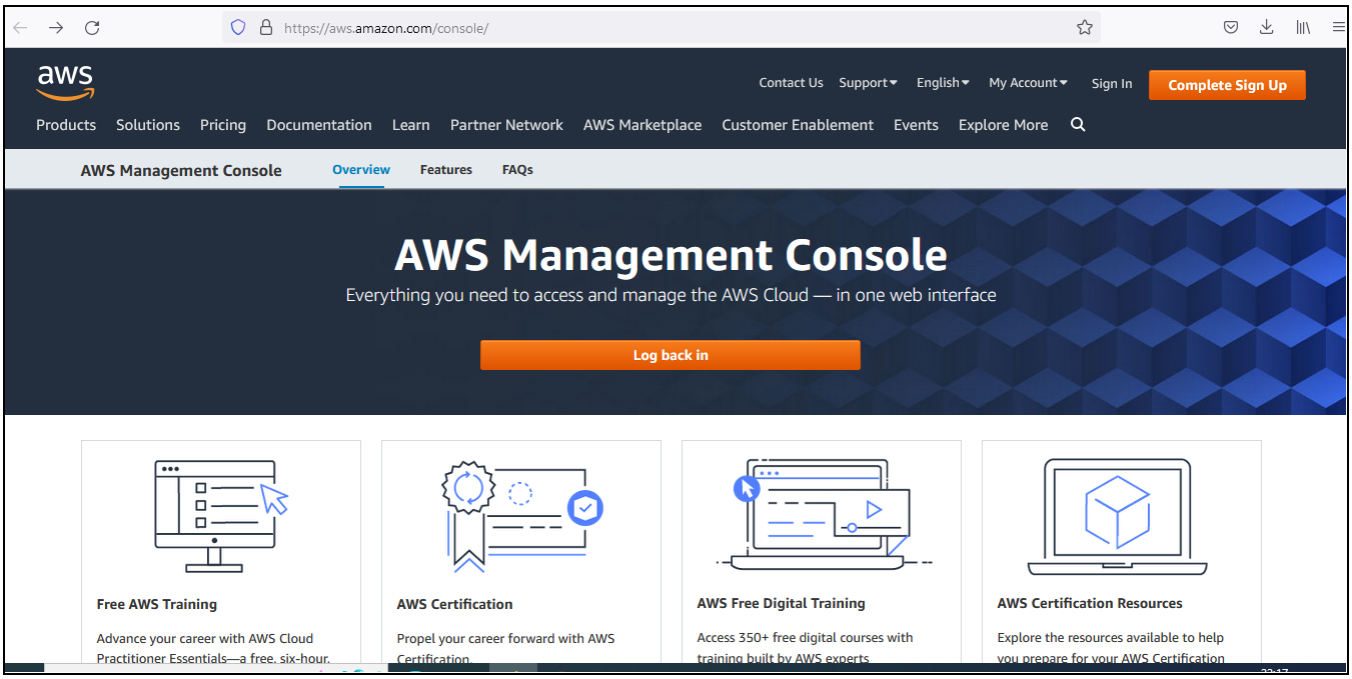
AWS Cloud Practice - Part 1

CLOUD COMPUTING TEAM
CDAC
CHENNAI

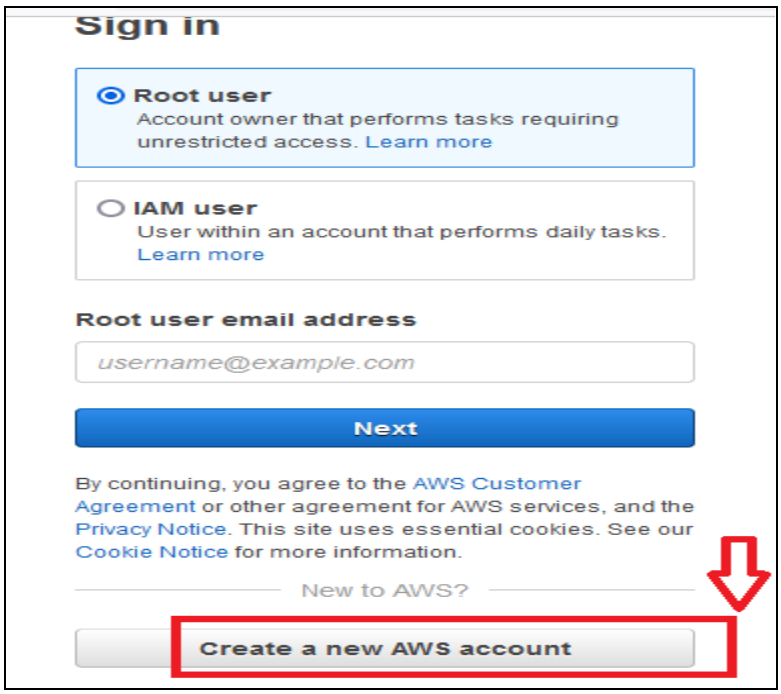
Table of Contents

AWS Management Console

Step:1 Login to the Console : https://aws.amazon.com/console Click Sign In to the Console



Step2: Sign Up as the first time user by clicking the **Create a new AWS account.**



Step 3: Verify email address

aws

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

Root user email address
Used for account recovery and some administrative functions

prabhav@cdac.in

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

Prabhasathesh

Verify email address

OR

Sign in to an existing AWS account

aws

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

Confirm you are you

Making sure you are secure -- it's what we do.

We sent an email with a verification code to **maruthicarstudio@gmail.com**. (not you?)

Enter it below to confirm your email.

Verification code

361421

Verify

Resend code

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.

Always free
Never expires

12 months free
Start from initial sign-up date

Trials
Start from service activation date

Sign up for AWS

Contact Information

How do you plan to use AWS?

- ○ Business - for your work, school, or organization
- ◉ Personal - for your own projects

Who should we contact about this account?

Full Name
Sathesh

Phone Number
Enter your country code and your phone number.
91-9999999999

Country or Region
India

City
Chennai

State, Province, or Region
TamilNadu

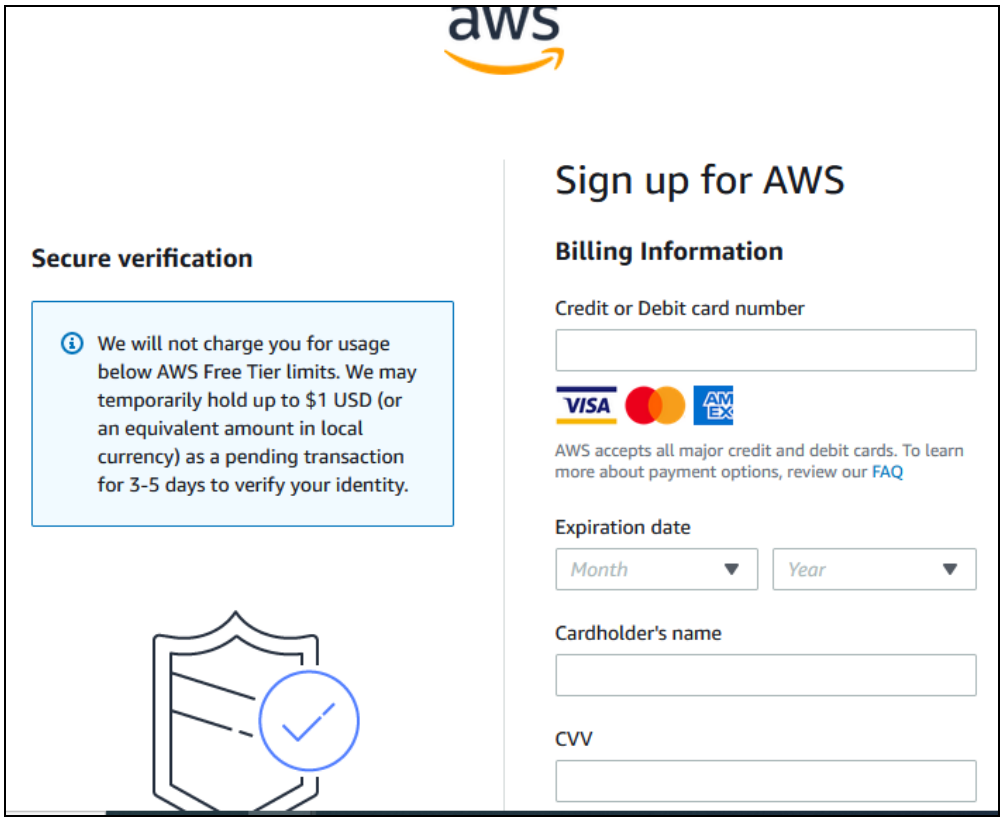
Postal Code
600100

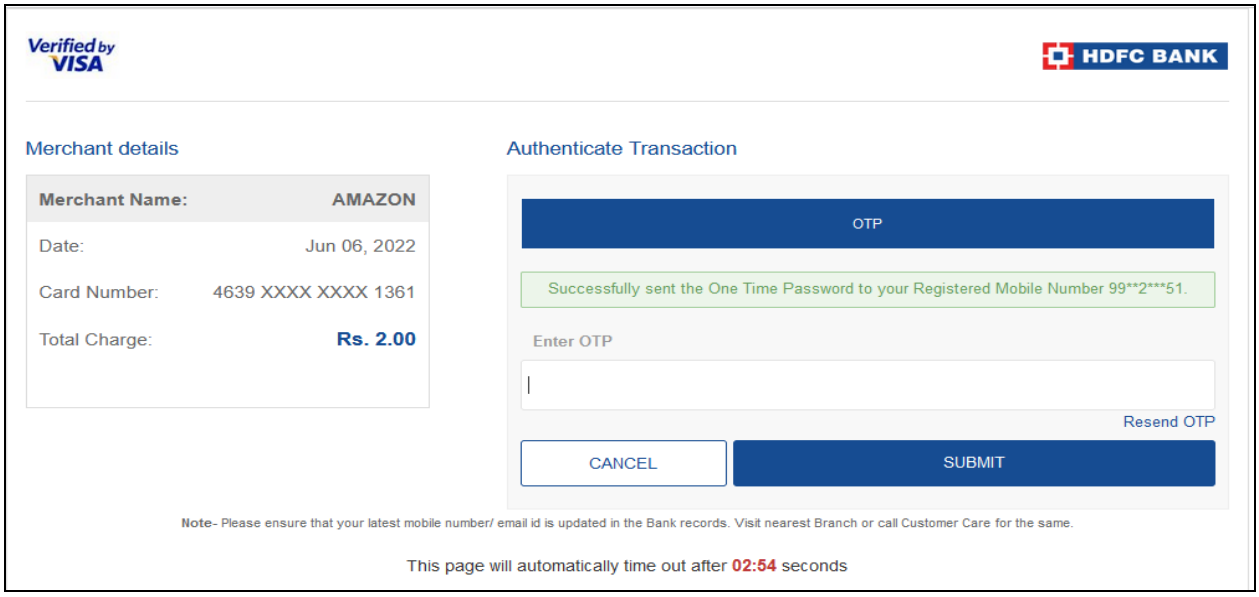
Customers with an Indian contract address are served by Amazon Internet Services Private Ltd. (AISPL). AISPL is the local seller for AWS services in India.

☐ I have read and agree to the terms of the AWS Customer Agreement.

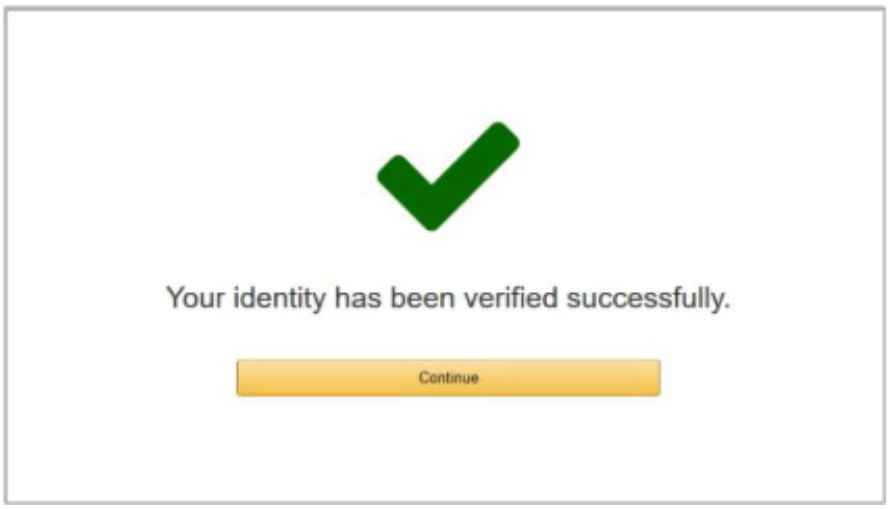
Continue (step 2 of 5)

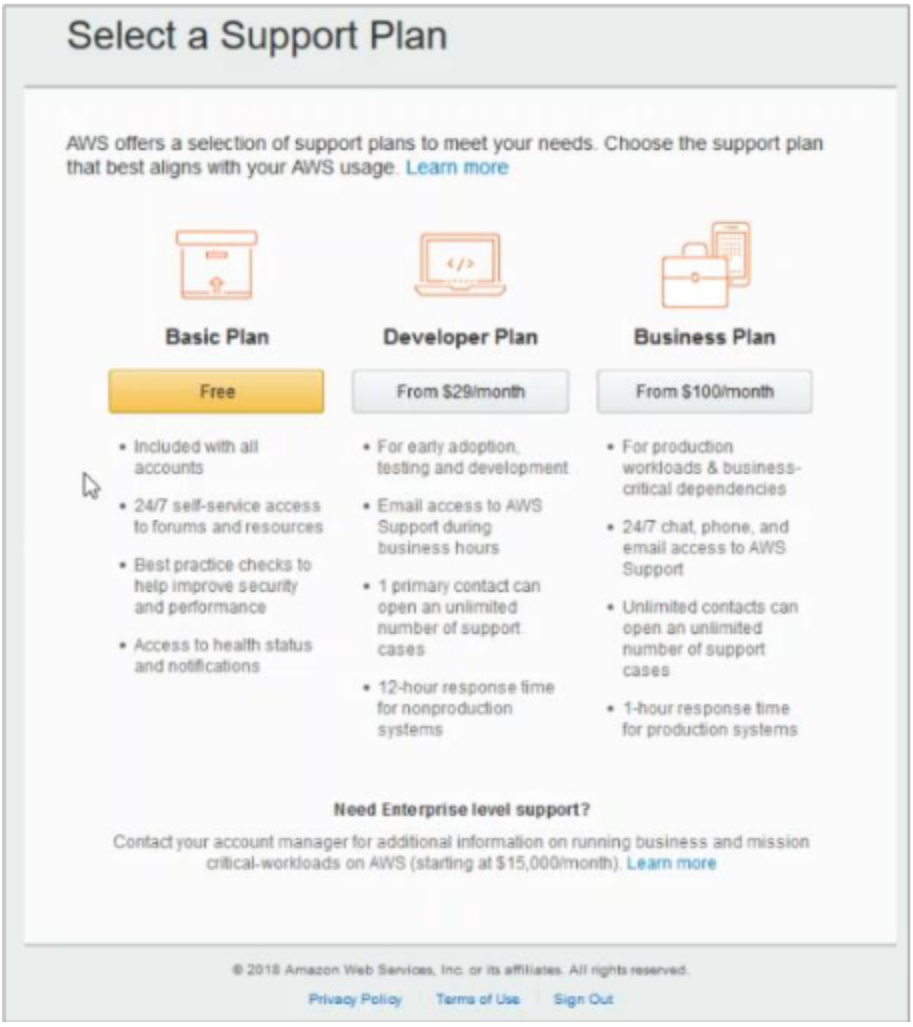
Step 4: Give the credit card details correctly, Card Number, Expiry Date and Card Holder Name. Click on Secure Submit



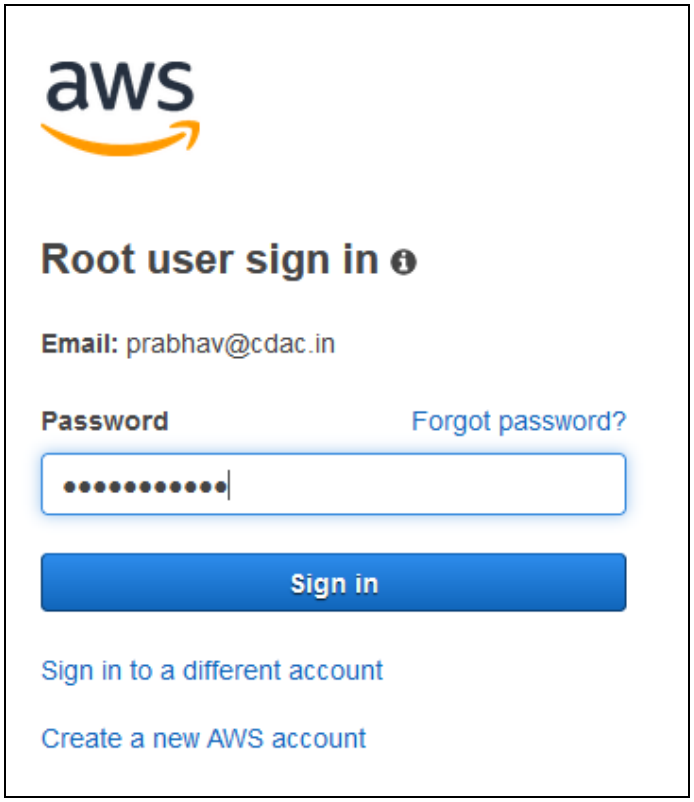


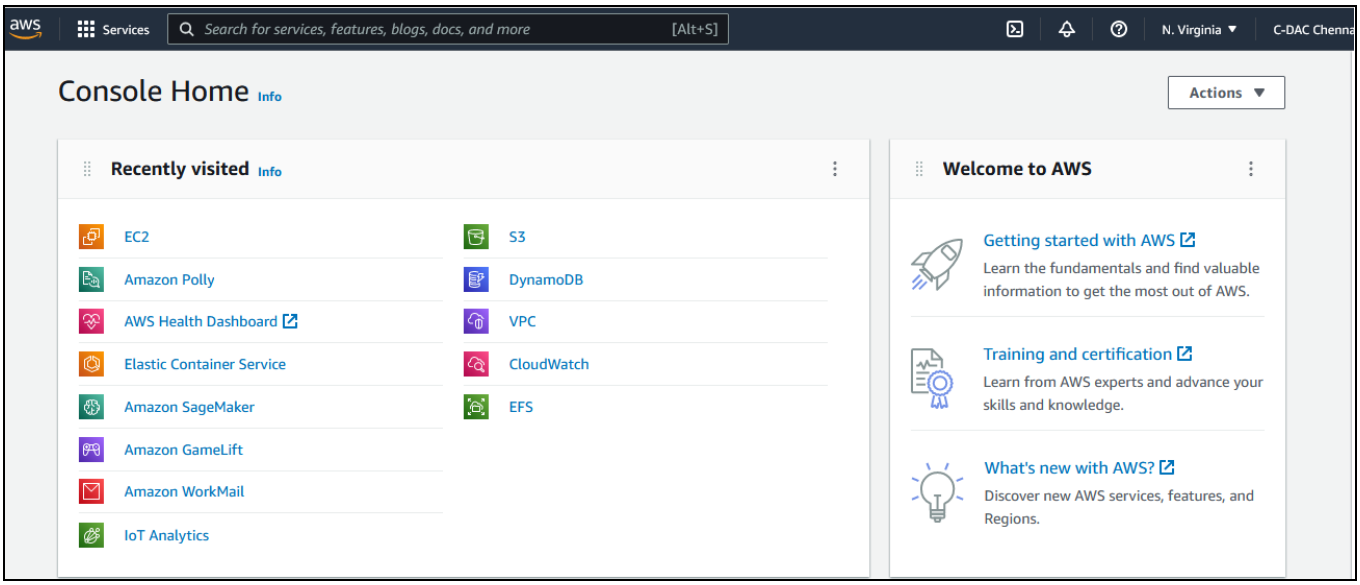
Step 5: After successful verification,Select the Support plan as Basic Plan (Free)





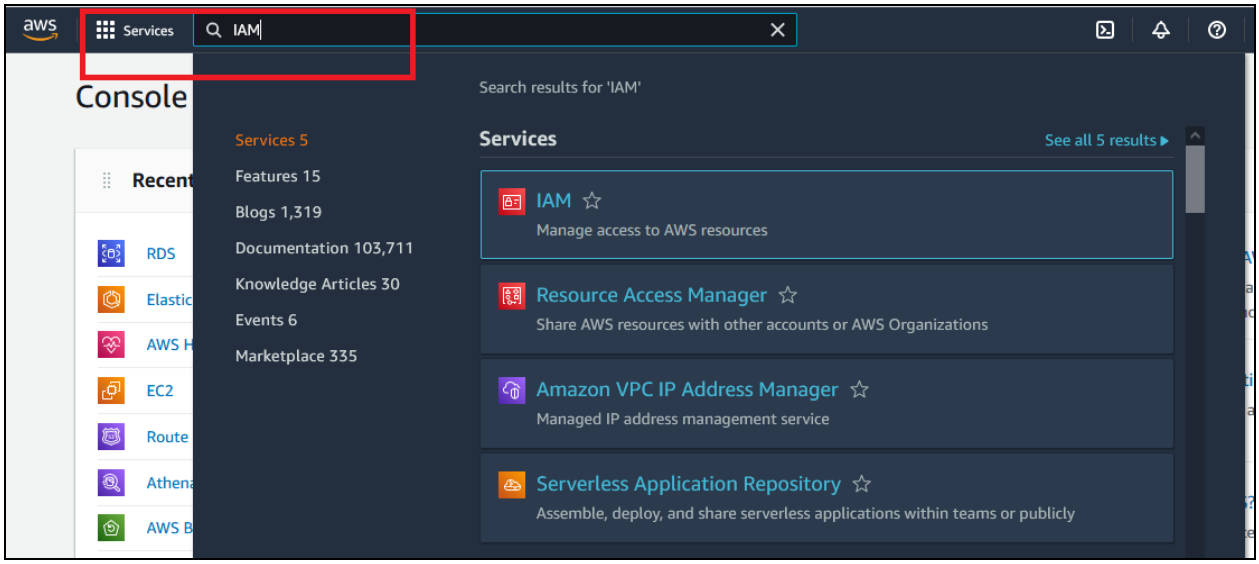
Step 6: Once account is created, login using the credentials



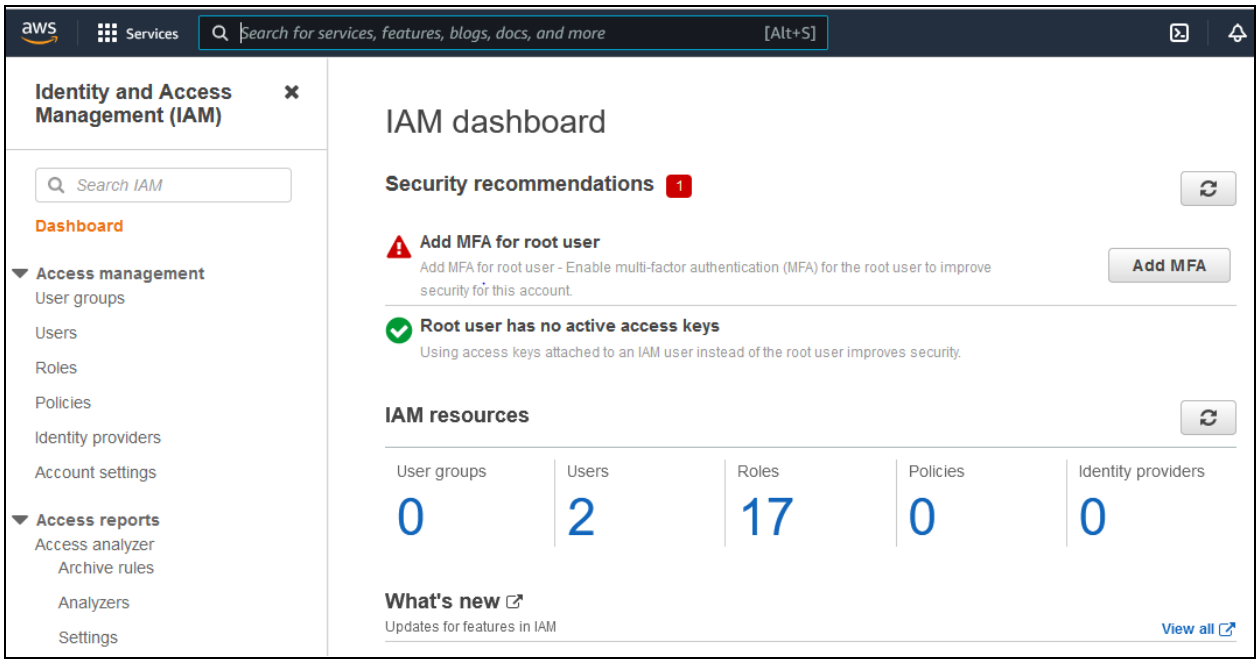


Identity and Access Management (IAM)

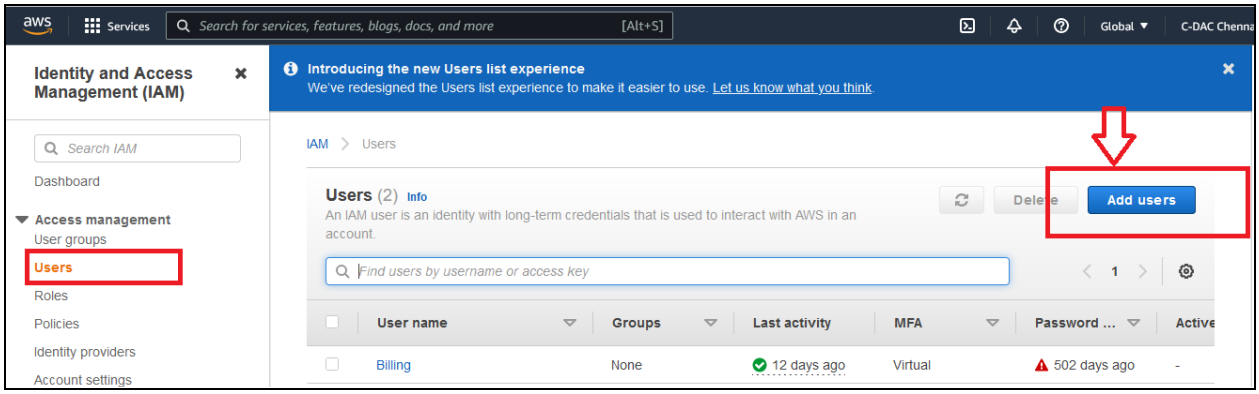
Step 7 - Search IAM in Services

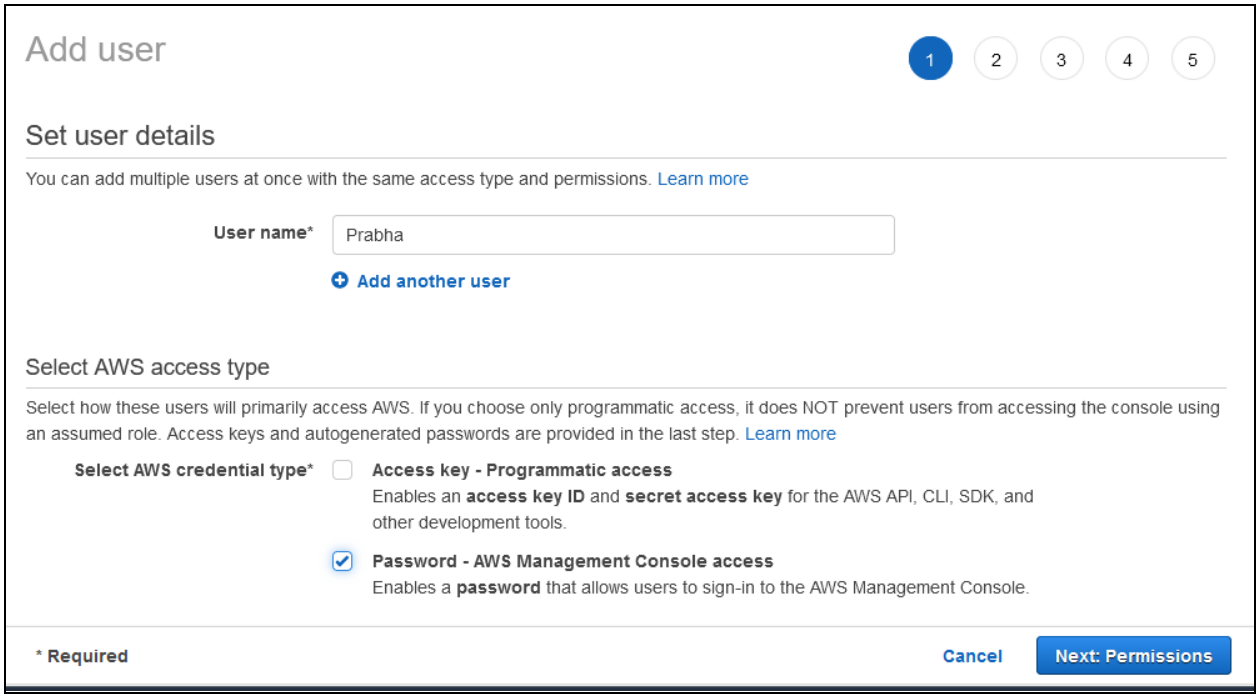


Step 8 - Create Users, Roles and Policies using IAM dashboard

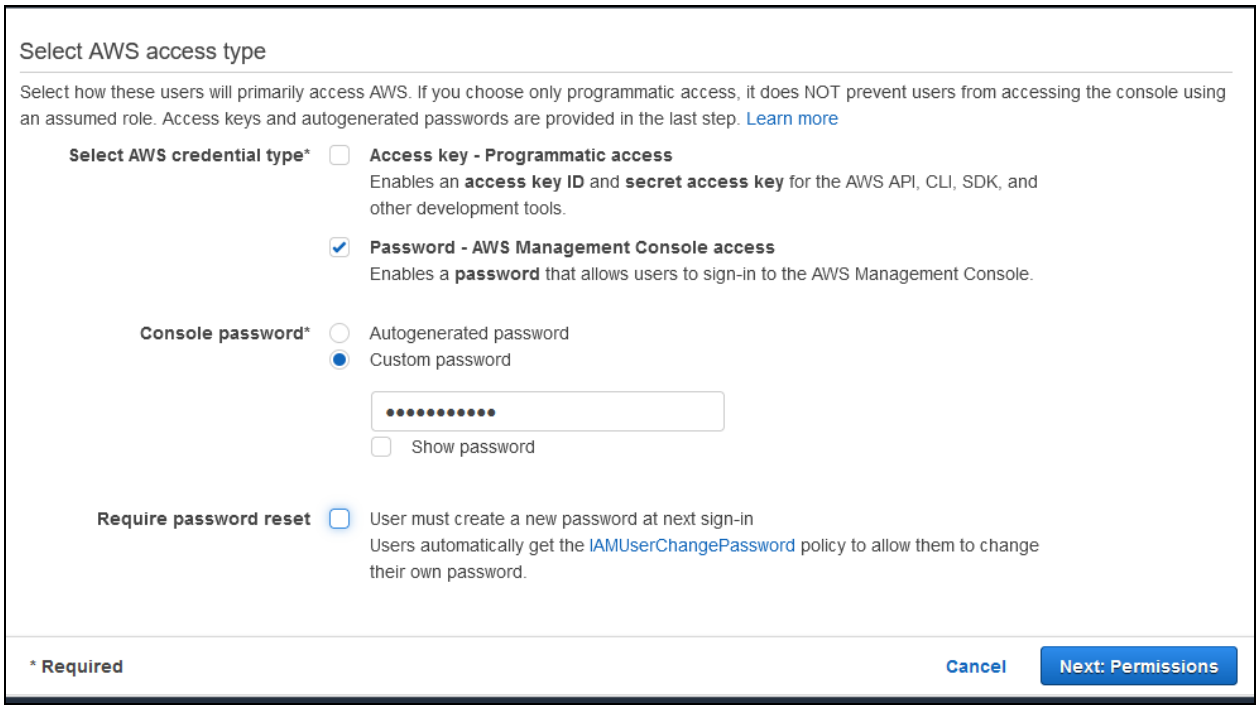


Step 9: To create new user- Select Users → Add users

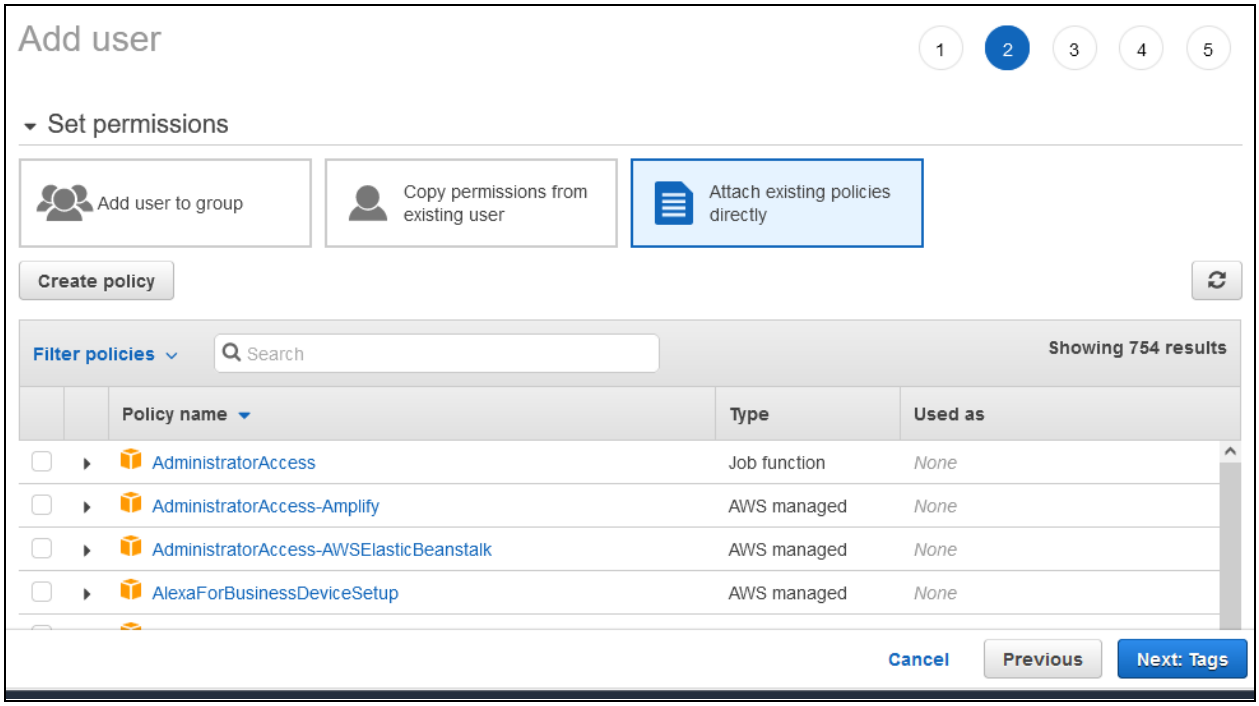




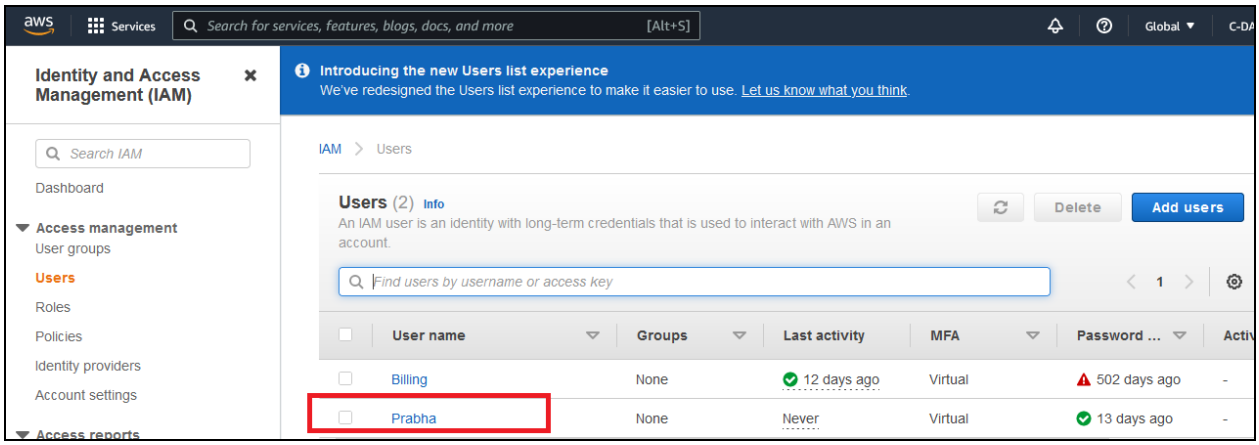
Step 10: Select AWS credential type as Password and create a custom password



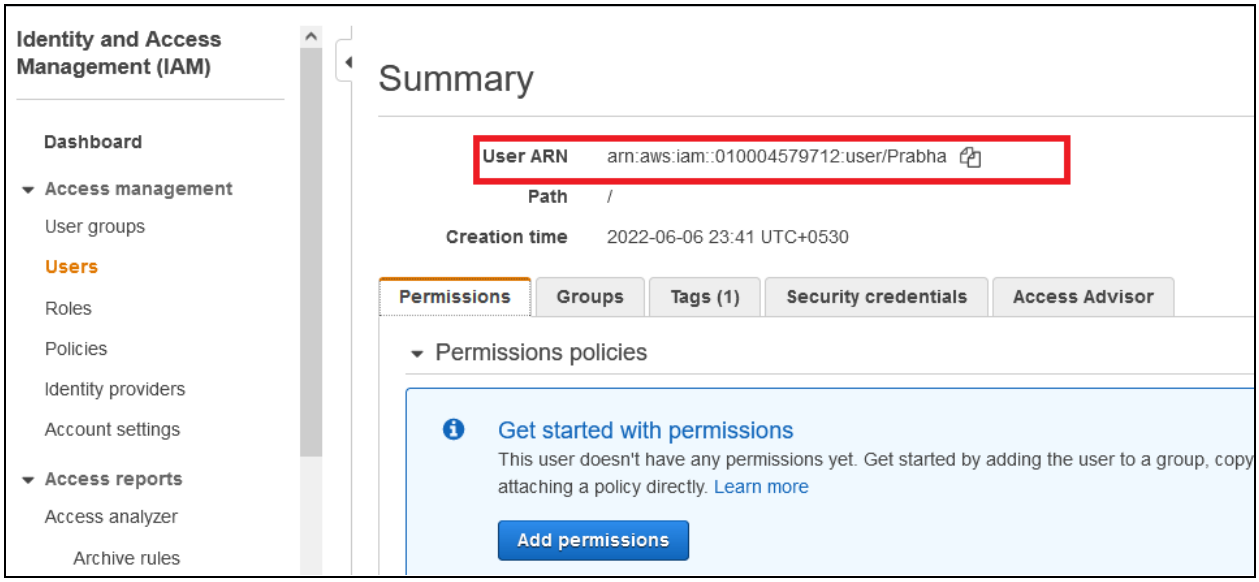
Step 11: Attach policy to the newly created user



Step 12: View the newly created user

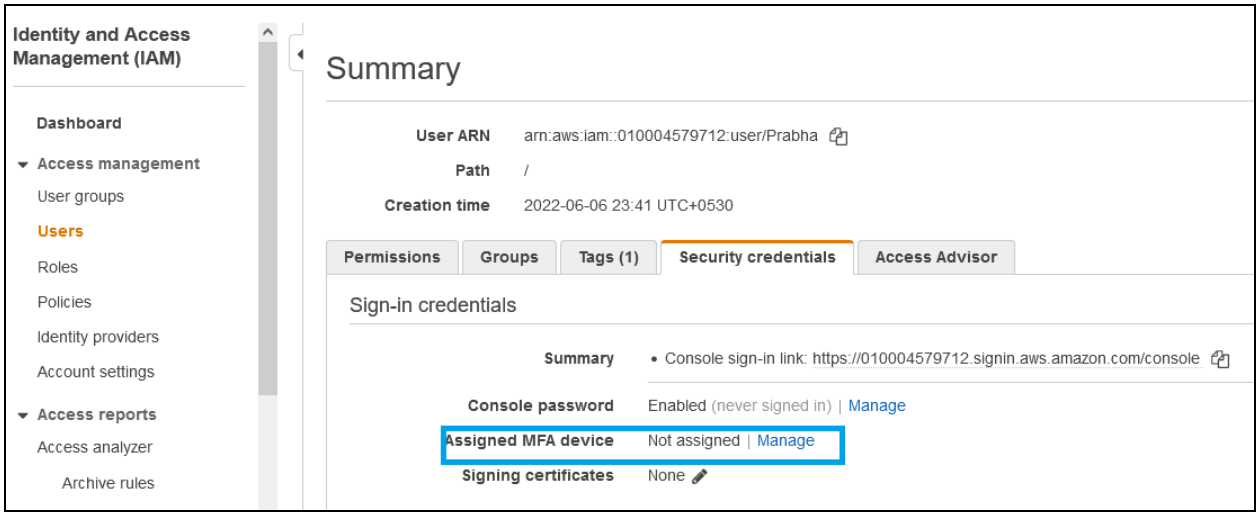


User creation has been completed successfully now you will get an access URL with your account number. Note the URL for access

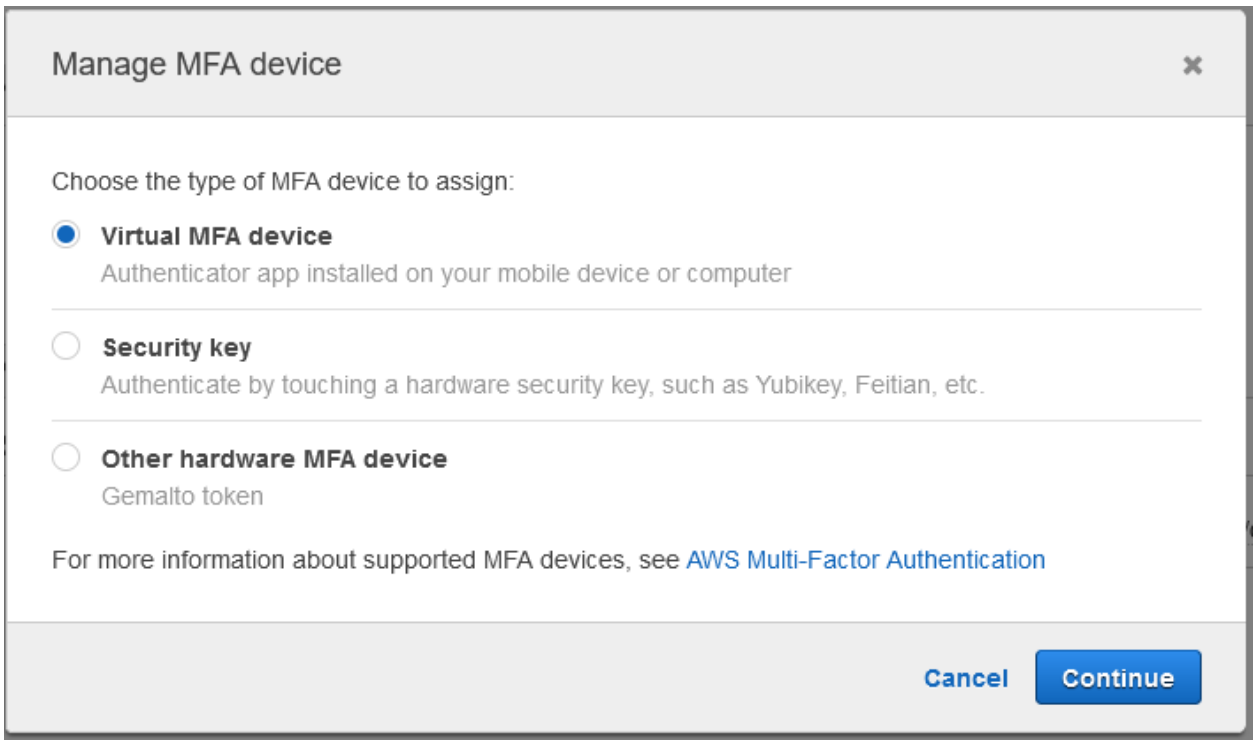


Multi-factor Authentication creation

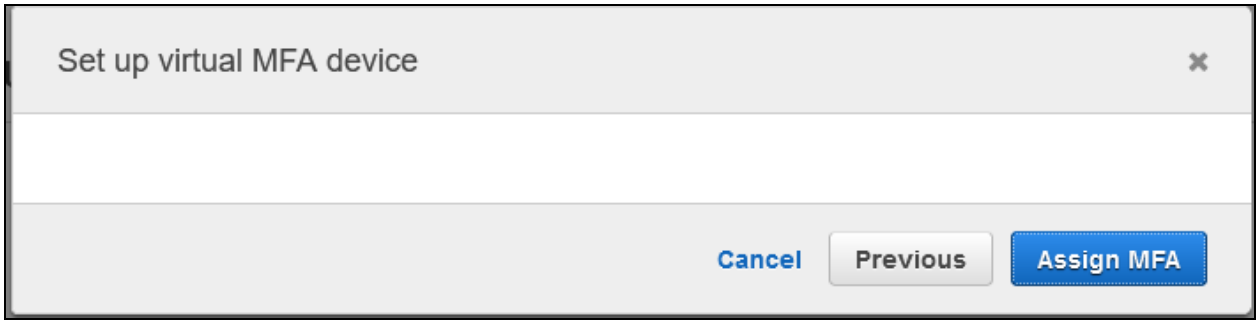
Step 13: View the newly created user

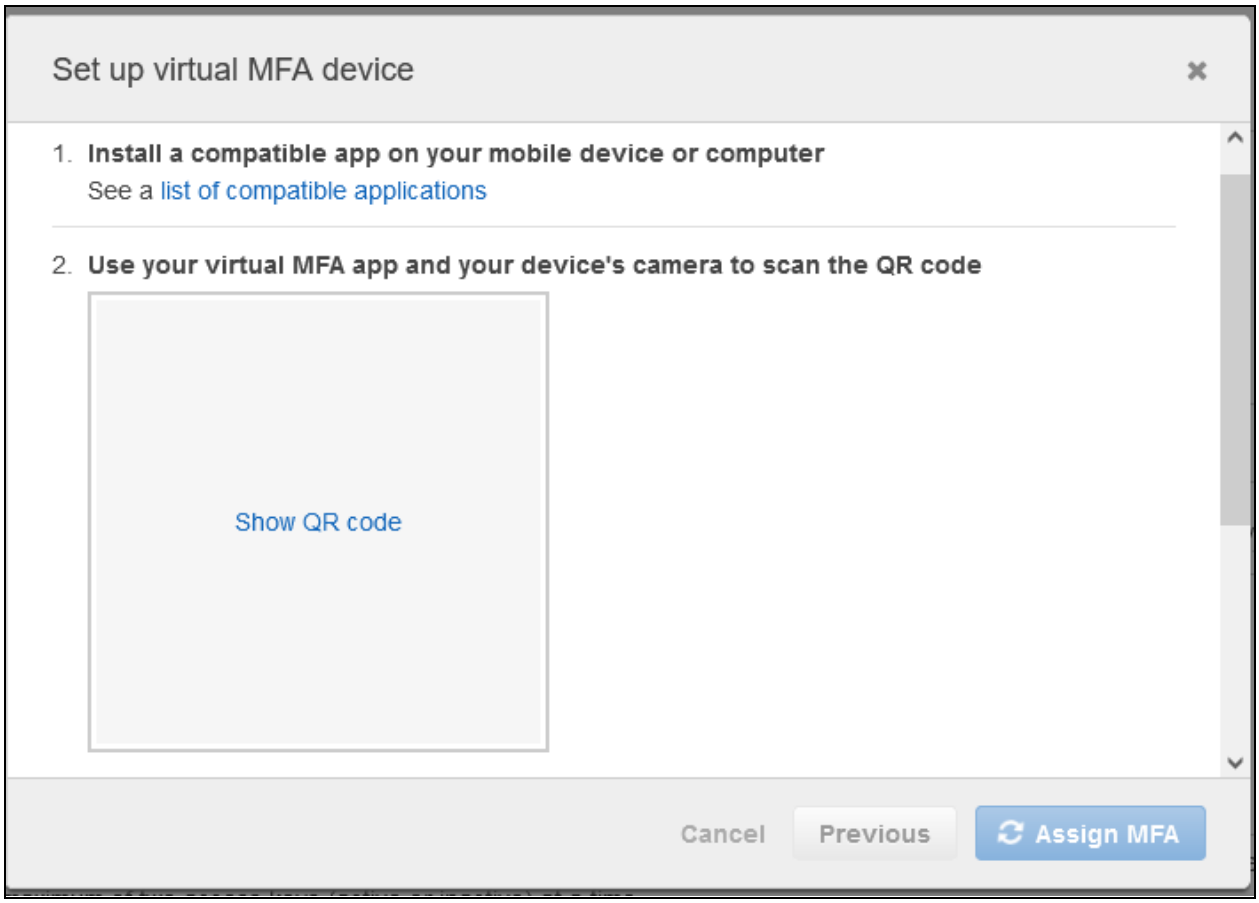


Step 14: Install Google Authenticator in smart phone and ready to pair. Click Continue in Manage MFA device



Step 15: Click Assign MFA in Setup Virtual MFA device

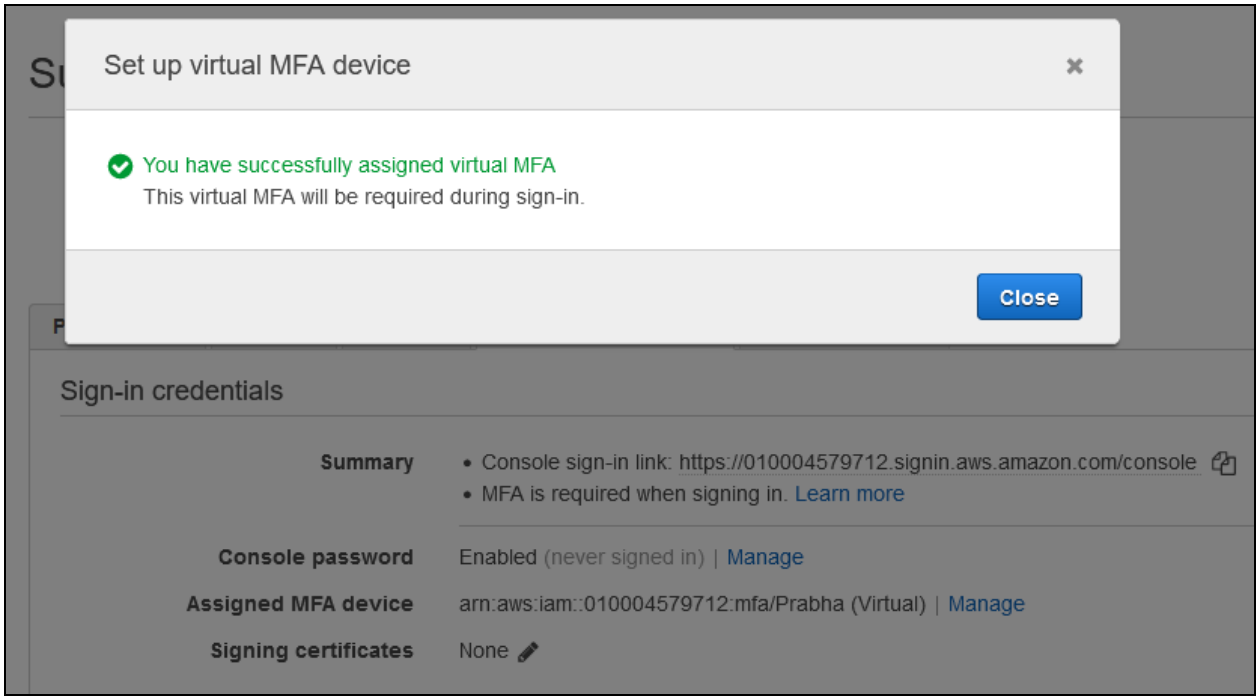




Step 16: Click in Show QR Code and scan the same code from your Google authenticator App. It will generate six digit codes enter one code in first MFA code 1 wait 1 minute and second code in MFA Code 2 Click on Assign MFA

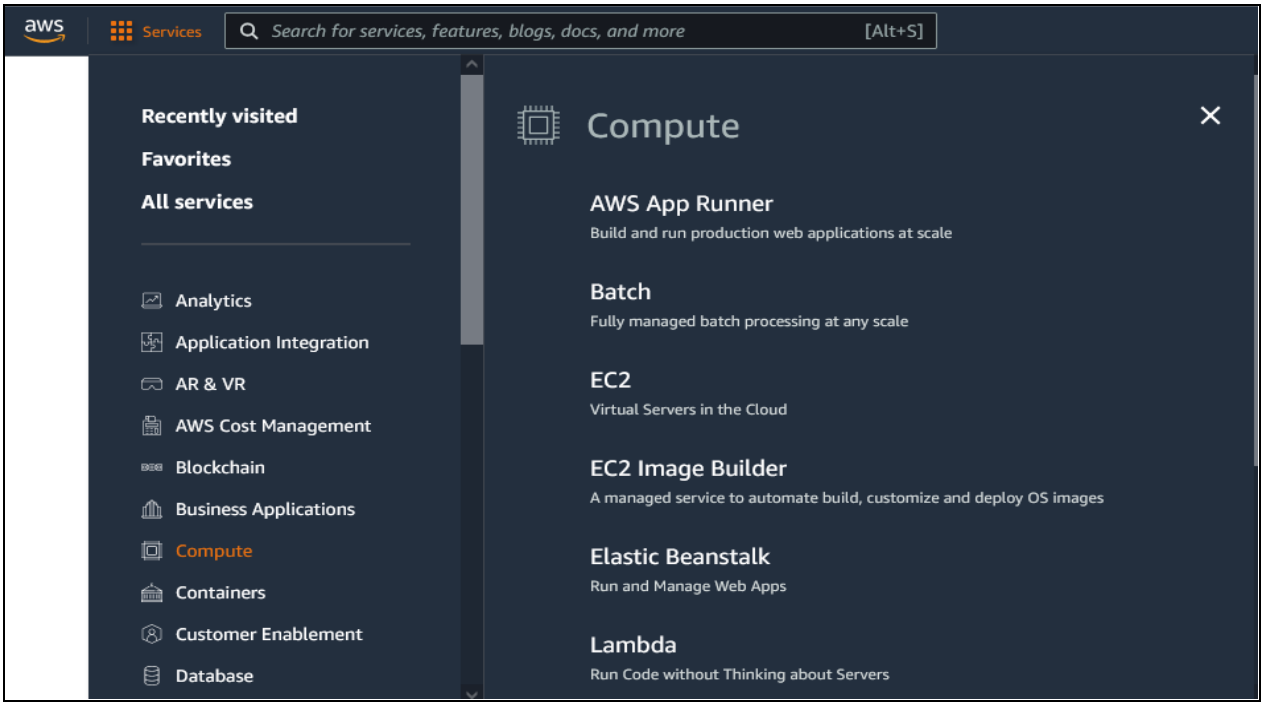
That's it, now you successfully enabled MFA (Multi-Factor Authentication).

Hereafter if you want to login, you have to enter credentials and MFA code to Login.

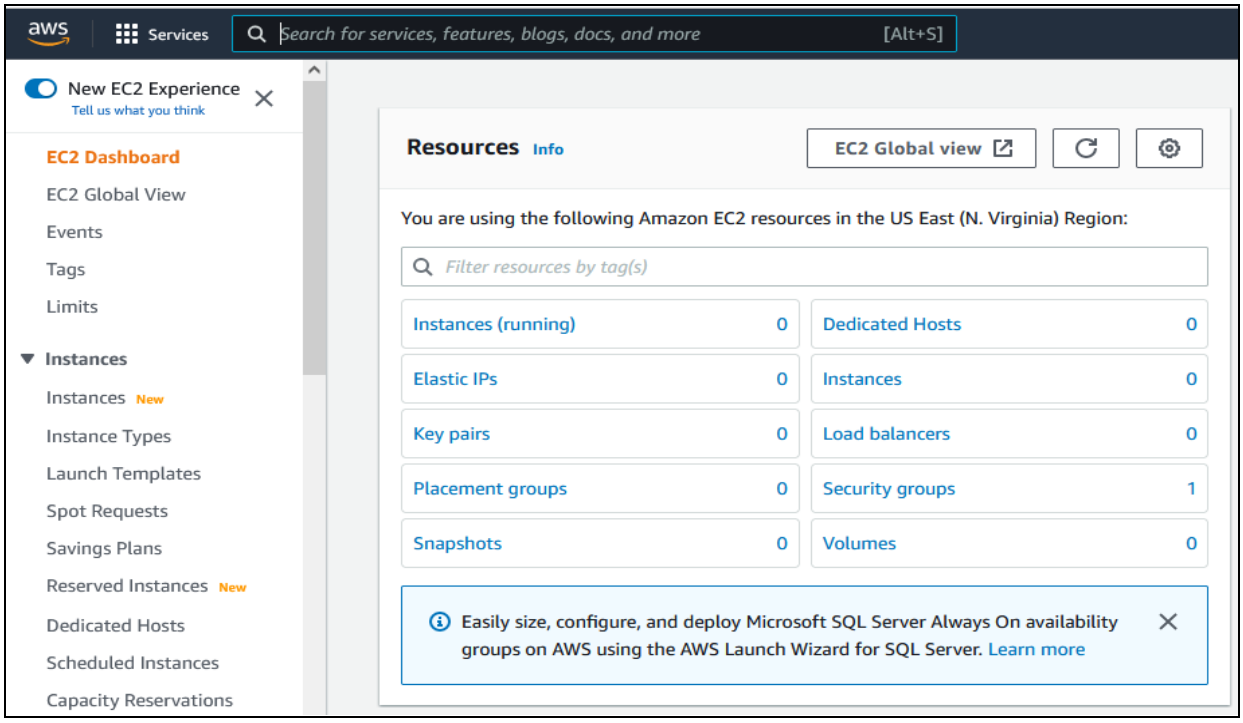


Launching of first EC2 instance

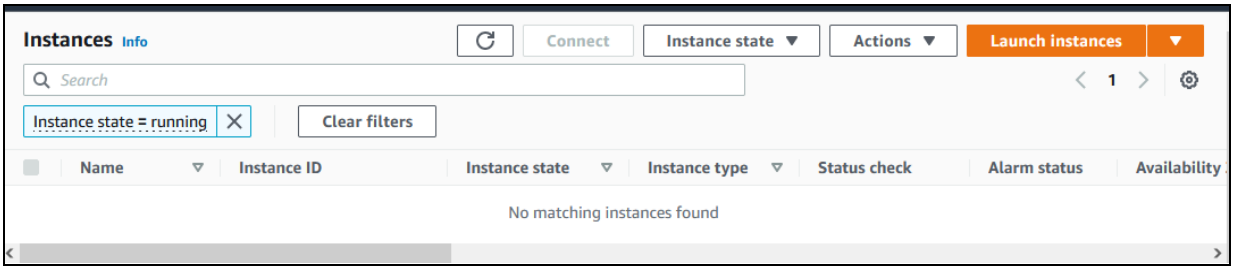
Step 17: Go to Services drop down click on Compute → EC2



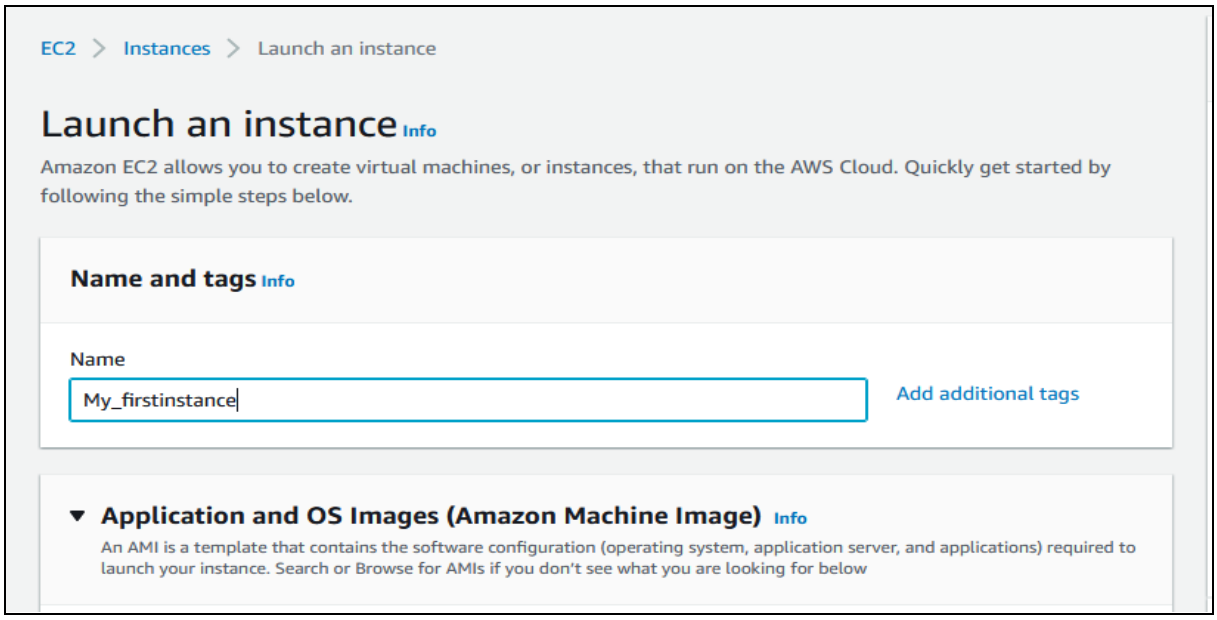
Step 18: Resource provides an overview of the Compute → EC2



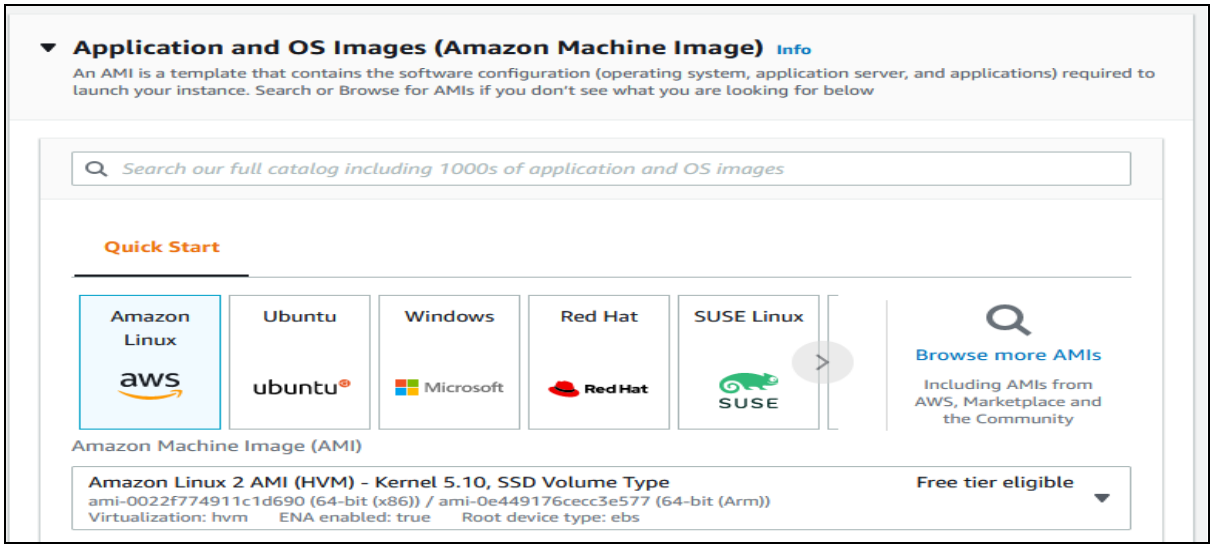
Step 19: Go to Instances → Launch Instances



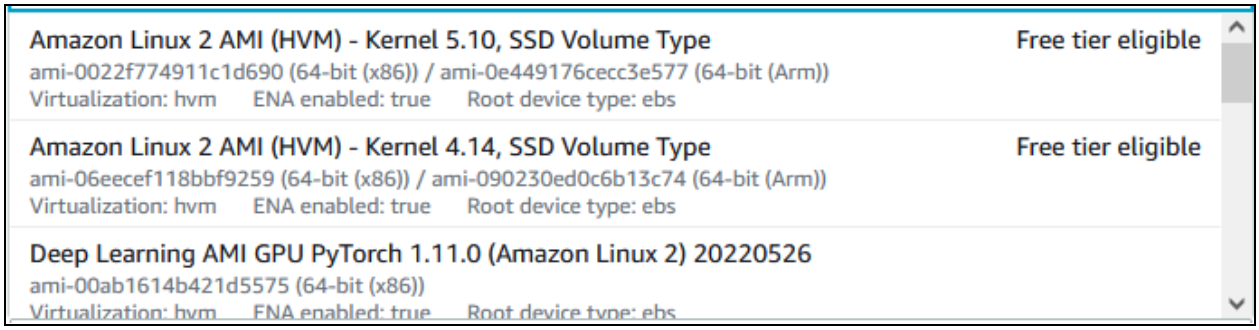
Step 20: Provide a Name to the instance

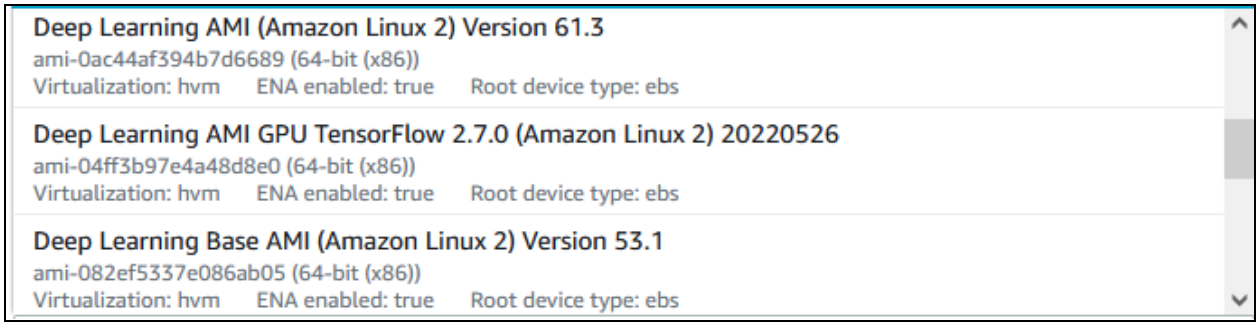


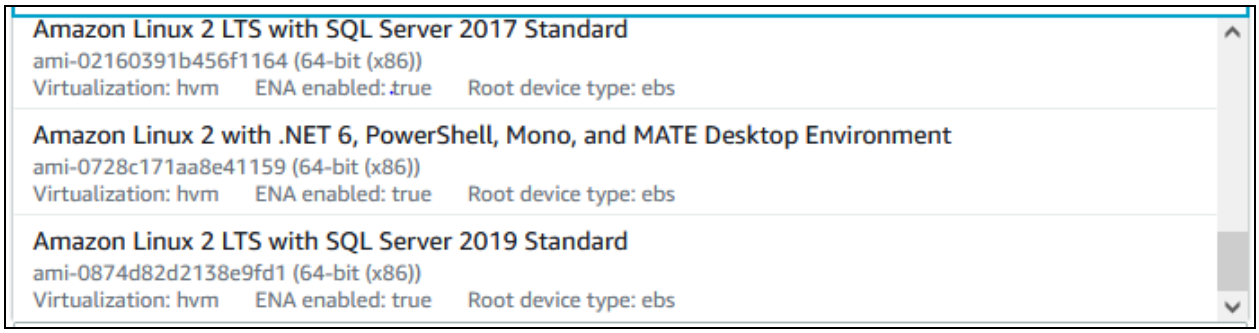
Step 21: Select the Image from the List



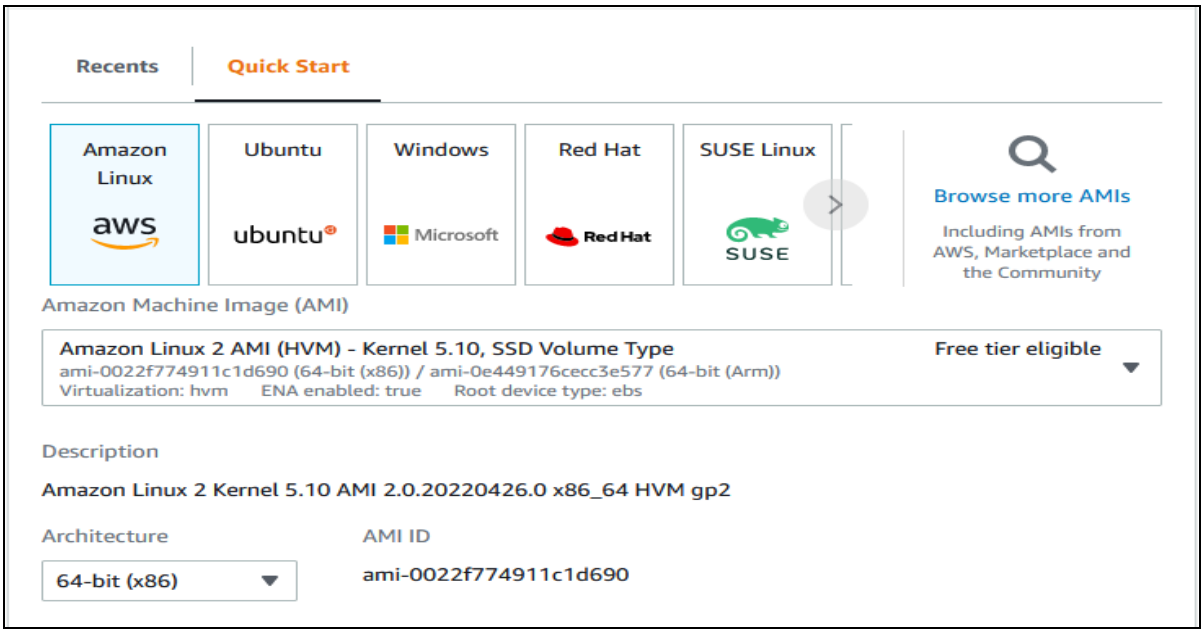
Step 22: Select the AMI Flavors (free tier) that suits the requirement



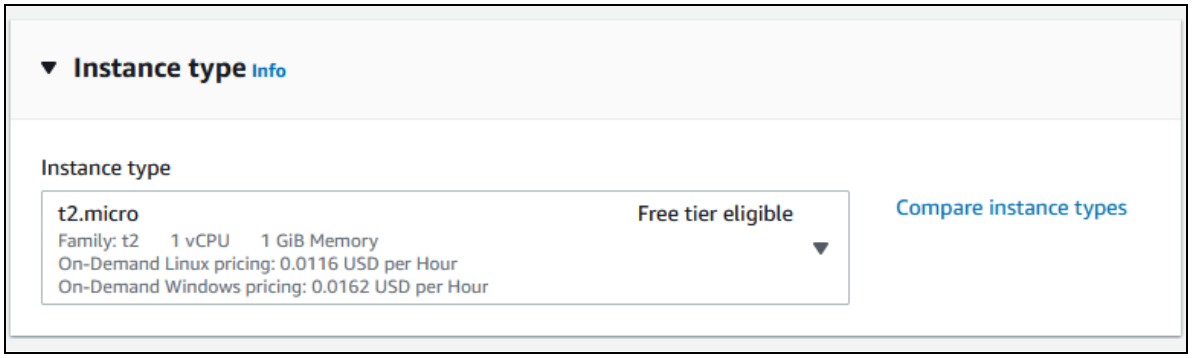




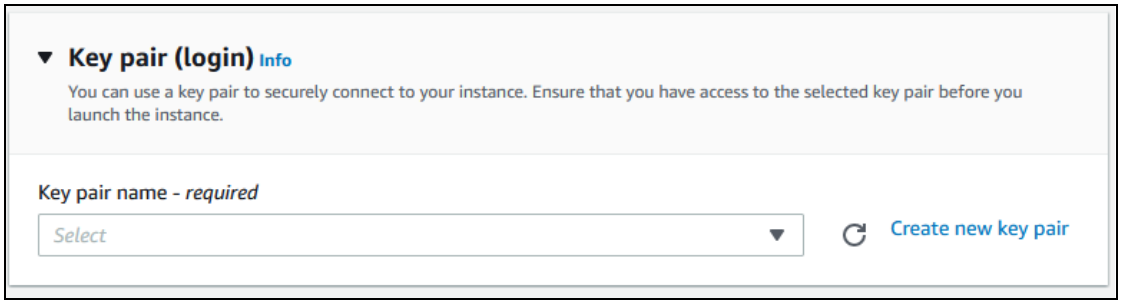
Step 23: Select the Amazon Linux Image with Free tier eligible



Step 24 : Select the Instance Flavor in free tier eligible

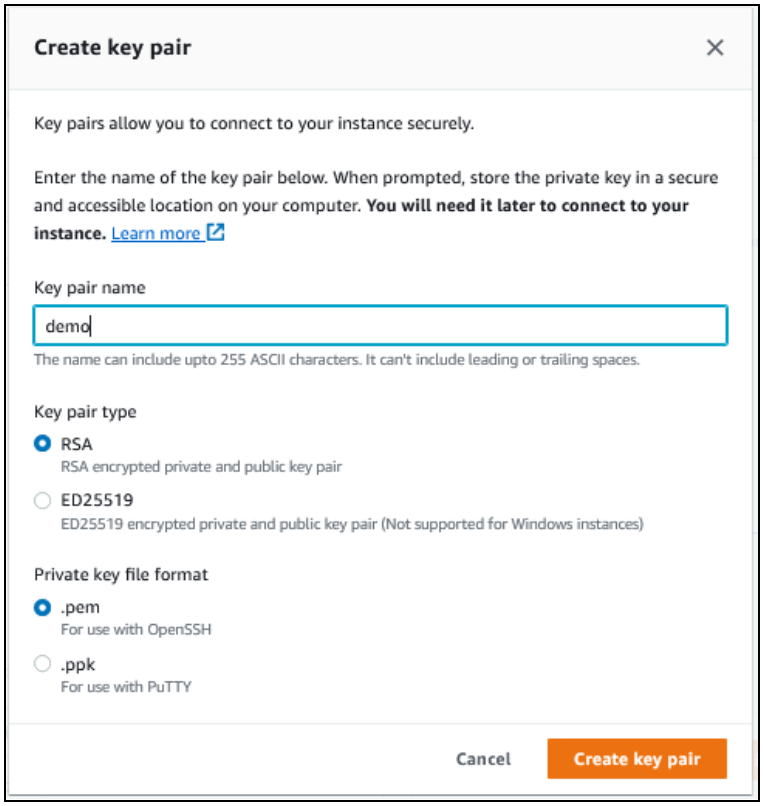


Step 25 : Select the Key pair (already existing) to login the instances using the SSH key pair. If no existing key pair Click on Create new key pair

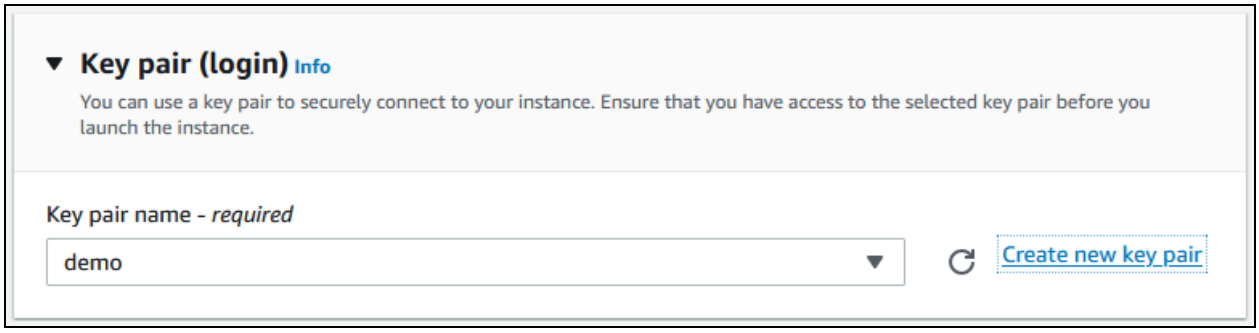


Step 26 : Create a Key pair name with preferred type as RSA(RSA private key cryptographic algorithm) and Private key file format as .pem.

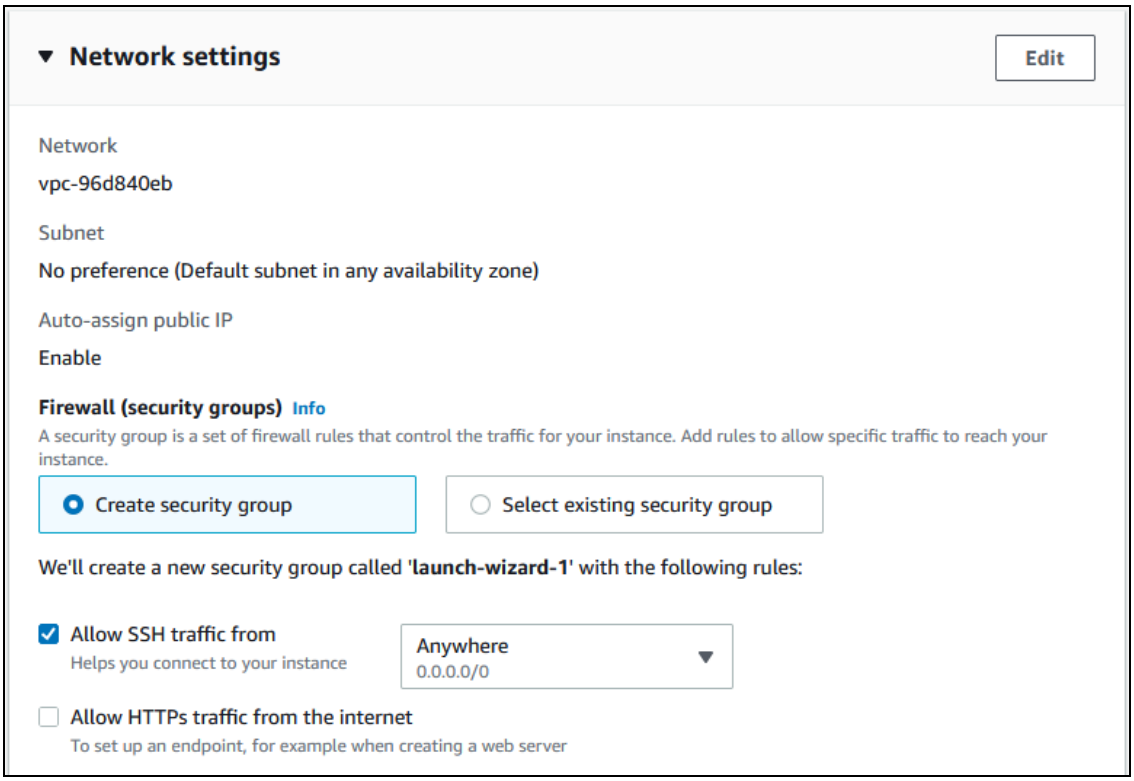
Note : Download the private key file (demo.pem) and keep it safe. If the key is lost, then the VM becomes inaccessible.



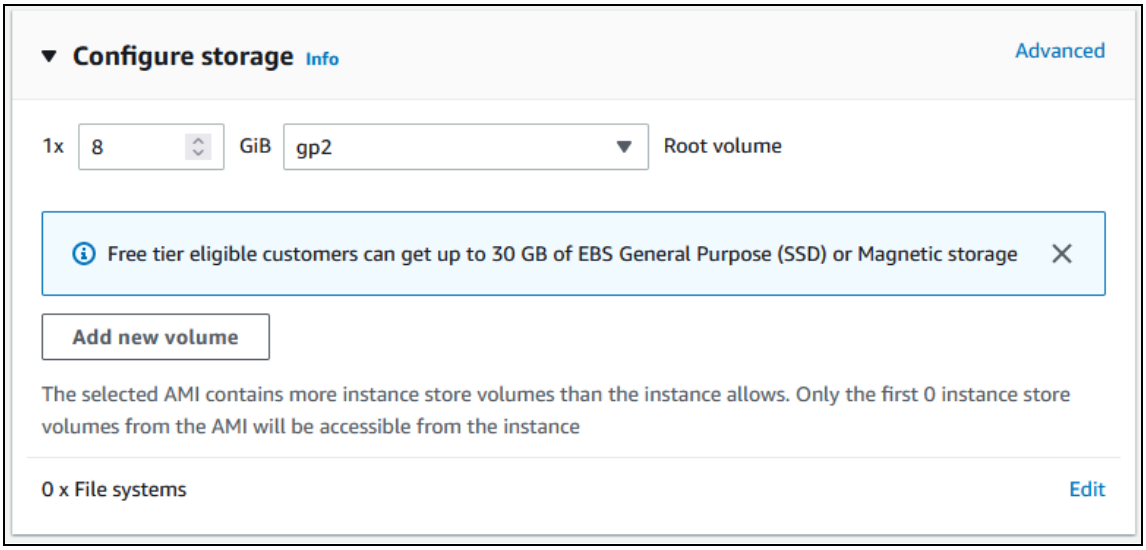
Step 27 : Use the created key pair

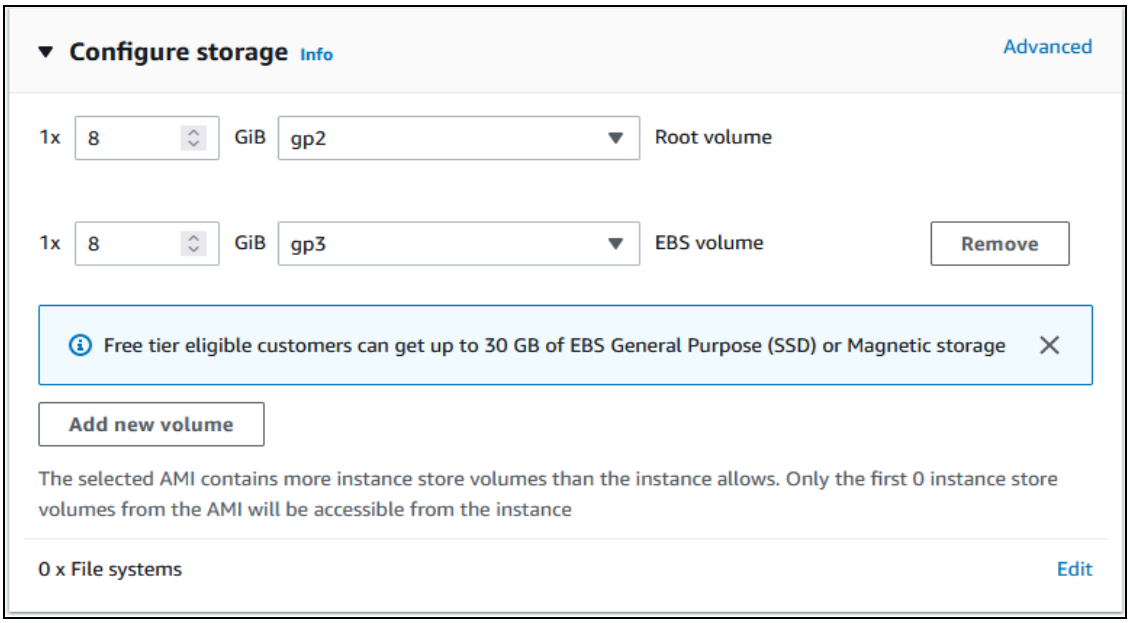


Step 28: A default VPC Network is created. Create Security Groups for Firewall policies that create inbound and outbound connections

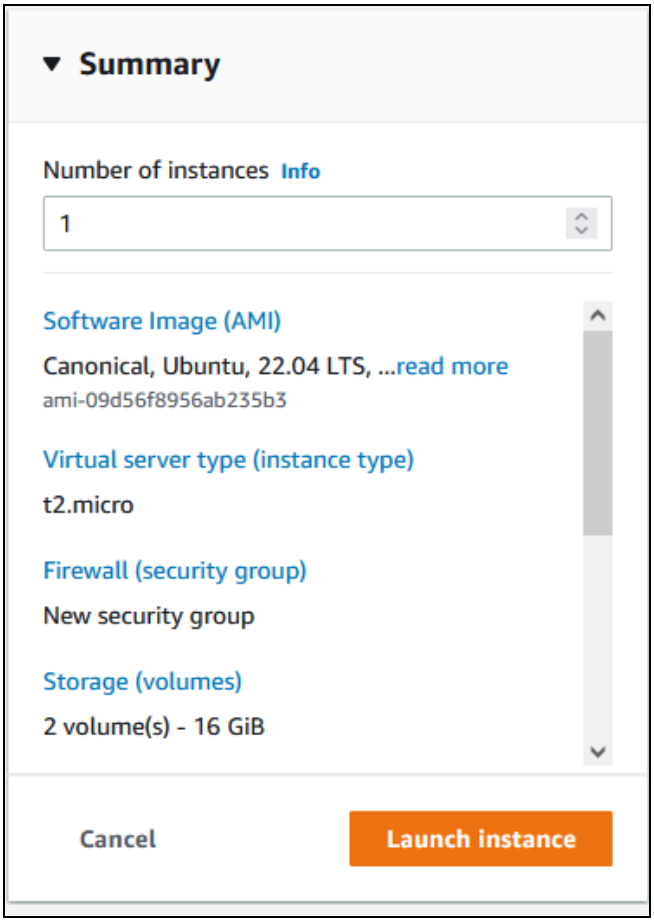


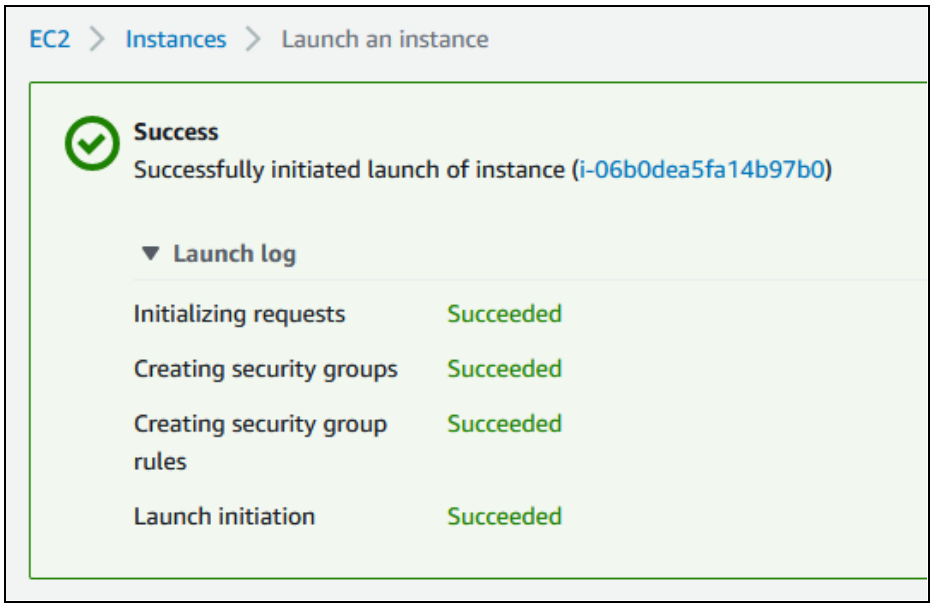
Step 29: Additional EBS storage volumes can be created and attached to the instance.



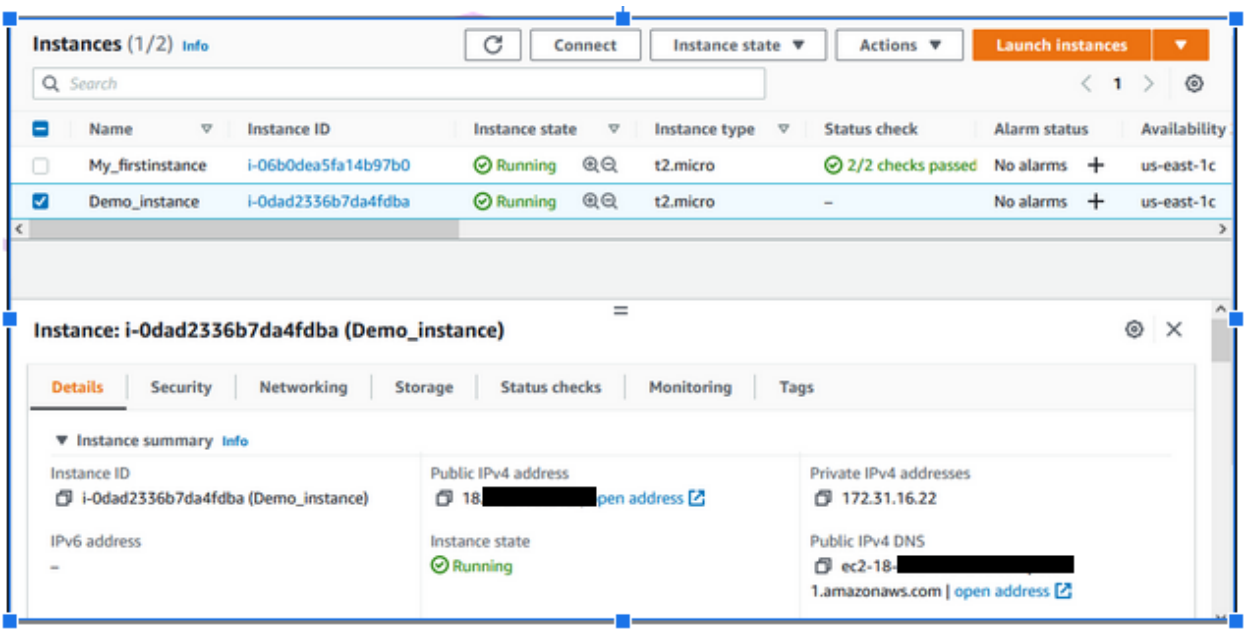


Step 30 : Summary of the Instance



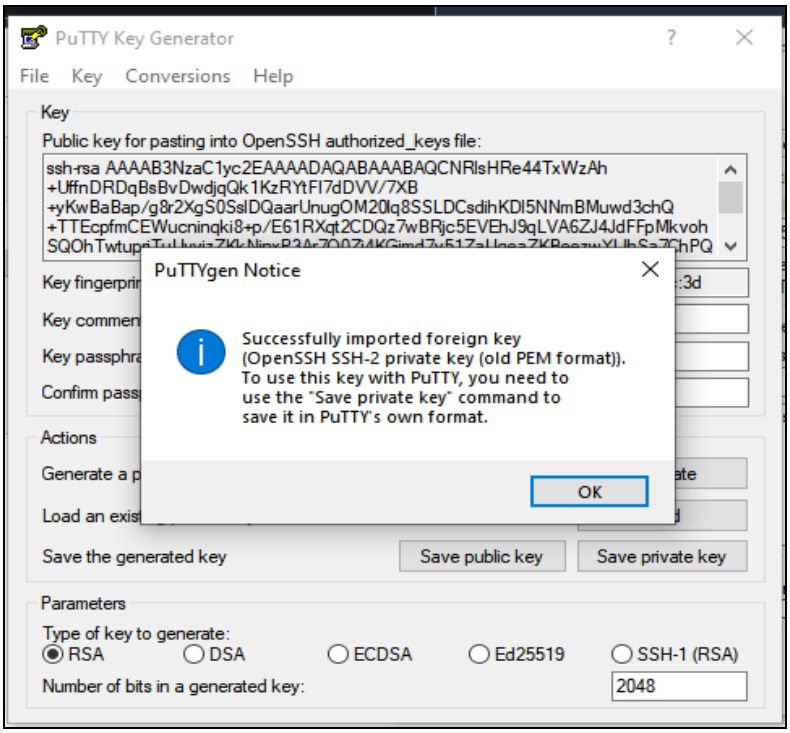


Step 31: Dashboard view of the instance

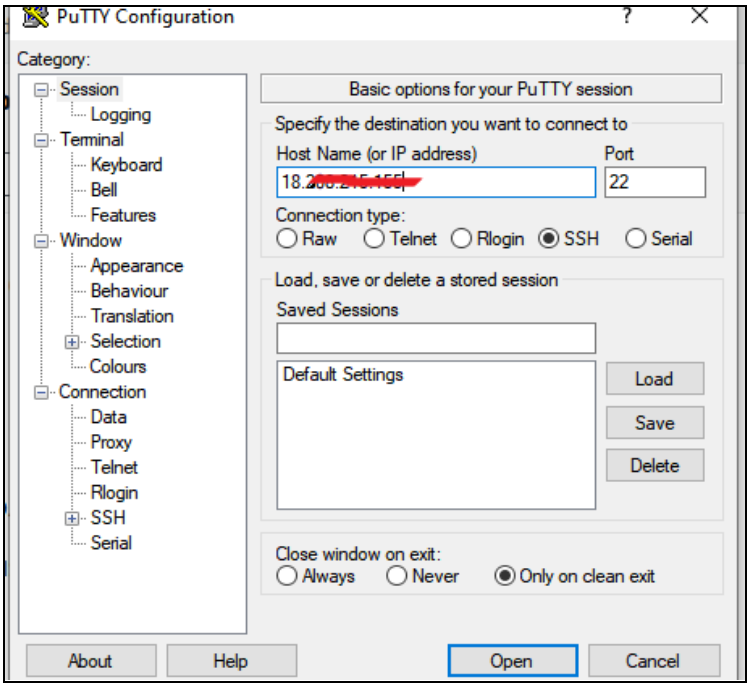


Step 32: Install putty msi installer you will get PuttyGen and Putty for accessing Linux VM. Open PuttyGen and load the demo.pem file downloaded from Step 26.

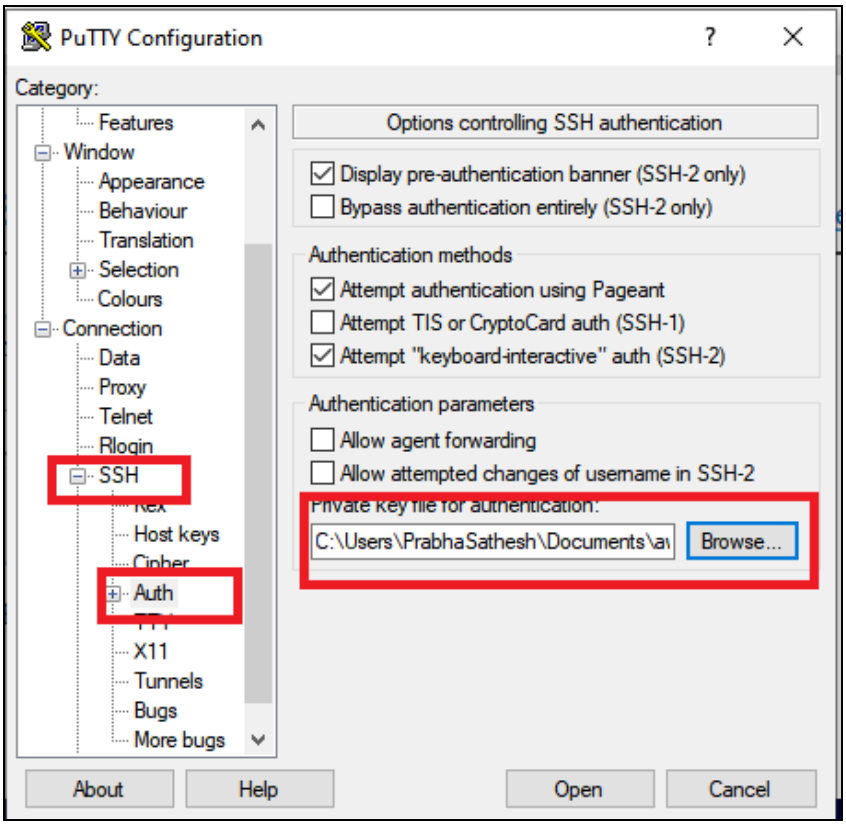
Click OK and save the Private key.(demo.ppk)



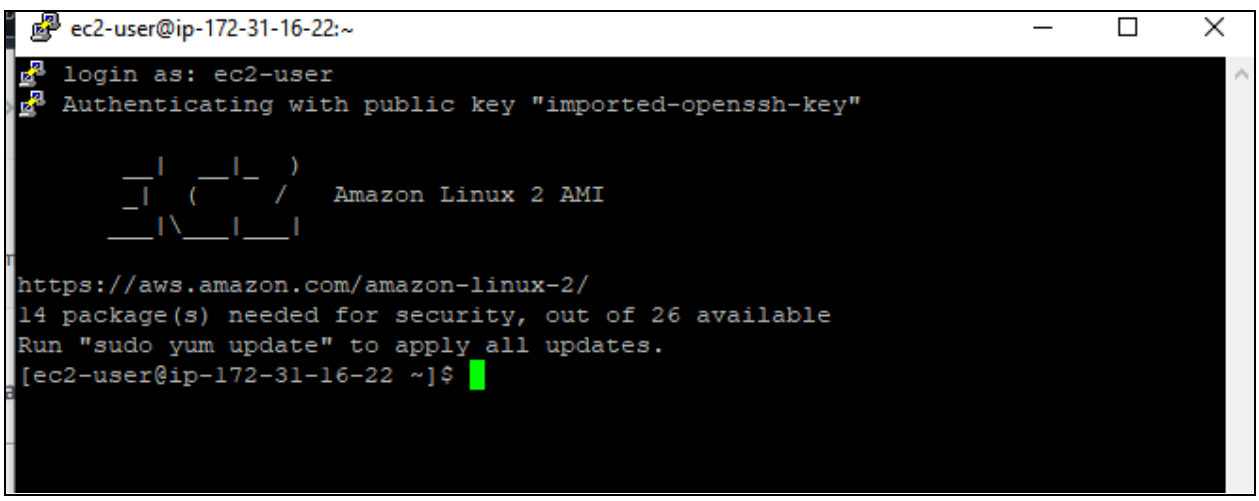
Step 33: Enter the public IP address of the VM in Putty.



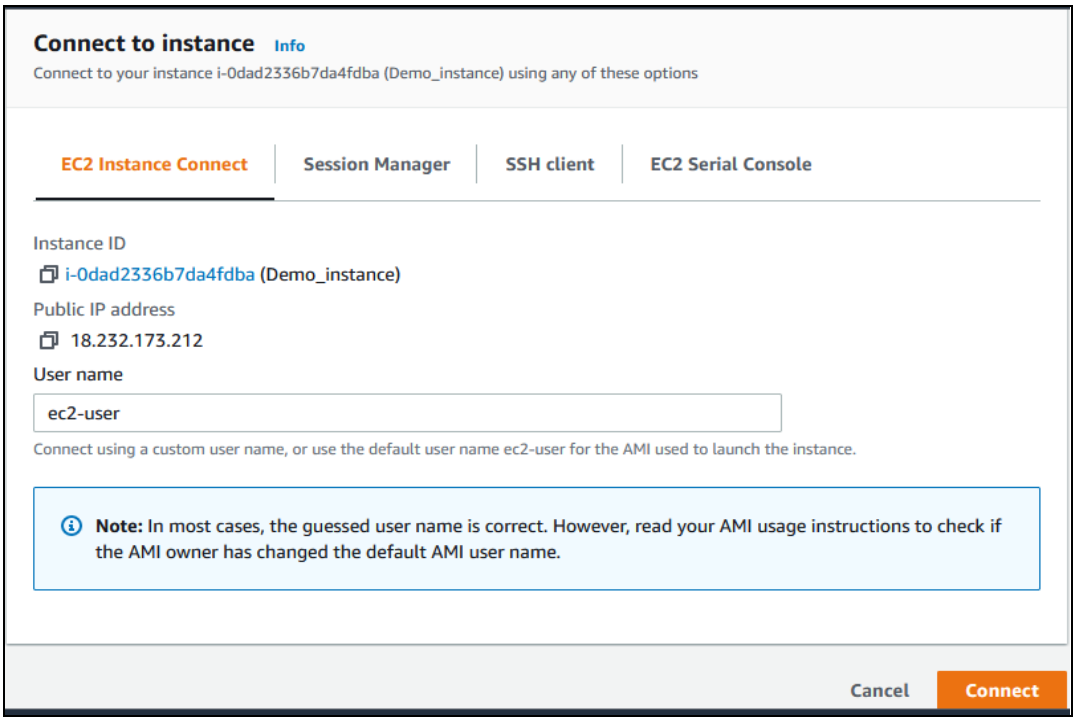
Expand SSH Click on Auth Browse and attach demo.ppk file downloaded from Step 32

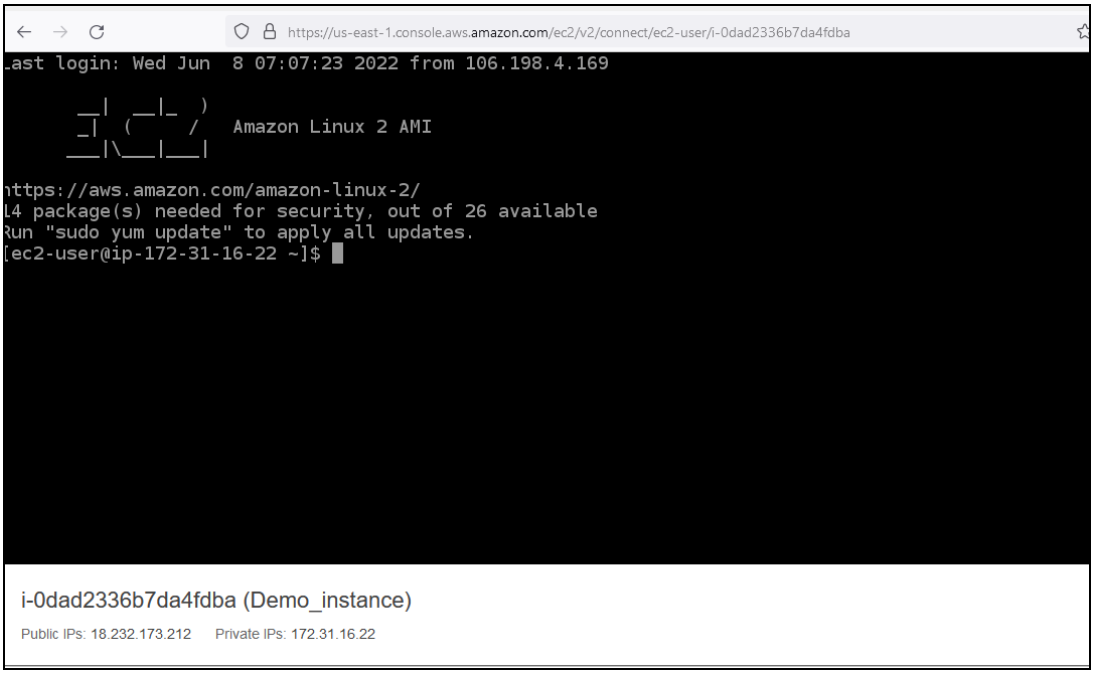


Step 34: Now we have successfully logged inside the VM



Step 35: Another method to connect to EC2 instance is using EC2 Instance Connect





Step 36: Creating a Web server inside the Virtual Machine.Update the repository using yum update.

```
[ec2-user@ip-172-31-16-22 ~]$ sudo yum update -y;
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                | 3.7 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package curl.x86_64 0:7.79.1-1.amzn2.0.1 will be updated
---> Package curl.x86_64 0:7.79.1-2.amzn2.0.1 will be an update
---> Package dracut.x86_64 0:033-535.amzn2.1.5 will be updated
---> Package dracut.x86_64 0:033-535.amzn2.1.6 will be an update
---> Package dracut-config-generic.x86_64 0:033-535.amzn2.1.5 will be updated
---> Package dracut-config-generic.x86_64 0:033-535.amzn2.1.6 will be an update
---> Package iproute.x86_64 0:5.10.0-2.amzn2.0.1 will be updated
---> Package iproute.x86_64 0:5.10.0-2.amzn2.0.2 will be an update
---> Package kernel.x86_64 0:5.10.112-108.499.amzn2 will be installed
---> Package kernel-tools.x86_64 0:5.10.109-104.500.amzn2 will be updated
```

```
ec2-user@ip-172-31-16-22:~

Installed:
  kernel.x86_64 0:5.10.112-108.499.amzn2

Updated:
  curl.x86_64 0:7.79.1-2.amzn2.0.1
  dracut.x86_64 0:033-535.amzn2.1.6
  dracut-config-generic.x86_64 0:033-535.amzn2.1.6
  iproute.x86_64 0:5.10.0-2.amzn2.0.2
  kernel-tools.x86_64 0:5.10.112-108.499.amzn2
  libcurl.x86_64 0:7.79.1-2.amzn2.0.1
  libgcc.x86_64 0:7.3.1-15.amzn2
  libgomp.x86_64 0:7.3.1-15.amzn2
  libstdc++.x86_64 0:7.3.1-15.amzn2
  libtiff.x86_64 0:4.0.3-35.amzn2.0.2
  microcode_ctl.x86_64 2:2.1-47.amzn2.0.12
  openldap.x86_64 0:2.4.44-23.amzn2.0.4
  openssl.x86_64 1:1.0.2k-24.amzn2.0.3
  openssl-libs.x86_64 1:1.0.2k-24.amzn2.0.3
  python.x86_64 0:2.7.18-1.amzn2.0.5
  python-devel.x86_64 0:2.7.18-1.amzn2.0.5
  python-libs.x86_64 0:2.7.18-1.amzn2.0.5
  systemd.x86_64 0:219-78.amzn2.0.18
  systemd-libs.x86_64 0:219-78.amzn2.0.18
  systemd-sysv.x86_64 0:219-78.amzn2.0.18
  vim-common.x86_64 2:8.2.4857-1.amzn2.0.1
  vim-data.noarch 2:8.2.4857-1.amzn2.0.1
  vim-enhanced.x86_64 2:8.2.4857-1.amzn2.0.1
  vim-filesystem.noarch 2:8.2.4857-1.amzn2.0.1
  vim-minimal.x86_64 2:8.2.4857-1.amzn2.0.1

Complete!
```

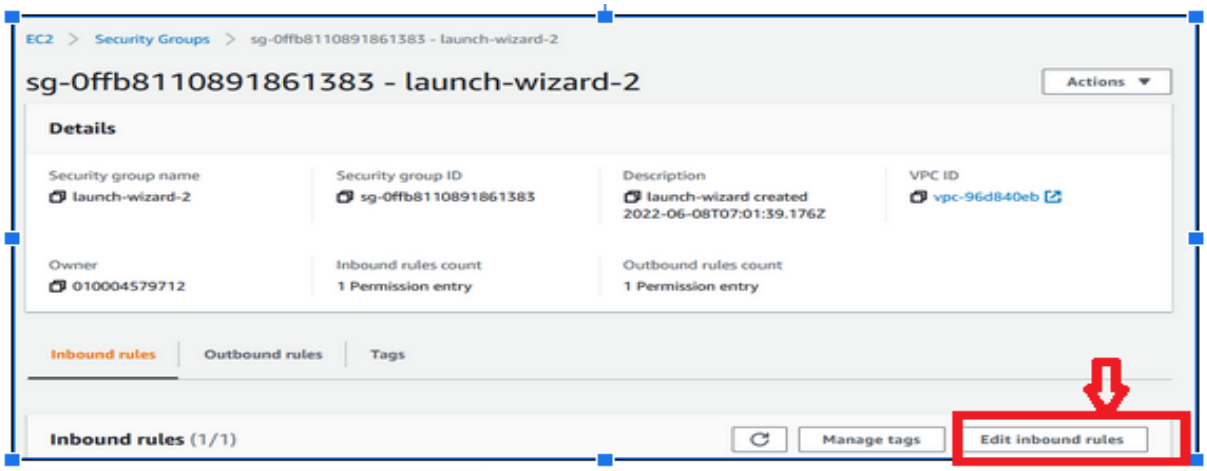
Step 37: Install Apache http server

```
[ec2-user@ip-172-31-16-22 ~]$ sudo yum install httpd -y;
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.53-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem = 2.4.53-1.amzn2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: mod_http2 for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem for package: httpd-2.4.53-1.amzn2.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.53-1.amzn2.x86_64
```

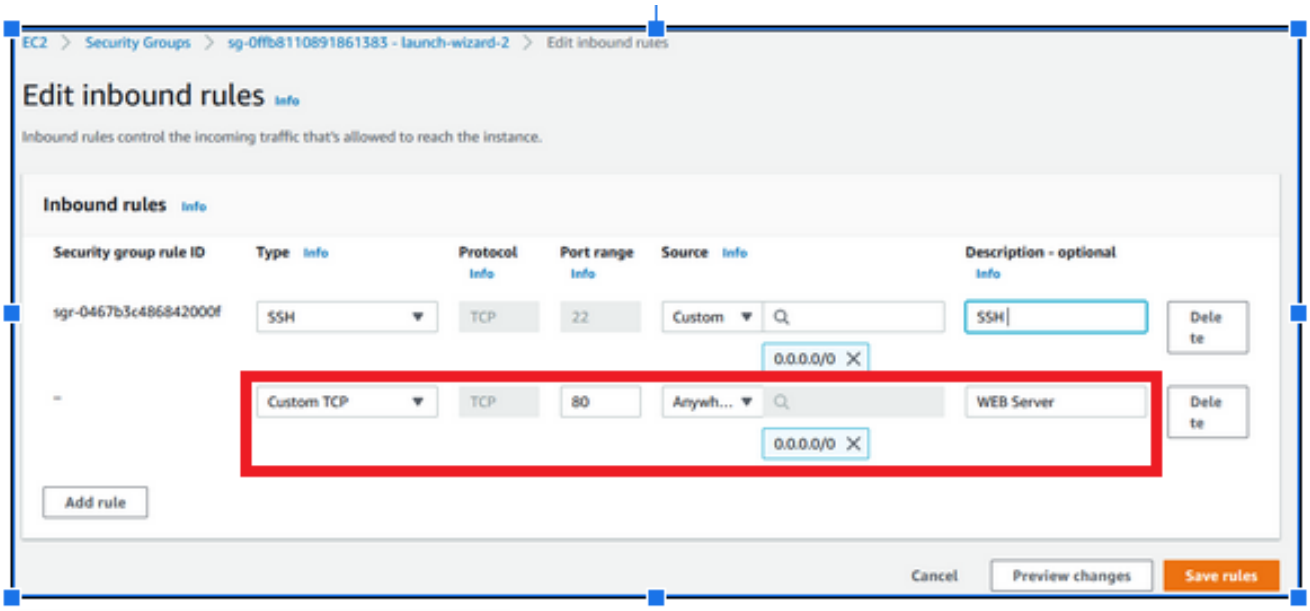
```
Installed:
  httpd.x86_64 0:2.4.53-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.7.0-9.amzn2                                apr-util.x86_64 0:1.6.1-5.amzn2.0.2
  apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2                   generic-logos-httpd.noarch 0:18.0.0-4.amzn2
  httpd-filesystem.noarch 0:2.4.53-1.amzn2                  httpd-tools.x86_64 0:2.4.53-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2                           mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
```

```
ec2-user@ip-172-31-16-22:~
[ec2-user@ip-172-31-16-22 ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[ec2-user@ip-172-31-16-22 ~]$ 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; vendor preset: disabled)
   Active: active (running) since Wed 2022-06-08 07:20:39 UTC; 13s ago
     Docs: man:httpd.service(8)
 Main PID: 10440 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─10440 /usr/sbin/httpd -DFOREGROUND
           ├─10441 /usr/sbin/httpd -DFOREGROUND
           ├─10442 /usr/sbin/httpd -DFOREGROUND
           ├─10443 /usr/sbin/httpd -DFOREGROUND
           ├─10444 /usr/sbin/httpd -DFOREGROUND
           └─10445 /usr/sbin/httpd -DFOREGROUND

Jun 08 07:20:39 ip-172-31-16-22.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Jun 08 07:20:39 ip-172-31-16-22.ec2.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-172-31-16-22 ~]$ sudo chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
```

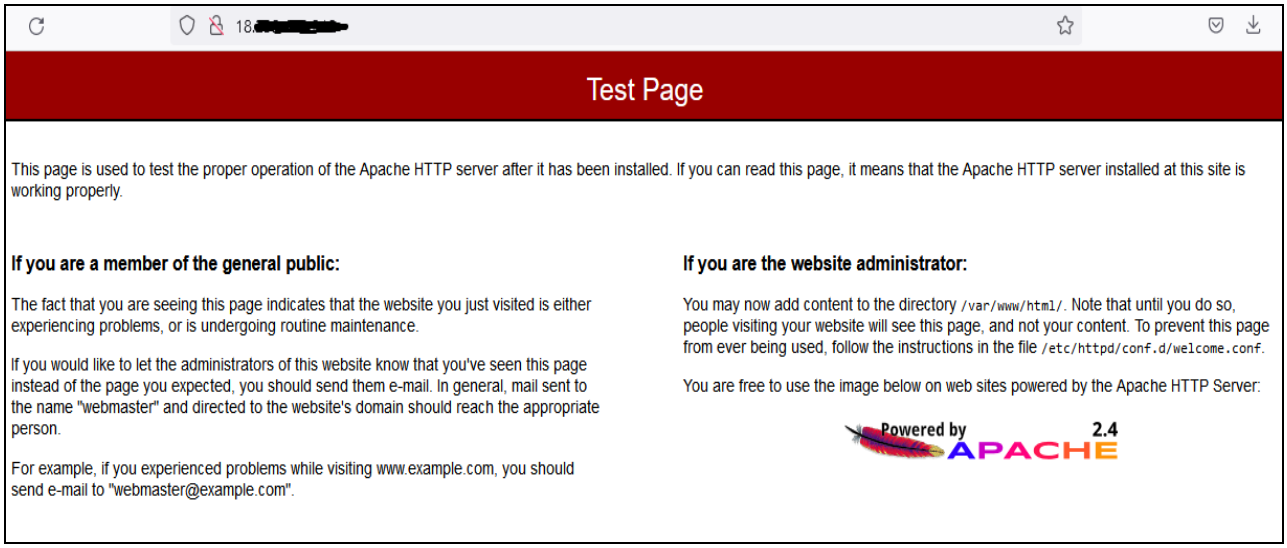
Step 38: Now go back to EC2 Security Groups and Click Edit inbound rules



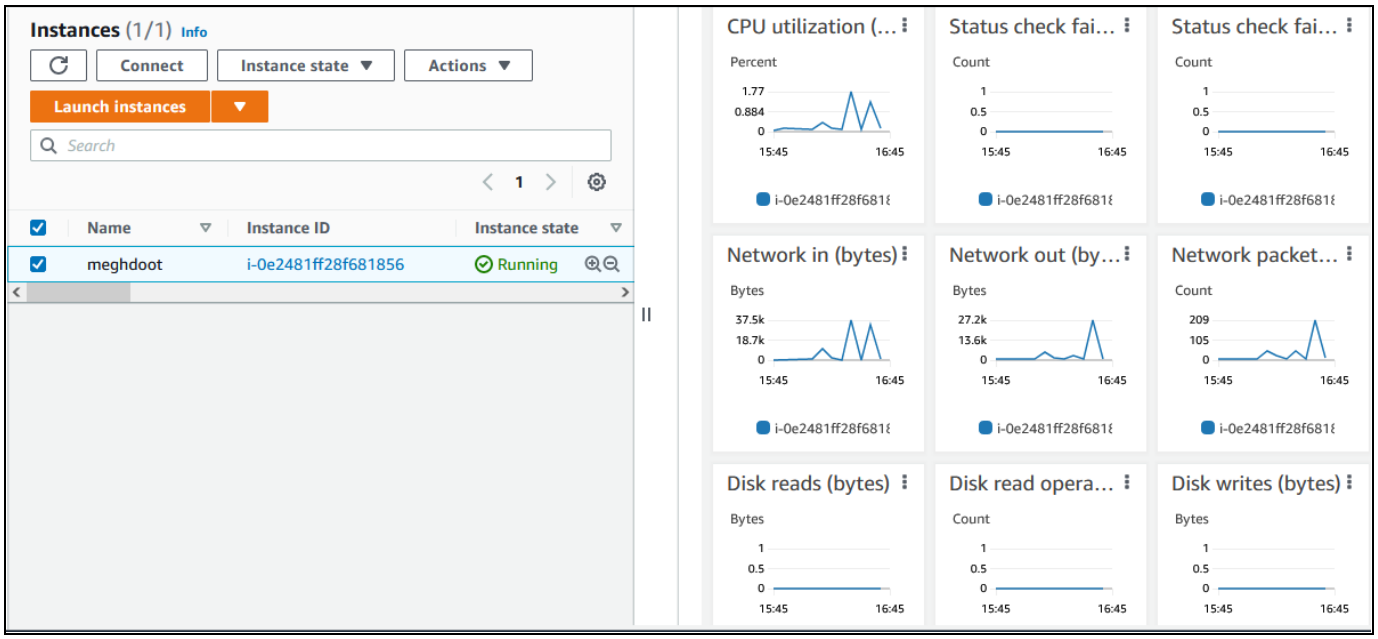
Step 39: Add 80 port as custom TCP protocol



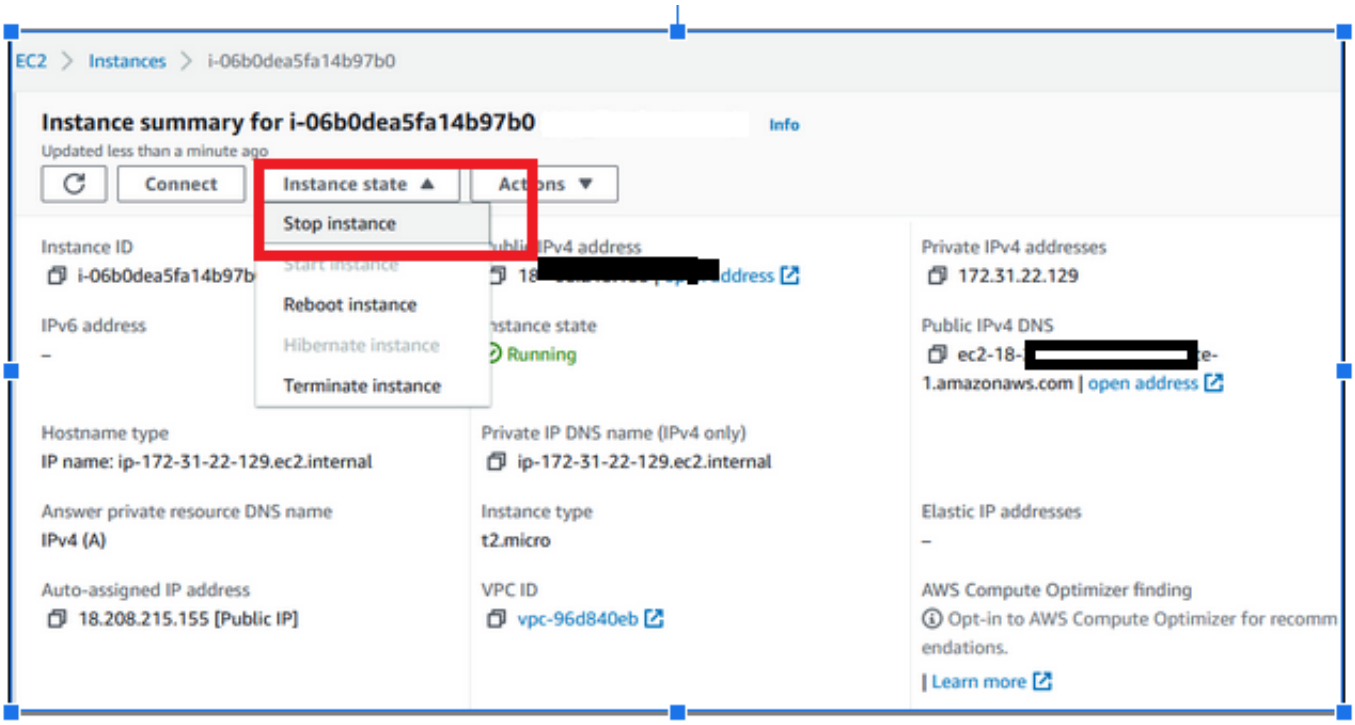
Step 40: Access the web server using Public IP



Step 41: EC2 instance Monitoring

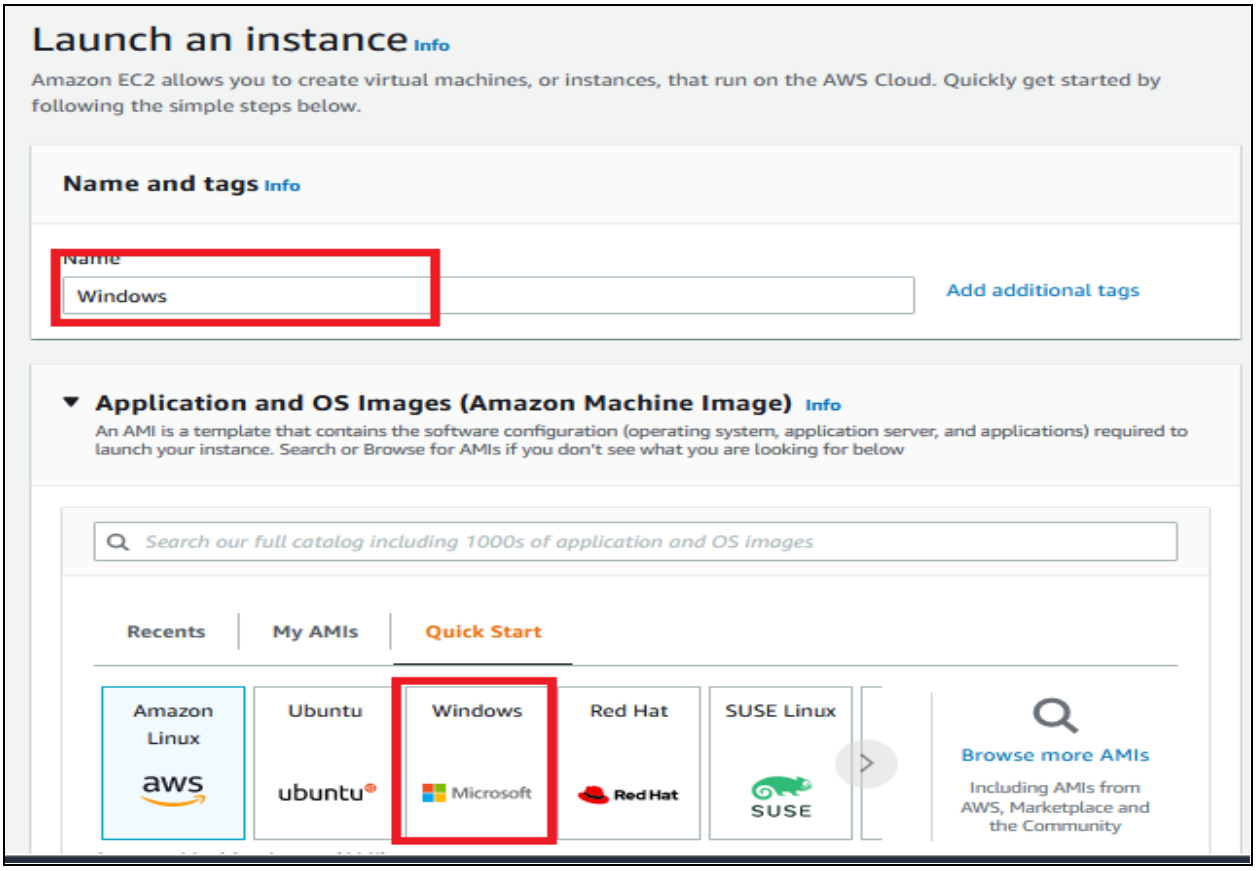


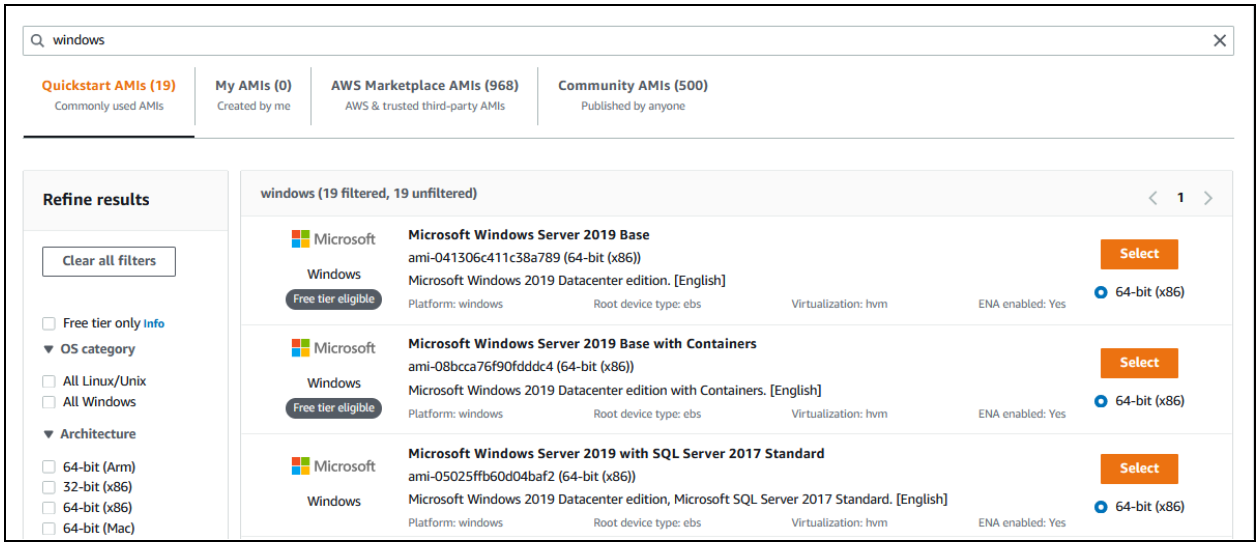
Step 42: To Stop/Terminate an instance



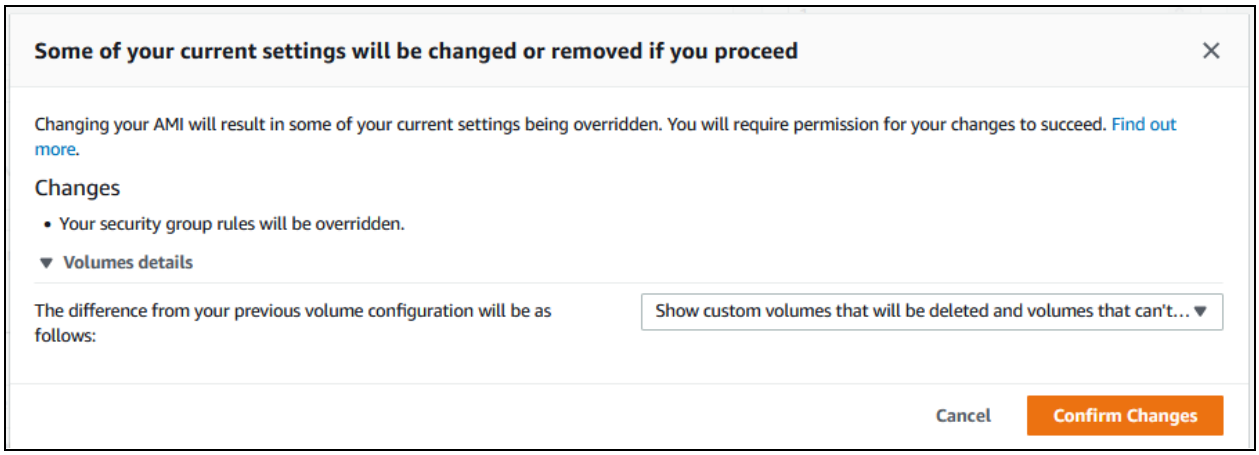
Launch Windows Instances

Step 43 : Select Launch instance and assign a name to the instance and select Windows AMI(free tier eligible)

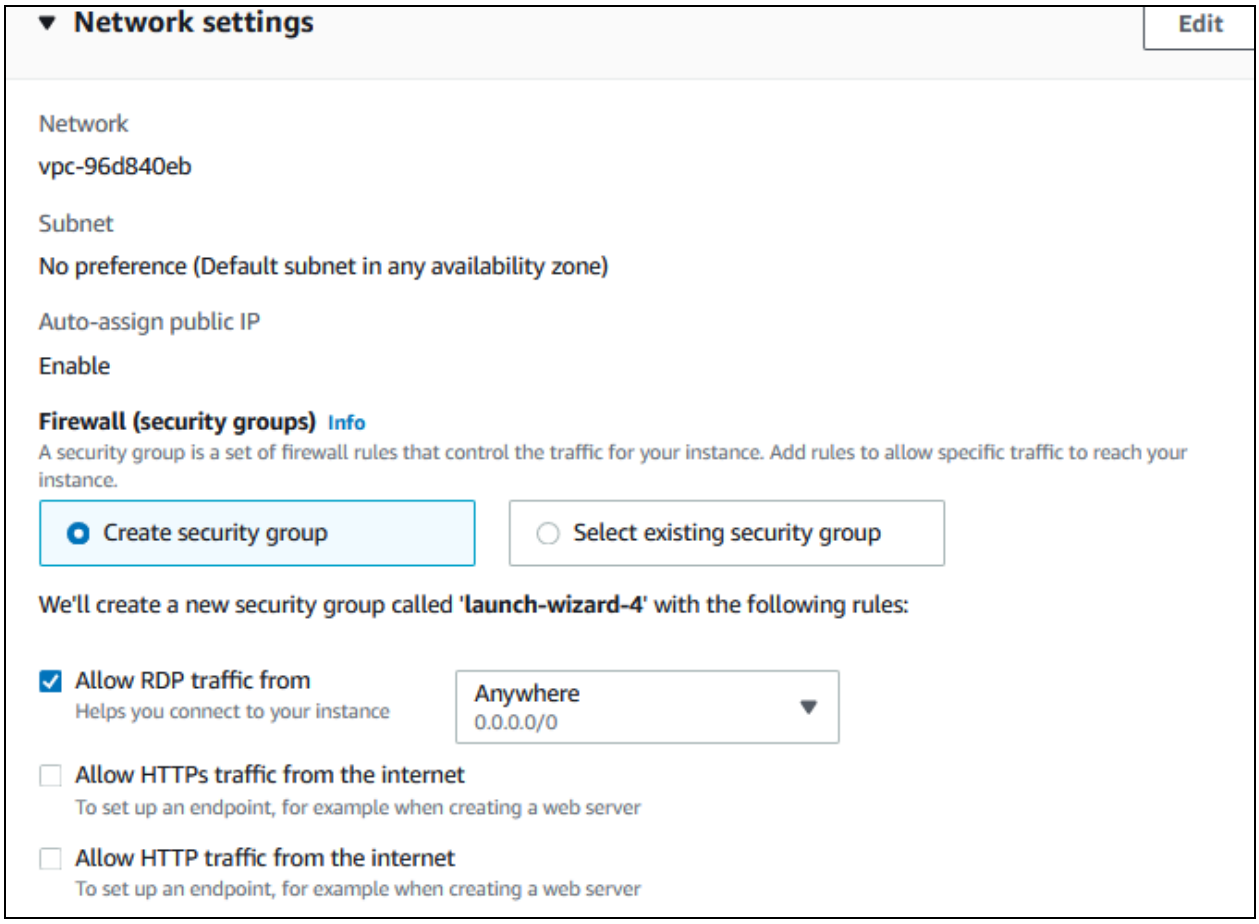




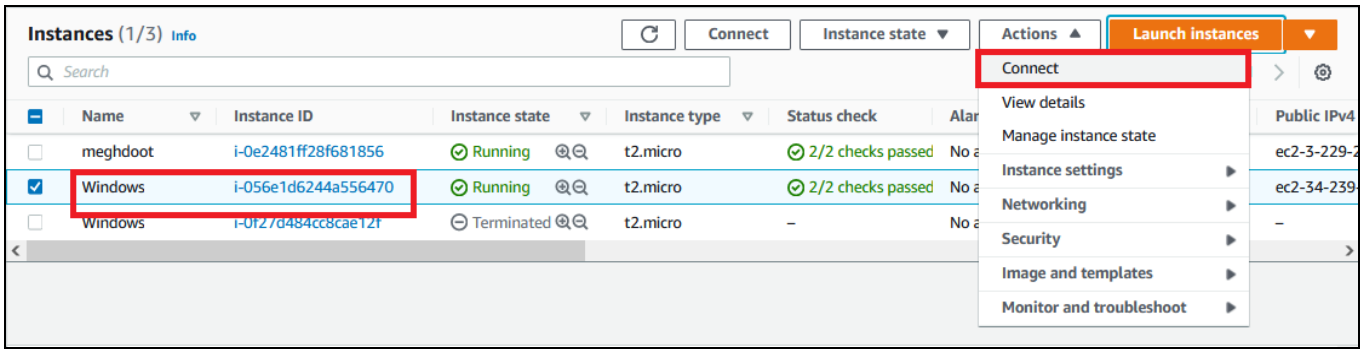
Step 44 : Confirmation to the changes of the existing policy of Security Groups and Volumes

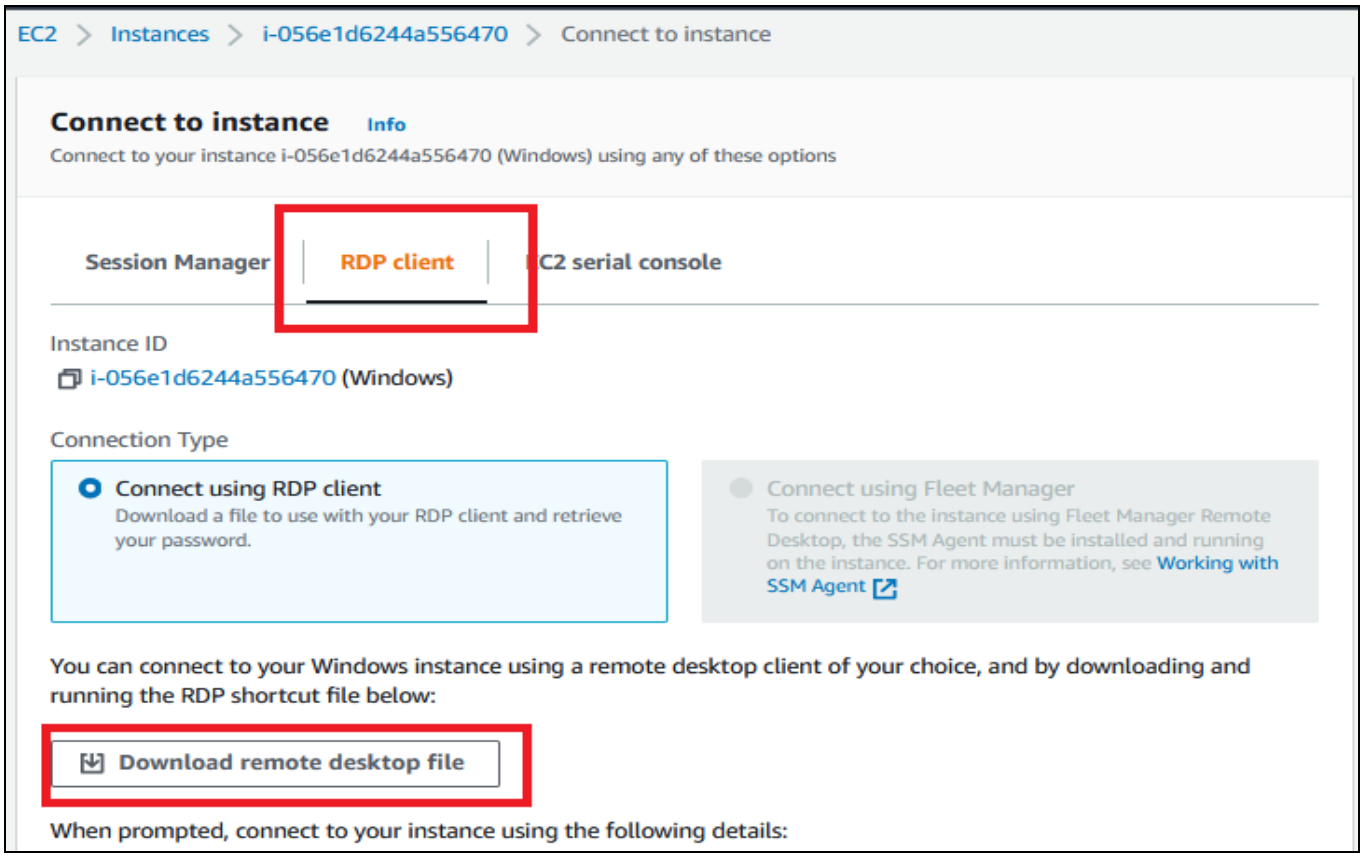


Step 45: Select the VPC, subnet and Security Groups (new or existing .pem file)



Step 46: Connect to the Windows Instance and select the RDP client





Step 47: Click on Get password

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 details:

Public DNS
ec2-34-239-1-181.compute-1.amazonaws.com

User name
Administrator

Password **Get password**

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Step 48: Keep a note of the Password

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

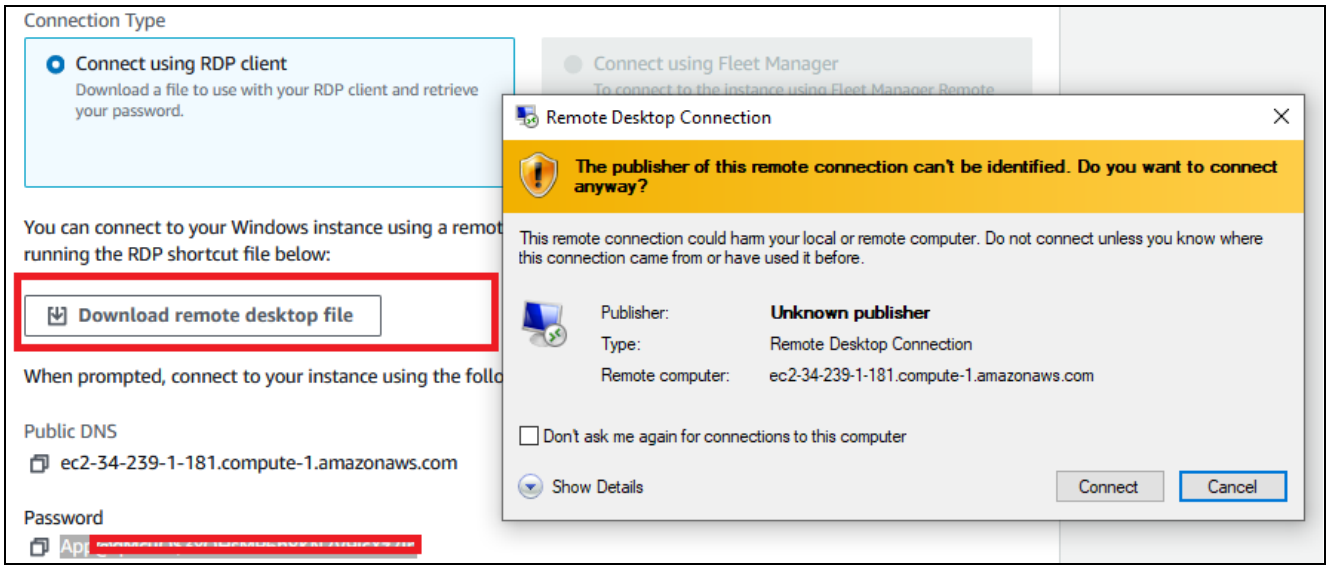
When prompted, connect to your instance using the following details:

Public DNS
ec2-34-239-1-181.compute-1.amazonaws.com

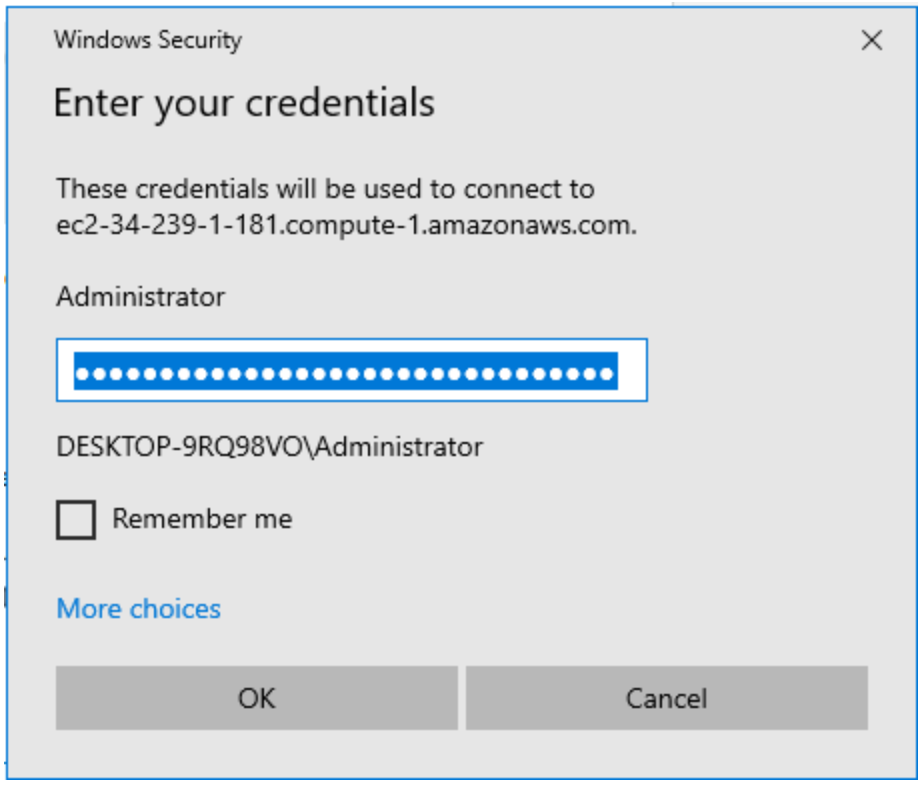
User name
Administrator

Password
App@[redacted]

Step 49: Click Download remote desktop file and Windows.rdp client file would be downloaded. Click on the Windows.rdp file



Step 50 : Enter the password which is copied from the previous step



Finally, the Windows instance is accessible