

# Active Directory Lab Build

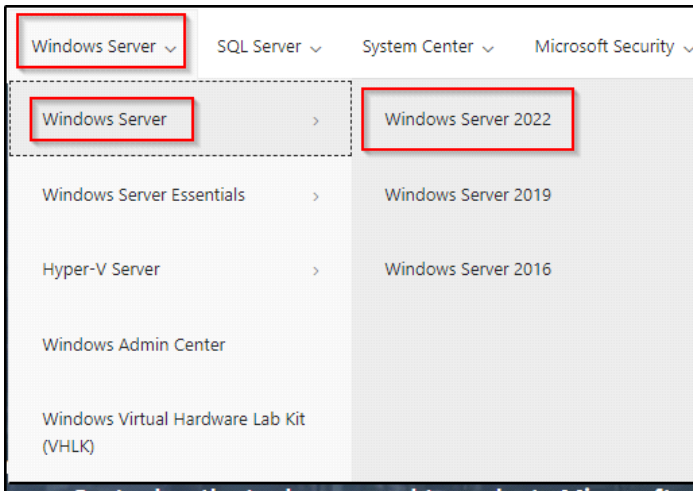
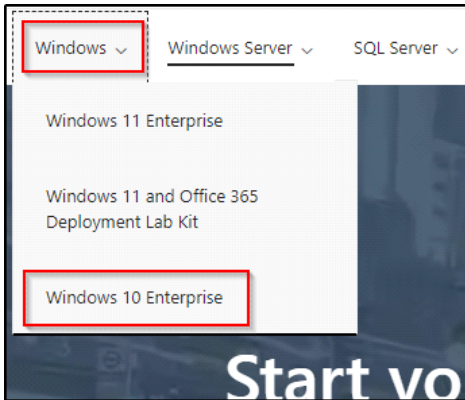
Thursday, May 16, 2024 11:05 PM

# Downloading Necessary ISO's

Thursday, May 16, 2024 11:05 PM

First go to this page: <https://www.microsoft.com/en-us/evalcenter>

Then we'll need to download Windows 10 Enterprise and Windows Server 2022:



Links:

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>

<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022>

To download Windows 10 Enterprise and Server 2022, just fill anything on this forms:

# Evaluate Windows 10 Enterprise

Windows 10 Enterprise is designed to address the needs of large and midsize organizations by providing IT professionals with:

- Advanced protection against modern security threats
- Flexible deployment, update, and support options
- Comprehensive device and app management and control

Windows 10, version 21H2 makes it easier to protect your endpoints, detect advanced attacks, automate response to emerging threats, and improve your security posture. It also helps you streamline deployment and updates—and deliver enterprise-ready devices to your users straight from the manufacturer.

Learn more about the features of [Windows 10](#).

## Register for your free trial today

Complete the form below.

\* First name

\* Last name

\* Email

\* Company name

\* Country/Region

Country/region \*

\* Company size

Company size

\* Job role

\* Phone

Country Code \*

Questions/Comments

Download now

And hit download.

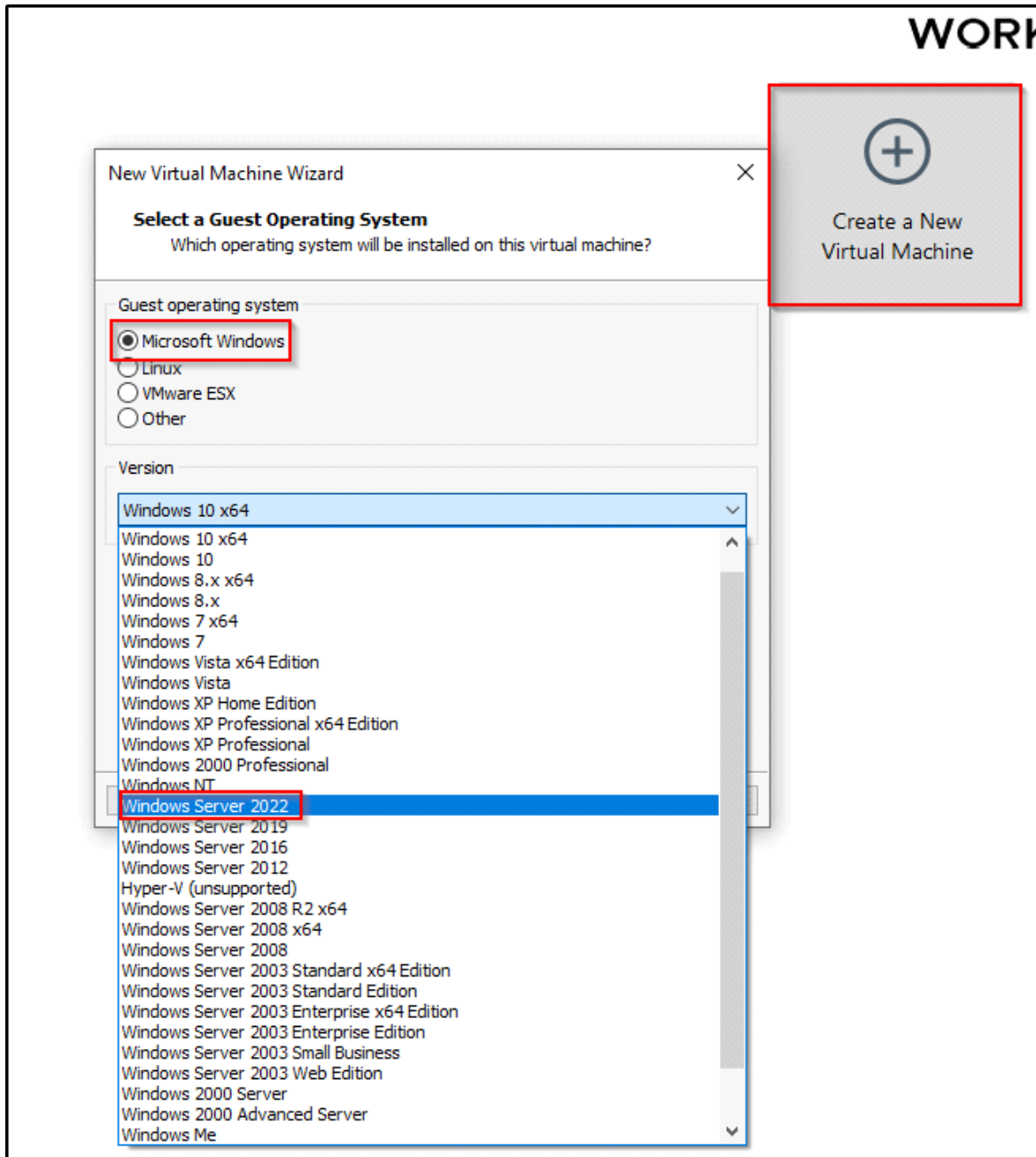
# Setting Up the Domain Controller

Thursday, May 16, 2024 11:20 PM

★ IF ANY STEP ISN'T SHOWN HERE, KEEP IN MIND THAT YOU SHOULD LEAVE IT AS DEFAULT AND HIT NEXT OR INSTALL.

Step 1: On Vmware, create a new virtual machine

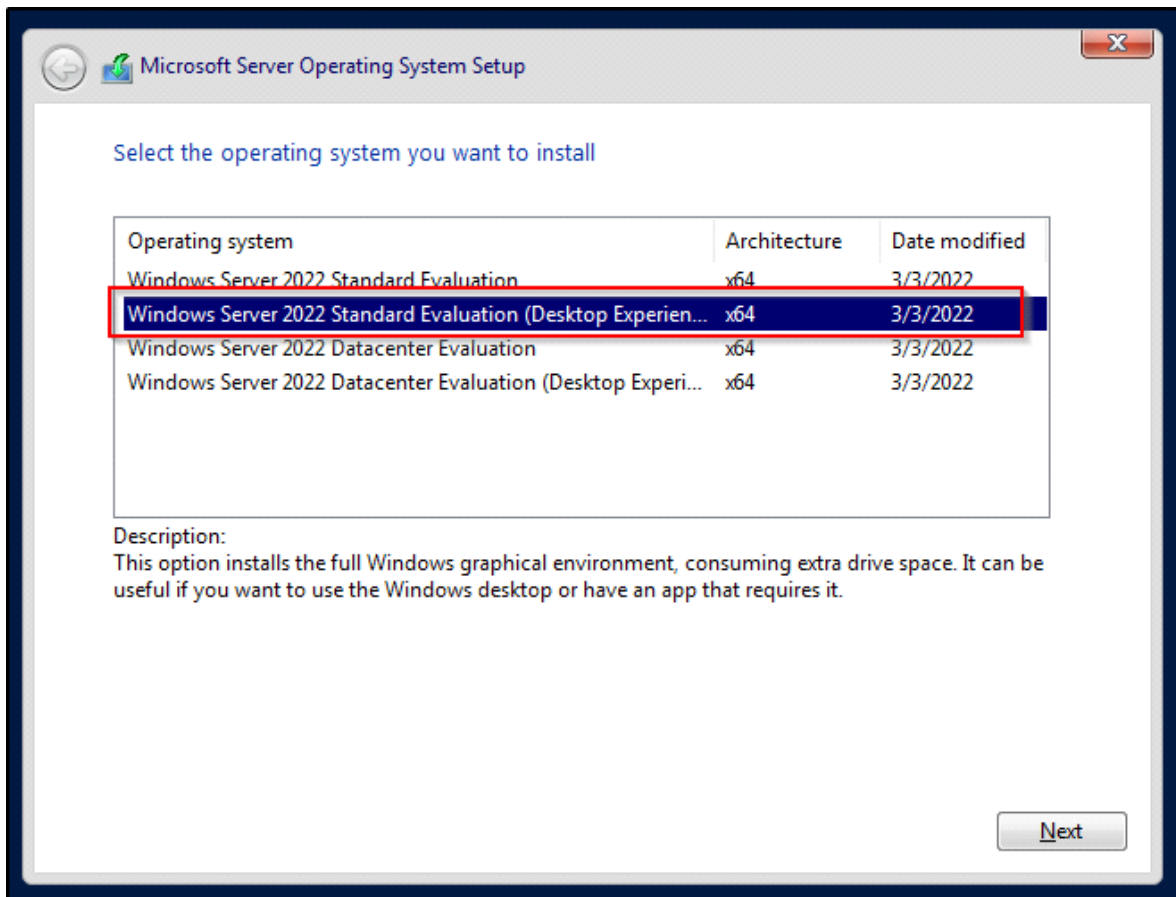
Step 2: Choose Microsoft Windows > Windows Server 2022:



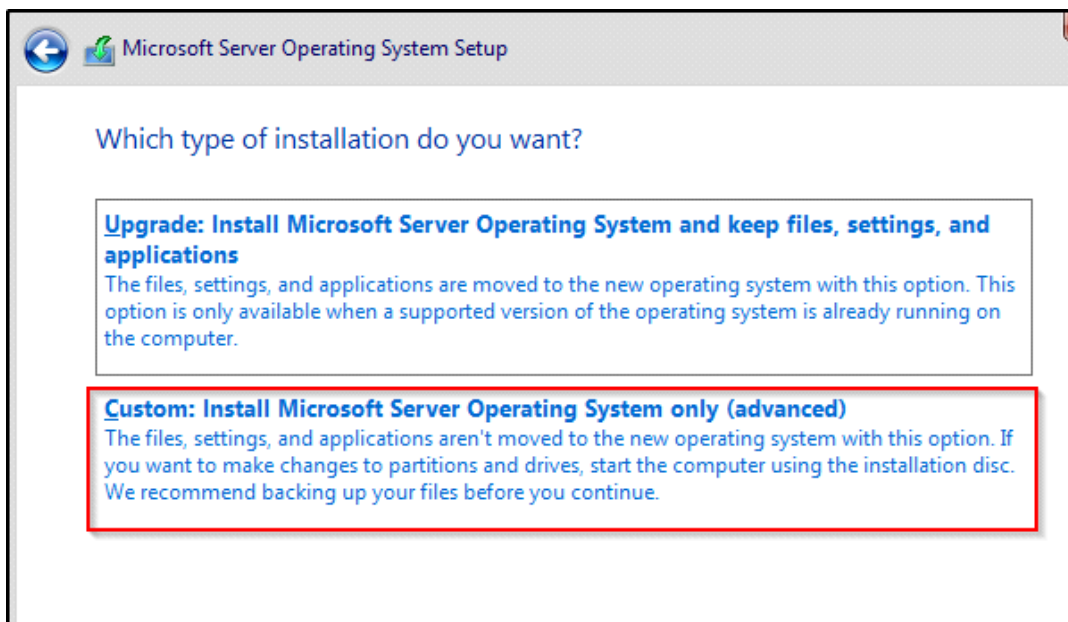
Step 3: Choose the ISO file that we downloaded.

Step 4: You can set the Memory to 6GB and disk space to 60GB

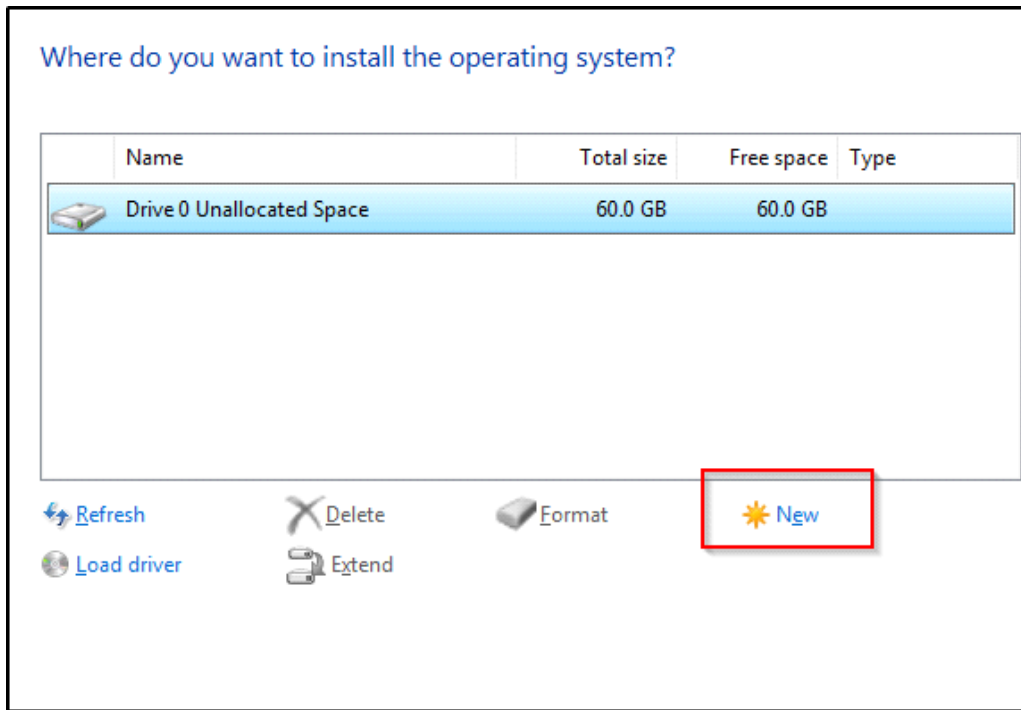
Step 5: Once the machine is powered on, select the Standard Evaluation (Desktop Experience) version to download:



Step 6: Select Custom Install:

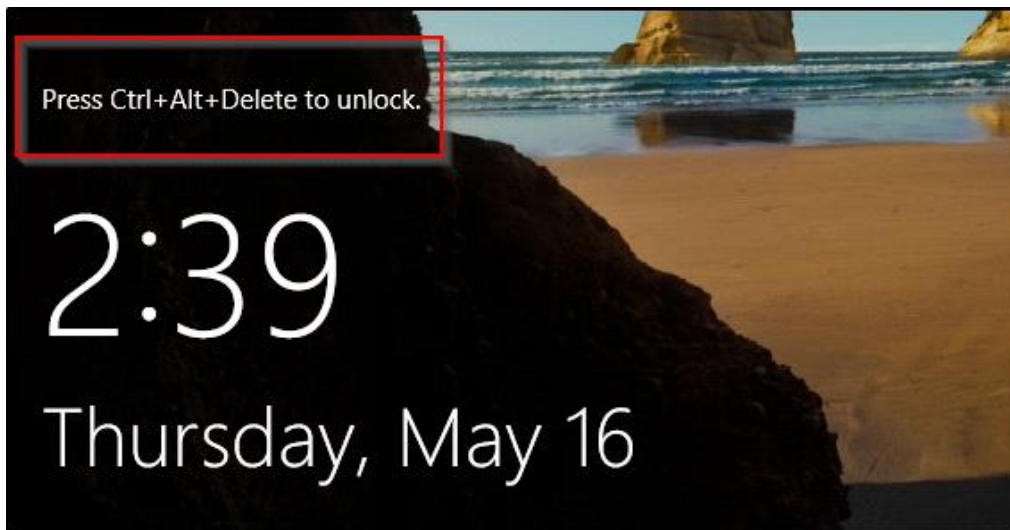


Step 7: Press on NEW>Apply and click Next:

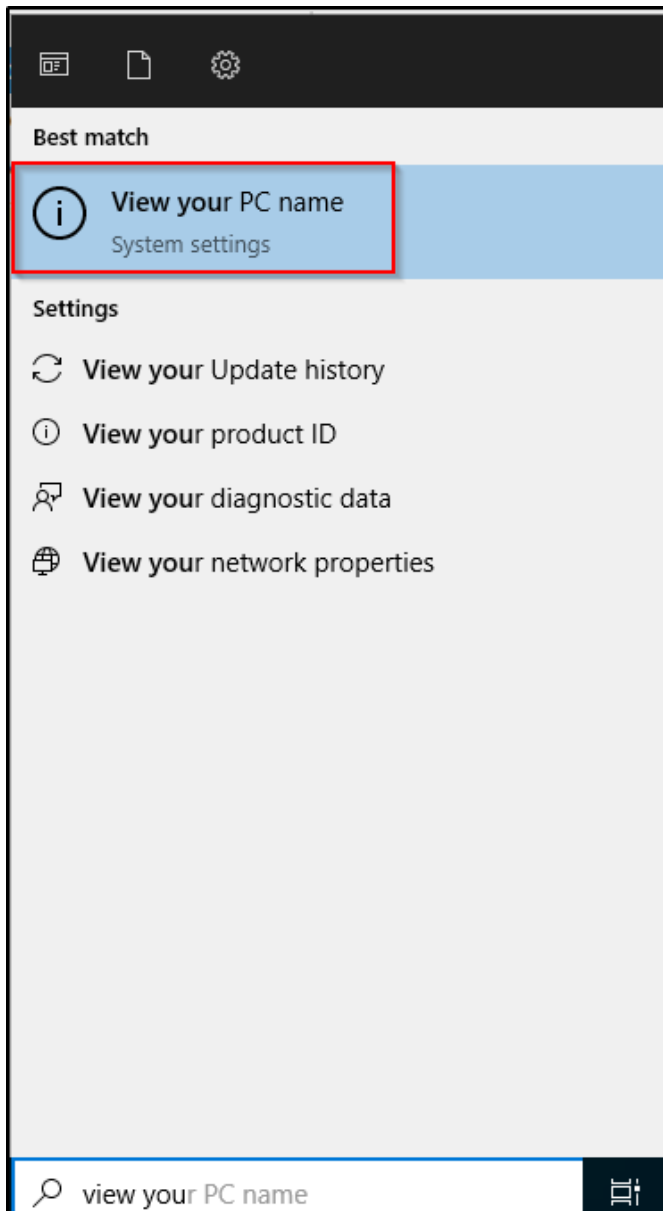


Step 8: Now we'll have to set up a password, for our lab we're going to use a weak password, for example: Password123@

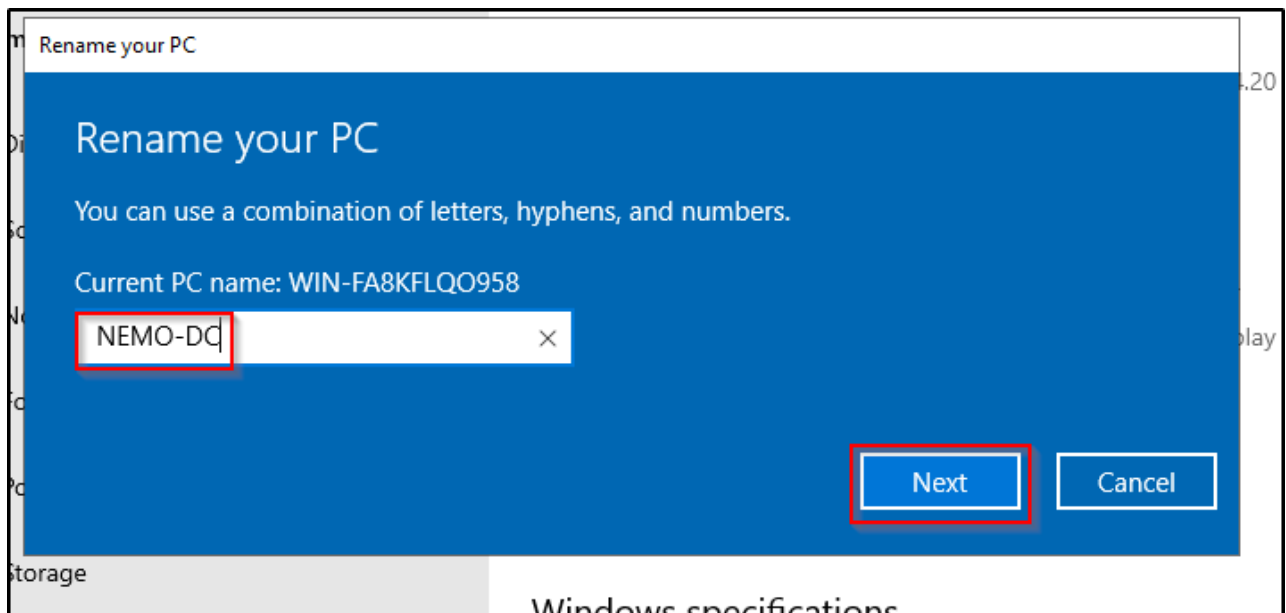
Step 9: And once all steps are completed, we can get started by pressing (CTRL+ALT+DELETE):



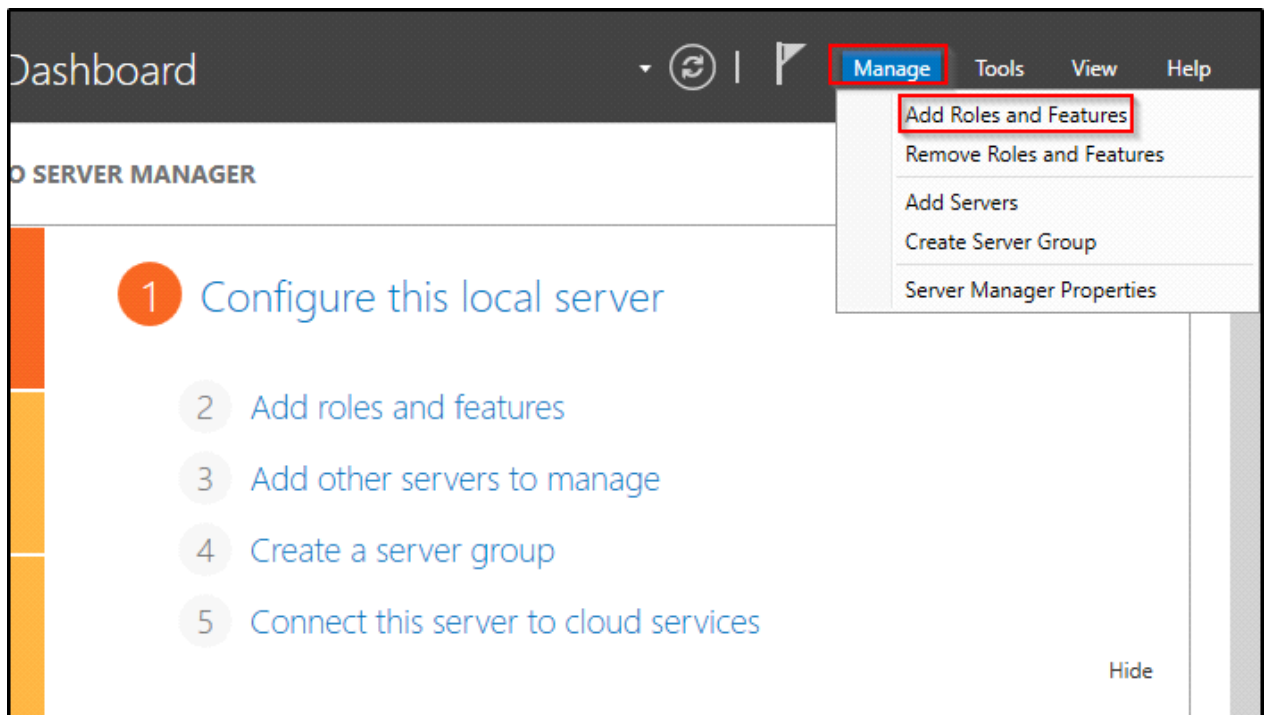
Step 10: Go to start and type:



And change it to whatever name you want, so we can easily identify which is the Domain Controller and Reboot the machine:

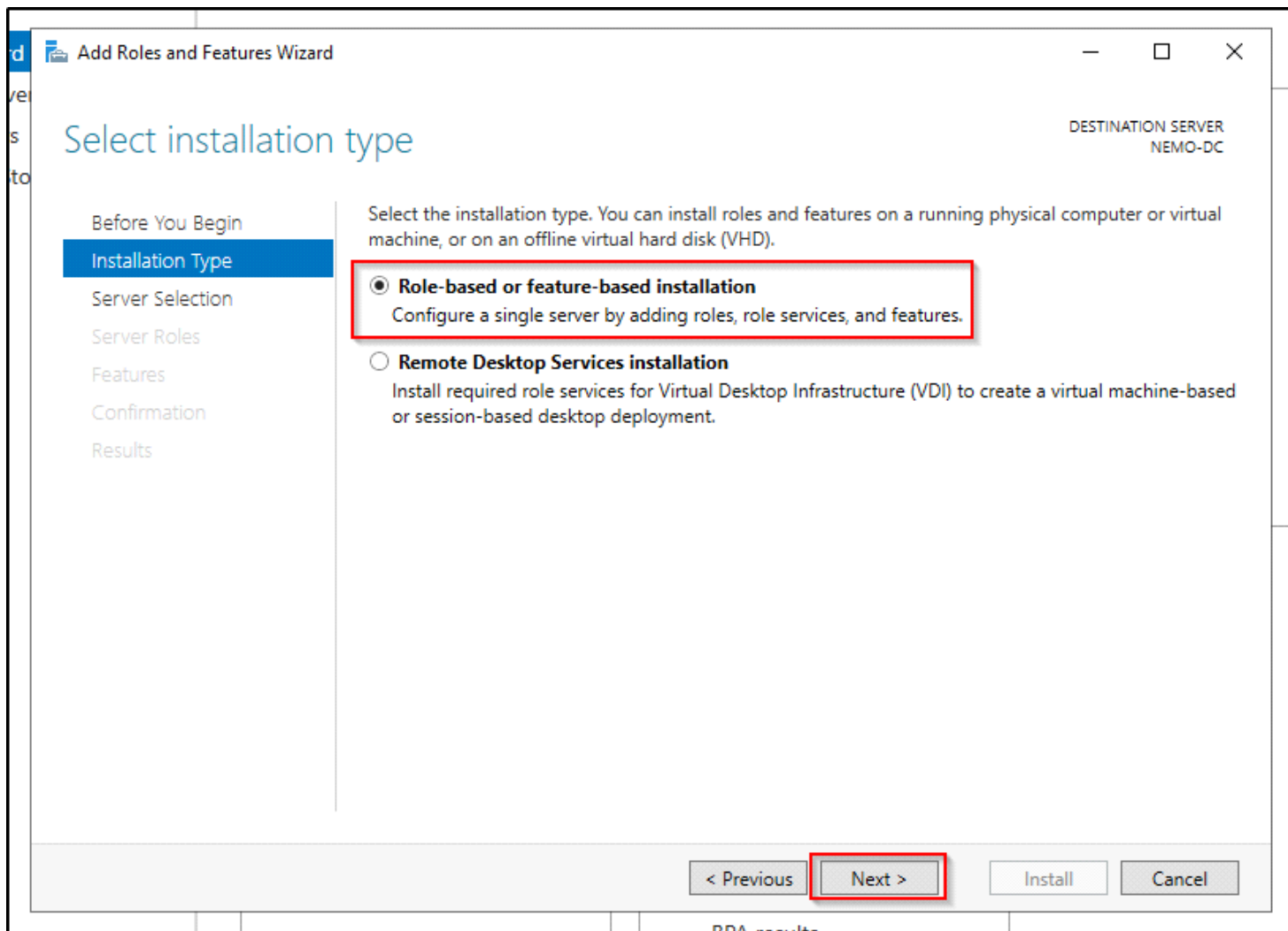


Step 11: Once rebooted, now we want to make this a Domain Controller, to do so click on:

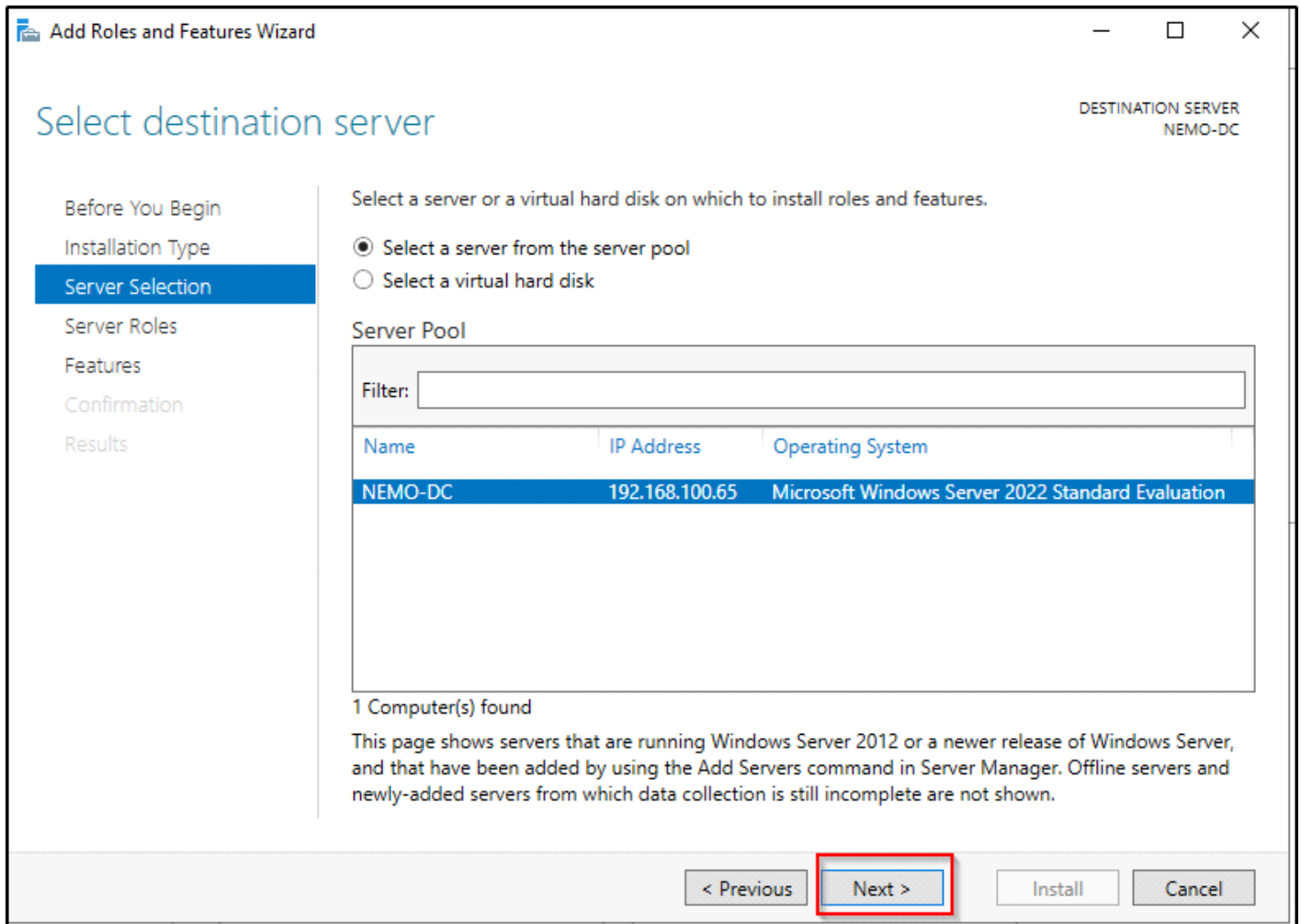


Step 12: And then:

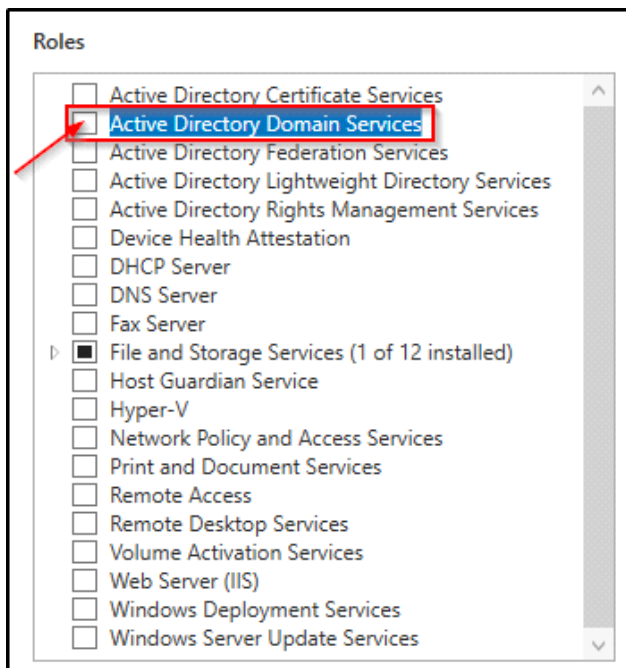


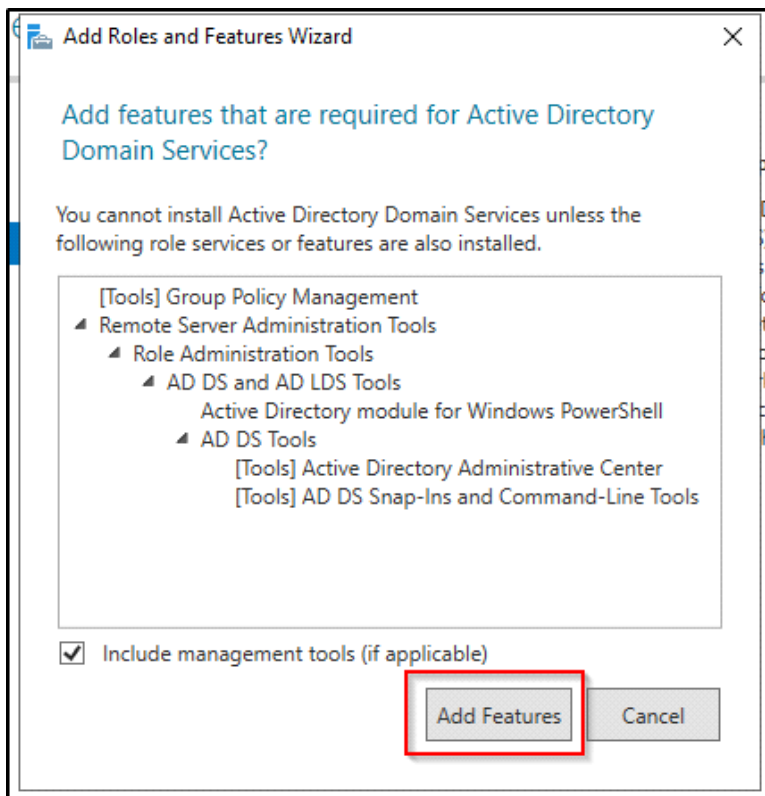


Step 13: Here leave everything on default and click next:

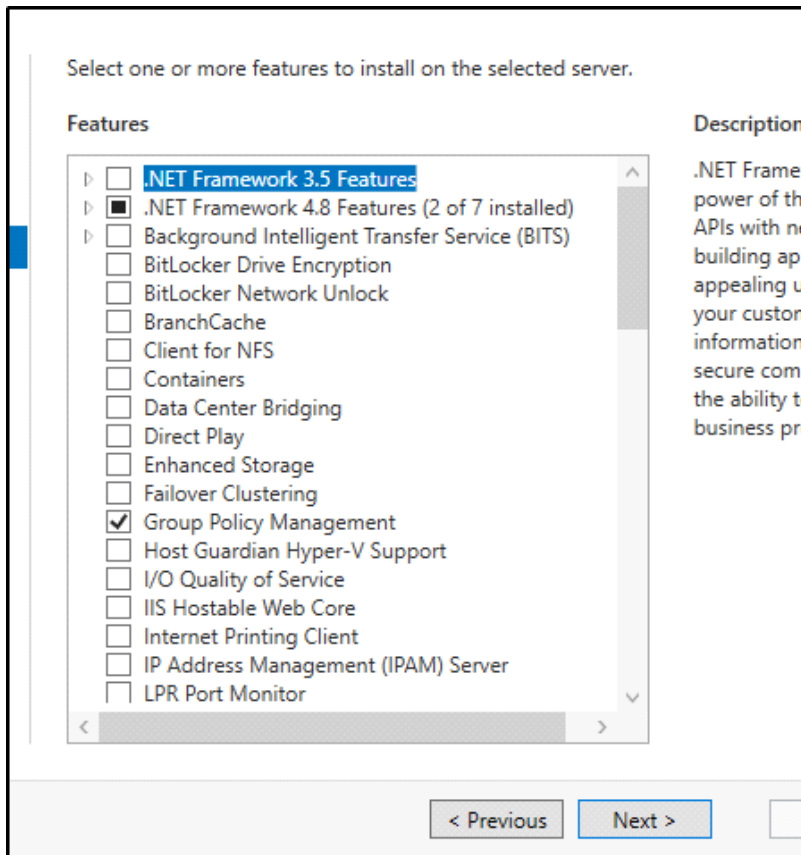


Step 14: Now we'll need to select AD DS and hit Next:





Step 15: Here we'll leave everything on default:



Step 16: We need to check this box here and click Install:

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

    Role Administration Tools

        AD DS and AD LDS Tools

            Active Directory module for Windows PowerShell

        AD DS Tools

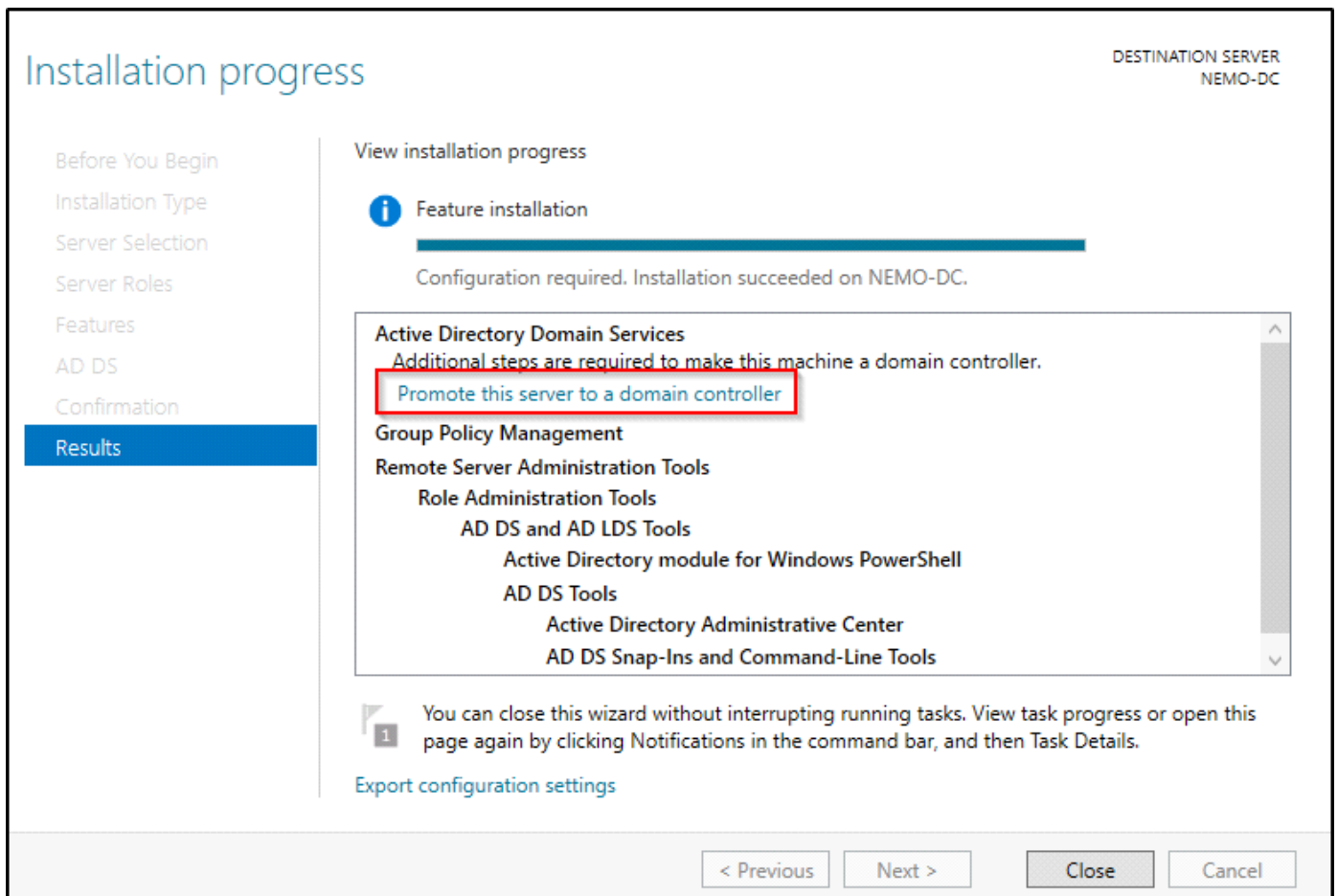
            Active Directory Administrative Center

            AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)  
[Specify an alternate source path](#)

< Previous    Next >    Install    Cancel

Step 17: Before closing the setup, let's click on:



Step 18: Here we need to Add a new forest since we don't have an existing domain or forest:

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER  
NEMO-DC

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name: NEMO.local

[More about deployment configurations](#)

< Previous

Next >

Install

Cancel

Step 19: Now here, we can use the same password that we created:

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER  
NEMO-DC

Deployment Configuration  
Domain Controller Options  
DNS Options  
Additional Options  
Paths  
Review Options  
Prerequisites Check  
Installation  
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server  
☒ Global Catalog (GC)  
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: \*

Confirm password: \*

[More about domain controller options](#)

< Previous Next > Install Cancel

Step 20: Here we can just hit Next:

A delegation for this DNS server cannot be created because the authoritative parent zone cannot

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

< Previous

Next >

Step 21: Now on this step, we just have to wait until the system gives us the name automatically, so don't write anything:



Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER  
NEMO-DC

Deployment Configuration  
Domain Controller Options  
DNS Options  
**Additional Options**  
Paths  
Review Options  
Prerequisites Check  
Installation  
Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous   Next >   Install   Cancel

Step 22: Leave it as default here:

# Paths

TARGET SERVER  
NEMO-DC

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

**Paths**

Review Options

Prerequisites Check

Installation

Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:

C:\Windows\NTDS

...

Log files folder:

C:\Windows\NTDS

...

SYSVOL folder:

C:\Windows\SYSVOL

...

[More about Active Directory paths](#)

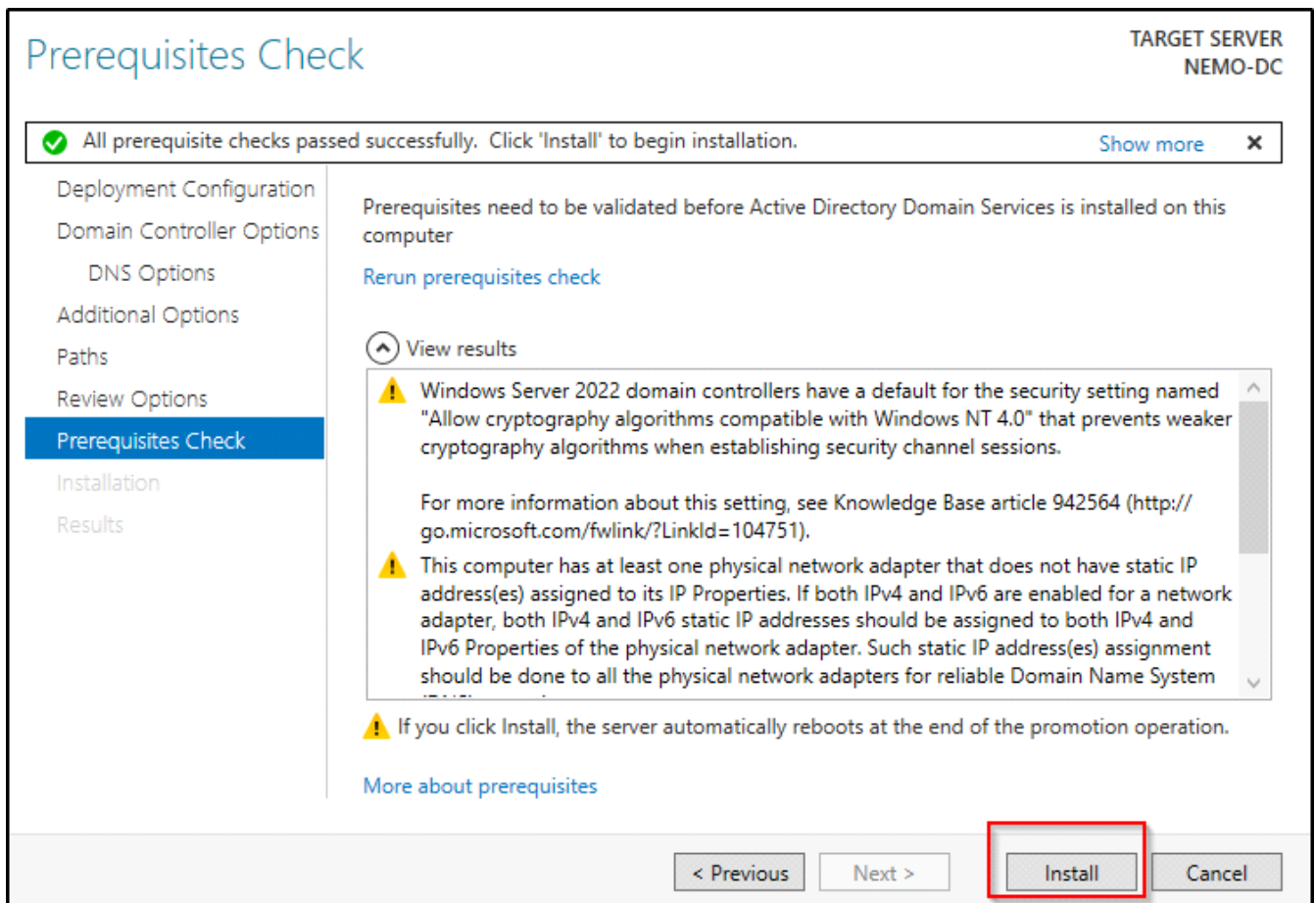
< Previous

Next >

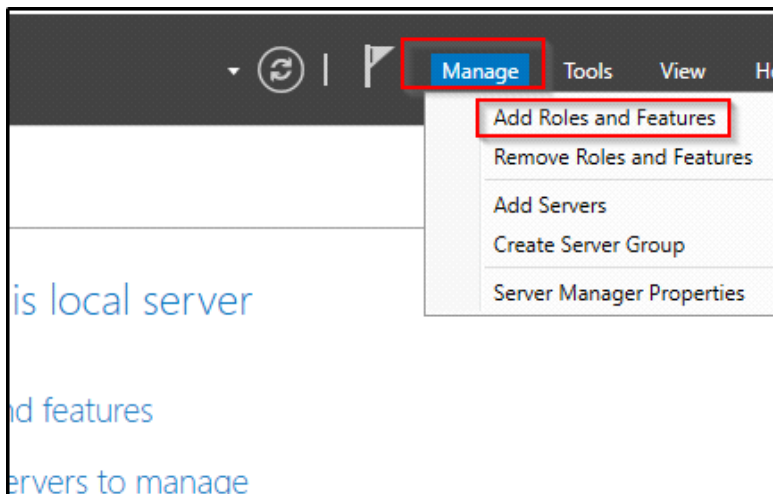
Install

Cancel

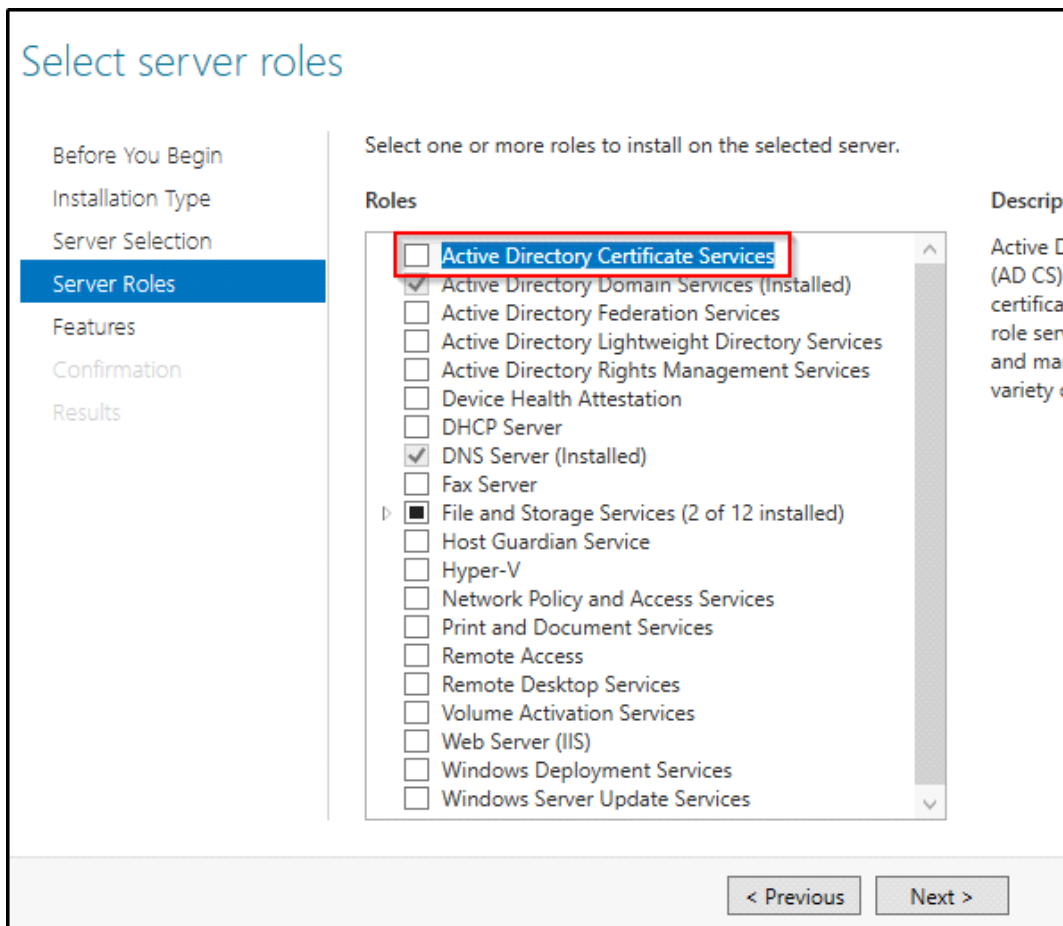
Step 23: Hit install, and it will require to reboot the system:



Step 24: Once rebooted, now we need to also setup Certificate Services:

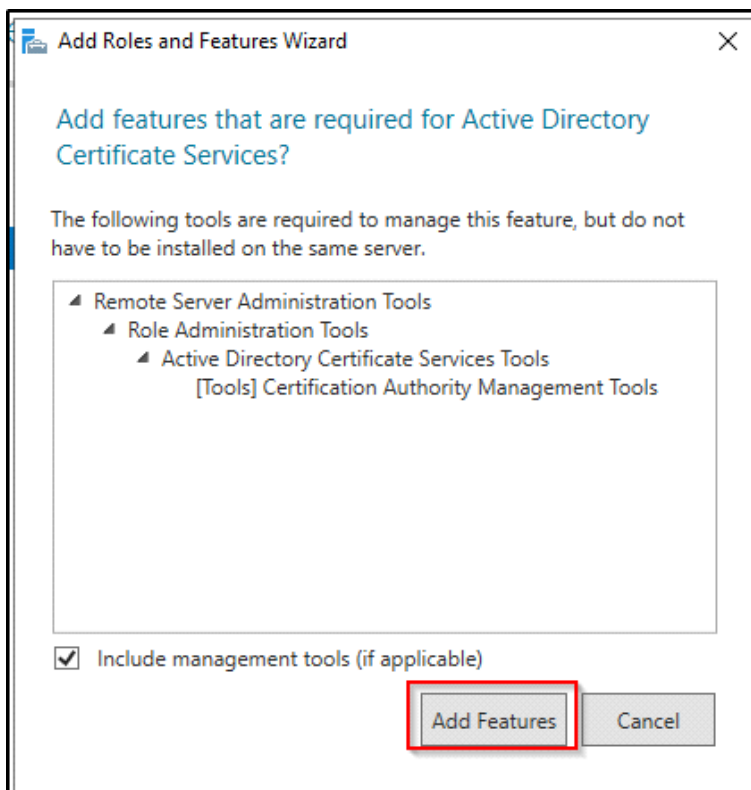


Step 25: Hit Next, until you see this one:



Certificate Services are used to verify identities in a Domain Controller

Select Add Features:



Hit Next again, until you see this one:

Installation selections

DESTINATION SERVER  
NEMO-DC.NEMO.local

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Certificate Services
  - Certification Authority
- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
    - Certification Authority Management Tools

[Export configuration settings](#)  
[Specify an alternate source path](#)

< Previous   Next >   **Install**   Cancel

Check Restart and hit Install

Step 26: Now again press on Configure:

# Installation progress

DESTINATION SERVER  
NEMO-DC.NEMO.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

View installation progress

Feature installation

Configuration required. Installation succeeded on NEMO-DC.NEMO.local.

Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on the destination server

Configure Active Directory Certificate Services on the destination server

Certification Authority

Remote Server Administration Tools

Role Administration Tools

Active Directory Certificate Services Tools

Certification Authority Management Tools

1

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

Step 27: Make sure to check Certification Authority:

## Role Services

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Select Role Services to configure

☒ Certification Authority

☐ Certification Authority Web Enrollment

☐ Online Responder

☐ Network Device Enrollment Service

☐ Certificate Enrollment Web Service

☐ Certificate Enrollment Policy Web Service

Step 28: Now let's create a new private key, since we don't have it:

Private Key NEMO-DC.NE

Credentials  
Role Services  
Setup Type  
CA Type  
**Private Key**  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
Confirmation  
Progress  
Results

### Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ **Create a new private key**  
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key  
Use this option to ensure continuity with previously issued certificates when reinstalling.

☐ Select a certificate and use its associated private key  
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer  
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous **Next >** Configure

Step 29: Select SHA256 as default:

### Specify the cryptographic options

Select a cryptographic provider: Key length:

RSA#Microsoft Software Key Storage Provider 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256  
SHA384  
SHA512  
SHA1  
MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

Step 30: In case we're keeping this lab long term, change it to 99 years:

Period

DESTINATION  
NEMO-DC.NEMO

es

graphy

e

Period

Database

n

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

99

Years

CA expiration Date: 5/16/2123 3:35:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous

Next >

Configure

Ca

Step 31: And lastly, hit Configure, and Reboot the Server:



# Confirmation

DESTINATION SERVER  
NEMO-DC.NEMO.local

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation**
- Progress
- Results

To configure the following roles, role services, or features, click Configure.

## Active Directory Certificate Services

### Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	5/16/2123 3:35:00 PM
Distinguished Name:	CN=NEMO-NEMO-DC-CA,DC=NEMO,DC=local
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous

Next >

**Configure**

Cancel

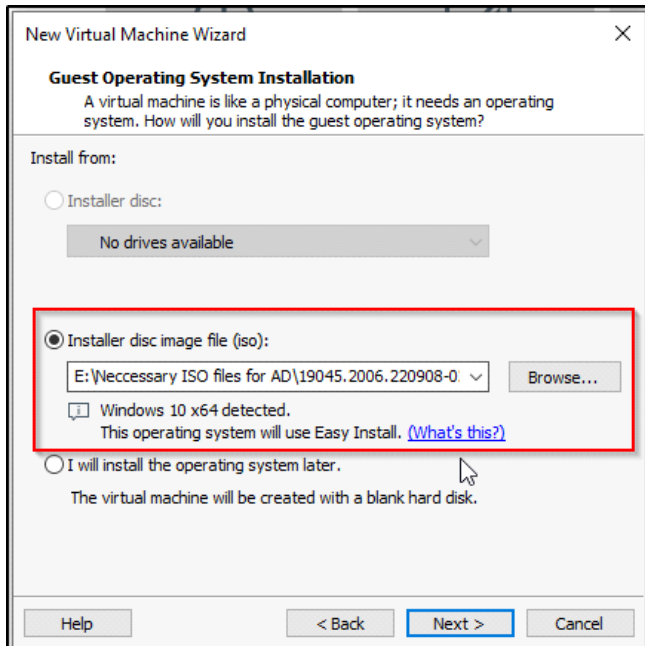
# Setting Up the User Machines

Saturday, June 8, 2024 2:58 PM

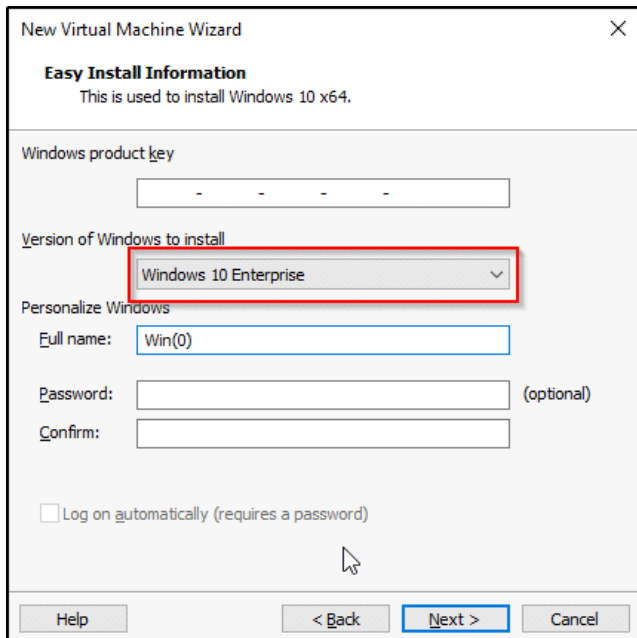
For this lab, we will need 2 user machines, so the steps below are the same

Step 1: On Vmware press Create a New Virtual Machine

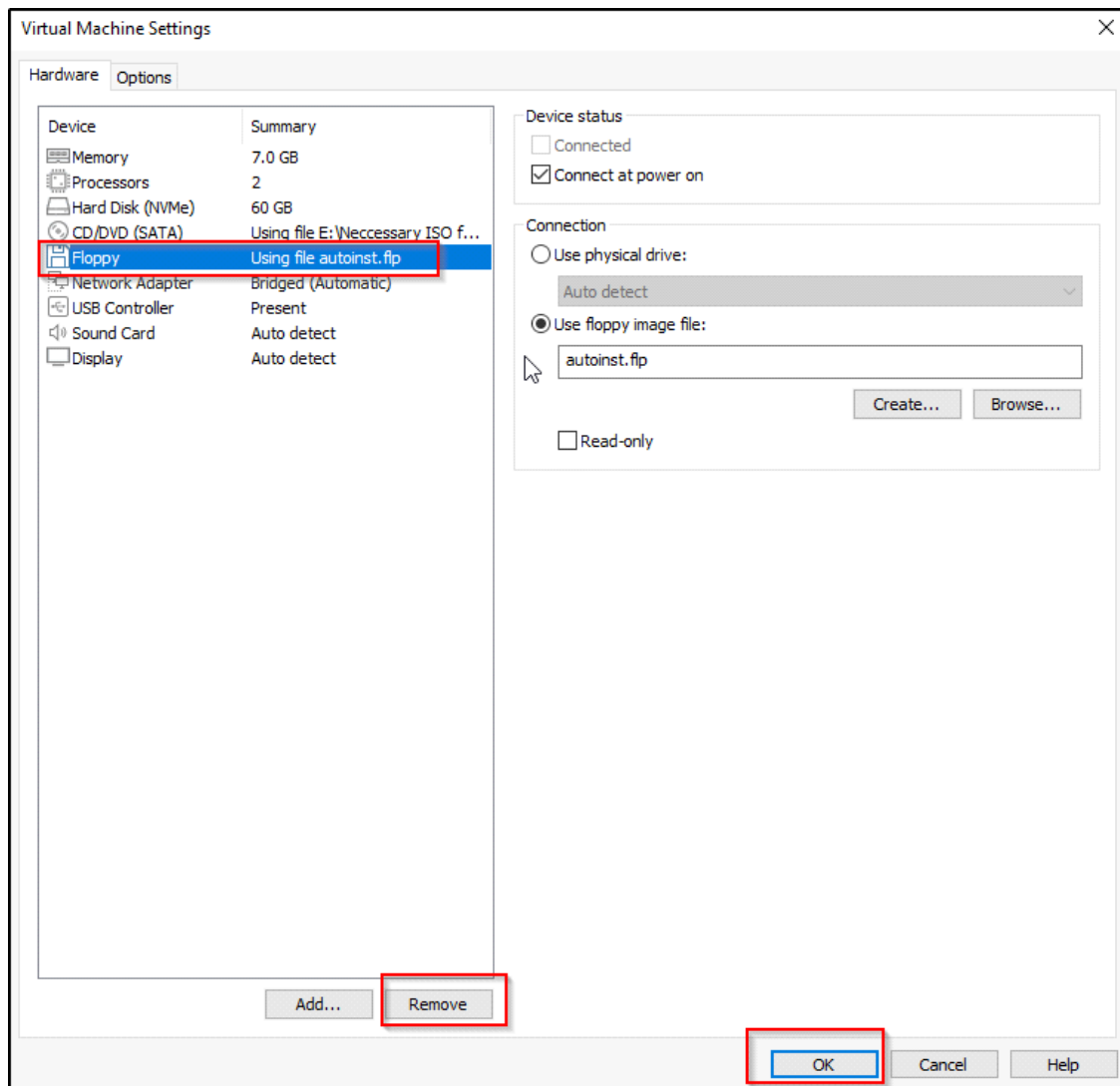
Step 2: Choose the ISO file:



Step 3: Now here all we need to do is select the Windows 10 Enterprise and hit next:



Step 4: This is the most important part, when you create the new machine this way, a floppy disk will appear here, so we need to remove it otherwise we will face an error while installing:



Step 5: After powering on the machine the setup is straightforward, just like we would install windows 10 usually. But here we will need to select "Domain join instead":



# Sign in with Microsoft

Work or school account

someone@example.com

Sign in with a security key

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

Domain join instead

Privacy & cookies

Terms of use

Next

Step 6: After setup is completed, we need to rename the PC like we did with Domain Controller.

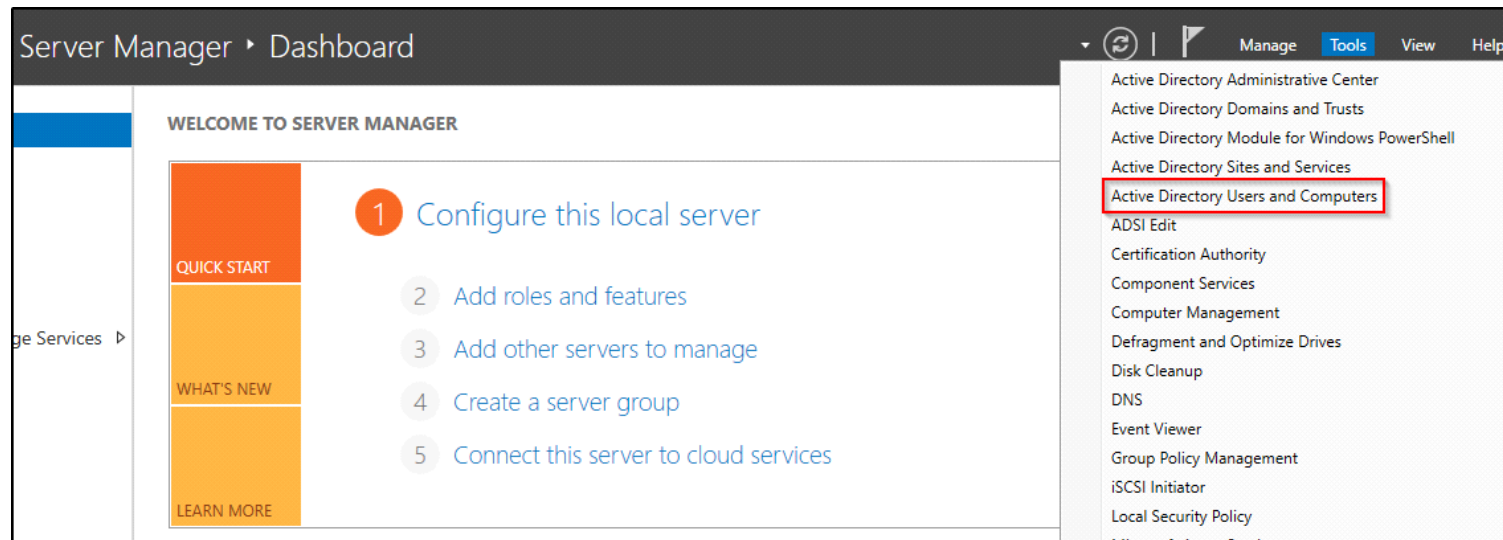
# Setting Up Users, Groups, and Policies

Sunday, June 9, 2024 12:28 PM

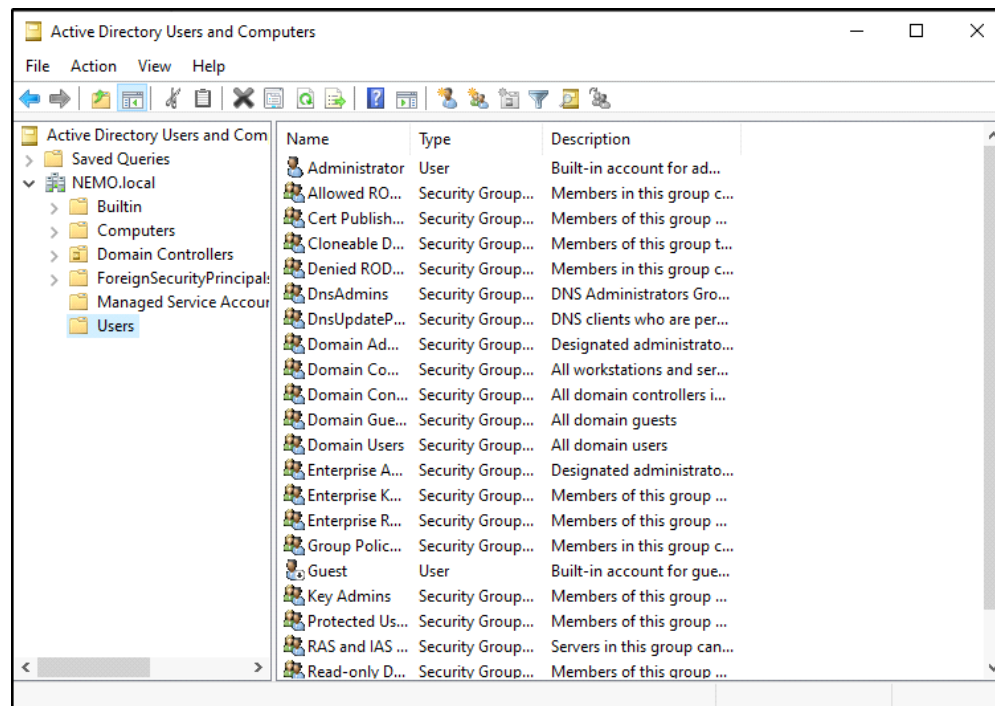
We're going to create some users, groups and some policies

Creating users:

Step 1: When you log in, click here:

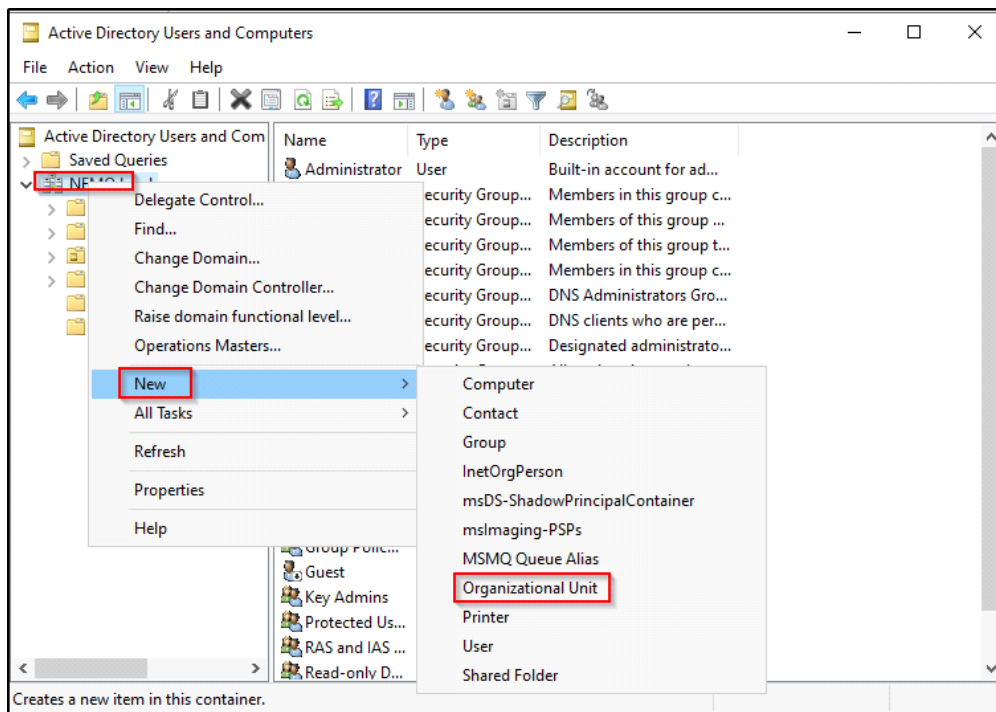


Step 2: Now we're going to see a lot of users here:

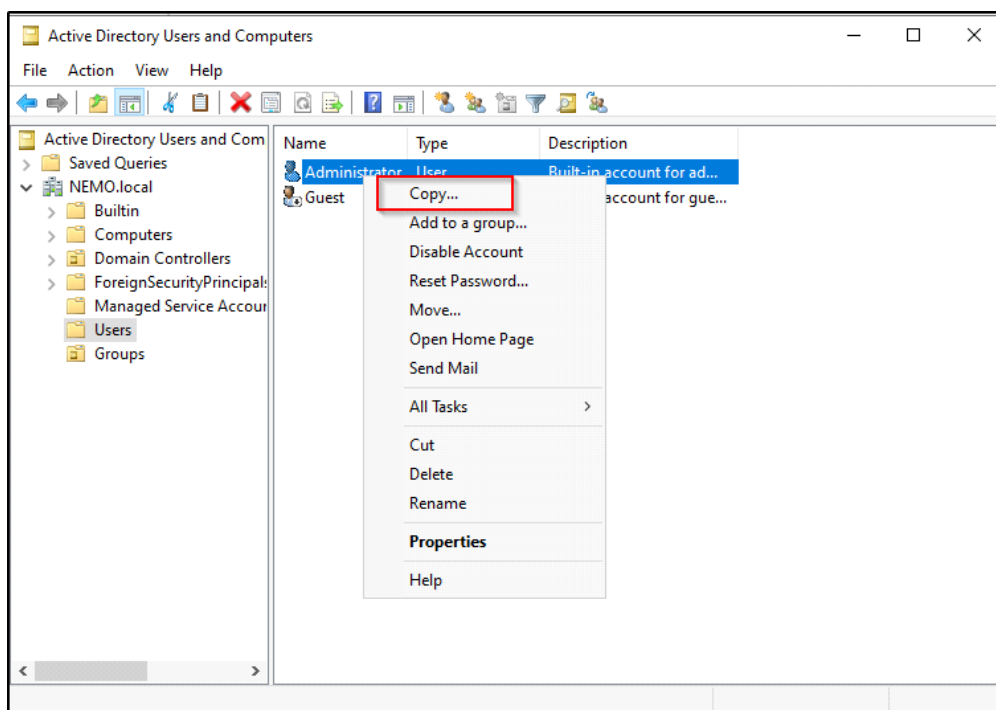


Step 3: Let's clean this up a bit, let's create an Organizational Unit (OU) named Groups and store all these usernames there except: Administrator and Guest

First right click on NEMO.local then select New then Organizational Unit and name it Groups:



Step 4: Now let's create a domain admin, to do so we can right click on current Administrator and click Copy. This will copy all the privileges that the account has:



And let's give the name as Tony Stark, and the initials as tstark:

Copy Object - User

Create in: NEMO.local/Users

First name: Tony Initials:

Last name: Stark

Full name: Tony Stark

User logon name: tstark @NEMO.local

User logon name (pre-Windows 2000): NEMO\ tstark

< Back Next > Cancel

Copy Object - User

Create in: NEMO.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Password: Password1234

Step 5: Now let's duplicate the Administrator account again, so we can create a Service Account that is a domain administrator (they're used to run a service):

Copy Object - User

Create in: NEMO.local/Users

First name: SQL Initials:

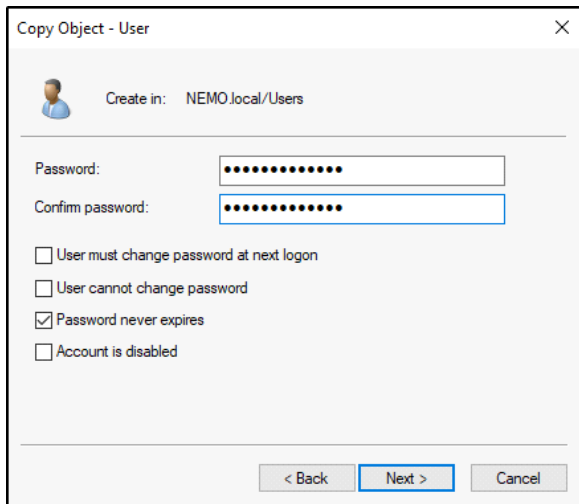
Last name: Service

Full name: SQL Service

User logon name: SQLService @NEMO.local

User logon name (pre-Windows 2000): NEMO\ SQLService

< Back Next > Cancel



Copy Object - User

Create in: NEMO.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

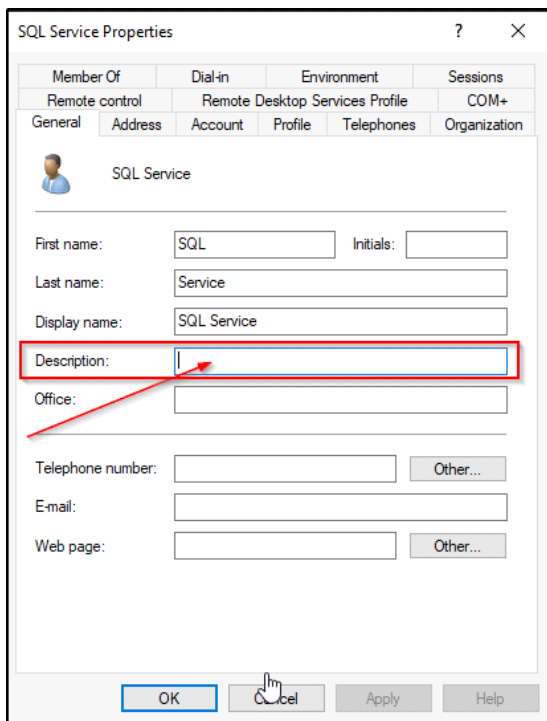
☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Password: Password12345

Step 6: If we double click on SQL Service now, we will see something like description, NEVER EVER EVER put your password there, since a simple user can read it to, this is something a lot of domain administrators do:



SQL Service Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+

General Address Account Profile Telephones Organization

SQL Service

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:  Other...

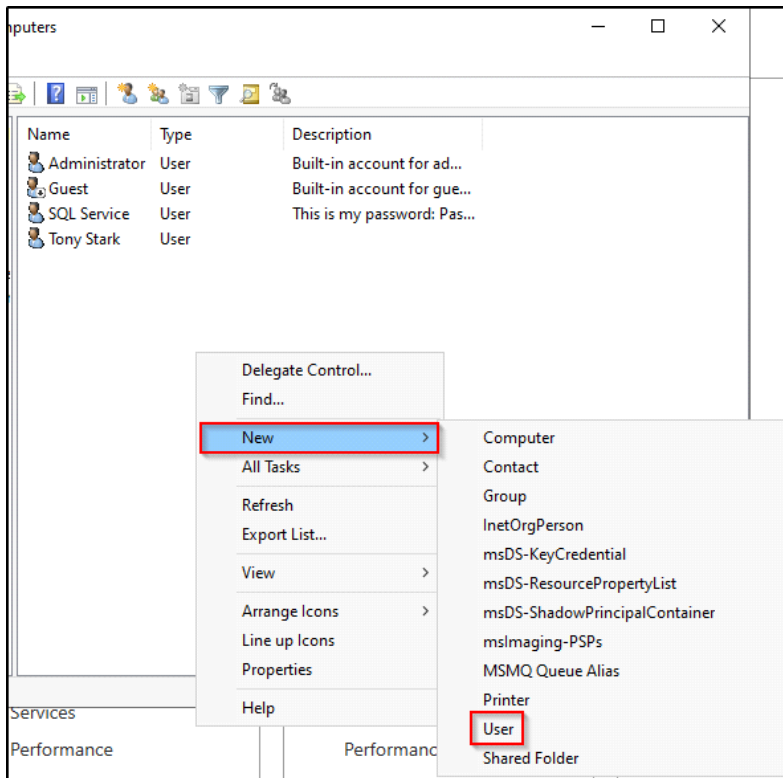
E-mail:

Web page:  Other...

OK Cancel Apply Help

Step 7: Now let's create 2 simple users, to do so right click anywhere inside the users, New > User:





The 'New Object - User' dialog box is shown in its first step. It contains the following fields and options:

- Create in:** NEMO.local/Users
- First name:** Frank
- Initials:** (empty)
- Last name:** Castle
- Full name:** Frank Castle
- User logon name:** fcastle
- User logon name (pre-Windows 2000):** NEMO\
- Domain:** @NEMO.local

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue rectangle.

The 'New Object - User' dialog box is shown in its second step. It contains the following fields and options:

- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled

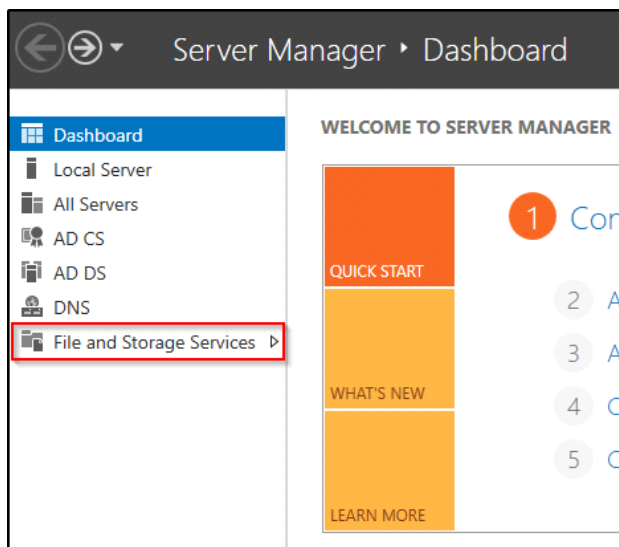
At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue rectangle.

Password: Password1

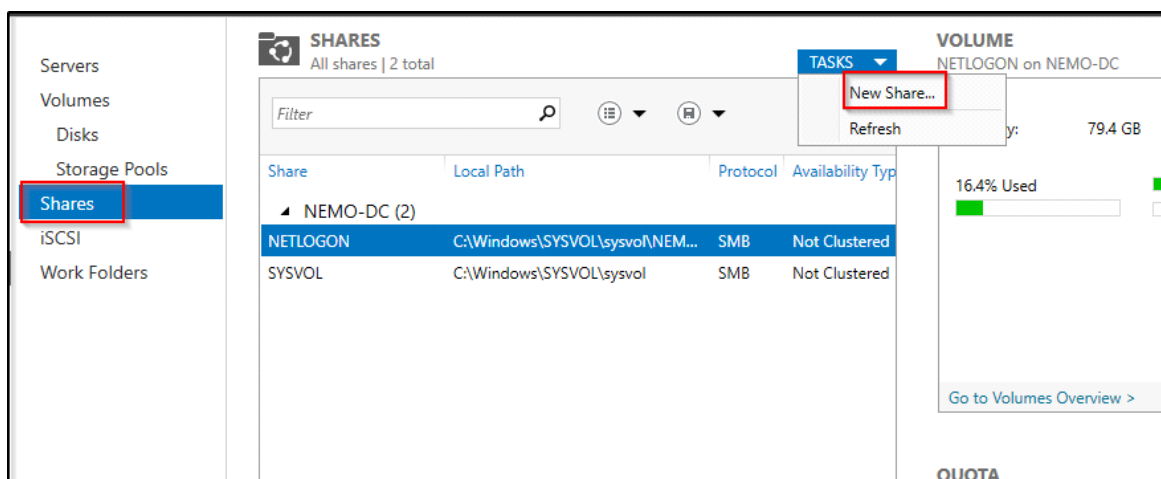
Repeat the same process for user: Peter Parker, password: Password2

Now let's create a file share that we will abuse later on:

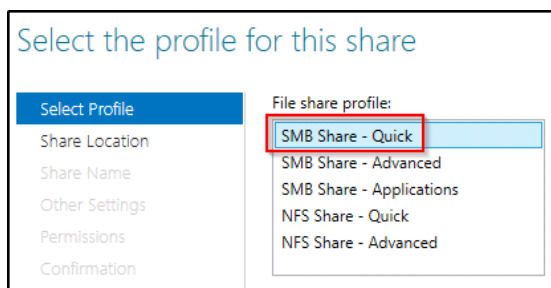
Step 1: At the Dashboard, click on File and Storage Services:



Step 2: Click on Shares and then Tasks > New Share:



Step 3: Select SMB Share - Quick:



Step 4: Leave it as default here:

## Select the server and path for this share

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Server:

Server Name	Status	Cluster Role	Owner Node
NEMO-DC	Online	Not Clustered	

Share location:

☒ Select by volume:

Volume	Free Space	Capacity	File System
C:	66.3 GB	79.4 GB	NTFS

Step 5: And here give it whatever name you want, in our case: hackme:

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Specify share name

Share name:

hackme

Share description:

Local path to share:

C:\Shares\hackme

!

 If the folder does not exist, the folder is created.

Remote path to share:

\\NEMO-DC\hackme

Step 6: Leave it as default here:

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Configure share settings

☐ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☐ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

Step 7: Leave it as default, and hit create:

## Specify permissions to control access

Select Profile

Share Location

Share Name

Other Settings

**Permissions**

Confirmation

Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files

Customize permissions...

Now let's set the service account fully that we had before:

Step 1: to do so open cmd as administrator

Step 2: Please check the command multiple times before you execute it, since a back slash instead of forward slash cannot work or anything else:

```
C:\Users\Administrator>setspn -a NEMO-DC/SQLService.NEMO.local:60111 NEMO\SQLService
Checking domain DC=NEMO,DC=local

Registering ServicePrincipalNames for CN=SQL Service,CN=Users,DC=NEMO,DC=local
NEMO-DC/SQLService.NEMO.local:60111
Updated object
```

```
setspn -a NEMO-DC/SQLService.NEMO.local:60111 NEMO\SQLService
```

Step 3: Now that we updated object, let's query it to make sure that we really updated it:

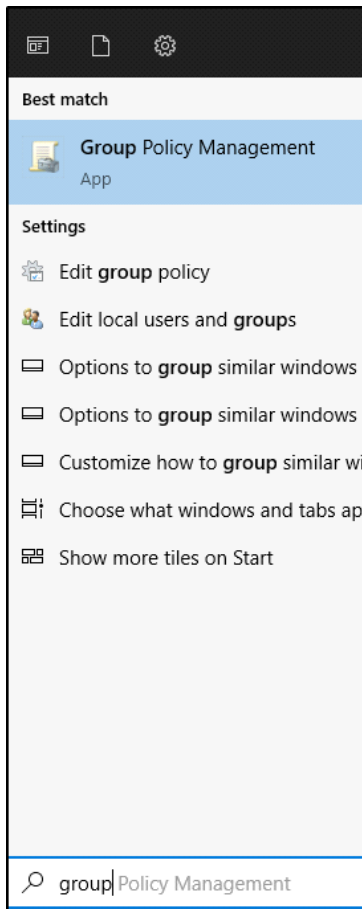
```
C:\Users\Administrator>setspn -T NEMO.local -Q */*
Checking domain DC=NEMO,DC=local
CN=NEMO-DC,OU=Domain Controllers,DC=NEMO,DC=local
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/NEMO-DC.NEMO.local
ldap/NEMO-DC.NEMO.local/ForestDnsZones.NEMO.local
ldap/NEMO-DC.NEMO.local/DomainDnsZones.NEMO.local
DNS/NEMO-DC.NEMO.local
GC/NEMO-DC.NEMO.local/NEMO.local
RestrictedKrbHost/NEMO-DC.NEMO.local
RestrictedKrbHost/NEMO-DC
RPC/a7667643-14dd-4fca-b0fe-1ea4fcb10116._msdcs.NEMO.local
HOST/NEMO-DC/NEMO
HOST/NEMO-DC.NEMO.local/NEMO
HOST/NEMO-DC
HOST/NEMO-DC.NEMO.local
HOST/NEMO-DC.NEMO.local/NEMO.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/a7667643-14dd-4fca-b0fe-1ea4fcb10116/NEMO.local
ldap/NEMO-DC/NEMO
ldap/a7667643-14dd-4fca-b0fe-1ea4fcb10116._msdcs.NEMO.local
ldap/NEMO-DC.NEMO.local/NEMO
ldap/NEMO-DC
ldap/NEMO-DC.NEMO.local
ldap/NEMO-DC.NEMO.local/NEMO.local
CN=krbtgt,CN=Users,DC=NEMO,DC=local
kadmin/changepw
CN=SQL Service,CN=Users,DC=NEMO,DC=local
NEMO-DC/SQLService.NEMO.local:60111

Existing SPN found!
```

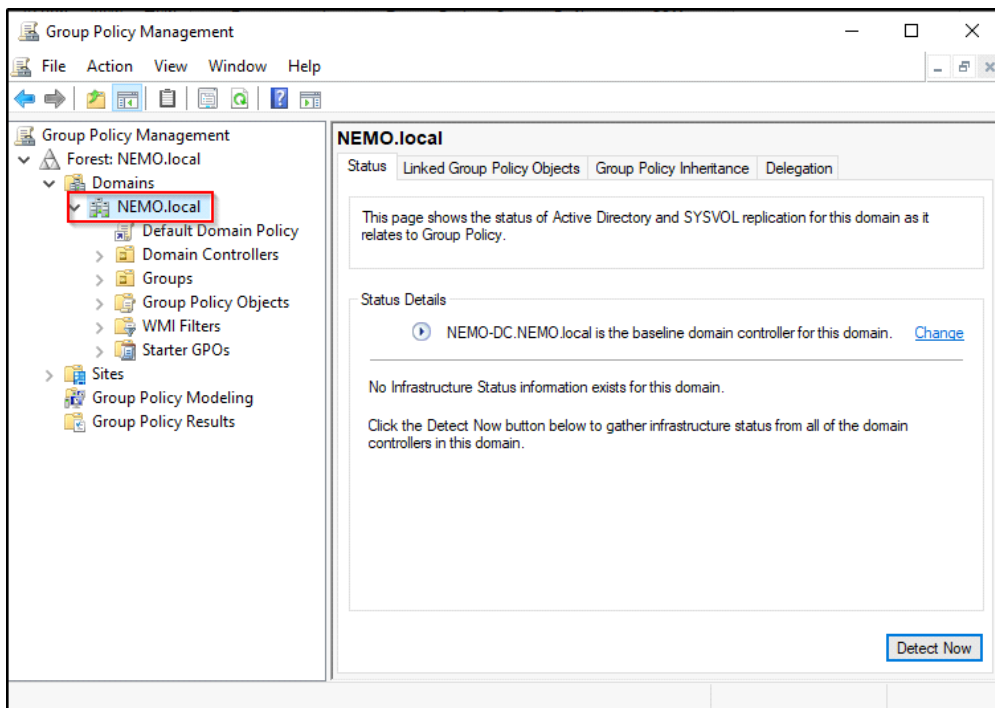
```
setspn -T NEMO.local -Q */*
```

Now let's set up a group policy

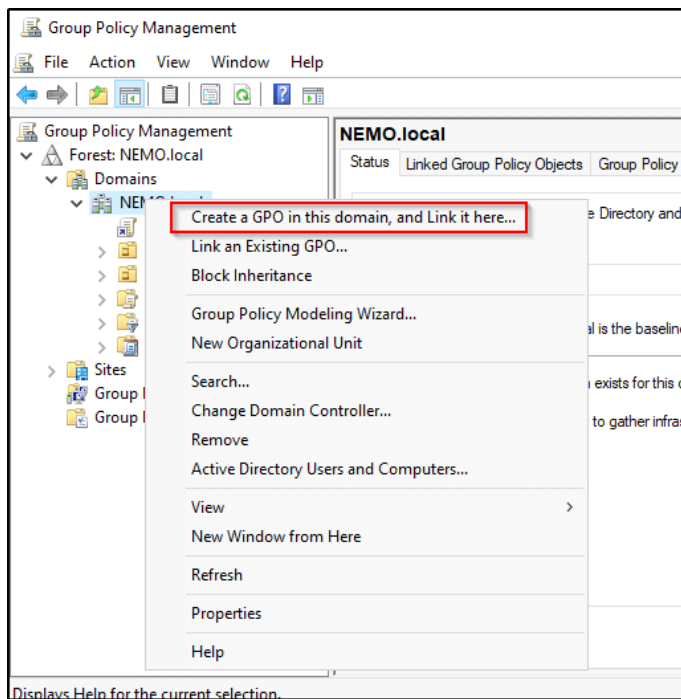
Step 1: At the start search for Group Policy Management:



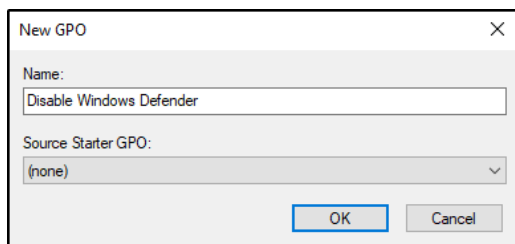
Step 2: We can set a specific GPO for a specific group or anything here, but we're going to do for the whole domain:



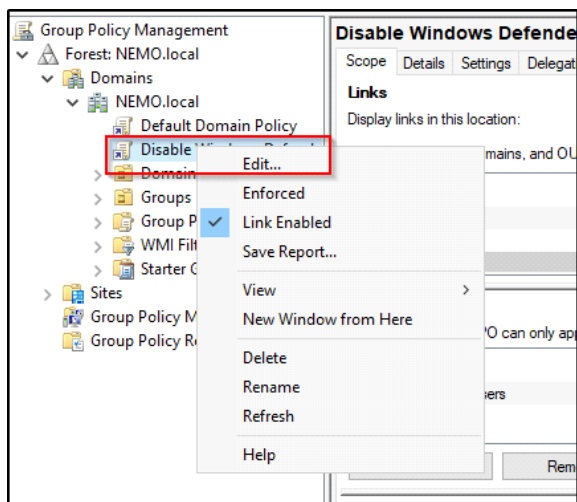
Step 3: Right click on NEMO.local and select:



Step 4: And we're going to call it: Disable Windows Defender:

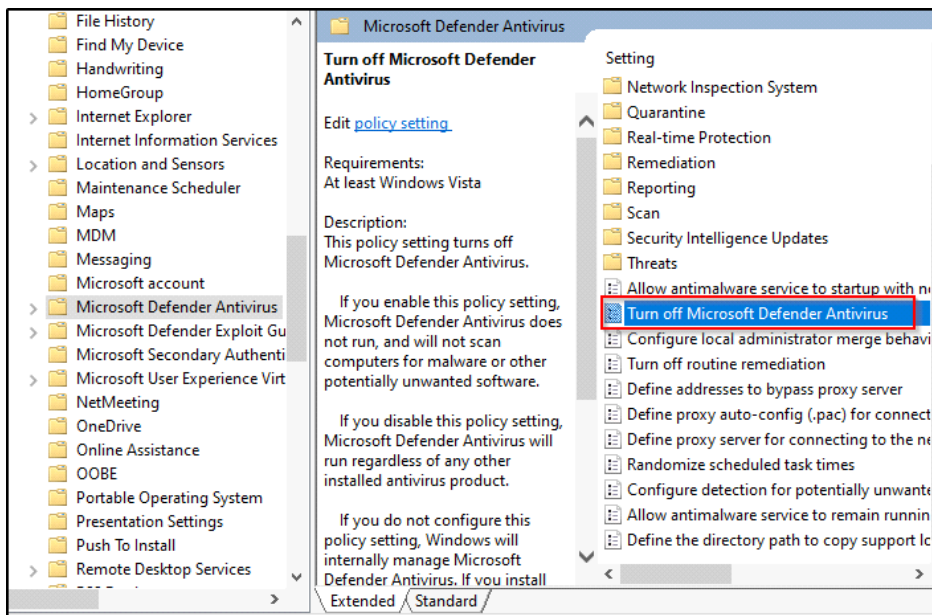


Step 5: Right click on the GPO that we just created and select Edit:

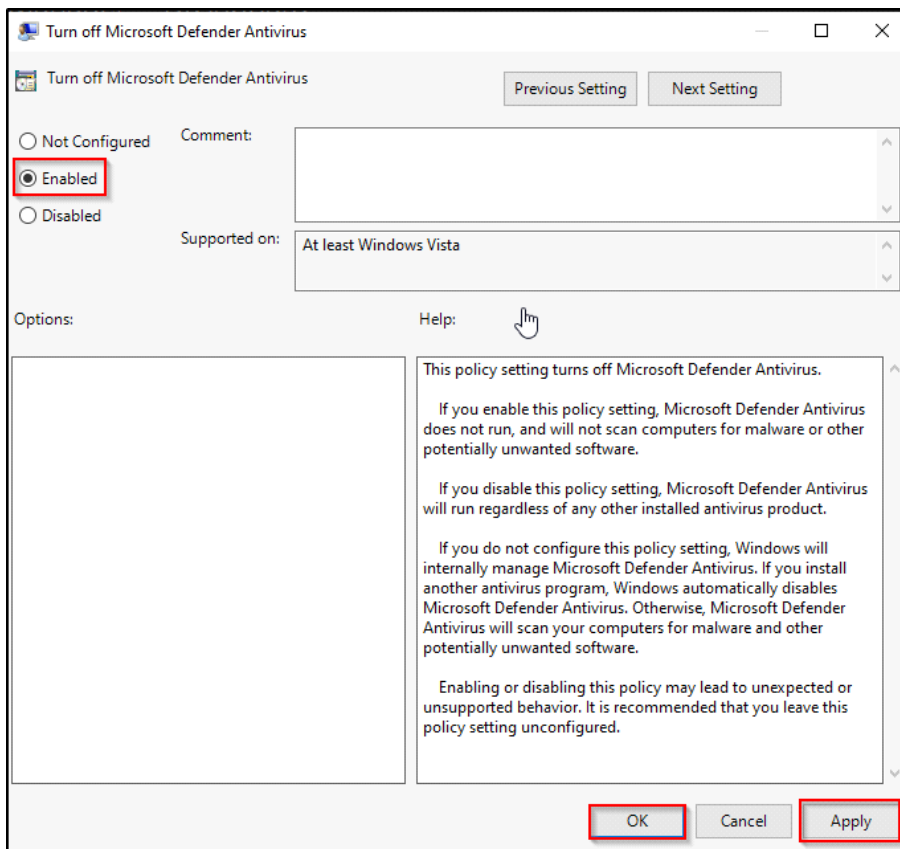


Step 6: Under Computer Configuration select: Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus

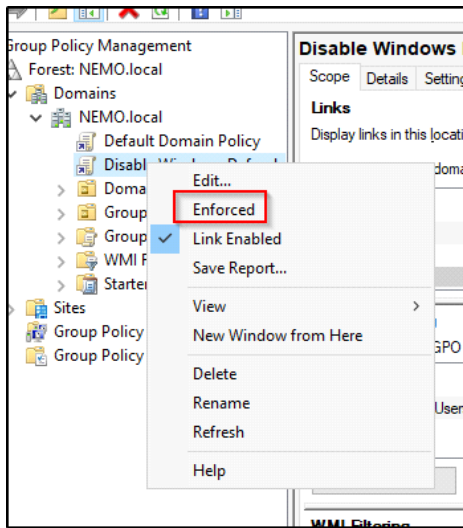
Step 7: Once we found Microsoft Defender Antivirus, click once on it and look at the right side:



Double click on Turn off Microsoft Defender Antivirus, select Enabled > Apply > Ok:



Step 8: Last thing that we're going to do here is right click on GPO that we created again, and select Enforced, any time a user joins this domain it's going to get this policy:



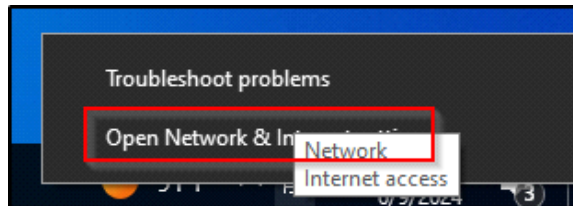


# Joining Our Machines to the Domain

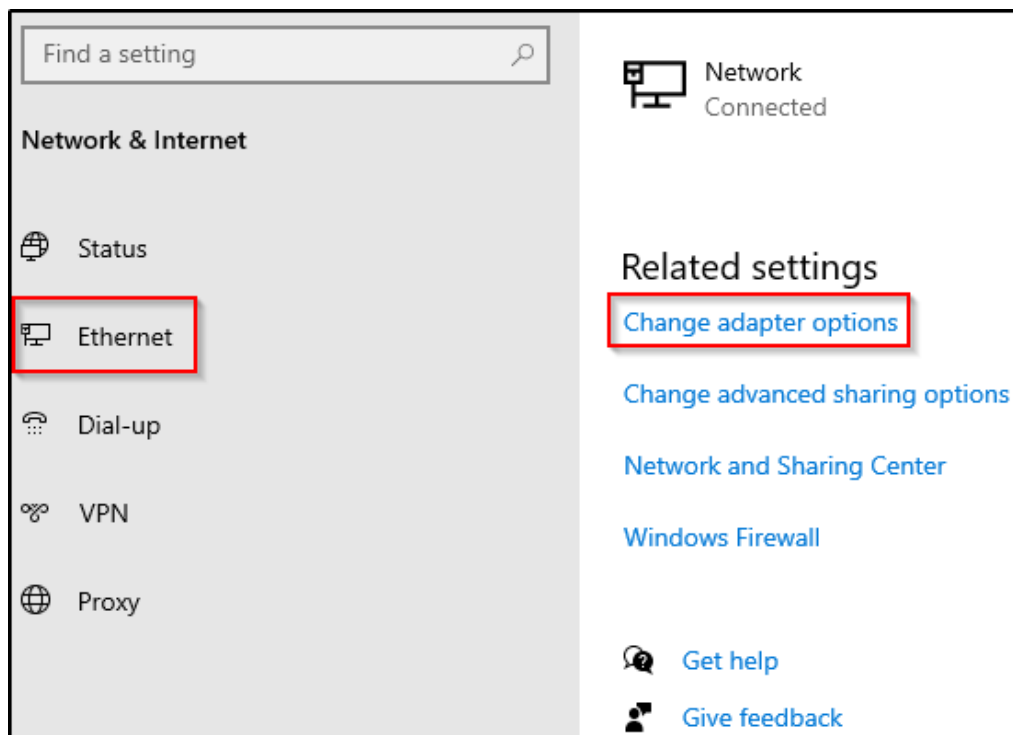
Sunday, June 9, 2024 2:56 PM

To join our machines to the domain we need to specify the IP address of AD in our case 192.168.100.79

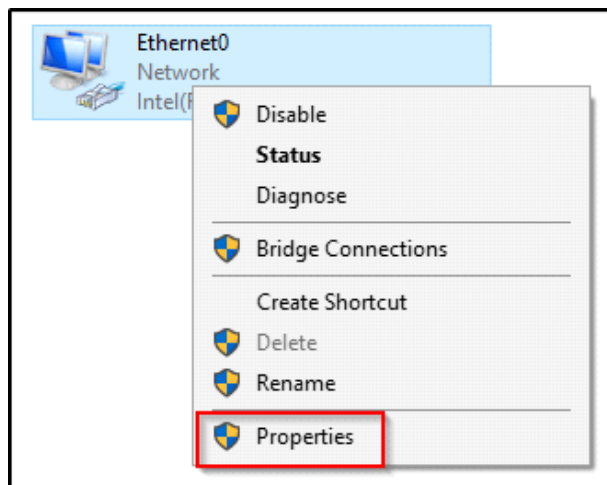
Step 1: On both machines that we've created, go to:



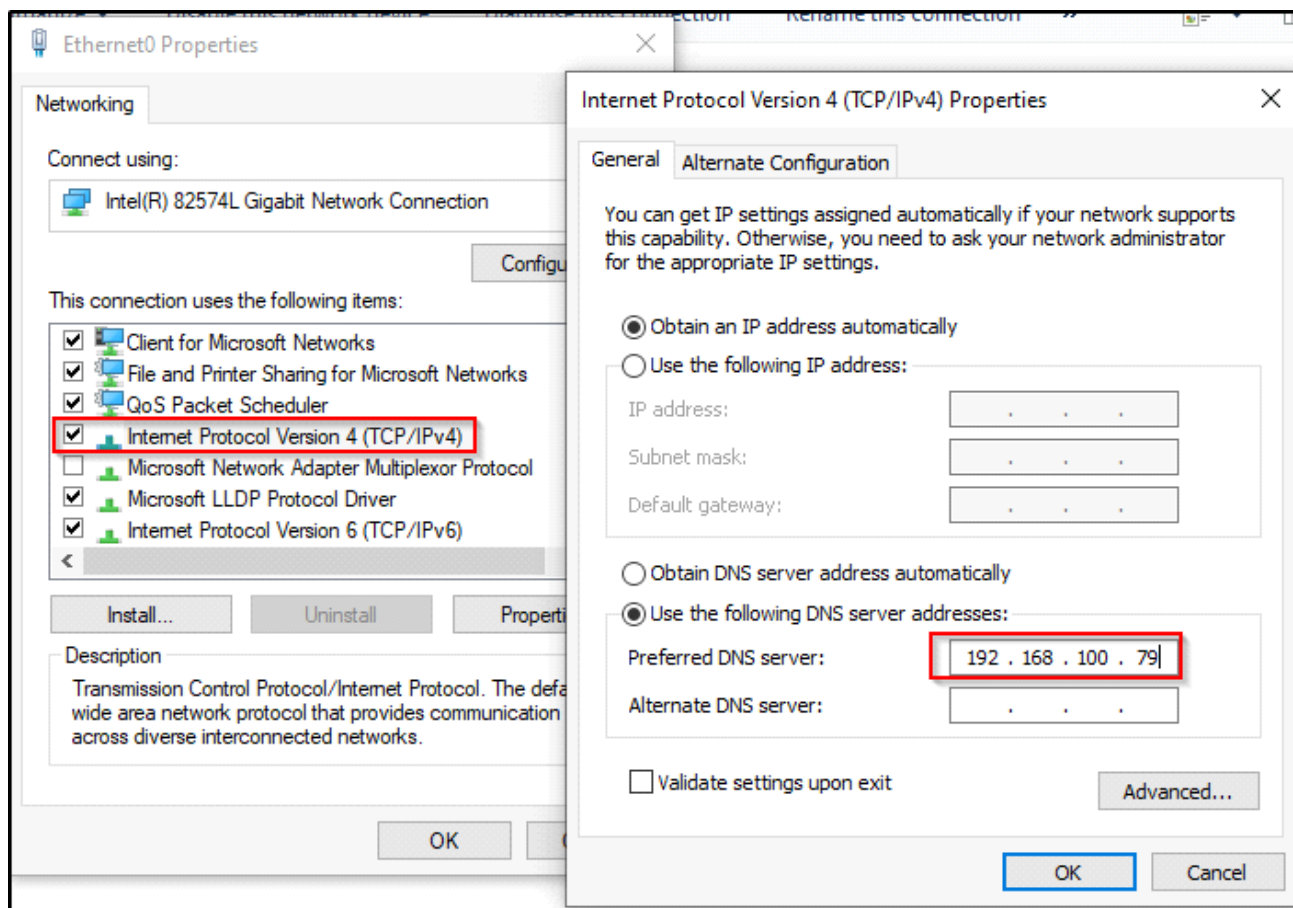
Step 2: Press on Ethernet and Change adapter options:



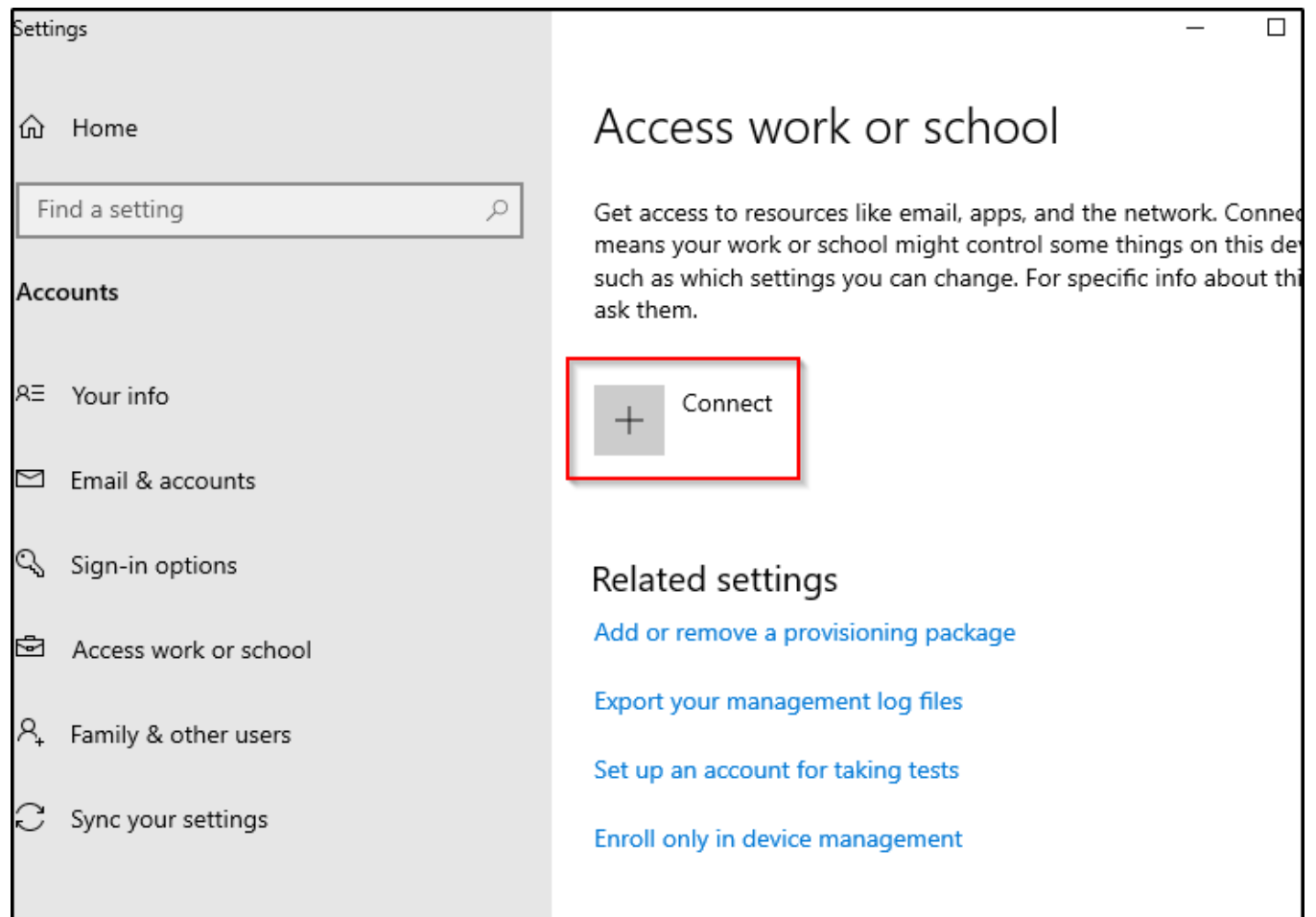
Step 3: Right click on Ethernet0 and click Properties:



Step 4: Click on IPv4 and set the DNS server our AD IP:



Step 5: Now we're going to join the domain, at the start search for: Access work or school, and hit connect:



Step 6: Now select Join this device to a local Active Directory domain:

## Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

### Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

[Join this device to Microsoft Entra ID](#)

[Join this device to a local Active Directory domain](#)

Next

Step 7: Specify the domain name that we want to join:

Join a domain

Join a domain

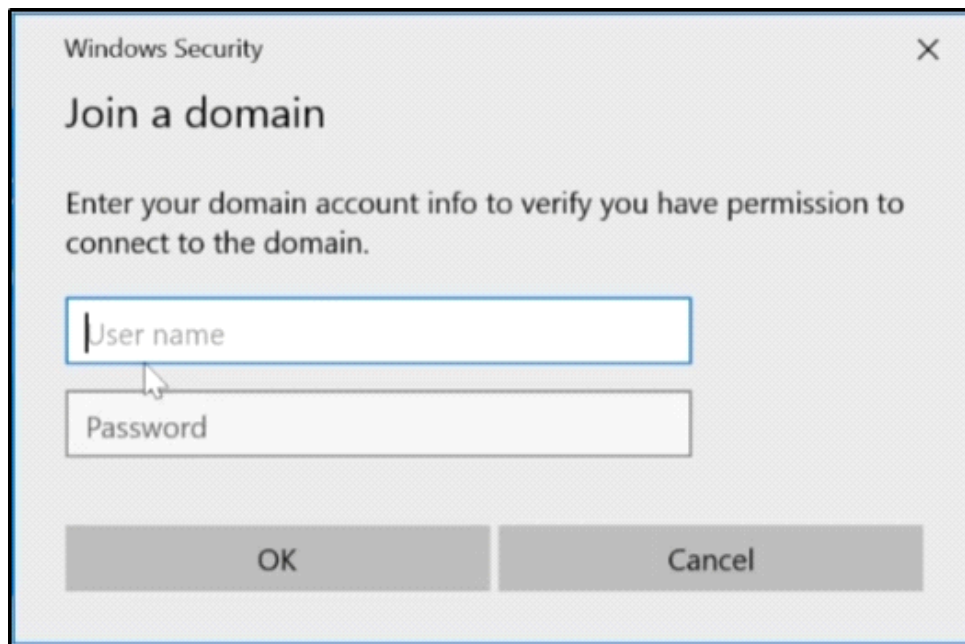
Domain name

NEMO.local

Next

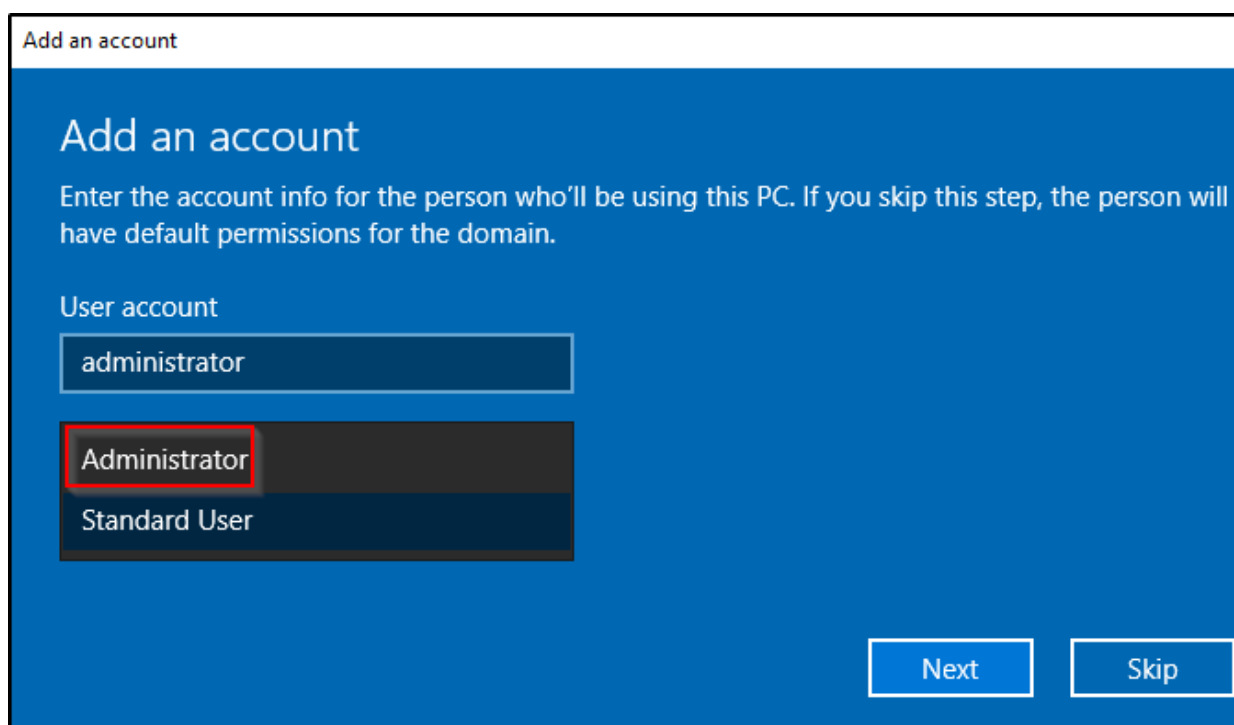
Cancel

Step 8: If it finds the domain, then we'll get a pop up like this:

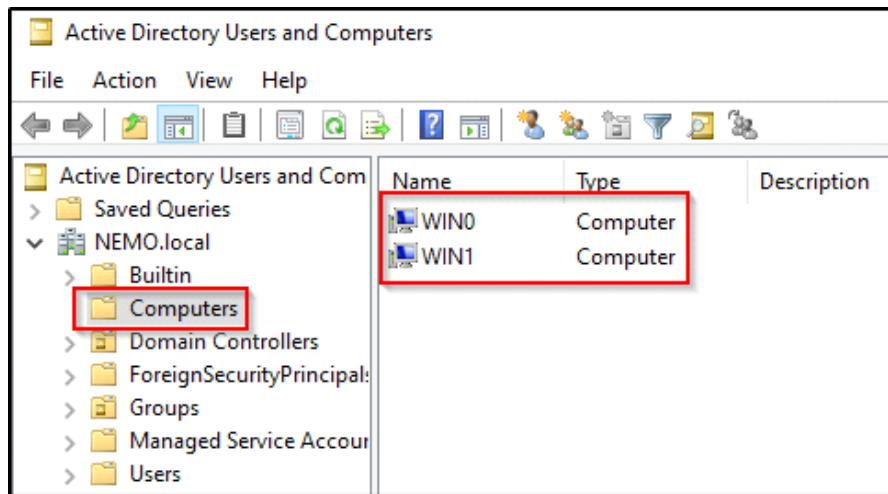
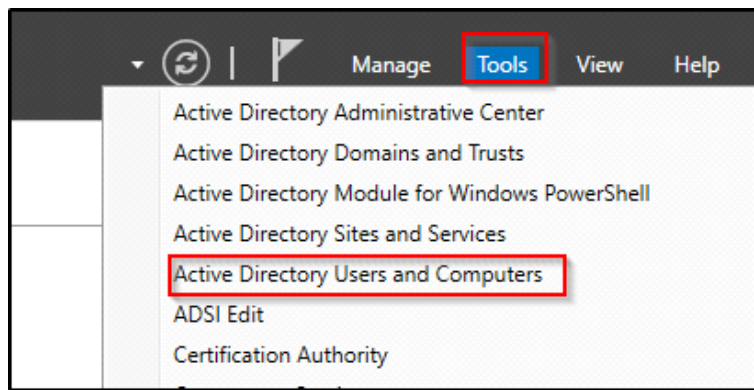


Login with administrator/Password123@ that we created

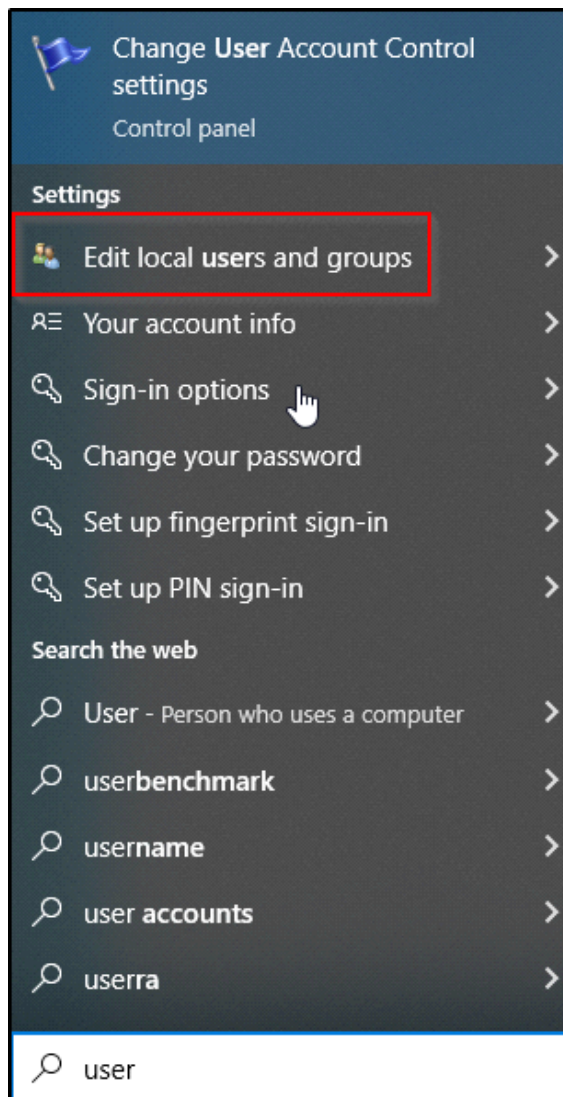
Step 9: Here let's choose Administrator:



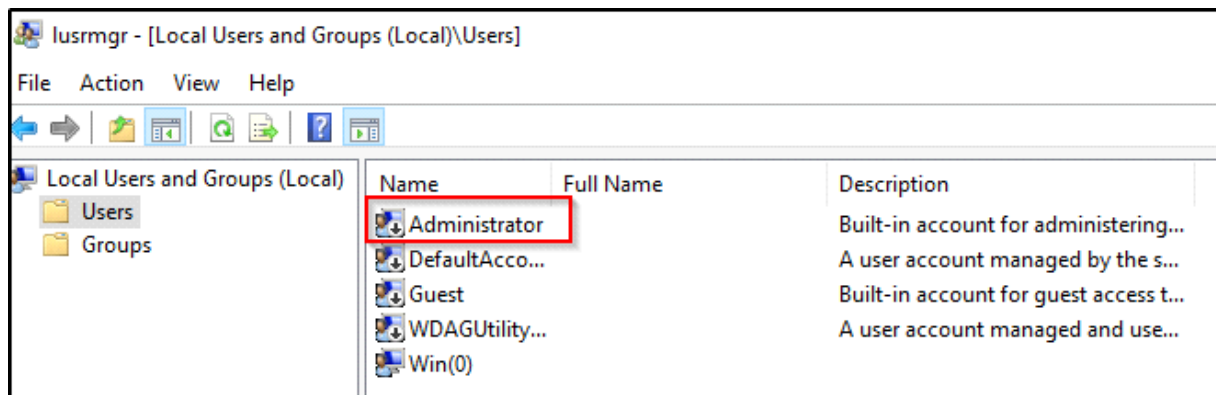
Step 10: Now let's check real quick if we added successfully computers on AD, on the dashboard select Tools > Active Directory Users and Computers:



Step 11: Now let's create a local admin on both PC's, at start search for Edit local users and groups:

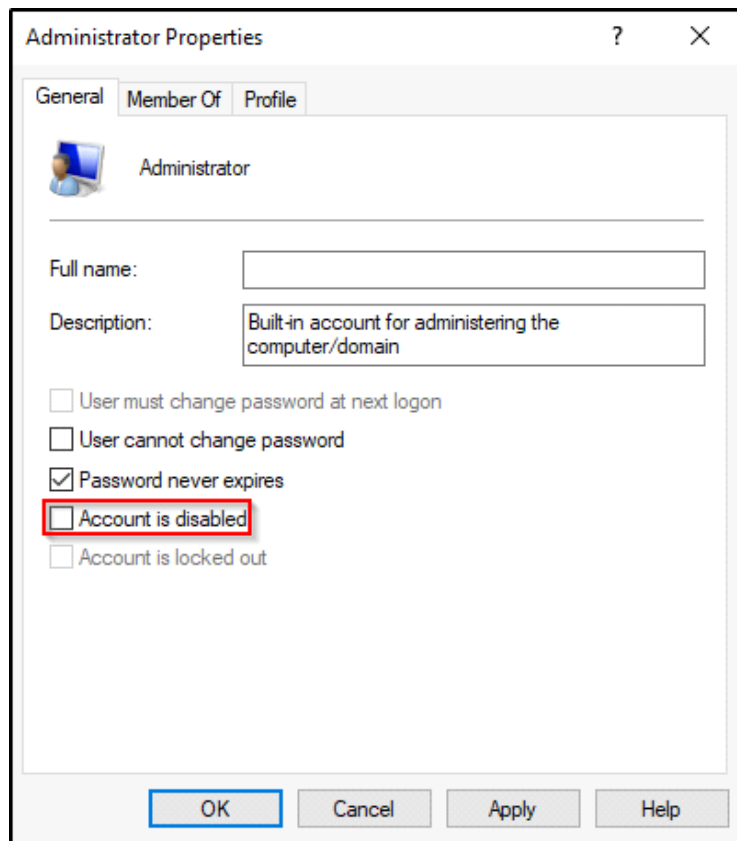


Step 12: Here, right click on Administrator and choose Set Password, let's set a password for Administrator:

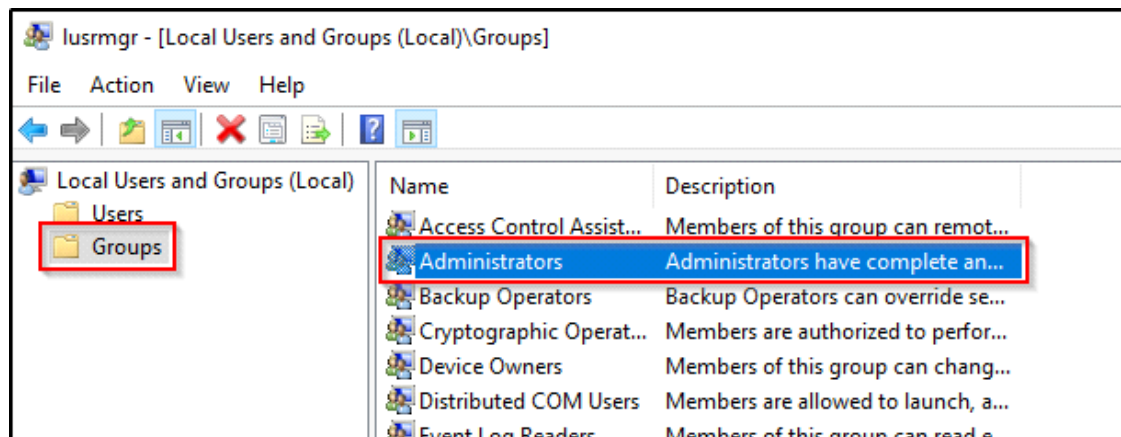


Password: Password12

Step 13: Now double click on Administrator and uncheck Account is disabled:

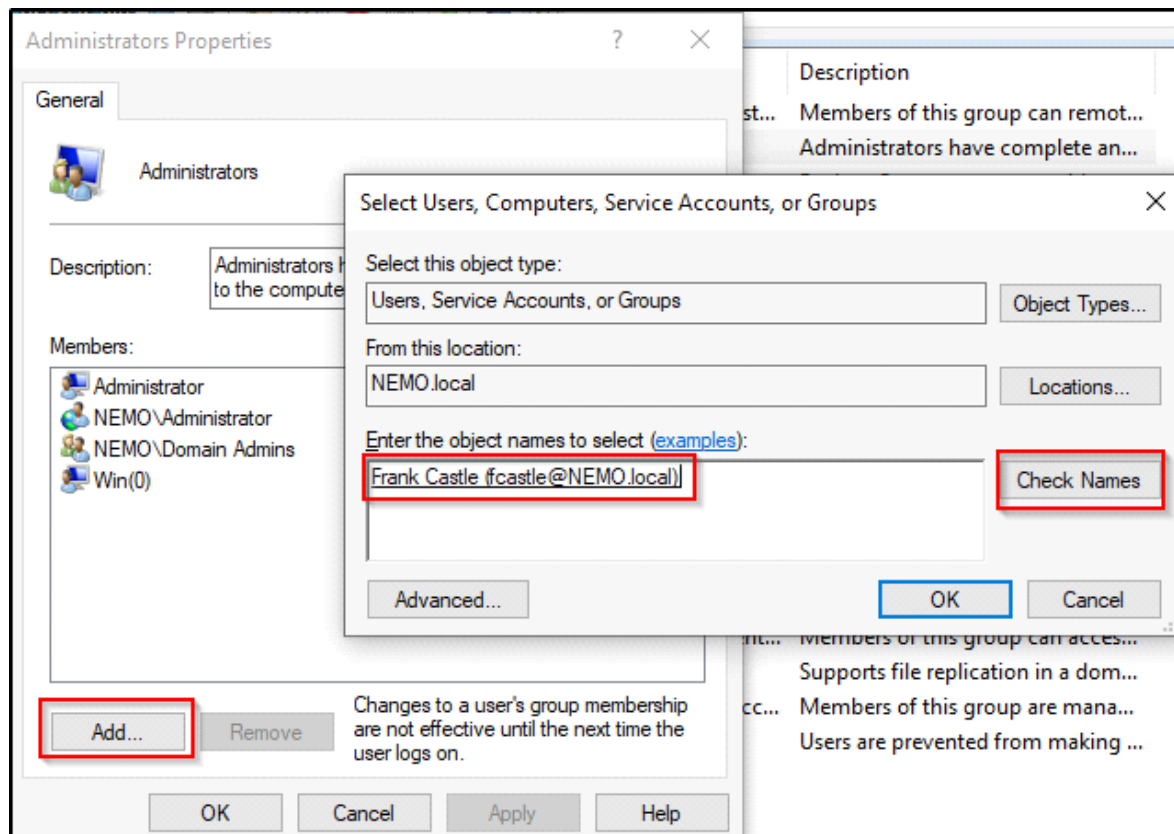


Step 14: Now let's go to Groups and double click on Administrators:



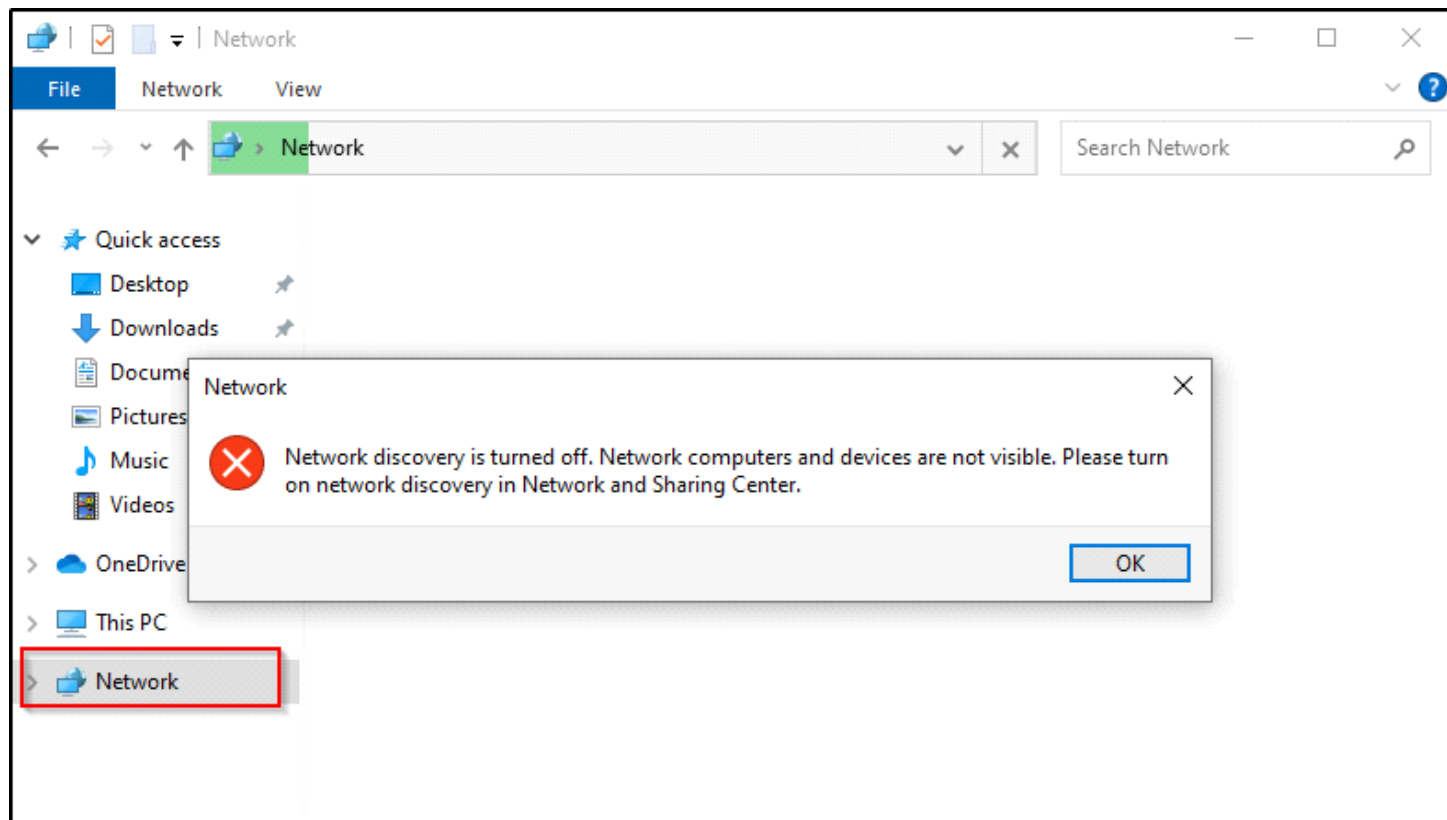
Step 15: Let's add 1 more user to this machine which we created also in AD, Frank Castle:

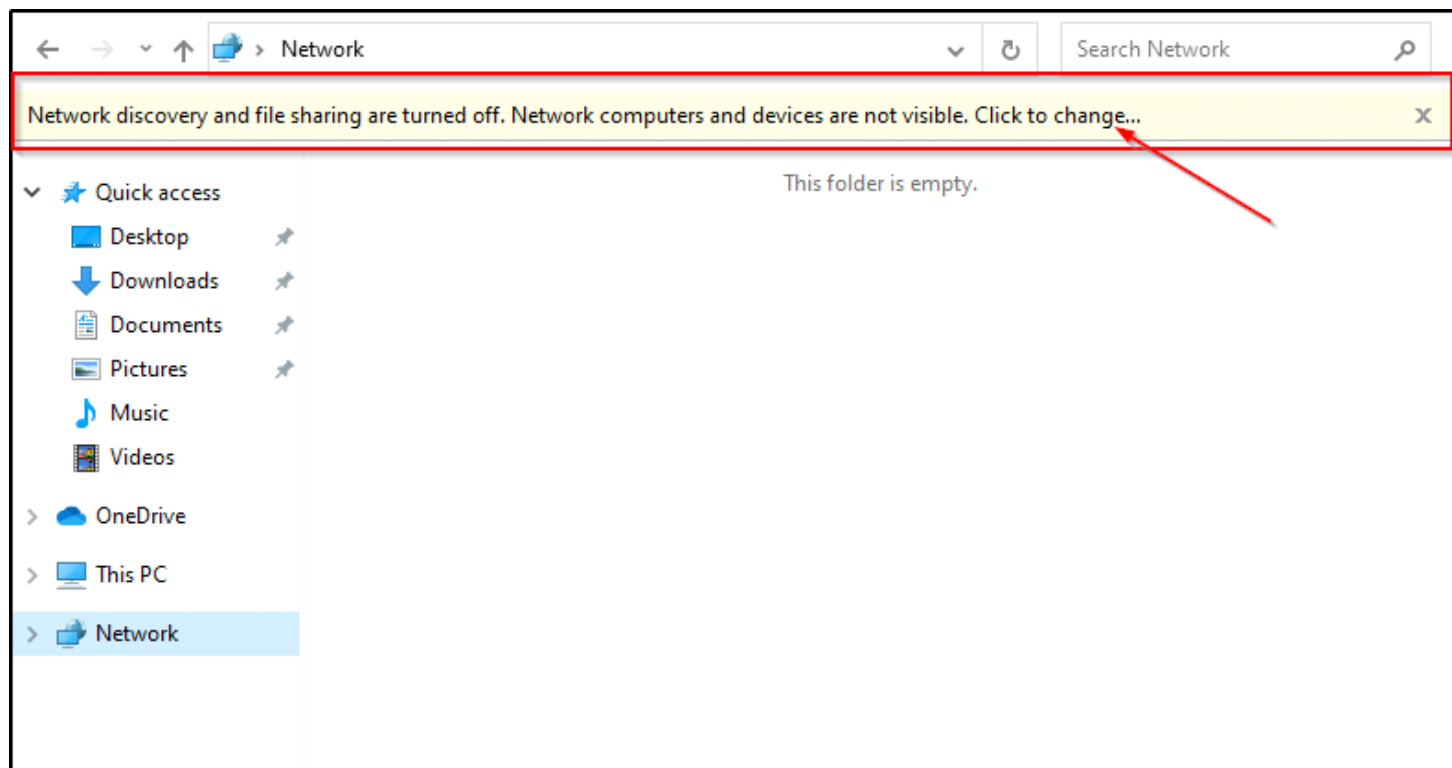




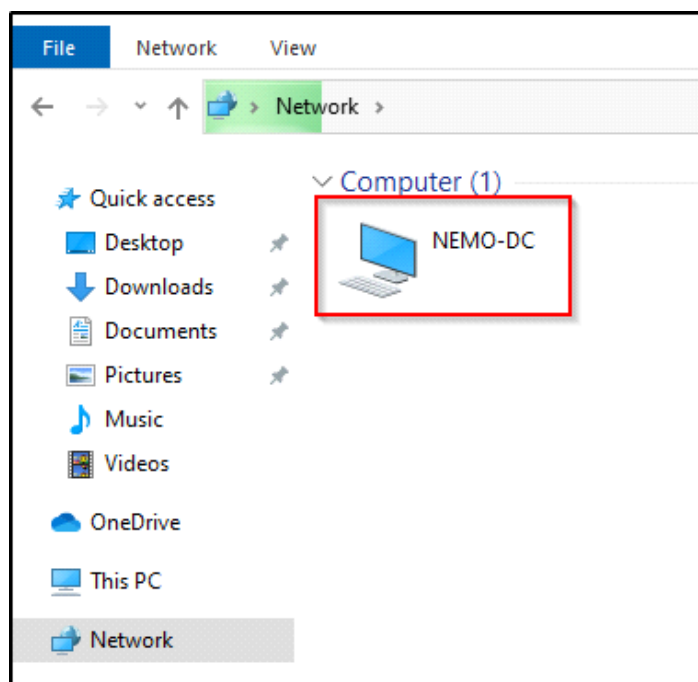
At the: Enter the object names to select just type: fcastle and then Check Names, it will automatically complete.

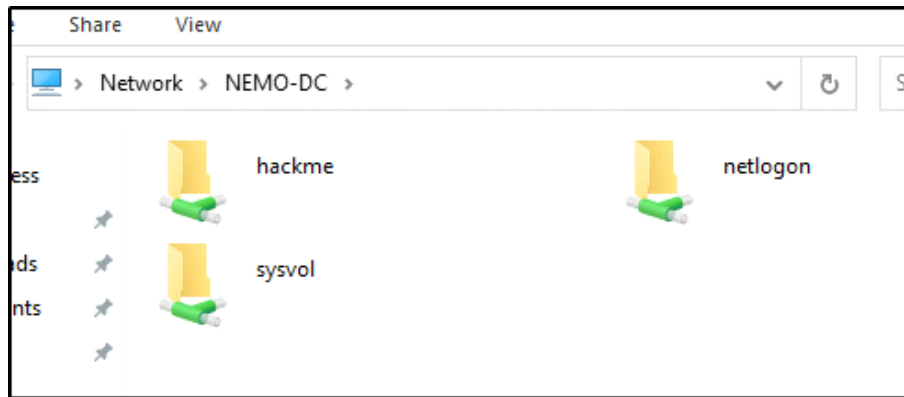
Step 16: Now go to File Explorer and select the Network, if it shows this error then enable Network discovery on 2nd picture:





Step 17: Now we can see our DC:





Now repeat the same process on the other PC too, just remember at step 12 passwords need to be identical between the 2 PC's.

At the 2nd PC in our case Win(1) add 2 users, fcastle and pparker

Differences of logging into the accounts that we created:

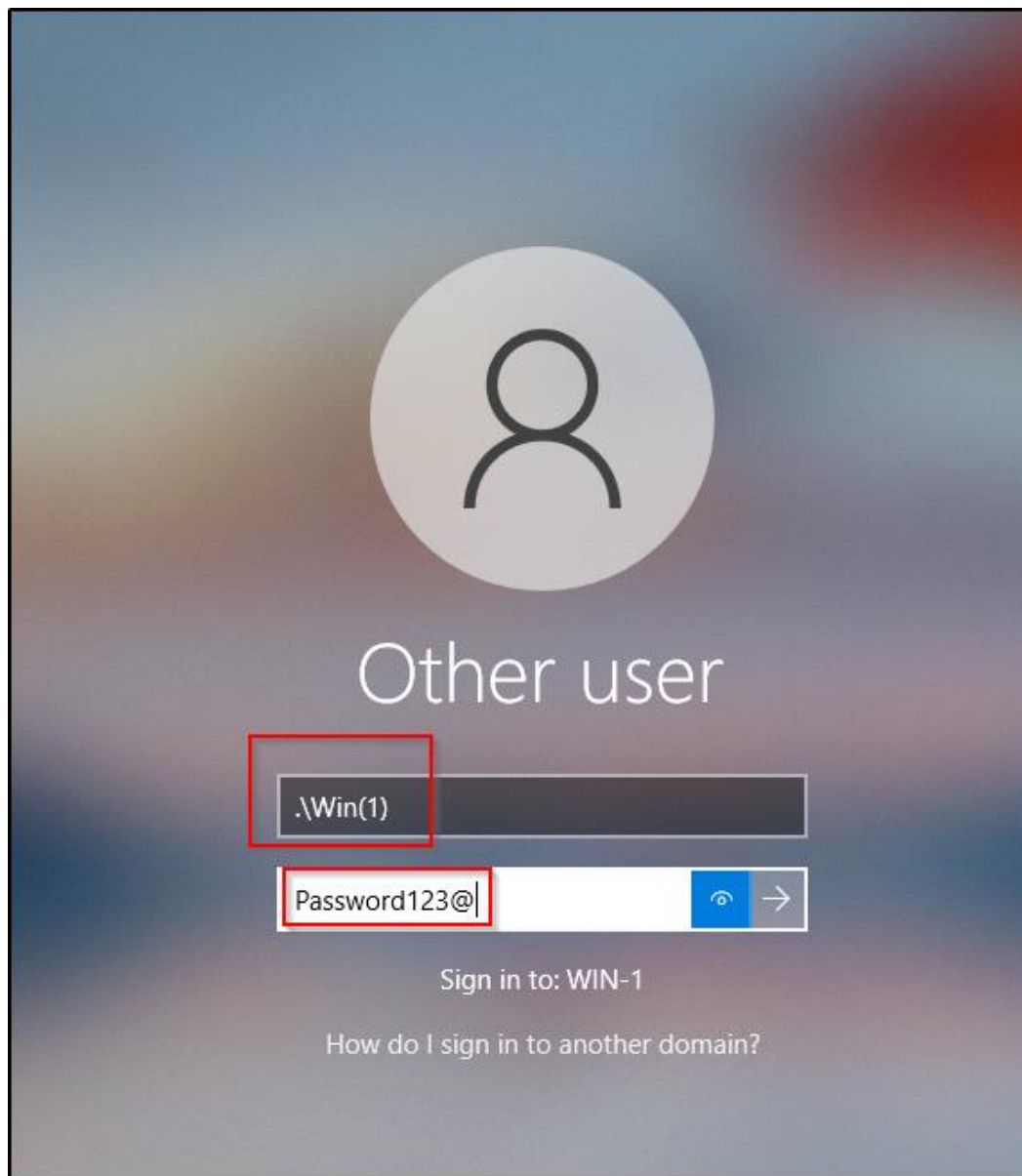
**Logging in with .\Win(0) or .\Win(1):**

- You are using a local user account that exists only on that specific machine.
- Useful for standalone systems or when domain services are unavailable.

**Logging in with fcastle@NEMO.local:**

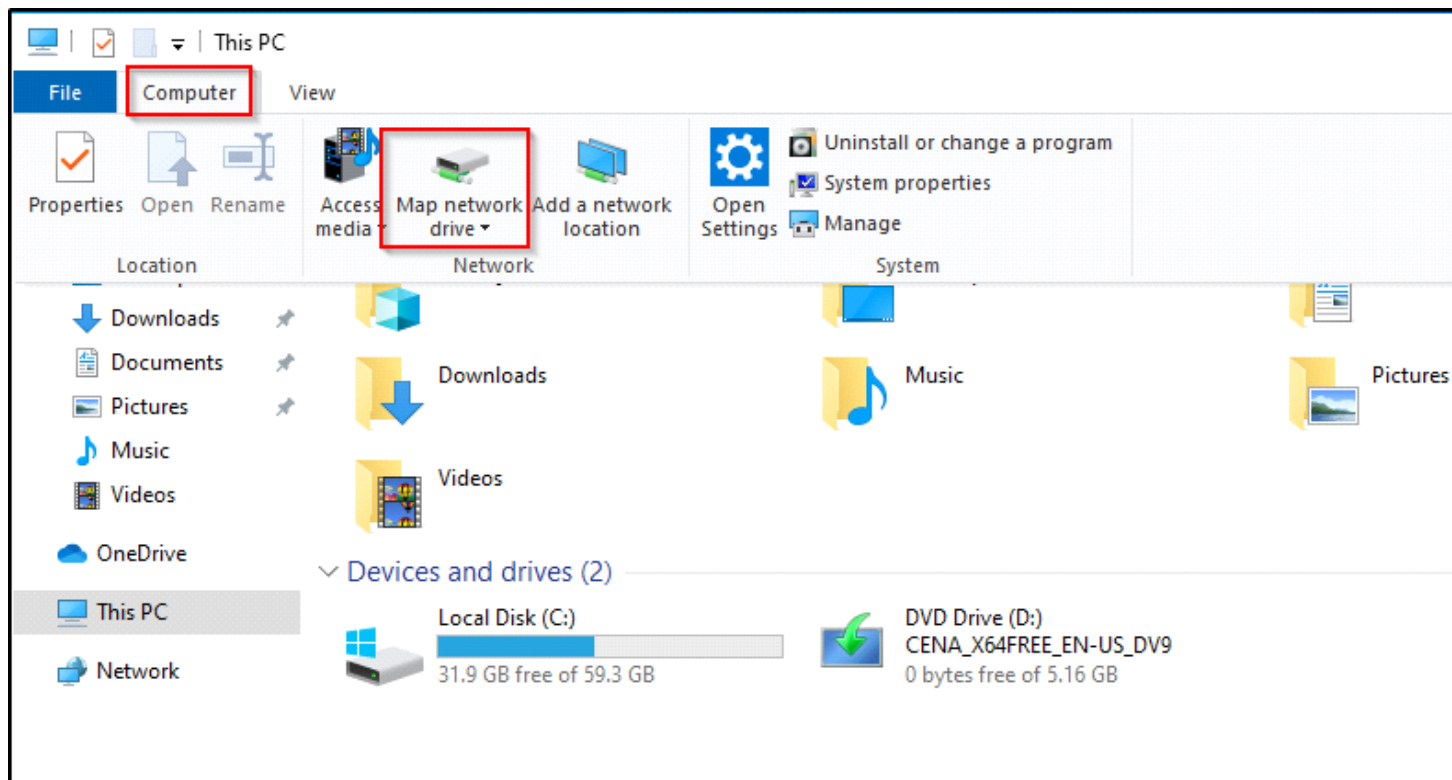
- You are using a domain user account that is recognized across the entire network.
- Necessary for accessing domain resources and for centrally managed user accounts and policies.

Step 18: Now that we know the differences between logging in locally and with domain, let's login locally at Win(1), this way:

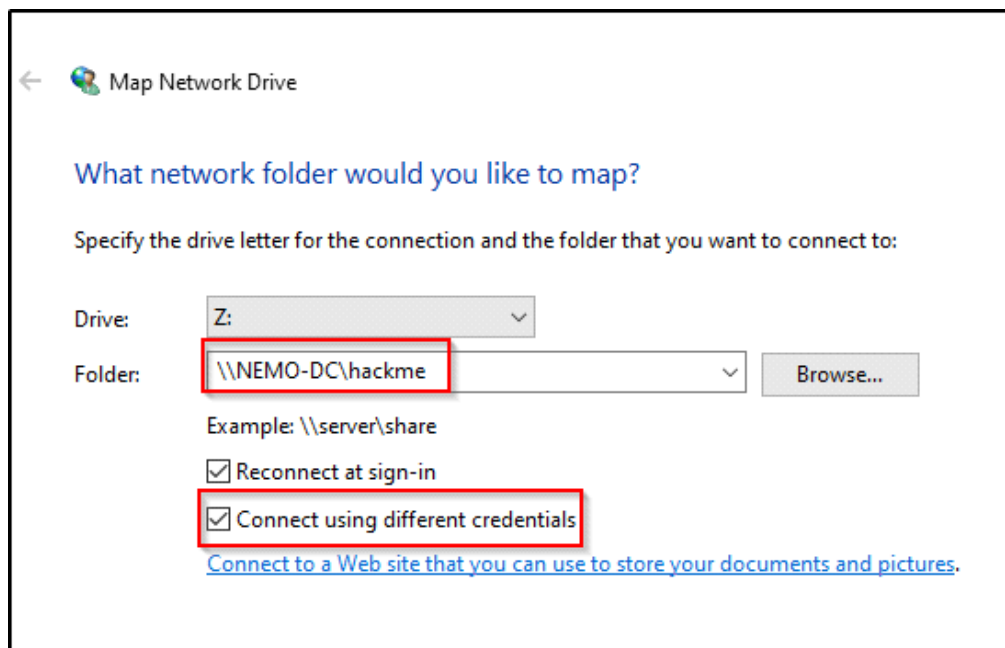


So we're using .\Win(1) and the password that we created when we created this machine: Password123@

Step 19: We're doing this because this will lead to an attack later, go to This PC > Computer > Map network drive:



Step 20: And now here, pick whatever drive you want, check "Connect using different credentials" and specify this path:



Remember we're doing this only on Win(1) not (0)

After it's finished, we should have that as a share drive on our machine:

Devices and drives (2)

Local Disk (C:) 32.0 GB free of 59.3 GB

DVD Drive (D:) CENA\_X64FREE\_EN-US\_DV9 0 bytes free of 5.16 GB

Network locations (1)

hackme (\\NEMO-DC) (Z:) 66.6 GB free of 79.3 GB