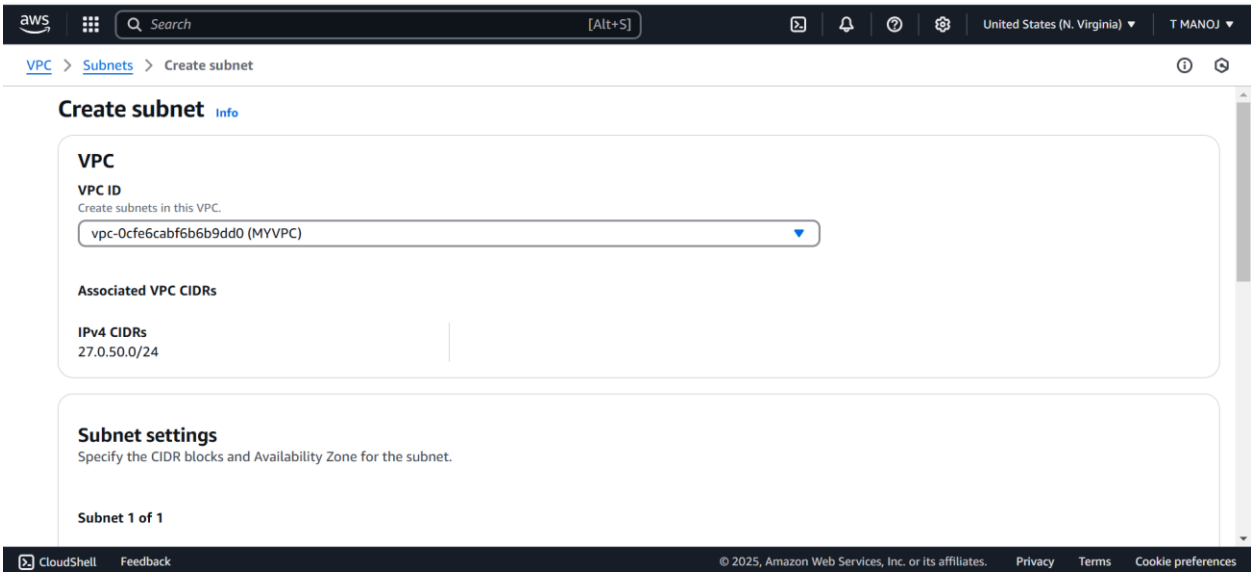
VPC CIDR Block: `27.0.50.0/24`

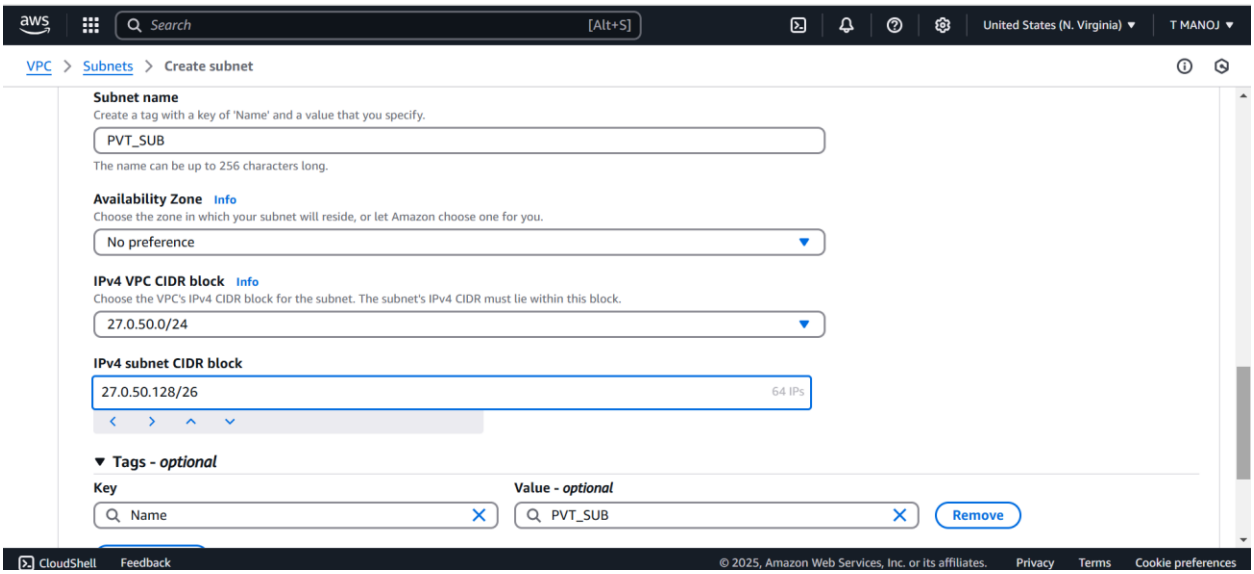
- Public Subnet: `27.0.50.0/26`
  - First IP: 27.0.50.1
  - Last IP: 27.0.50.62
  - Gateway IP: 27.0.50.63
- Private Subnet: `27.0.50.128/26`
  - First IP: 27.0.50.129

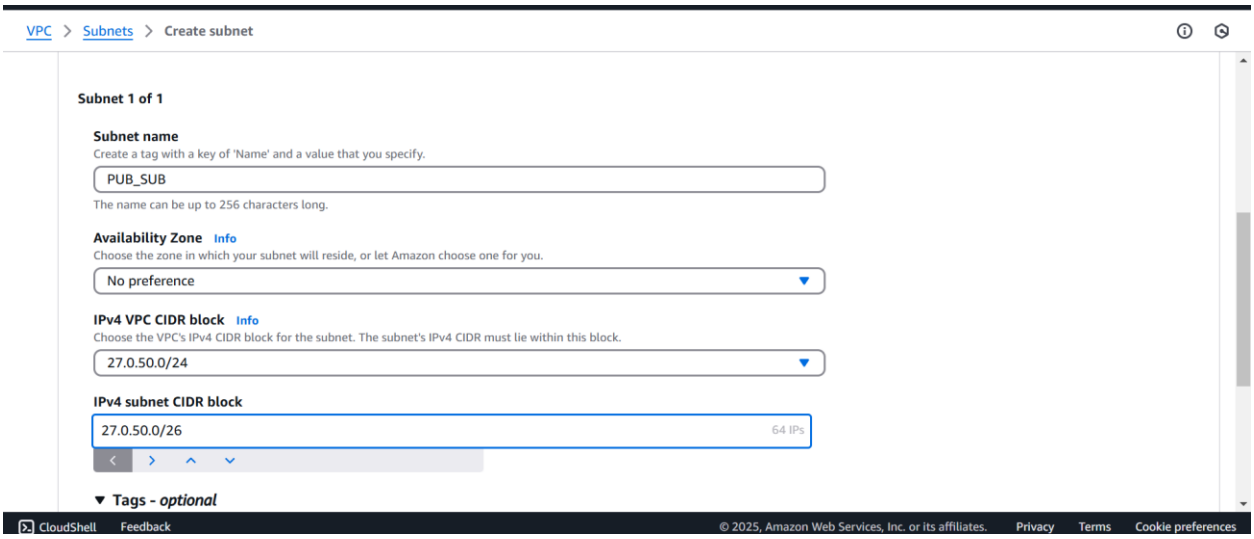
- Last IP: 27.0.50.190
- Gateway IP: 27.0.50.191

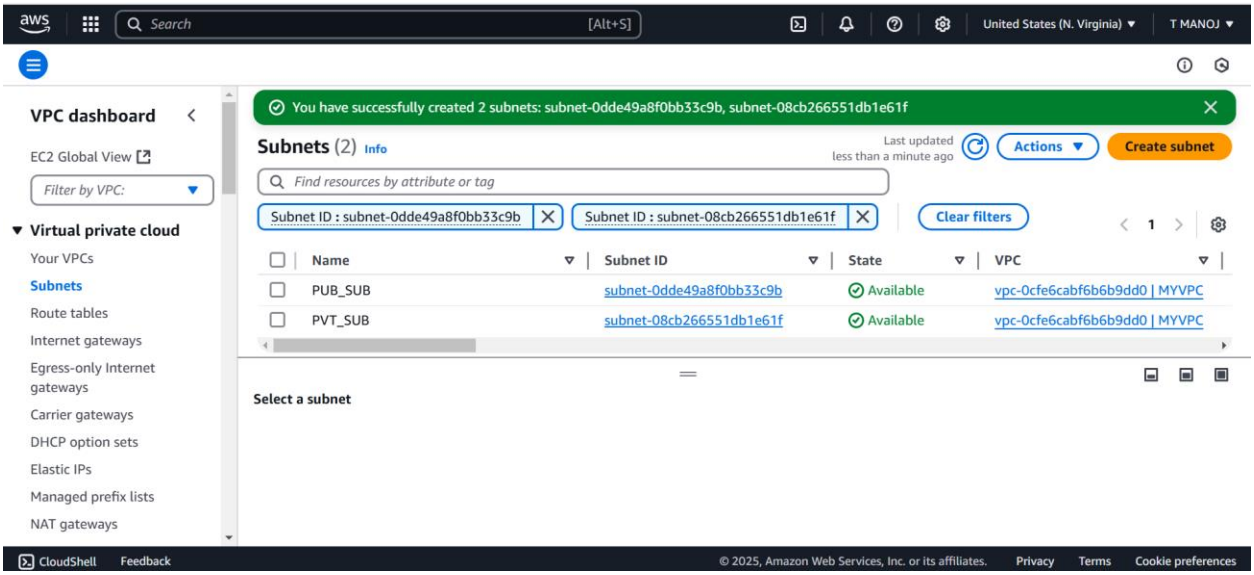
Step 3: Create Subnets

1. Go to Subnets → Create subnet.
2. Select VPC: MyVPC.
3. Subnet Name: `Public-Subnet` → CIDR block: `27.0.50.0/26` → AZ: Select any → Create.
4. Subnet Name: `Private-Subnet` → CIDR block: `27.0.50.128/26` → Create.



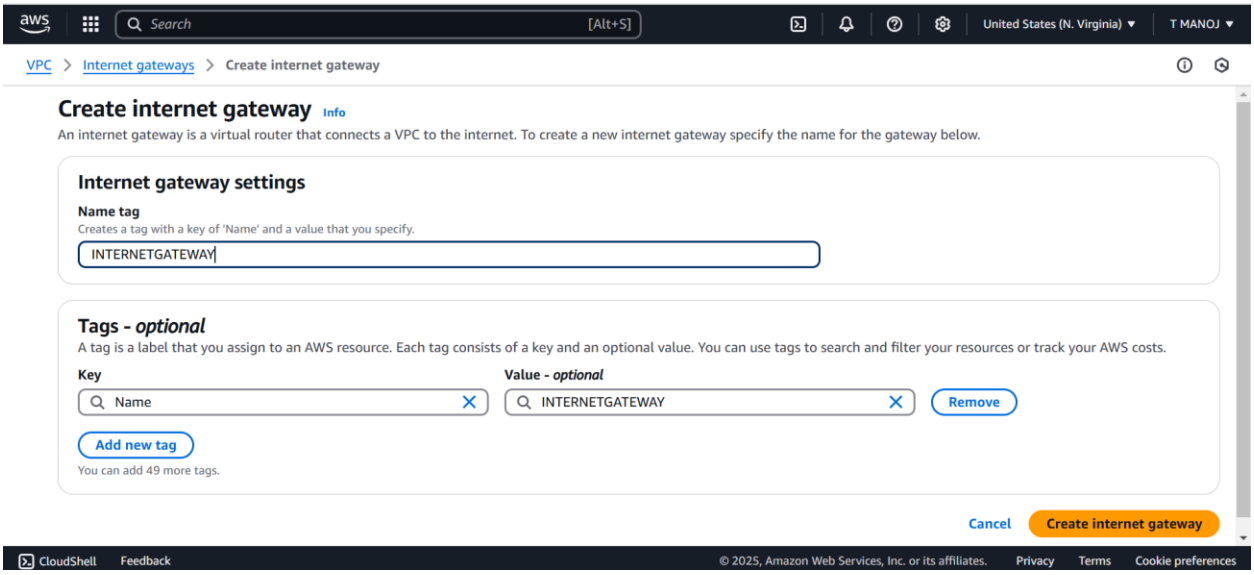


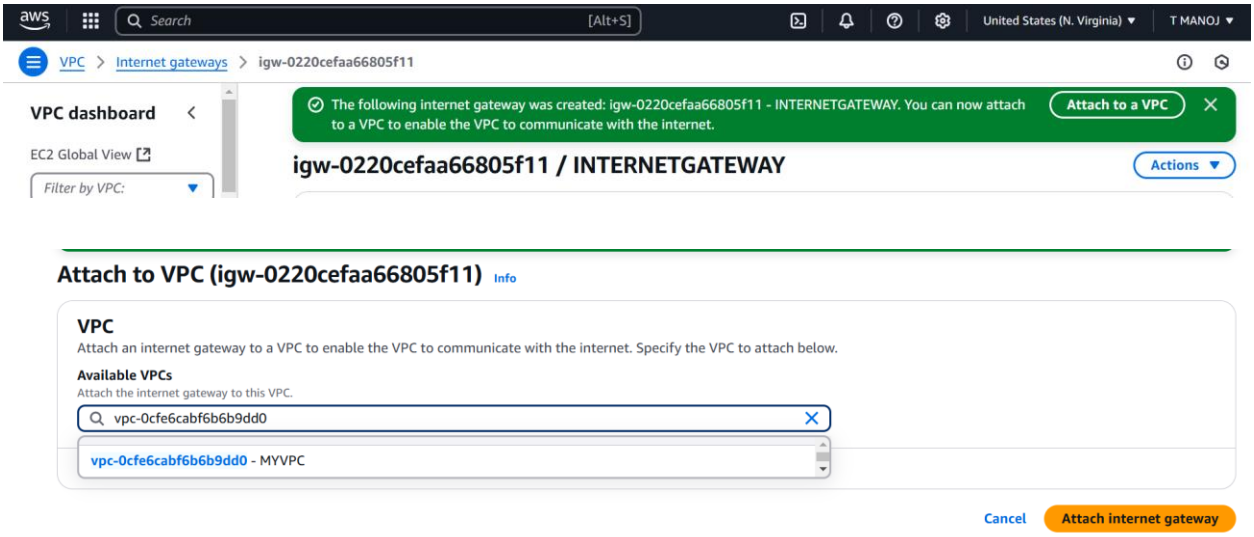


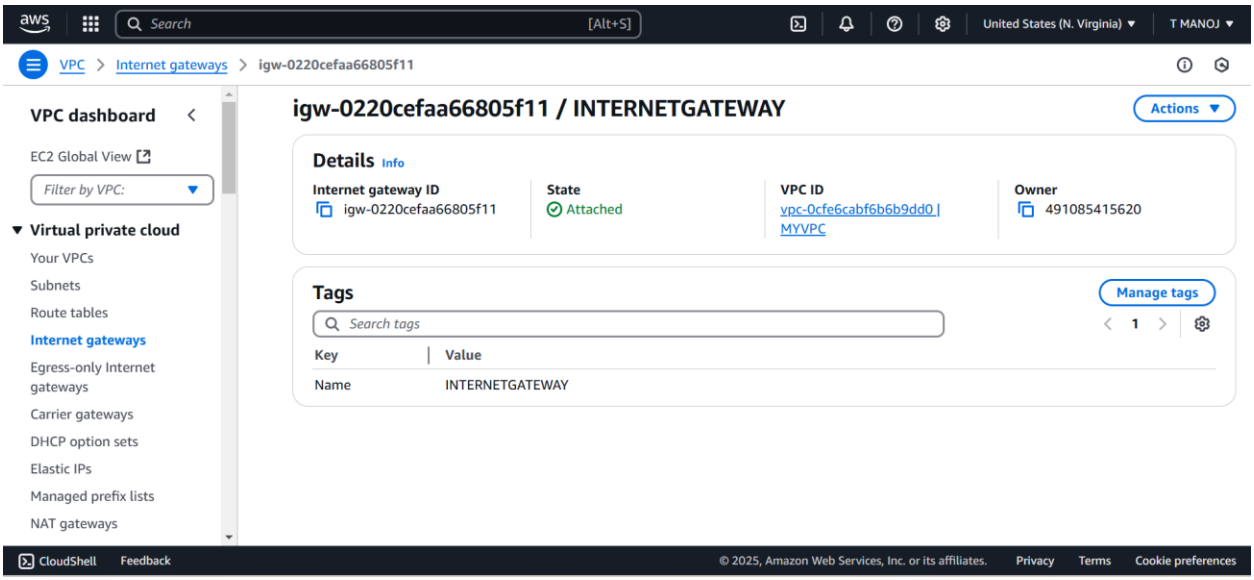


Step 4: Create and Attach Internet Gateway (IGW)

1. Go to Internet Gateways → Create internet gateway.
2. Name tag: `MyIGW` → Create.
3. Select MyIGW → Actions → Attach to VPC → Select MyVPC → Attach.

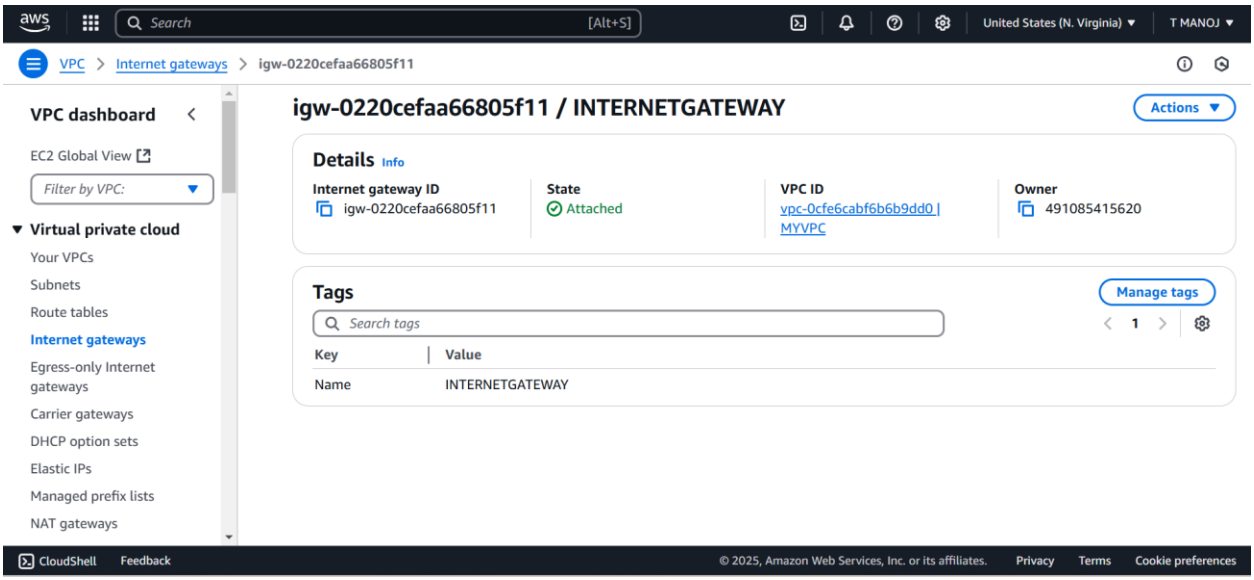

Search
[Alt+S]
United States (N. Virginia)
T MANOJ
VPC > Internet gateways > Create internet gateway
Create internet gateway Info
An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.
Internet gateway settings
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
INTERNETGATEWAY
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
INTERNETGATEWAY
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

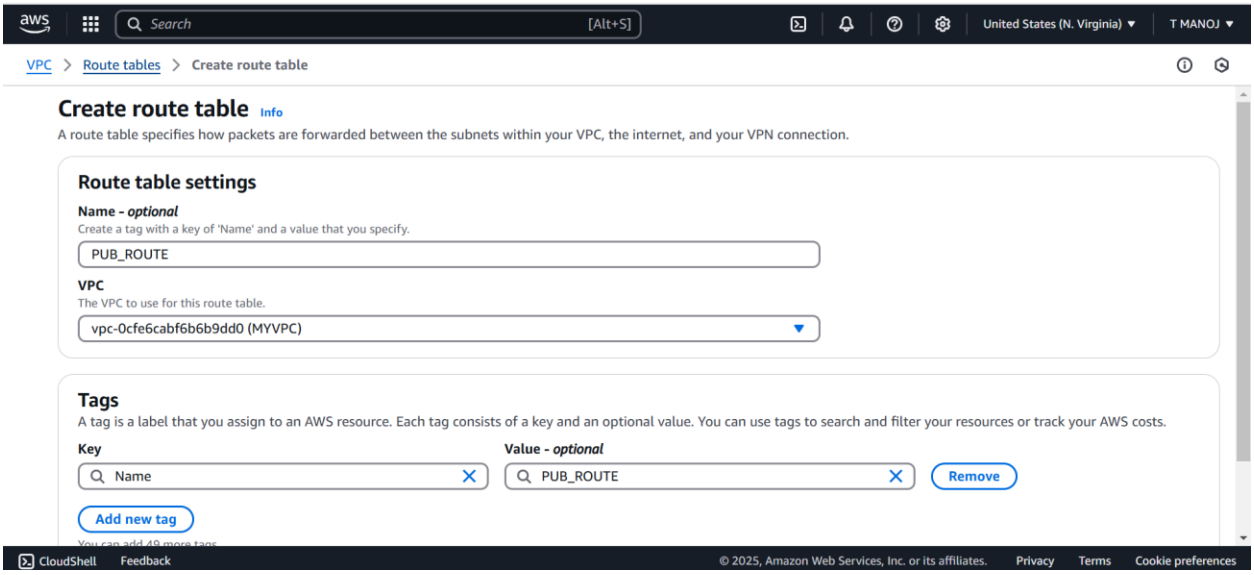

Search
[Alt+S]
United States (N. Virginia)
T MANOJ
VPC > Internet gateways > igw-0220cefaa66805f11
VPC dashboard
EC2 Global View
Filter by VPC:
The following internet gateway was created: igw-0220cefaa66805f11 - INTERNETGATEWAY. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
igw-0220cefaa66805f11 / INTERNETGATEWAY
Actions
Attach to VPC (igw-0220cefaa66805f11) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
vpc-0cfe6cabf6b6b9dd0
vpc-0cfe6cabf6b6b9dd0 - MYVPC
Cancel
Attach internet gateway

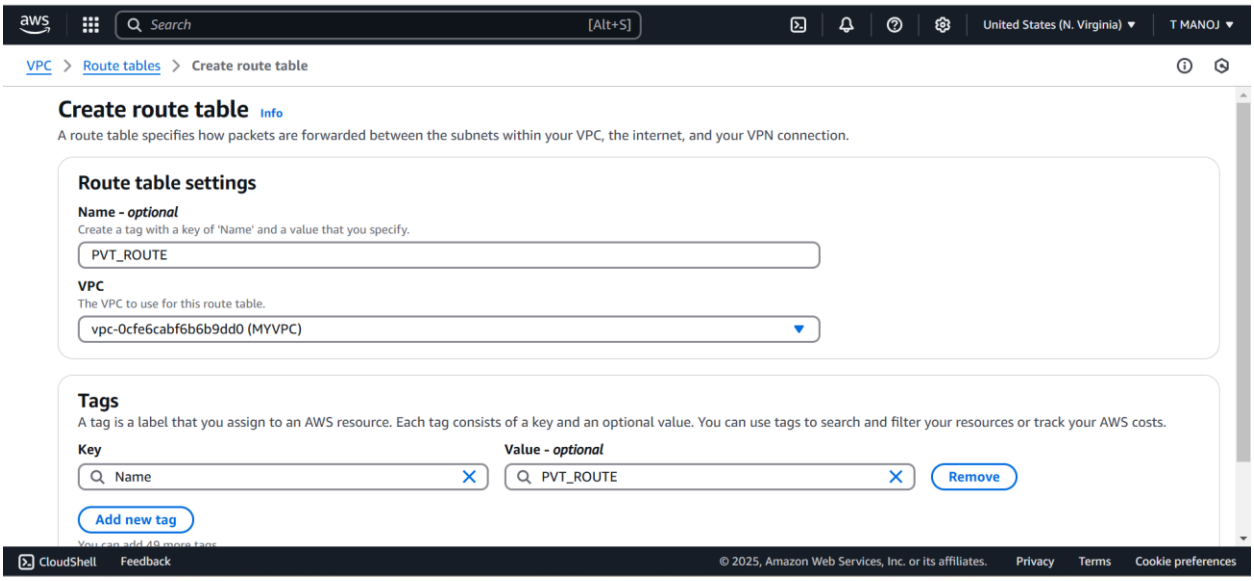


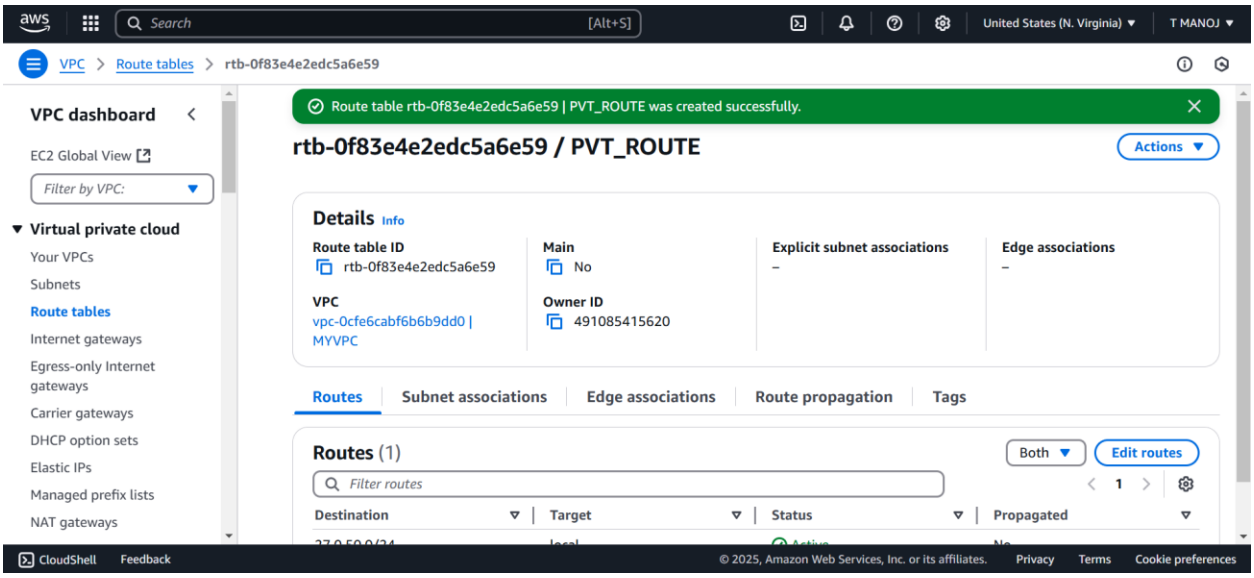
Step 5: Create Route Tables

1. Go to Route Tables → Create route table.
2. Name tag: `Public-Route-Table` → VPC: MyVPC → Create.
3. Name tag: `Private-Route-Table` → VPC: MyVPC → Create.




aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
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
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
PUB_ROUTE
VPC
The VPC to use for this route table.
vpc-0cfe6cabf6b6b9dd0 (MYVPC)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
PUB_ROUTE
Remove
Add new tag
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

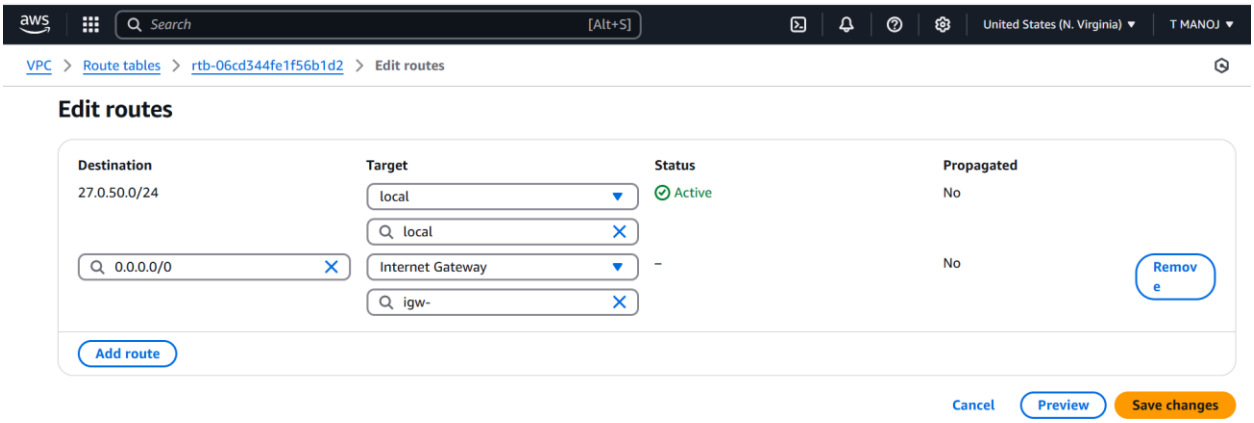

aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
PVT_ROUTE
VPC
The VPC to use for this route table.
vpc-0cfe6cabf6b6b9dd0 (MYVPC)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
PVT_ROUTE
Remove
Add new tag
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

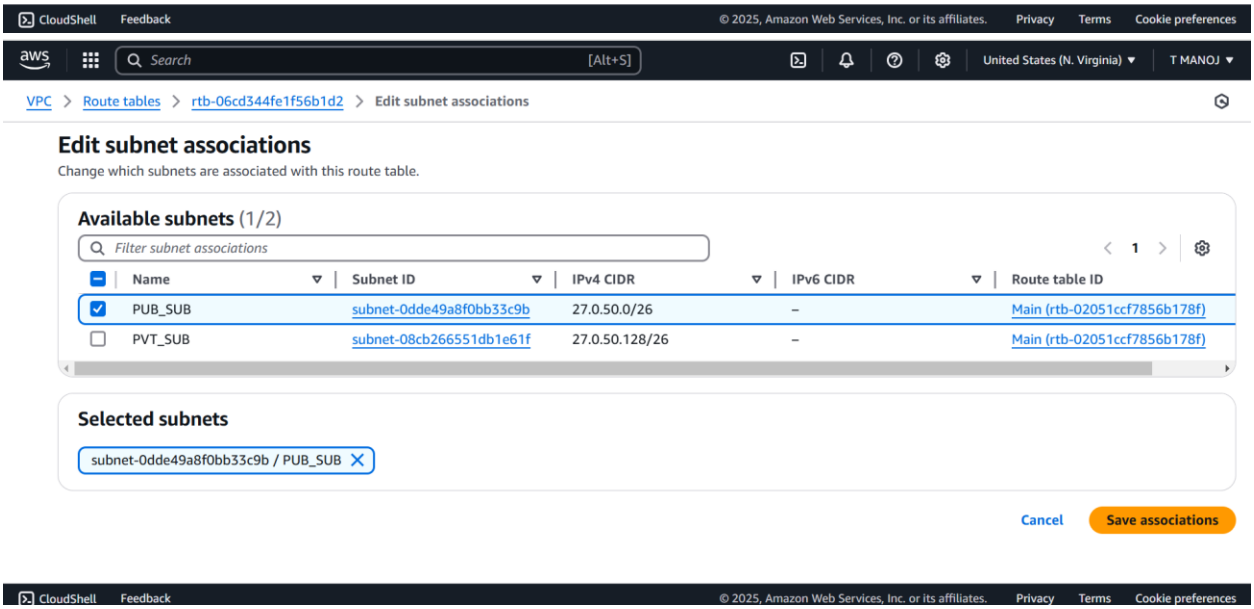


Step 6: Configure Public Route Table

1. Select Public-Route-Table → Routes → Edit routes.
2. Add route: Destination: `0.0.0.0/0` → Target: Select Internet Gateway (MyIGW) → Save.

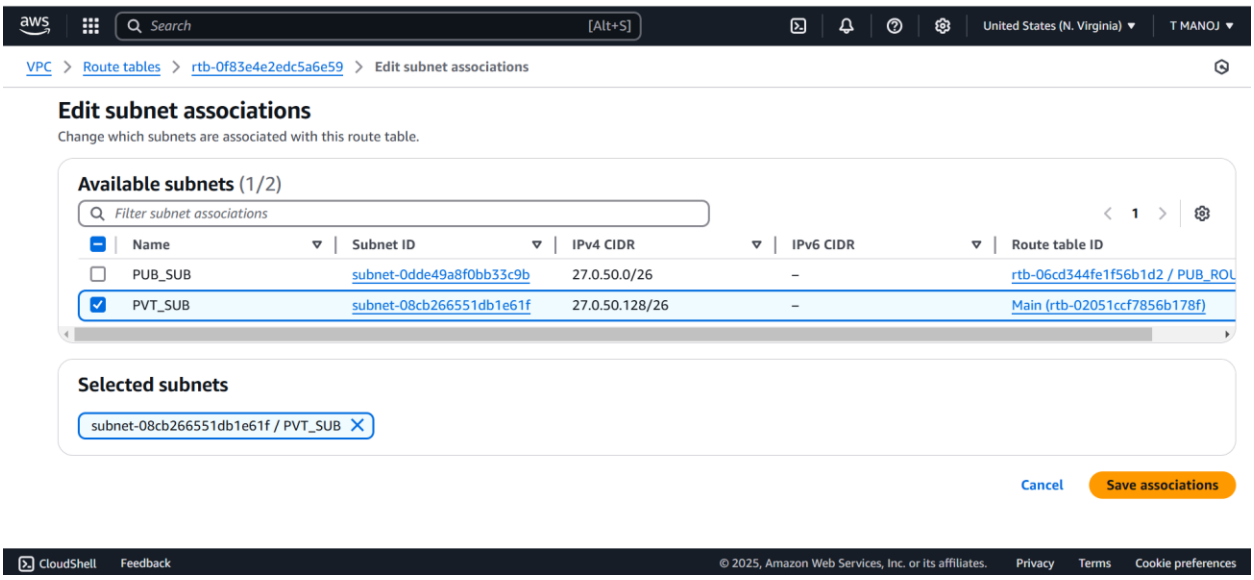
3. Subnet associations → Edit subnet associations → Select Public-Subnet → Save.





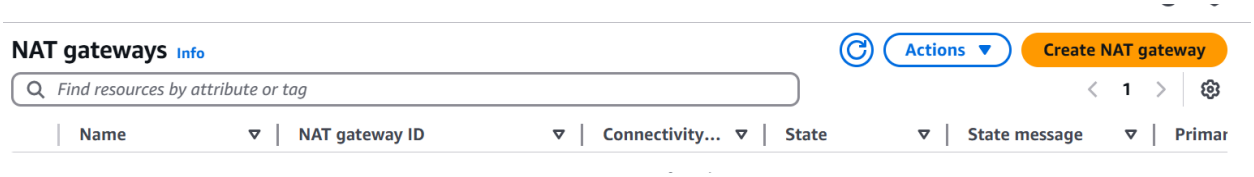
Step 7: Configure Private Route Table

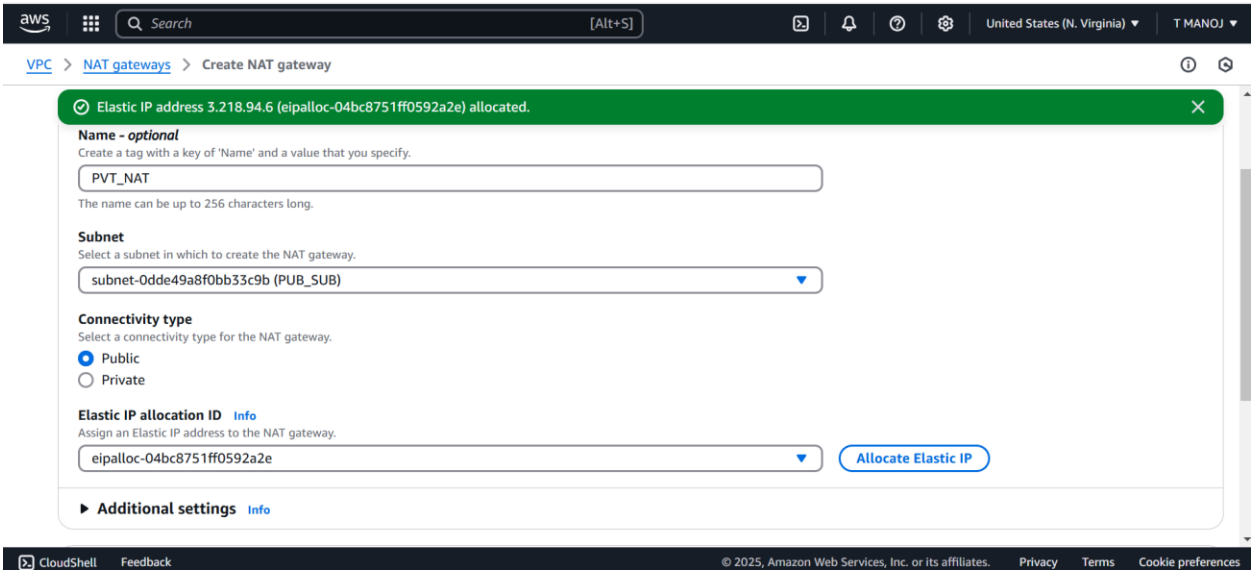
1. Select Private-Route-Table → Subnet associations → Select Private-Subnet → Save.

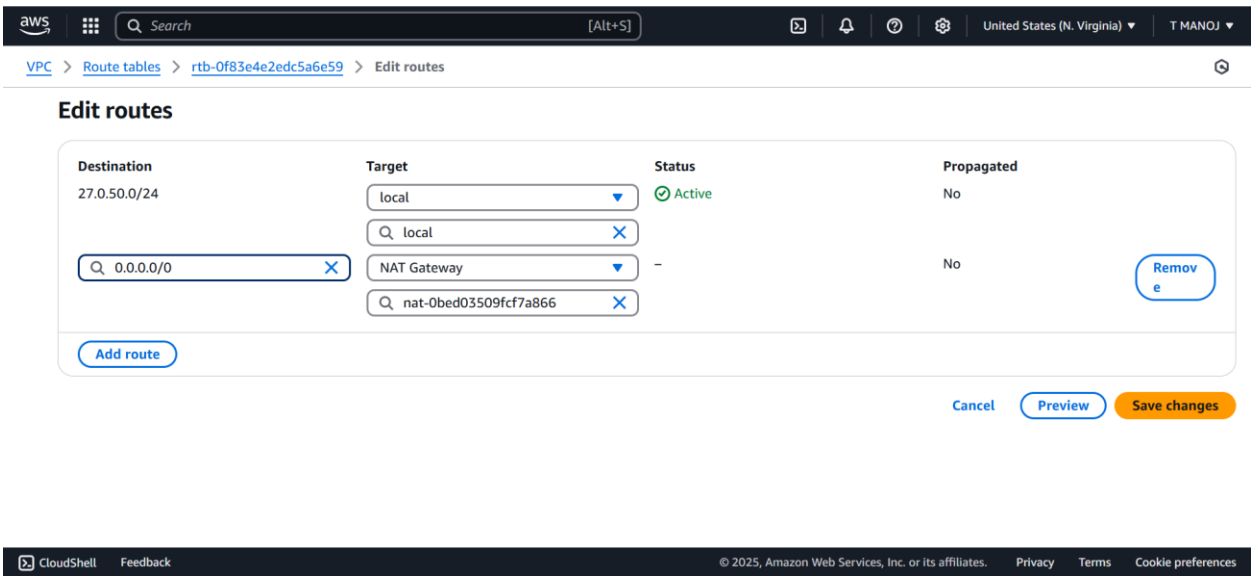


Step 8: Create NAT Gateway for Private Subnet Internet Access

1. Go to Elastic IPs → Allocate Elastic IP → Allocate.
2. Go to NAT Gateways → Create NAT gateway.
3. Subnet: `Public-Subnet` → Elastic IP: Select the allocated EIP → Create NAT gateway.
4. Wait for the NAT gateway to become available.
5. Go back to Private-Route-Table → Routes → Edit routes.
    a. Destination: `0.0.0.0/0` → Target: Select NAT Gateway → Save.

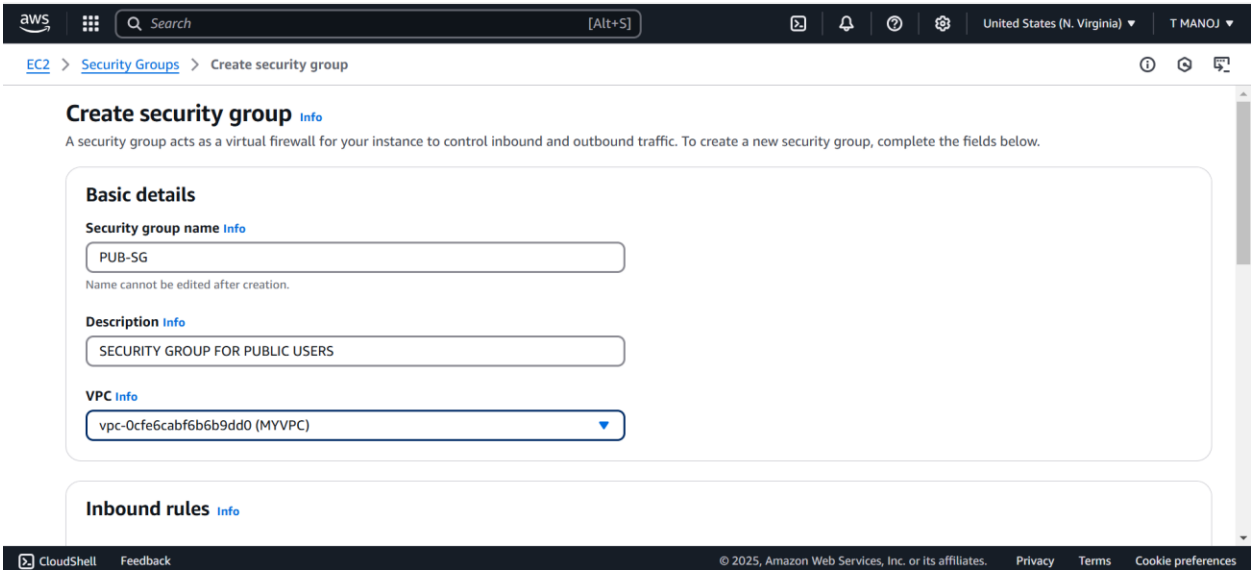


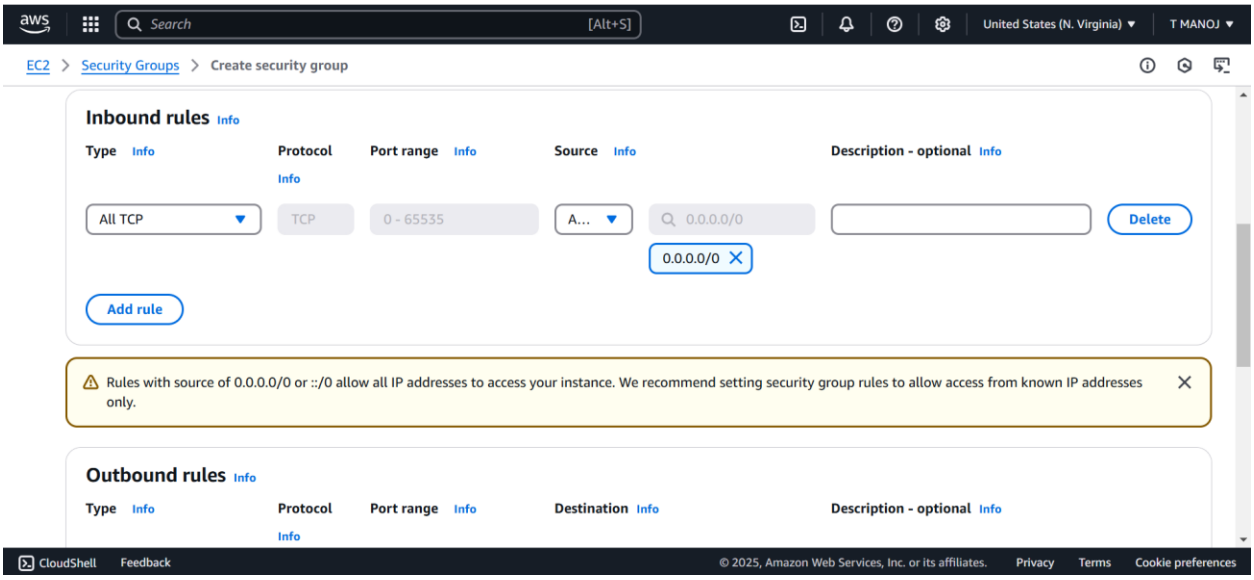


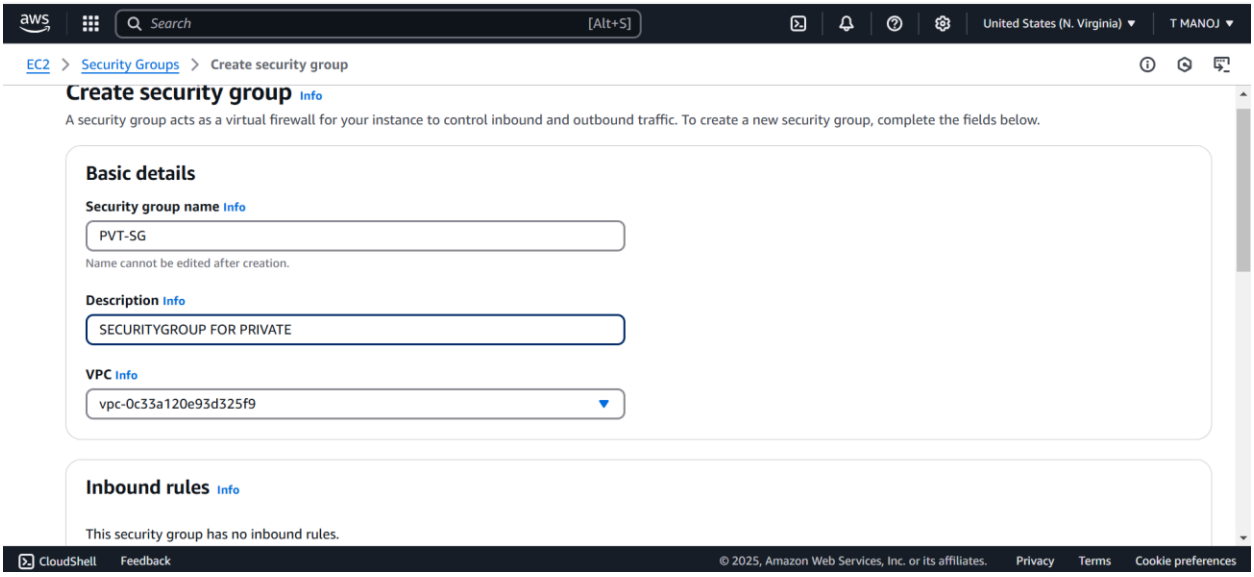


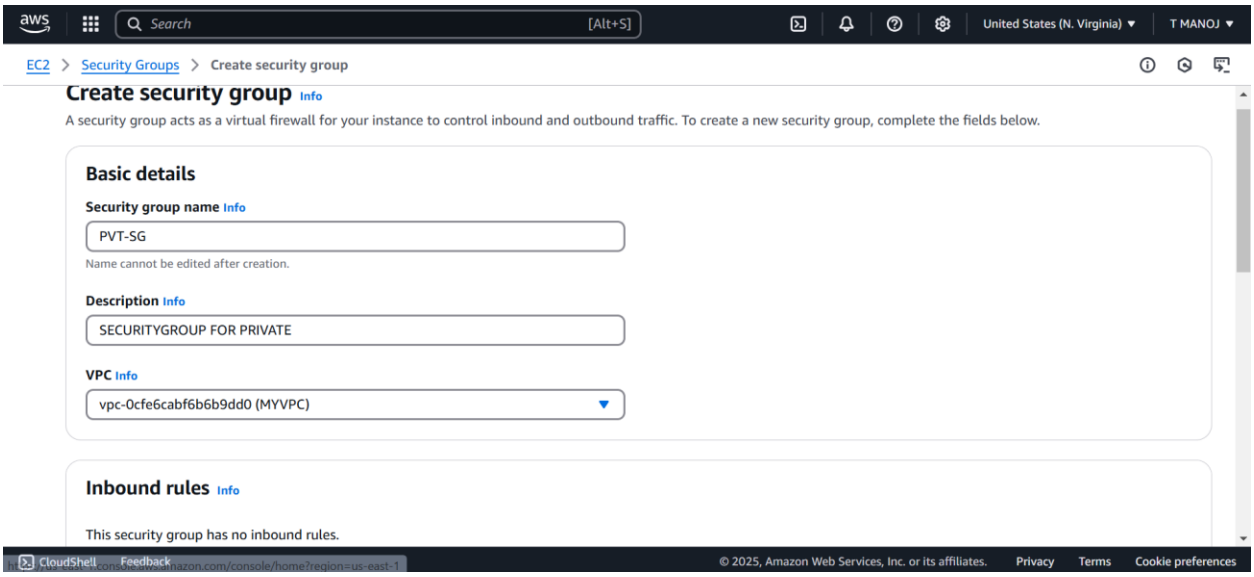
Step 9: Configure Security Groups

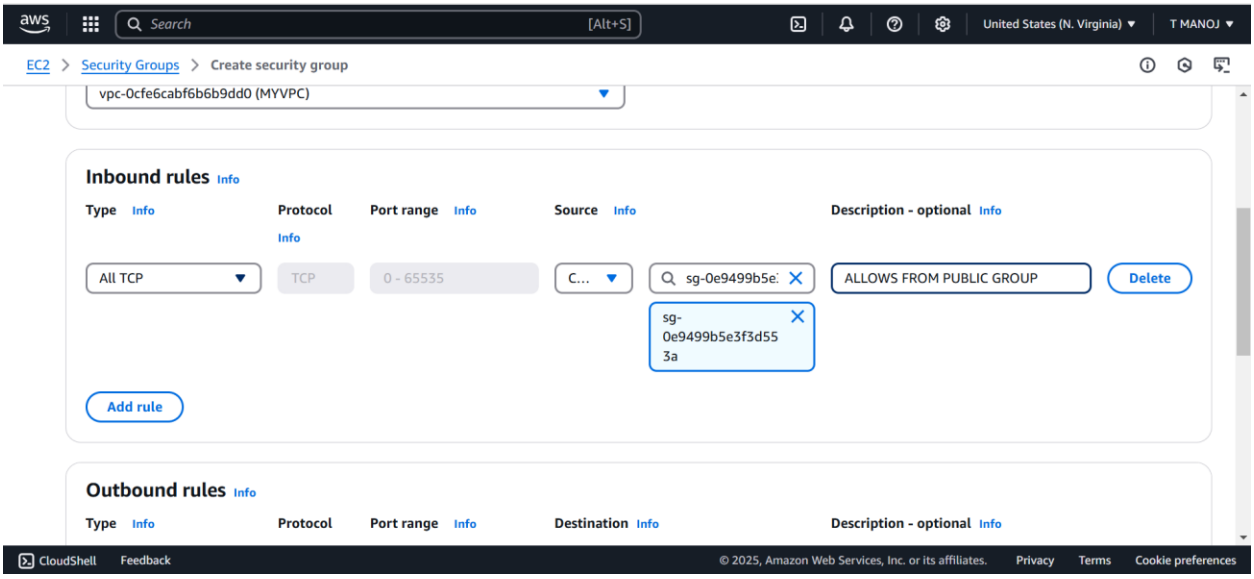
- Public Security Group (Public-SG):
  - Inbound: All TCP, Port range: 0-65535, Source: `0.0.0.0/0`
  - Outbound: All traffic, `0.0.0.0/0`
- Private Security Group (Private-SG):
  - Inbound: All TCP, Source: `Public-SG`
  - Outbound: All traffic, `0.0.0.0/0`


aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
PUB-SG
Name cannot be edited after creation.
Description Info
SECURITY GROUP FOR PUBLIC USERS
VPC Info
vpc-0cfe6cabf6b6b9dd0 (MYVPC)
Inbound rules Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Security Groups > Create security group
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
All TCP
TCP
0 - 65535
A...
0.0.0.0/0
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

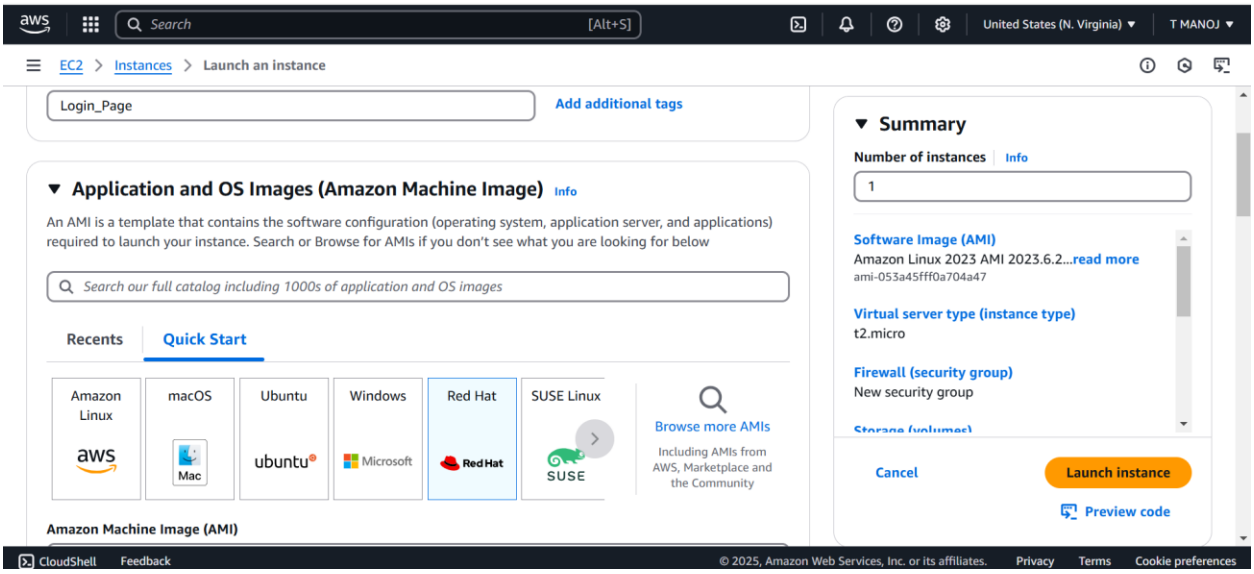

aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
PVT-SG
Name cannot be edited after creation.
Description Info
SECURITYGROUP FOR PRIVATE
VPC Info
vpc-0c33a120e93d325f9
Inbound rules Info
This security group has no inbound rules.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
PVT-SG
Name cannot be edited after creation.
Description Info
SECURITYGROUP FOR PRIVATE
VPC Info
vpc-0cfe6cabf6b6b9dd0 (MYVPC)
Inbound rules Info
This security group has no inbound rules.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Step 10: Launch EC2 Instances

1. Home Page Instance (Public EC2):
    a. Go to EC2 → Launch instance.
    b. Name: `HomePageInstance`
    c. Network settings:
        i. VPC: `MyVPC`
        ii. Subnet: `Public-Subnet`
        iii. Auto-assign Public IP: Enable
        iv. Security group: Select `Public-SG`
    d. Launch instance.
2. Login Page Instance (Private EC2):
    a. Name: `LoginPageInstance`
    b. VPC: `MyVPC`
    c. Subnet: `Private-Subnet`
    d. Auto-assign Public IP: Disable
    e. Security group: Select `Private-SG`
    f. Launch instance.



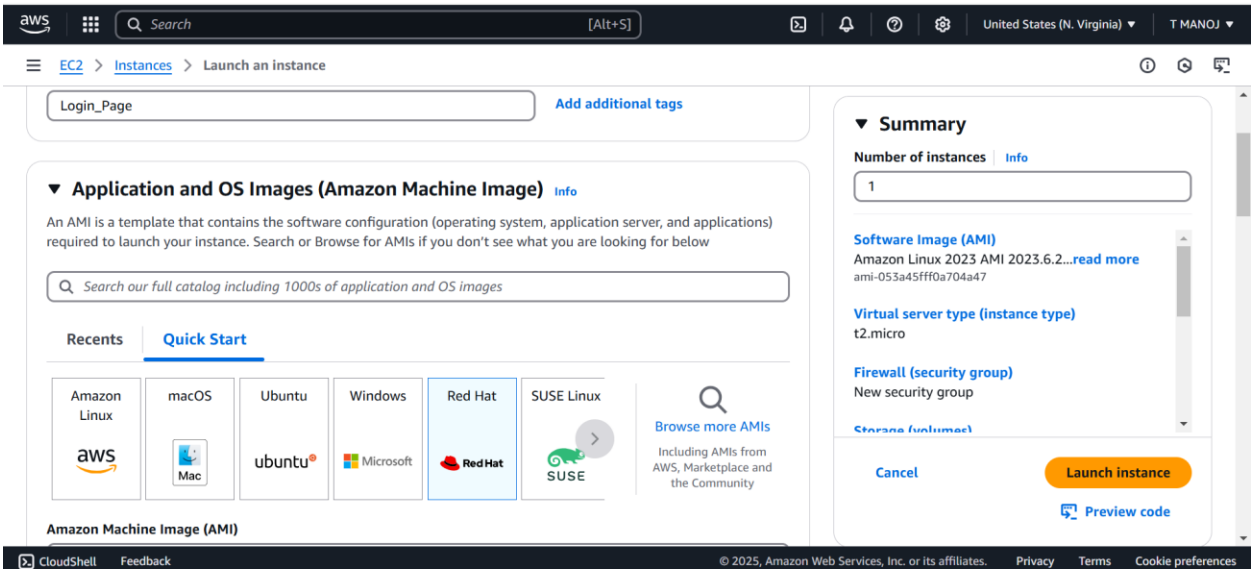
Key pair (login) Info

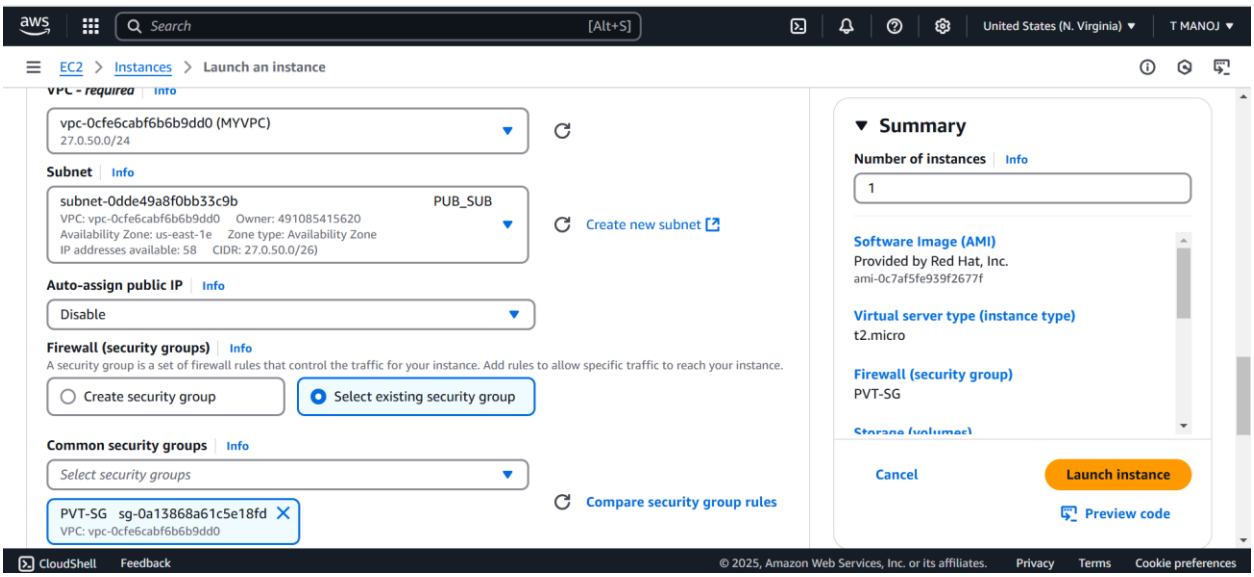
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

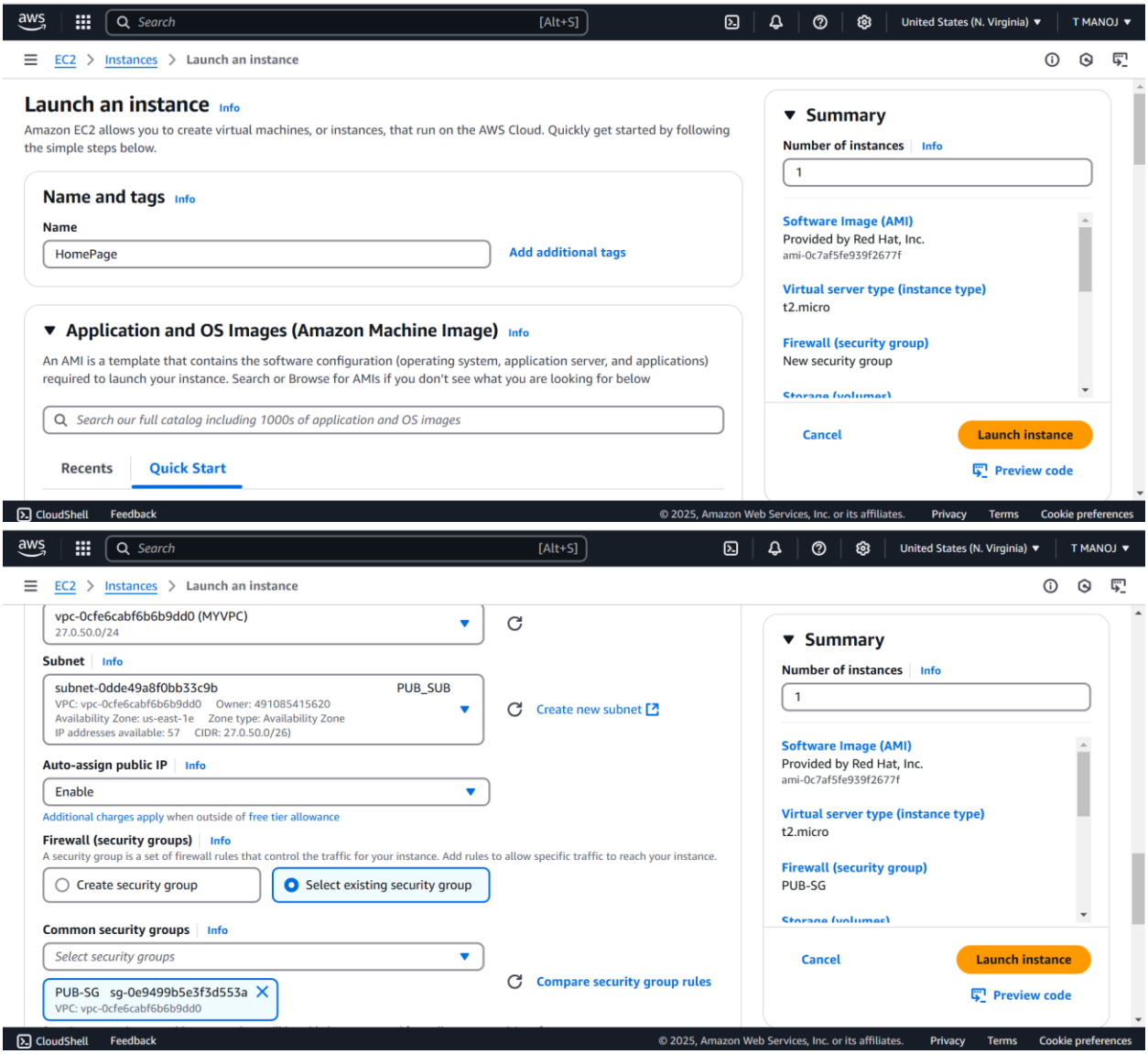
Key pair name - *required*

RHLLINUX

Create new key pair


aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Instances > Launch an instance
Login_Page
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
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-053a45fff0a704a47
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
United States (N. Virginia)
T MANOJ
EC2 > Instances > Launch an instance
VPC - required Info
vpc-0cfe6cabf6b6b9dd0 (MYVPC)
27.0.50.0/24
Subnet Info
subnet-0dde49a8f0bb33c9b
PUB_SUB
VPC: vpc-0cfe6cabf6b6b9dd0 Owner: 491085415620
Availability Zone: us-east-1e Zone type: Availability Zone
IP addresses available: 58 CIDR: 27.0.50.0/26)
Create new subnet
Auto-assign public IP Info
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups Info
Select security groups
PVT-SG sg-0a13868a61c5e18fd
VPC: vpc-0cfe6cabf6b6b9dd0
Compare security group rules
Summary
Number of instances Info
1
Software Image (AMI)
Provided by Red Hat, Inc.
ami-0c7af5fe939f2677f
Virtual server type (instance type)
t2.micro
Firewall (security group)
PVT-SG
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Step 11: Connect Instances and Configure HTTPD

1. Connect to Public EC2:

```
ssh -i "/path/to/key.pem" ec2-user@<Public-Instance-Public-IP>
```

2. From Public EC2, SSH into Private EC2:

```
ssh -i "/path/to/key.pem" ec2-user@<Private-Instance-Private-IP>
```

3. Install HTTPD on Both Instances:

```
sudo yum update -y
sudo yum install httpd -y
sudo systemctl start httpd
sudo systemctl enable httpd
```

4. Add HTML Files:
    a. On Private Instance (`/var/www/html/login.html`):

```
<html><body><h2>Login Page</h2></body></html>
```

    b. On Public Instance (`/var/www/html/index.html`):

Step 12: Configure Reverse Proxy on Public Instance

1. Enable Proxy Modules:

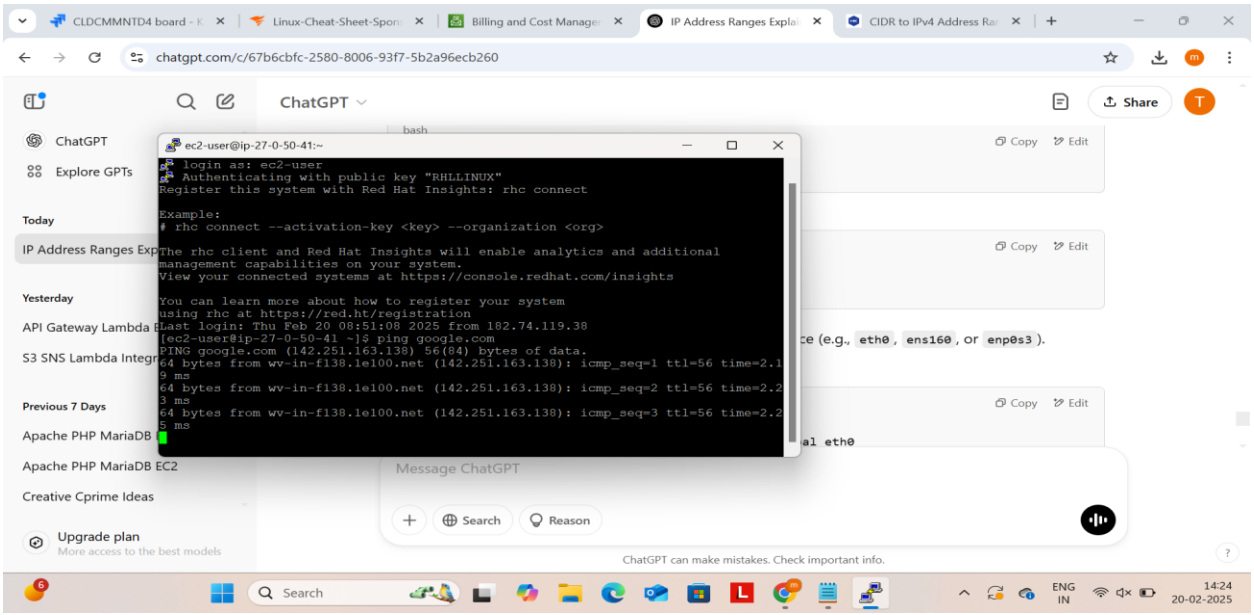
```
sudo yum install mod_proxy -y
sudo yum install mod_proxy_http -y
```

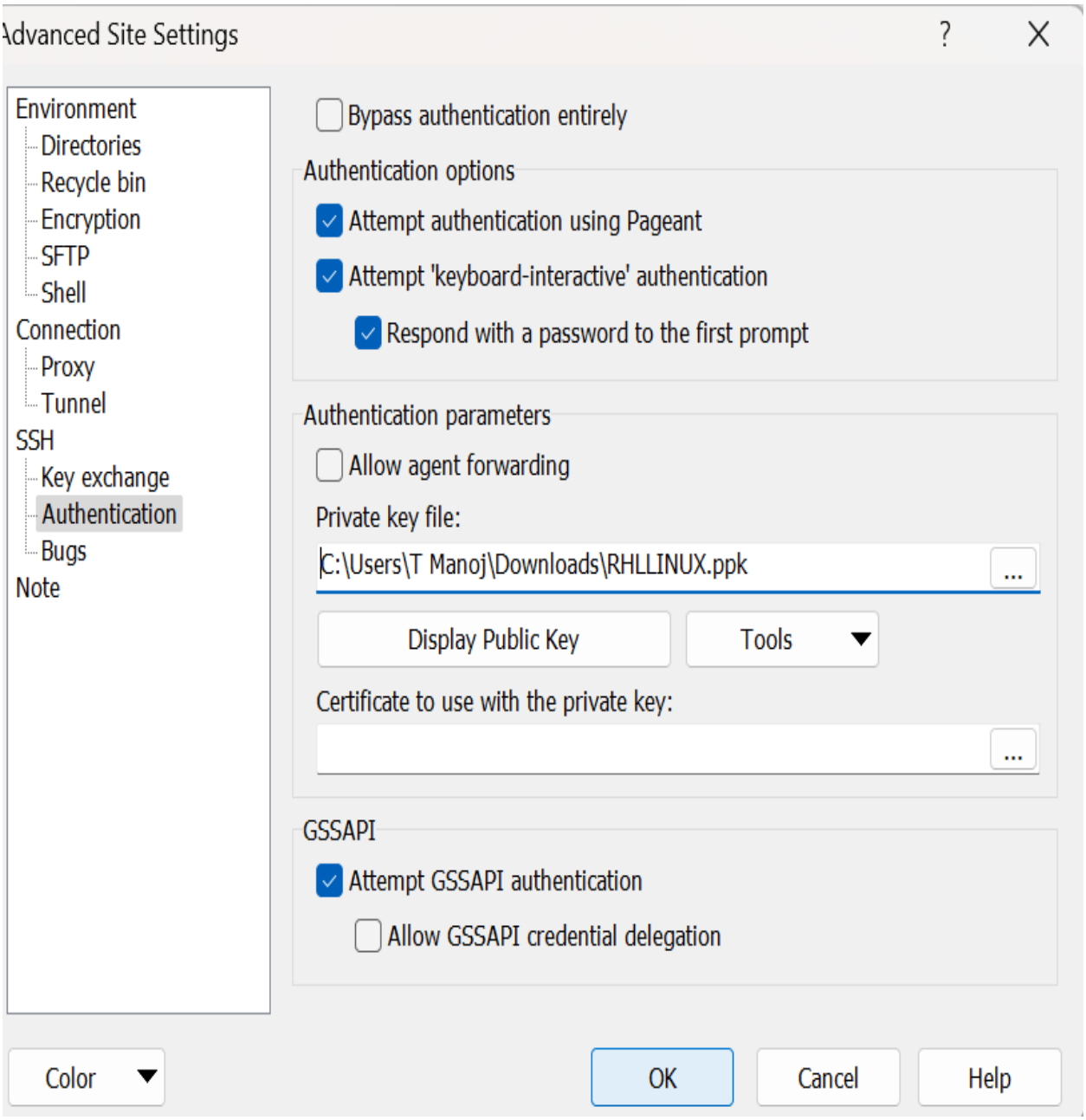
2. Edit Apache Config:

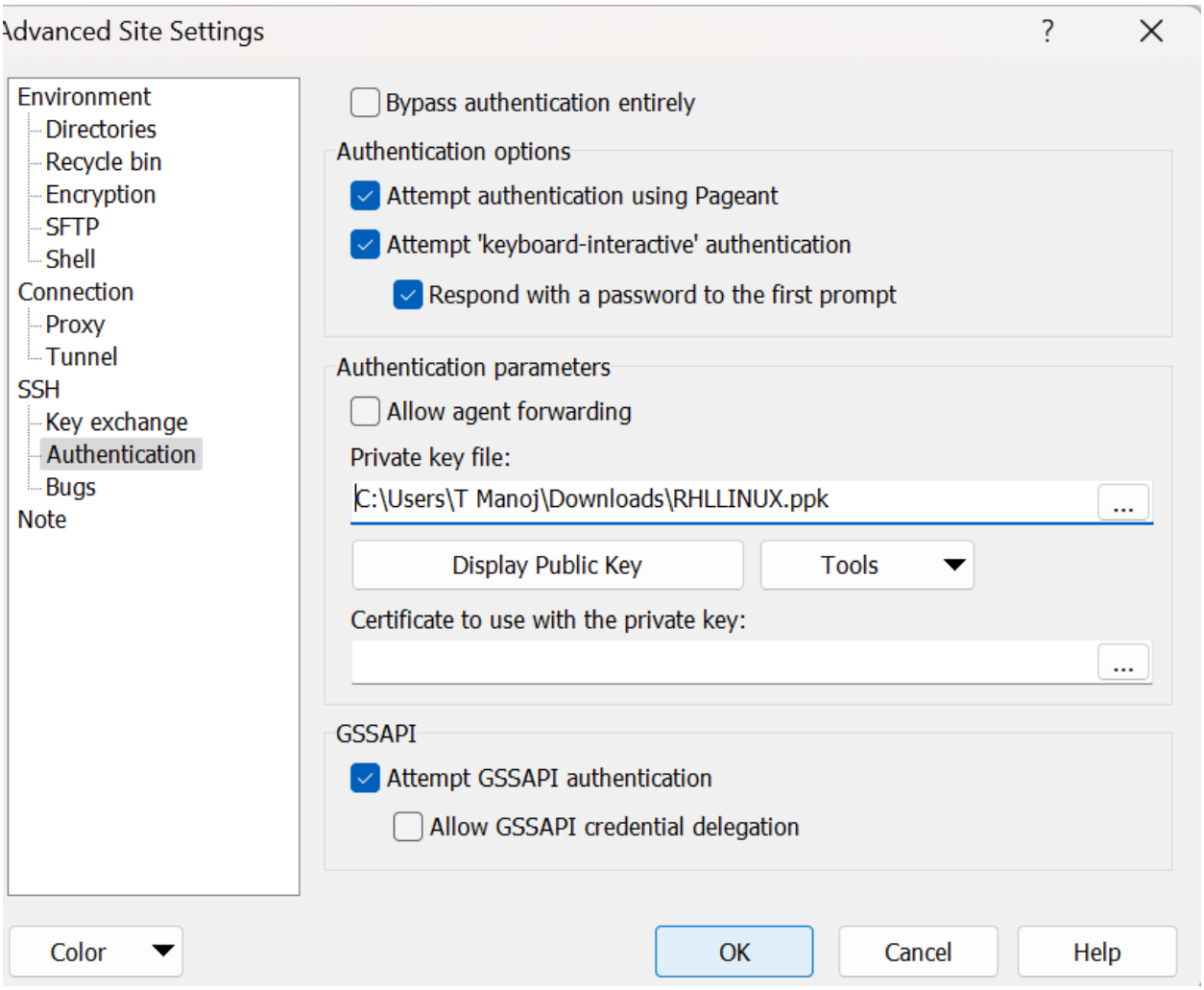
```
sudo vi /etc/httpd/conf/httpd.conf

<VirtualHost *:80>
    ServerName PublicIP

    ProxyPreserveHost On
    ProxyPass ‘/login’  ‘http://privateIP/’
    ProxyPassReverse /login’  ‘http://privateIP/’

    ErrorLog /var/log/httpd/reverse-proxy-error.log
    CustomLog /var/log/httpd/reverse-proxy-access.log combined
</VirtualHost>
```

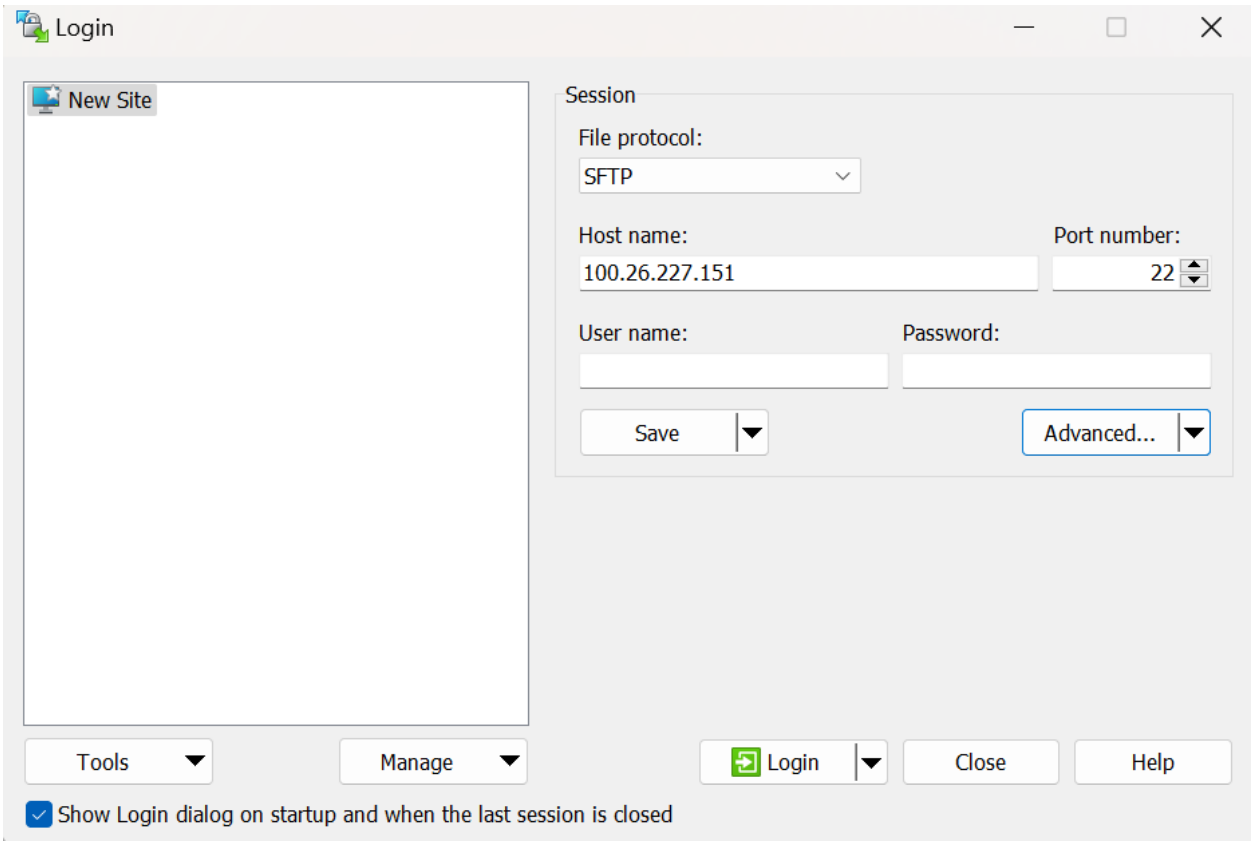
3. Restart HTTPD:

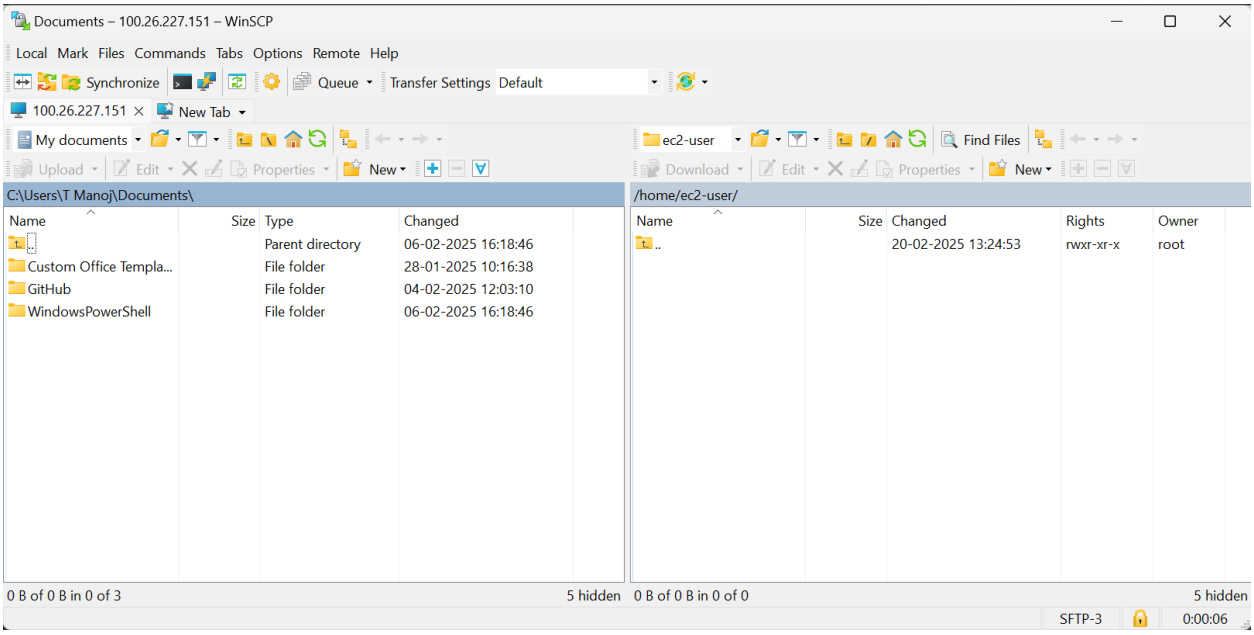
```
sudo systemctl restart httpd
```

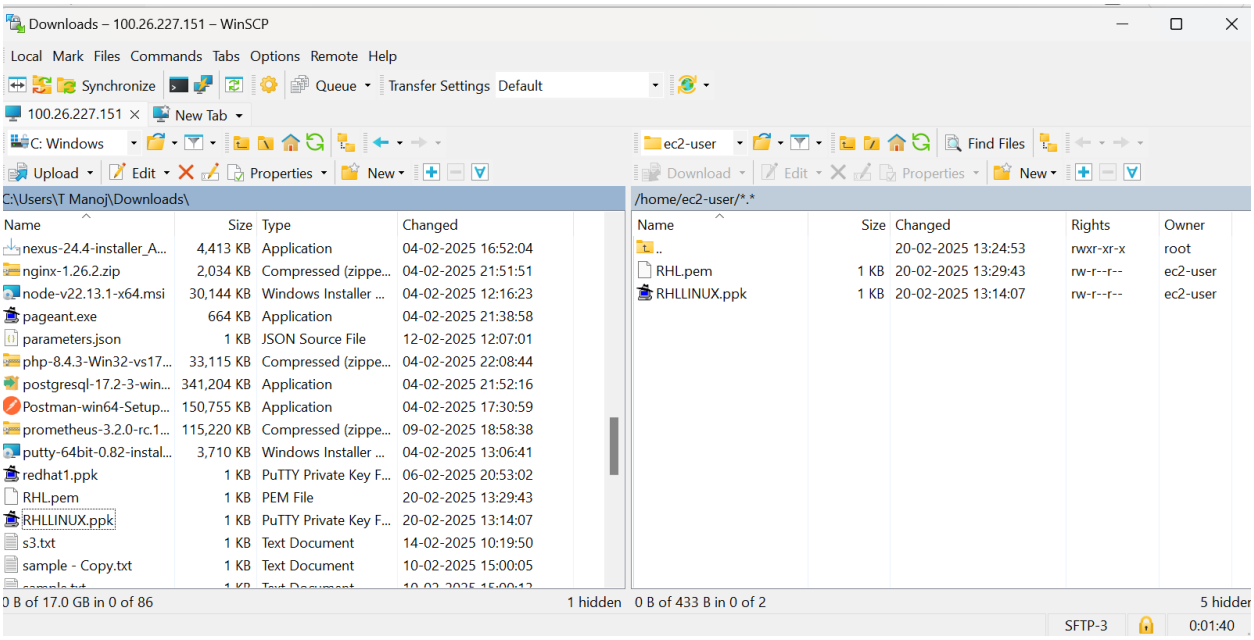


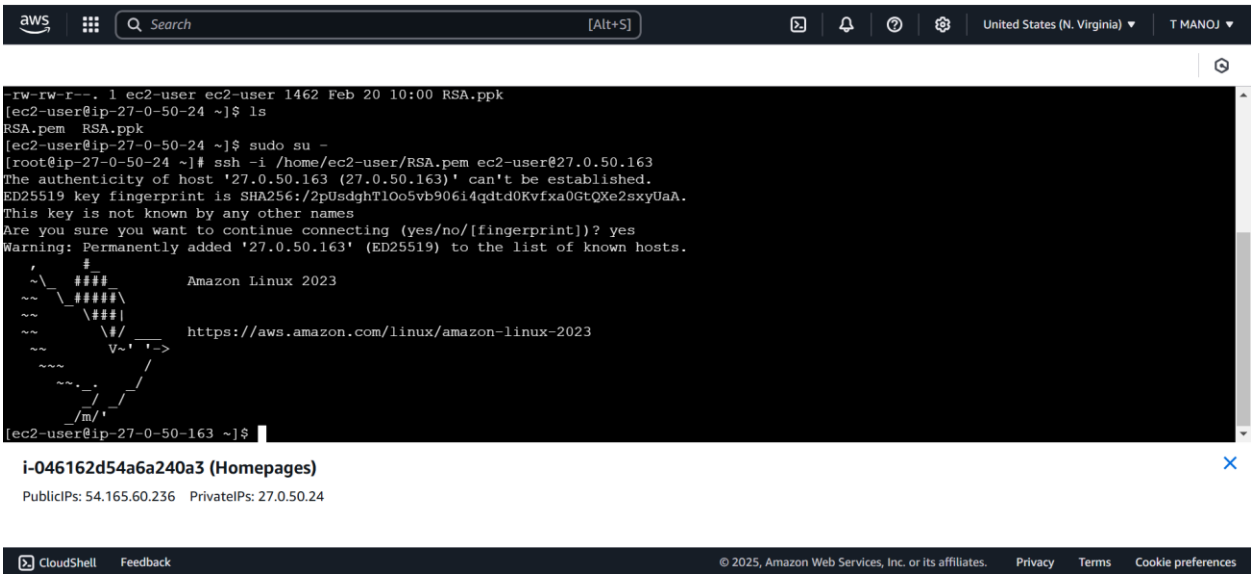

Advanced Site Settings
Environment
Directories
Recycle bin
Encryption
SFTP
Shell
Connection
Proxy
Tunnel
SSH
Key exchange
Authentication
Bugs
Note
Bypass authentication entirely
Authentication options
Attempt authentication using Pageant
Attempt 'keyboard-interactive' authentication
Respond with a password to the first prompt
Authentication parameters
Allow agent forwarding
Private key file:
C:\Users\T Manoj\Downloads\RHLLINUX.ppk
Display Public Key
Tools
Certificate to use with the private key:
GSSAPI
Attempt GSSAPI authentication
Allow GSSAPI credential delegation
Color
OK
Cancel
Help


Advanced Site Settings
Environment
Directories
Recycle bin
Encryption
SFTP
Shell
Connection
Proxy
Tunnel
SSH
Key exchange
Authentication
Bugs
Note
Bypass authentication entirely
Authentication options
Attempt authentication using Pageant
Attempt 'keyboard-interactive' authentication
Respond with a password to the first prompt
Authentication parameters
Allow agent forwarding
Private key file:
C:\Users\T Manoj\Downloads\RHLLINUX.ppk
Display Public Key
Tools
Certificate to use with the private key:
GSSAPI
Attempt GSSAPI authentication
Allow GSSAPI credential delegation
Color
OK
Cancel
Help


Login
New Site
Session
File protocol:
SFTP
Host name:
100.26.227.151
Port number:
22
User name:
Password:
Save
Advanced...
Tools
Manage
Login
Close
Help
Show Login dialog on startup and when the last session is closed


Documents – 100.26.227.151 – WinSCP
Local Mark Files Commands Tabs Options Remote Help
Synchronize
Queue
Transfer Settings Default
100.26.227.151
New Tab
My documents
Upload
Edit
Properties
New
C:\Users\T Manoj\Documents\
Name Size Type Changed
Parent directory 06-02-2025 16:18:46
Custom Office Templa... File folder 28-01-2025 10:16:38
GitHub File folder 04-02-2025 12:03:10
WindowsPowerShell File folder 06-02-2025 16:18:46
0 B of 0 B in 0 of 3
5 hidden
ec2-user
Find Files
Download
/home/ec2-user/
Name Size Changed Rights Owner
.. 20-02-2025 13:24:53 rwxr-xr-x root
0 B of 0 B in 0 of 0
5 hidden
SFTP-3
0:00:06






```
       _/m/'
[ec2-user@ip-27-0-50-163 ~]$ ifconfig
enX0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 27.0.50.163  netmask 255.255.255.192  broadcast 27.0.50.191
        inet6 fe80::47c:24ff:fe4e:8bd3  prefixlen 64  scopeid 0x20<link>
        ether 06:7c:24:4e:8b:d3  txqueuelen 1000  (Ethernet)
        RX packets 875  bytes 117059 (114.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1076  bytes 119761 (116.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 1020 (1020.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1020 (1020.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[ec2-user@ip-27-0-50-163 ~]$
```

```
        TX packets 1076  bytes 119761 (116.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 1020 (1020.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1020 (1020.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[ec2-user@ip-27-0-50-163 ~]$ ping google.com
PING google.com (172.253.115.113) 56(84) bytes of data.
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=1 ttl=103 time=2.65 ms
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=2 ttl=103 time=2.23 ms
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=3 ttl=103 time=5.00 ms
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=4 ttl=103 time=2.26 ms
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=5 ttl=103 time=2.26 ms
64 bytes from bg-in-f113.1e100.net (172.253.115.113): icmp_seq=6 ttl=103 time=2.27 ms
```

```
<head>
    <meta charset="UTF-8">
    <title>Home Page</title>
    <style>
        body { text-align: center; font-family: Arial, sans-serif; }
        button { padding: 10px 20px; font-size: 18px; border-radius: 10px; }
    </style>
</head>
<body>
    <h1>Welcome to the Home Page</h1>
    <p>Click the button to go to the Login Page.</p>
    <button onclick="window.location.href='http://27.0.50.163/index.html'">Go to Login</button>
</body>
</html>
[root@ip-27-0-50-24 ~]# ls
index.html
[root@ip-27-0-50-24 ~]# mv index.html /var/www/html
[root@ip-27-0-50-24 ~]# cd /var/www/html
[root@ip-27-0-50-24 html]# ls
index.html
[root@ip-27-0-50-24 html]#
```

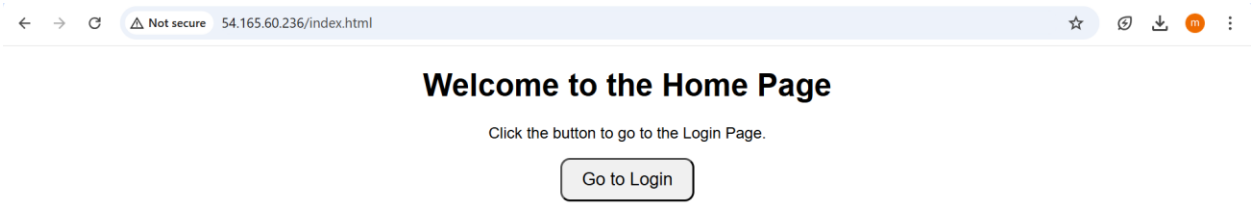
i-046162d54a6a240a3 (Homepages)

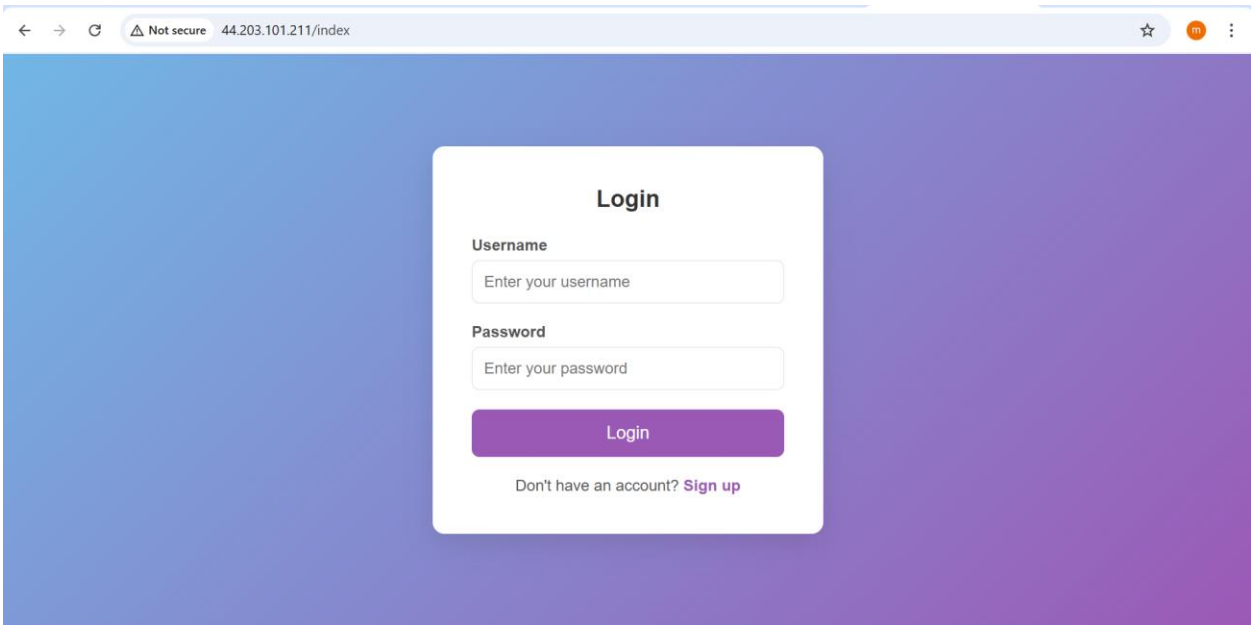
PublicIPs: 54.165.60.236 PrivateIPs: 27.0.50.24


```
        .action-btn:hover {
            background-color: #8e44ad;
        }

        @media (max-width: 480px) {
            .container {
                padding: 30px 20px;
            }
        }
    </style>
</head>
<body>
    <div class="container">
        <h2>Access Private IP Page</h2>
        <a href="http://44.203.101.211/index" class="action-btn">Go to Private Page</a>
    </div>
</body>
</html>
[root@ip-27-0-50-137 html]# systemctl restart httpd
[root@ip-27-0-50-137 html]#
```

Step 13: Final Testing

- Open browser: http://<Public-Instance-Public-IP>
- Click Login button. It should load the login page from the private instance via reverse proxy.





Advantages

The primary advantage of this setup lies in its robust security model. By separating resources into public and private subnets, sensitive data and applications in the private subnet remain shielded from direct internet exposure. The use of a NAT Gateway provides controlled outbound internet access for private instances, ensuring updates without compromising security. Implementing a reverse proxy on the public instance enhances accessibility and reduces the attack surface by routing requests securely. Additionally, this architecture ensures scalability, allowing businesses to expand their applications seamlessly while maintaining a secure and efficient network infrastructure.

Conclusion

In conclusion, this VPC setup demonstrates best practices in building a secure, scalable, and highly available AWS environment. By effectively leveraging AWS components such as VPC, subnets, Internet and NAT Gateways, security groups, and EC2 instances, the project achieves a functional web application infrastructure. The reverse proxy configuration ensures that sensitive backend services remain protected while still being accessible when needed. This architecture is ideal for organizations seeking a balanced approach between

accessibility and security in their cloud deployments, making it suitable for web applications, microservices, and database-driven solutions.