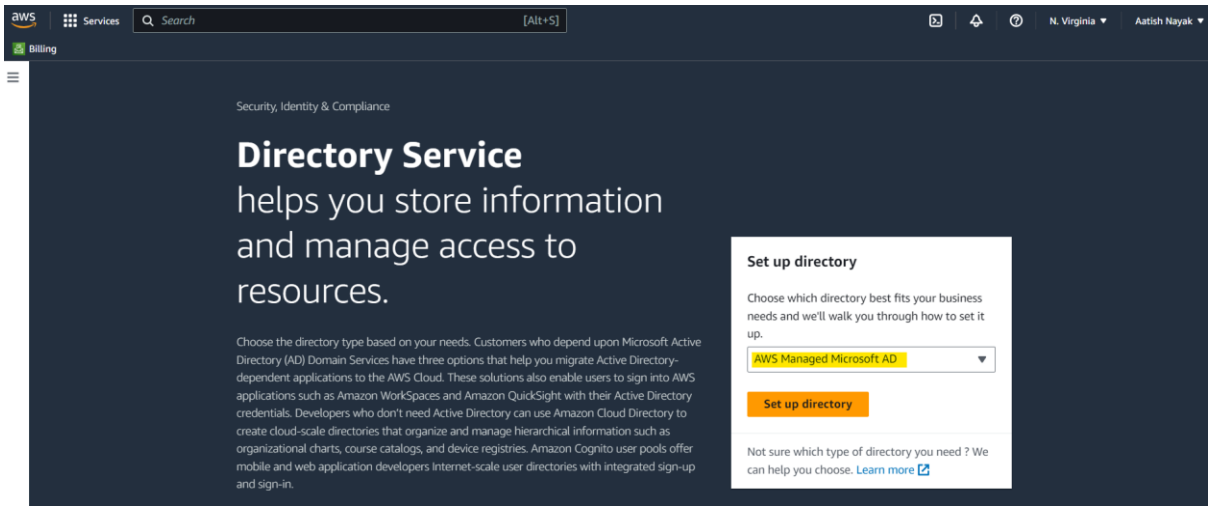
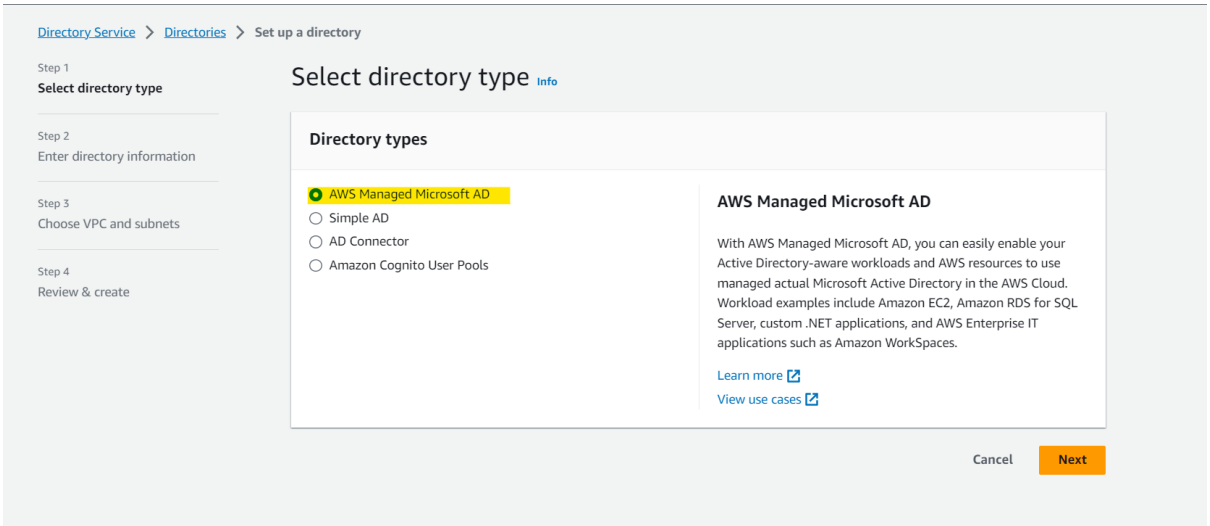
AWS Directory Service

- Create AWS Managed Microsoft AD

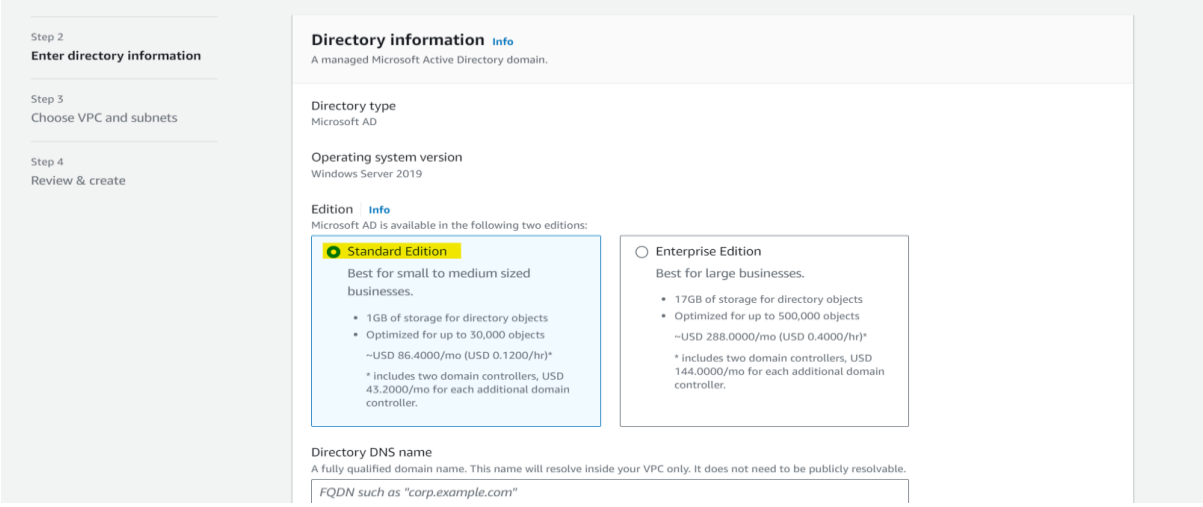


Click on Set up directory

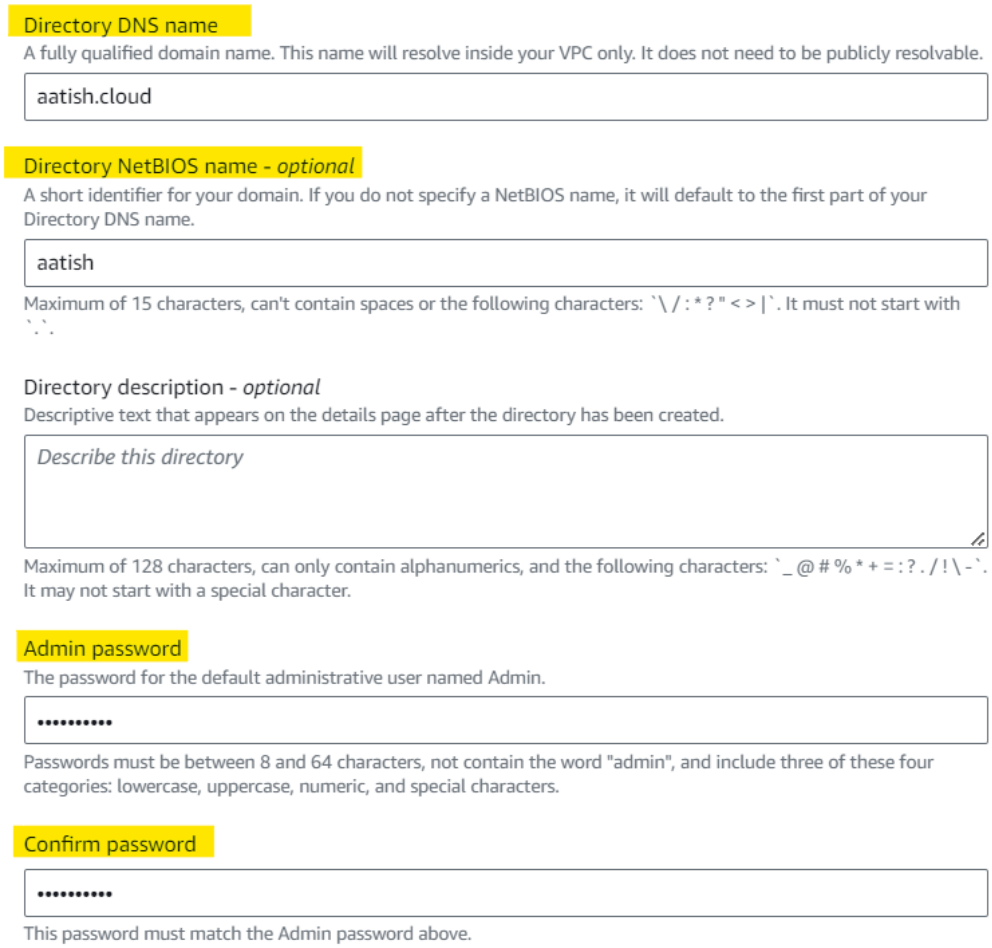
- Select directory type



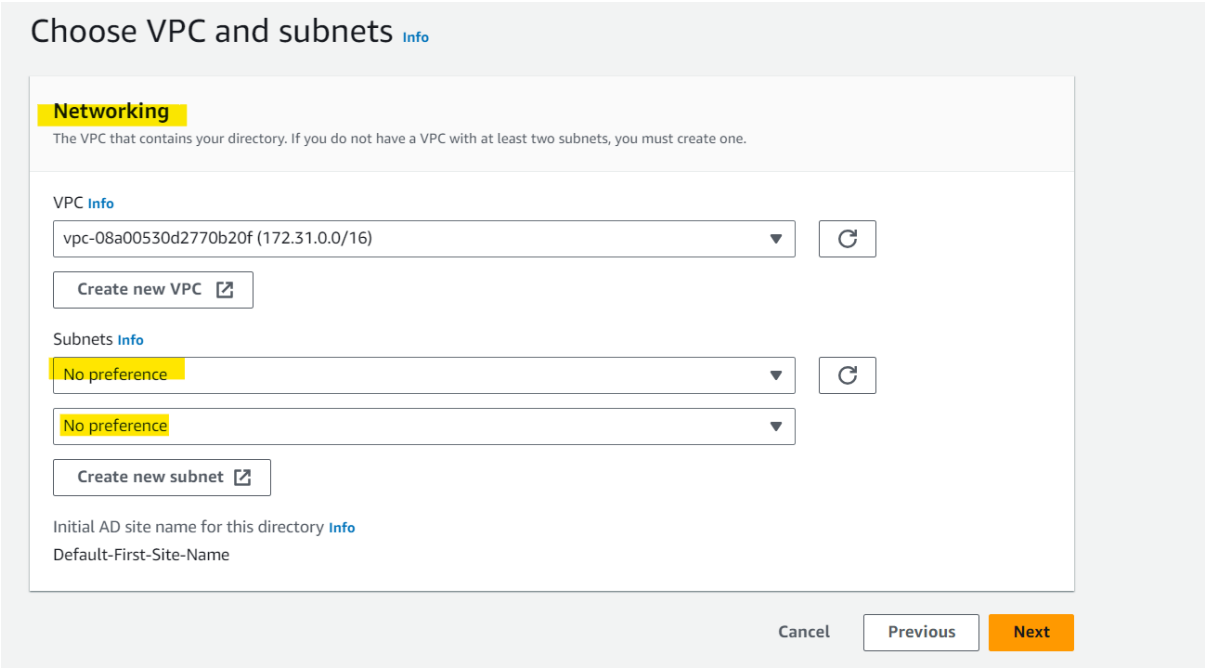
- Enter directory information



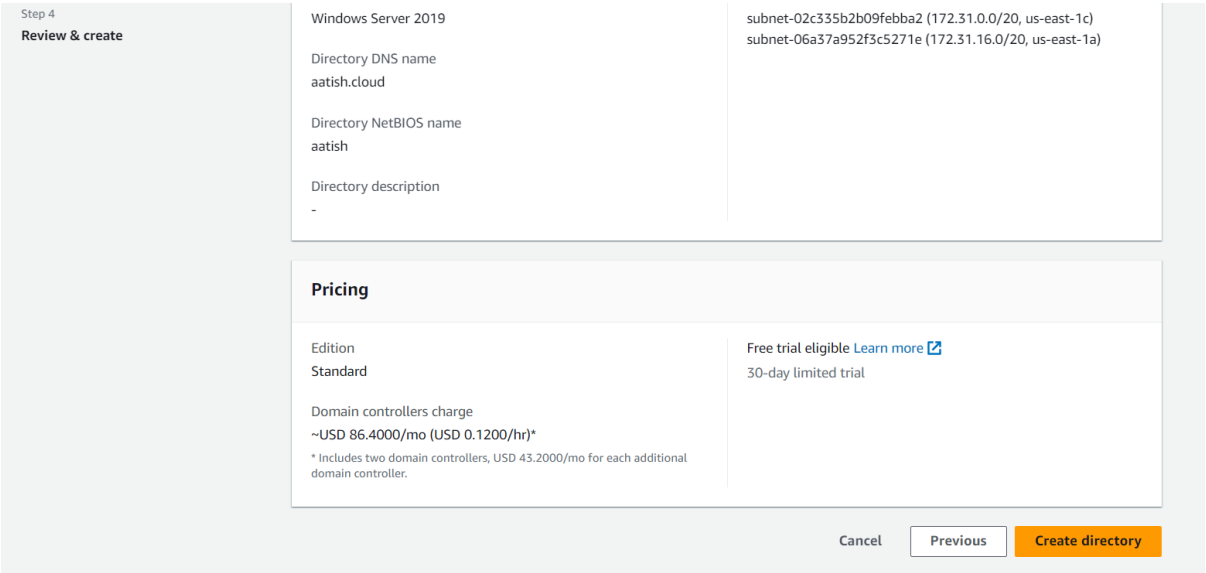
- Please fill in the following details and click on next



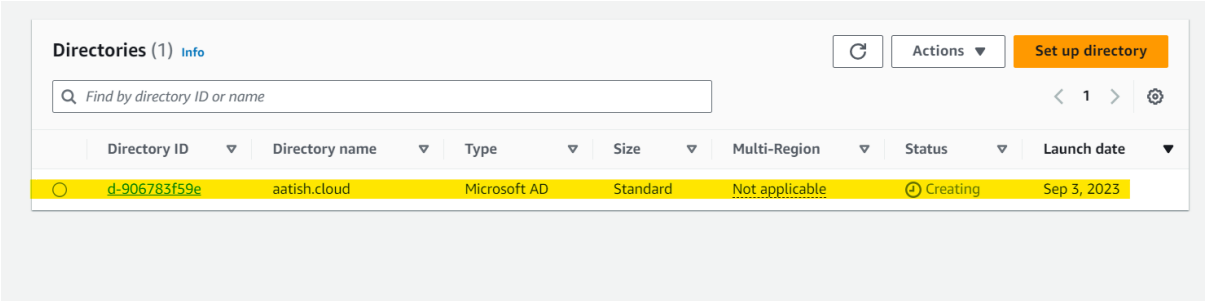
- Choose VPC and subnets
- Please select the Subnets in two zones or keep it as No preference



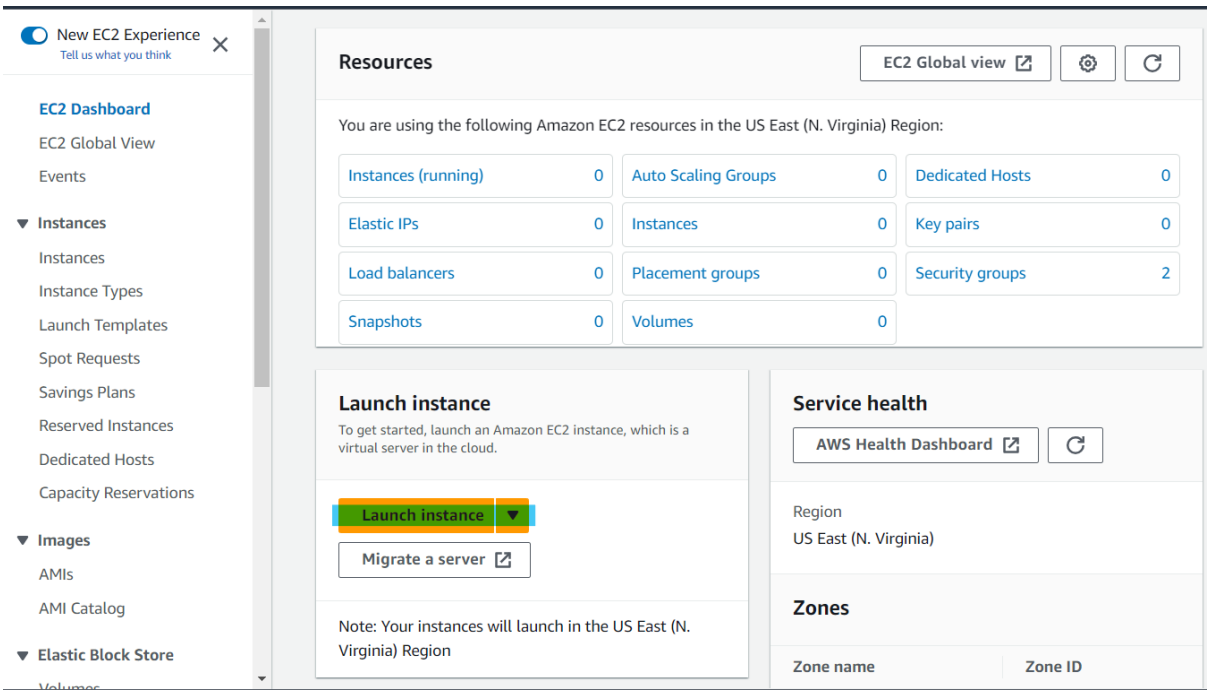
- Review & create



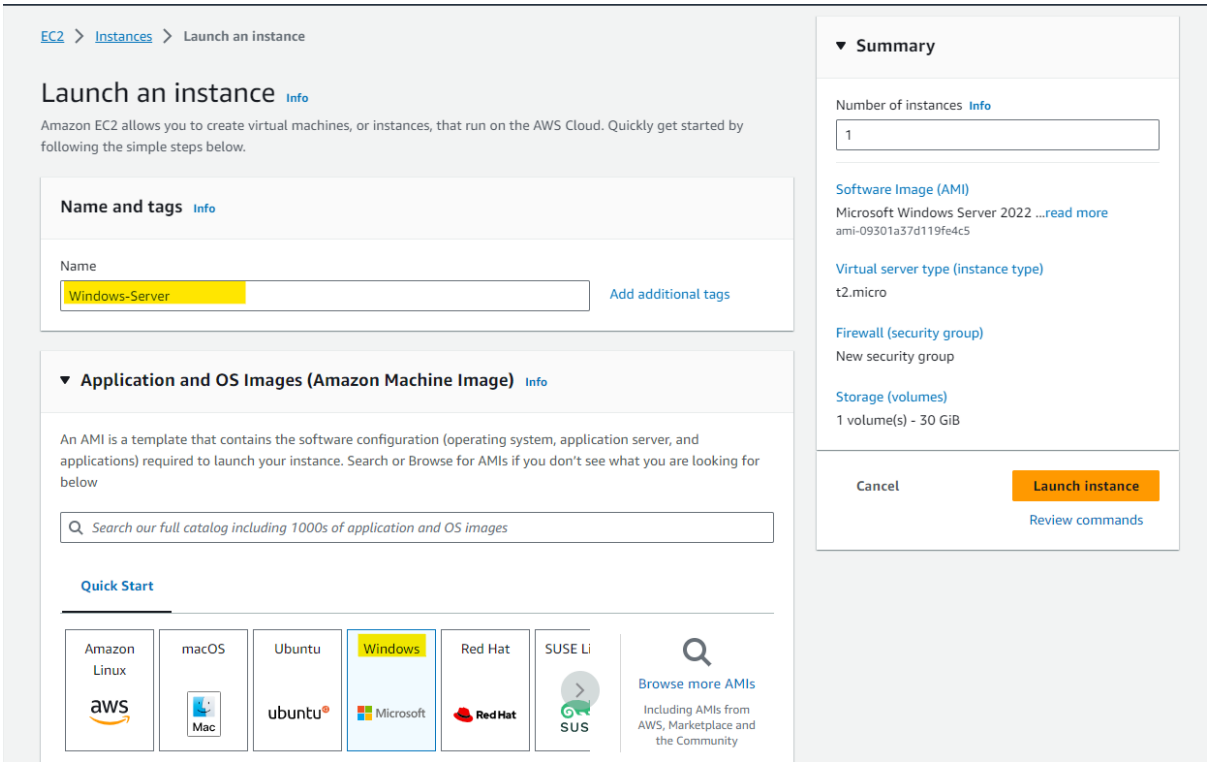
- It will take 30 mins to set up the Directory



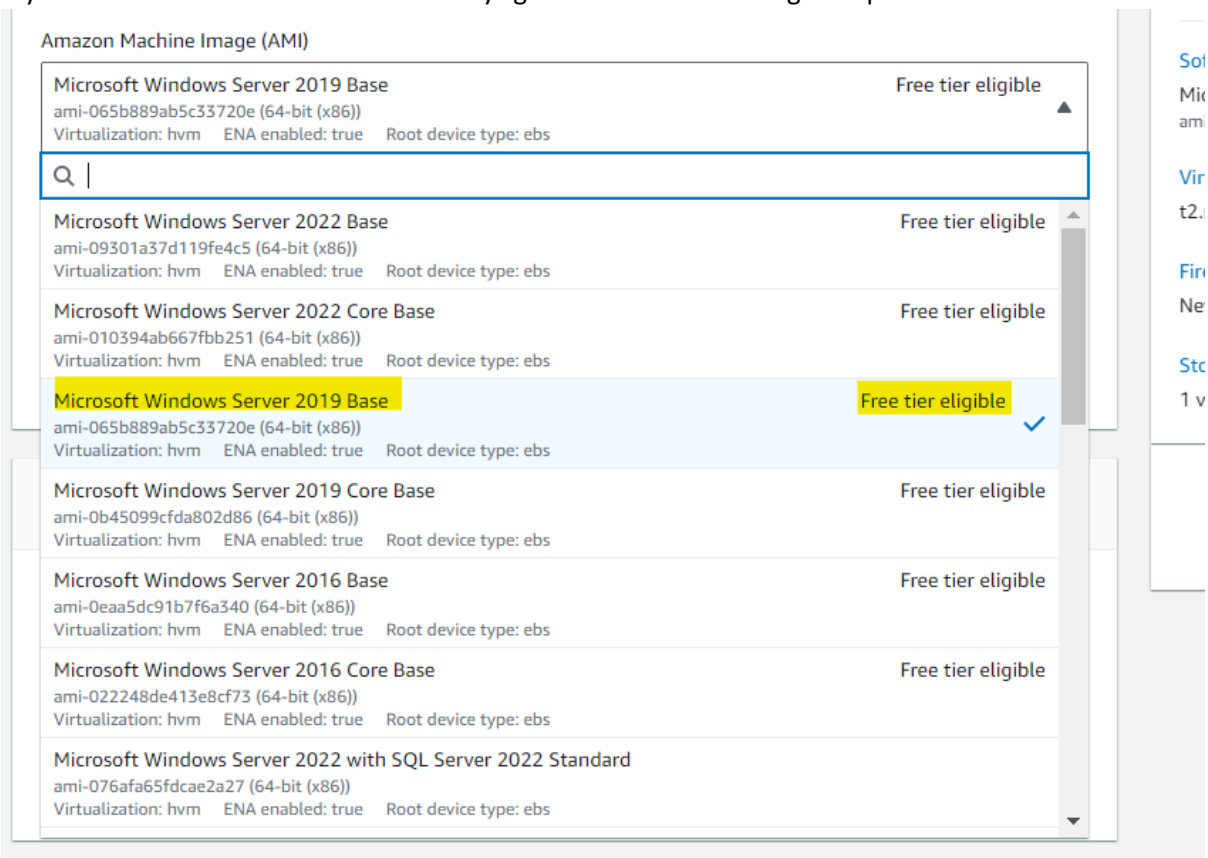
- Create a EC2 Instance with Windows-Server 2019
- Click on Launch instance



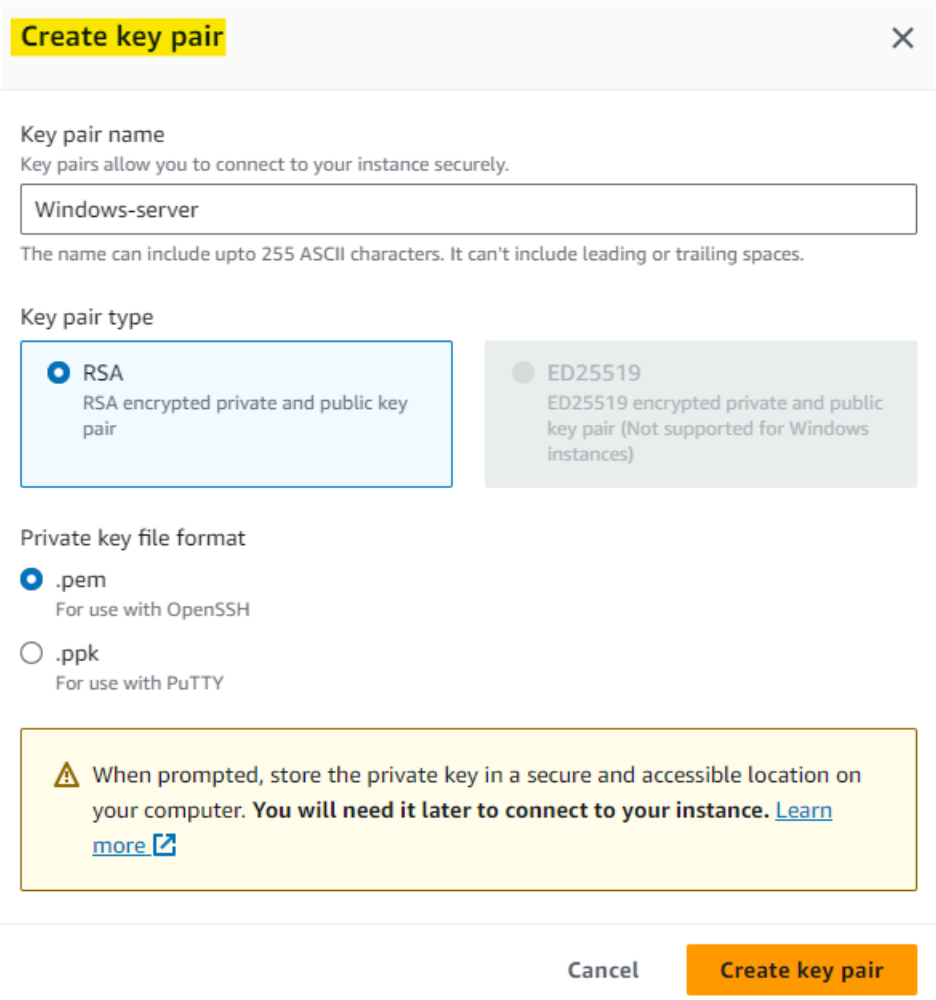
- Select Microsoft Windows



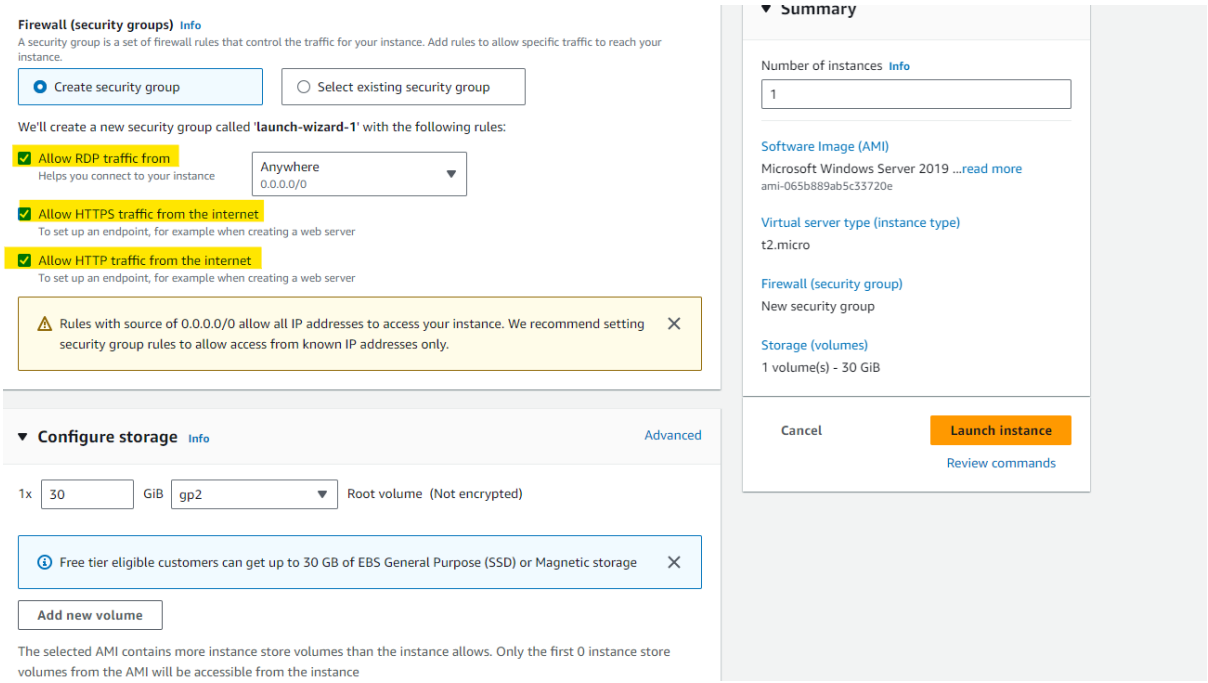
- If you have a free tier account then always go with the free tier eligible option



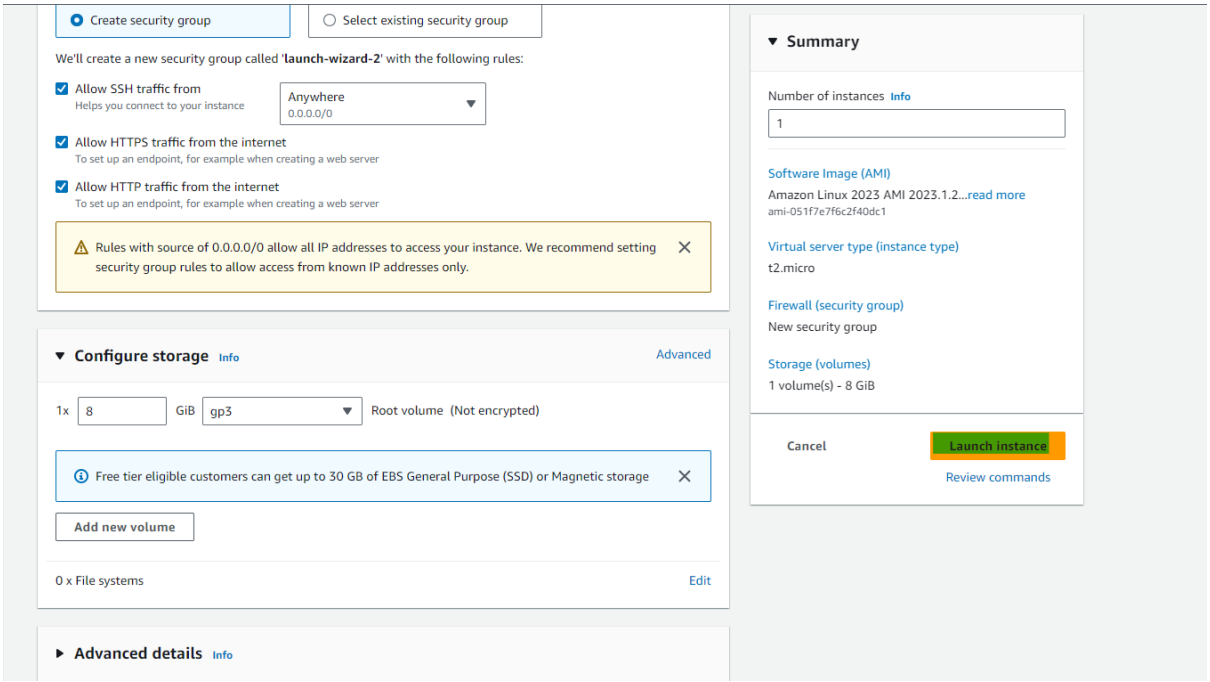
- Create a .Pem key for Secure login



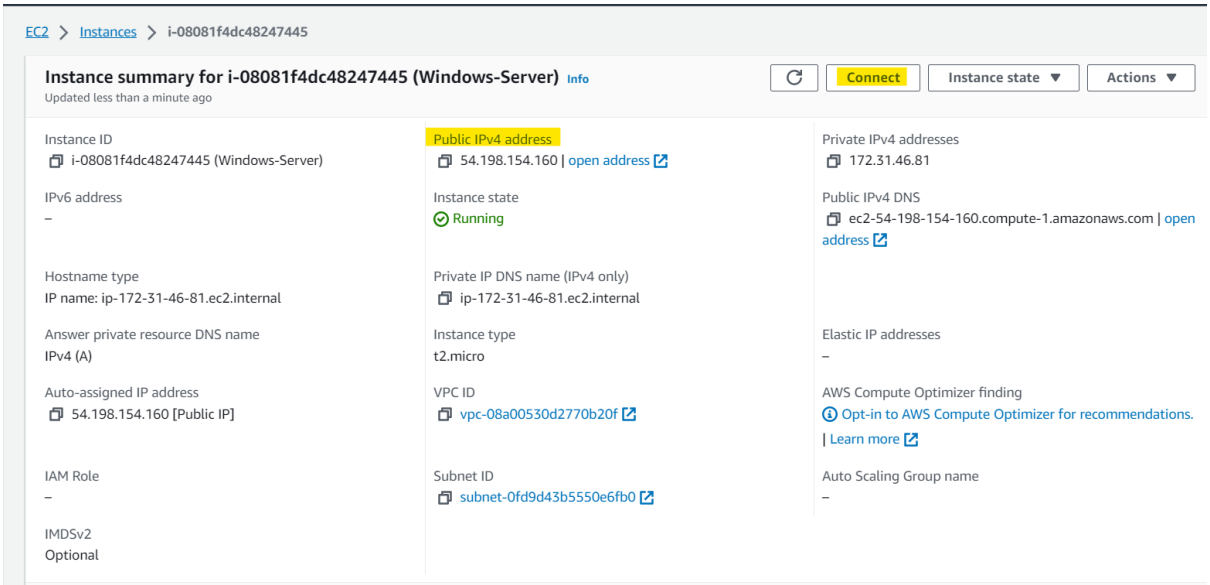
- Please Allow RDP Traffic, HTTP, HTTPS



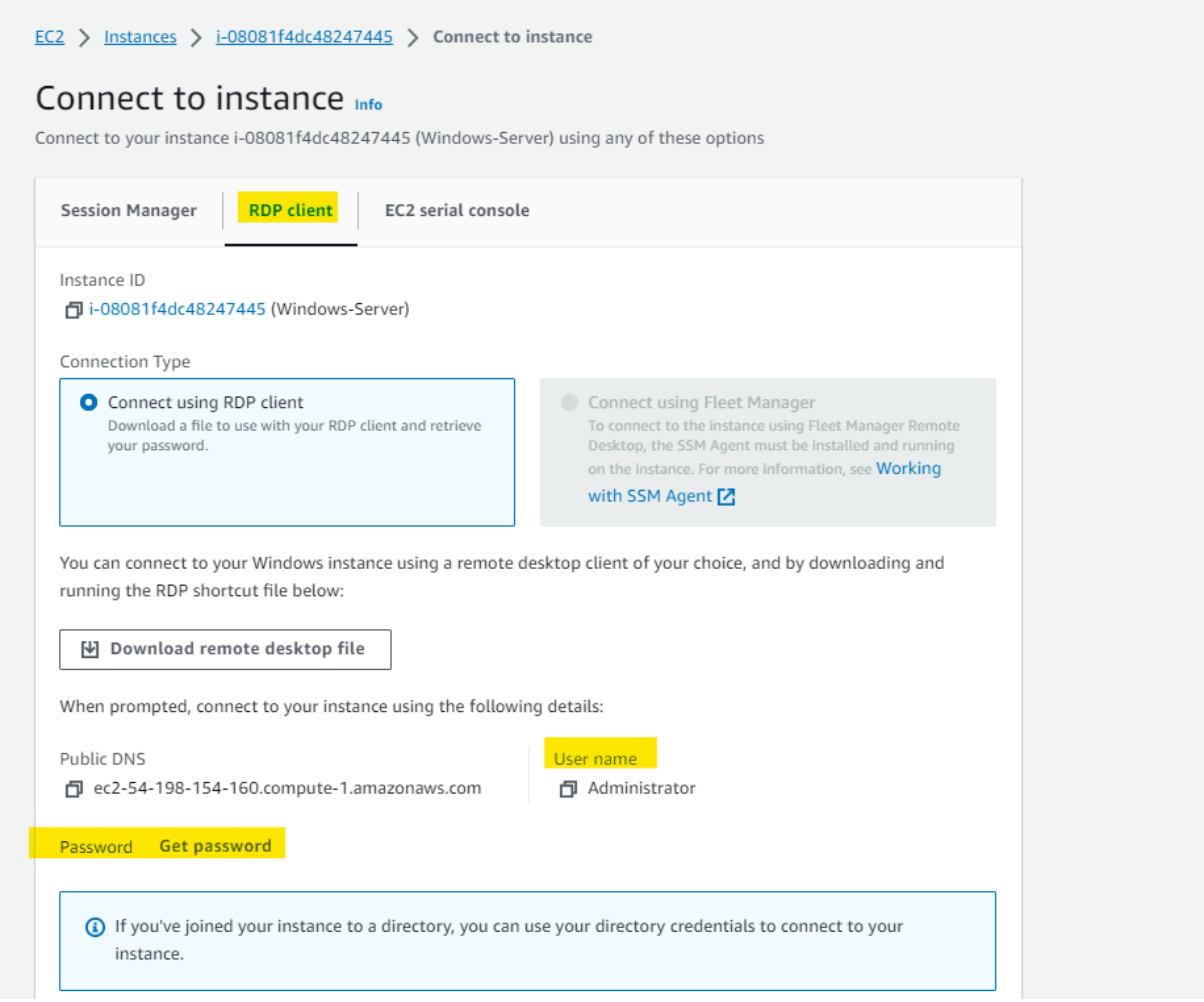
- Once you have selected the required options, please check on launch Instance



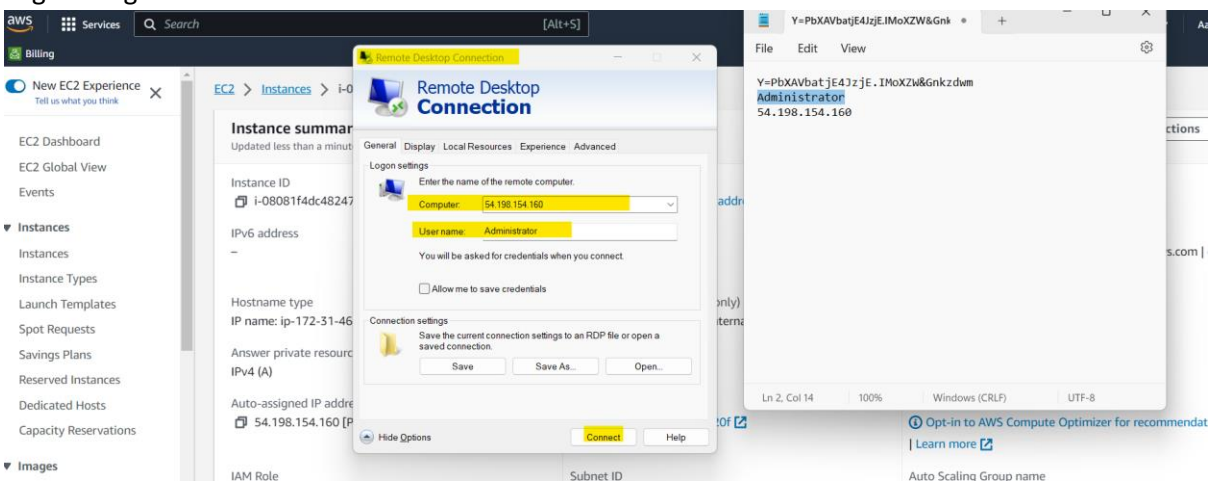
- Steps to login with Remote Desktop Connection
- Collect the Public IP, User Name, And Generate the Password using .Pemkey
- Copy the Public IP and click on Connect
-



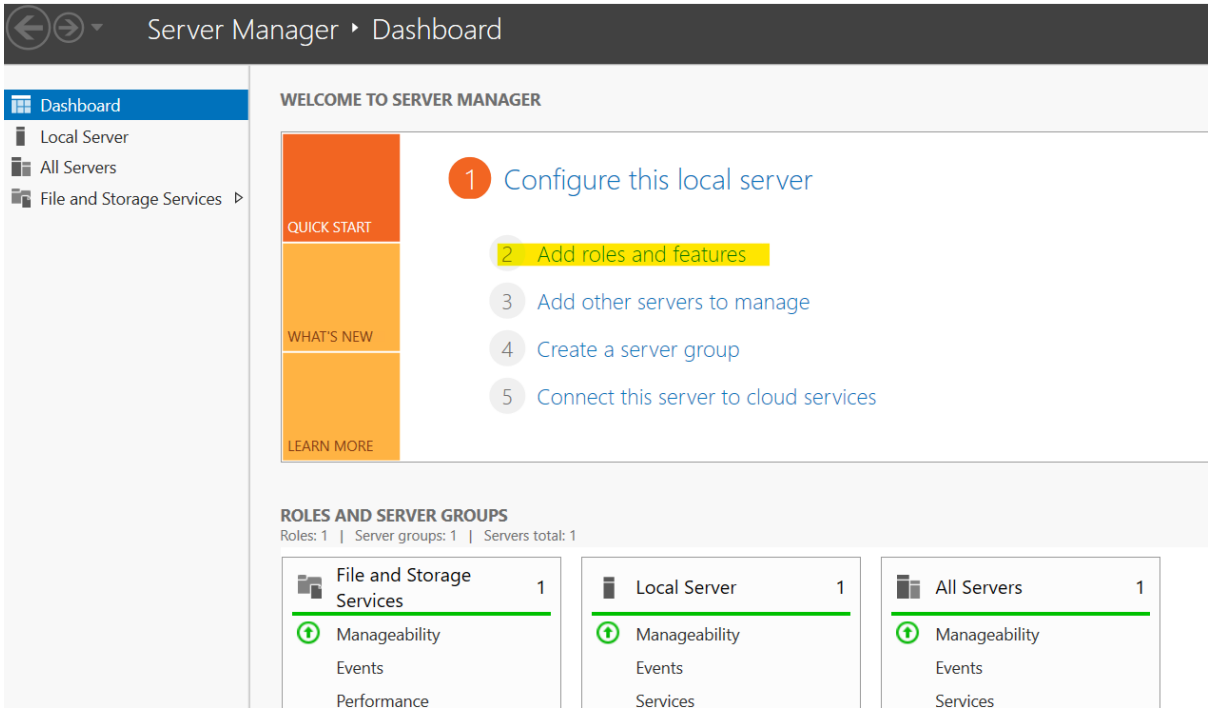
- Click on RDP Client
- Copy the User Name
- Click on Get password and Upload the Pem-key
- Once you upload the Key, Click on Decrypt Password



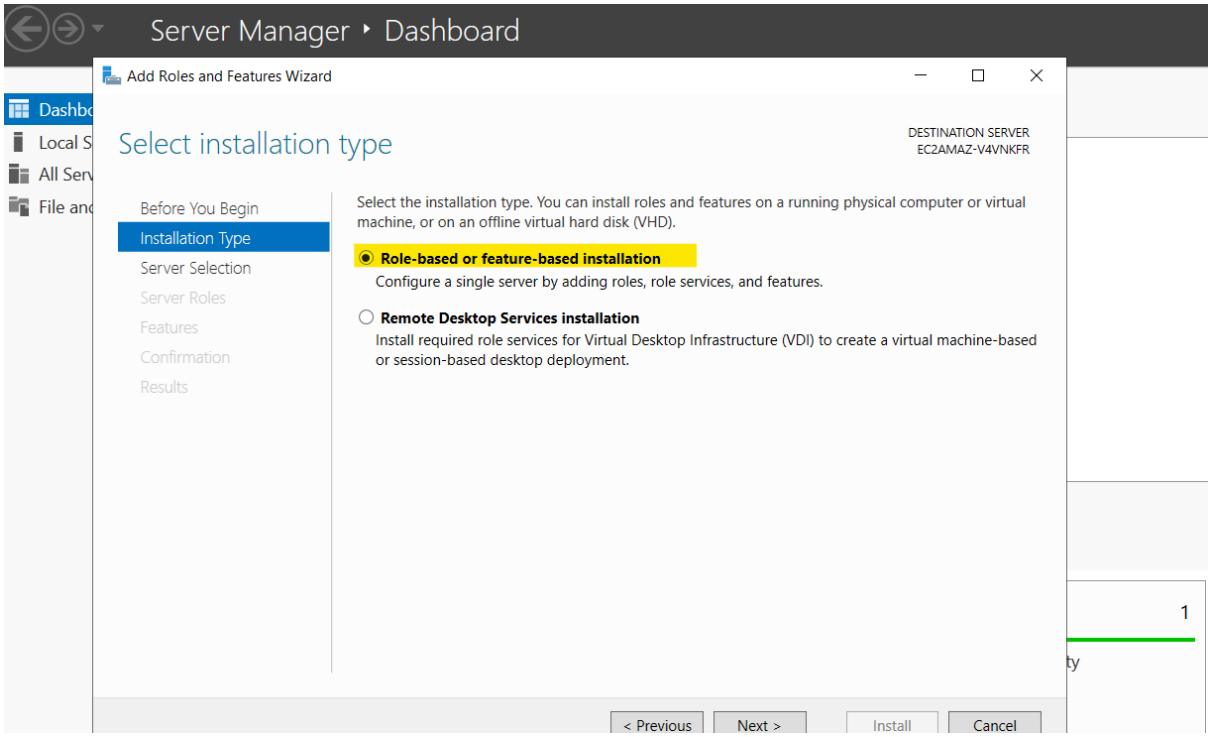
- Login using RDP



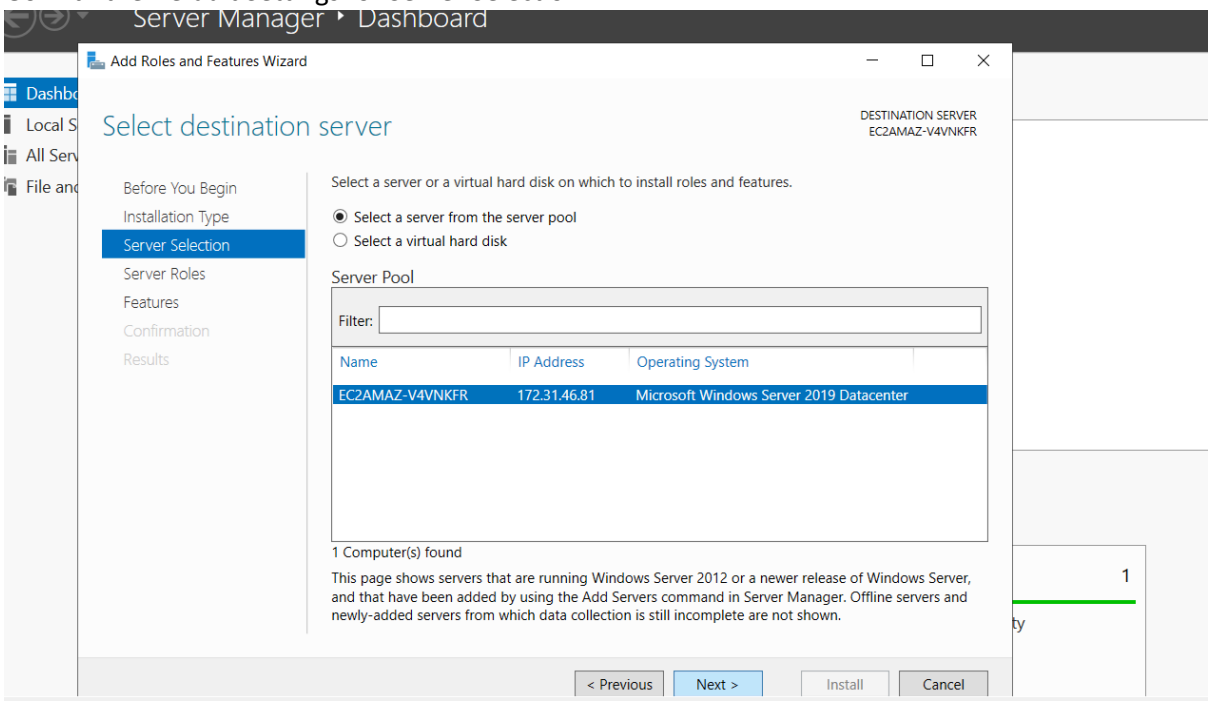
- Once you log in, go to server manager and click on add roles and features



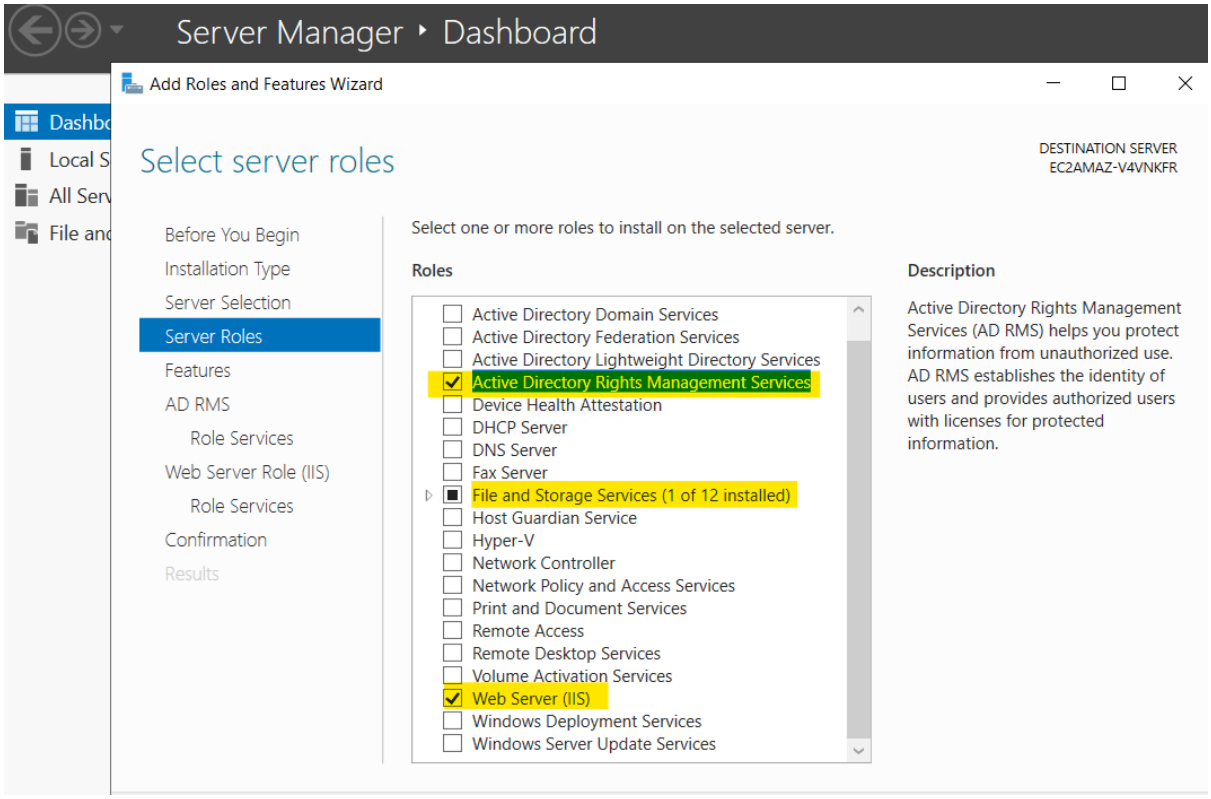
- Start the Installation



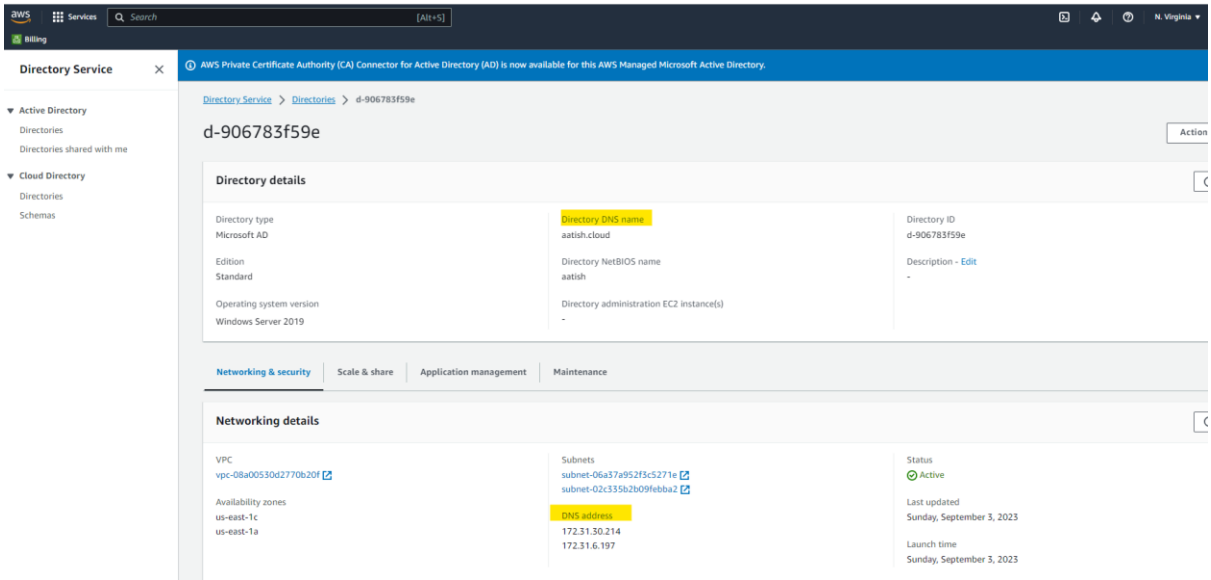
- Go with the Default Settings for Server Selection



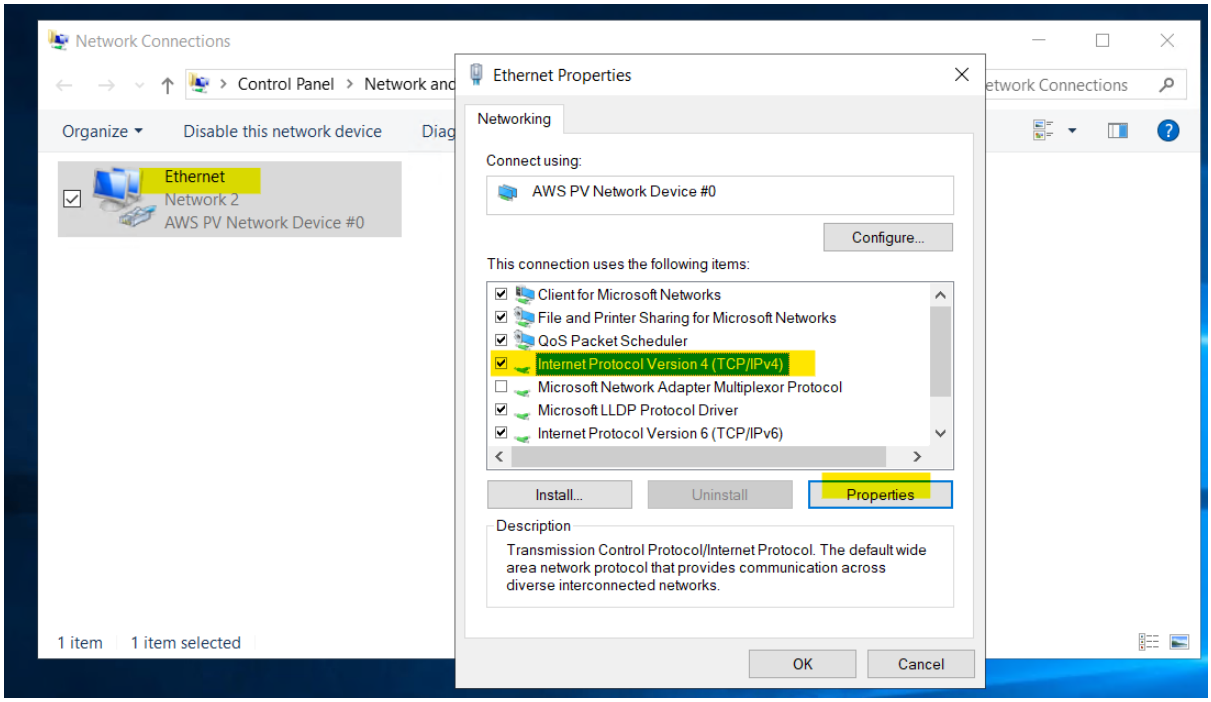
- Server Roles



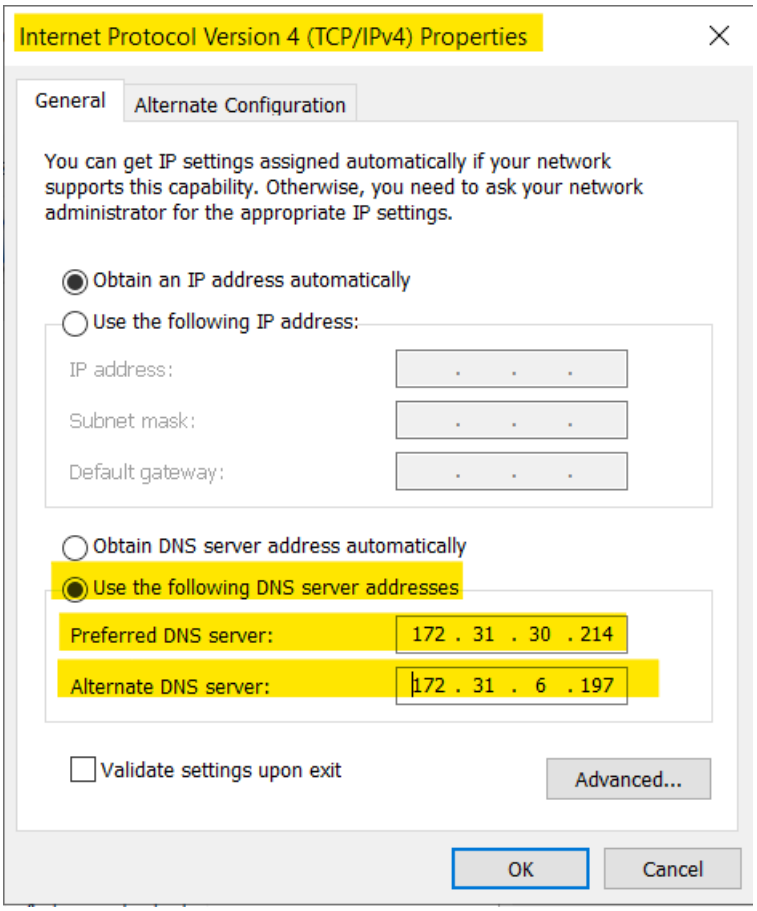
- Double Click on roles administration and Select AD DS And AD LDS tools
- Please click on Next and keep the default settings and Install
- Link the Server with the AWS managed Actice Directory Service
- Collect the DNS Name And the DNS IP



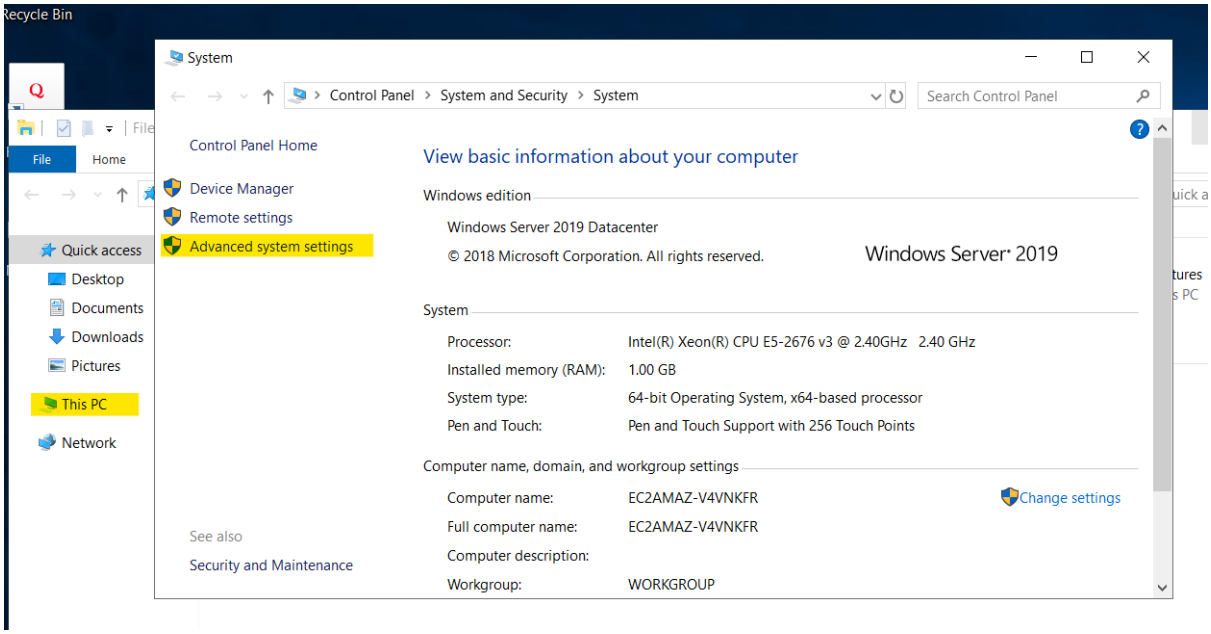
- Add the DNS IP using ncpa.cpl using Run function
- Right click on Ethernet and go properties
- Select Internet Protocol Version 4 (TCP/IPV4) and go to Properties



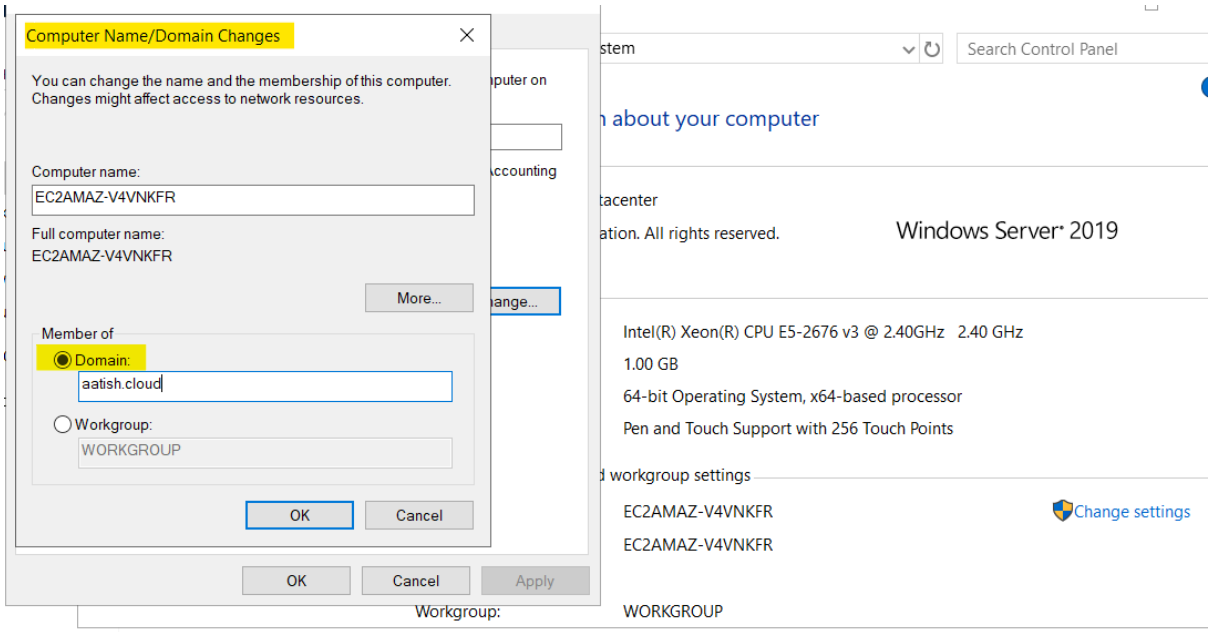
- Select Use DNS Server IP From AWS Directory Service
- And Save/Ok

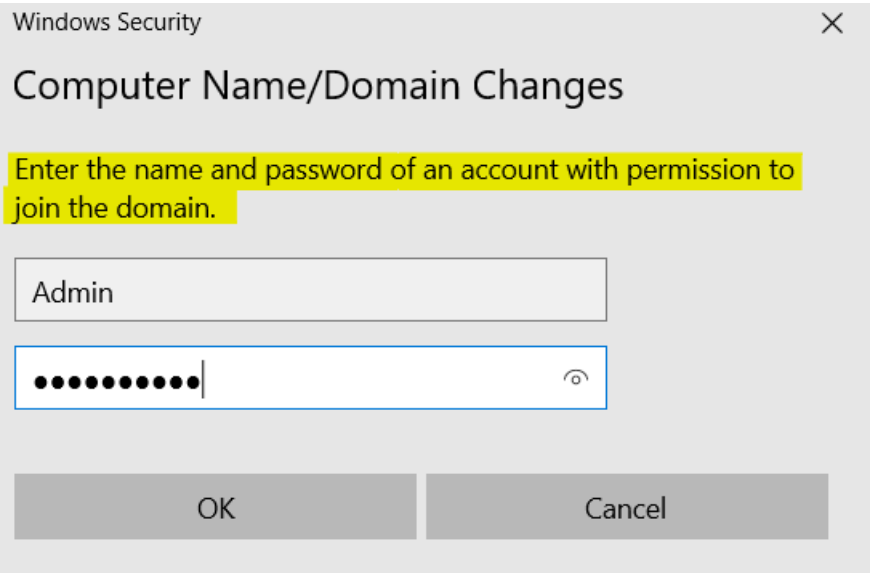


- Go to Files Explorer and Right Click on This PC
- Click on properties
- Click on Advance Settings

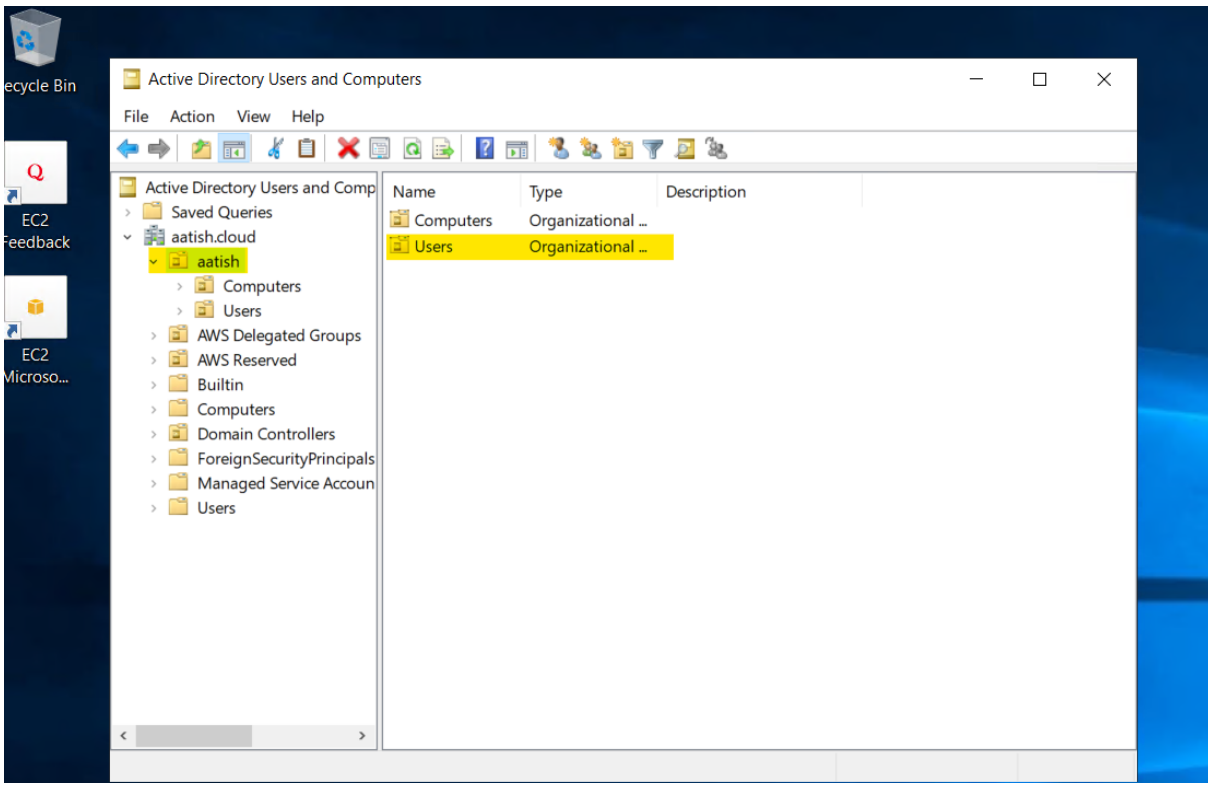


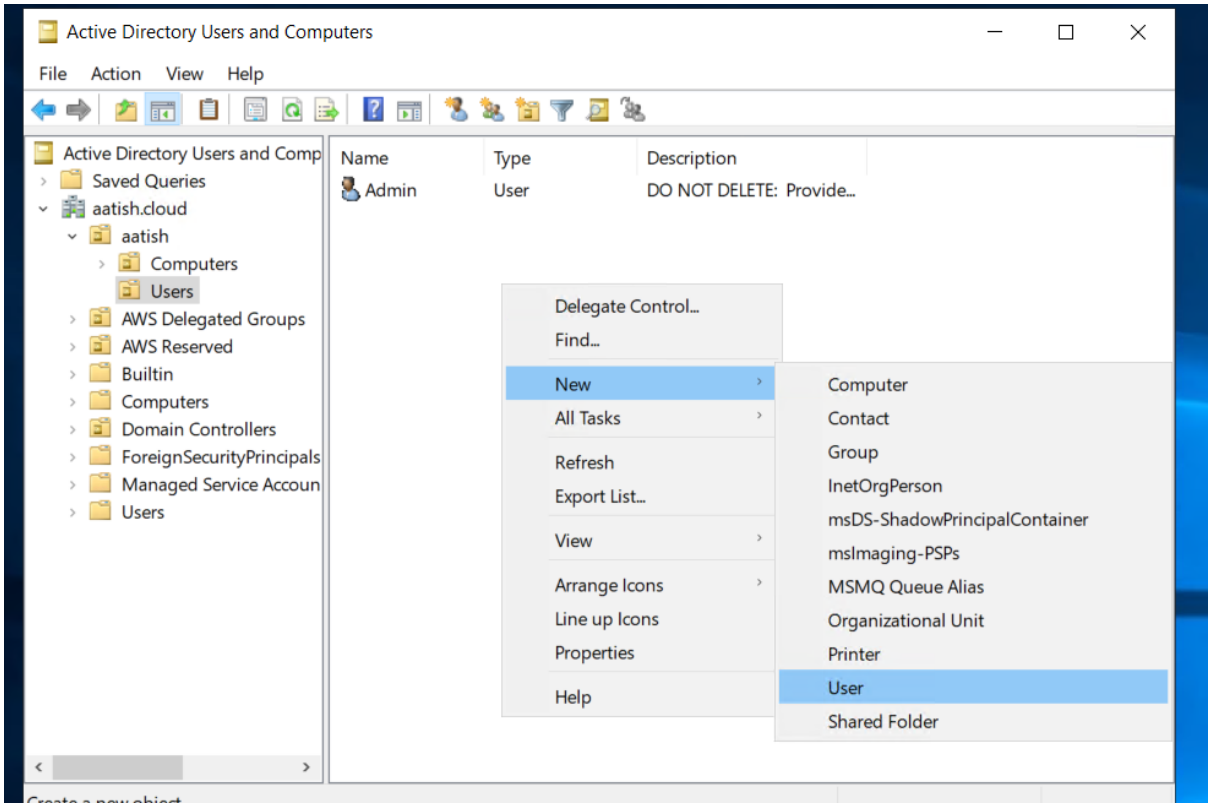
- System Properties will be opened
- Click on Computer Name
- Change the Domain Name same as your AWS Directory Service Name and Save
- And Please Enter the Admin Password Which was created When Creating the Directory Service on AWS
- Once you have Successfully Changed the Domain Name, the System will Restart

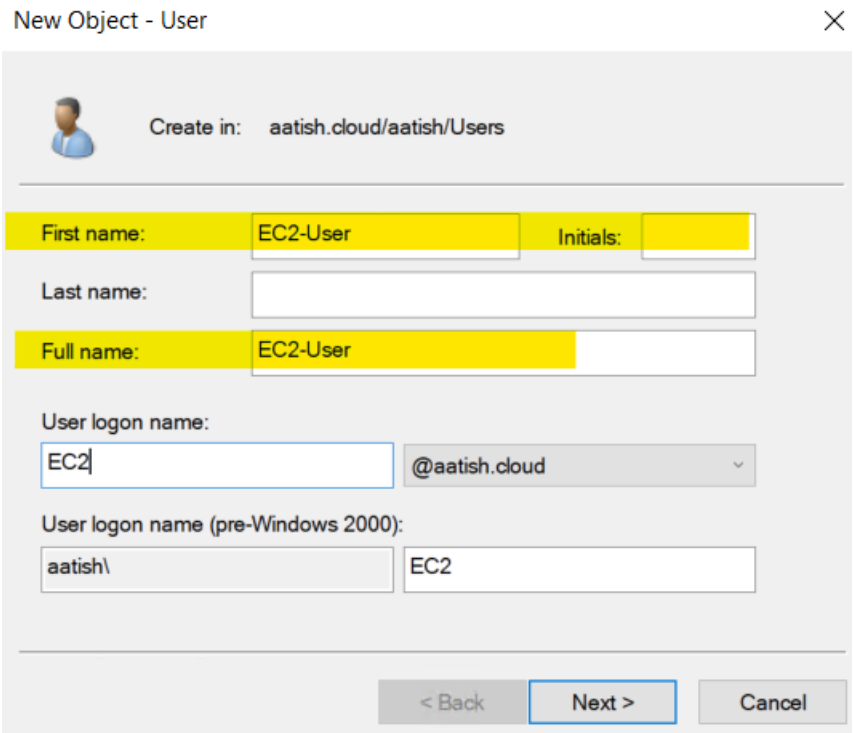


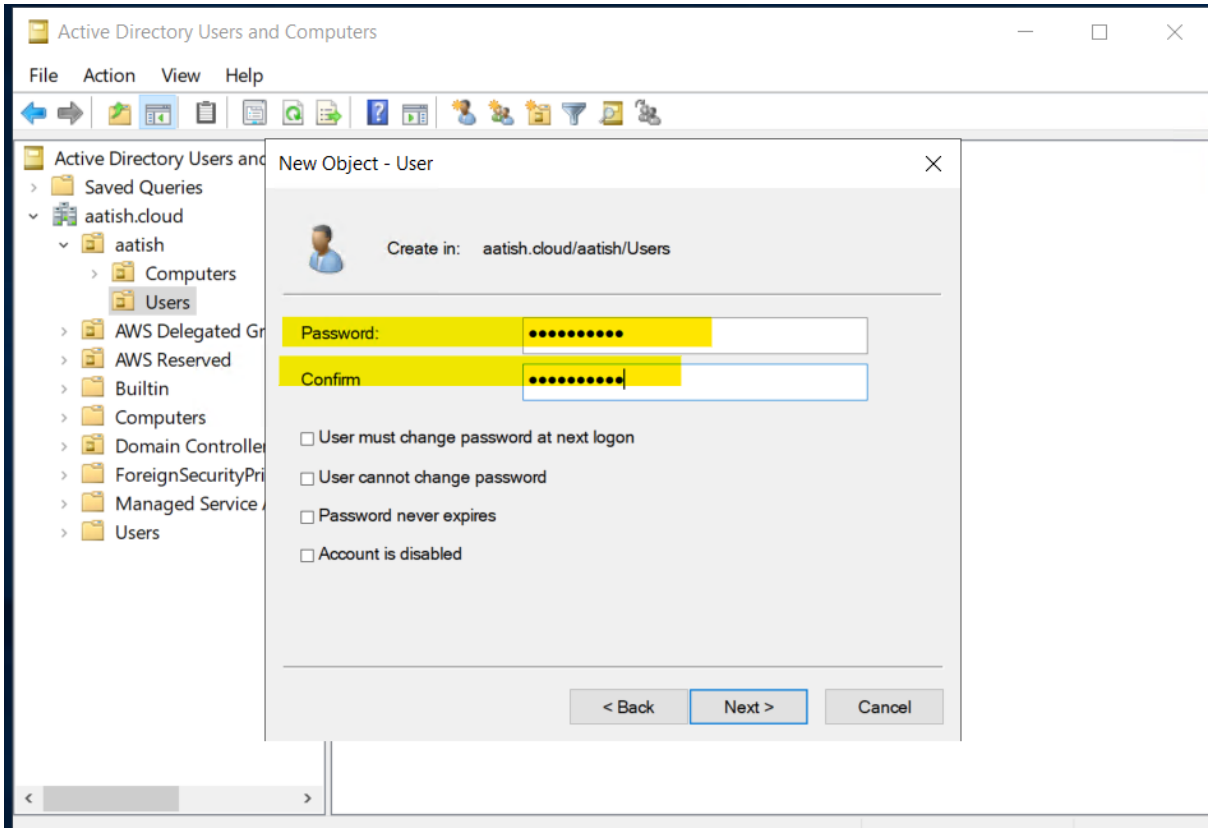


- Now Please Login as Admin@domain.com
- Create User (dsa.msc)
- Create Two User EC2-User and S3-User

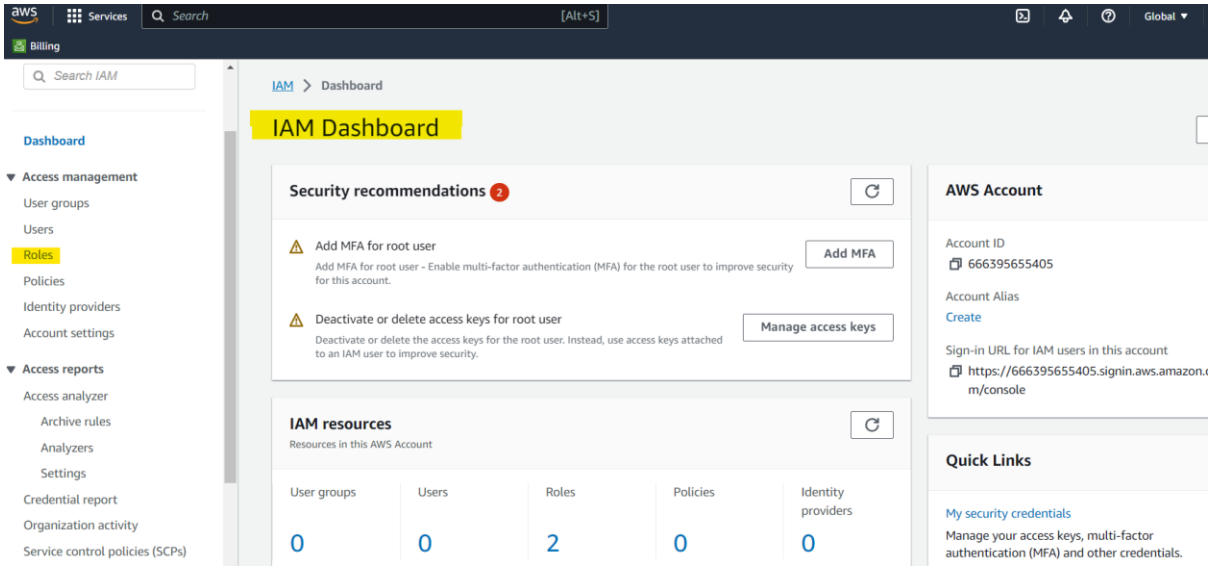



Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Comp
Saved Queries
aatish.cloud
aatish
Computers
Users
AWS Delegated Groups
AWS Reserved
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accoun
Users
Name
Type
Description
Admin
User
DO NOT DELETE: Provide...
Delegate Control...
Find...
New
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder

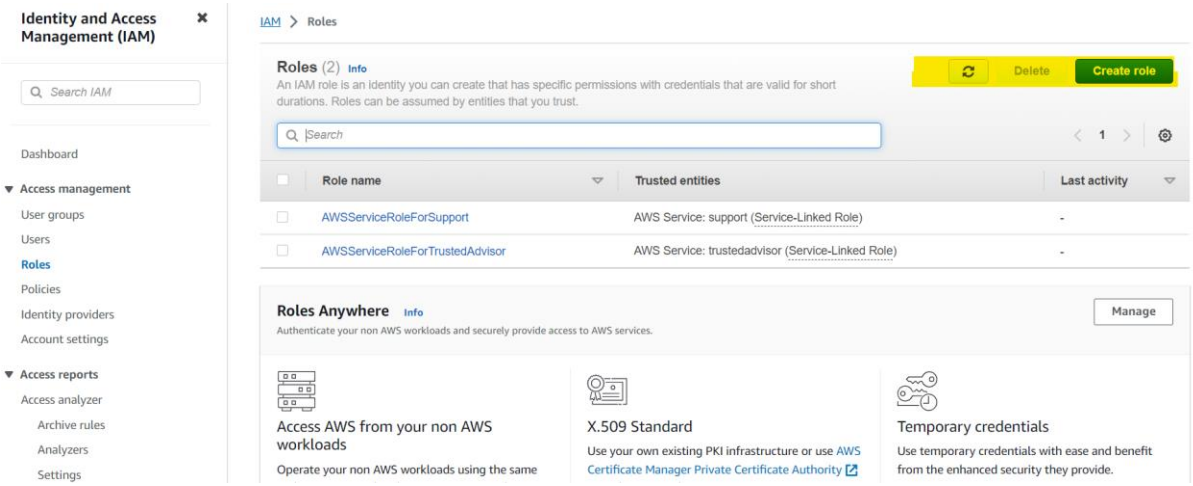

New Object - User
Create in: aatish.cloud/aatish/Users
First name:
EC2-User
Initials:
Last name:
Full name:
EC2-User
User logon name:
EC2
@aatish.cloud
User logon name (pre-Windows 2000):
aatish\
EC2
< Back
Next >
Cancel



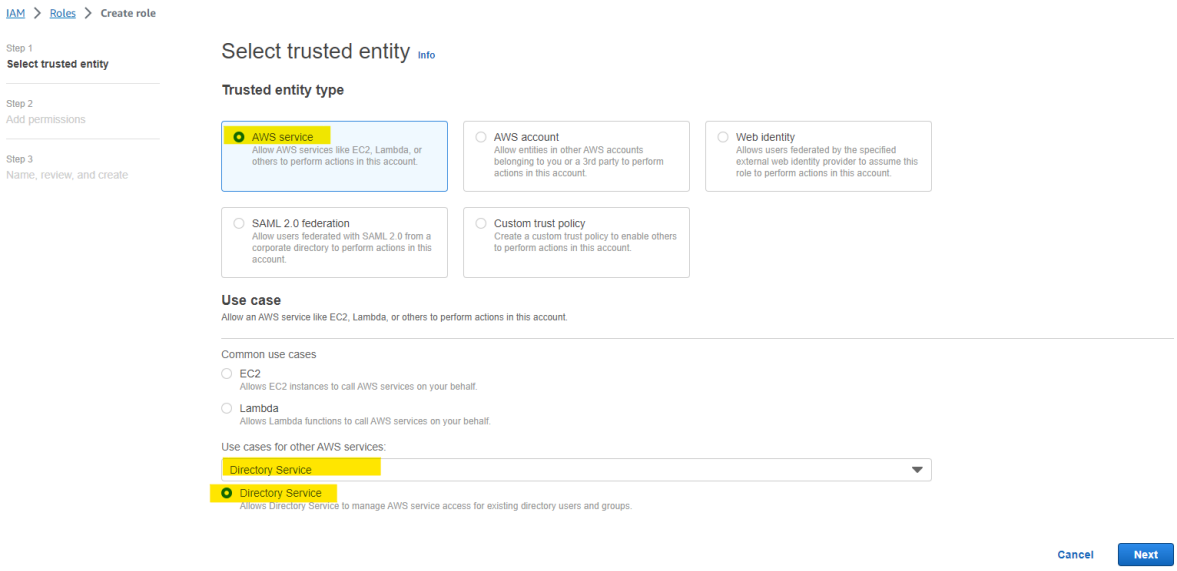
- Go inside AWS Console And Search for IAM
- Create Roles



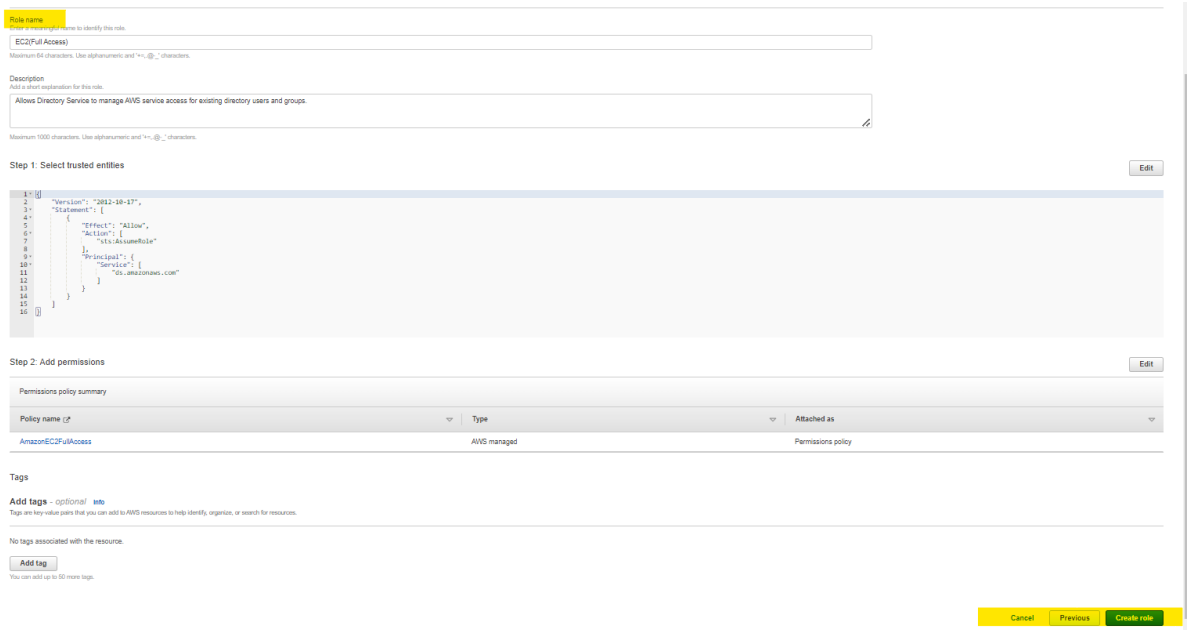
- Click on create roles



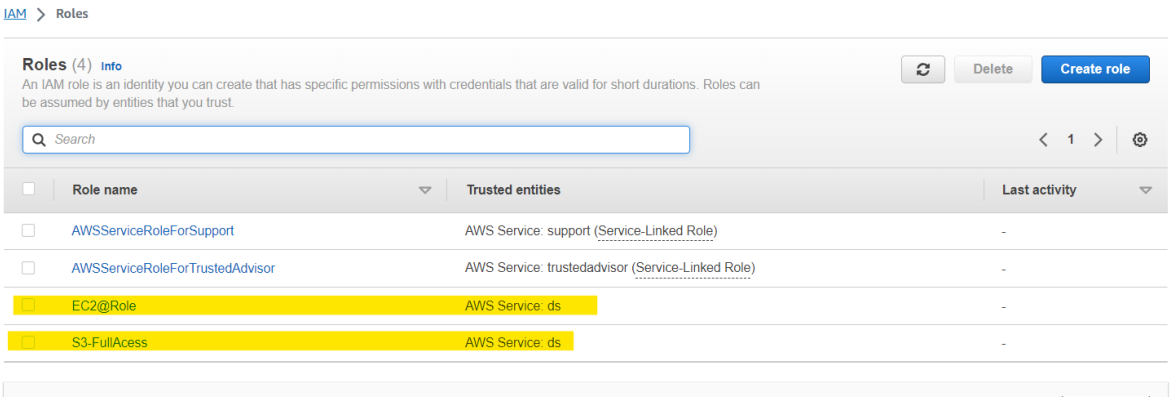
- Create a Role for AWS Directory Services



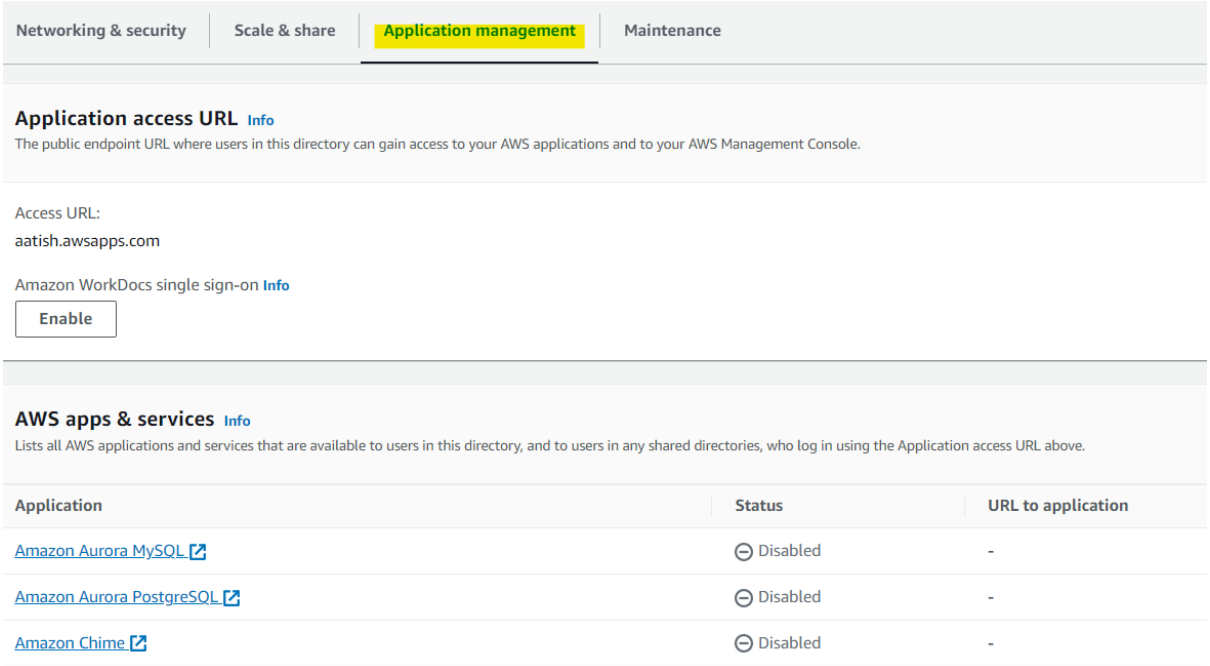
- Select the Roles as EC2 Full Access
- Name, review, and create



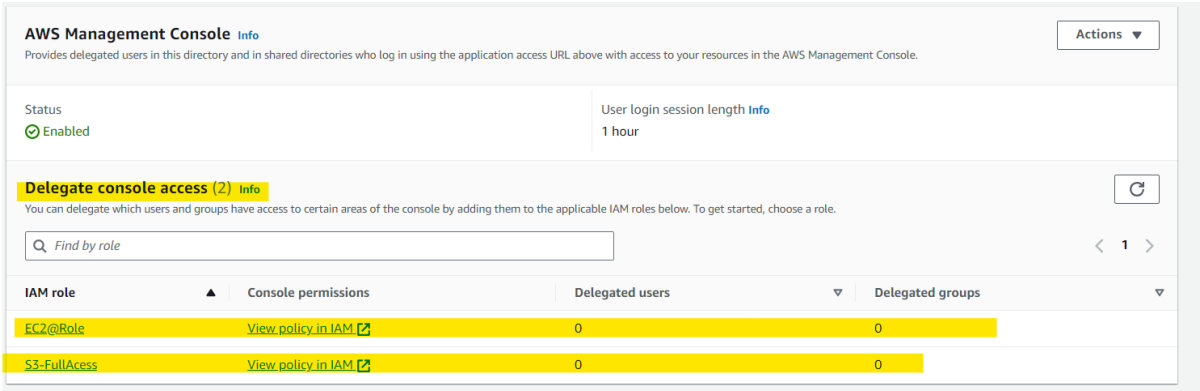
- The roles Should reflect on the Dashboard



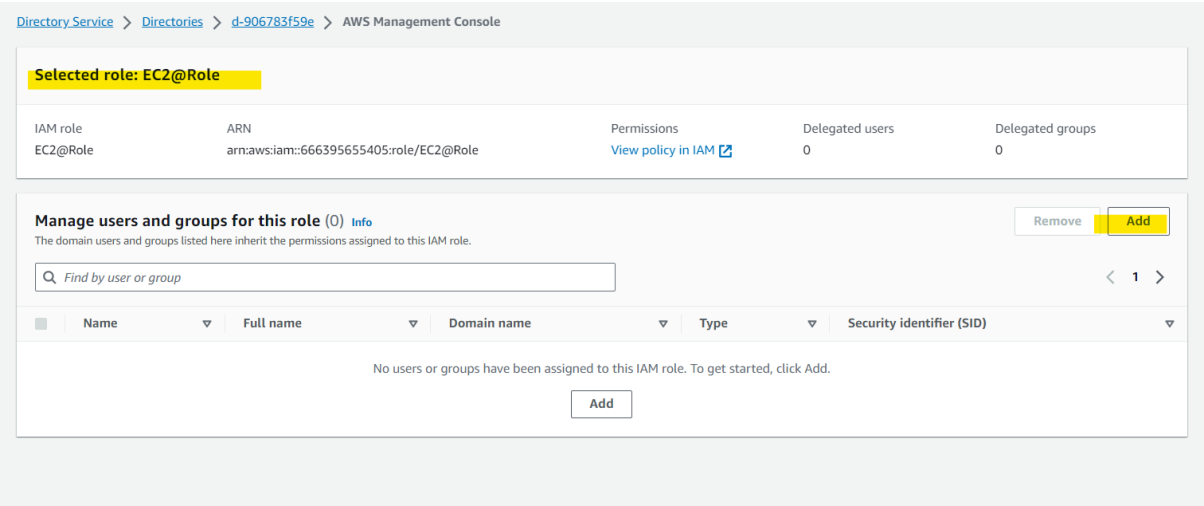
- Assign the roles to the users created
- Go to directory Services (dashboard)
- Click on your Directory and go to Application Management
- Scroll Down to Delegate console access

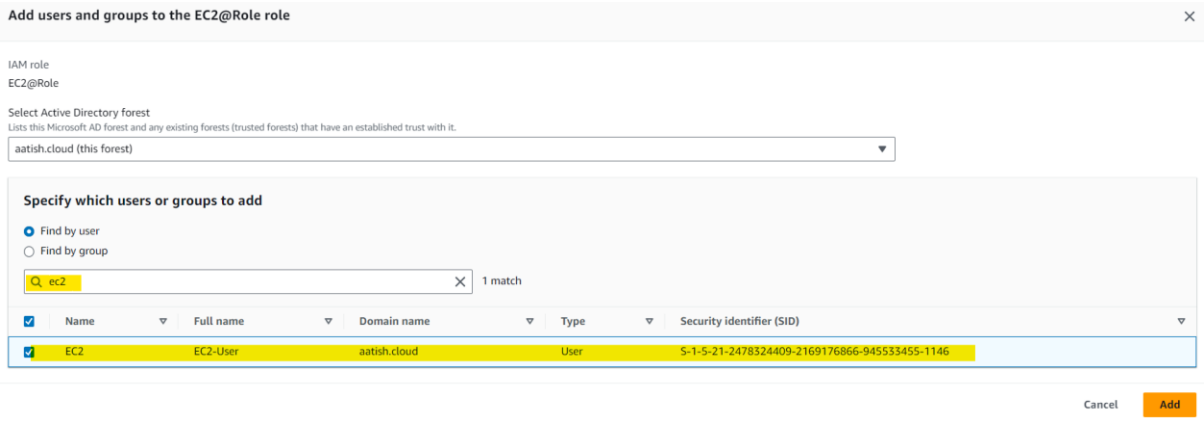


- Click on the Role and assign the roles to the users
- Assign one role to each user



- Click on Add and assign the role





- Click on Application management and Enable Console login to user
- Copy the AWS console URL and check by logging in using your User Credentials