Setting Up Active Directory lab

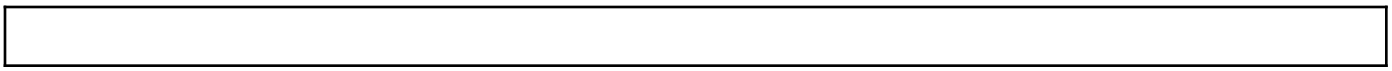
By Michael N (mm0)

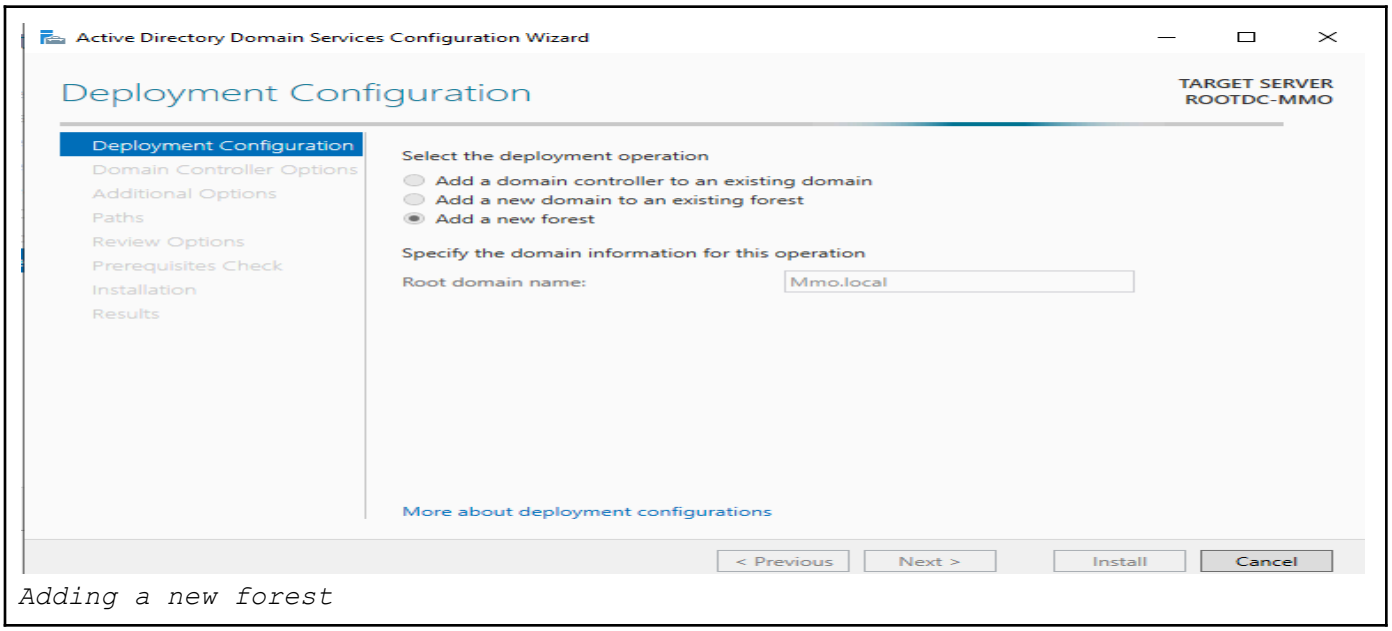
Setting up Domain Controller

I am using the windows server 2022 eval image for my domain controller. And windows 10 eval image for both of my users in this lab.

In This write up I will be showing the steps I took to set up my active directory environment where I will be conducting pen-testing experiments/labs exploiting active directory and performing different types of attacks.

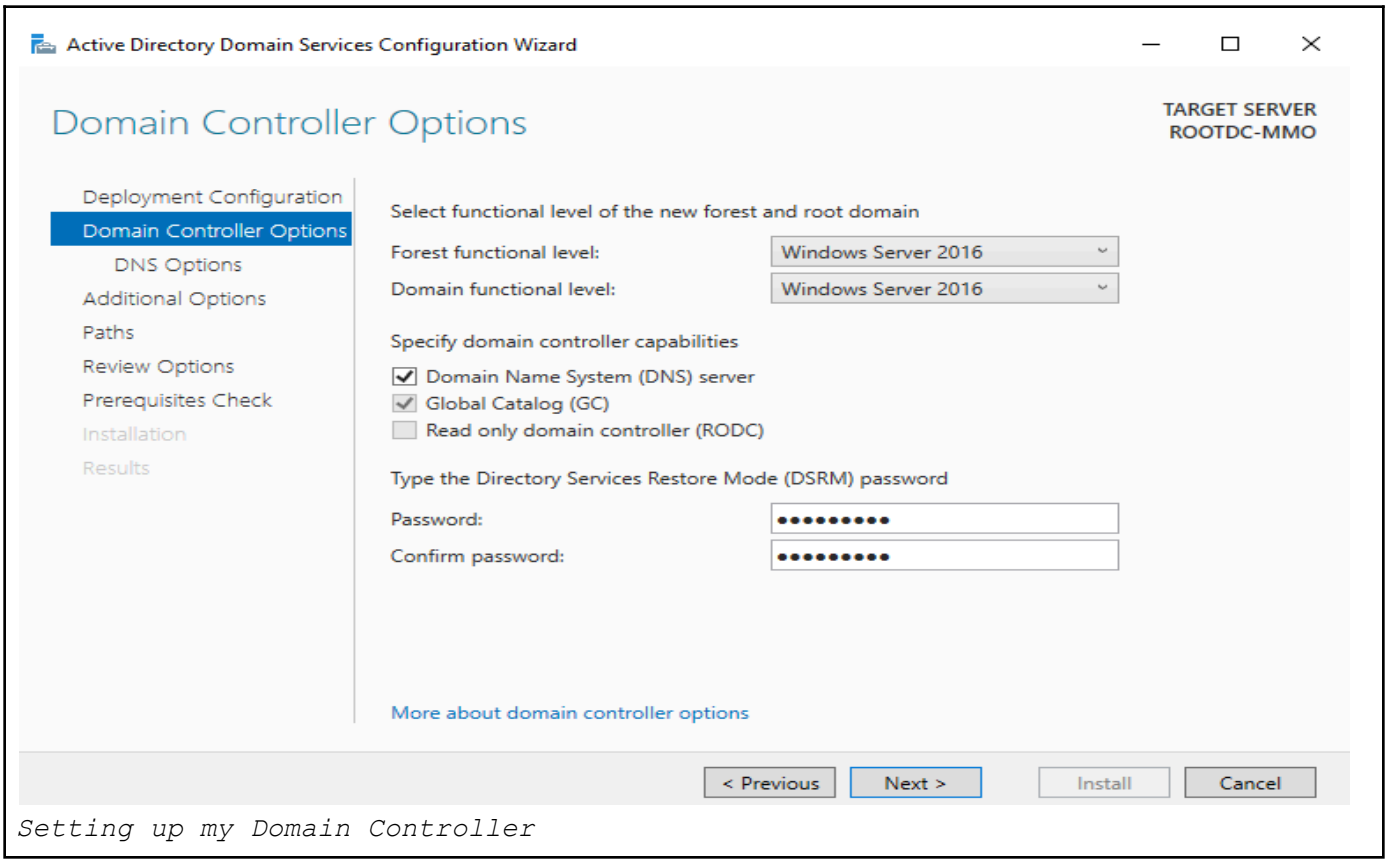
Installing the Server





Adding a new forest

Active Directory forest is a logical component that is a collection of one or more domains that share a common root domain. I created my domain called *'mmo.local'* .
For the rest of my lab I will be creating network shares and doing my pen-testing lab within this domain.



Setting up my Domain Controller

Our AD DS has **DNS service** built into it to add the capability for clients to locate the Domain controllers, and for Domain controllers to locate each other to facilitate communication. The DNS is an essential part of this lab.

Learn more: DNS and AD DS | Microsoft Learn

The **Global Catalog(GC)** is used whenever needing to access and locate objects outside of its domain.

- In AD DS it contains 4 partitions by default.
    1.) **Schema Partition** - classSchema and attributeSchema objects
    2.) **Configuration Partition** - replication topology

3.) **Domain Partition** - directory objects

4.) **Application Directory Partition** - fine-grained control over replication scope.

The partitions are also known as Naming contexts.

The Global Catalog(GC) acts as a tool within Active Directory users to access and locate objects in a domain tree based on one or more attributes of the Target Objects. The Global Catalog contains a partial replica of every naming context which makes it easy for objects to be accessed and located without knowing the Distinguished name(DN).

Learn more: Global Catalog - Win32 apps | Microsoft Learn

Domain controller forest, and domain functional level we can see that it enabled some key features. Different functional options add or remove certain features.

The domain functional level isn't too important for the lab but just to give a bit of a background as to why I'm using Windows Server 2016 and what the functional level is.

What is domain, and forest functional level?

- When setting up an Active Directory environment, earlier I created a new forest with my domain called 'mmo.local' but now that I have this domain, how am I going to manage resources, users, and other domain objects? well.. with an AD DS.

  What is AD DS?

- The way I imagine AD DS is it is a Big database that stores Domain Objects which is everything we need to successfully manage our active directory network.

- AD DS has many different services and components which can be physical components and logical components which form the core of networks that use windows OS.

- The AD DS gives us an easy way to manage and search for objects and with a hierarchical directory structure and allows us to add security and configuration settings.

Why Windows Server 2016 functionality with Windows Server 2022 OS

- This lab is a part of the PJPT cert from TCM, the instructor is using a windows 2016 server eval image so the functionalities that he has within his forest and domain is limited to windows server 2016. So therefore by me setting it down to windows server 2016 I'm able to match that functionality level. Also the latest functional level that was released from microsoft is Windows server 2016.

- Depending on the functionality level this can change which OS is compatible on the Domain Controller.

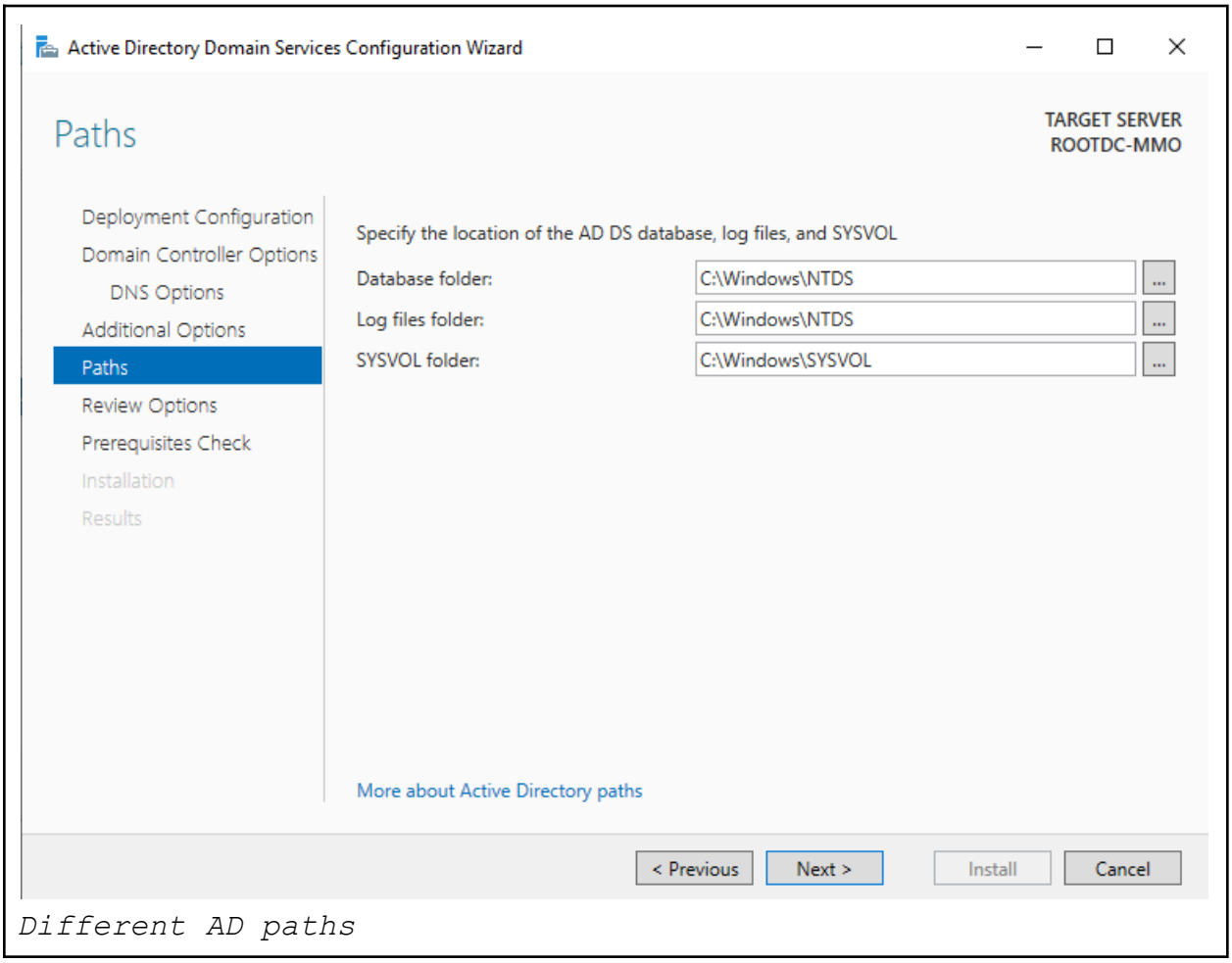
Windows Server 2016 functional levels

Supported domain controller operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Source:
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels

The reason I mention this is generally from my understanding when setting up an AD DS we should be using the highest forest and domain functional level supported.



Different AD paths

Here's an answer I got using Microsoft Copilot, the world's first AI-powered answer engine. Select to see the full answer or try it yourself. https://sl.bing.net/fBz5z3EBFBs

Database folder: NTDS folder contains a ISAM(*indexed and sequential access method*) database which uses ESE(*Extensible Storage Engine*). The '*Ntds.dit*' is the database file where all the active directory data is stored, so domain info and configuration info can be found here.

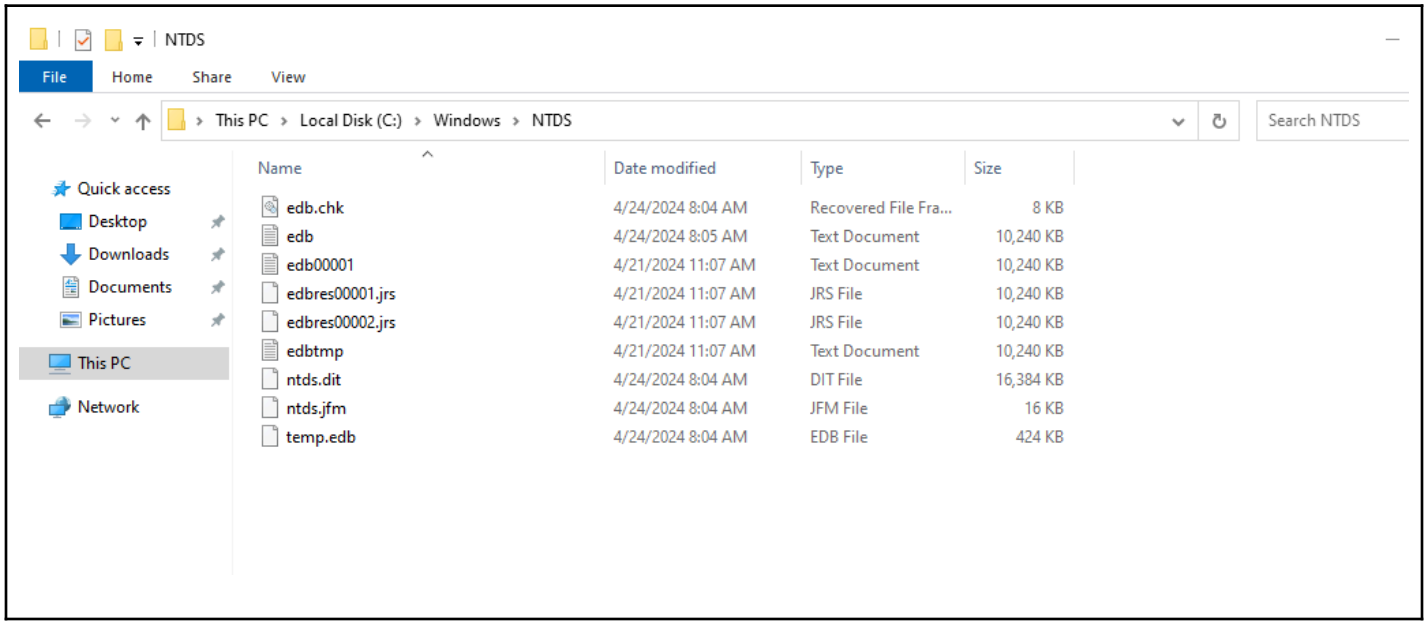
Upon doing more research i learned that the Ntds.dit database contains 3 main tables

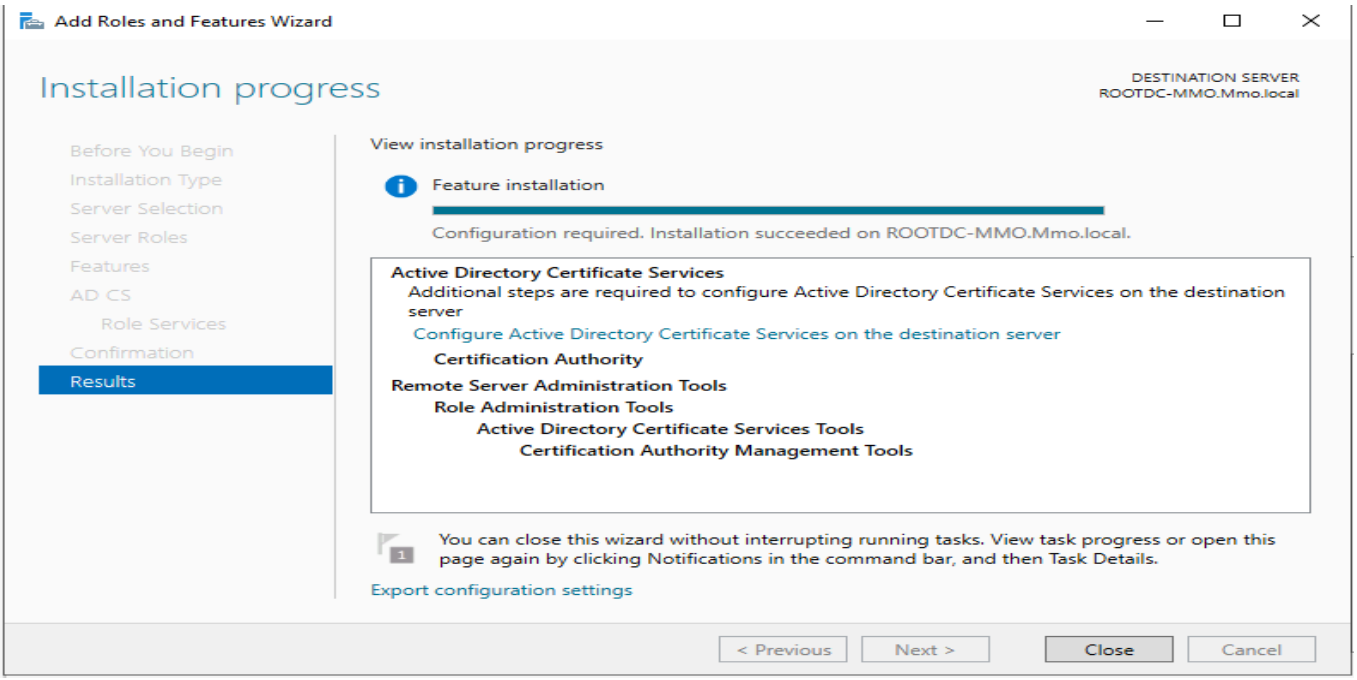
1. **Data table** - Contains domain objects.
2. **Link table** - relationships and links between objects, like group memberships and inheritance.
3. **Security Depositor table** - stores the security descriptors. And the configuration of which security events will be logged.

Log Files folder: The 'edb.log' file stores all changes that are made to active directory objects.
https://servergeeks.wordpress.com/

SYSVOL folder: Stores login scripts and group policies, it is a shared file that is replicated throughout the domain.

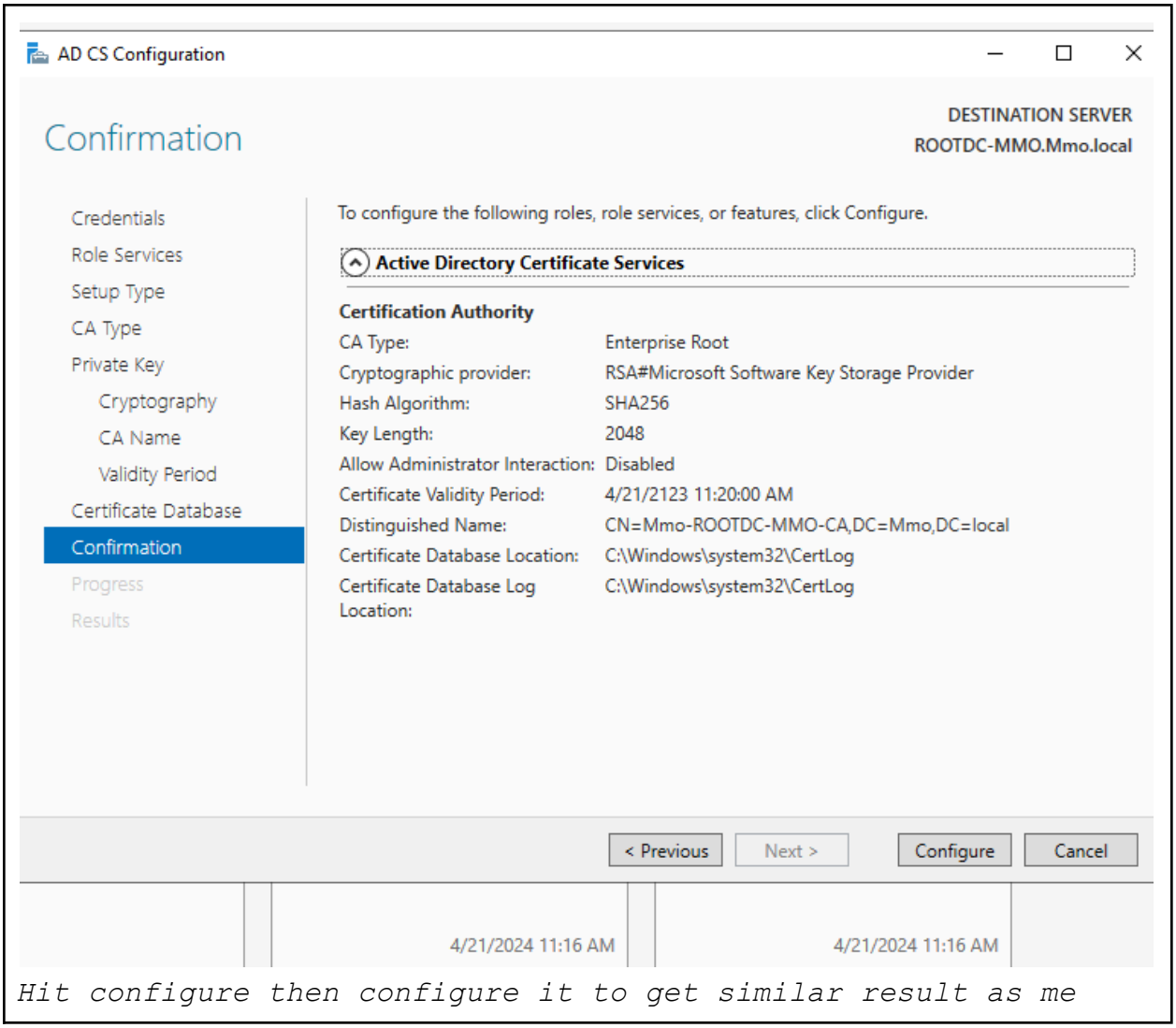
ScreenShot of Contents in NTDS folder


NTDS
File
Home
Share
View
This PC
Local Disk (C:)
Windows
NTDS
Search NTDS
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
edb.chk 4/24/2024 8:04 AM Recovered File Fra... 8 KB
edb 4/24/2024 8:05 AM Text Document 10,240 KB
edb00001 4/21/2024 11:07 AM Text Document 10,240 KB
edbres00001.jrs 4/21/2024 11:07 AM JRS File 10,240 KB
edbres00002.jrs 4/21/2024 11:07 AM JRS File 10,240 KB
edbtmp 4/21/2024 11:07 AM Text Document 10,240 KB
ntds.dit 4/24/2024 8:04 AM DIT File 16,384 KB
ntds.jfm 4/24/2024 8:04 AM JFM File 16 KB
temp.edb 4/24/2024 8:04 AM EDB File 424 KB



Now using the same steps as before I added a new user/service for my certificate services.

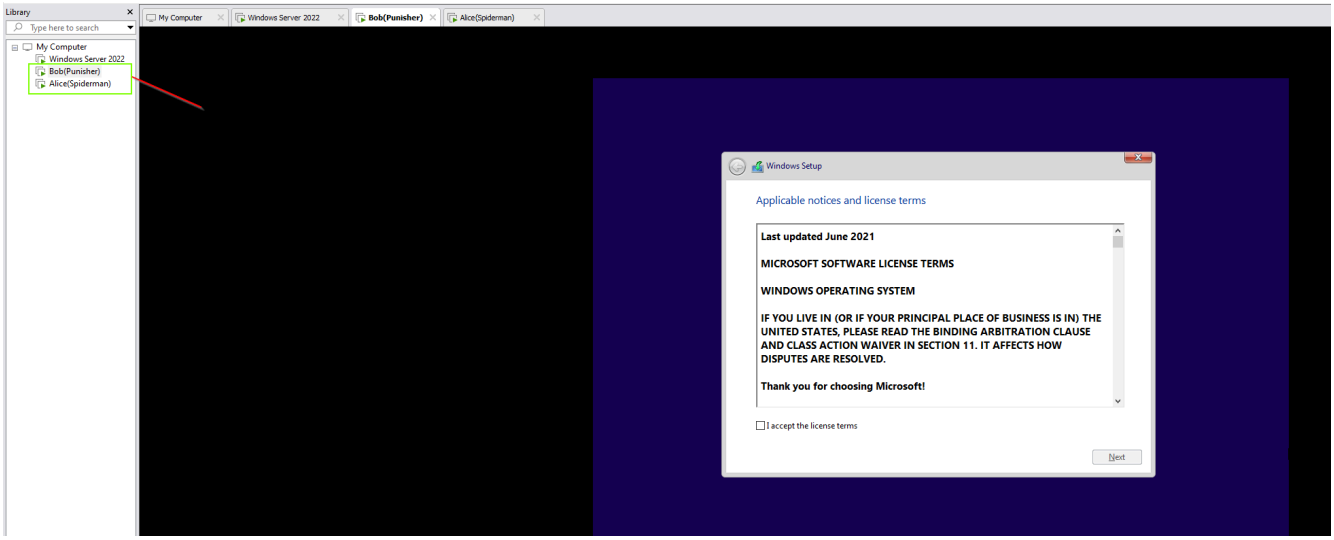
- Certificate for encryption and digital signatures, authentication.



Hit configure then configure it to get similar result as me

- Earlier I mentioned a distinguished name, the DN is critical for LDAP to identify objects within a domain, and the DN is built up of multiple Relative Distinguished Names.

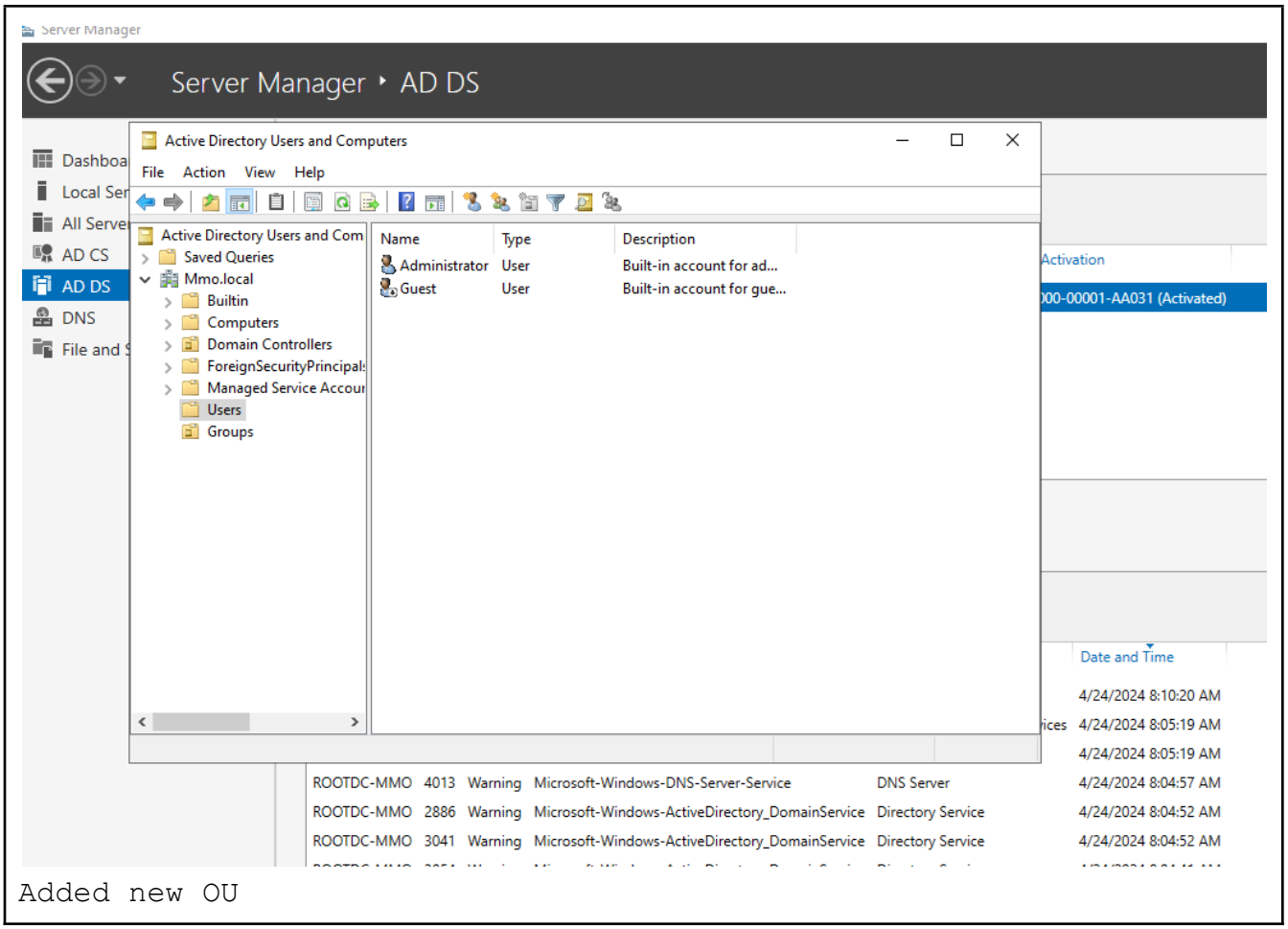
Setting up Users



Created 2 Virtual Machines for my Users Alice, and Bob.

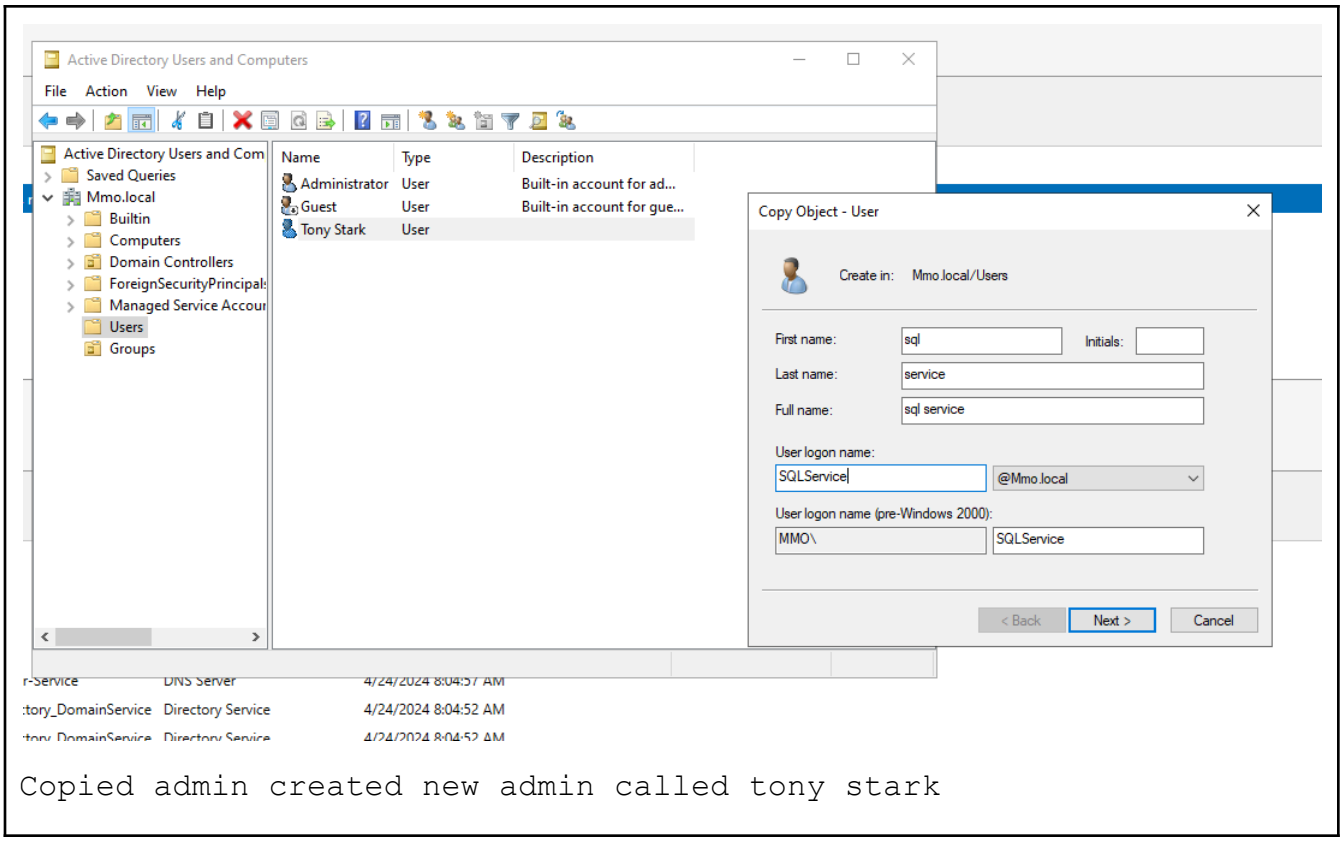
For my users I created the VM with the windows 10 enterprise eval image.

Creating users in our DC



Added new OU

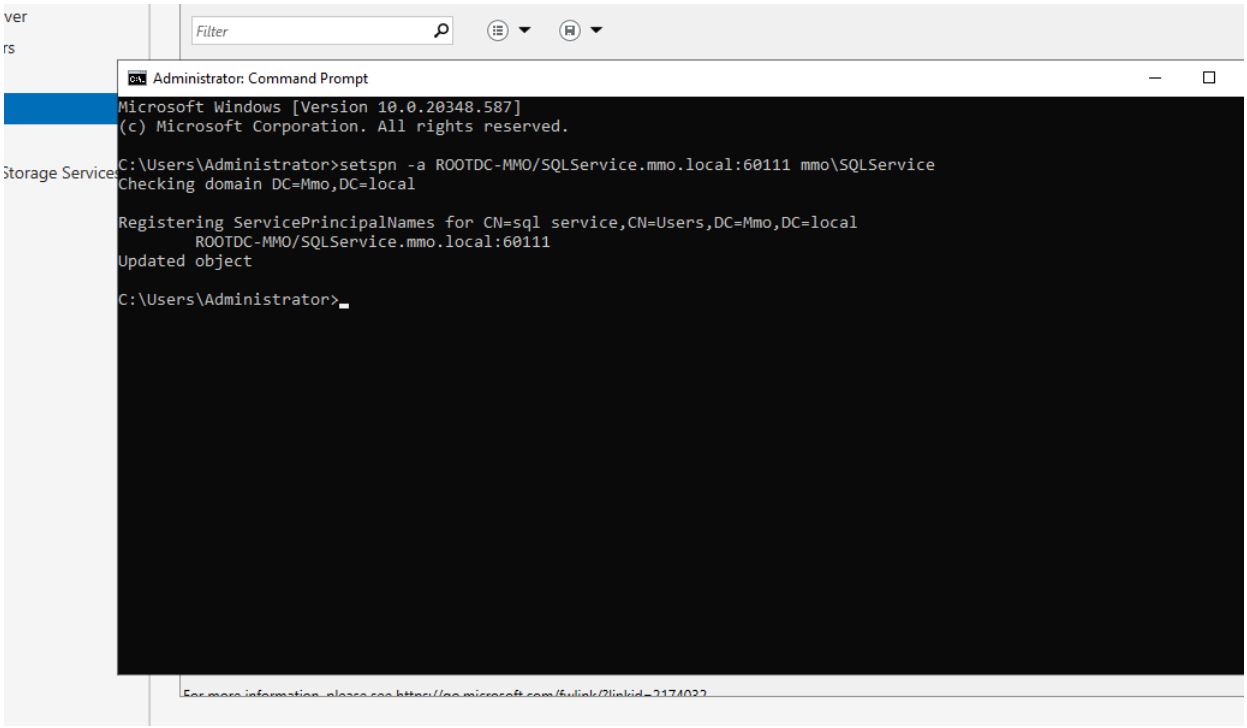
In the active directory the default group that all the users are placed in is called Users, so I created a new group called groups and placed all the users but my Admin, and guest account.



Copied admin created new admin called tony stark

I am creating a Service account with an active directory for SQLService.

Now the way that we are able to Identify or associate a certain service account with the instance of their service that is running is with the **SPN (Service Principal Name).** This will be extremely important for the lab since later on in my learning journey i hope to do some type of Kerberoasting attack the the SPN play a crucial role in the kerberos authentication process.



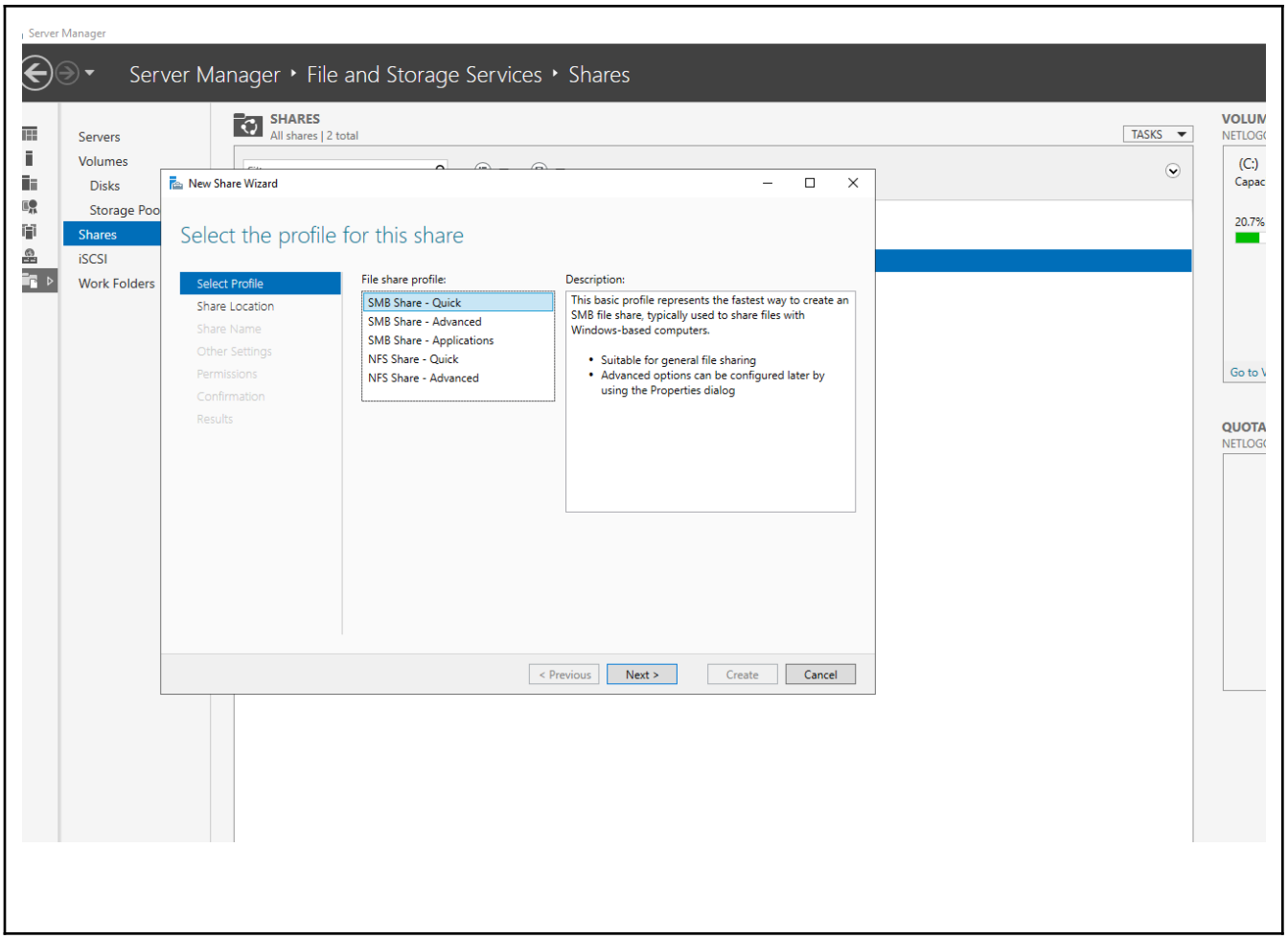
To give the user account a spn i used the CMD tool in windows and the 'setspn -a' command.

This associates the SPN http/webserver.example.com with the webserver

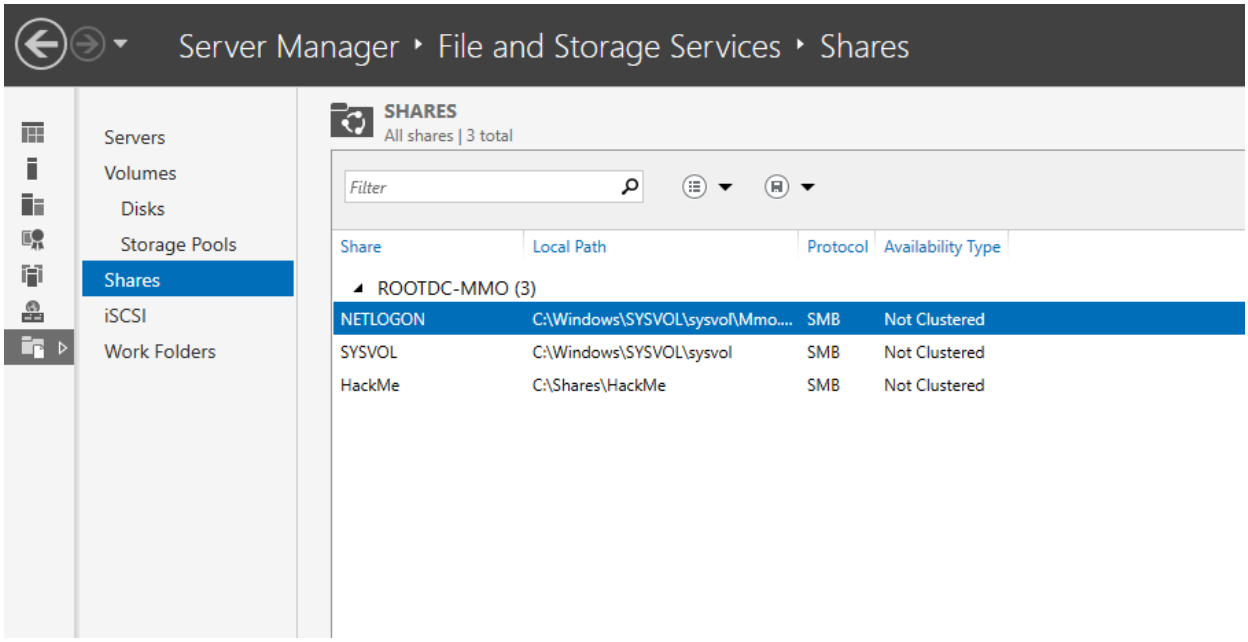
Command Breakdown

- **ROOTDC-MMO/SQLService.mmo.local:** The SPN we're adding. Used to associate service instance with a specific service account (SQLService) on my mmo.local domain
- **mmo\SQLService:** At the end we specify for the service account we are assigning the SPN.

Creating a Share

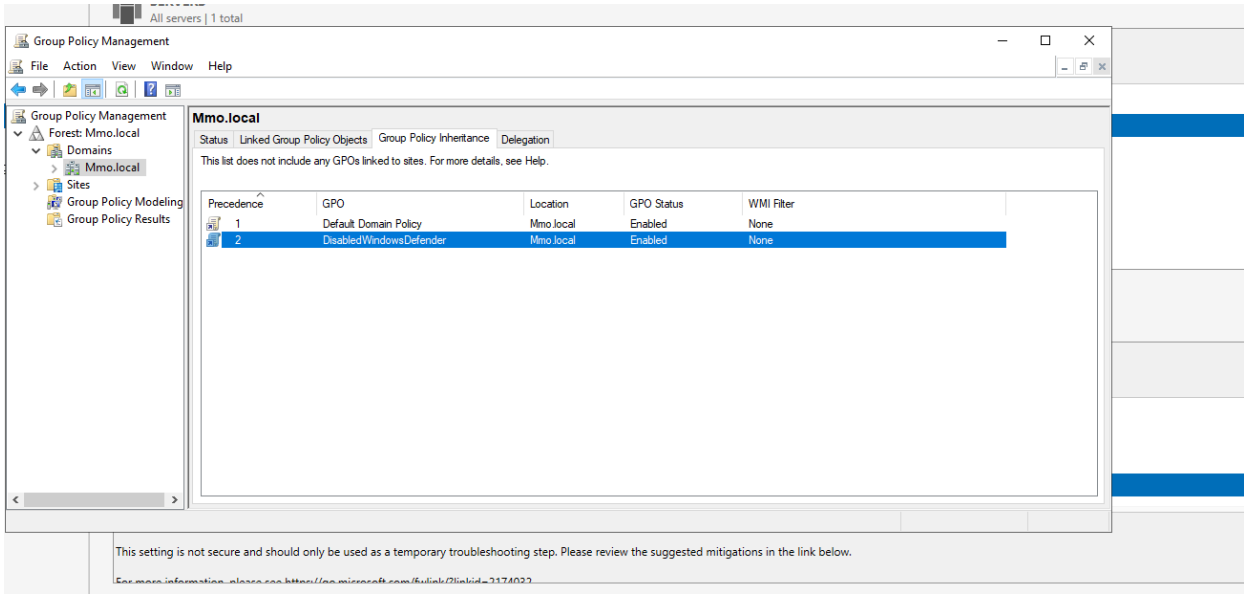


Creating a new share

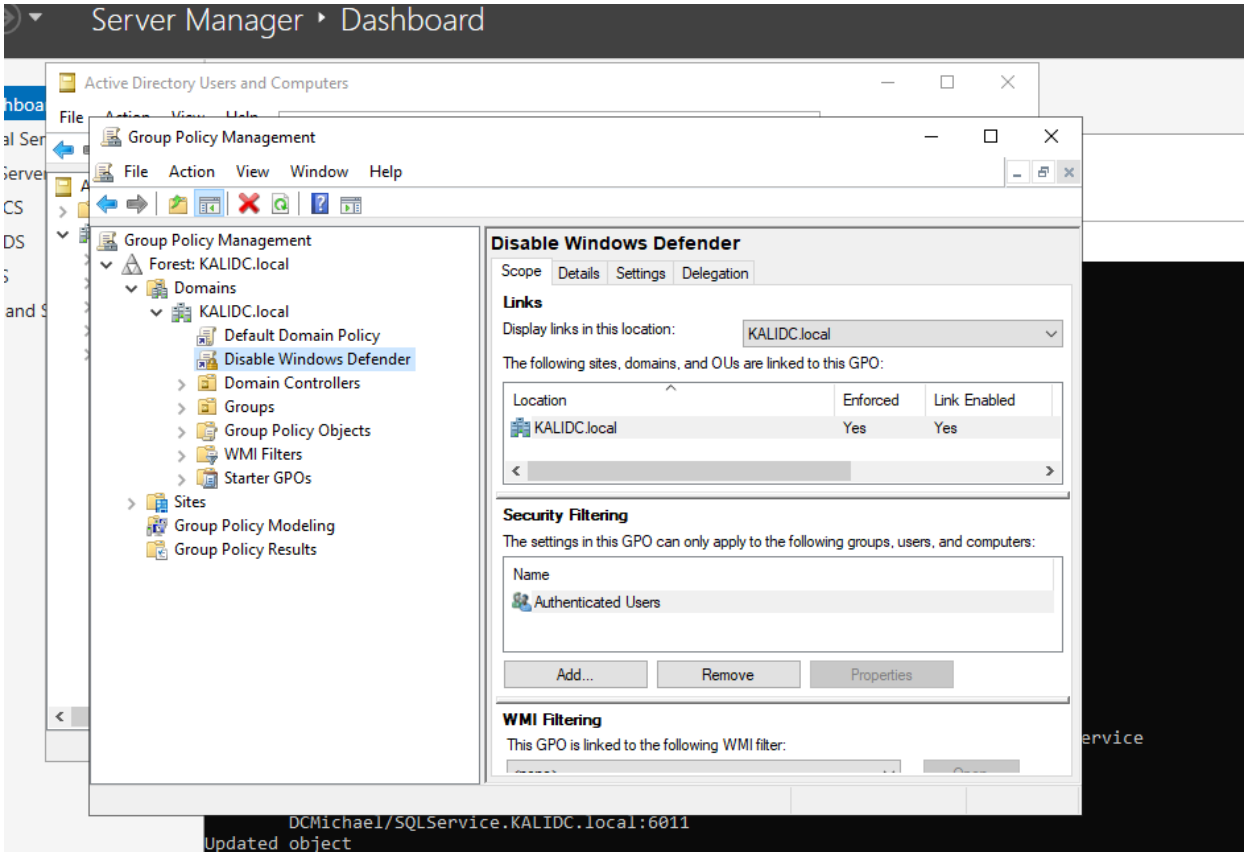


SETTING THE USER SPN:

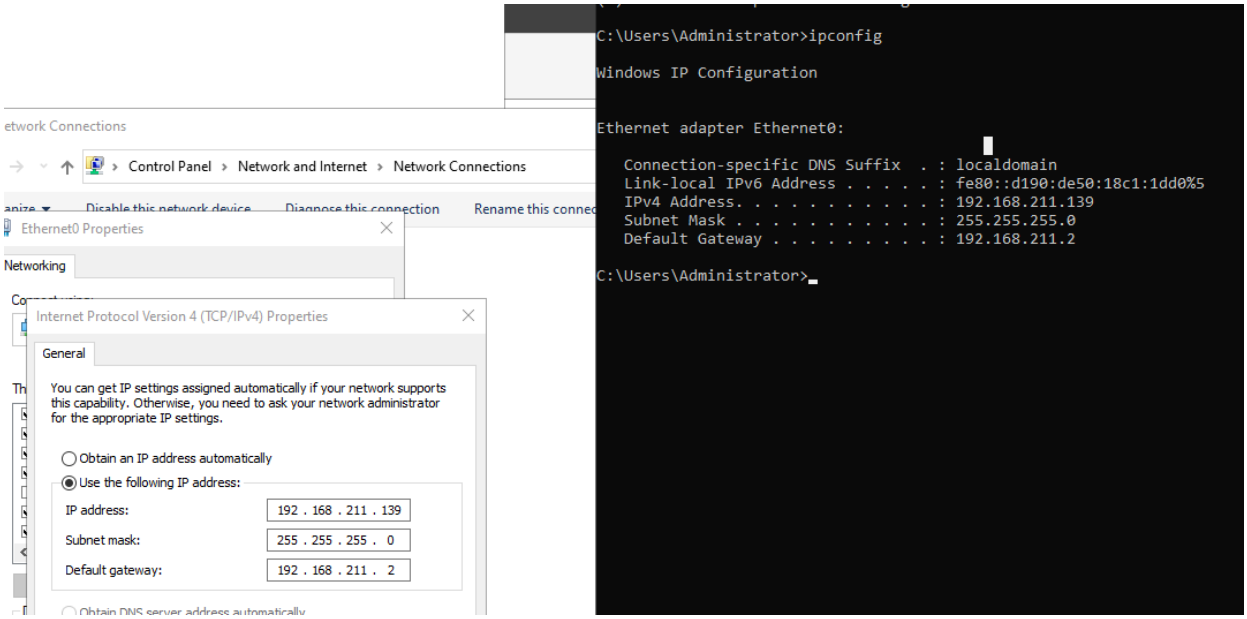
Created a GPO called DisabledWindowsDefender:



Now we will want to enforce this policy:



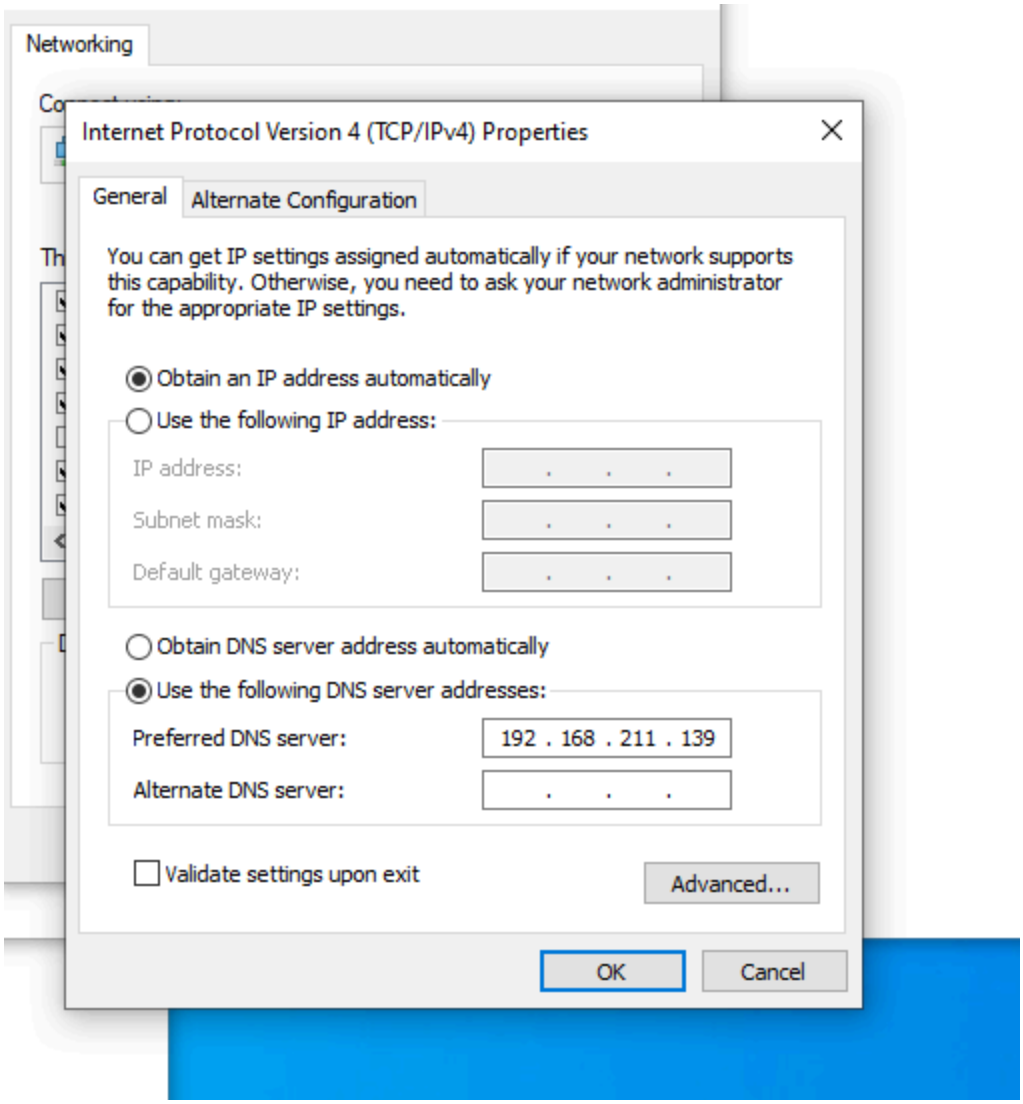
Next im going to set up static IP address:



- By changing the gate way it will prevent internet access.

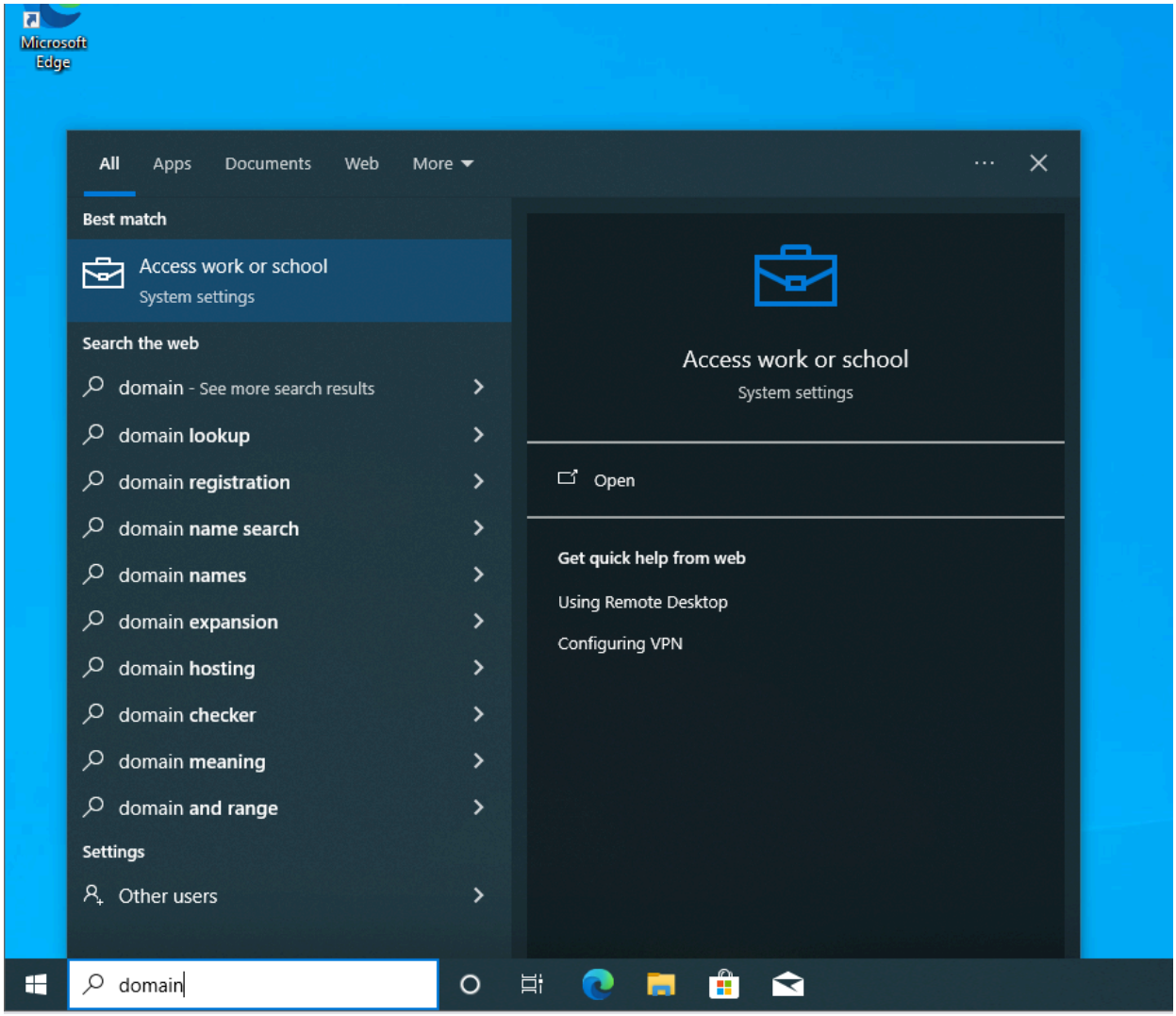
Connecting Domain Users to the Domain:

First I will set a static IP for both Systems with a preferred DNS to allow our systems to access the DC:

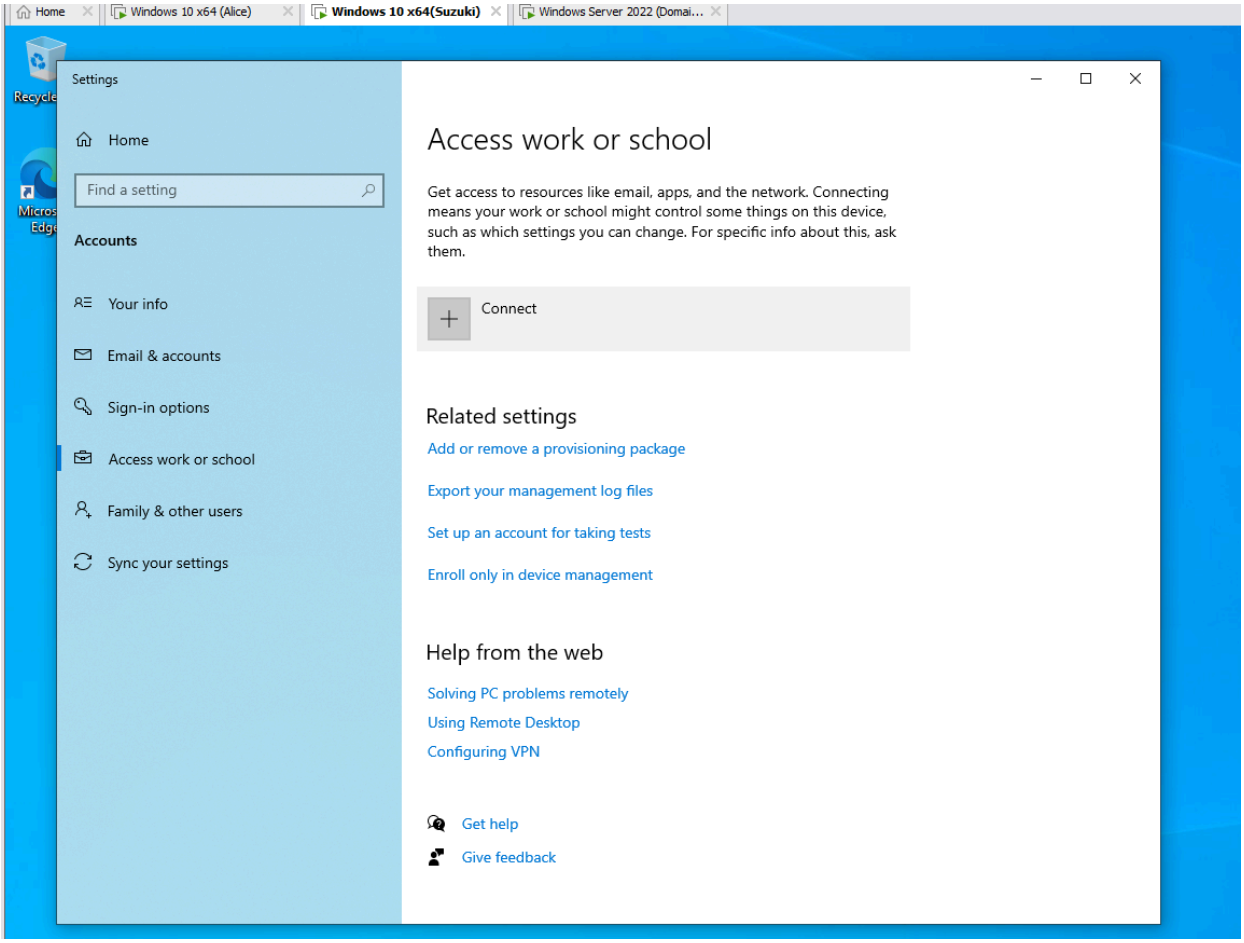


- Set the DNS IP to Domain Controller IP

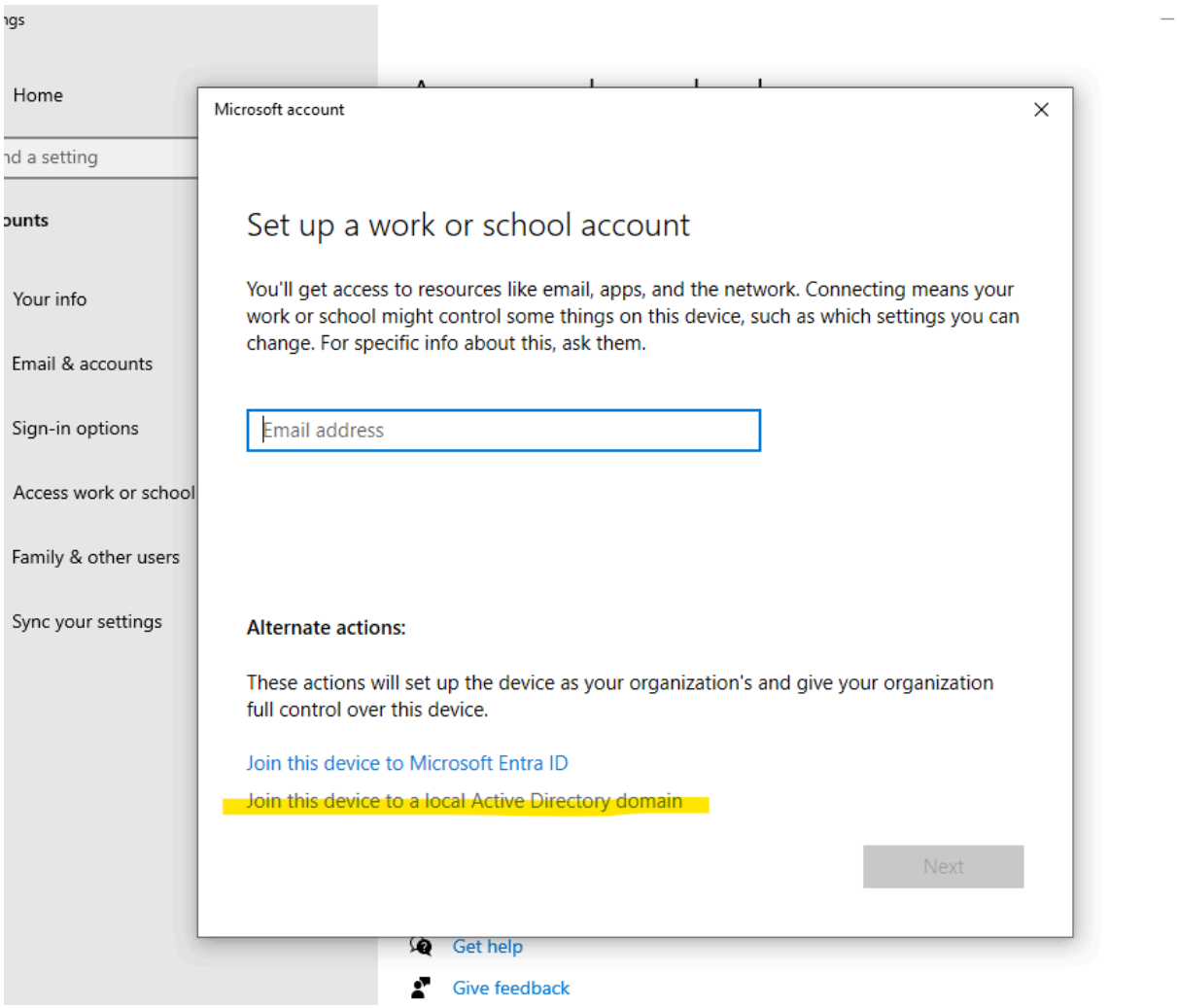
Joining Account to Domain:



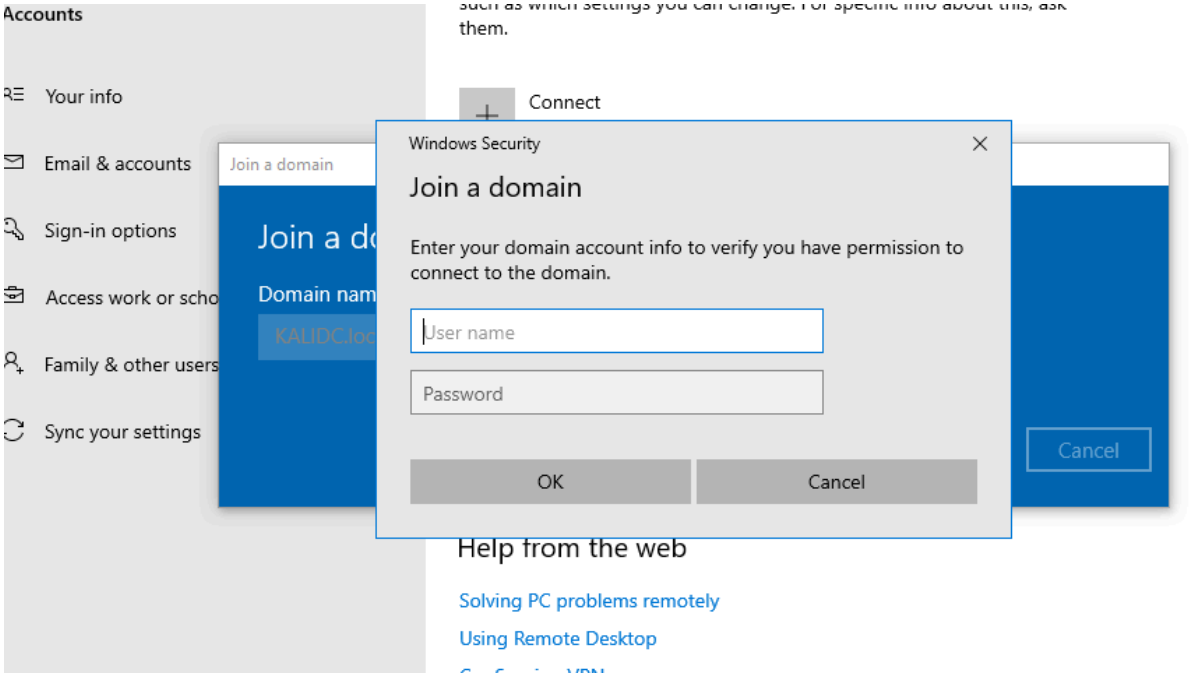
Click on access work or school



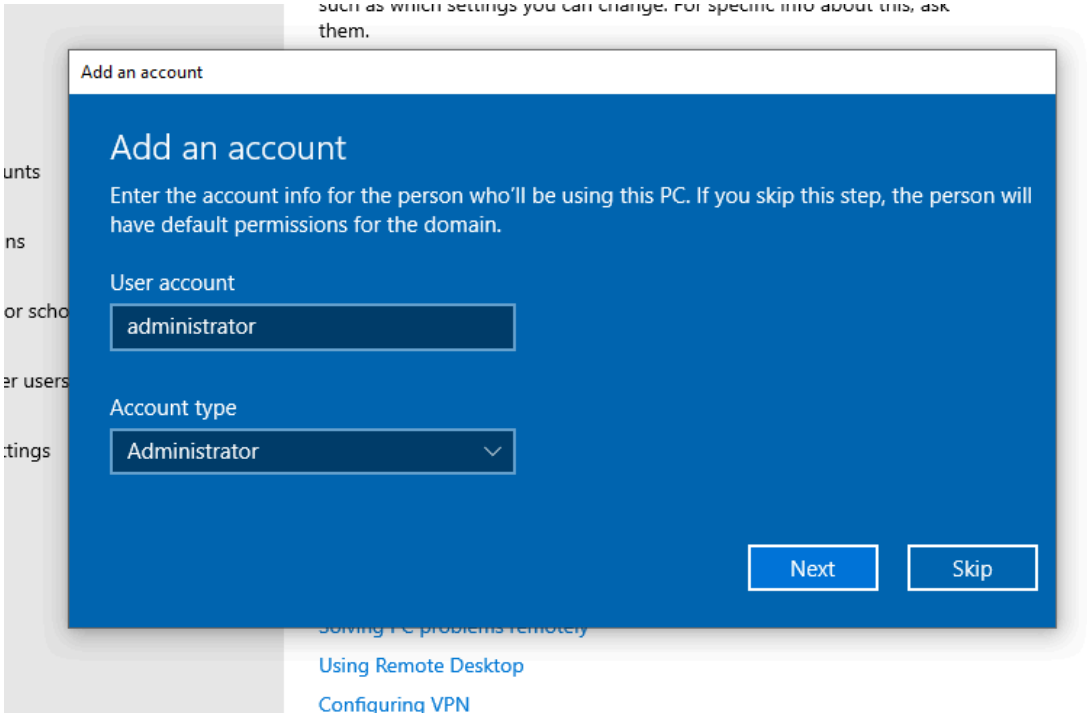
Then click connect.



Join Local Domain and then when prompted enter the name of the domain we created.



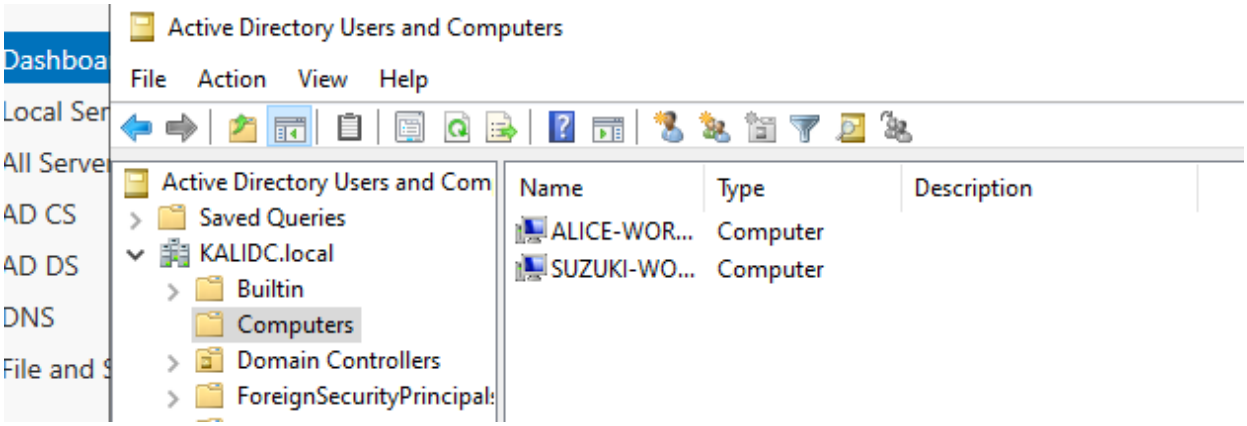
Add the administrator user and enter there password:



Hit next

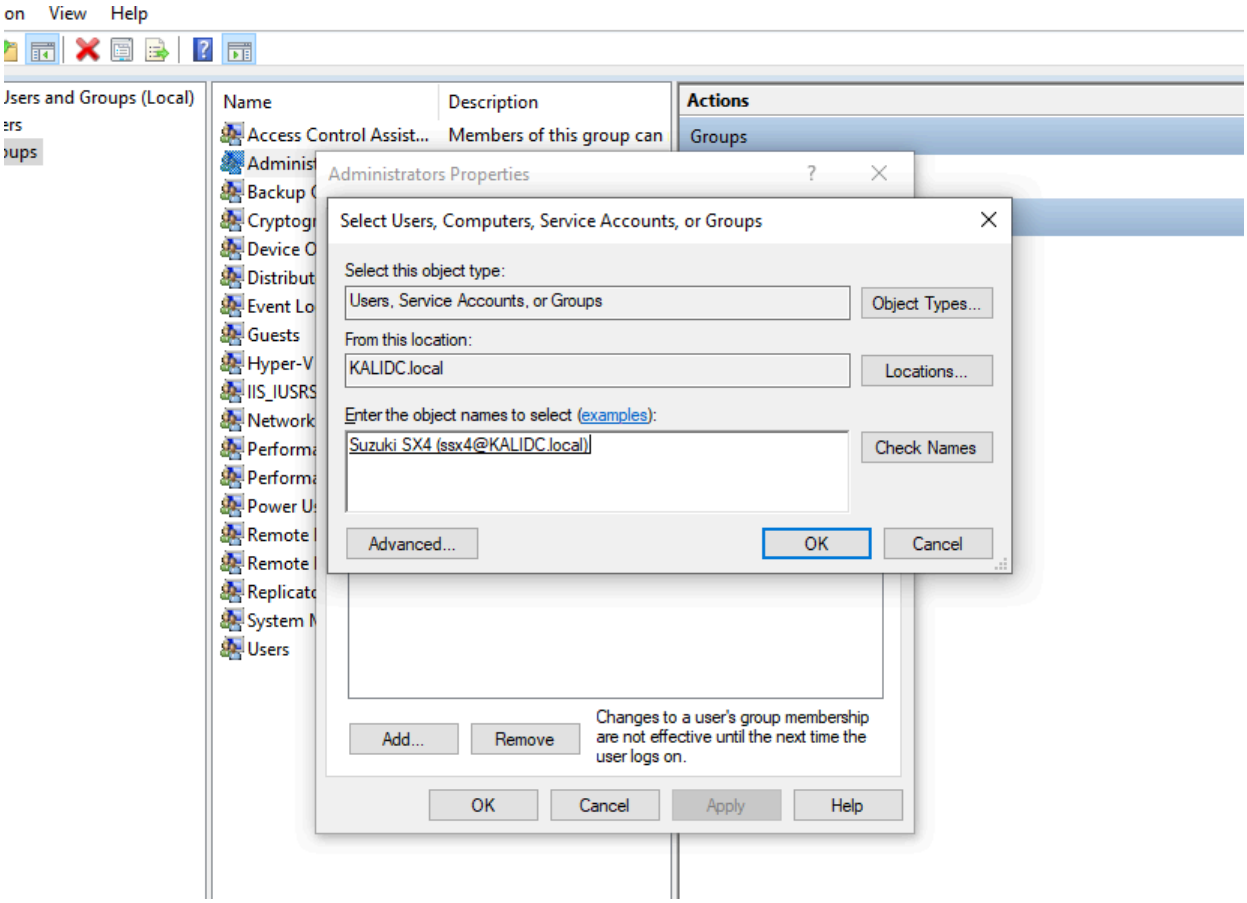
- Then when prompted restart you machine

Verify BOTH Computer are add to Domain:

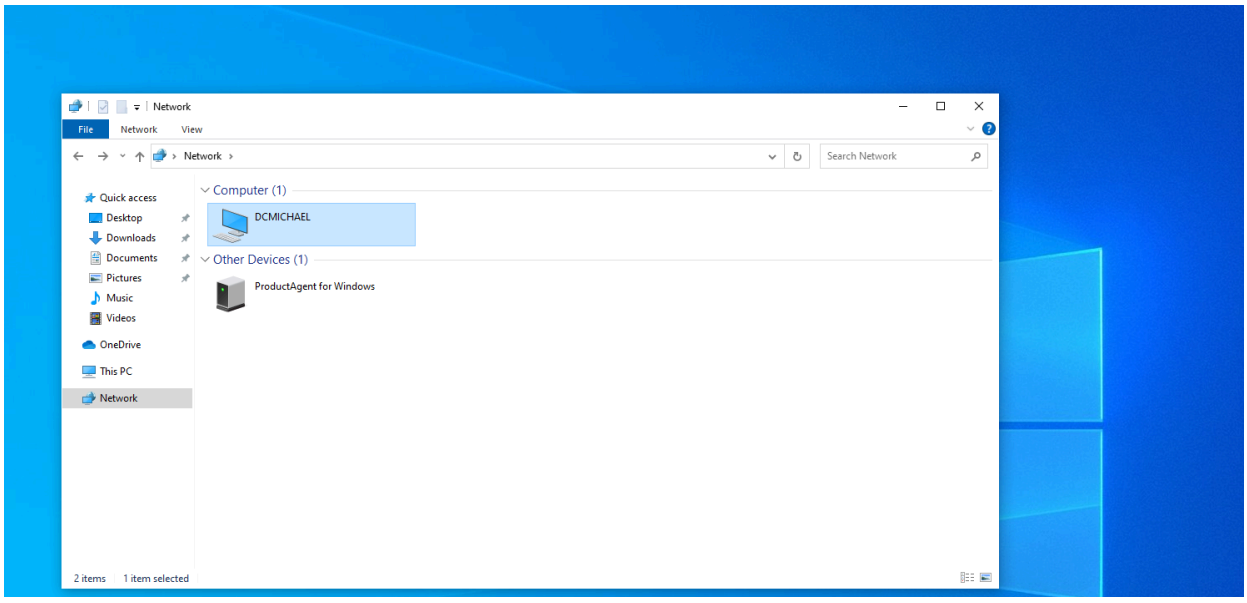


- In computers group you should see name of both of you machines.

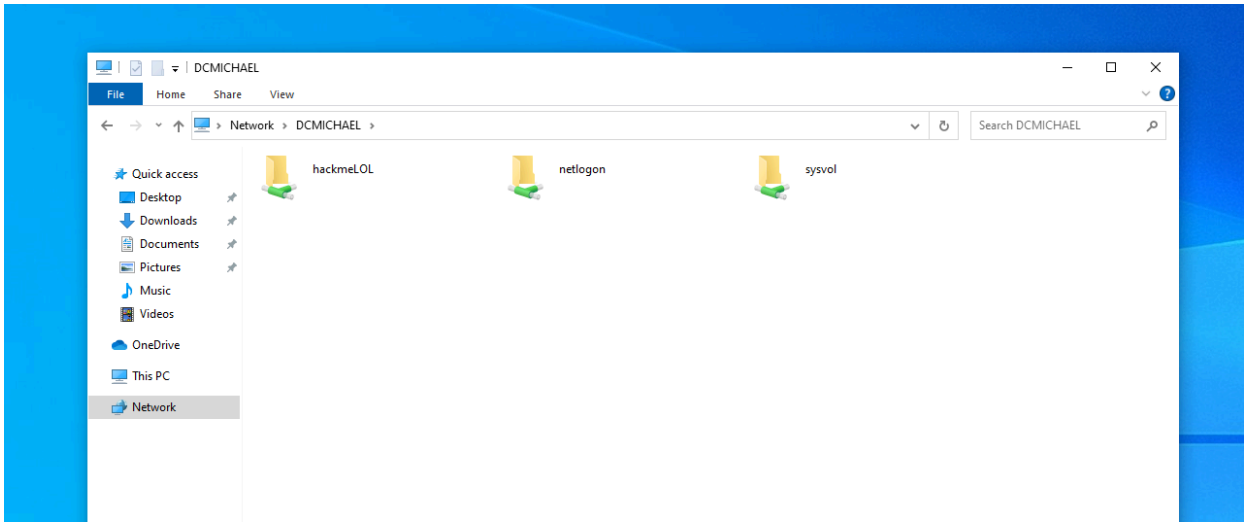
Now lets add the Domain Accounts to out workstation:



Also make sure to turn network discovery for both accounts on:

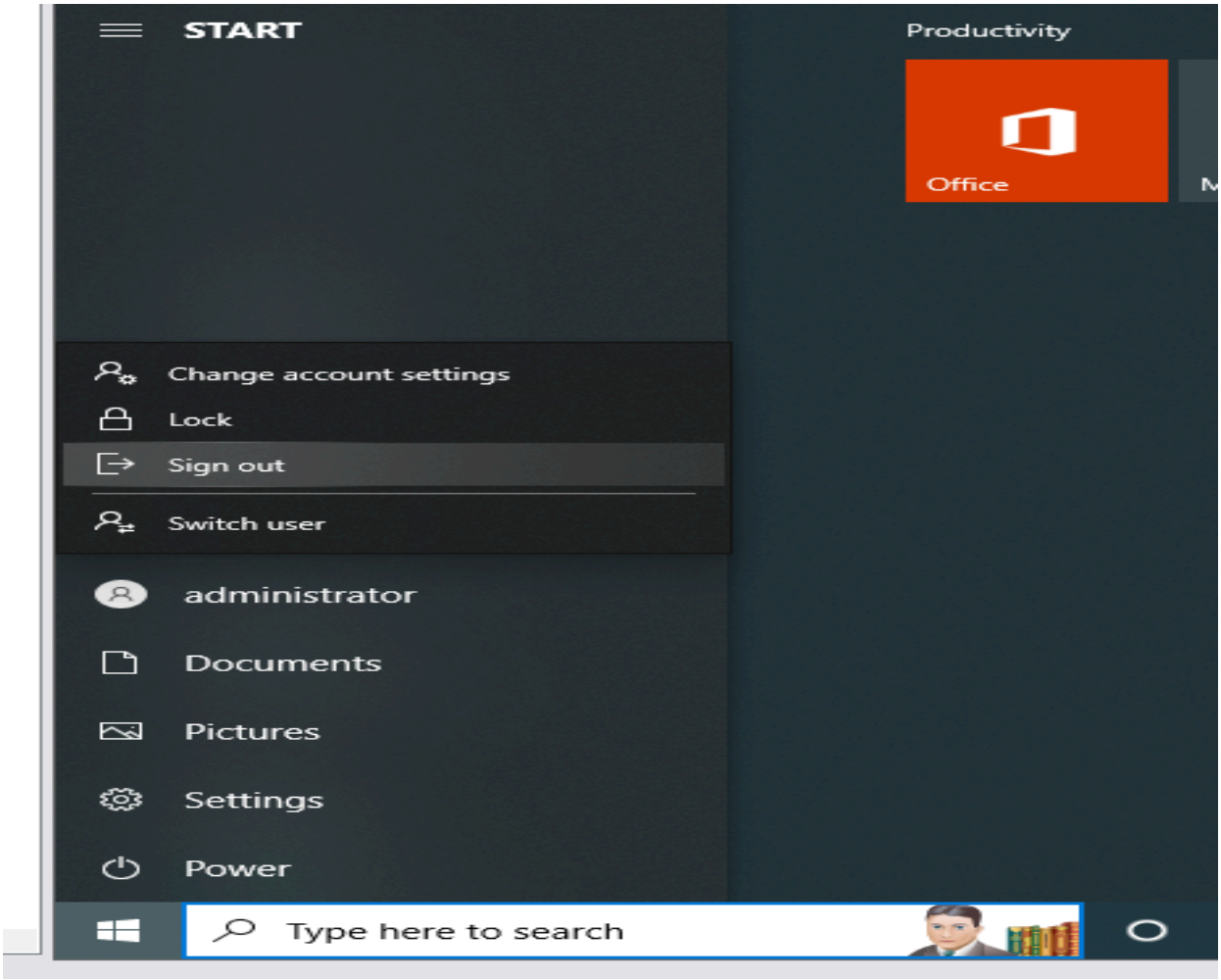


Verify we can see the share we created earlier:

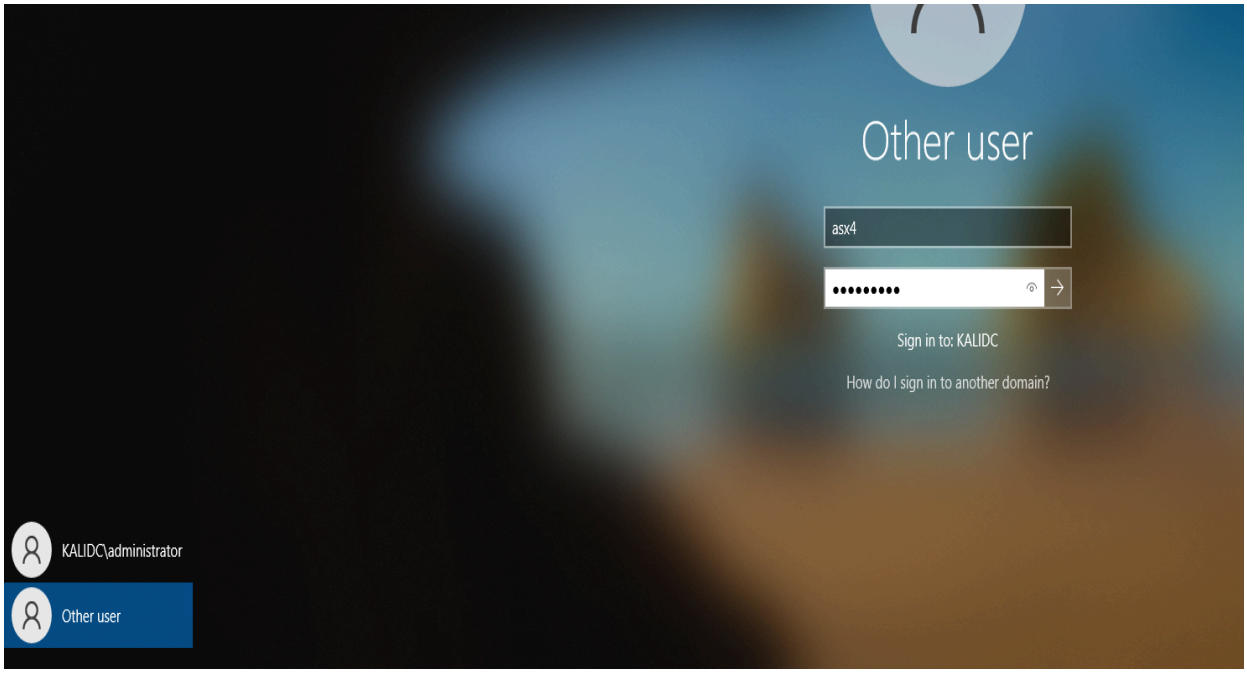


Good.. Now it is done just repeat for the second account.

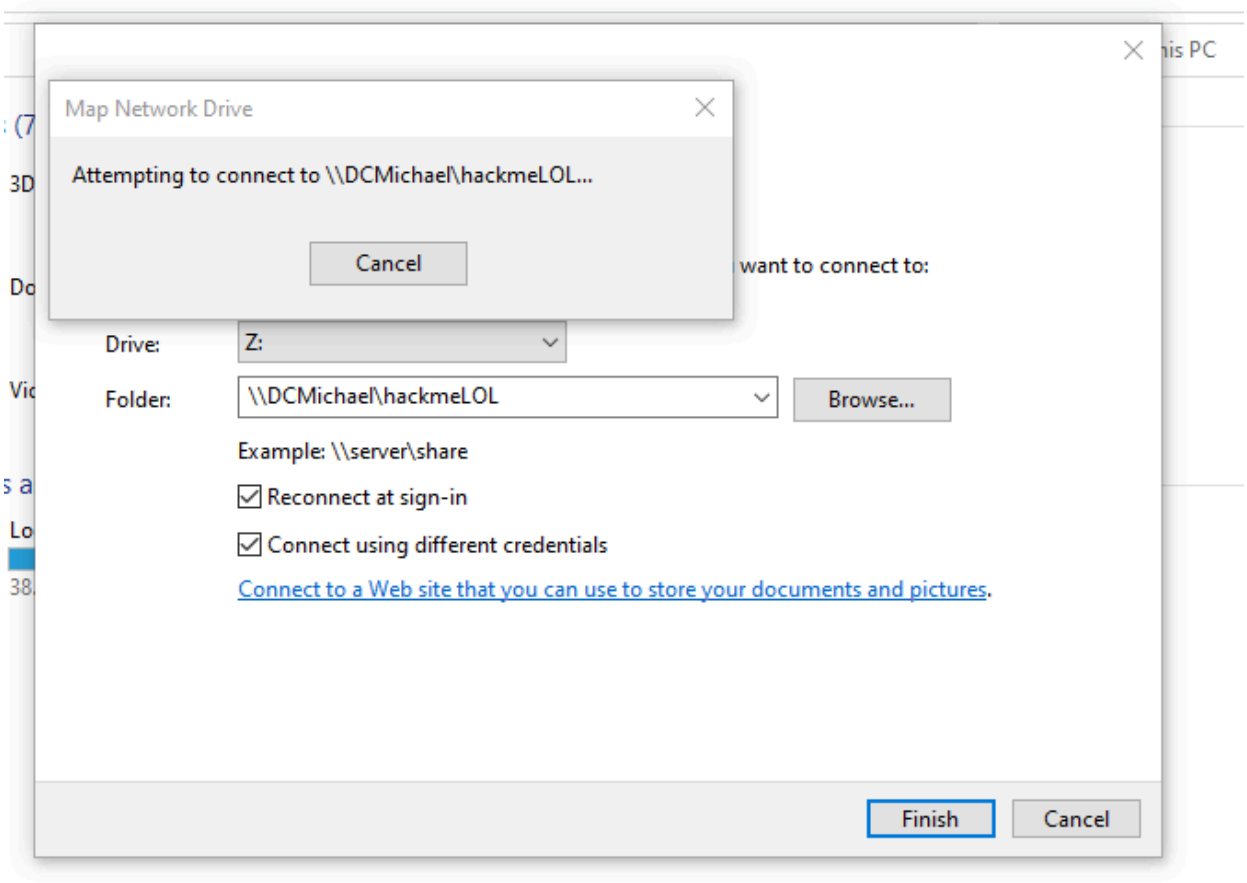
Sign out of the administrator account:



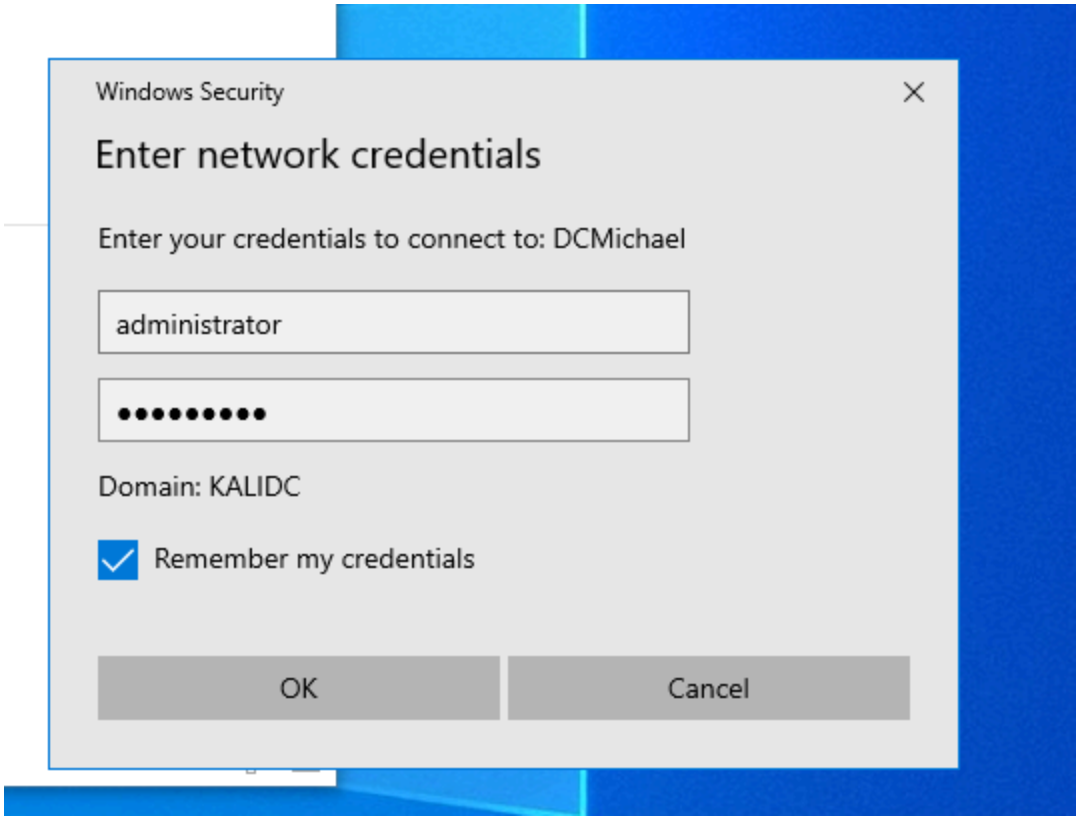
- Then when you can login select other users and put in the samAccountLogOn name of the account you created and it should take second to set account up after you successfully login.


Other user
asx4
Sign in to: KALIDC
How do I sign in to another domain?
KALIDC\administrator
Other user

Lets map our network share to our computer:



Sign in with admin:



Now its added: