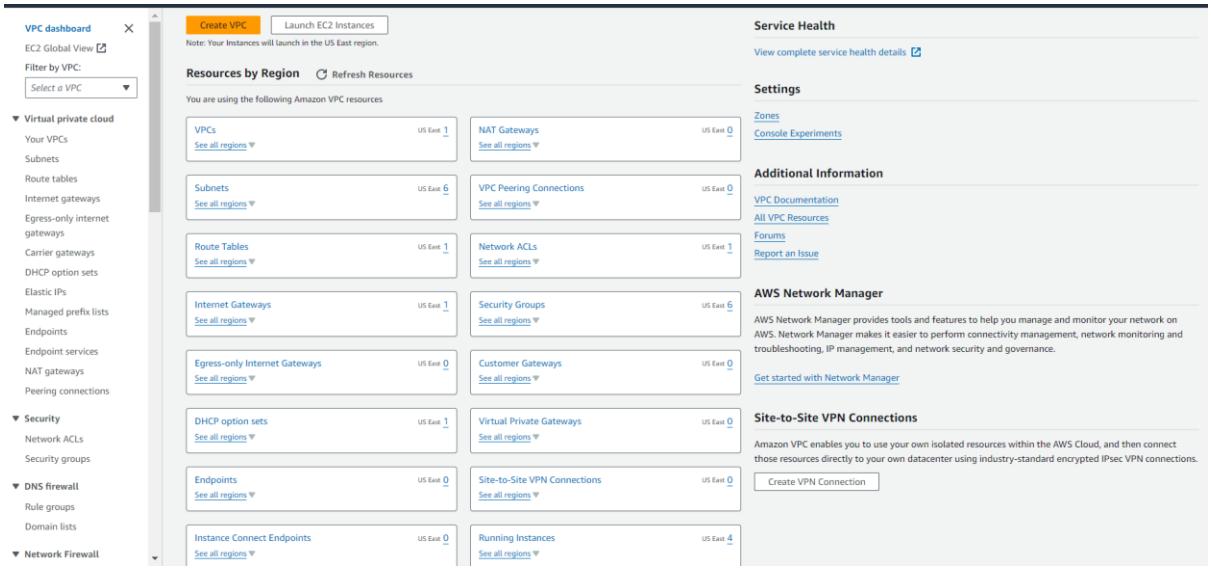
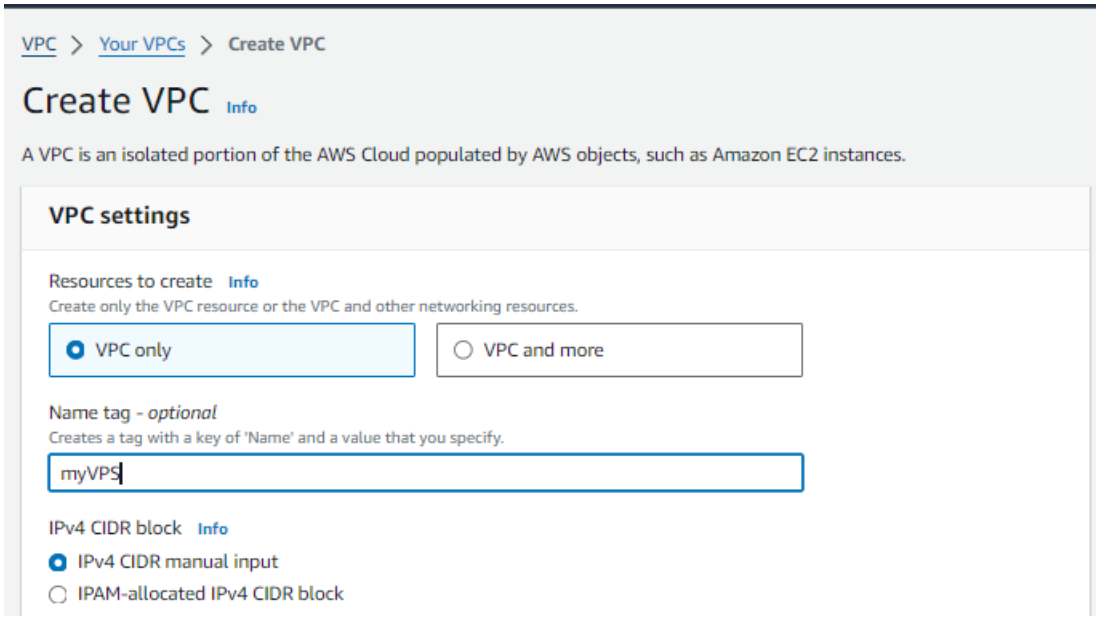
# VPC Workshop



IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- (•) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info

Default

## Tags

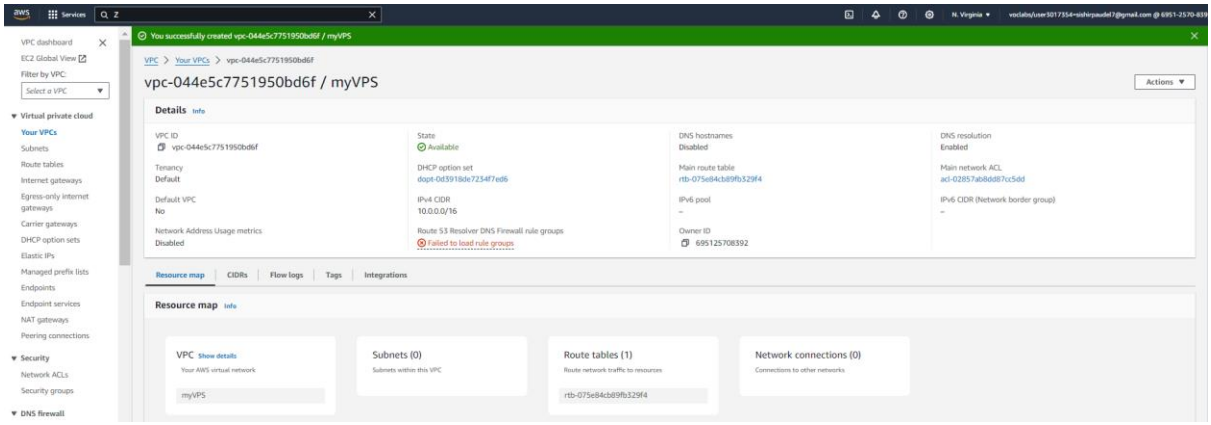
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* | |
|---|---|---|
| Name | myVPS | Remove tag |

Add tag

You can add 49 more tags

Cancel | Create VPC



▼ **Virtual private cloud**

Your VPCs

**Subnets**

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

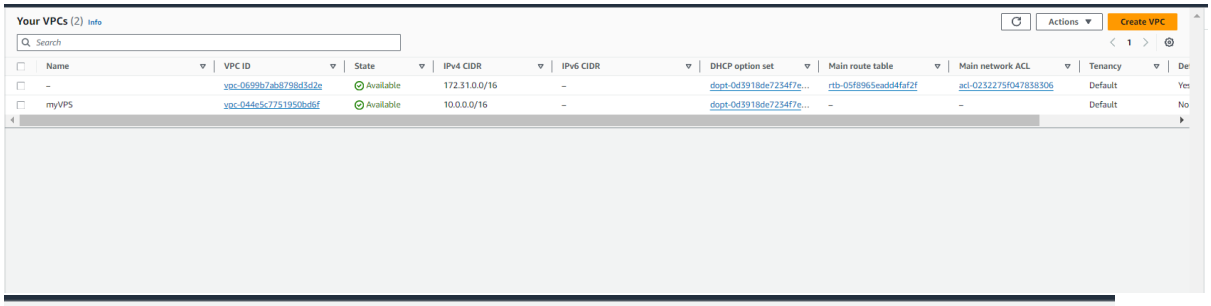
Managed prefix lists

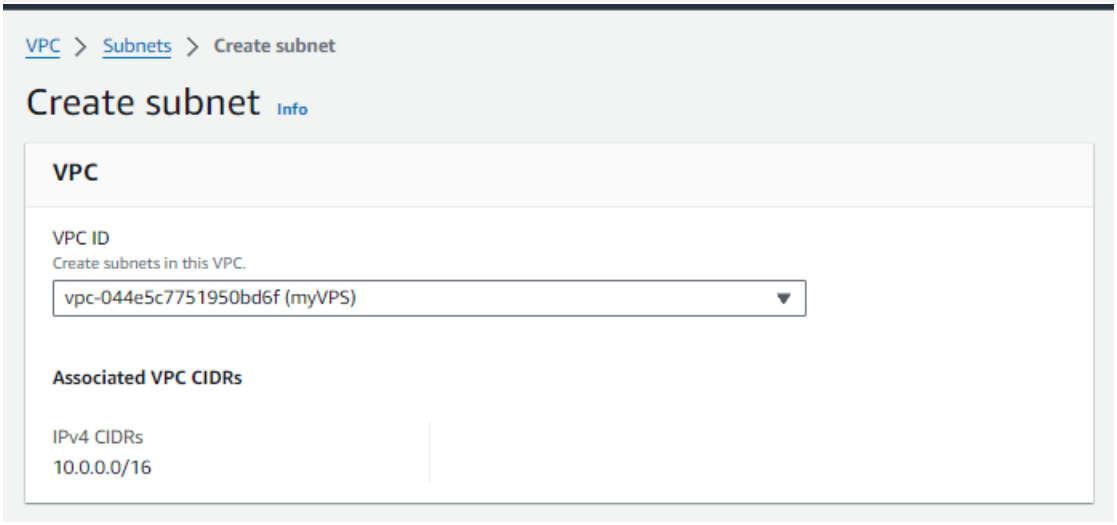
Endpoints

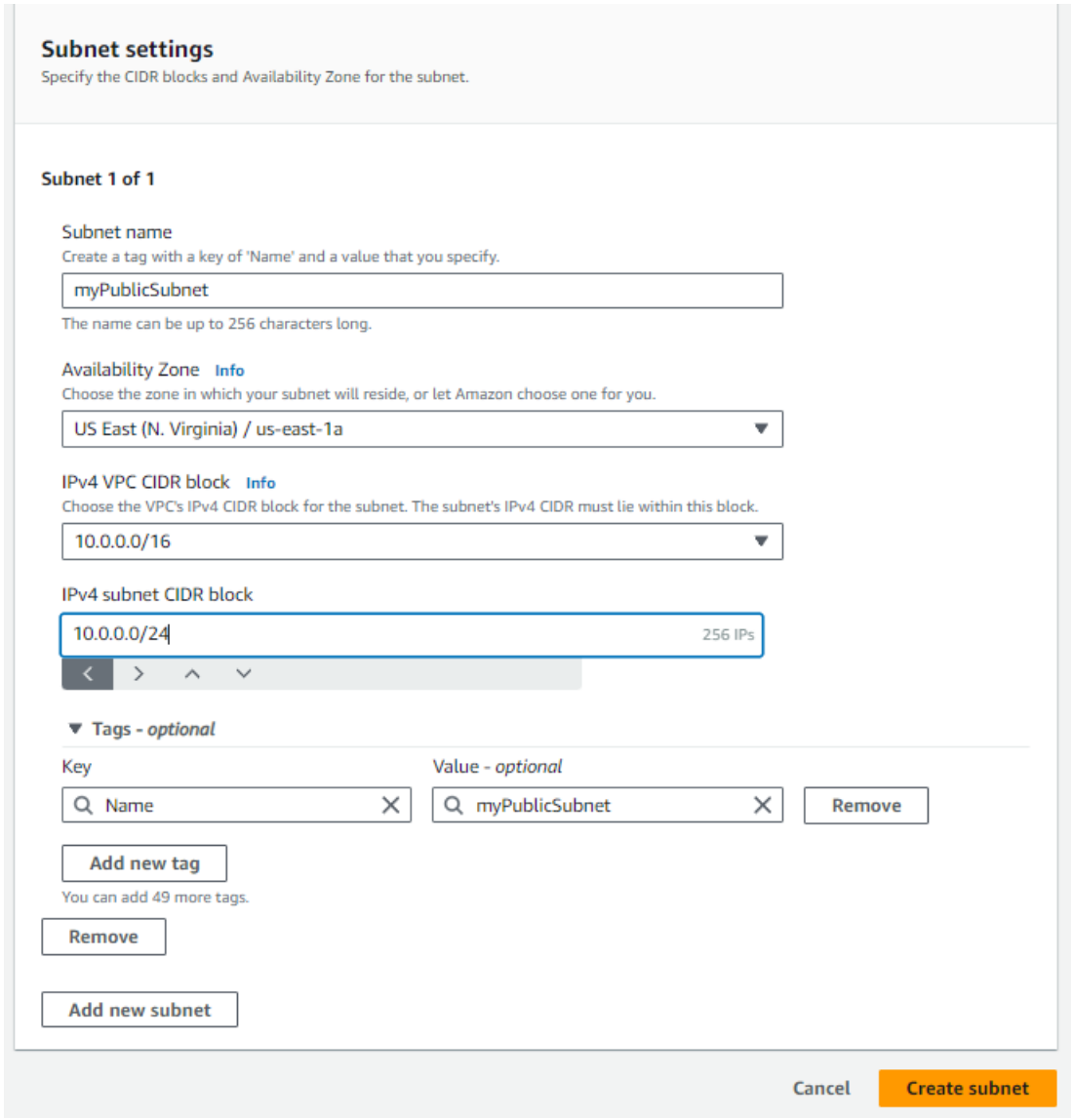
Endpoint services

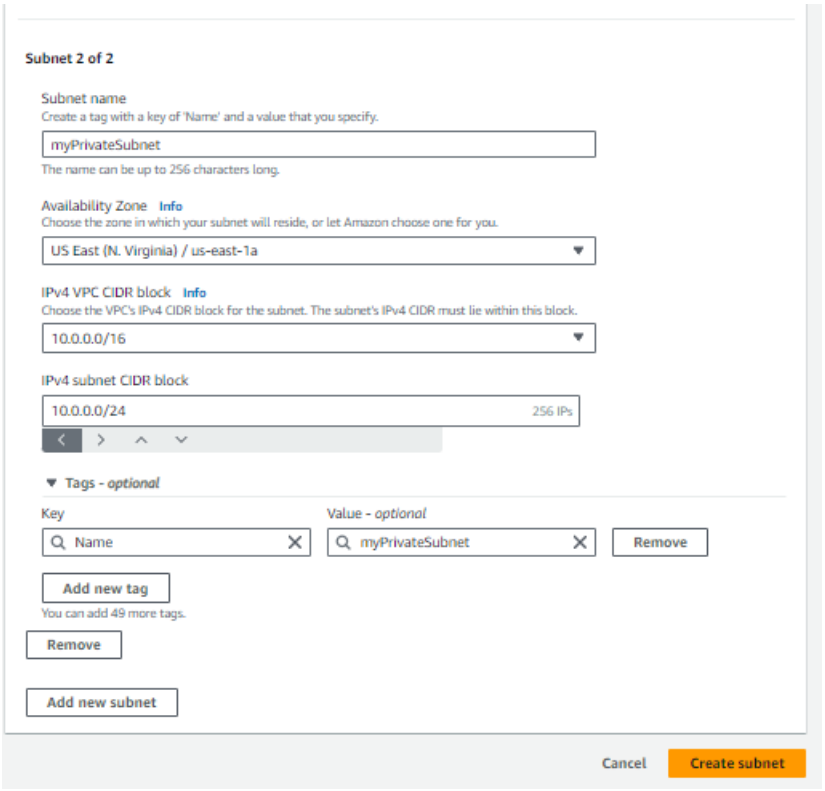
NAT gateways

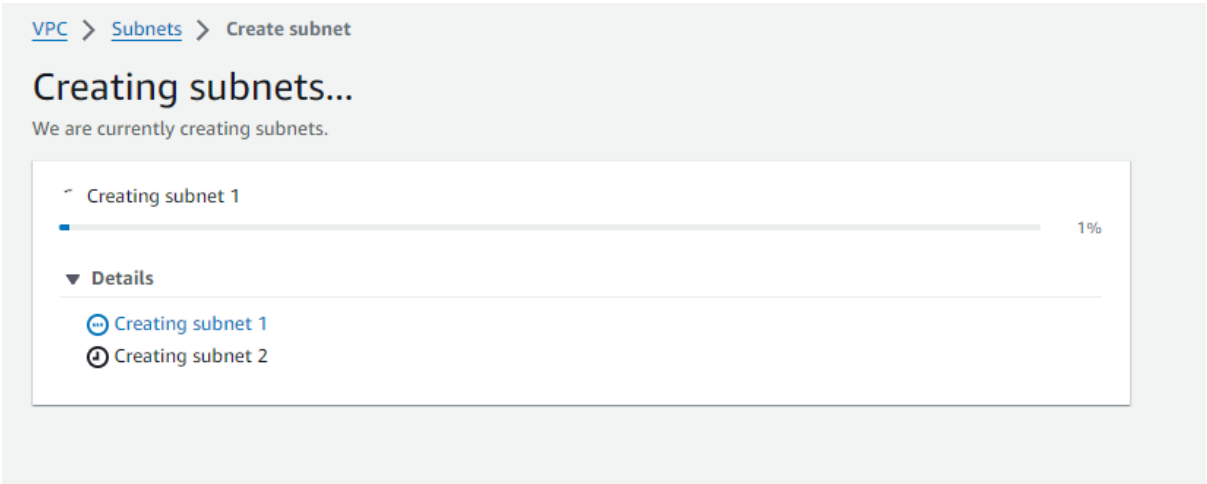
Peering connections

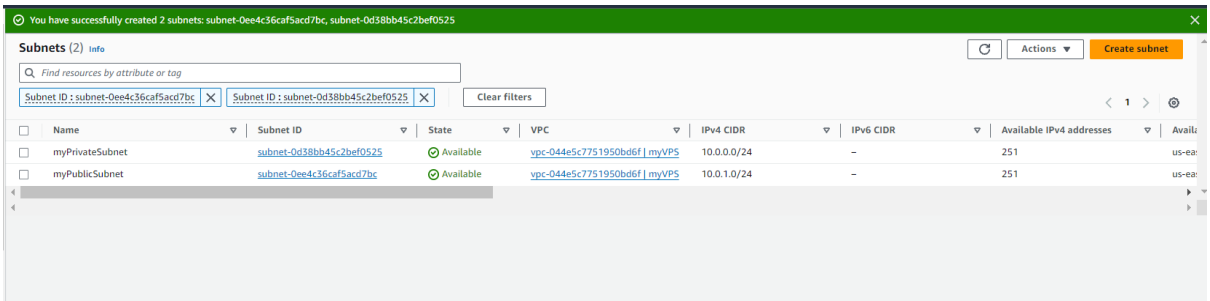

Your VPCs (2) Info
Search
Actions
Create VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
Main route table
Main network ACL
Tenancy
–
vpc-0699b7ab8798d3d2e
Available
172.31.0.0/16
–
dopt-0d3918de7234f7e...
rtb-05f8965eadd4faf2f
acl-0232275f047838306
Default
myVPS
vpc-044e5c7751950bd6f
Available
10.0.0.0/16
–
dopt-0d3918de7234f7e...
–
–
Default


VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-044e5c7751950bd6f (myVPS)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16


Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
myPublicSubnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.0.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
myPublicSubnet
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

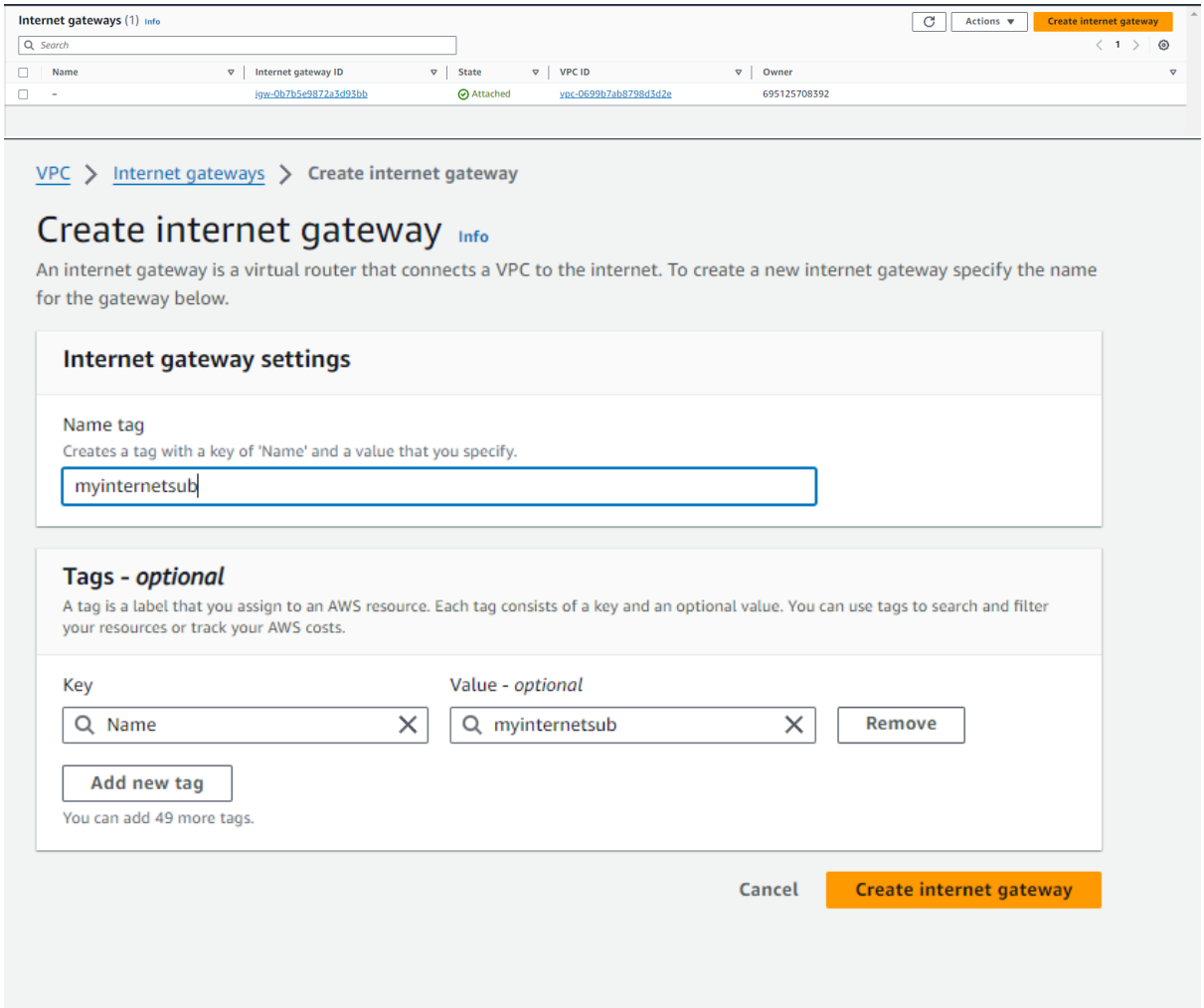

Subnet 2 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
myPrivateSubnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.0.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
myPrivateSubnet
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet
Cancel
Create subnet

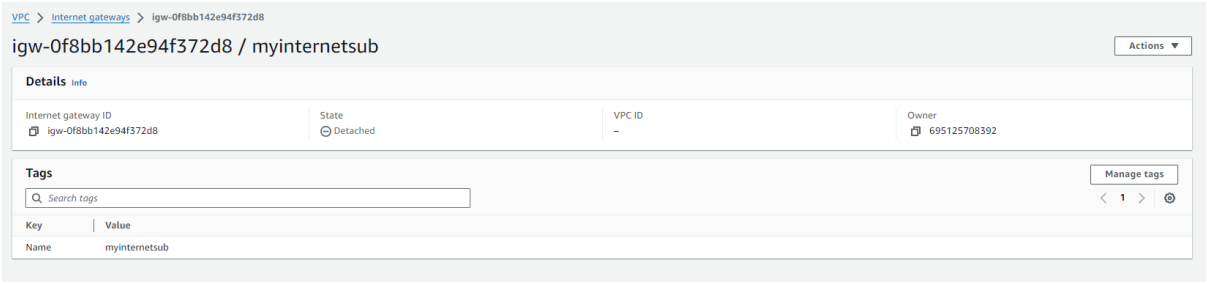

VPC > Subnets > Create subnet
Creating subnets...
We are currently creating subnets.
Creating subnet 1
1%
Details
Creating subnet 1
Creating subnet 2

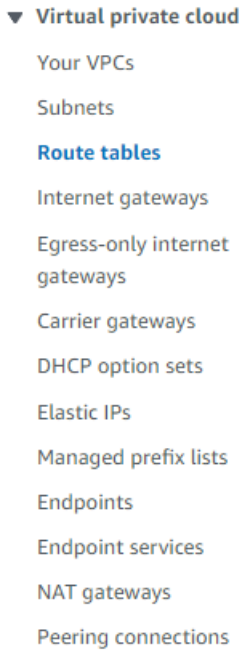

You have successfully created 2 subnets: subnet-0ee4c36caf5acd7bc, subnet-0d38bb45c2bef0525
Subnets (2) Info
Actions
Create subnet
Find resources by attribute or tag
Subnet ID : subnet-0ee4c36caf5acd7bc
Subnet ID : subnet-0d38bb45c2bef0525
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Available IPv4 addresses
myPrivateSubnet
subnet-0d38bb45c2bef0525
Available
vpc-044e5c7751950bd6f | myVPS
10.0.0.0/24
251
myPublicSubnet
subnet-0ee4c36caf5acd7bc
Available
vpc-044e5c7751950bd6f | myVPS
10.0.1.0/24
251

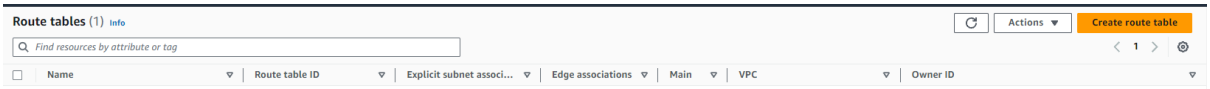
▼ Virtual private cloud

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




VPC > Internet gateways > igw-0f8bb142e94f372d8
igw-0f8bb142e94f372d8 / myinternetsub
Actions
Details Info
Internet gateway ID
igw-0f8bb142e94f372d8
State
Detached
VPC ID
–
Owner
695125708392
Tags
Manage tags
Search tags
1
Key
Value
Name
myinternetsub


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


Route tables (1) Info
Actions
Create route table
Find resources by attribute or tag
1
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
Owner ID

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.

myvpc-route-table

VPC

The VPC to use for this route table.

vpc-044e5c7751950bd6f (myVPS)

## Tags

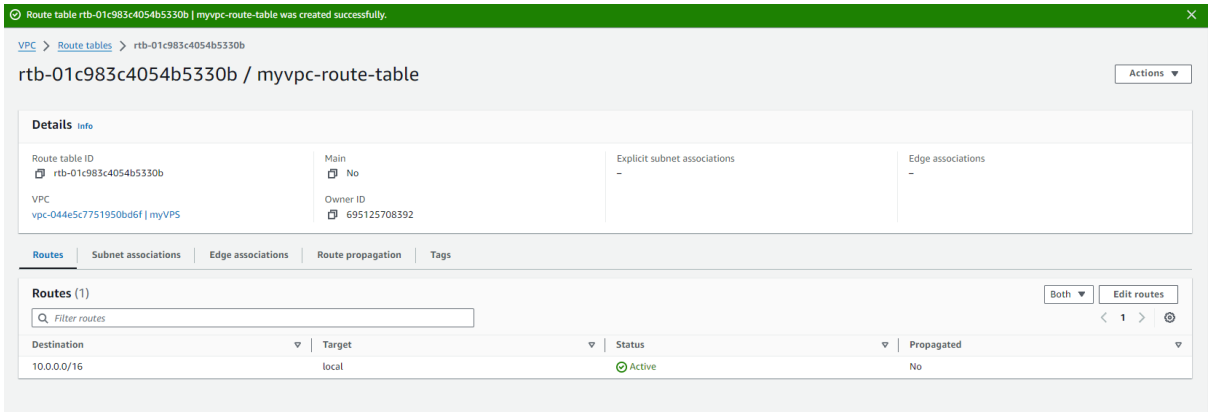
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

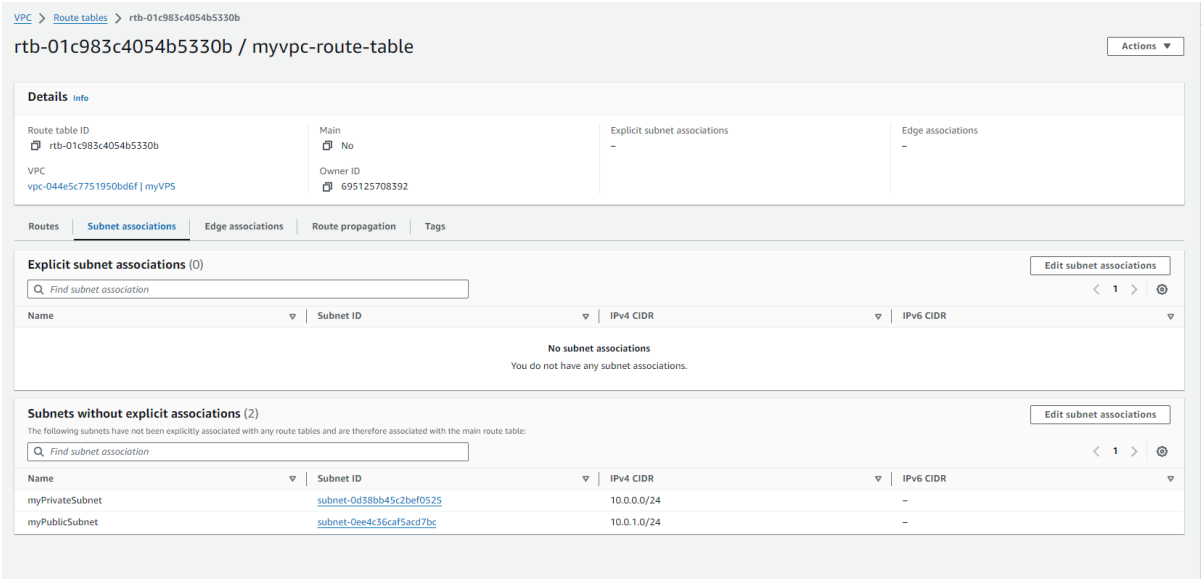
| Key | Value - *optional* | |
|---|---|---|
| Name | myvpc-route-table | Remove |

Add new tag

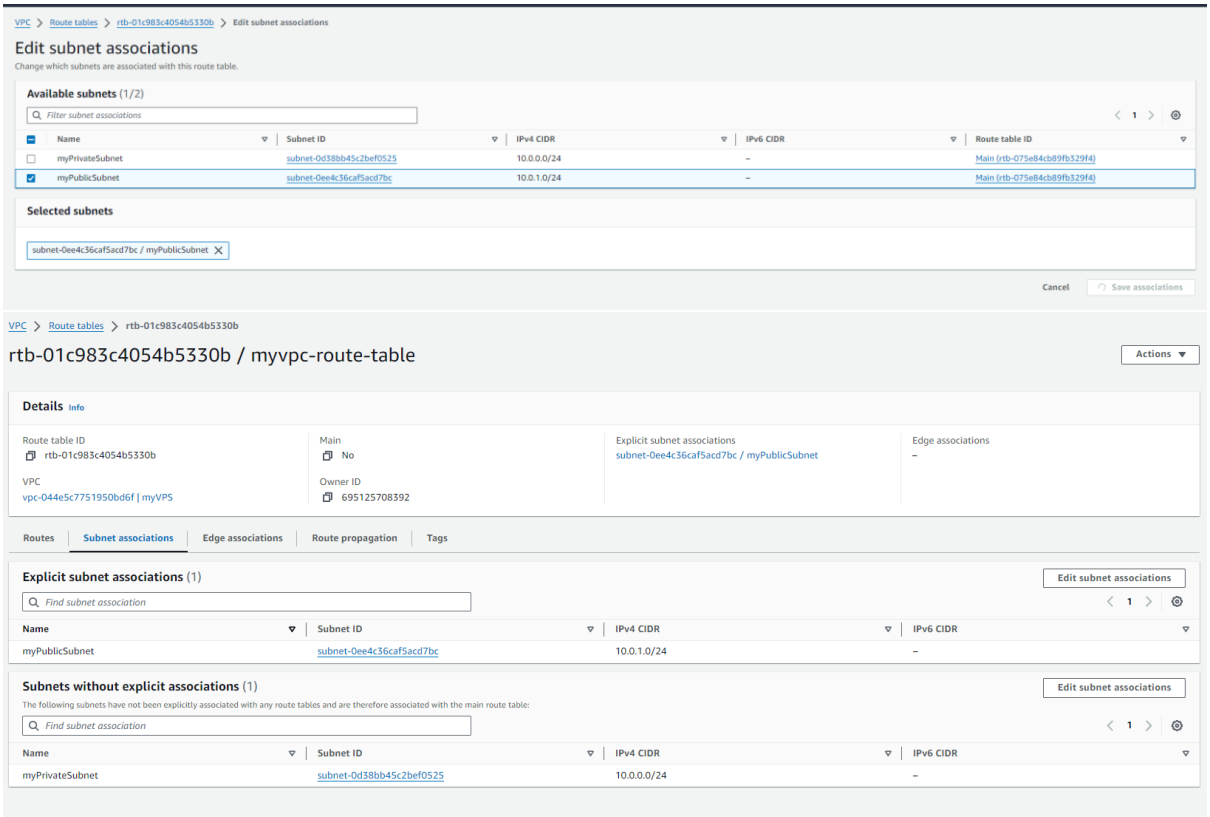
You can add 49 more tags.

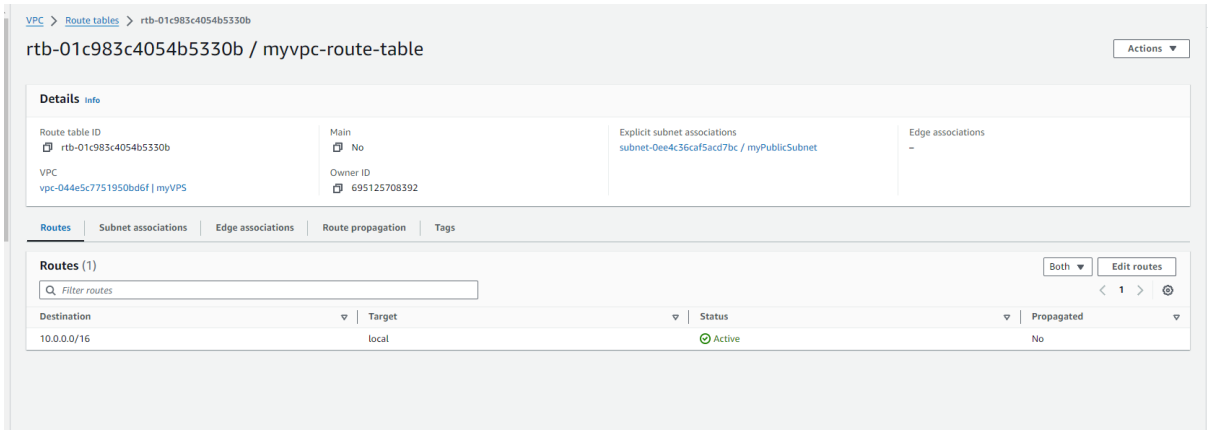
Cancel | Create route table

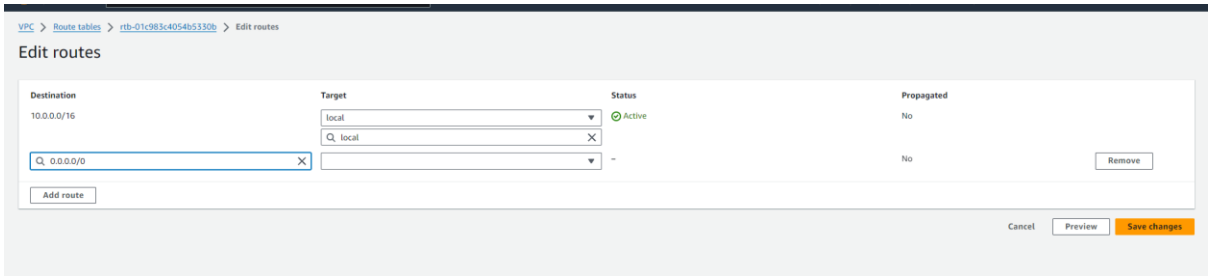


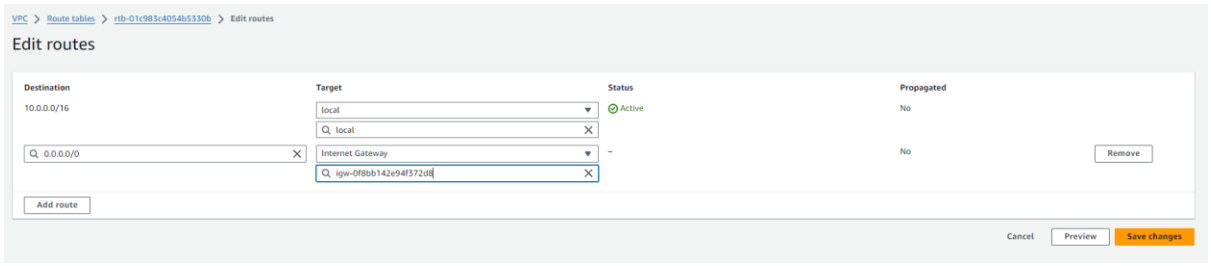


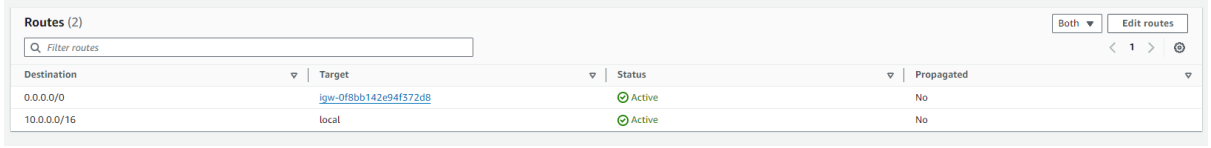

Add which route you want to explore to the internet



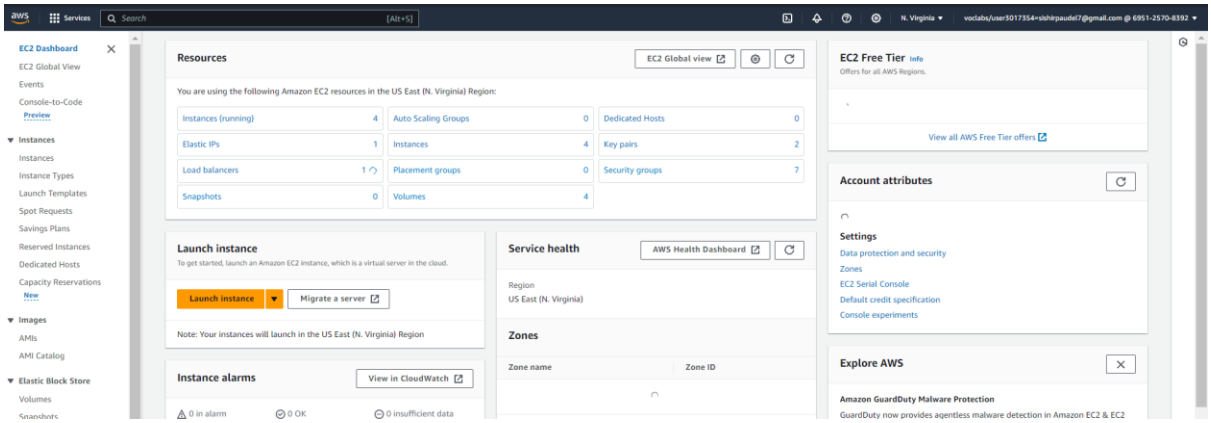



Now create a ec2 instance




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

myvpcinstance

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 L

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

ami-0440d3b780d96b29d (64-bit (x86), uefi-preferred) / ami-0f93c02efd1974b8b (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

## Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

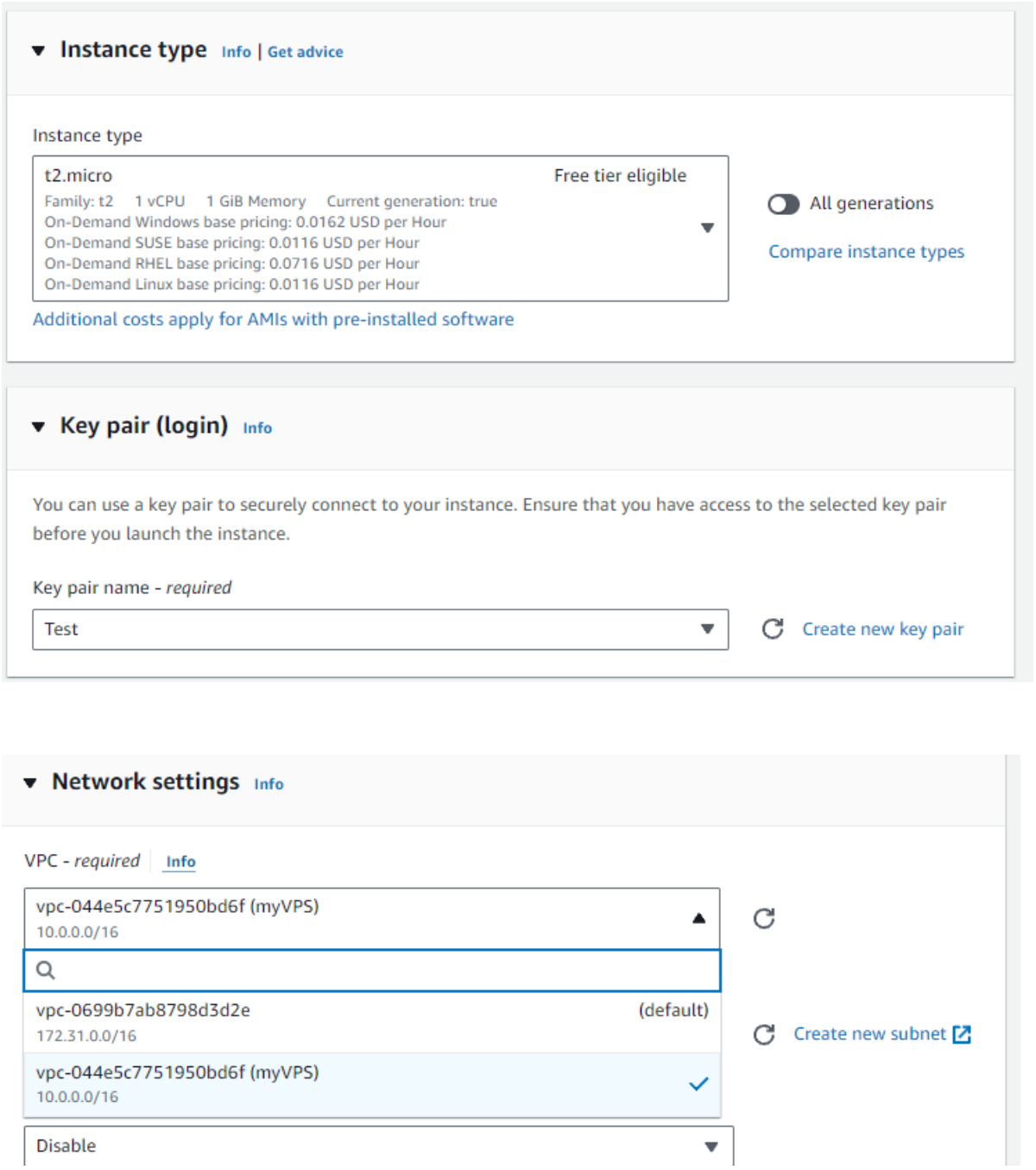
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

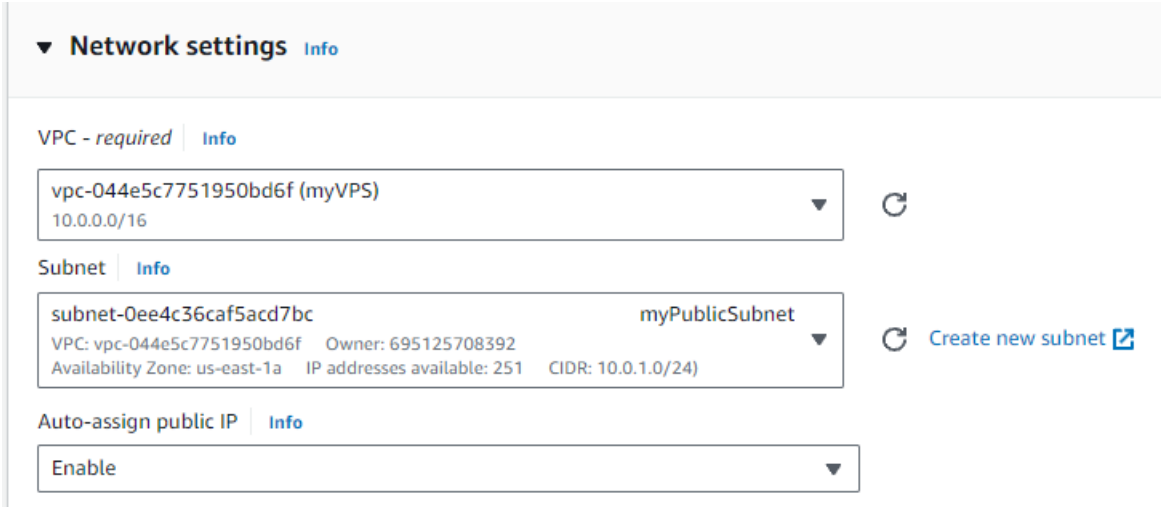
Review commands





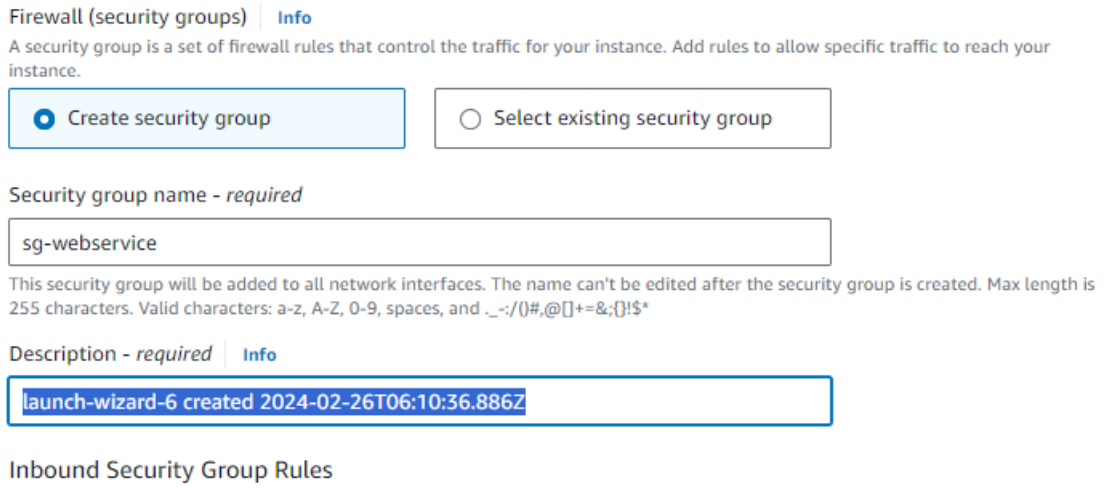


CHOOSE OUR VPC

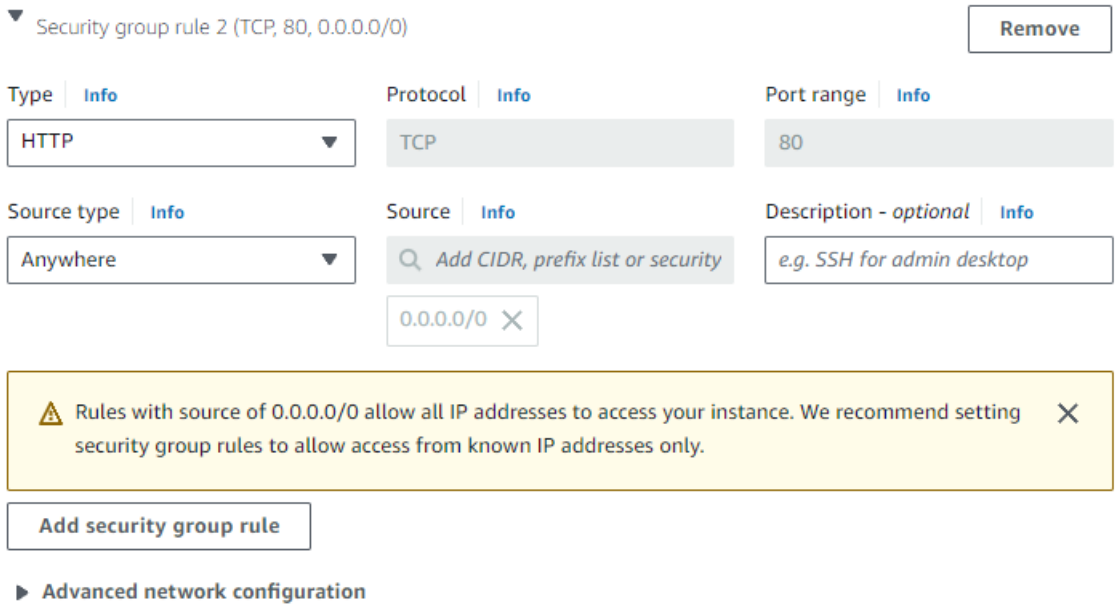



Choose the public subnet to access, then enable the auto assign public IP

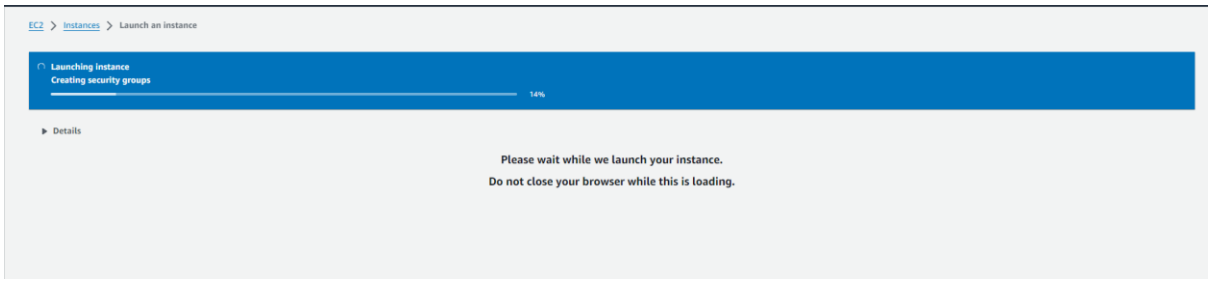
Now create a new security group / firewalls

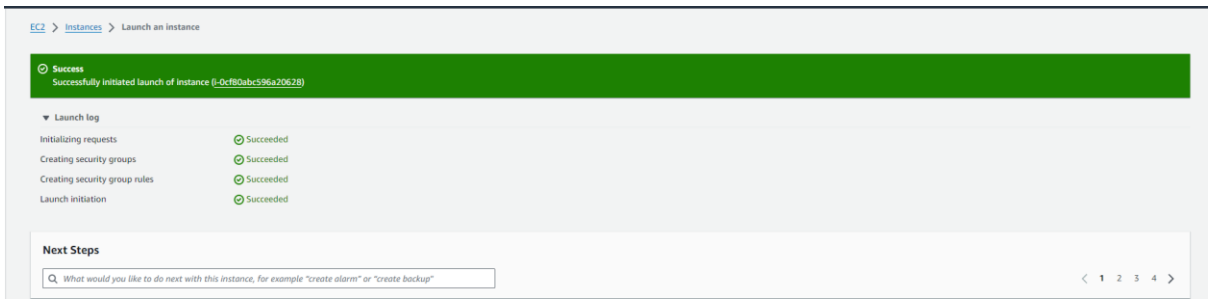


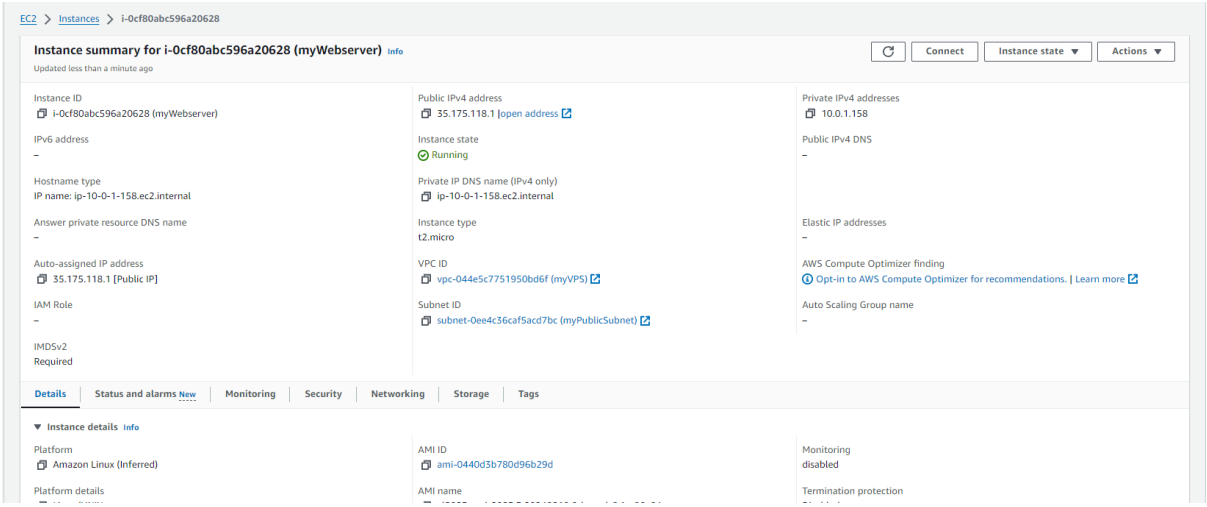
Now add rules for security groups



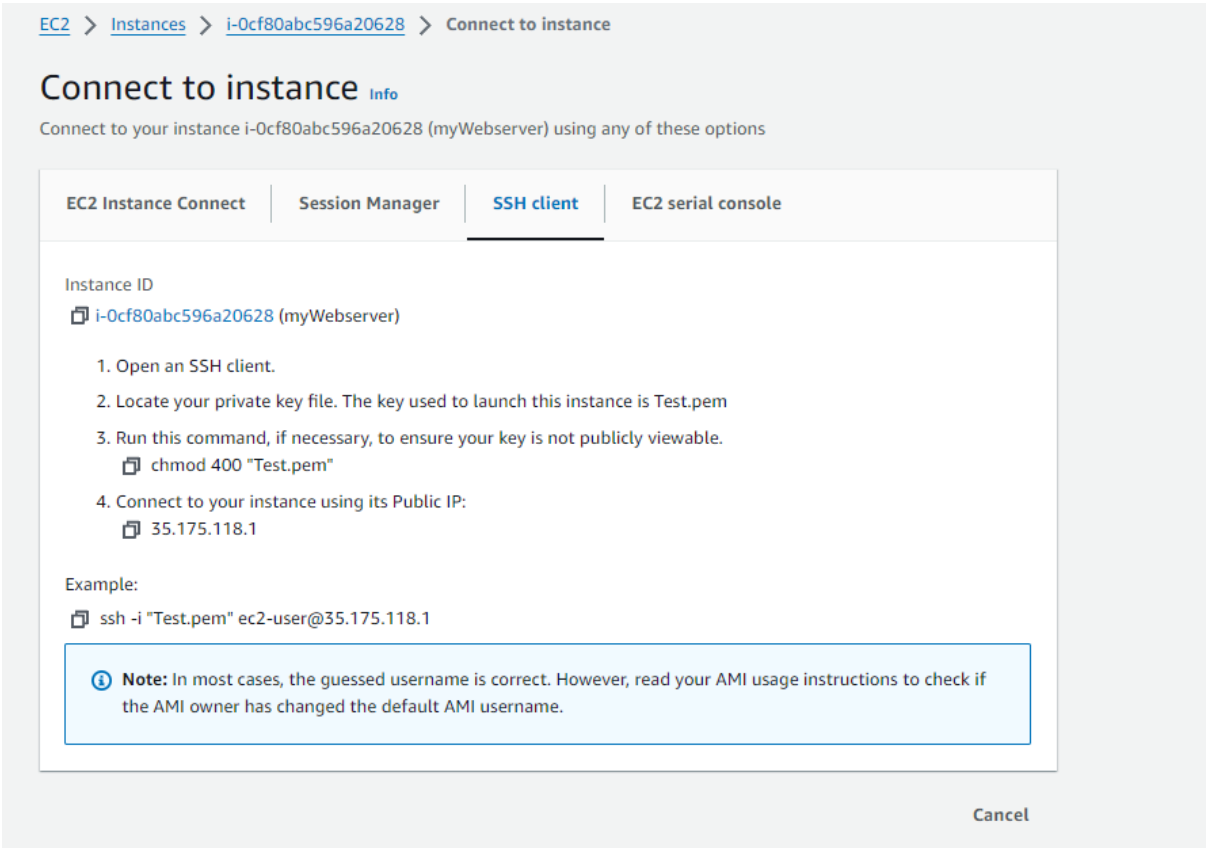

Now launch the instance



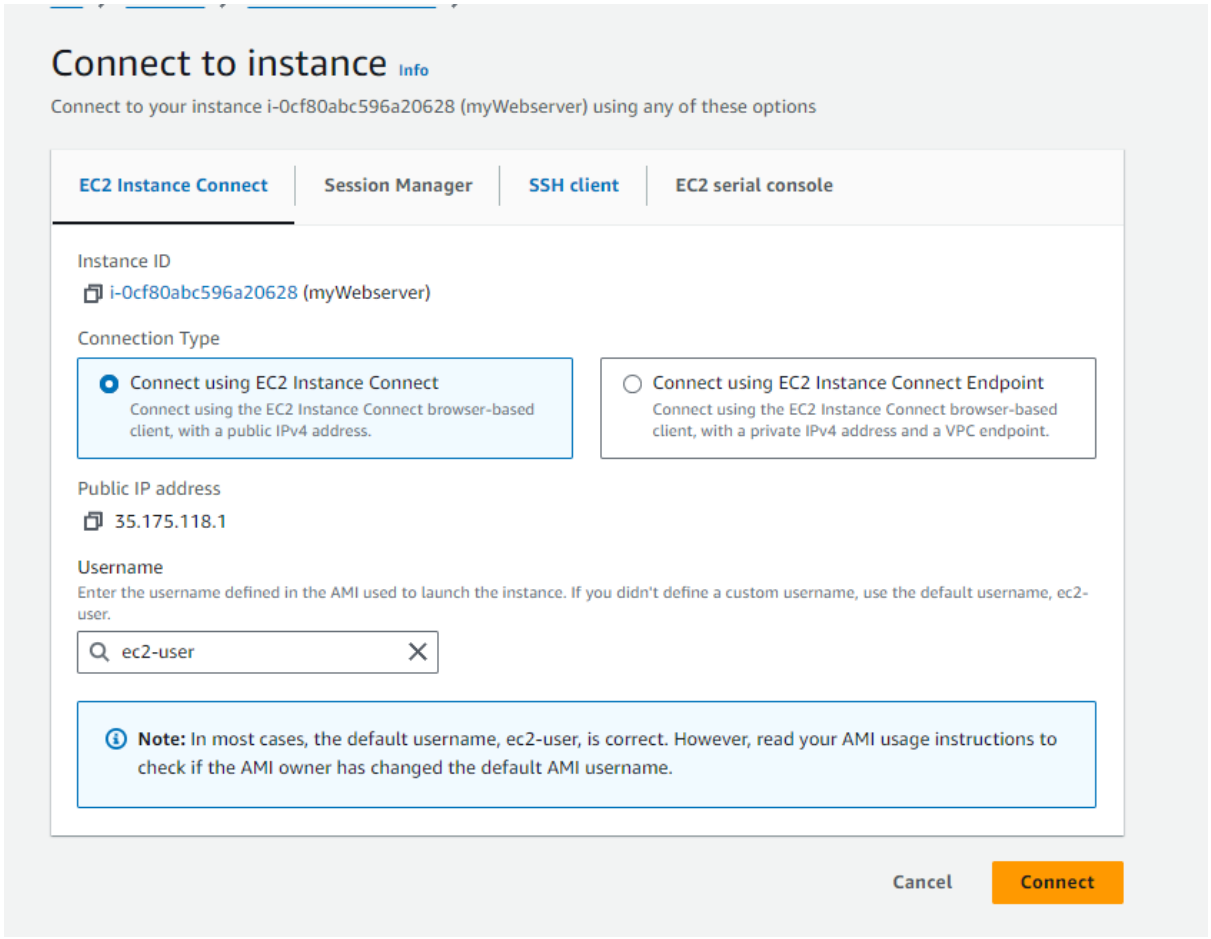





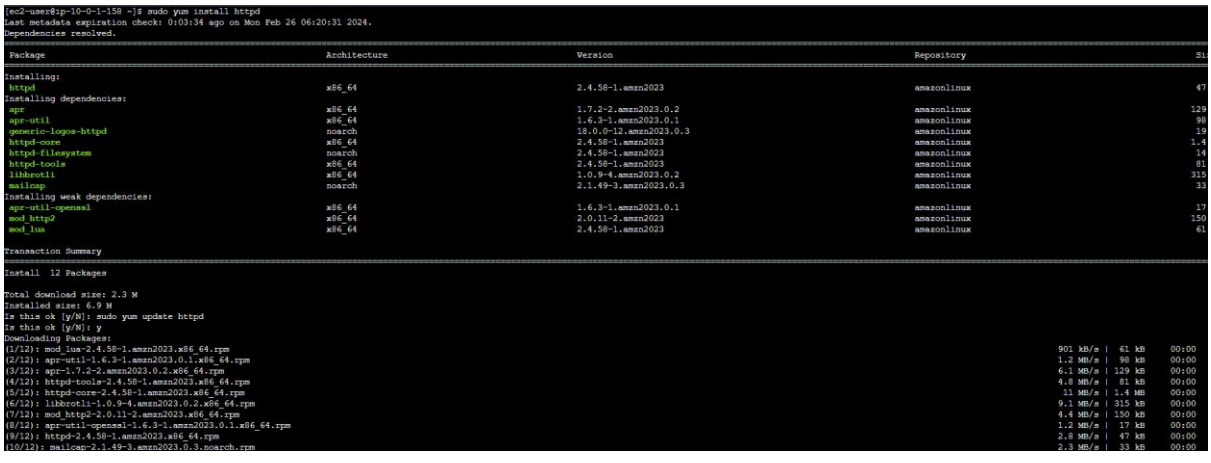

Go to connect




Now connect it




this page is redirected



```
[ec2-user@ip-10-0-1-158 ~]$ sudo yum update httpd
Last metadata expiration check: 0:04:14 ago on Mon Feb 26 06:20:31 2024.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-1-158 ~]$
```

Code :

Sudo yum update

Sudo yum install httpd

Sudo yum update httpd

Sudo service httpd start

Sudo service httpd status

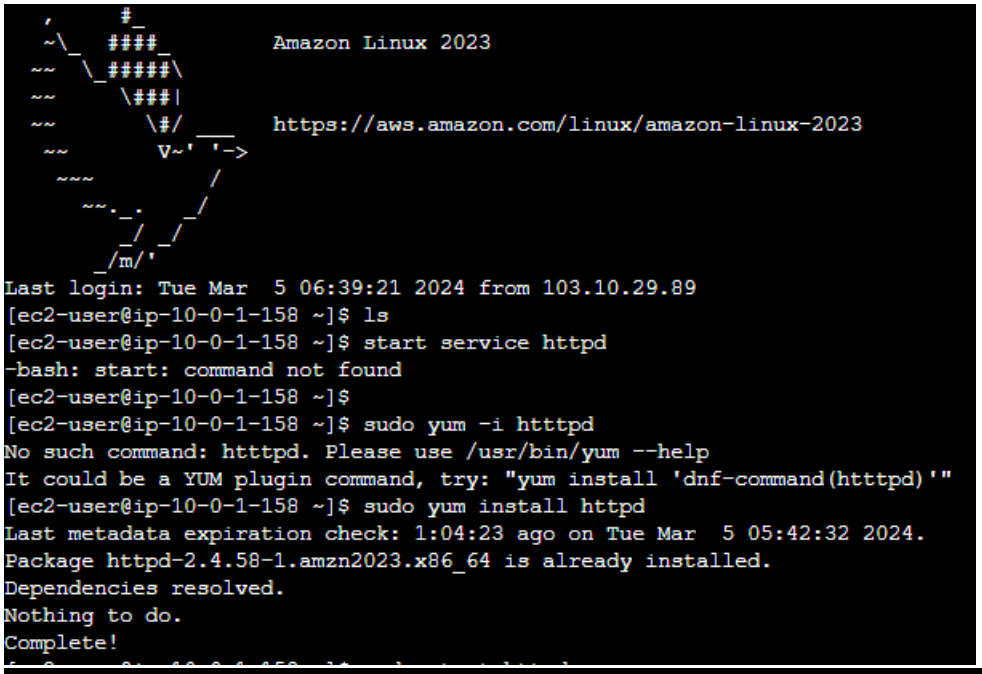
```
[ec2-user@ip-10-0-1-158 ~]$ sudo service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2024-02-26 06:25:53 UTC; 5min ago
       Docs: man:httpd.service(8)
   Main PID: 25942 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 1114)
     Memory: 13.4M
        CPU: 258ms
     CGroup: /system.slice/httpd.service
             ├─25942 /usr/sbin/httpd -DFOREGROUND
             ├─25964 /usr/sbin/httpd -DFOREGROUND
             ├─25965 /usr/sbin/httpd -DFOREGROUND
             ├─25966 /usr/sbin/httpd -DFOREGROUND
             └─25967 /usr/sbin/httpd -DFOREGROUND

Feb 26 06:25:53 ip-10-0-1-158.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Feb 26 06:25:53 ip-10-0-1-158.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Feb 26 06:25:53 ip-10-0-1-158.ec2.internal httpd[25942]: Server configured, listening on: port 80
[ec2-user@ip-10-0-1-158 ~]$
```

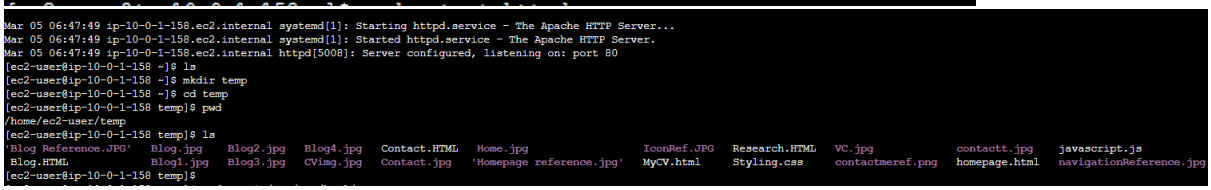
i-0cf80abc596a20628 (myWebserver)

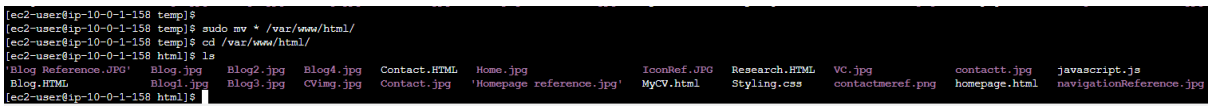
PublicIPs: 35.175.118.1 PrivateIPs: 10.0.1.158


# It works!

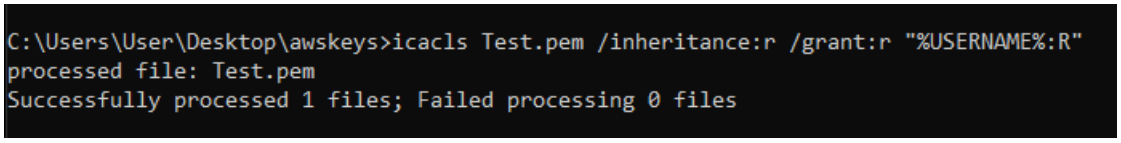
# Hosting Portfolio Using linux server



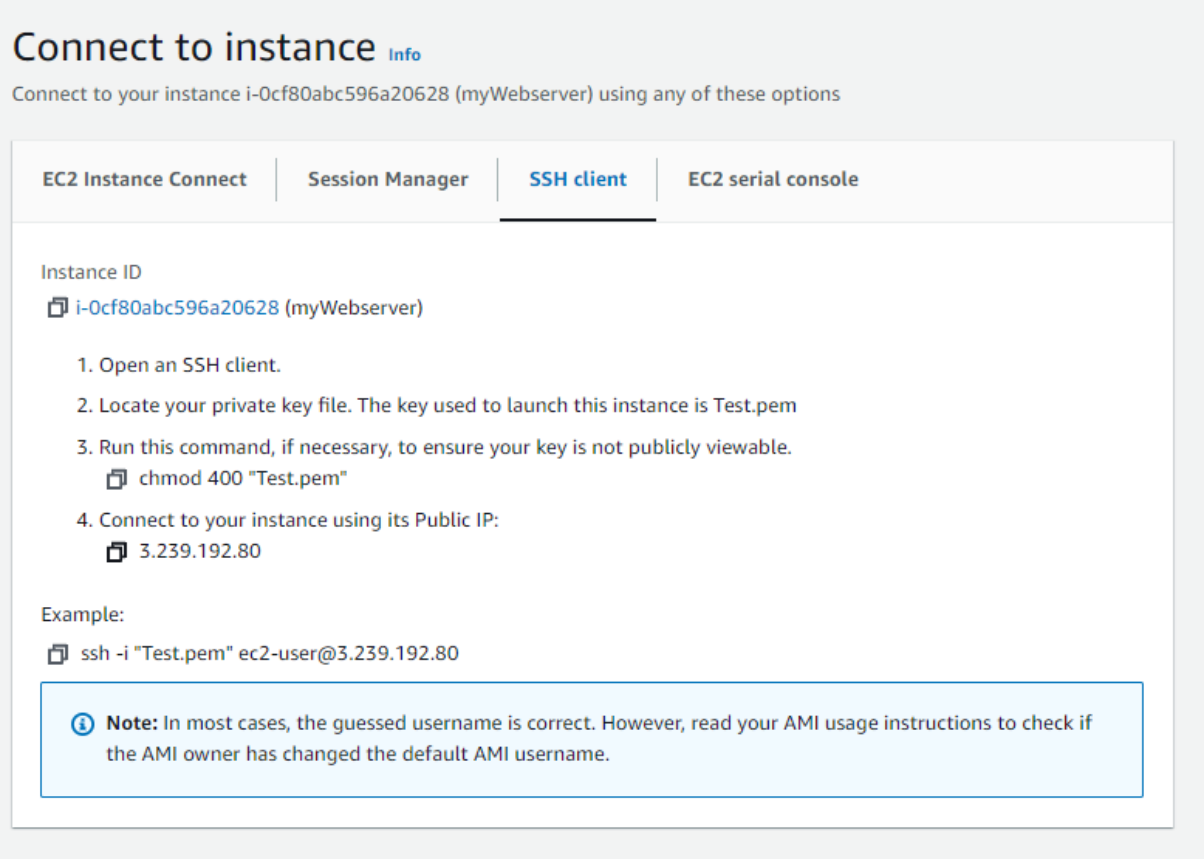




Giving permission to access test.pem key




Loading a folder from local machine to that ec2 instance

```
C:\Users\User\Desktop\awskeys>scp -i "Test.pem" C:\Users\User\Desktop\portfoliio/* ec2-user@3.239.192.80:temp
Blog Reference.JPG                                            100%  114KB 101.4KB/s   00:01
Blog.HTML                                                     100% 7909    27.1KB/s   00:00
Blog.jpg                                                      100% 2574KB   1.5MB/s   00:01
Blog1.jpg                                                     100%  686KB   1.6MB/s   00:00
Blog2.jpg                                                     100% 2608KB   1.4MB/s   00:01
Blog3.jpg                                                     100%   39KB 131.6KB/s   00:00
Blog4.jpg                                                     100% 1017KB   1.5MB/s   00:00
CVimg.jpg                                                     100%  206KB 599.7KB/s   00:00
Contact.HTML                                                  100% 4768    15.3KB/s   00:00
Contact.jpg                                                   100%   88KB 262.6KB/s   00:00
Home.jpg                                                      100%  575KB   1.4MB/s   00:00
Homepage reference.jpg                                        100%  106KB 359.4KB/s   00:00
IconRef.JPG                                                   100%   79KB 259.3KB/s   00:00
MyCV.html                                                     100% 4174    14.7KB/s   00:00
Research.HTML                                                 100% 3626    12.8KB/s   00:00
Styling.css                                                   100% 6223    21.7KB/s   00:00
VC.jpg                                                        100%  650KB   1.6MB/s   00:00
contactmeref.png                                              100%   53KB 181.3KB/s   00:00
contactt.jpg                                                  100%  136KB 445.4KB/s   00:00
homepage.html                                                 100% 2674     9.5KB/s   00:00
javascript.js                                                 100%  296     1.1KB/s   00:00
navigationReference.jpg                                       100%   26KB  93.0KB/s   00:00

C:\Users\User\Desktop\awskeys>ls
```




Check the instance in Public IP

# Connect to instance Info

Connect to your instance i-0cf80abc596a20628 (myWebserver) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

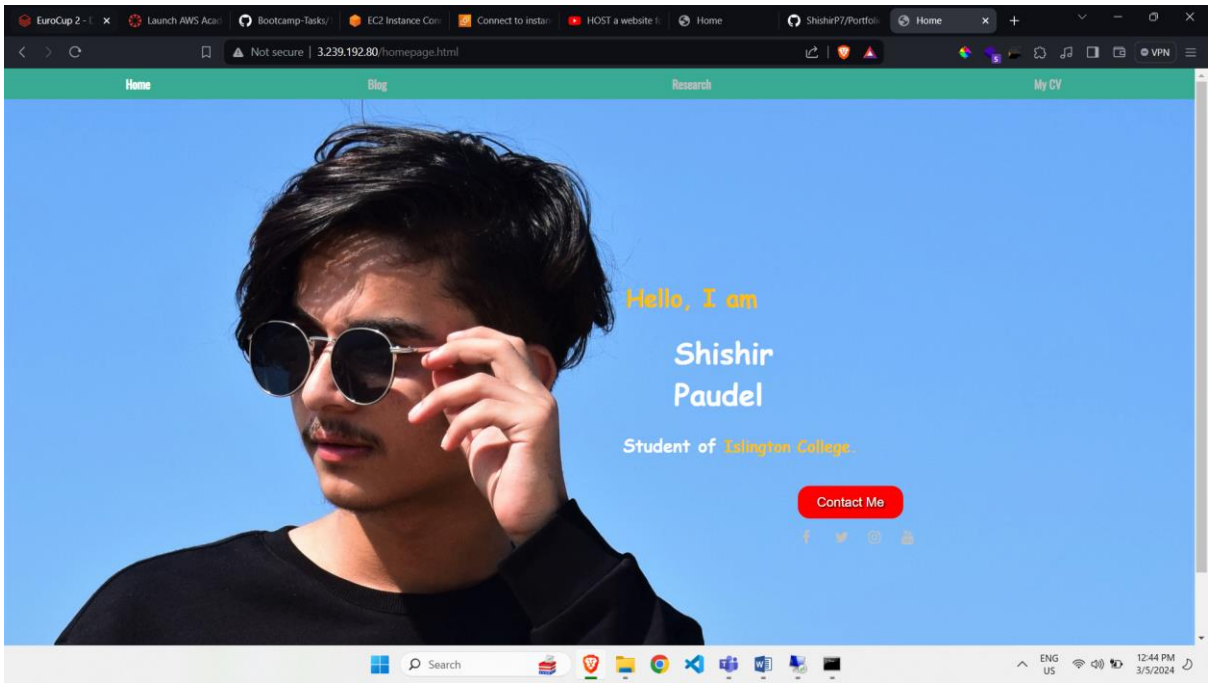
i-0cf80abc596a20628 (myWebserver)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Test.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 "Test.pem"
4. Connect to your instance using its Public IP:
   3.239.192.80

Example:

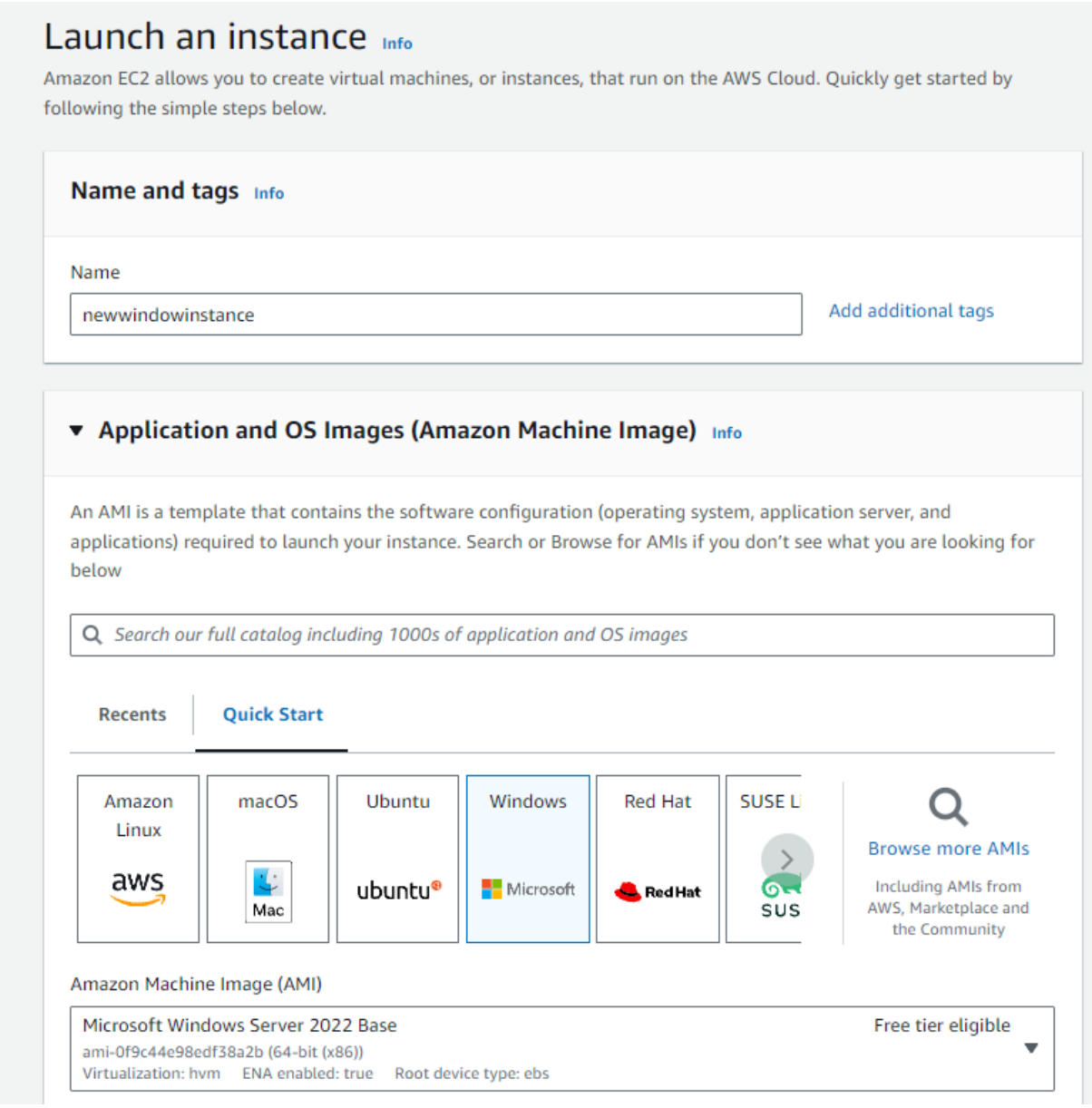
ssh -i "Test.pem" ec2-user@3.239.192.80

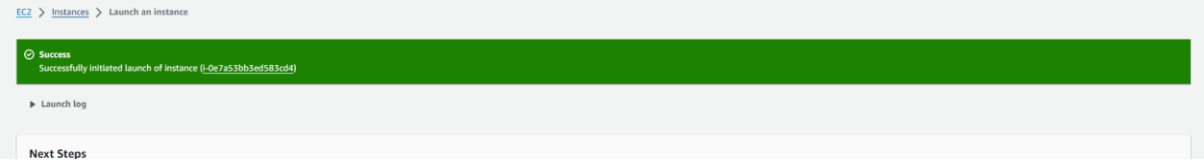
**Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

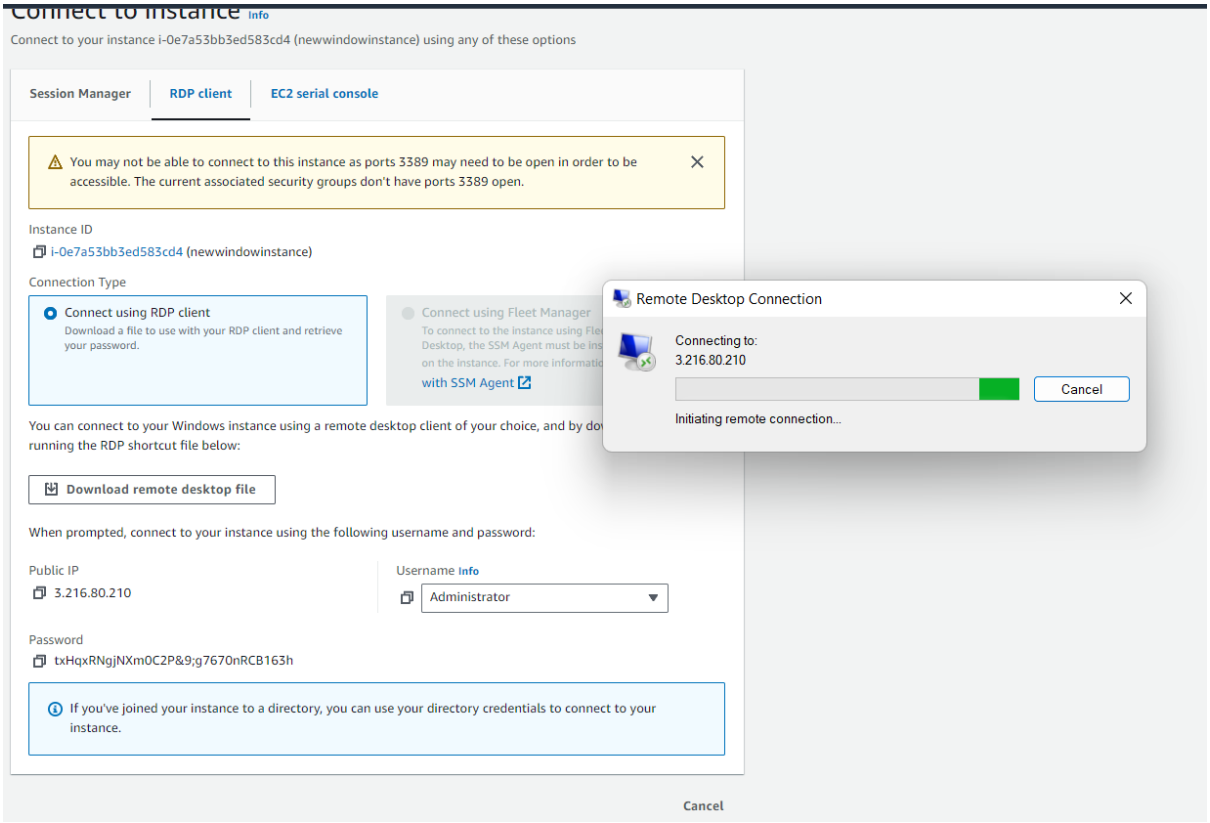


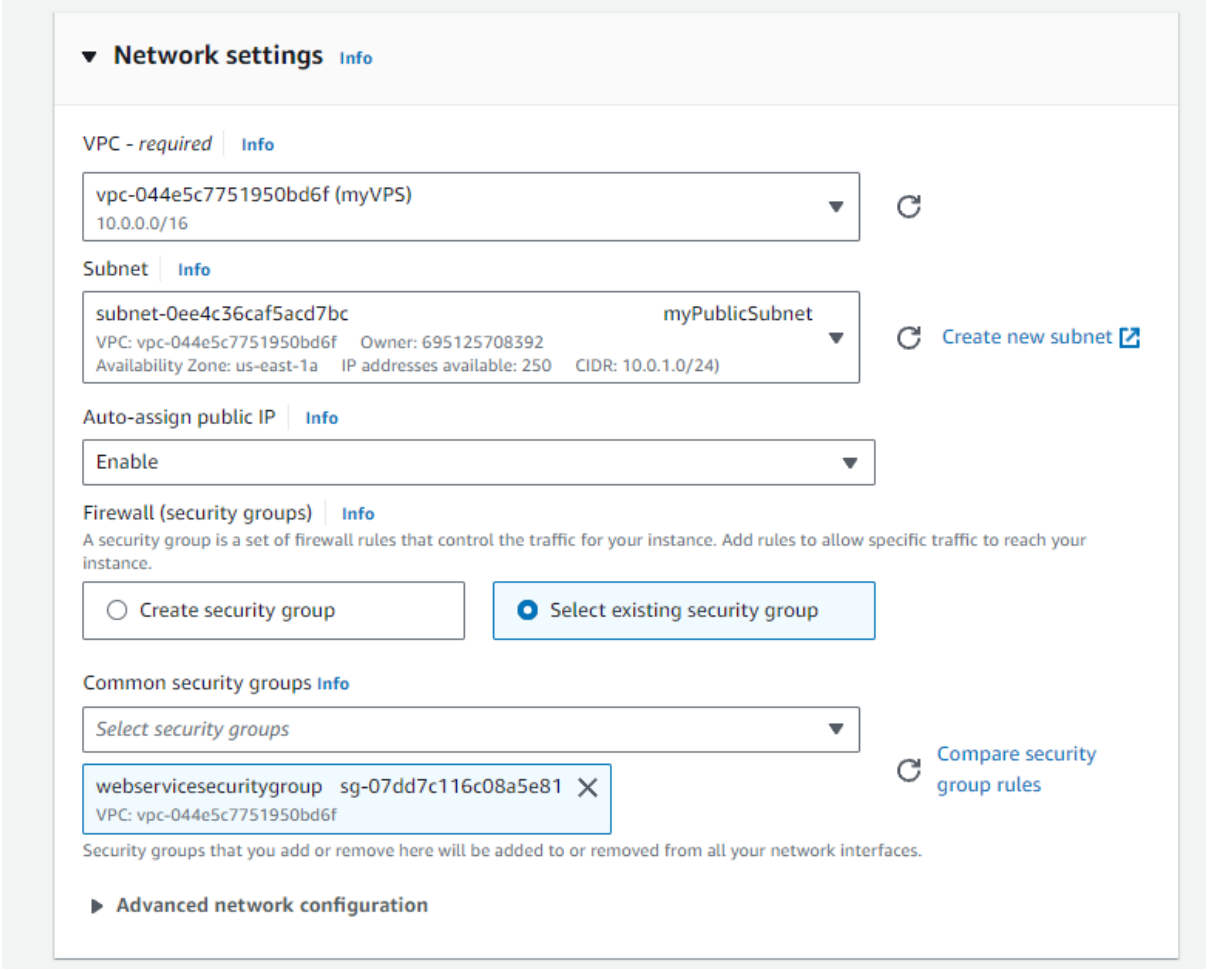
# Now hosting portfolio using windows server

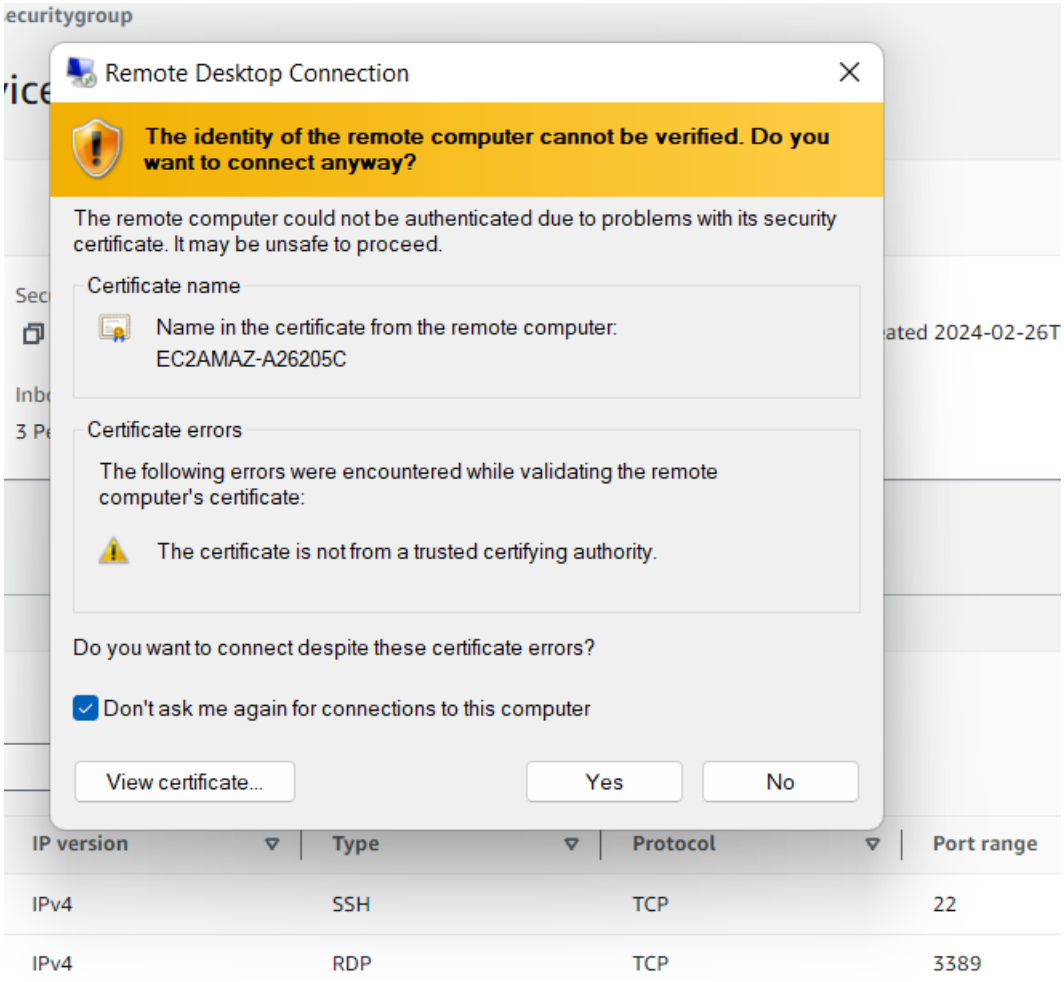
Create a new instance with Windows OS

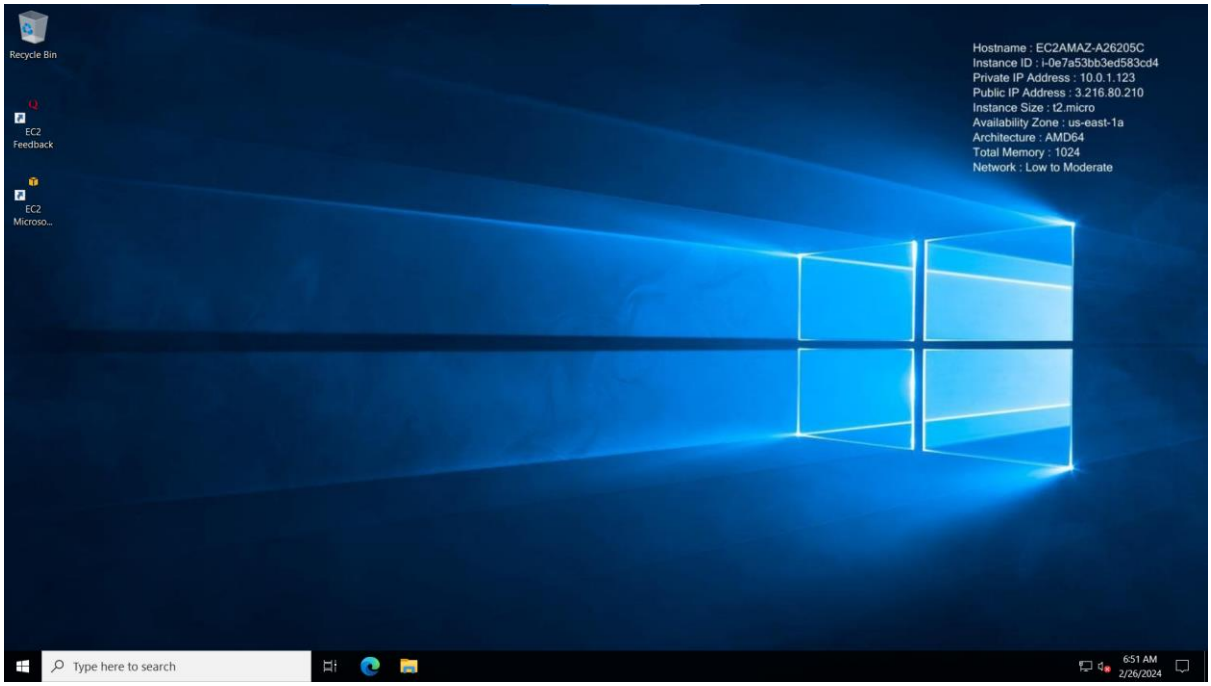


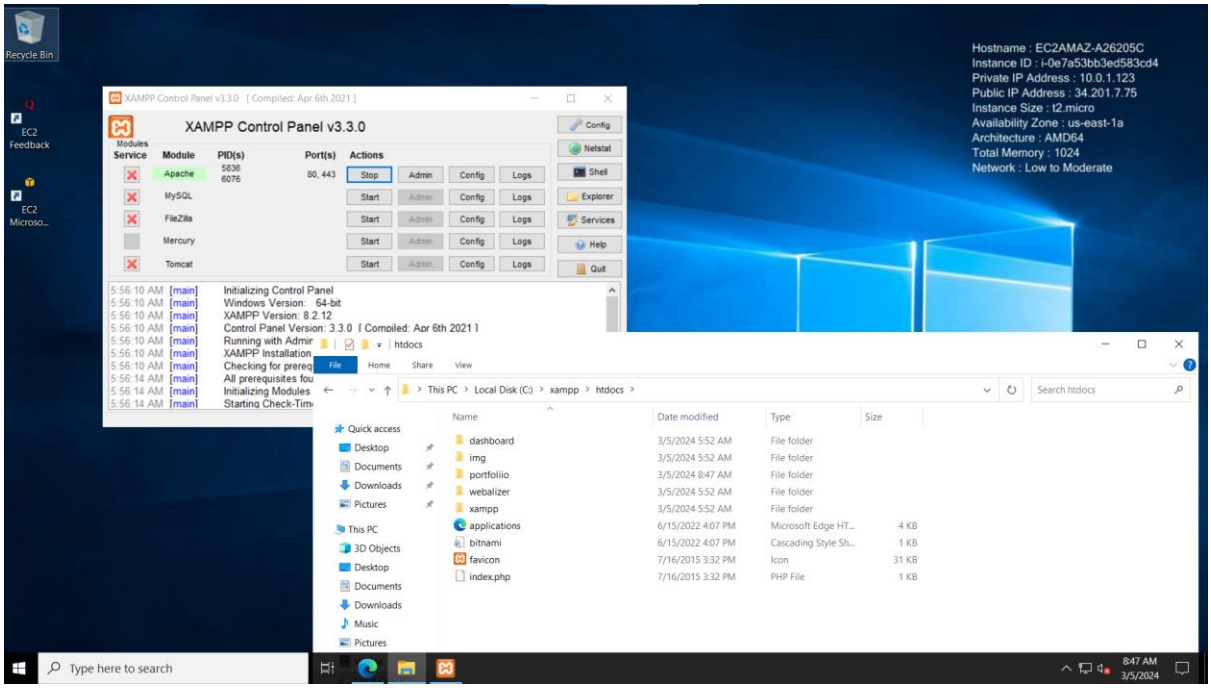



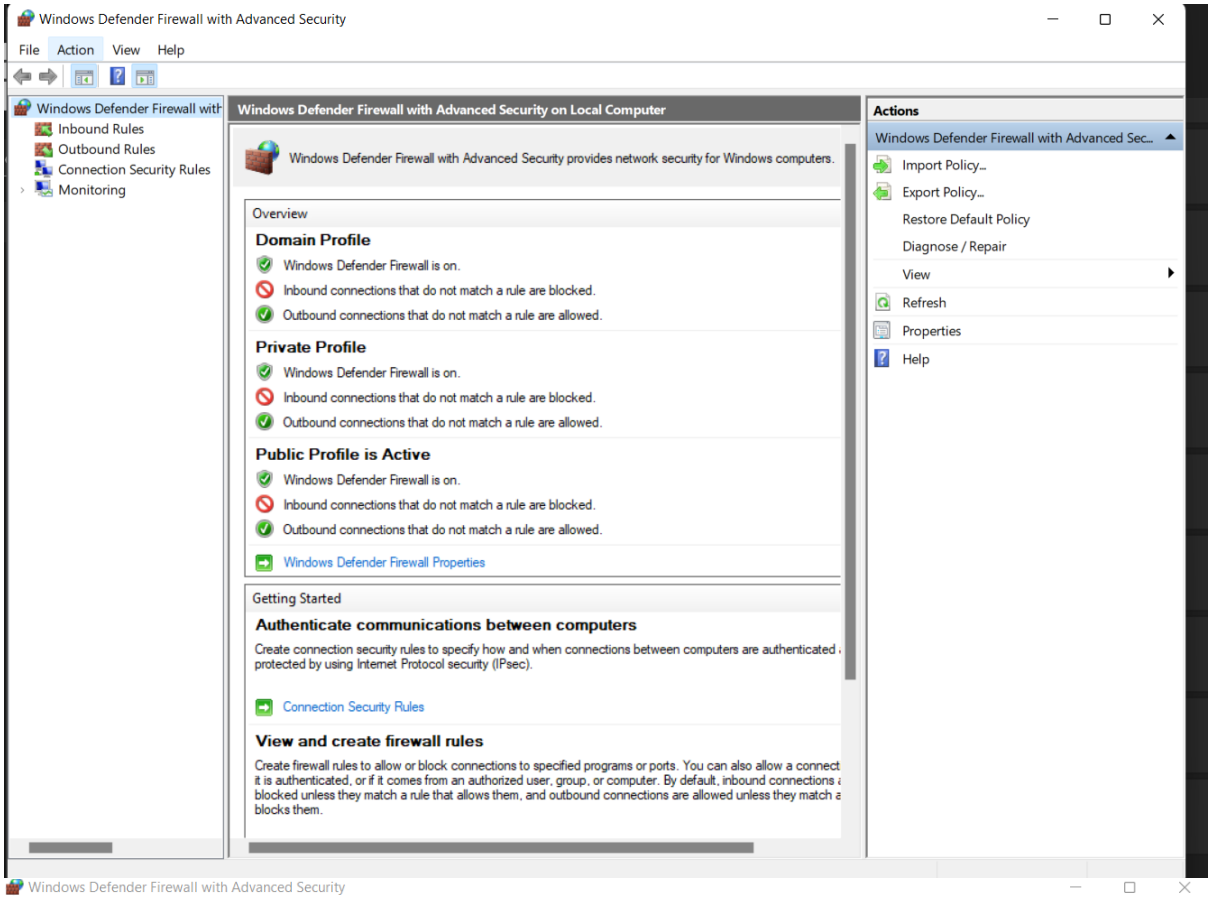

Connect to instance Info
Connect to your instance i-0e7a53bb3ed583cd4 (newwindowinstance) using any of these options
Session Manager
RDP client
EC2 serial console
You may not be able to connect to this instance as ports 3389 may need to be open in order to be accessible. The current associated security groups don't have ports 3389 open.
Instance ID
i-0e7a53bb3ed583cd4 (newwindowinstance)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
Connect using Fleet Manager
with SSM Agent
You can connect to your Windows instance using a remote desktop client of your choice, and by do
running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Public IP
3.216.80.210
Username Info
Administrator
Password
txHqxRNgjNXm0C2P&9;g7670nRCB163h
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel
Remote Desktop Connection
Connecting to:
3.216.80.210
Cancel
Initiating remote connection...

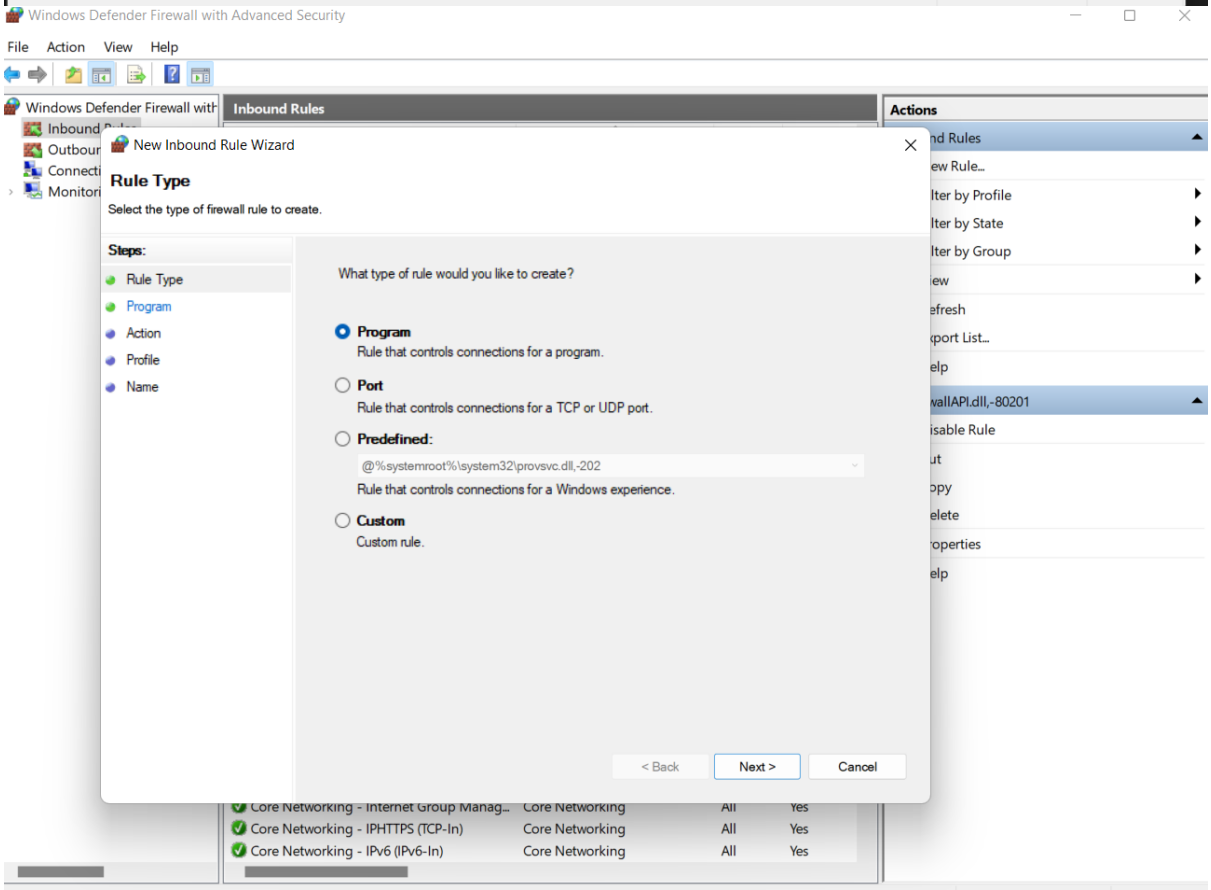

Network settings Info
VPC - required Info
vpc-044e5c7751950bd6f (myVPS)
10.0.0.0/16
Subnet Info
subnet-0ee4c36caf5acd7bc myPublicSubnet
VPC: vpc-044e5c7751950bd6f Owner: 695125708392
Availability Zone: us-east-1a IP addresses available: 250 CIDR: 10.0.1.0/24)
Create new subnet
Auto-assign public IP Info
Enable
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
webservicesecuritygroup sg-07dd7c116c08a5e81
VPC: vpc-044e5c7751950bd6f
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration

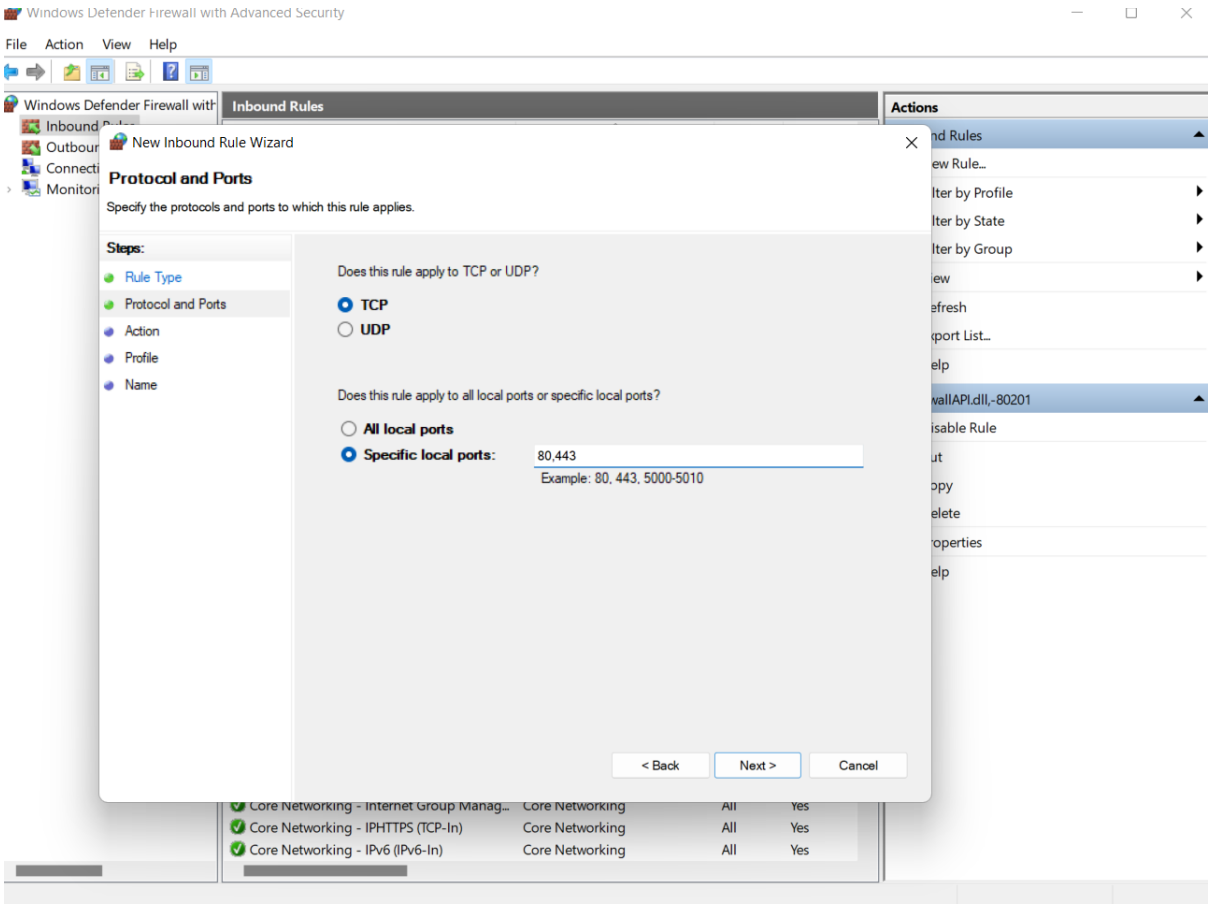

ecuritygroup
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
EC2AMAZ-A26205C
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
IP version
Type
Protocol
Port range
IPv4
SSH
TCP
22
IPv4
RDP
TCP
3389


Recycle Bin
EC2 Feedback
EC2 Microso...
Hostname : EC2AMAZ-A26205C
Instance ID : i-0e7a53bb3ed583cd4
Private IP Address : 10.0.1.123
Public IP Address : 3.216.80.210
Instance Size : t2.micro
Availability Zone : us-east-1a
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate
Type here to search
6:51 AM
2/26/2024

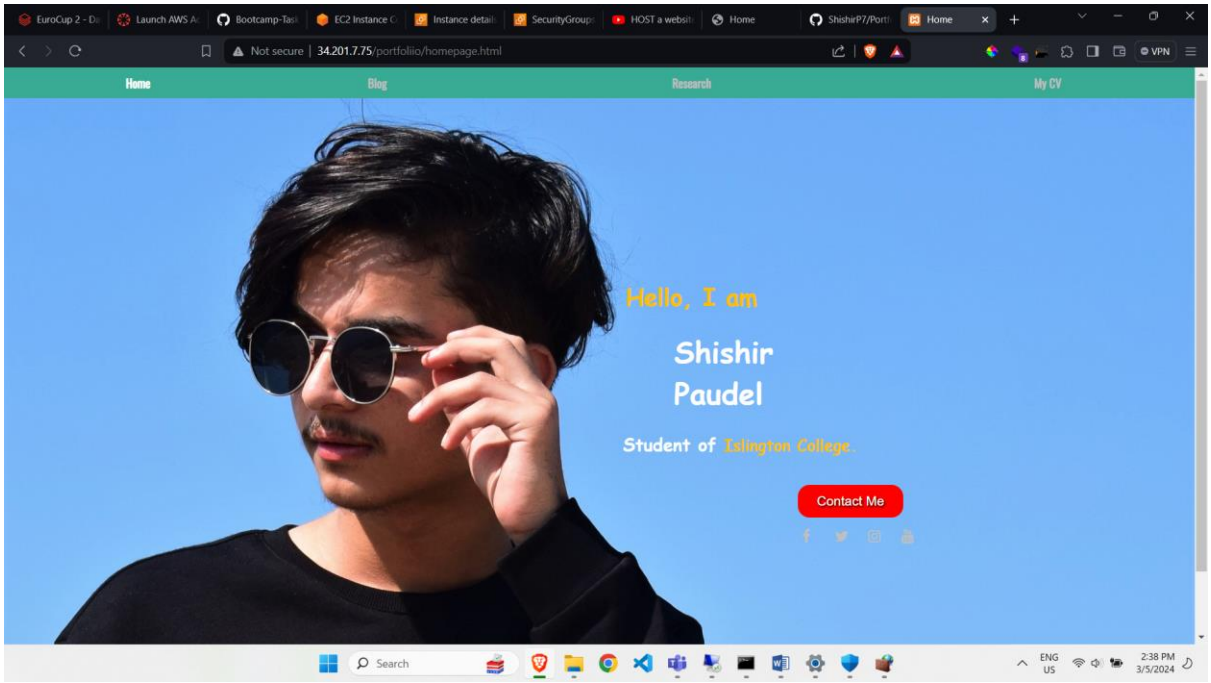

Recycle Bin
EC2 Feedback
EC2 Microso...
Hostname : EC2AMAZ-A26205C
Instance ID : i-0e7a53bb3ed583cd4
Private IP Address : 10.0.1.123
Public IP Address : 34.201.7.75
Instance Size : t2.micro
Availability Zone : us-east-1a
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate
XAMPP Control Panel v3.3.0
Modules
Service Module PID(s) Port(s) Actions
Apache 5836 6076 80, 443 Stop Admin Config Logs
MySQL Start Admin Config Logs
FileZilla Start Admin Config Logs
Mercury Start Admin Config Logs
Tomcat Start Admin Config Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
Initializing Control Panel
Windows Version: 64-bit
XAMPP Version: 8.2.12
Control Panel Version: 3.3.0 [ Compiled: Apr 6th 2021 ]
Running with Admin rights
XAMPP Installation directory: "c:\xampp\"
Checking for prerequisites
All prerequisites found
Initializing Modules
Starting Check-Timer
htdocs
File Home Share View
This PC > Local Disk (C:) > xampp > htdocs >
Search htdocs
Quick access
Desktop
Documents
Downloads
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Name Date modified Type Size
dashboard 3/5/2024 5:52 AM File folder
img 3/5/2024 5:52 AM File folder
portfoliio 3/5/2024 8:47 AM File folder
webalizer 3/5/2024 5:52 AM File folder
xampp 3/5/2024 5:52 AM File folder
applications 6/15/2022 4:07 PM Microsoft Edge HT... 4 KB
bitnami 6/15/2022 4:07 PM Cascading Style Sh... 1 KB
favicon 7/16/2015 3:32 PM Icon 31 KB
index.php 7/16/2015 3:32 PM PHP File 1 KB
Type here to search
8:47 AM
3/5/2024


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connect
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections
blocked unless they match a rule that allows them, and outbound connections are allowed unless they match
blocks them.
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
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:
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
Actions
Core Networking - Internet Group Manag... Core Networking All Yes
Core Networking - IPHTTPS (TCP-In) Core Networking All Yes
Core Networking - IPv6 (IPv6-In) Core Networking All Yes




Then check the public ip




The website is hosted successfully.