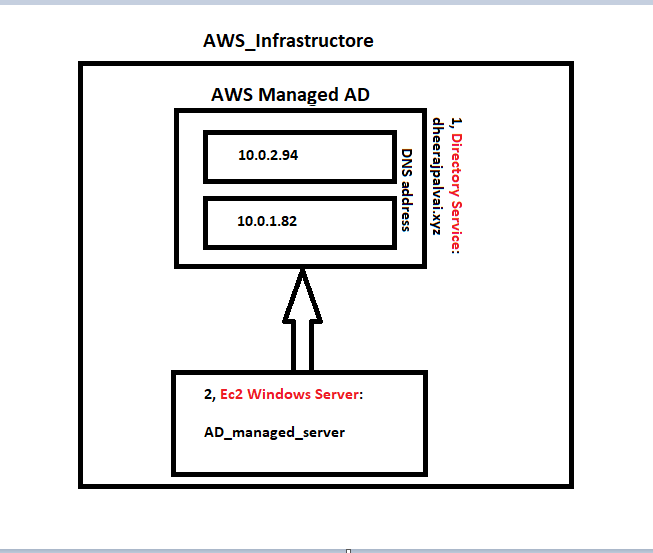
**AWS Managed Microsoft AD:**

* If my Active Directory is already on On-premises (e.g.: Ec2 windows) we use this AWS “AD connector”
* If my Active Directory is not on On-premises we use this “AWS Managed Microsoft AD”

**Lab:**



1, **Directory Service**

Here AWS automatically create two Ec2 servers on two different subnets (we need to create manually)

Security, Identity, & Compliance -> Directory Service -> Directories -> Set up directory -> select "AWS Managed Microsoft AD" -> select "Standard Edition" & Directory DNS name: dheerajpalvai.xyz & Admin password, Confirm Password: 06c61A0542 -> select "VPC" and two public "Subnets" Subnet1 and Subnet2 -> Create directory

* If we click on created Directory -> **Networking & security** -> here we can see “DNS address 10.0.2.94, 10.0.1.82.
* And those DNS address are IP address of Ec2 windows servers, which is created by AWS. Those we can see in “**Scale & share**” -> Domain controllers (2) -> IP address

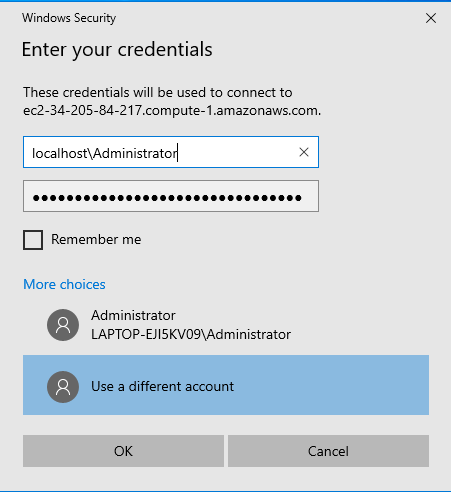
2, **Ec2**

Install two windows servers, in two subnets where we selected in “Directory Service”

i, Ec2 -> “Microsoft Windows Server 2019 Base” -> t2.large ->

Now open windows server -> select “Ec2 windows server” -> connect -> RDP client: click on "Get password" and upload **.pem** file -> Password: .j$sQHTKAikLMKbmobXQSoyhwvVuxYG8

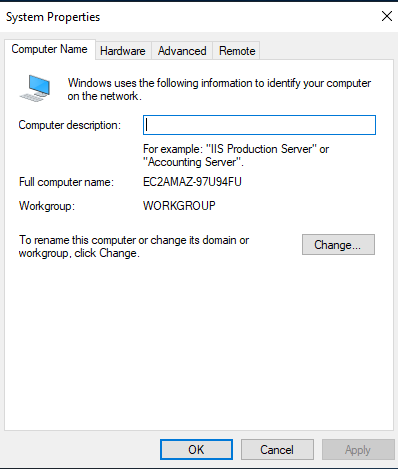
“**Download remote desktop file**”



* Now this a normal Ec2 server, we need to add this server in “Directory Service”

-------------------System Properties-----------------

* Run -> **sysdm.cpl** or (This PC -> RC -> Properties -> Advanced system settings) -> we get “system properties” with “Full computer name:” and “Workgroup”.



After adding this Ec2 server in “Directory Service”, we should get “Domain name” in place of “Workgroup” as “Directory DNS name (dheerajpalvai.xyz)”.

----------------------------

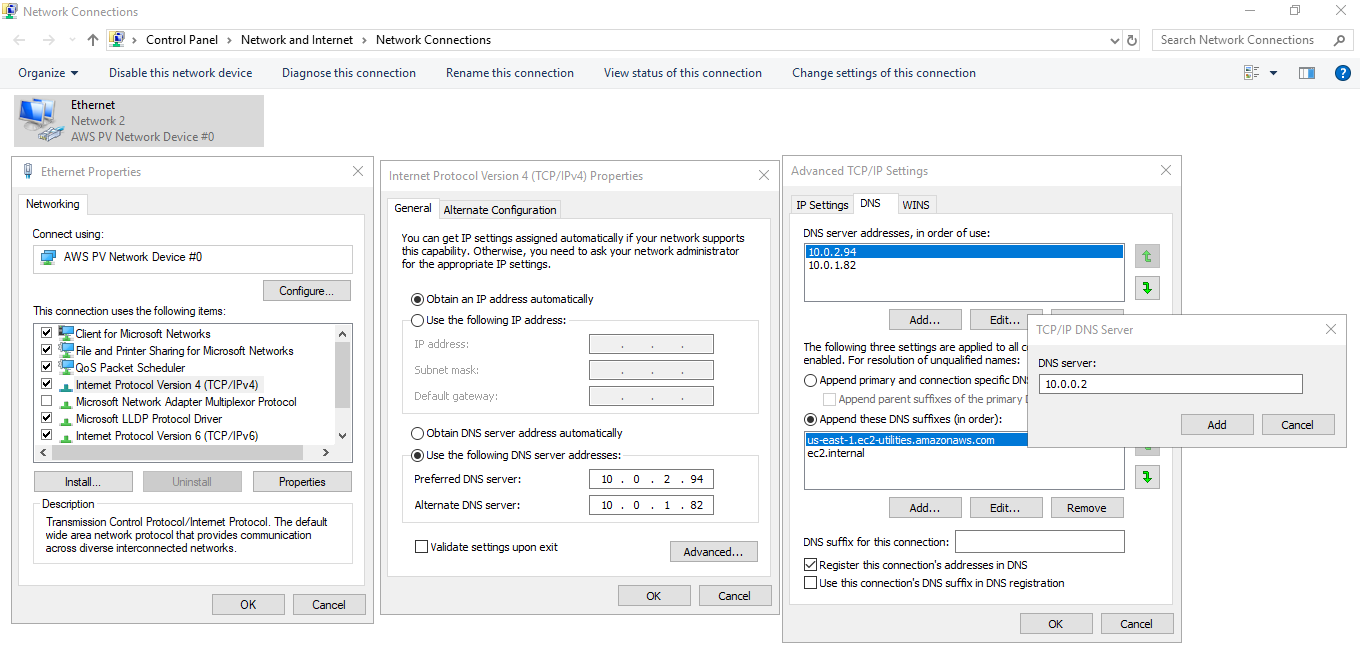
* For that go to “network connections”

Run -> ncpa.cpl or (Control Panel / Network and Internet / Network and Sharing Center / Change adapter settings) -> RC on “Ethernet” network connection -> Internet Protocol Version 4 (TCP / IPv4) -> Use the following DNS server address:

Preferred DNS server: 10.0.2.94

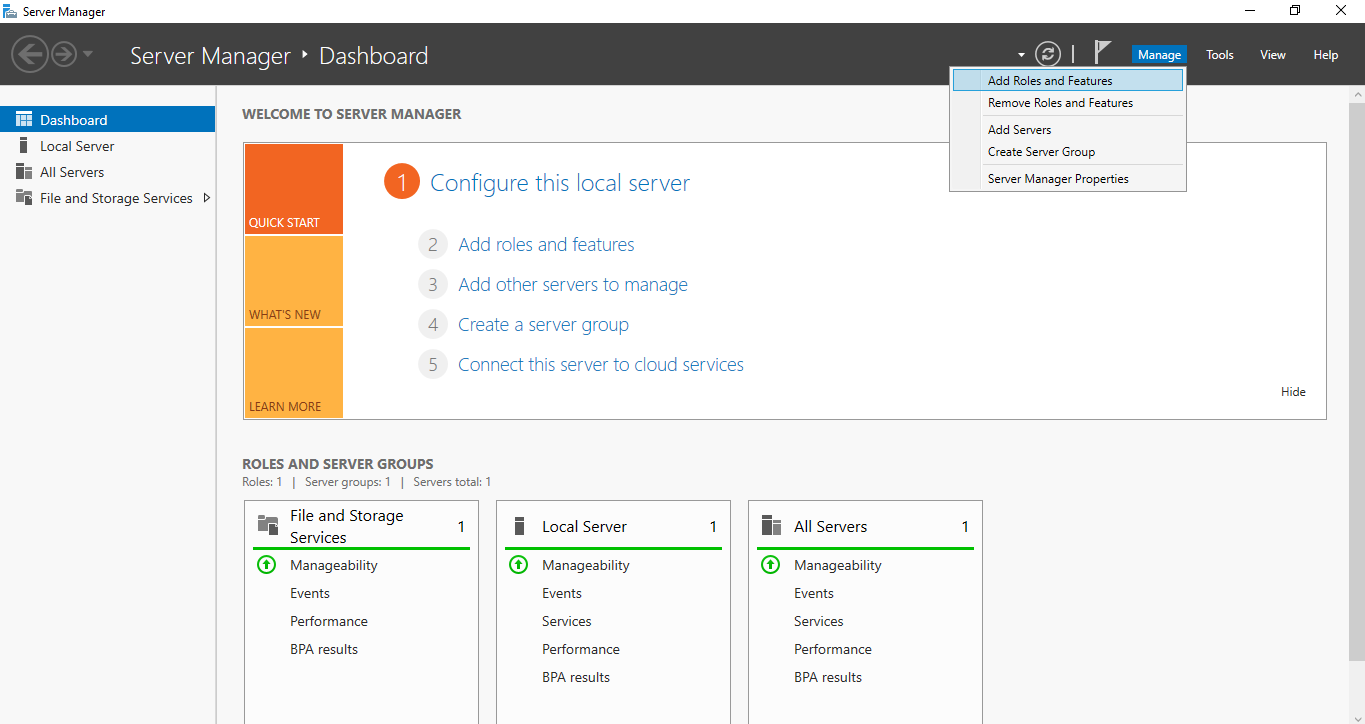
Alternate DNS server: 10.0.1.82

**[**these DNS server ip’s are took from Directory -> **Networking & security** -> here we can see “DNS address 10.0.2.94, 10.0.1.82**]** these servers are managed by AWS -> Advanced… -> DNS: Add… -> DNS Server: 10.0.0.2 (if we go to cmd prompt and type **ipconfig /all** we get **DNS Servers . . . . . . . . . . . : 10.0.0.2**)

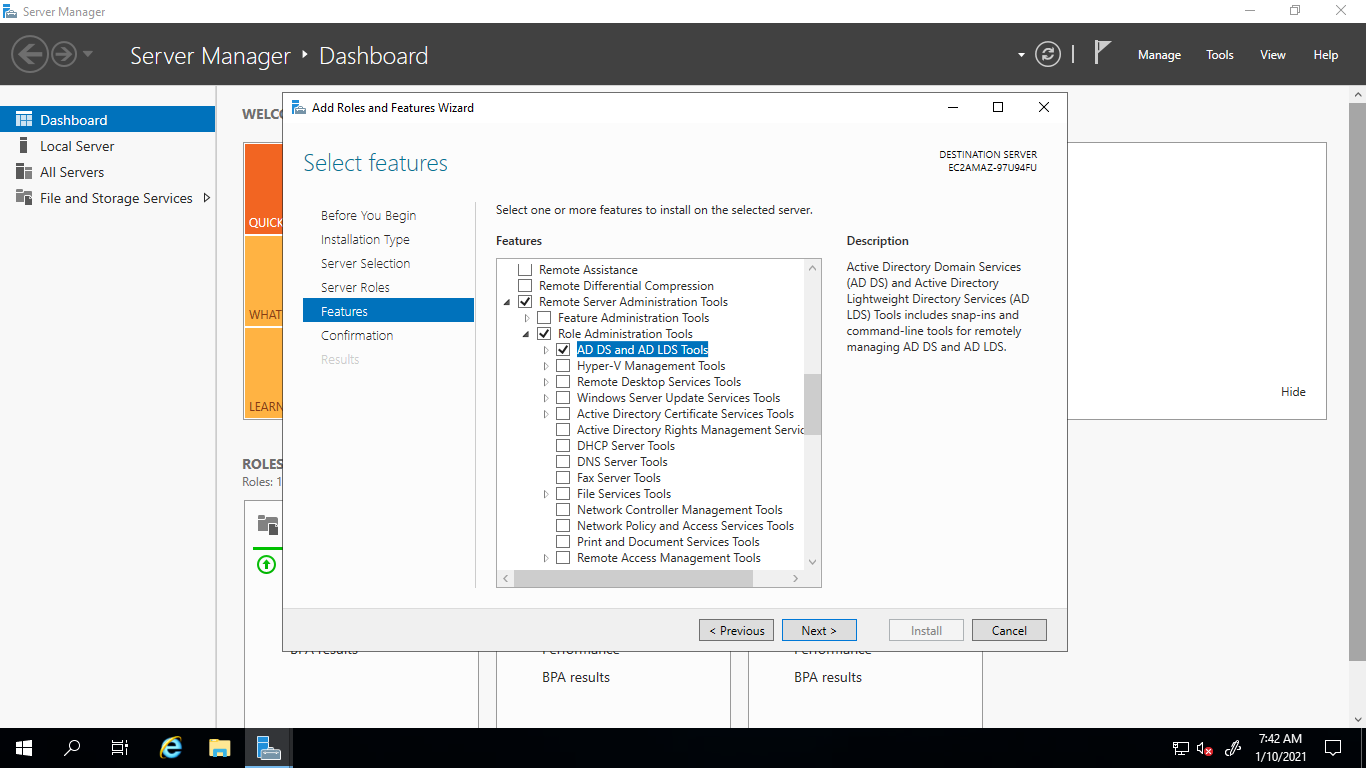


* Now we need some tools to add Ec2 to Directory Domain

Server Manager -> On top click "Manage" and select "Add Roles and Features"



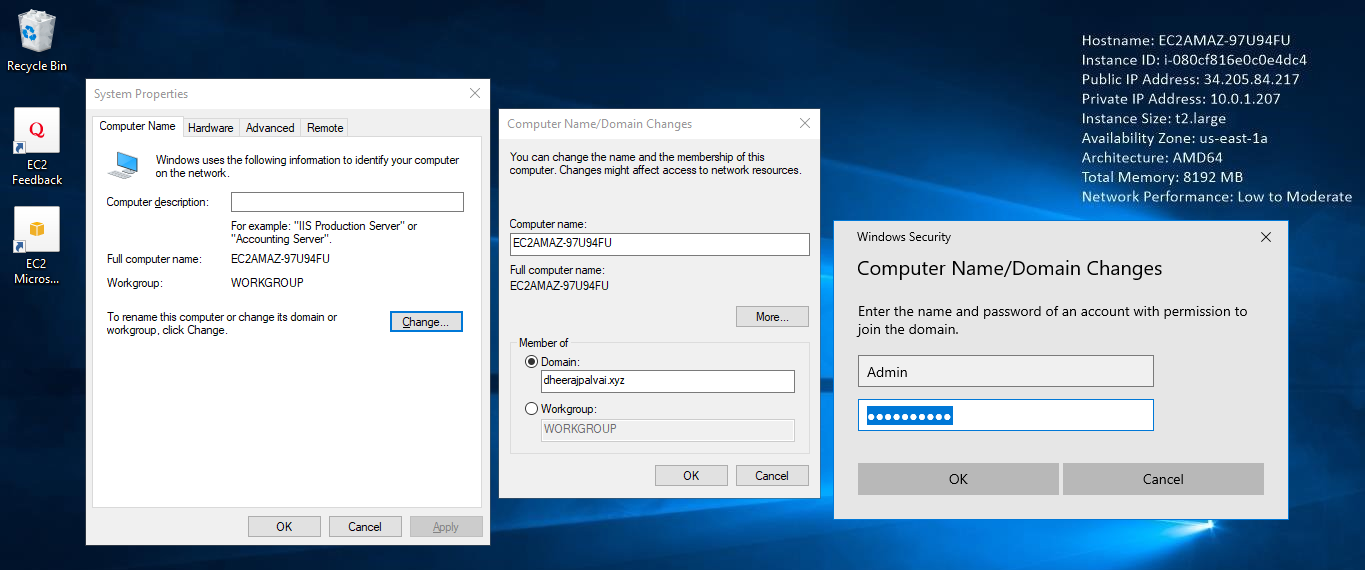
* Here we are not creating Active Directory, so we don’t need “Active Directory Domain Services”, We need Tools for managing Active Directory those tools are “AD DS and AD LDS Tools [Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS)]”
* Go to Features -> Remote Server Administration Tools -> Role Administration Tools **&** Telnet Client (use Telnet Client for Troubleshooting)



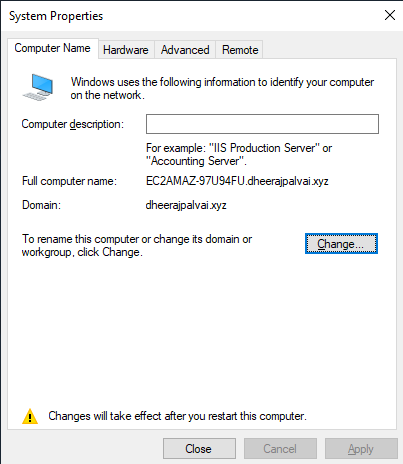
Go to CMD -> ipconfig /all ->we get all DNS address ip’s, that means we are connected to “1, **Directory Service** “

-------------------System Properties-----------------

Run -> **sysdm.cpl** or (This PC -> RC -> Properties -> Advanced system settings) -> we get “system properties” -> click on “Change…” -> Member of – Domain: dheerajpalvai.xyz (dheerajpalvai.xyz is our directory name in “1, **Directory Service**“) -> ok -> Computer Name / Domain Changes – User name: “Admin” & password: “06c61A0542” {When we created directory in “1, **Directory Service**“ we gave password: “06c61A0542” and “Admin” as it's User name}



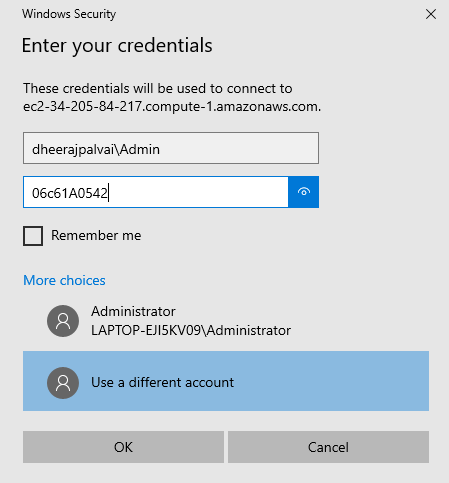
* Now “Workgroup” changes to “Domain”



Server will Reboot now

--------------------------------------------------------------------------------

Now Re-open windows server -> select “Ec2 windows server” -> connect -> RDP client: “**Download remote desktop file**” and Login in domain level (i.e, User name: dheerajpalvai\Admin and password: 06c61A0542)



Create Users: Go to -> Run -> **dsa.msc** -> “Active Directory Users and Computers” -> dheerajpalvai.xyz (we got it since we Logged in domain level ) -> dheerajpalvai -> Users -> RC -> New -> user -> (Ameer, Bobby, Chintu and passwords are 06c61A0542)

3, **AWS Single Sign-On**

Now give Access to these 3 Users (Ameer, Bobby, Chintu) to sub accounts

Integrate AWS to AD==>Security, Identity, & Compliance -> AWS Single Sign-On -> **Settings** -> click on Change

**“Identity source** AWS SSO | [Change](https://console.aws.amazon.com/singlesignon/home?region=us-east-1#/settings$identitySourceWizard)” -> Active Directory ->

**Existing directories in US East (N. Virginia) Region**

dheerajpalvai.xyz (d-906765f893)

**(**this is to integrate AWS Account to Active Directory which is managed by AWS [AWS Managed Microsoft AD]**)**

Assign Users to Sub Account==>Security, Identity, & Compliance -> AWS Single Sign-On -> **AWS accounts** -> select one sub account "dheeraj.nc24@gmail.com" -> Assign Users -> Users -> Search user(Ameer, Bobby, Chintu) and select that user -> Next: Permission sets -> Create new permission set (or) select existing permission set

Login with Users to Sub Accounts==>Security, Identity, & Compliance -> AWS Single Sign-On -> **Dashboard** -> User portal URL: <https://d-906765f893.awsapps.com/start>

(here you login to Sub Accounts with assigned users and his permission limits)

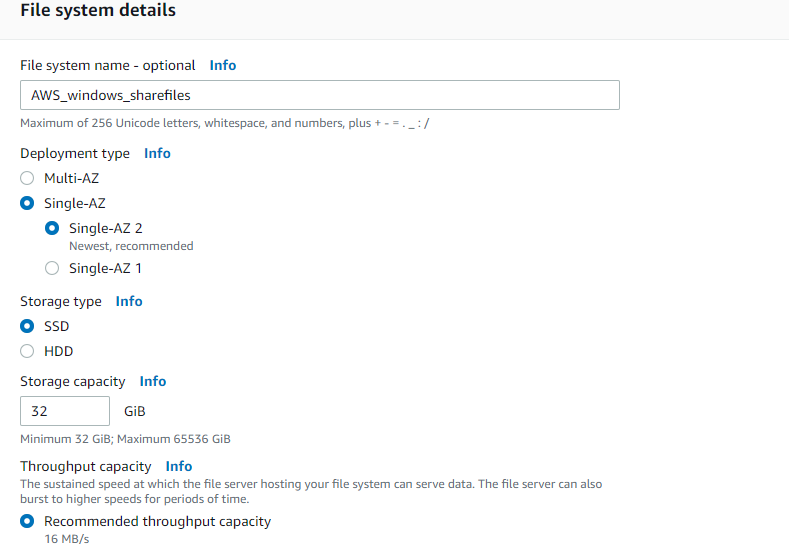
4, **FSx**

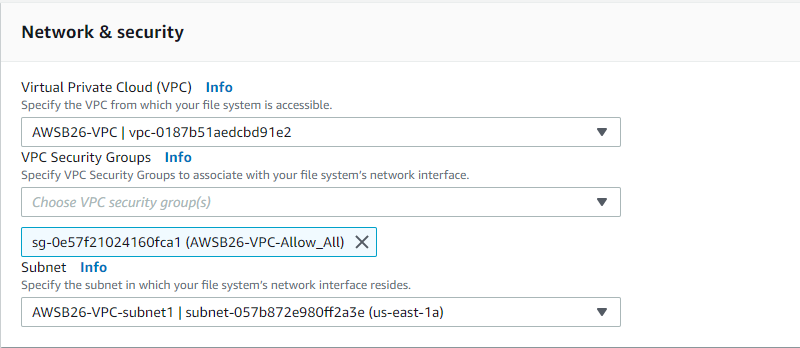
**Is used for “Share folder”**

**File system X** to integrate windows with Active Directory

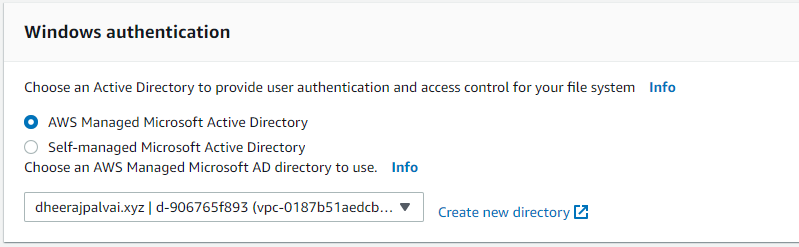
* This is used for share folders in Active Directory

Storage -> FSx -> Create file system ->select Amazon FSx for Windows File Server ->





Here we have to select Directory which is created in “1, **Directory Service**”



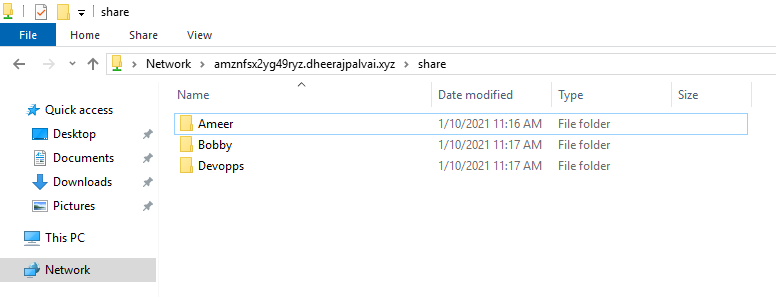
->Now open FSx -> File systems -> fs-0845c1630cfcfff38 -> Network & security -> DNS name: amznfsx2yg49ryz.dheerajpalvai.xyz (copy DNS name)

2, **Ec2**: creating folders in share folders and giving permissions to users on that folder

**Ec2** -> AD\_managed\_server -> open as Admin -> open with Domain level: Username: dheerajpalvai\Admin & Password: 06c61A0542

Run -> \\amznfsx2yg49ryz.dheerajpalvai.xyz (copy DNS name) \share

Create 3 folders in Share folder -> like this

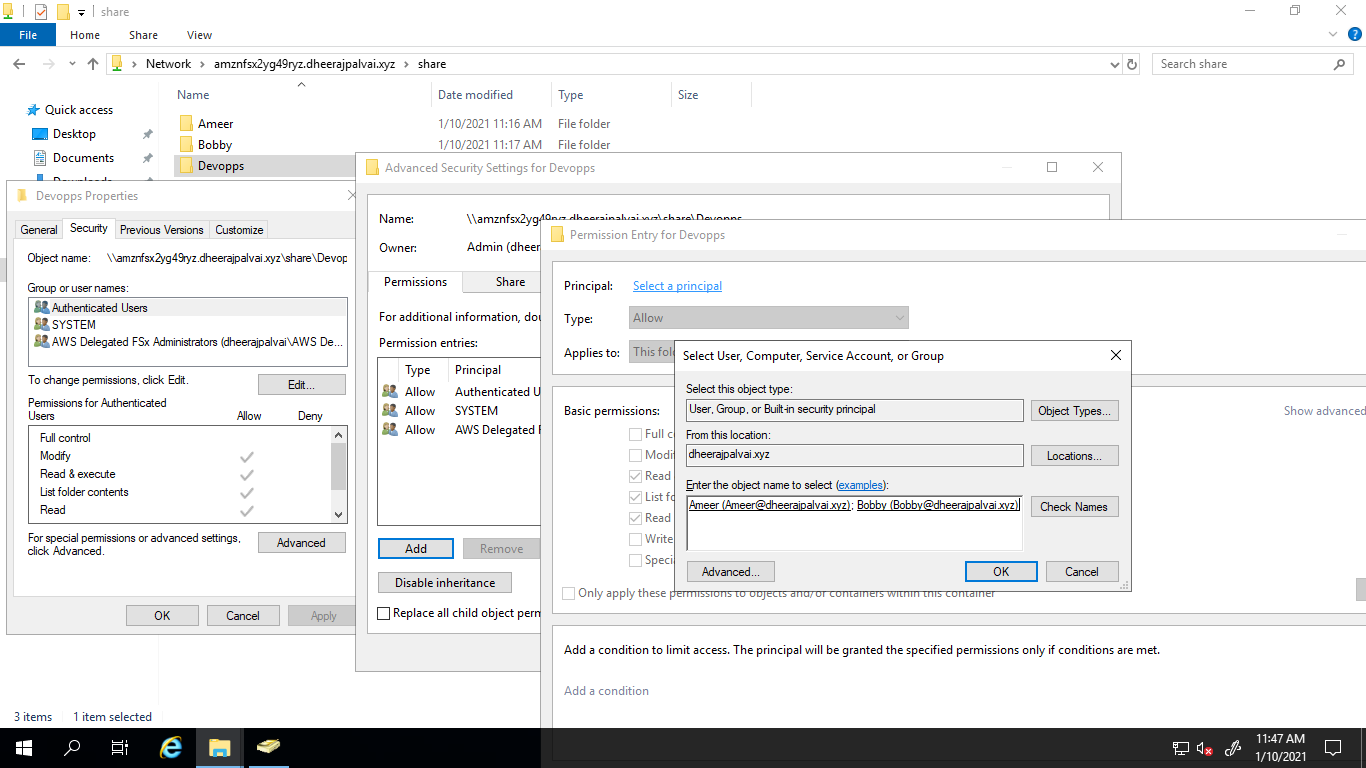


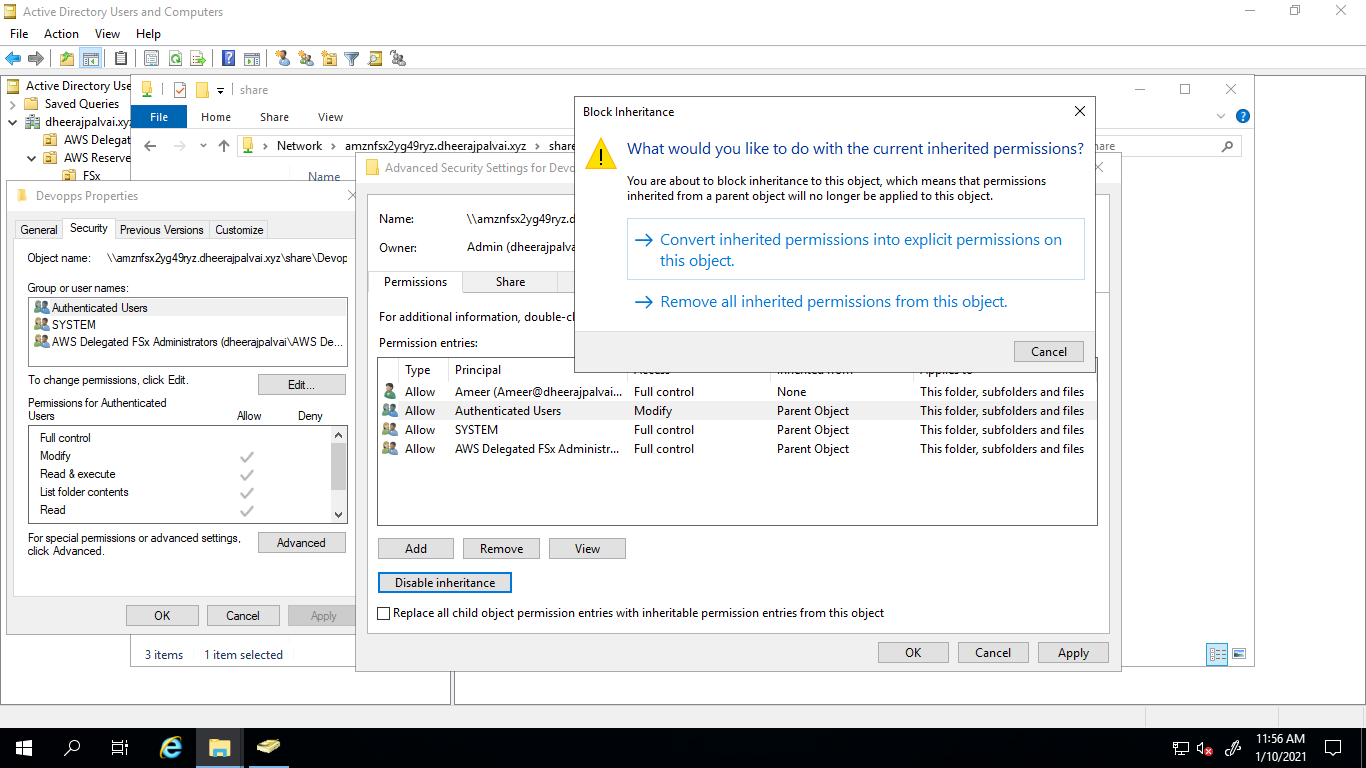
Give permission to user for that folder

RC on Ameer (folder kept same name of user for easy naming convention) -> Properties -> Security -> Advanced -> Add -> select a principle -> Enter users and assign permissions to that users on that folders. -> give “Full control” -> Remove other’s Permissions “Disable inheritance” & Remove.

* One user can not open a folder who has no permission

Eg: Ameer can not open the folder of Bobby but can open common folder i.e, Devopps





**2, Ec2:** Giving permissions to users to login server in user level

**Ec2** -> AD\_managed\_server -> open as Admin -> open with Domain level: Username: dheerajpalvai\Admin & Password: 06c61A0542

Run -> **lusrmgr.msc** (Local users and groups) -> Groups -> RC on “Remote Desktop Users“-> Properties -> Add.. -> Ameer; Bobby

**Shut Down…**

**Ec2** -> AD\_managed\_server -> open as User Ameer -> open with User level: Username: dheerajpalvai\Ameer & Password: 06c61A0542

Run -> \\amznfsx2yg49ryz.dheerajpalvai.xyz (copy DNS name) \share

Ameer can access only his folder and common folder

(or)

**Ec2**

Install new Ec2 Windows server -> t2.large -> Domain join directory: dheerajpalvai.xyz (d-906765f893) & IAM role: click on “Create new IAM role” that contain **AmazonSSMManagedInstanceCore** and **AmazonSSMDirectoryServiceAccess**,Role name: “User\_login\_Role” -> IAM role: “User\_login\_Role” -> Key: Name & Value: User\_Desktop

**Ec2** -> User\_Desktop -> open as Admin -> open with Domain level: Username: dheerajpalvai\Admin & Password: 06c61A0542

Run -> **lusrmgr.msc** (Local users and groups) -> Groups -> RC on “Remote Desktop Users“-> Properties -> Add.. -> Ameer; Bobby

**Shut Down…**

**Ec2** -> User\_Desktop -> open as User Ameer -> open with User level: Username: dheerajpalvai\Ameer & Password: 06c61A0542

Run -> \\amznfsx2yg49ryz.dheerajpalvai.xyz (copy DNS name) \share

To create shortcut for Share folder: This PC -> computer (on top menu) -> Map network drive

Ameer can access only his folder and common folder

Note: if I want to know who recent Login User is?

Go to CMD -> **set**

We get recent user details

**Workflow**: [Directory services (DNS Address IP’S dheerajpalvai.xyz) – Ec2 windows server (localhost\administrator -> ncpa.cpl -> Add tools ->sys prop DNS Address IP’S -> Login with dheerajpalvai\Admin) - AWS SSO(AWS AD connect AWS Directory services) – FSX (share folder) - Ec2 windows server(share folder -> User access permission to folder -> lusrmgr.msc -> Login with user dheerajpalvai\Ameer)]