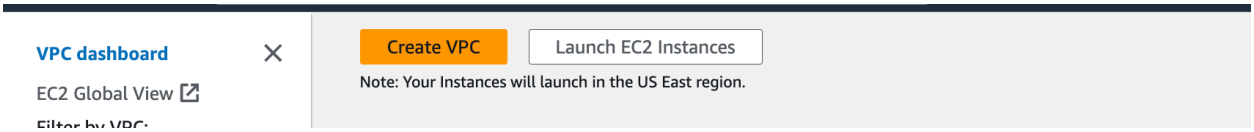
1. VPC Configuration

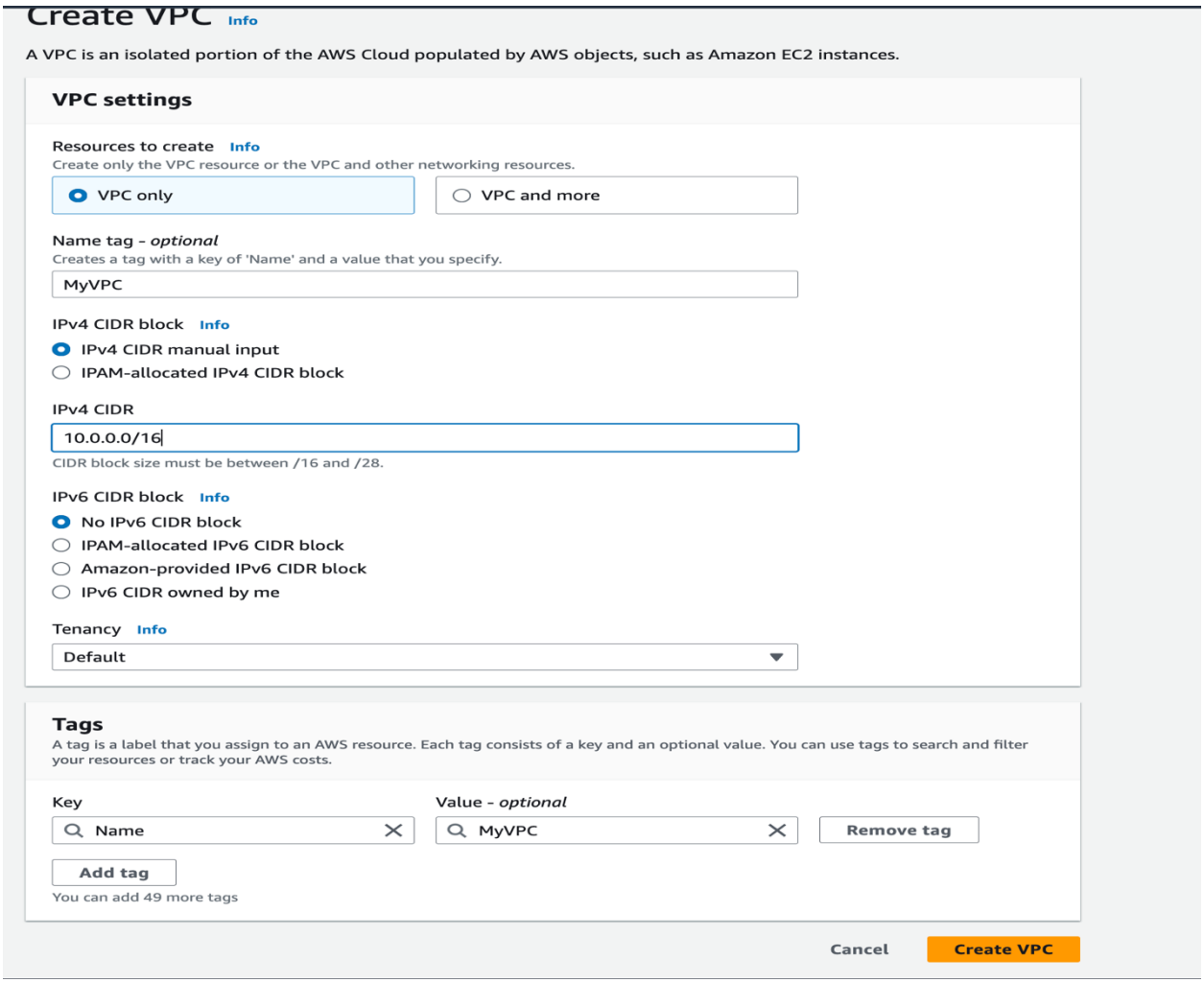
- Objective: To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- Approach: Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance within this VPC to demonstrate how resources are deployed in a custom network environment.
- Goal: By the end of this lab, students should be able to create and configure a VPC, understand subnetting, and the role of route tables and internet gateways in AWS.

1.1. Create VPC

Navigate to VPC dashboard and click “Create VPC” button to create a new VPC

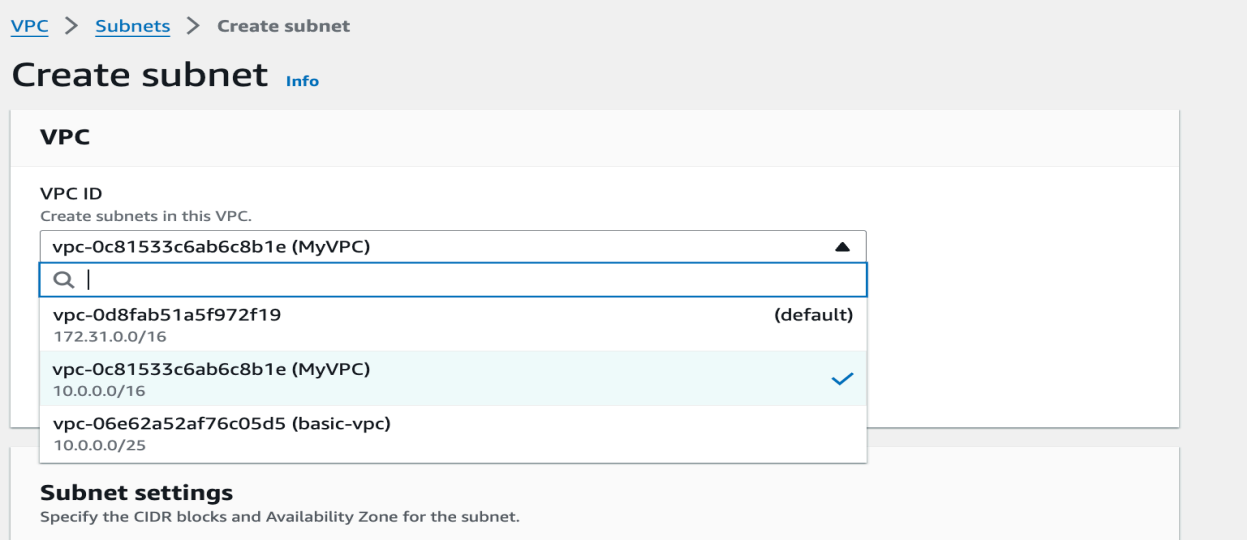


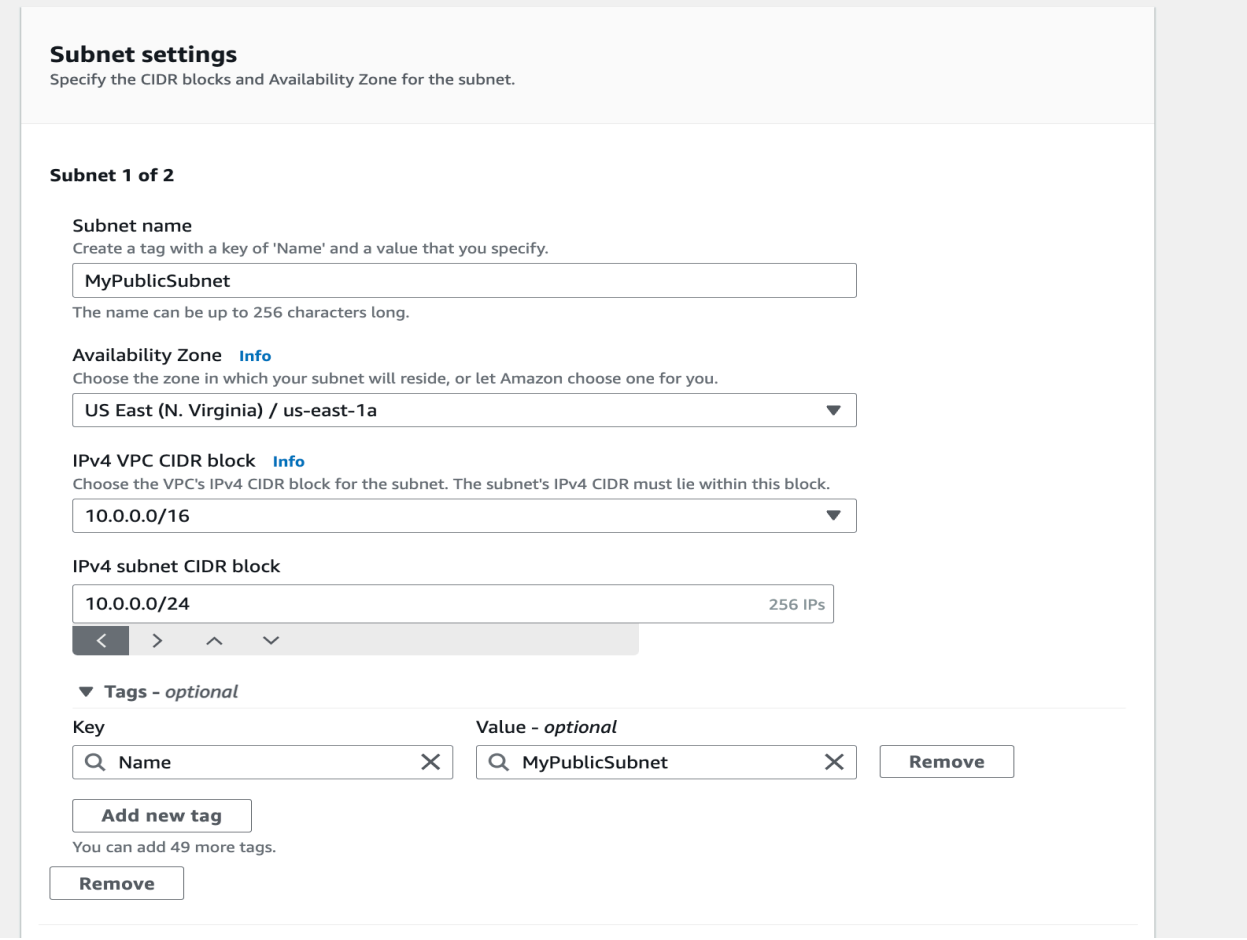
Select VPC only and provide required configuration.

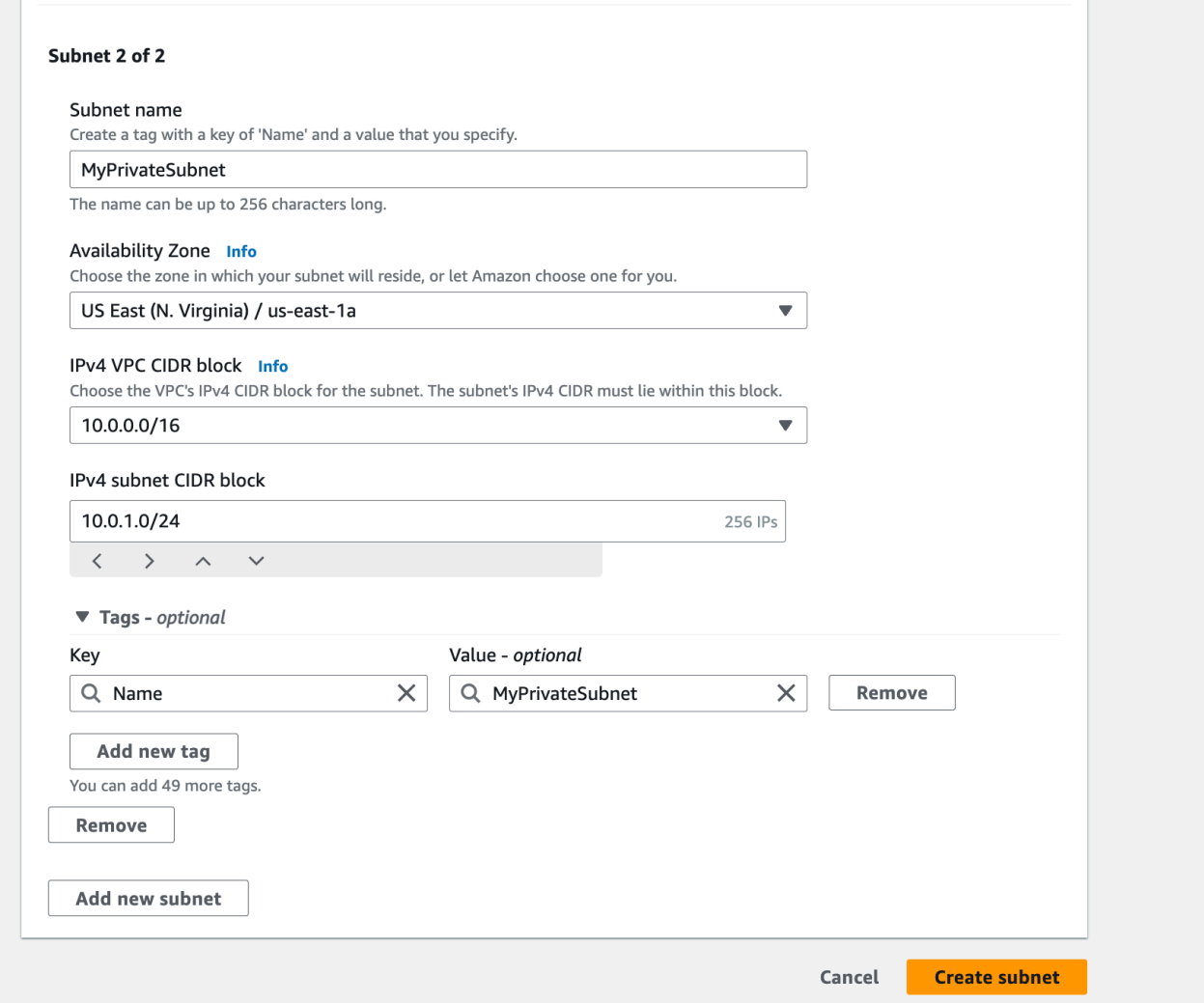


1.2. Create Subnets

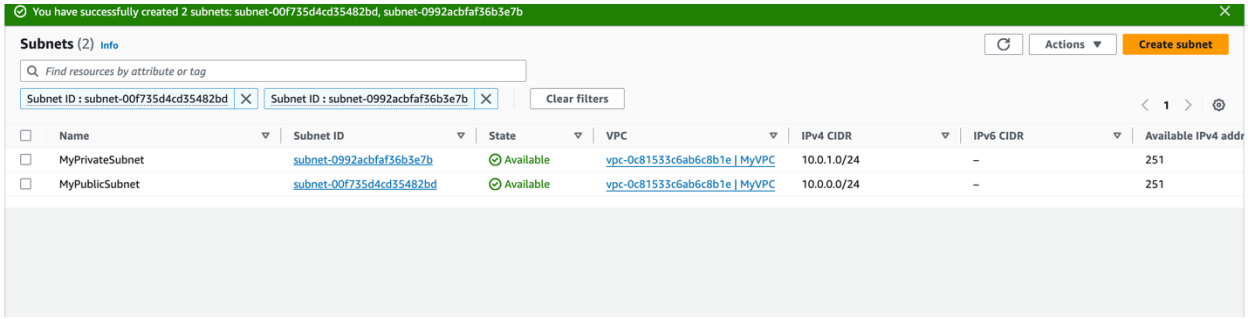
Creating two subnetworks and providing the required configurations





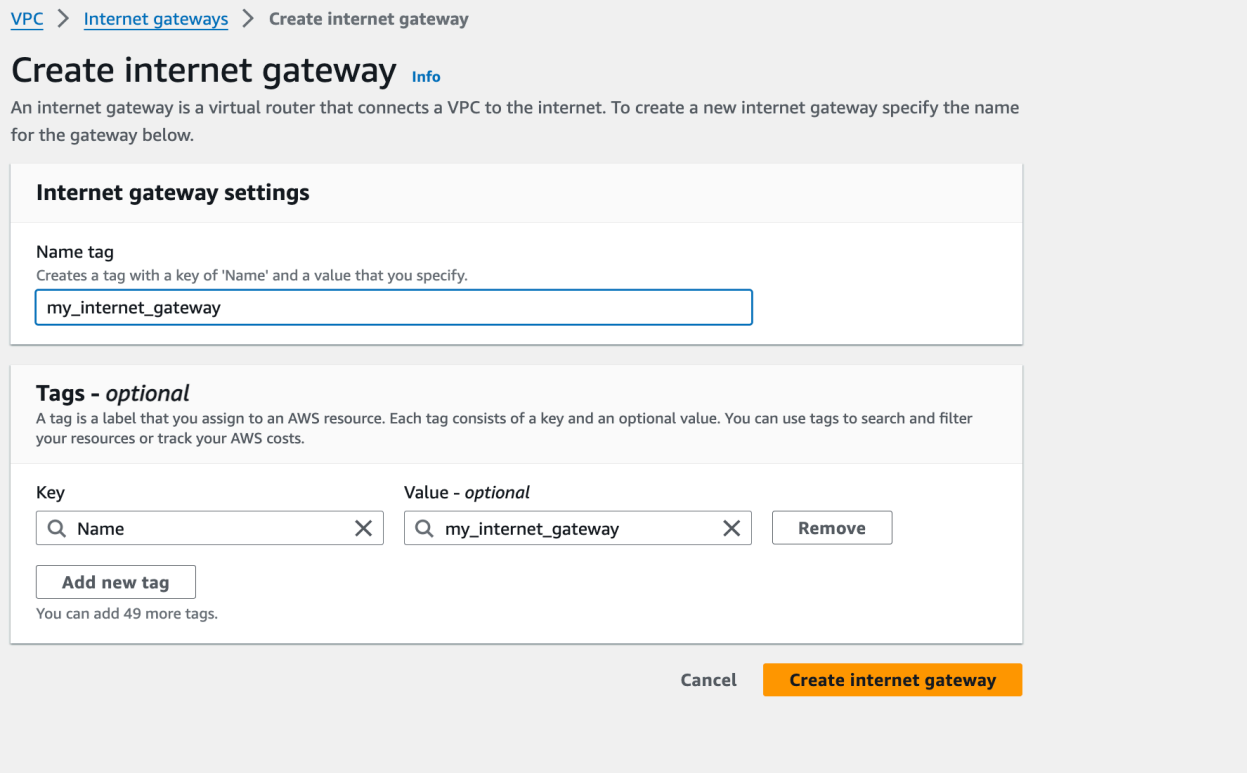


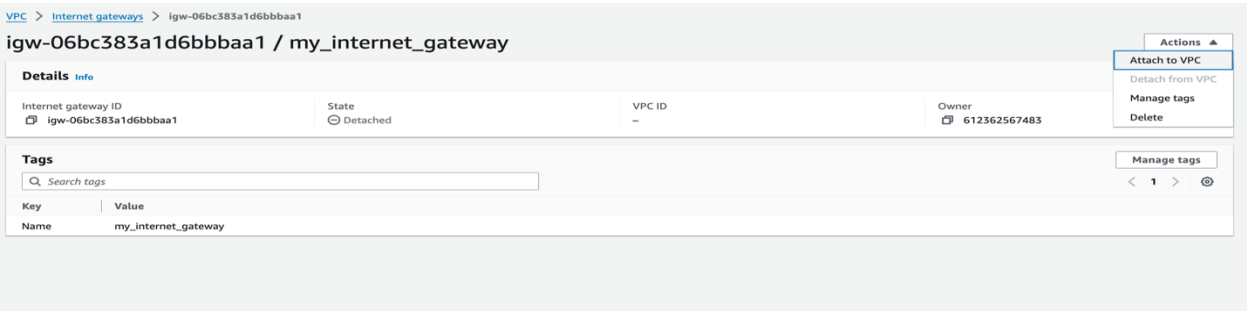
The list of created subnets can be viewed, and their state is Available.

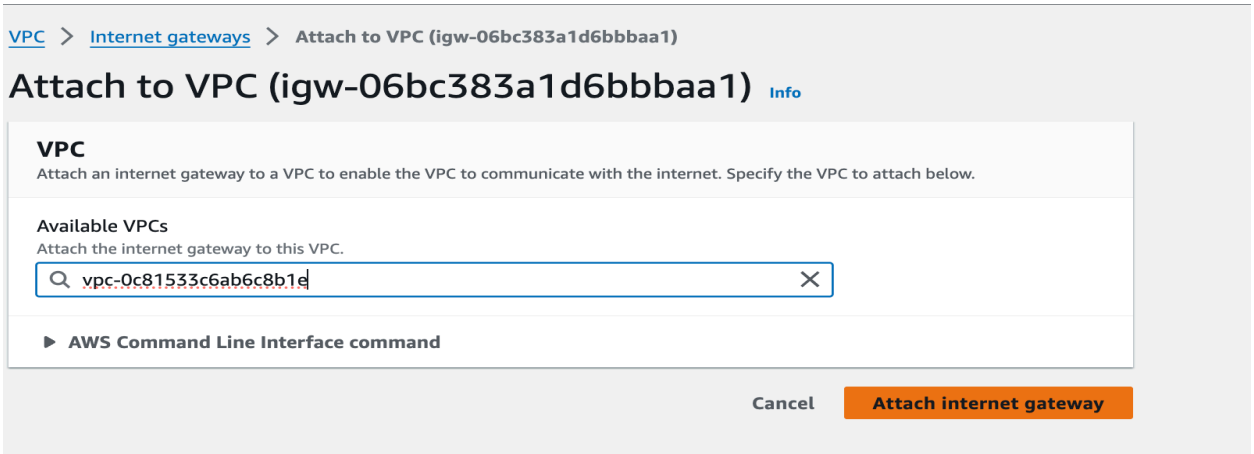


1.3. Create Internet Gateway

Internet gateway is created and attached to the newly created VPC.

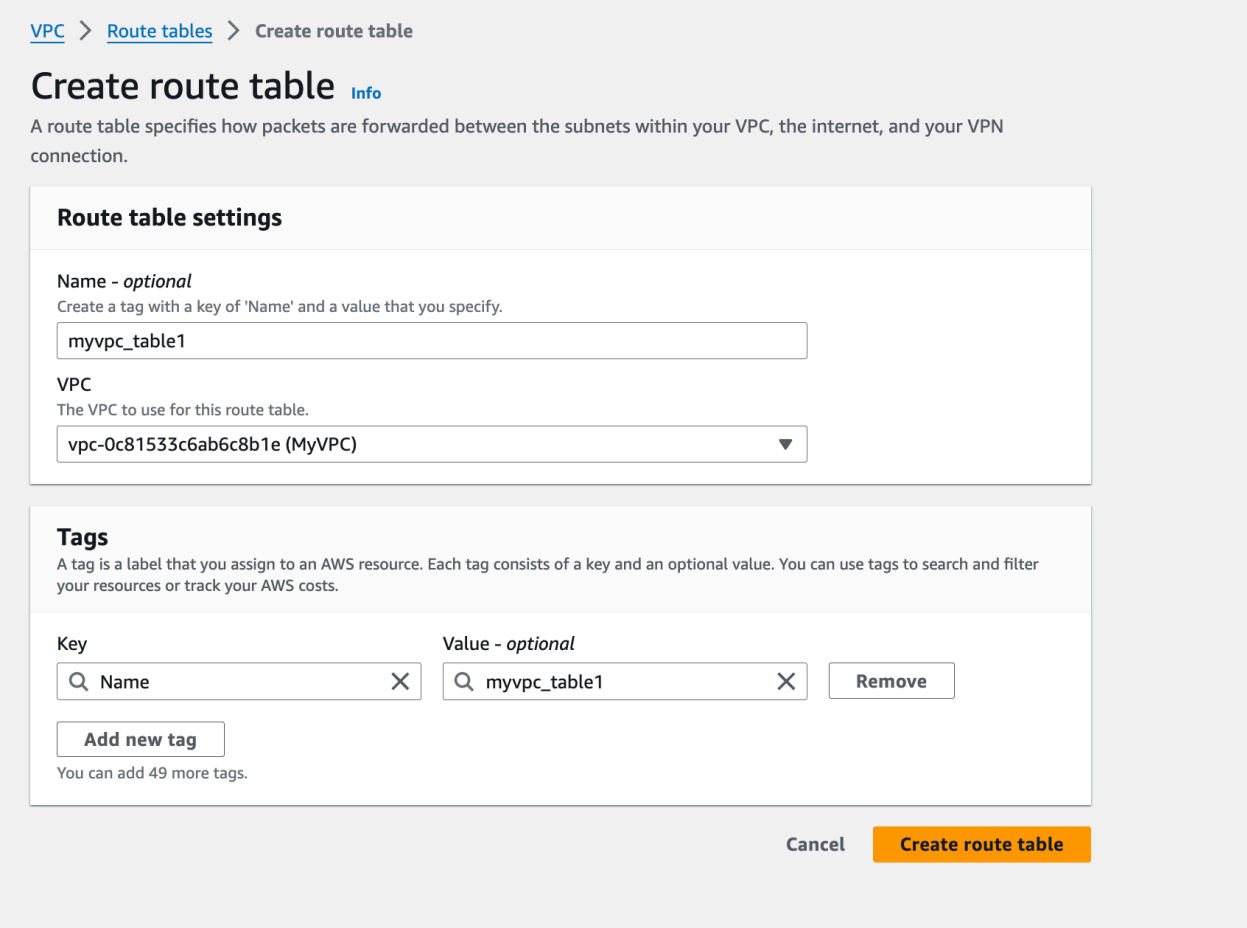


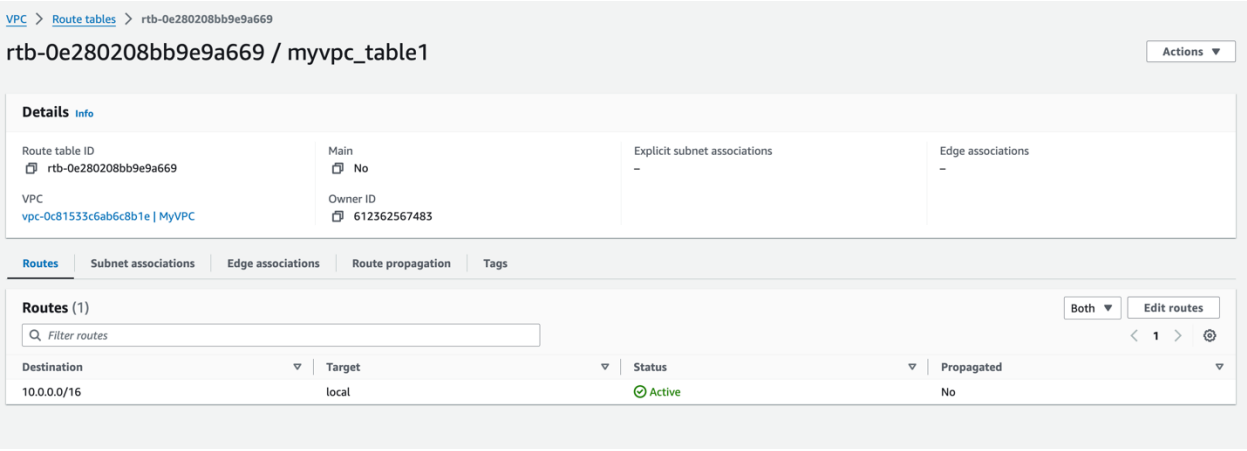




1.4. Create Route Table

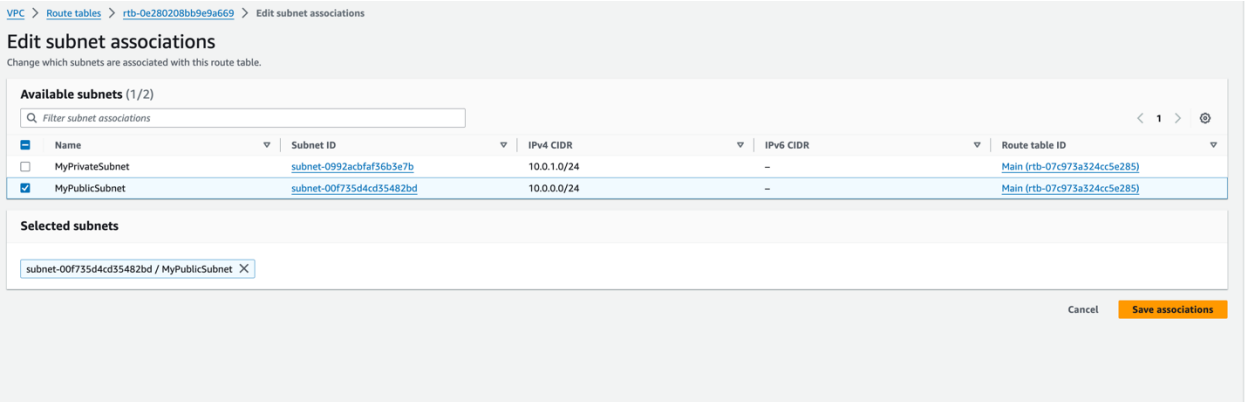
Then the route tables are created. Here, created VPC is selected in configuration.

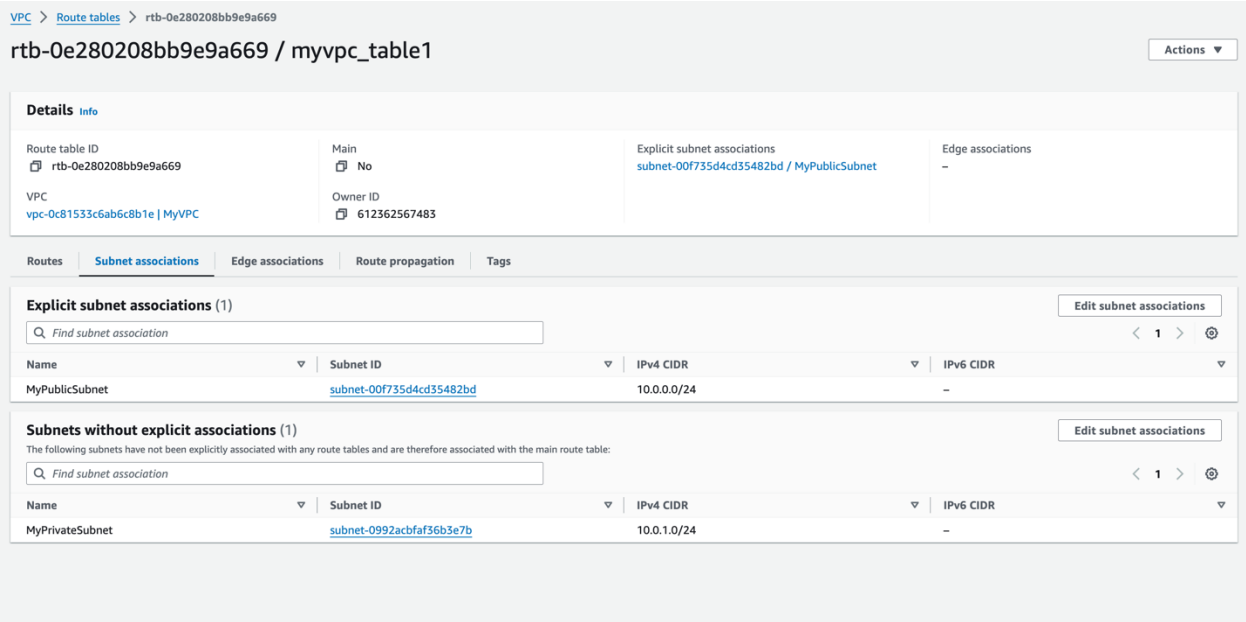




1.5. Subnet Associations

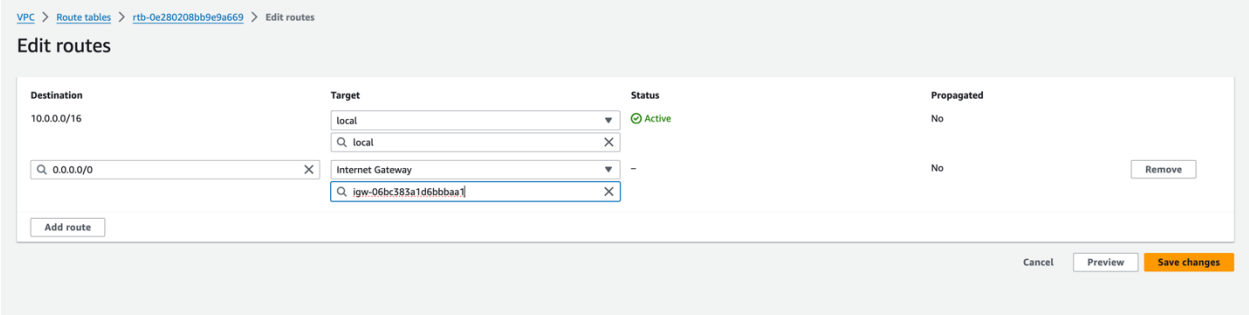
Subnet association of route table is done so that it can be exposed to internet.

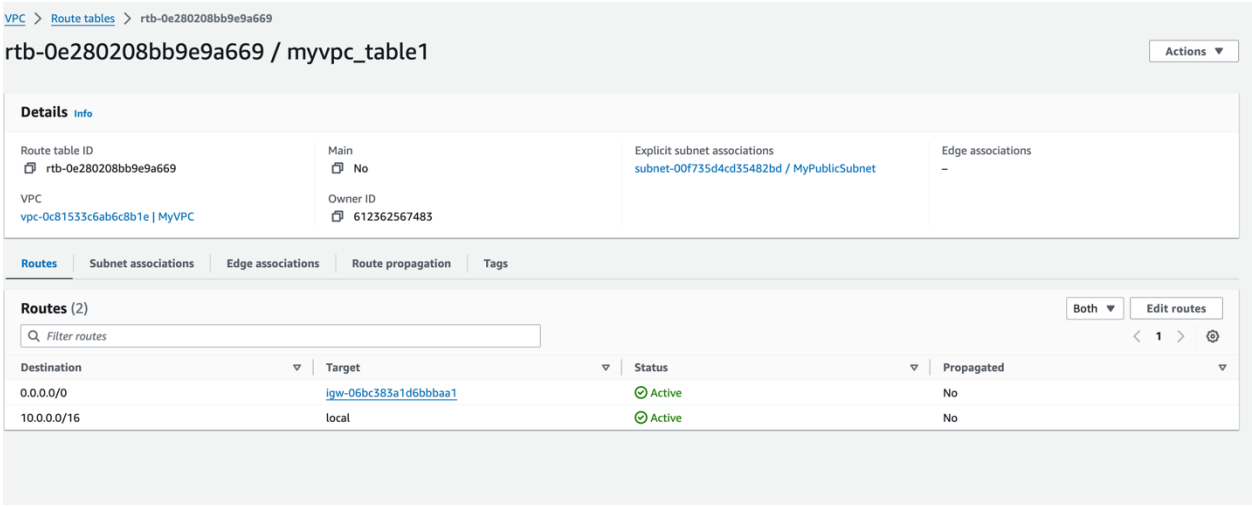




1.6. Edit routes of route table

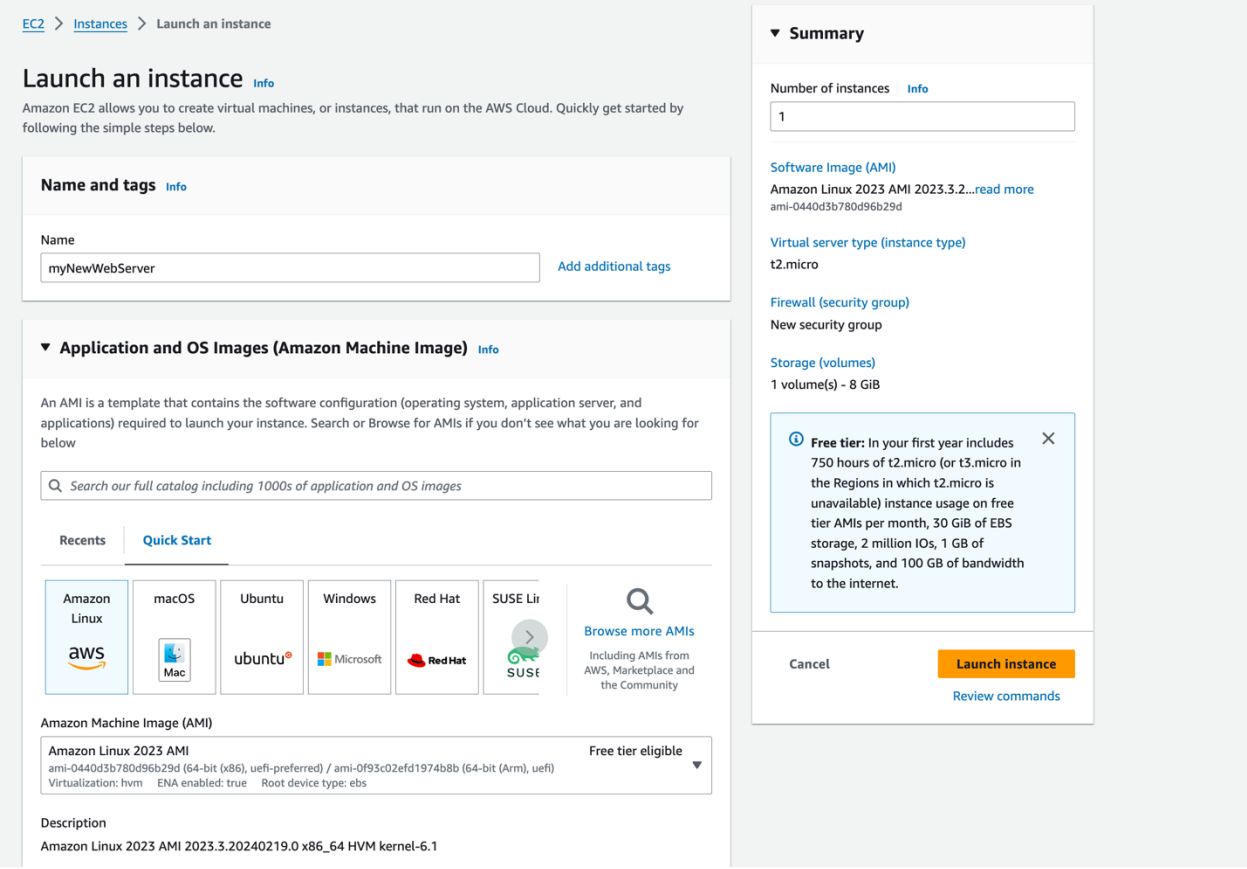
The created route table is edited to associate with internet gateway.



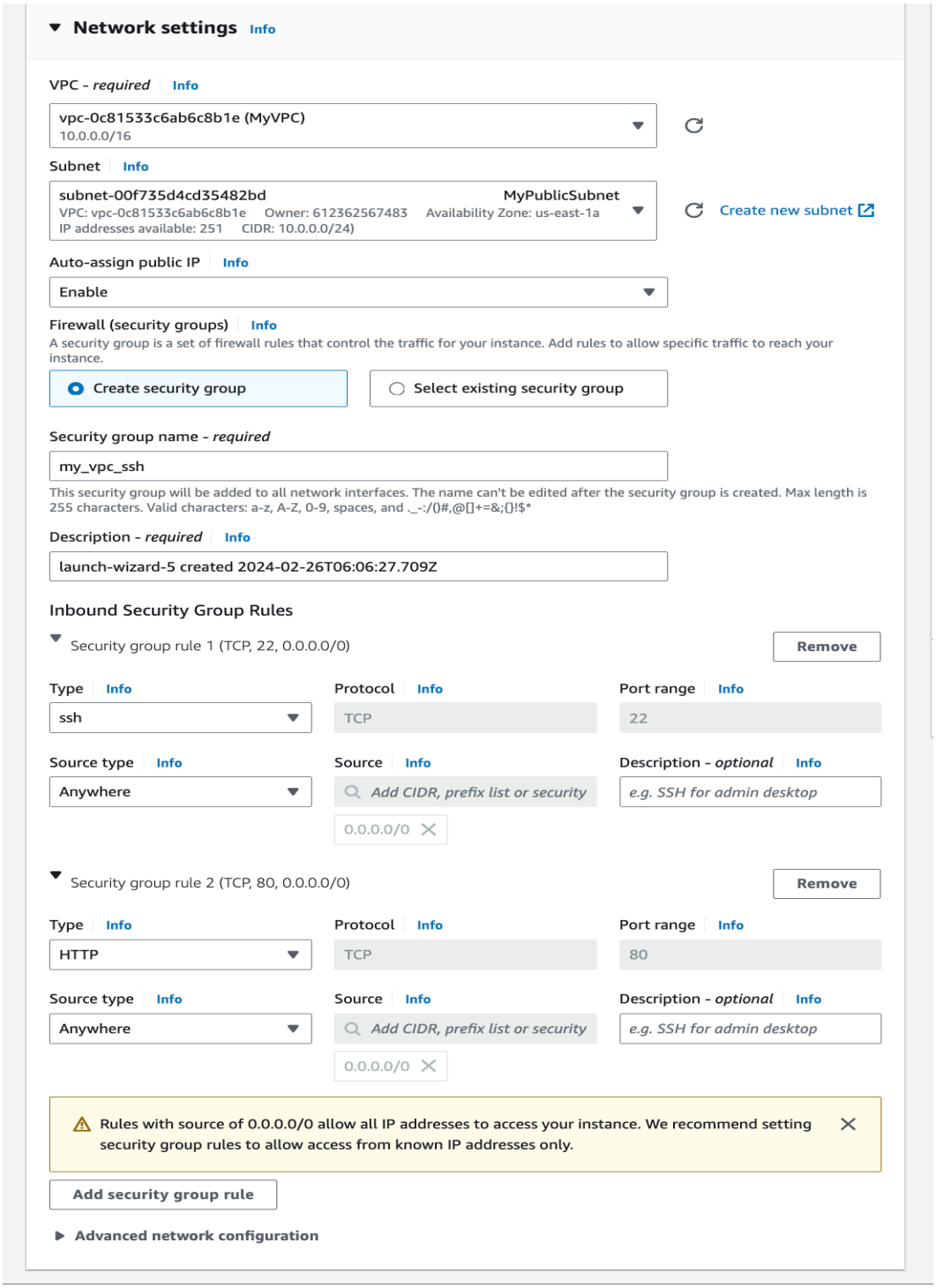


1.7. Testing with Linux EC2 instance

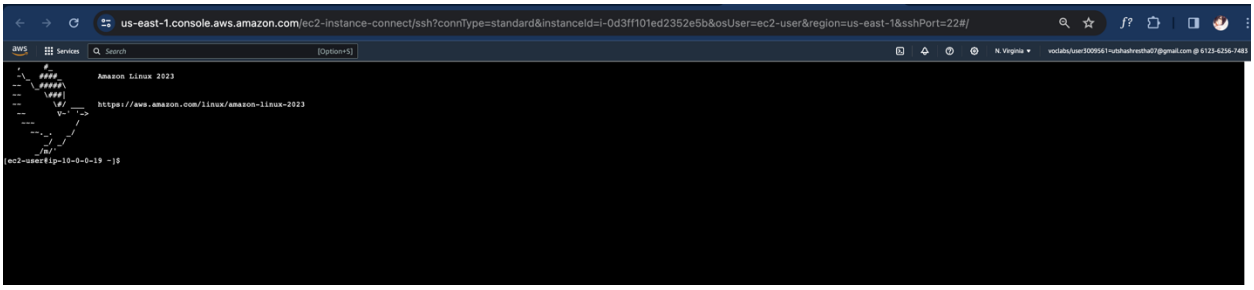
The new EC2 instance is launched to host a static website and configured.

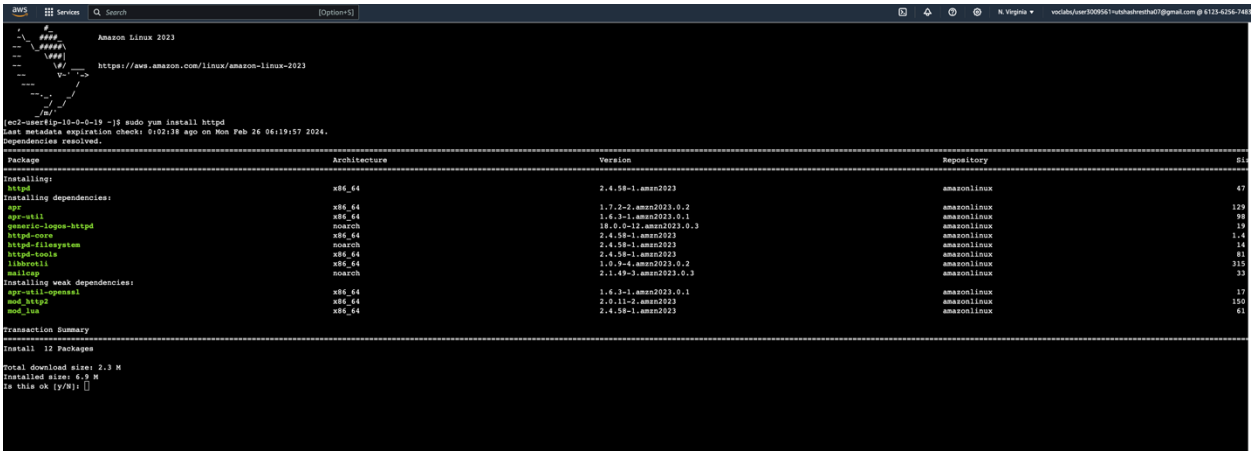


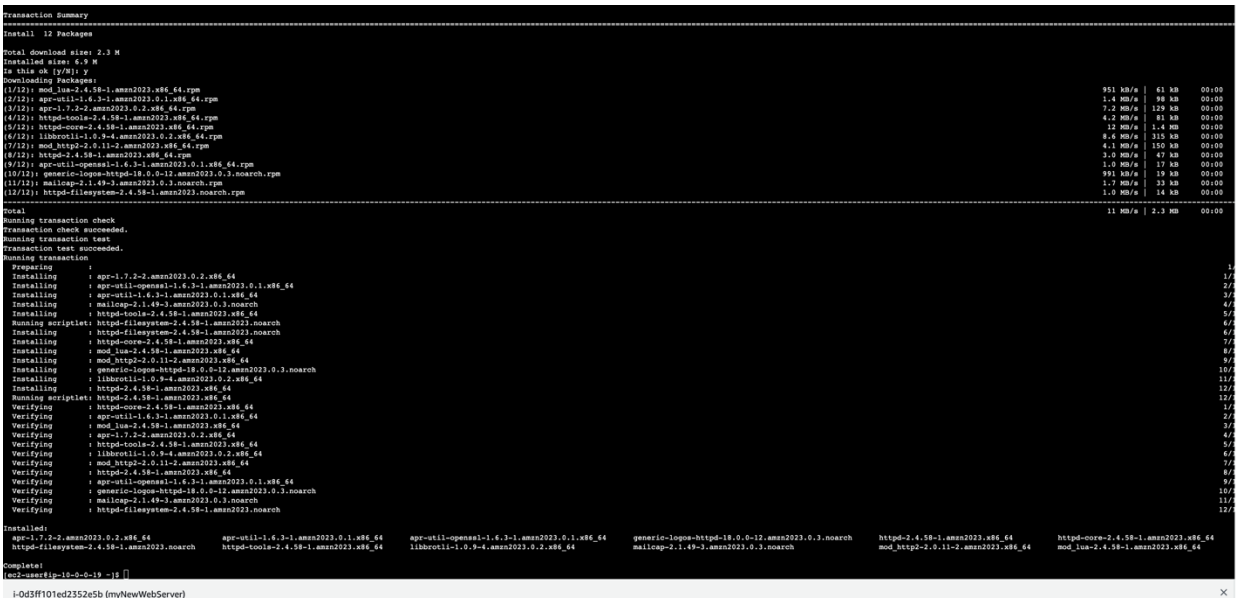
In network setting, it is ensured that the above created VPC and public subnet is chosen. Auto assign public IP is enabled and new security group with http and ssh inbound rule is created.



After launch of EC2 instance, it is connected from browser. The server of EC2 instance is started and tested in the browser with public IP of the EC2 instance. The followed steps can be viewed in below screenshots.





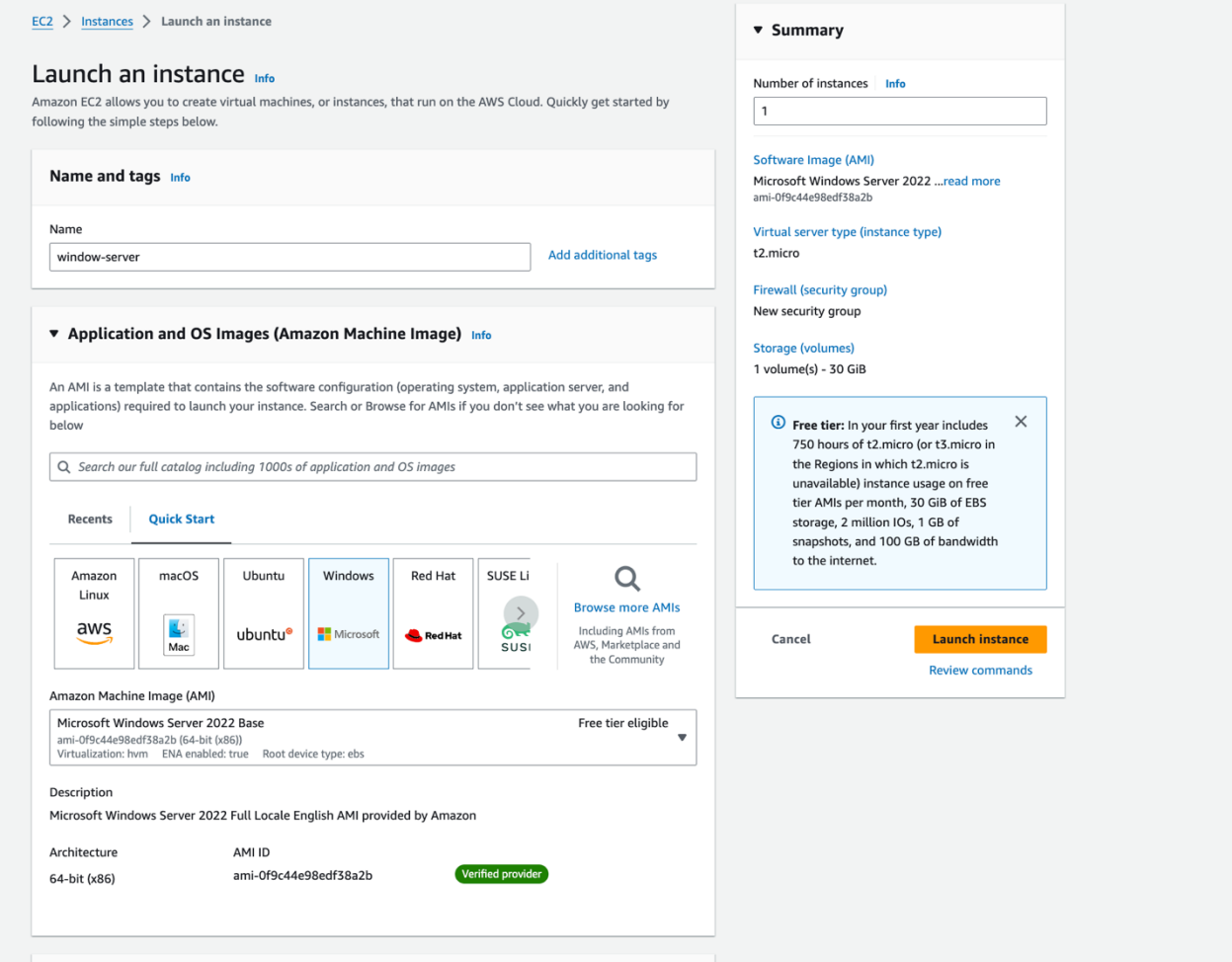

Transaction Summary
Install 12 Packages
Total download size: 2.3 M
Installed size: 6.9 M
Is this ok [y/N]: y
Downloading Packages:
(1/12): mod_lua-2.4.58-1.amzn2023.x86_64.rpm 951 kB/s | 61 kB 00:00
(2/12): apr-util-1.6.3-1.amzn2023.0.1.x86_64.rpm 1.4 MB/s | 98 kB 00:00
(3/12): apr-1.7.2-2.amzn2023.0.2.x86_64.rpm 7.2 MB/s | 129 kB 00:00
(4/12): httpd-tools-2.4.58-1.amzn2023.x86_64.rpm 4.2 MB/s | 81 kB 00:00
(5/12): httpd-core-2.4.58-1.amzn2023.x86_64.rpm 12 MB/s | 1.4 MB 00:00
(6/12): libbrotli-1.0.9-4.amzn2023.0.2.x86_64.rpm 8.6 MB/s | 315 kB 00:00
(7/12): mod_http2-2.0.11-2.amzn2023.x86_64.rpm 4.1 MB/s | 150 kB 00:00
(8/12): httpd-2.4.58-1.amzn2023.x86_64.rpm 3.0 MB/s | 47 kB 00:00
(9/12): apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64.rpm 1.0 MB/s | 17 kB 00:00
(10/12): generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch.rpm 991 kB/s | 19 kB 00:00
(11/12): mailcap-2.1.49-3.amzn2023.0.3.noarch.rpm 1.7 MB/s | 33 kB 00:00
(12/12): httpd-filesystem-2.4.58-1.amzn2023.noarch.rpm 1.0 MB/s | 14 kB 00:00
Total 11 MB/s | 2.3 MB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
Installing : apr-1.7.2-2.amzn2023.0.2.x86_64
Installing : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
Installing : apr-util-1.6.3-1.amzn2023.0.1.x86_64
Installing : mailcap-2.1.49-3.amzn2023.0.3.noarch
Installing : httpd-tools-2.4.58-1.amzn2023.x86_64
Running scriptlet: httpd-filesystem-2.4.58-1.amzn2023.noarch
Installing : httpd-filesystem-2.4.58-1.amzn2023.noarch
Installing : httpd-core-2.4.58-1.amzn2023.x86_64
Installing : mod_lua-2.4.58-1.amzn2023.x86_64
Installing : mod_http2-2.0.11-2.amzn2023.x86_64
Installing : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
Installing : libbrotli-1.0.9-4.amzn2023.0.2.x86_64
Installing : httpd-2.4.58-1.amzn2023.x86_64
Running scriptlet: httpd-2.4.58-1.amzn2023.x86_64
Verifying : httpd-core-2.4.58-1.amzn2023.x86_64
Verifying : apr-util-1.6.3-1.amzn2023.0.1.x86_64
Verifying : mod_lua-2.4.58-1.amzn2023.x86_64
Verifying : apr-1.7.2-2.amzn2023.0.2.x86_64
Verifying : httpd-tools-2.4.58-1.amzn2023.x86_64
Verifying : libbrotli-1.0.9-4.amzn2023.0.2.x86_64
Verifying : mod_http2-2.0.11-2.amzn2023.x86_64
Verifying : httpd-2.4.58-1.amzn2023.x86_64
Verifying : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
Verifying : mailcap-2.1.49-3.amzn2023.0.3.noarch
Verifying : httpd-filesystem-2.4.58-1.amzn2023.noarch
Installed:
apr-1.7.2-2.amzn2023.0.2.x86_64 apr-util-1.6.3-1.amzn2023.0.1.x86_64 apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch httpd-2.4.58-1.amzn2023.x86_64 httpd-core-2.4.58-1.amzn2023.x86_64
httpd-filesystem-2.4.58-1.amzn2023.noarch httpd-tools-2.4.58-1.amzn2023.x86_64 libbrotli-1.0.9-4.amzn2023.0.2.x86_64 mailcap-2.1.49-3.amzn2023.0.3.noarch mod_http2-2.0.11-2.amzn2023.x86_64 mod_lua-2.4.58-1.amzn2023.x86_64
Complete!
[ec2-user@ip-10-0-0-19 ~]$
i-0d3ff101ed2352e5b (myNewWebServer)

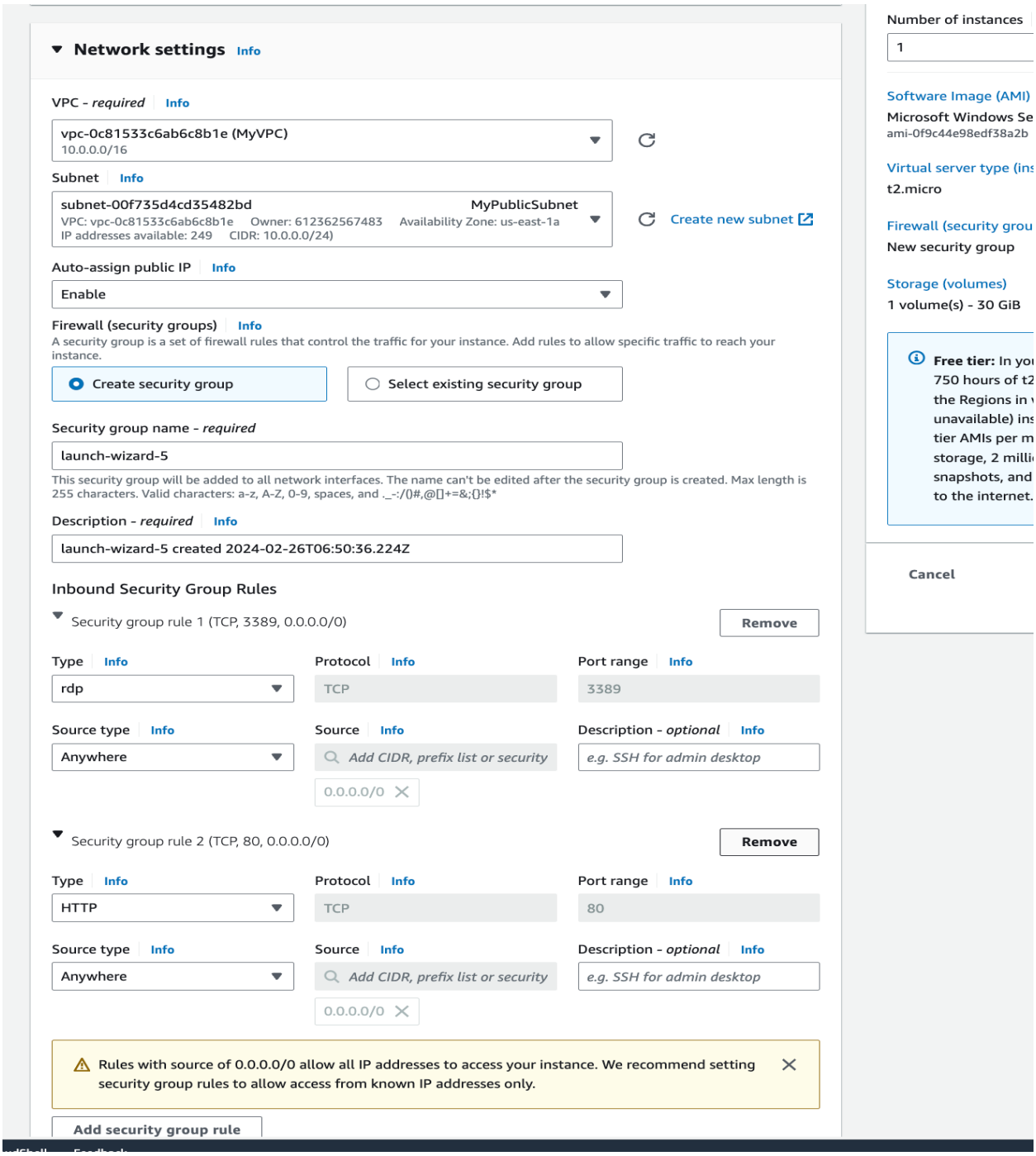

54.80.26.208
Not Secure
54.80.26.208

It works!

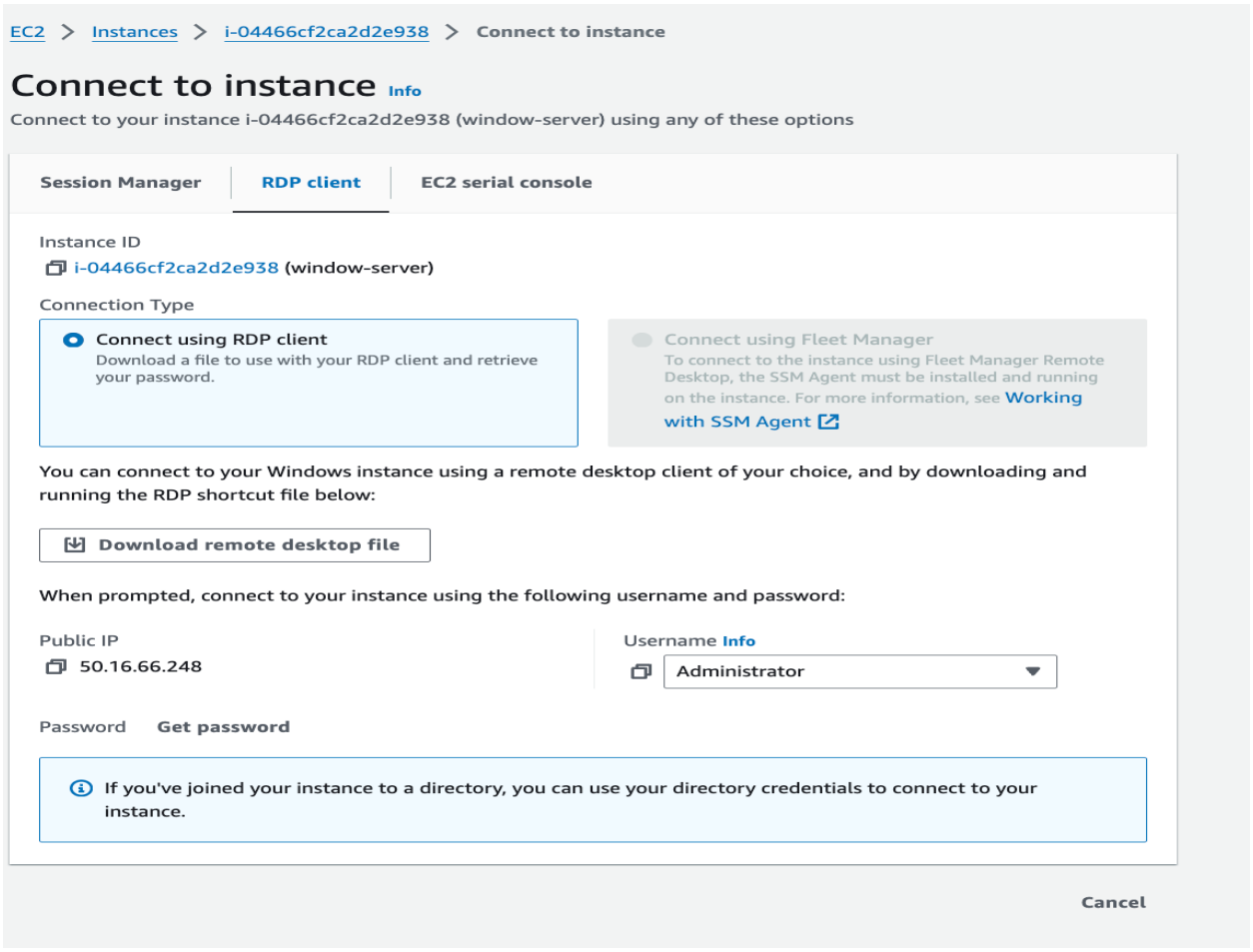
1.8. Testing with windows EC2 instance

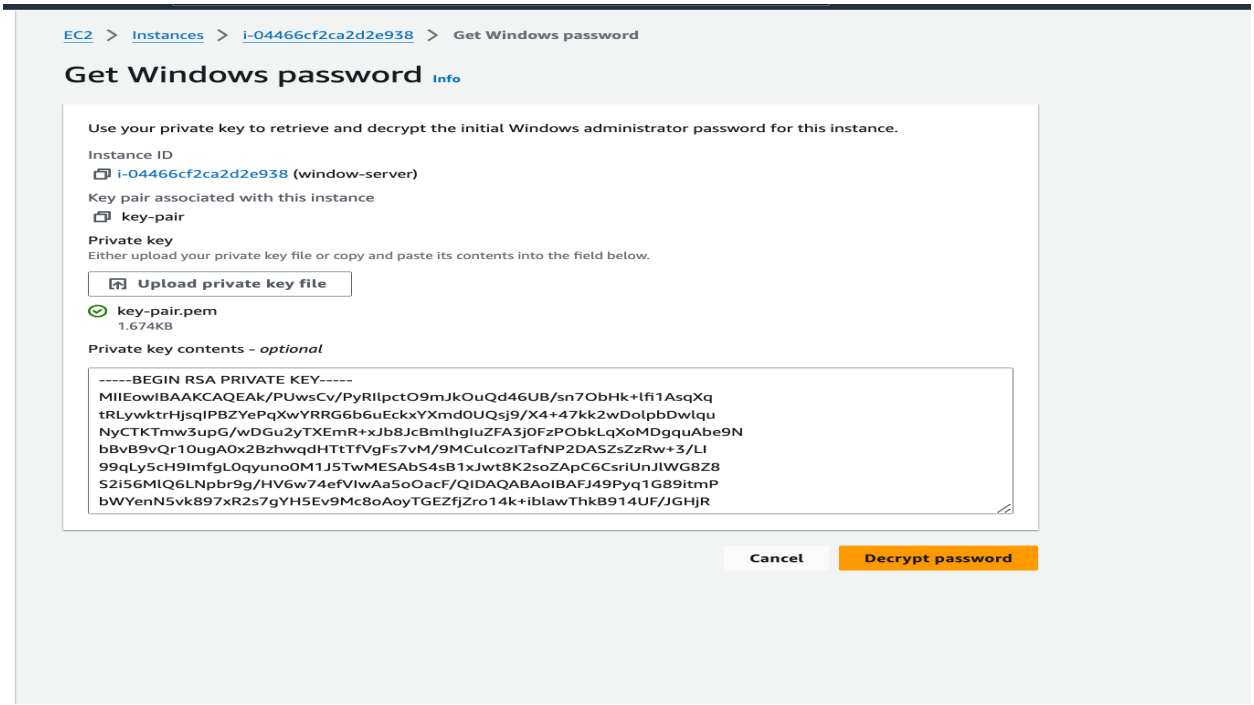
In this, same setup is made as mentioned in Linux EC2 instance. In network setting rdp and http inbound rules are given.

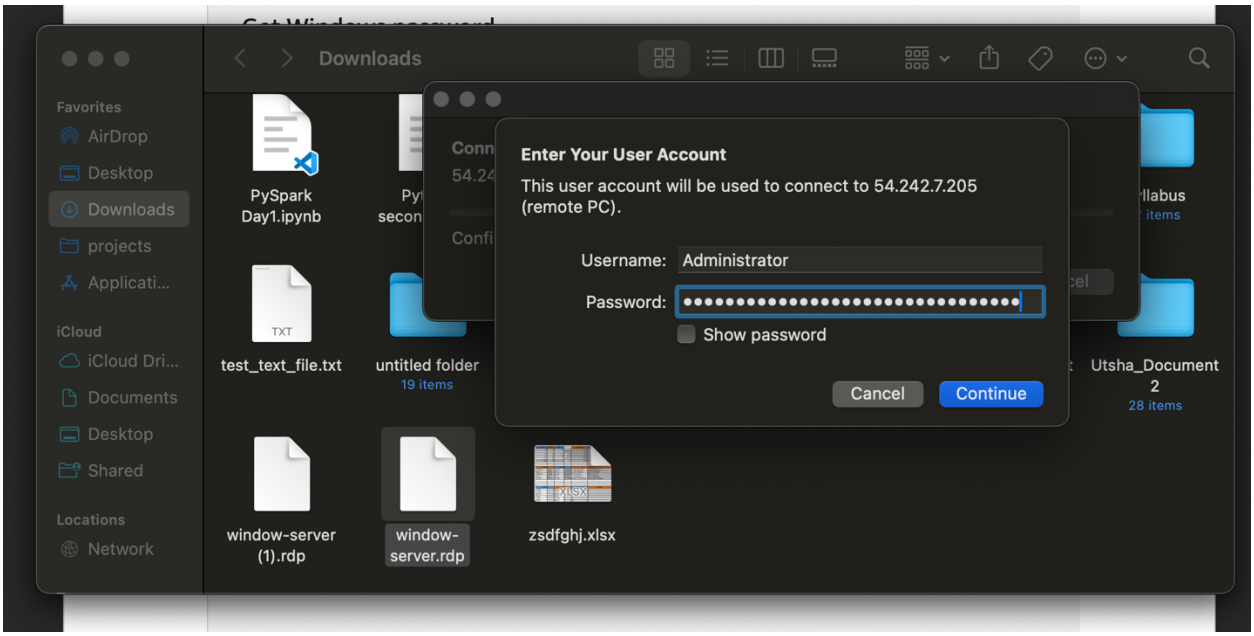


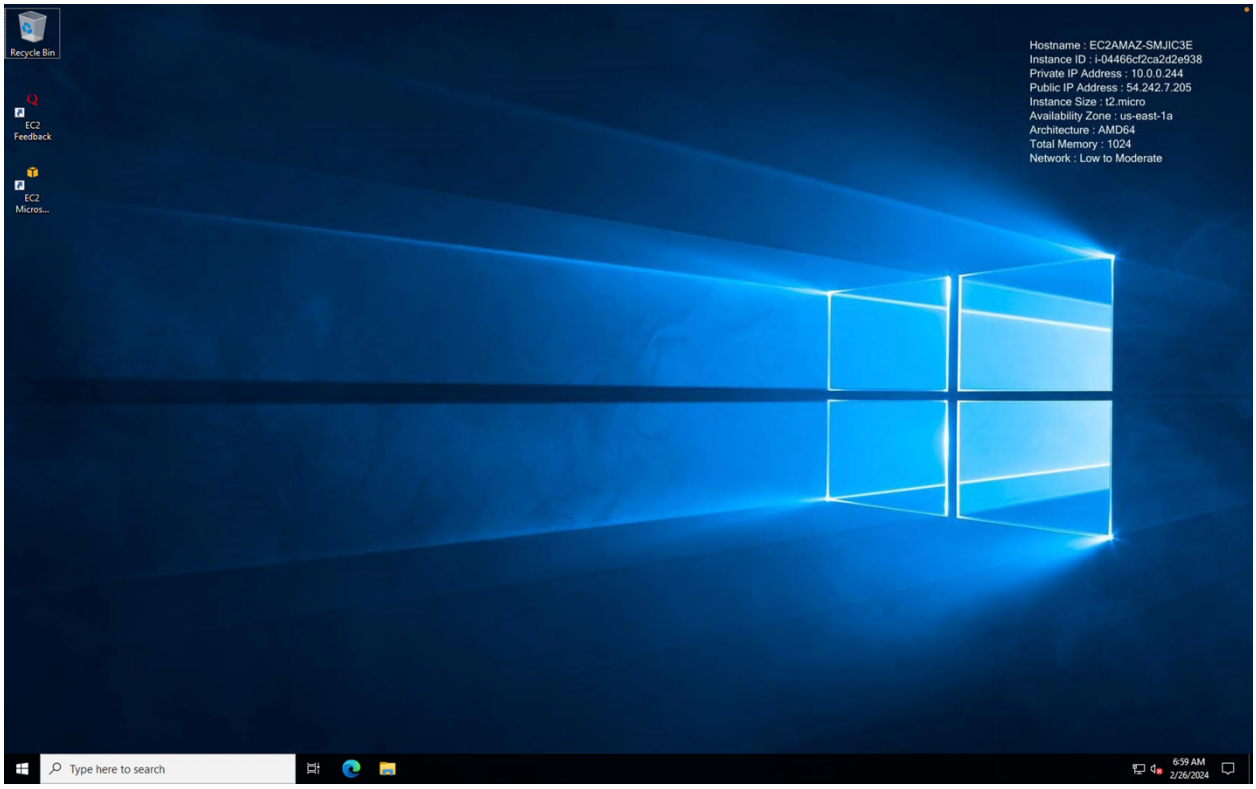


After launching the windows EC2 instance, the EC2 instance is connected from RDP client. The rdp file is downloaded and opened locally using the generated password.


EC2 > Instances > i-04466cf2ca2d2e938 > Connect to instance
Connect to instance Info
Connect to your instance i-04466cf2ca2d2e938 (window-server) using any of these options
Session Manager
RDP client
EC2 serial console
Instance ID
i-04466cf2ca2d2e938 (window-server)
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
50.16.66.248
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


EC2 > Instances > i-04466cf2ca2d2e938 > Get Windows password
Get Windows password Info
Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.
Instance ID
i-04466cf2ca2d2e938 (window-server)
Key pair associated with this instance
key-pair
Private key
Either upload your private key file or copy and paste its contents into the field below.
Upload private key file
key-pair.pem
1.674KB
Private key contents - optional
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAk/PUwsCv/PyRIlpctO9mJkOuQd46UB/sn7ObHk+lfi1AsqXq
tRLywktrHjsqIPBZYePqXwYRRG6b6uEckxYXmd0UQsj9/X4+47kk2wDolpbDwlqu
NyCTKTmw3upG/wDGu2yTXEmR+xJb8JcBmlhgluZFA3j0FzPObkLqXoMDgquAbe9N
bBvB9vQr10ugA0x2BzhwqdHTtTfVgFs7vM/9MCulcozITafNP2DASZsZzRw+3/LI
99qLy5cH9ImfgL0qyuno0M1J5TwMESAbS4sB1xJwt8K2soZApC6CsriUnJlWG8Z8
S2i56MlQ6LNpbr9g/HV6w74efVIwAa5oOacF/QIDAQABAoIBAFJ49Pyq1G89itmP
bWYenN5vk897xR2s7gYH5Ev9Mc8oAoyTGEZfjZro14k+iblawThkB914UF/JGHjR
Cancel
Decrypt password


Downloads
Favorites
AirDrop
Desktop
Downloads
projects
Applicati...
iCloud
iCloud Dri...
Documents
Desktop
Shared
Locations
Network
PySpark Day1.ipynb
test_text_file.txt
TXT
untitled folder
19 items
window-server (1).rdp
window-server.rdp
zsdfghj.xlsx
Utsha_Document 2
28 items
Enter Your User Account
This user account will be used to connect to 54.242.7.205 (remote PC).
Username: Administrator
Password:
Show password
Cancel
Continue


Recycle Bin
EC2 Feedback
EC2 Micros...
Hostname : EC2AMAZ-SMJIC3E
Instance ID : i-04466cf2ca2d2e938
Private IP Address : 10.0.0.244
Public IP Address : 54.242.7.205
Instance Size : t2.micro
Availability Zone : us-east-1a
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate
Type here to search
6:59 AM
2/26/2024

1.9. Hosting static website in Linux EC2 instance

Uploading the static file in linux .

```
utsha_mac@Utshas-MacBook-Pro Downloads % ssh -i "key-pair.pem" ec2-user@107.23.233.69
The authenticity of host '107.23.233.69 (107.23.233.69)' can't be established.
ED25519 key fingerprint is SHA256:f+xq7EU6Lg3dNa3IpYlxO2b9PNHVAK4DTZ9+sDWGmxg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '107.23.233.69' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Mar  1 06:27:42 2024 from 18.206.107.29
[ec2-user@ip-10-0-0-19 ~]$ mkdir temp
[ec2-user@ip-10-0-0-19 ~]$ ls
temp
```

Uploading the website files in ec2-instance temp directory

```
utsha_mac@Utshas-MacBook-Pro downloads % scp -i "key-pair.pem" /Users/utsha_mac/projects/techkraft/Bootcamp-Tasks/aws/vpc_revisio
n_lab/static_website/* ec2-user@107.23.233.69:temp/
portfolio.html                                100% 1234     4.1KB/s   00:00
utsha-img.jpg                                 100%  236KB 128.0KB/s   00:01
```

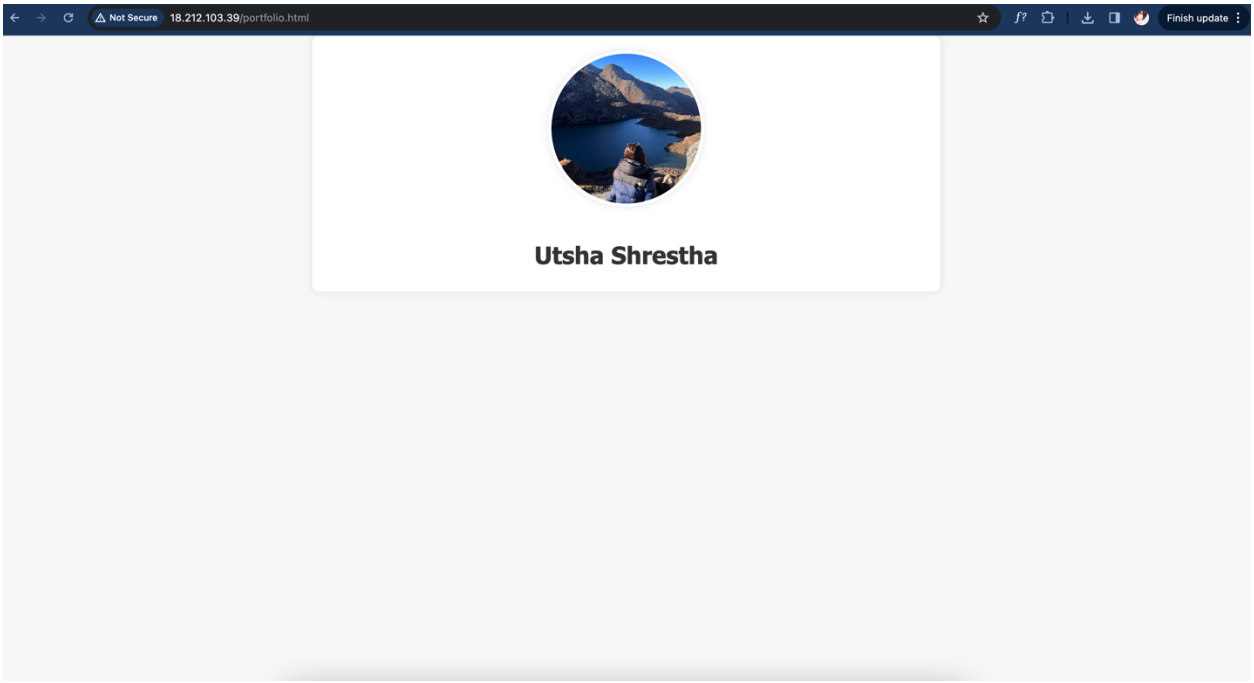
```
[ec2-user@ip-10-0-0-19 temp]$ ls
portfolio.html  utsha-img.jpg
```

Moving the website html content to html directory and starting the server.

```
utsha_mac@Utshas-MacBook-Pro downloads % ssh -i "key-pair.pem" ec2-user@107.23.233.69
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Mar  1 06:31:16 2024 from 110.44.121.23
[ec2-user@ip-10-0-0-19 ~]$ cd temp/
[ec2-user@ip-10-0-0-19 temp]$ ls
portfolio.html  utsha-img.jpg
[ec2-user@ip-10-0-0-19 temp]$ sudo mv * /var/www/html/
[ec2-user@ip-10-0-0-19 temp]$ cd /var/www/html/
[ec2-user@ip-10-0-0-19 html]$ ls
portfolio.html  utsha-img.jpg
[ec2-user@ip-10-0-0-19 html]$
```

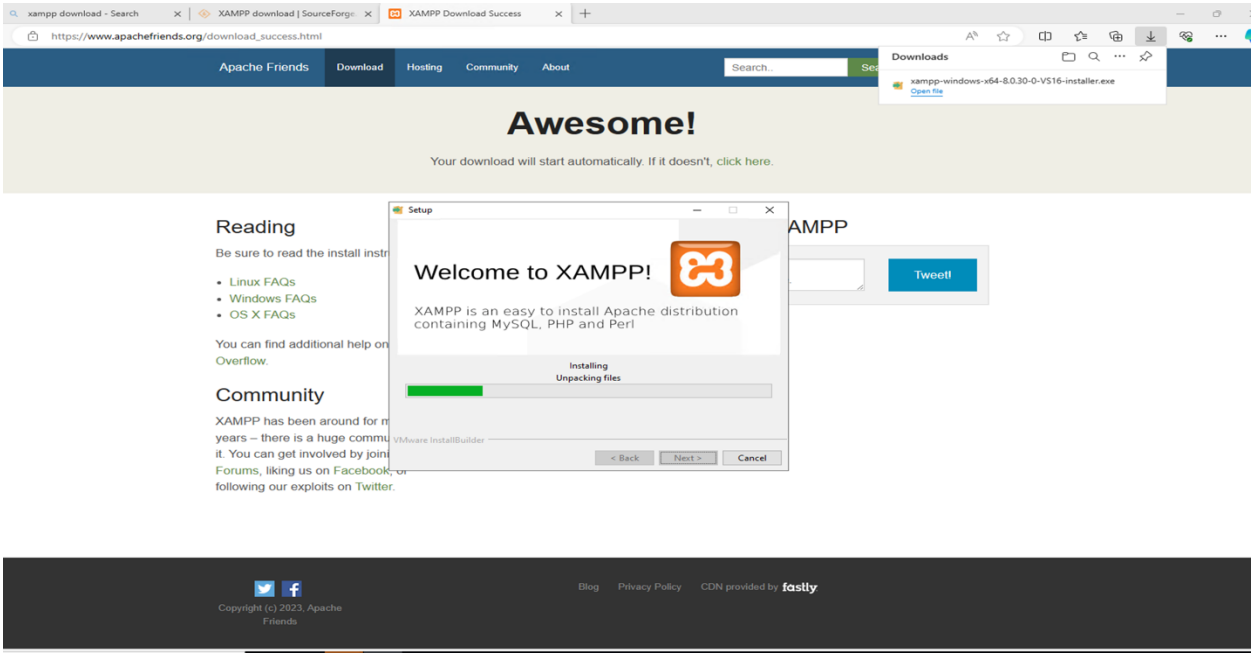
```
[ec2-user@ip-10-0-0-19 html]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
```

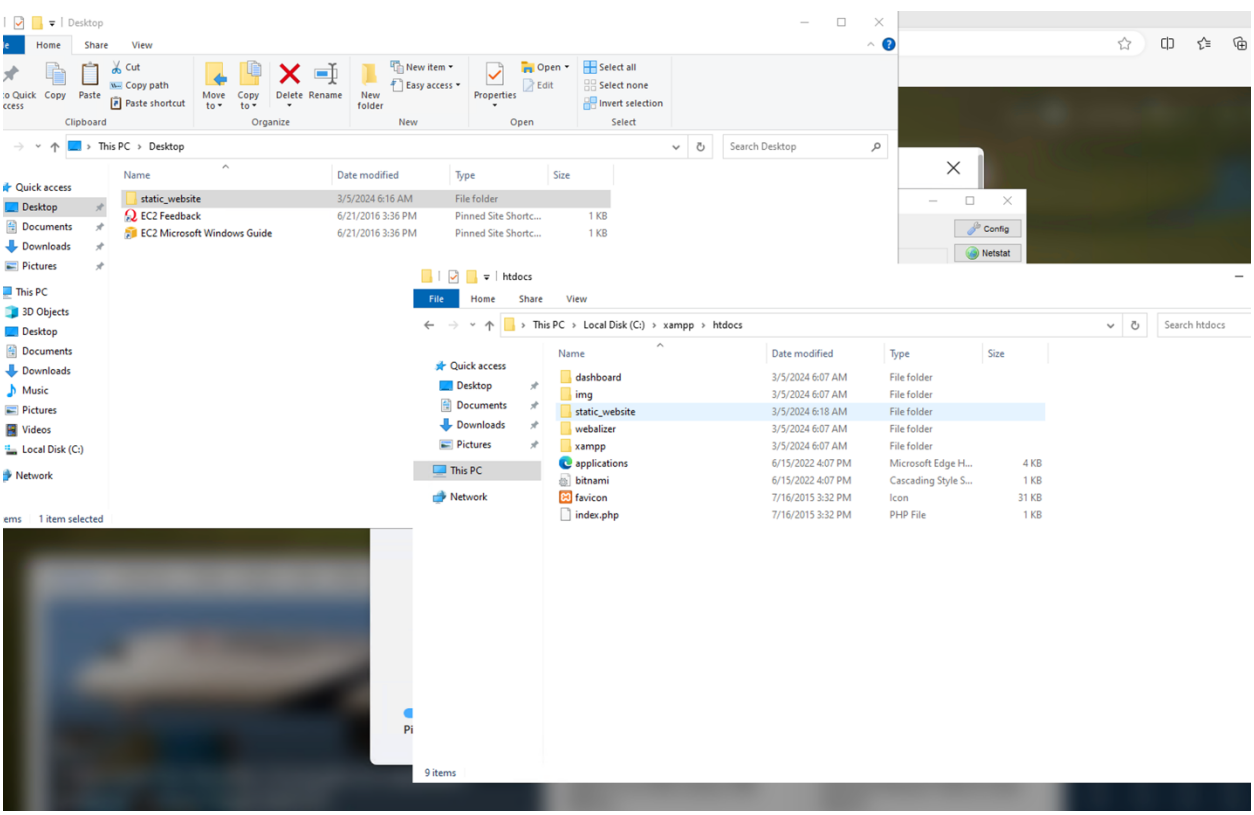
Then, the static website is hosted successfully, and it can be tested using public IP address.



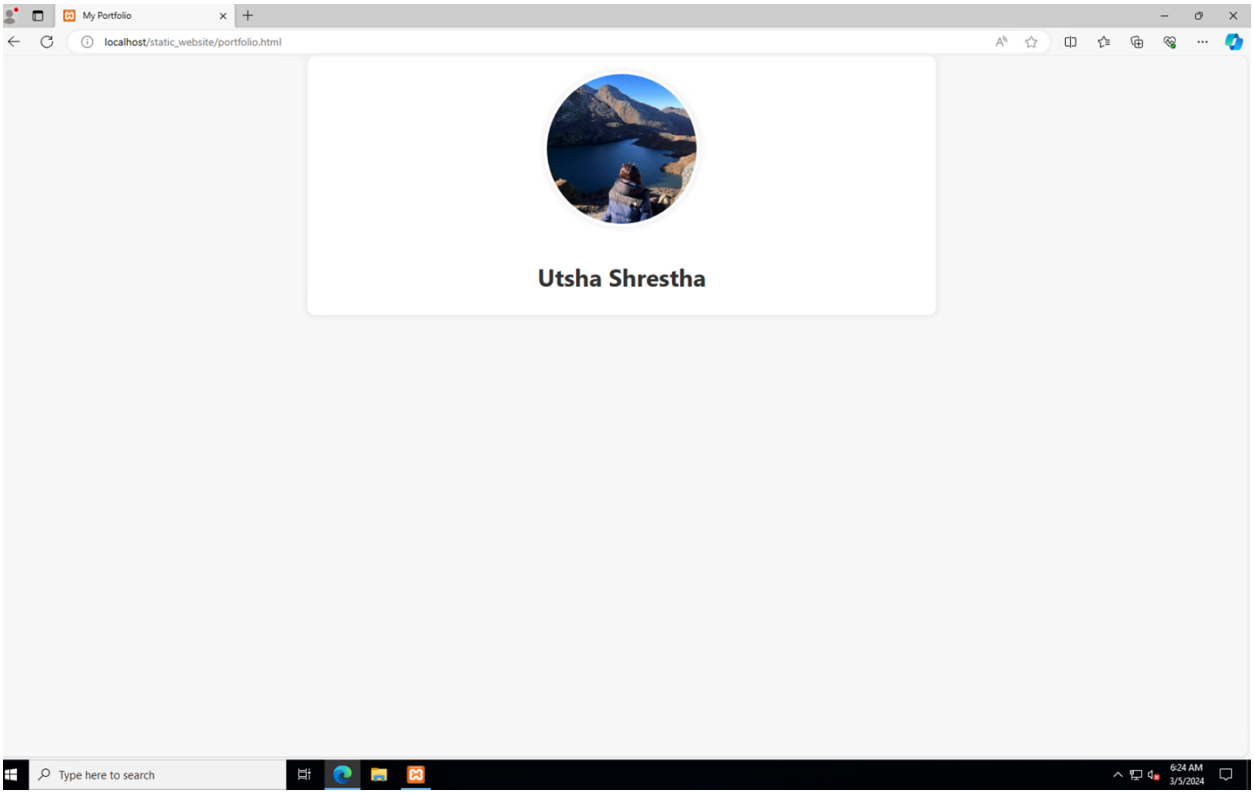
1.10. Hosting static website in Windows EC2 instance

The downloaded rdp file of Windows EC2 instance is opened. There XAMPP is installed and the static website folder is moved to the htdocs directory of XAMPP.

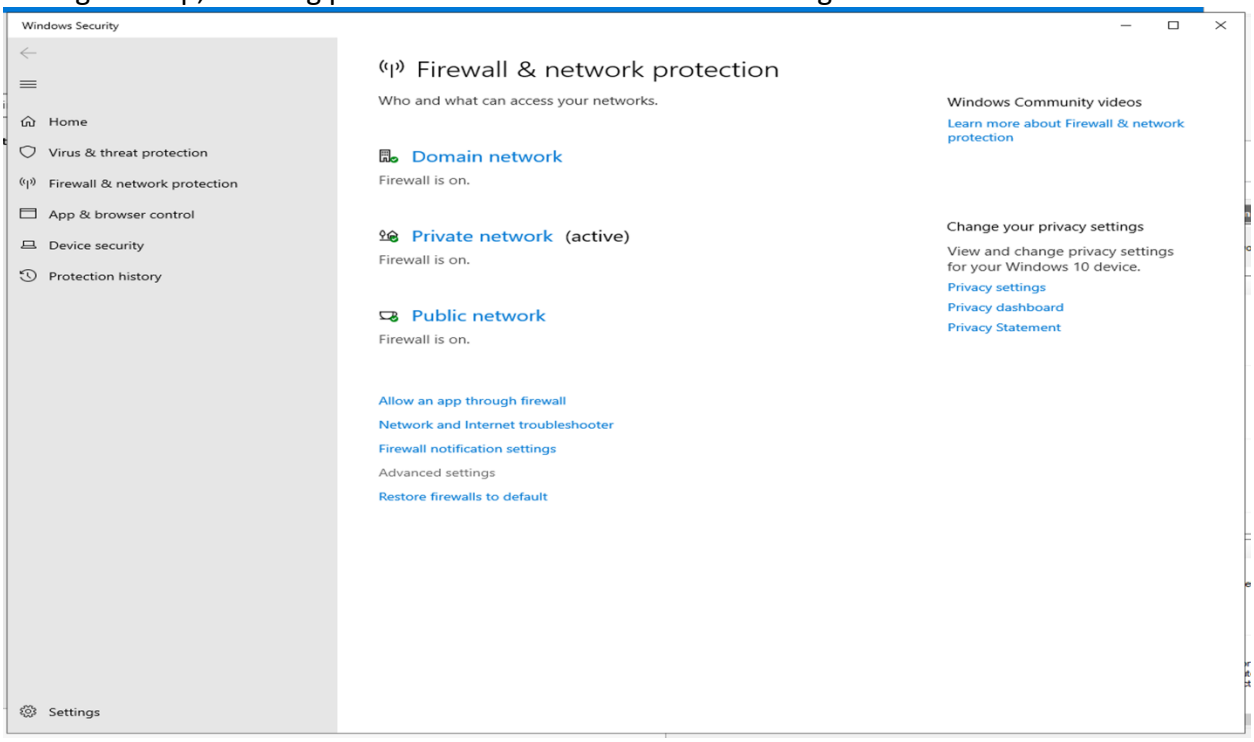


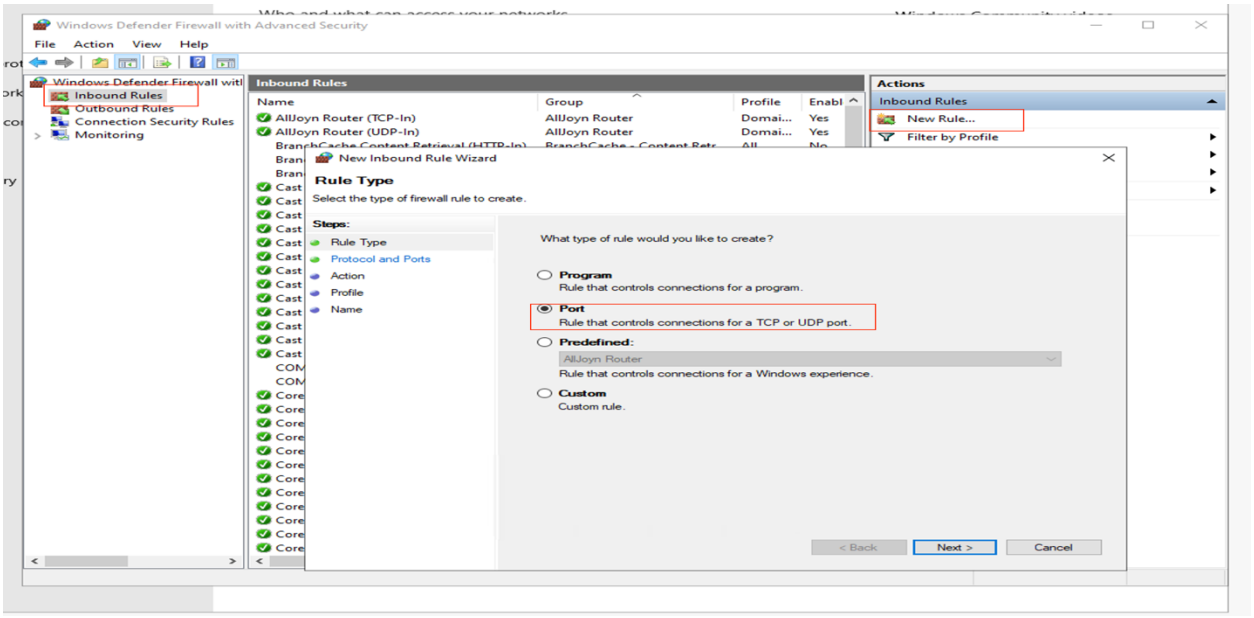


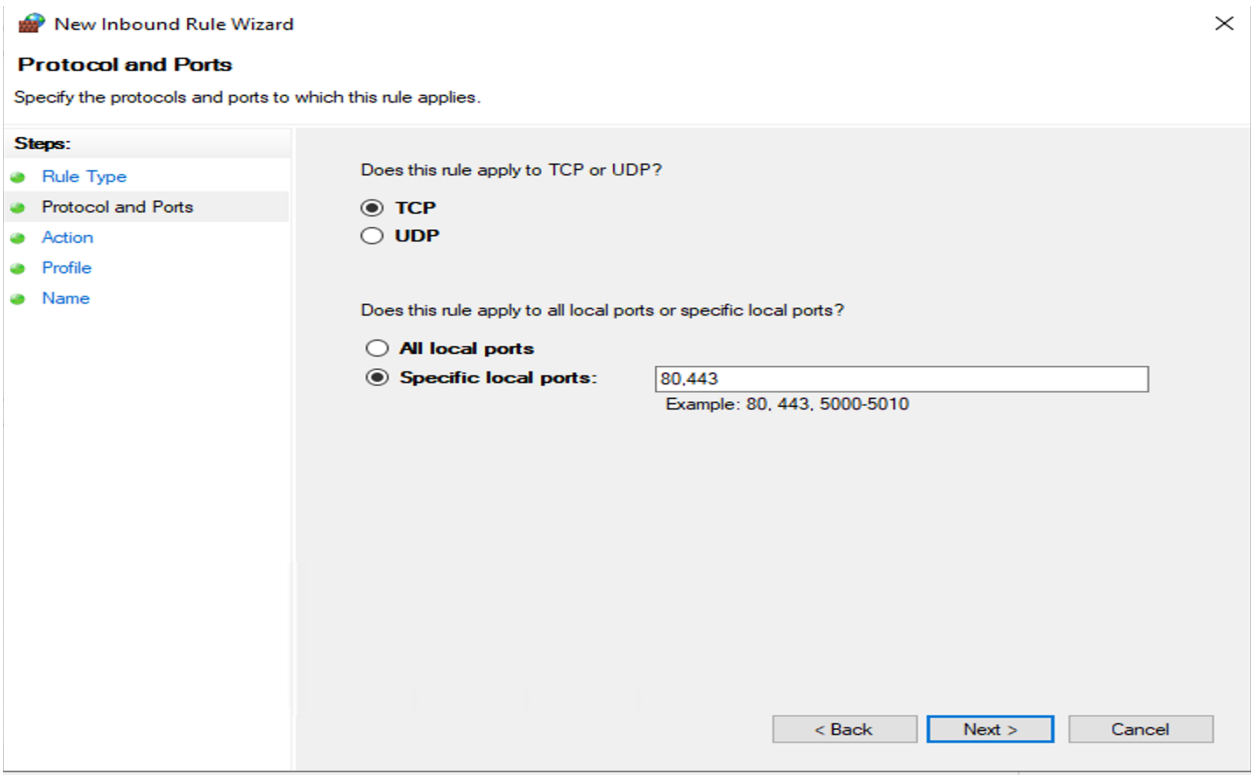
After that, the moved html content, working status is checked in windows remote desktop

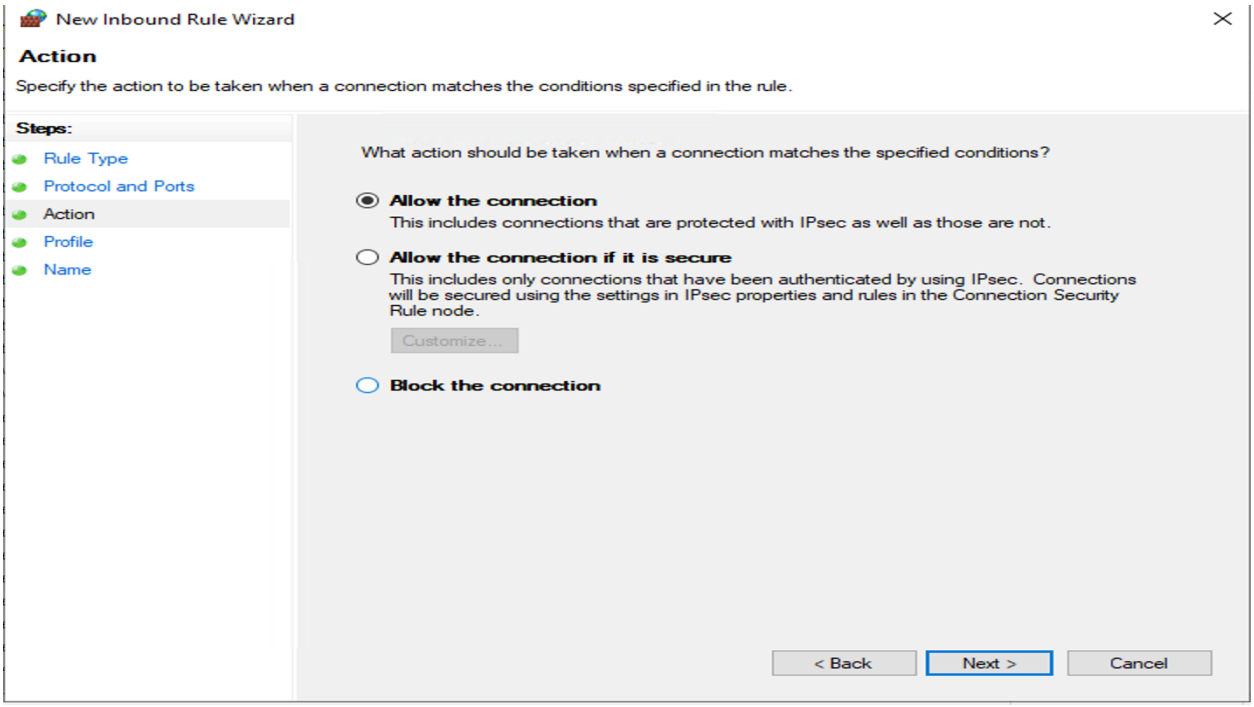


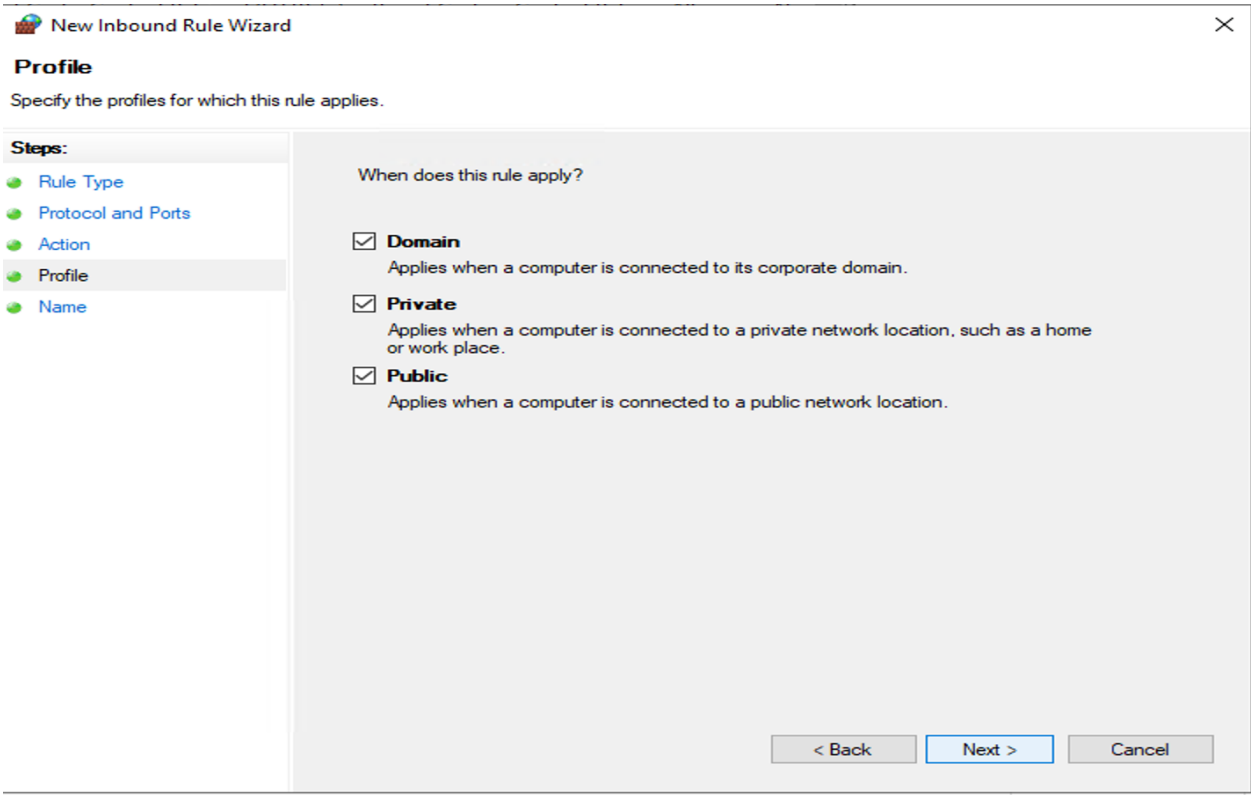
Now for checking, whether the static website is hosted in Windows EC2 instance, the firewall setting is setup, allowing port 80 and 443 from advanced setting.

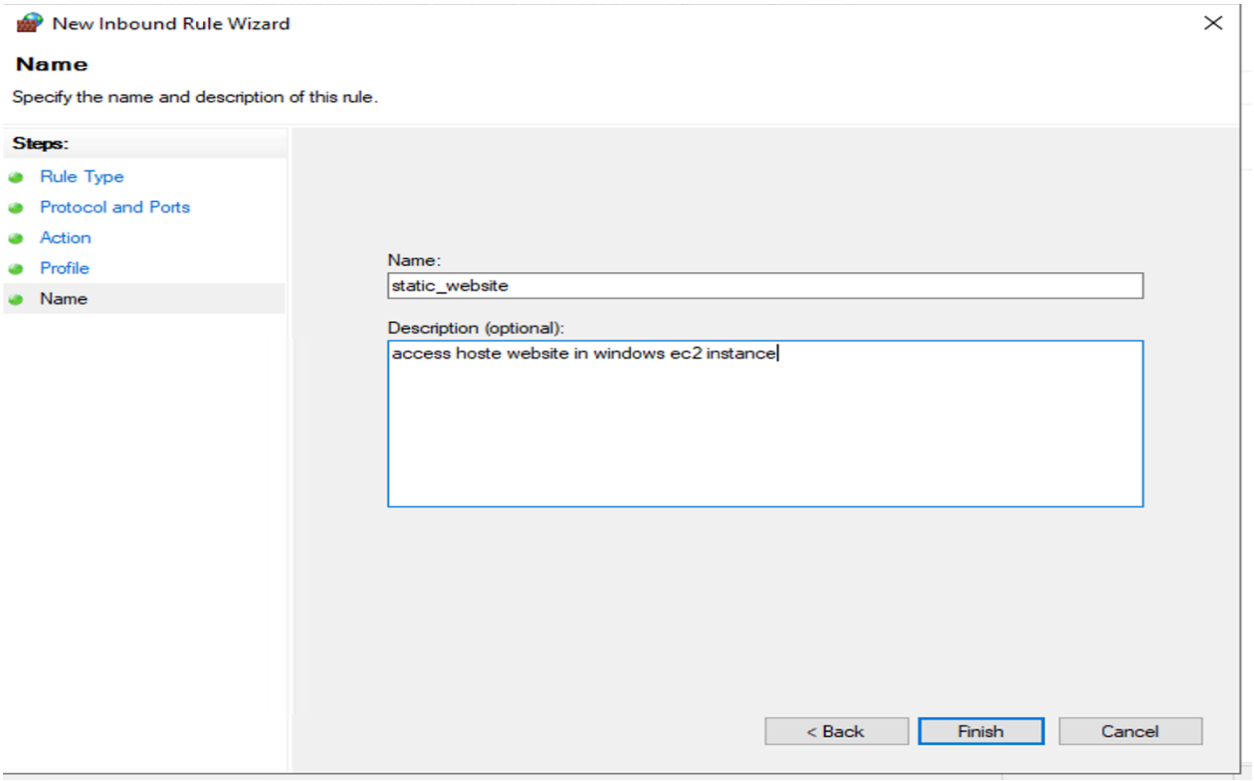



Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabl
AllJoyn Router (TCP-In)
AllJoyn Router (UDP-In)
AllJoyn Router
Domai...
Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
80,443
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel



After configuration of firewall setting in remote desktop. The static website is checked is checked locally using the public IP of windows EC2 instance.