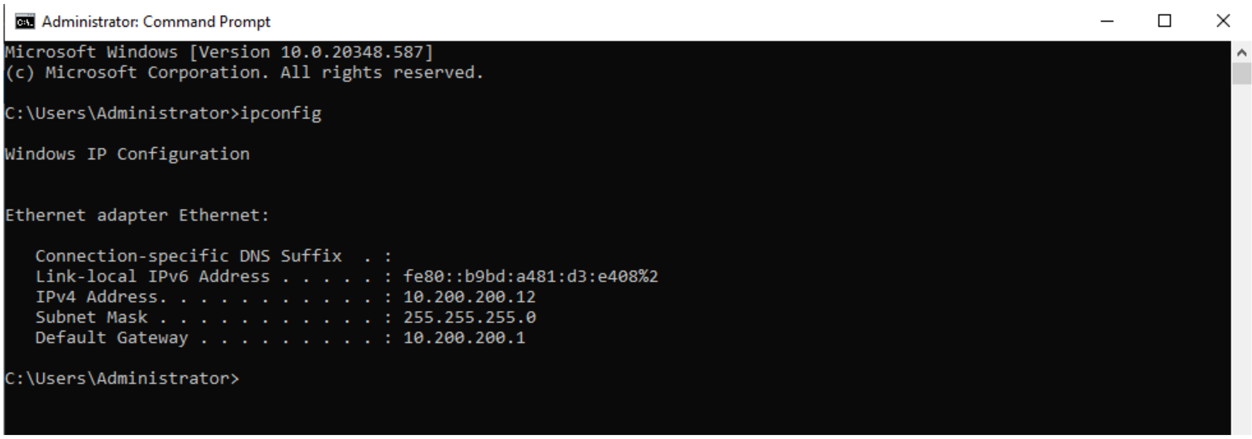
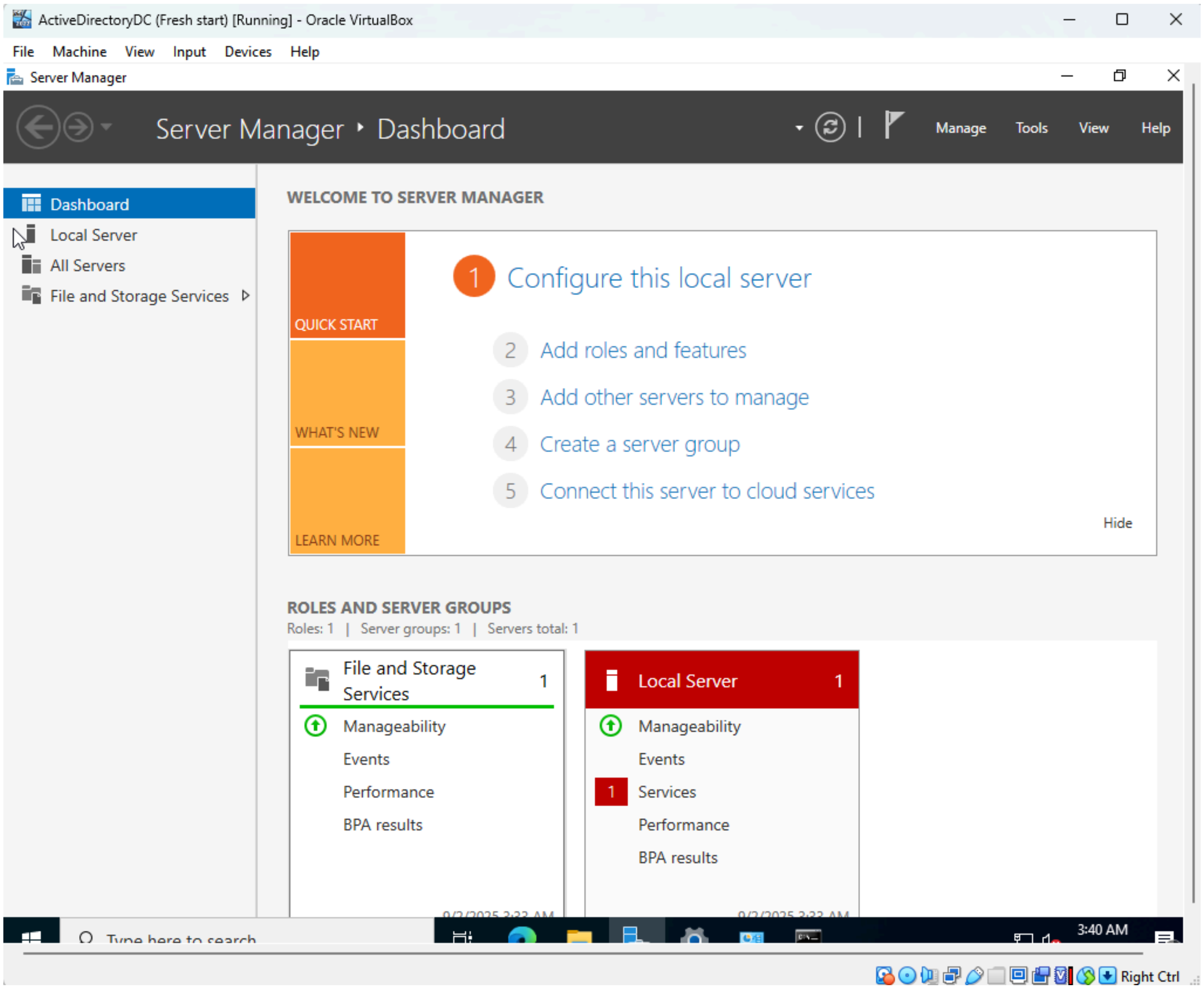
Active Directory Configuration

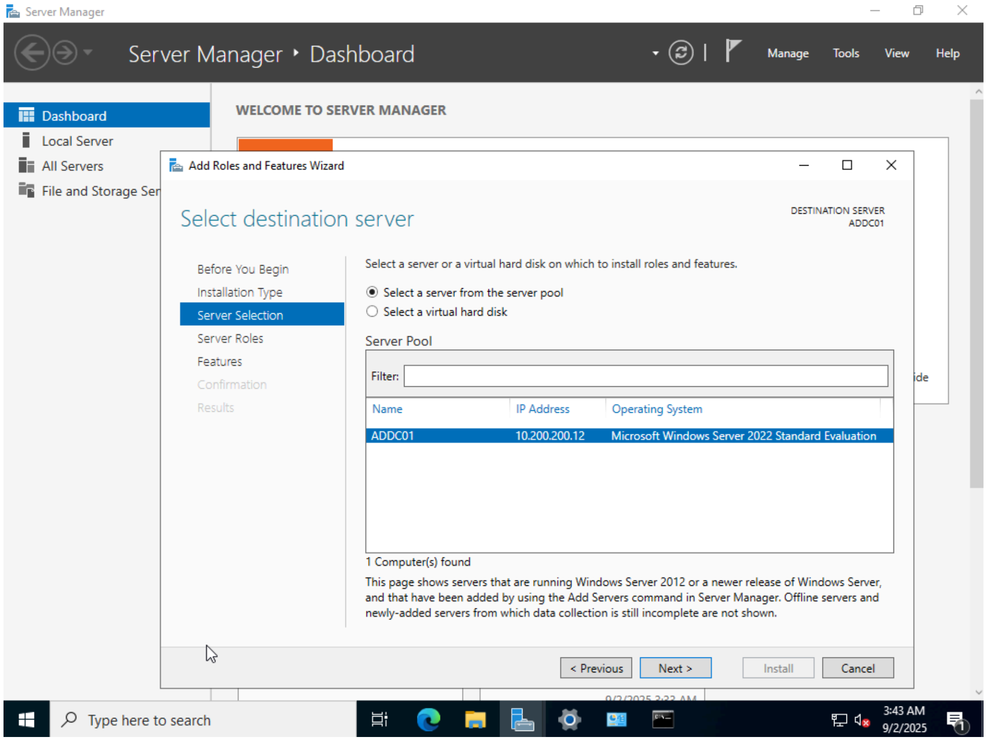
- Similar to the Splunk server configuration, we will first make sure our static IP is set to the address noted in my lab topology diagram.



```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b9bd:a481:d3:e408%2
   IPv4 Address. . . . . . . . . . . : 10.200.200.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.200.1

C:\Users\Administrator>
```


ActiveDirectoryDC (Fresh start) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
Type here to search
3:40 AM
Right Ctrl

- Inside of the windows server manager we will begin setting up our active directory
- On the top right of the page click on manage → Add Roles & Features
- Make sure installation type → Role-based installation is checked
- Server selection will show the available servers



Select destination server

DESTINATION SERVER
ADDC01

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

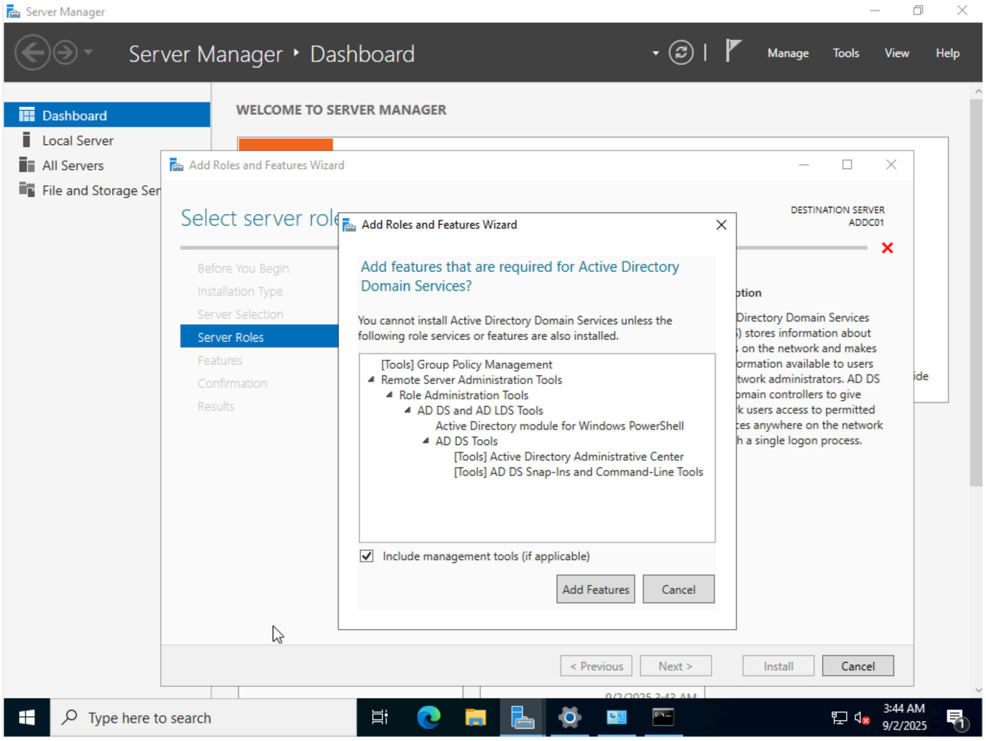
Filter:

Name	IP Address	Operating System
ADDC01	10.200.200.12	Microsoft Windows Server 2022 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

- In my lab I just have one
- In server roles we want to make sure Active Directory Domain Services is selected to add those features



Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

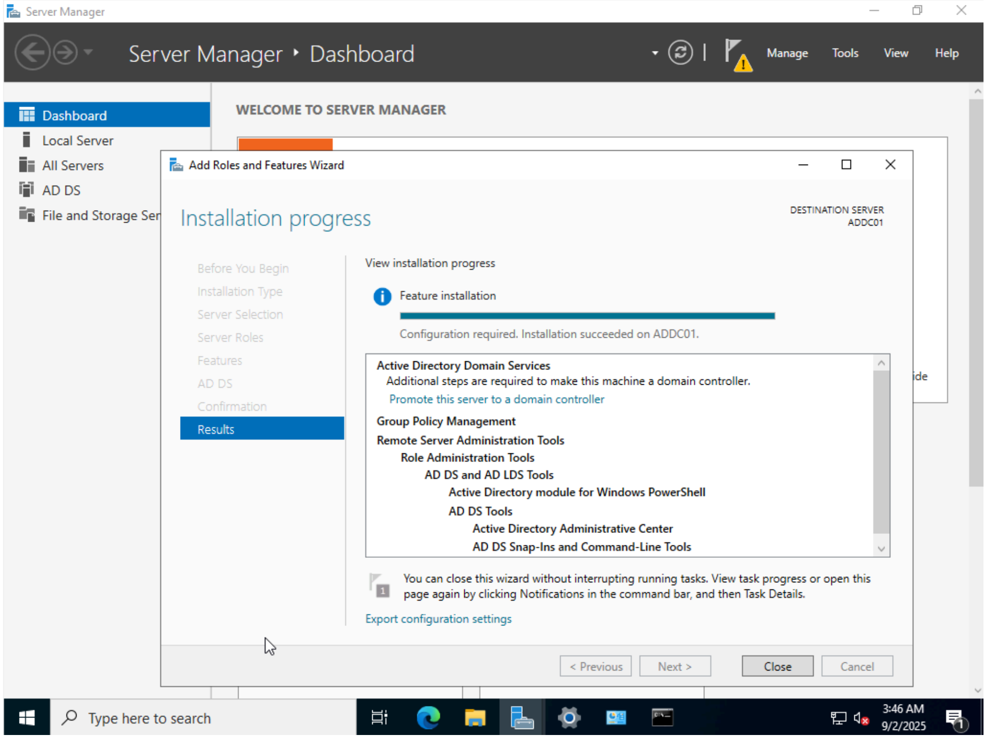
You cannot install Active Directory Domain Services unless the following role services or features are also installed.

```
[Tools] 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
              [Tools] Active Directory Administrative Center
              [Tools] AD DS Snap-Ins and Command-Line Tools
```

☑ Include management tools (if applicable)

Add Features   Cancel

- Then we can keep clicking next until the install button appears, which we will click



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
ADDC01

View installation progress

Feature installation

Configuration required. Installation succeeded on ADDC01.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

```
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
```

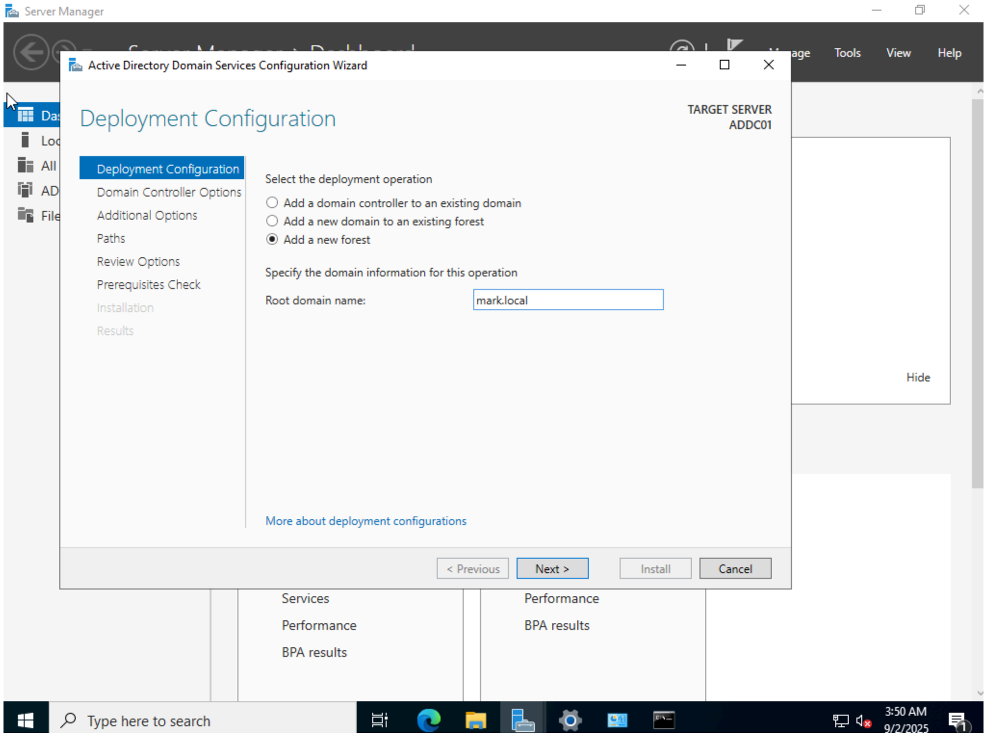
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

- Once finished we will click the flag at the top of the server manager dash board
- Then promote the server to a domain controller

Next steps include

- Add a new forest - since we are creating a brand new domain
- We will set the root domain name as mark.local
- The domain name cannot just be “mark” it must have a root “local”



Deployment Configuration

TARGET SERVER
ADDC01

Select the deployment operation

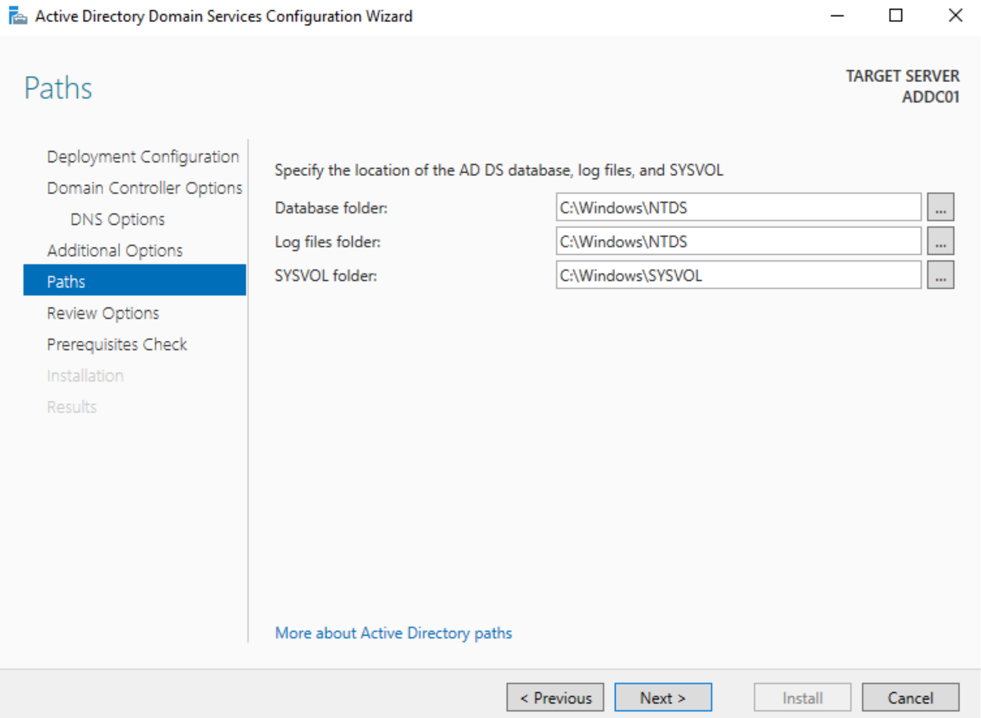
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: mark.local

More about deployment configurations

- We will then go through the rest of the domain service configurations



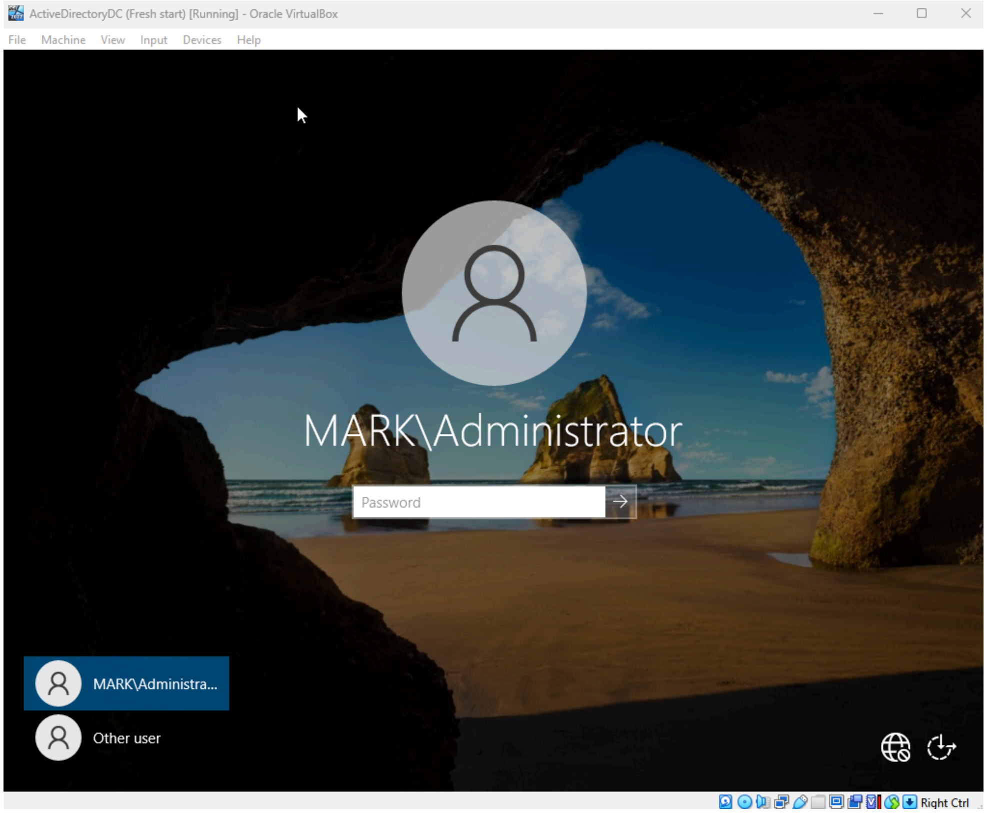
Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

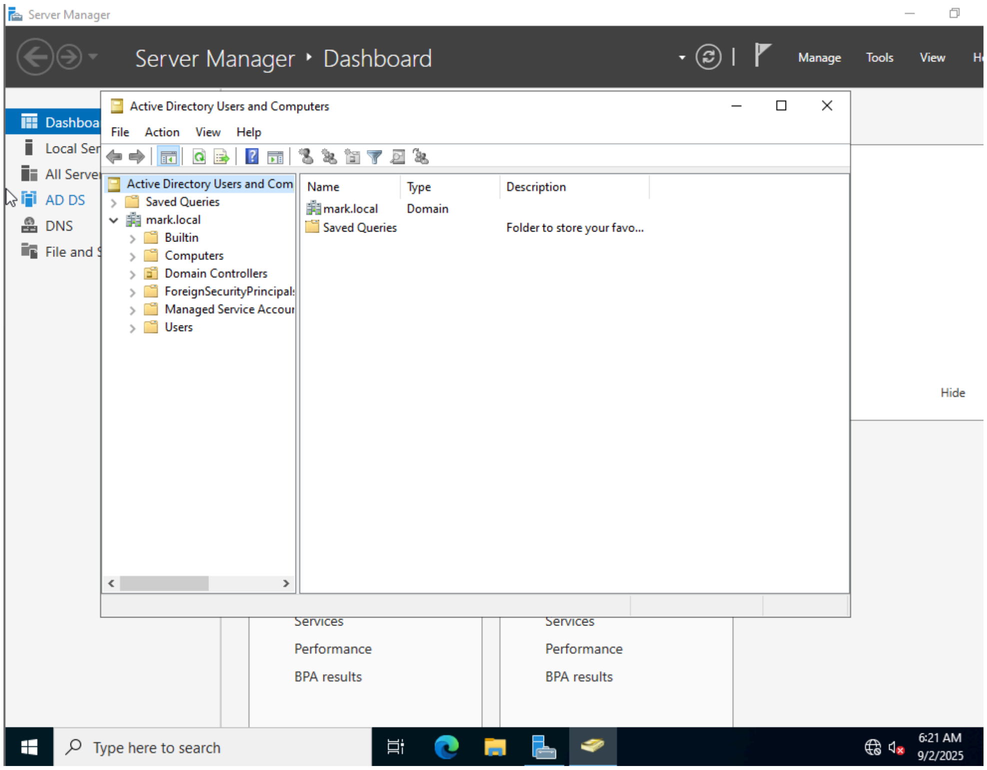
Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

- These are the paths use to store our database files
- Attackers love to target Domain controllers, not only because it has access to everything but because it contains everything related to AD including password hashes
- Any unauthorized activity towards these files can most likely be a domain compromise

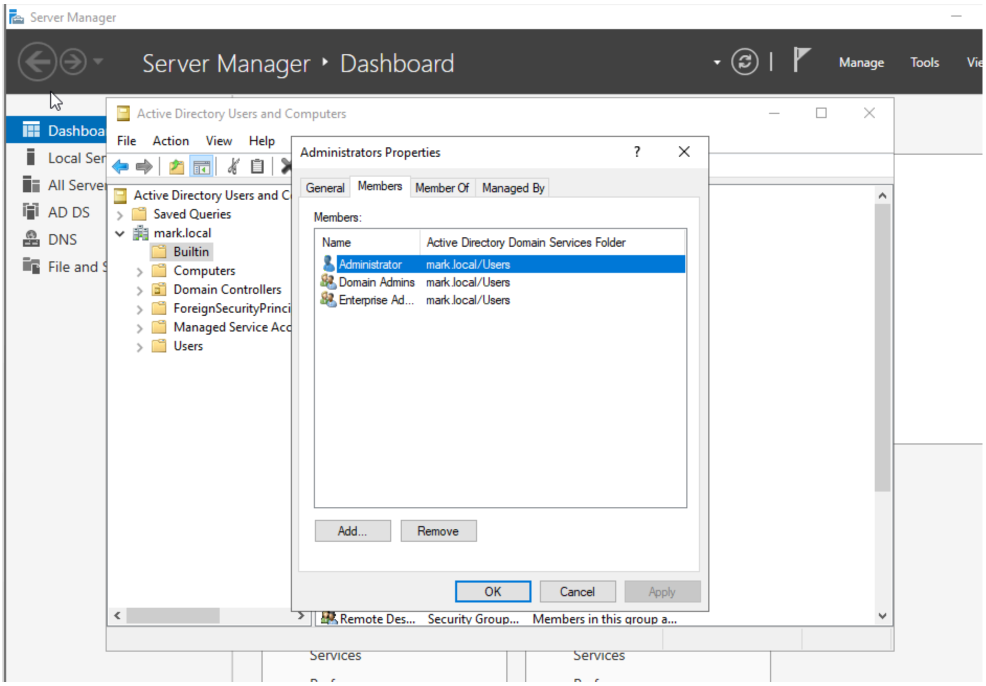


- Once configuration processes is finished the domain should be followed by a backslash which indicates that we have successfully install Active Directory Domain System and promoted our server to a Domain controller
- We can then create some users
- Go into Server Manager → Tools → Active Directory Users and Computers
- This is where we can create objects such as users, computers, groups etc.



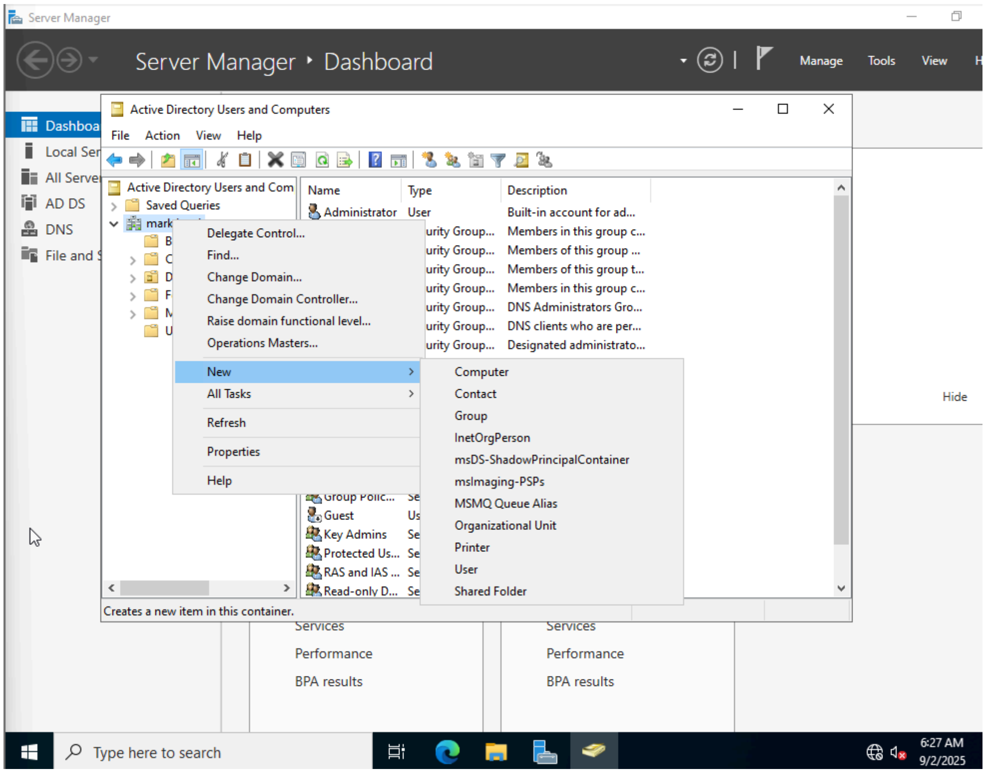
Name	Type	Description
mark.local	Domain	
Saved Queries		Folder to store your favo...

- The groups on the side (Builtin, computers....) have been created automatically by active directory



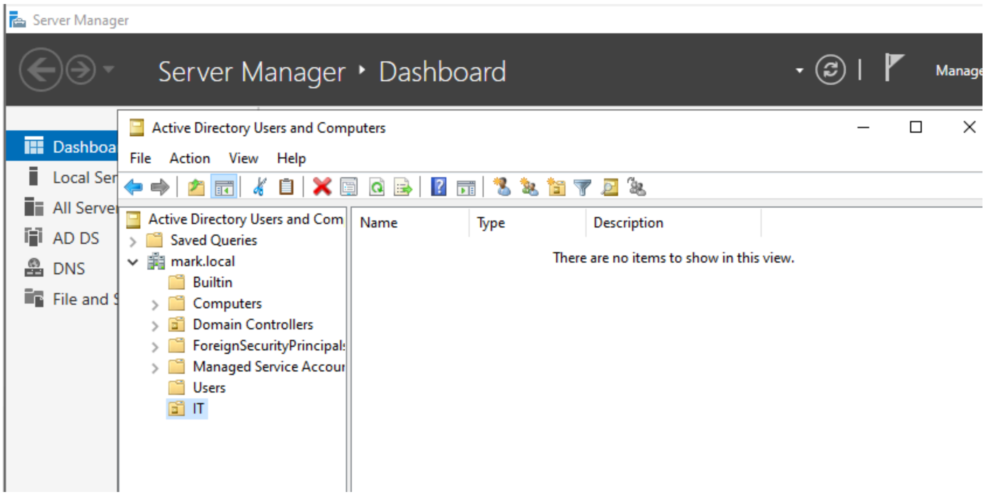
Name	Active Directory Domain Services Folder
Administrator	mark.local/Users
Domain Admins	mark.local/Users
Enterprise Ad...	mark.local/Users

- We can look through these folders to see which users have certain permissions along with descriptions of the policies
    - General - shows group name, description, email, notes
    - Members - shows who is assigned to the group
    - Member Of - we can see what other group this group is in
    - You cant add additional goups within a built in group but you can create a custom group and add that built in group to it
        - (new group → member OF → add... → any group you want)



Creates a new item in this container.

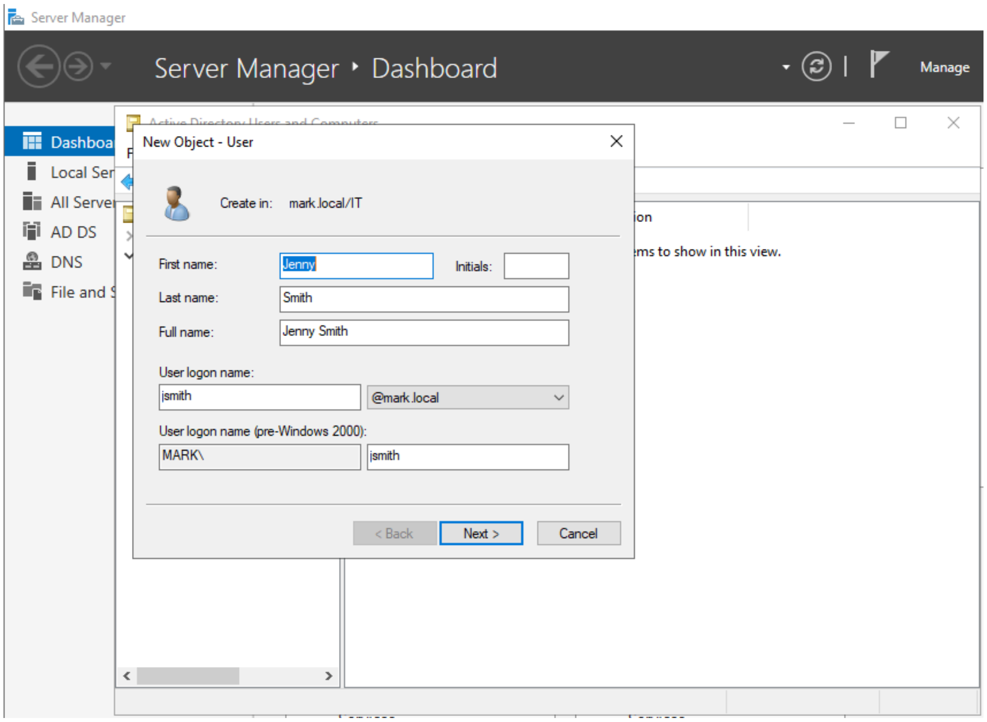
In organizations they will set up specific users in different departments such as finance, IT, HR, etc., to do this we can right click the domain and click organizational unit



There are no items to show in this view.

So now you can see I have created an organizational unit for IT

- Inside of it I can right click → new user, to start creating users



Create in: mark.local/IT

First name: Jenny

Initials:

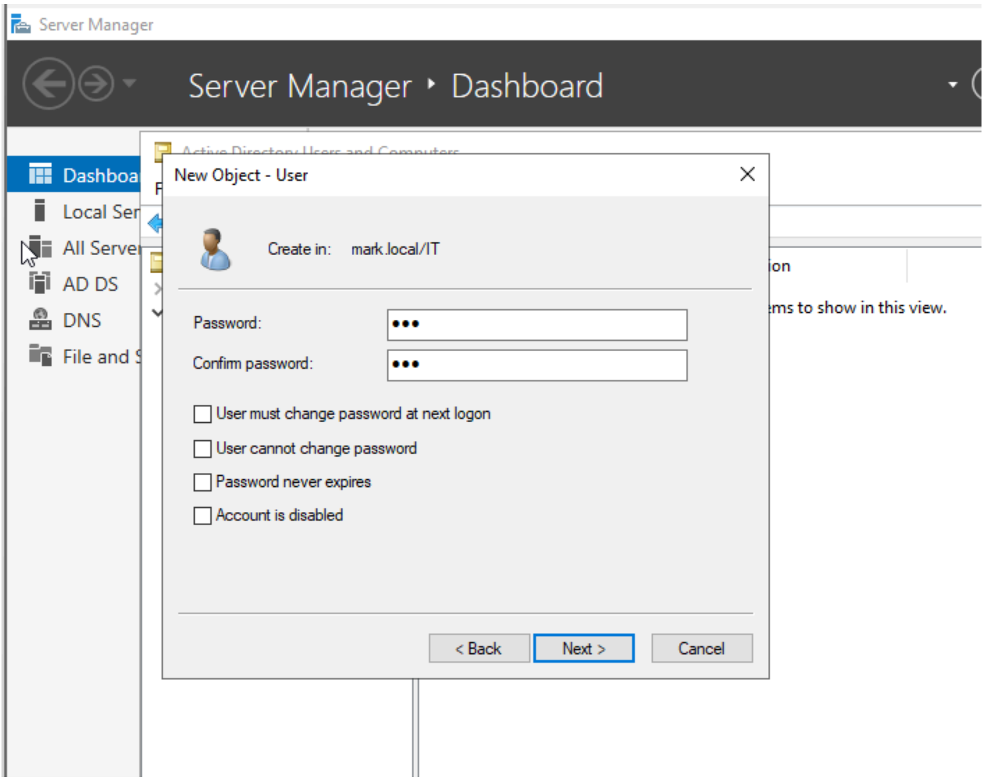
Last name: Smith

Full name: Jenny Smith

User logon name: jsmith @mark.local

User logon name (pre-Windows 2000): MARK\ jsmith

- Then we can work on a users information, simulating the organizations directory process



New Object - User

Create in: mark.local/IT

Password: •••

Confirm password: •••

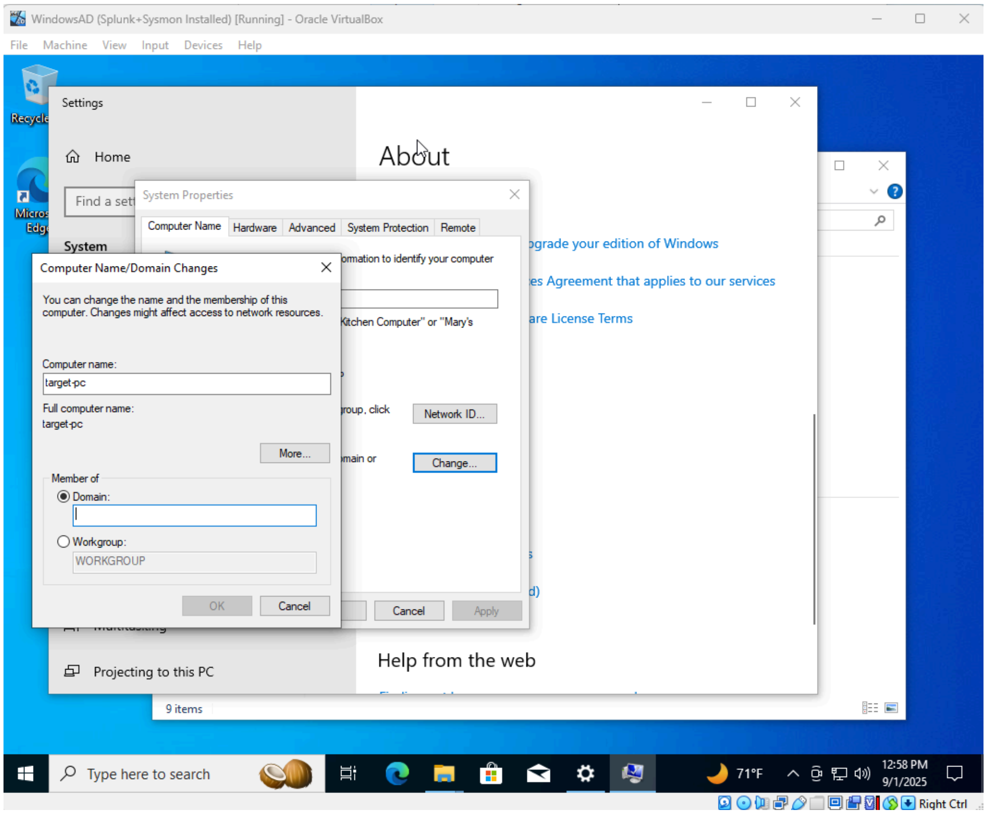
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

- Usually “user must change password at next login” is required but we will uncheck this for my lab
- Now that we have Splunk and active directory installed we can go to our windows (target) machine and join it to our new domain.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
target-pc

Full computer name:
target-pc

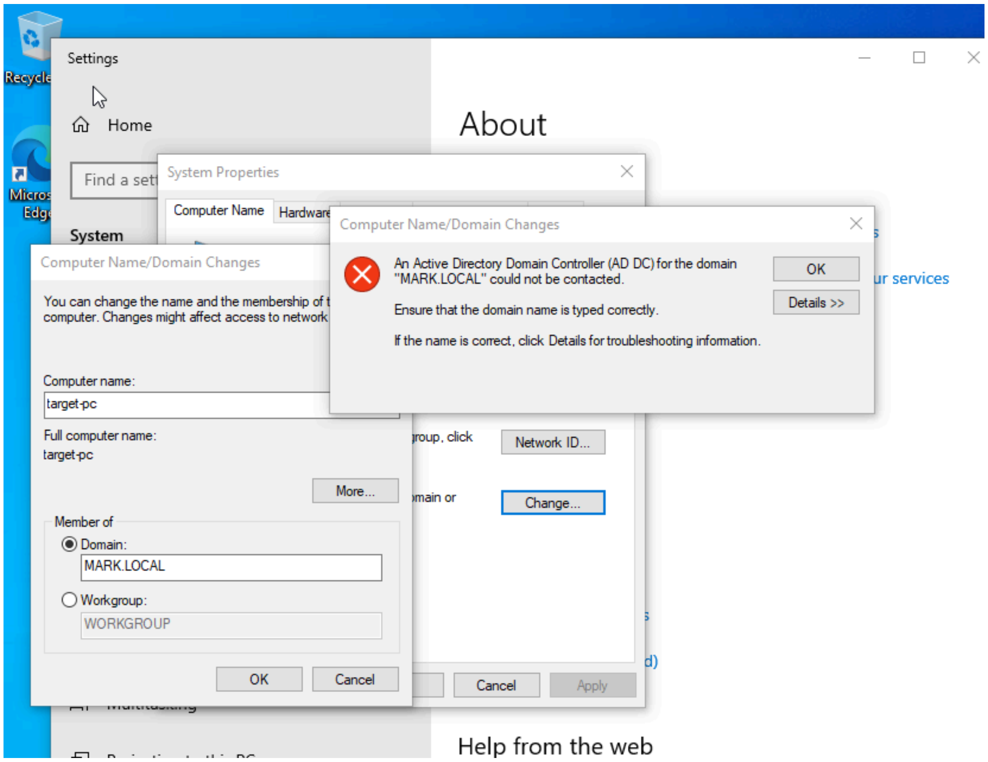
More...

Member of

● Domain:

○ Workgroup:
WORKGROUP

OK Cancel



Computer Name/Domain Changes

An Active Directory Domain Controller (AD DC) for the domain "MARK.LOCAL" could not be contacted.

Ensure that the domain name is typed correctly.

If the name is correct, click Details for troubleshooting information.

OK
Details >>

Computer Name/Domain Changes

You can change the name and the membership of t computer. Changes might affect access to network

Computer name:
target-pc

Full computer name:
target-pc

More...

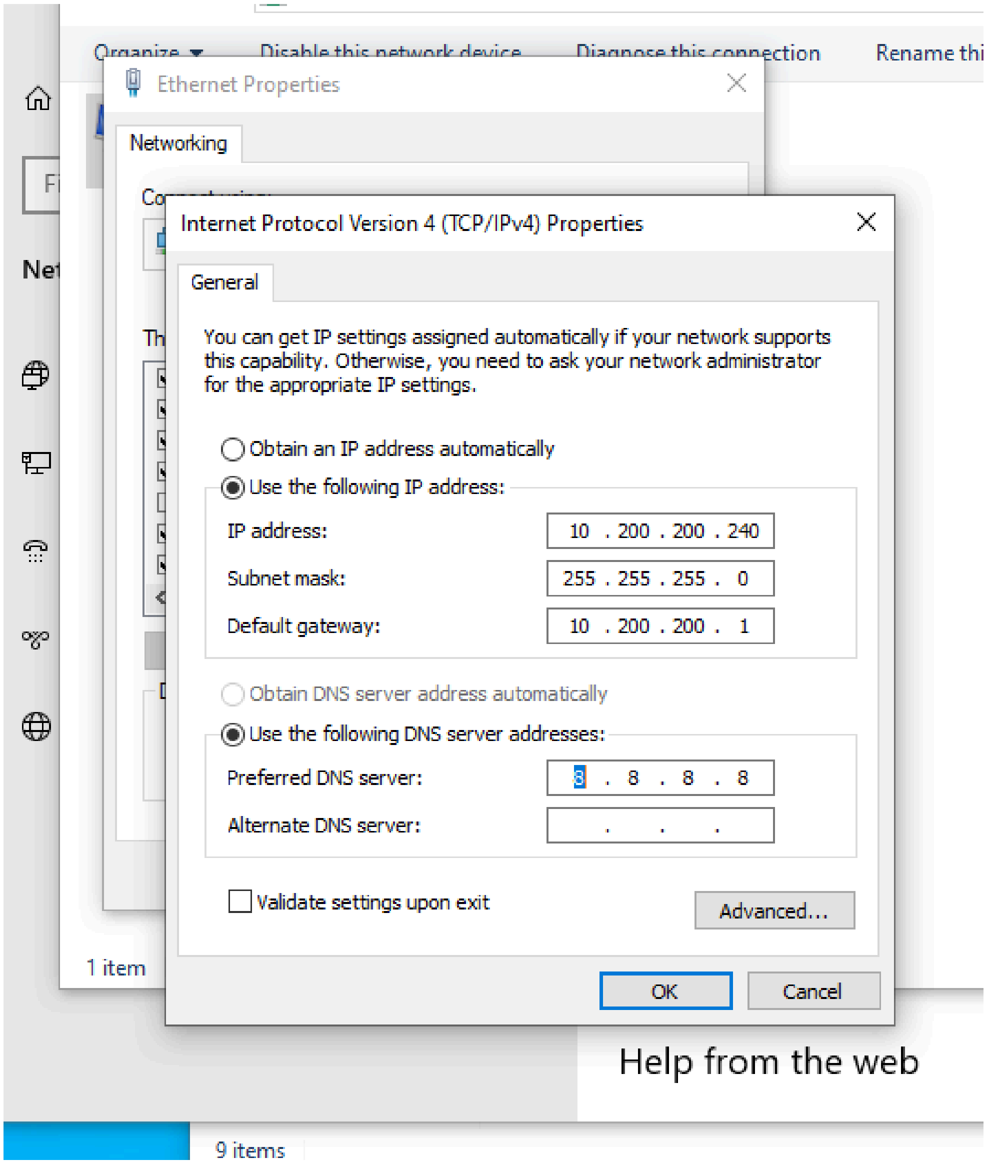
Member of

● Domain:
MARK.LOCAL

○ Workgroup:
WORKGROUP

OK Cancel

- If you type in the regular domain it wont recognize it, which goes back to how DNS works
- To fix it we must change the adapter, go to the network icon (bottom right) and right click → open network & intent settings → change adapter options → right click adapter → properties → click internet protocol version 4 → properties
- Change the DNS from the google DNS (8.8.8.8) which I added earlier to the domain controller ip.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	10 . 200 . 200 . 240
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 200 . 200 . 1

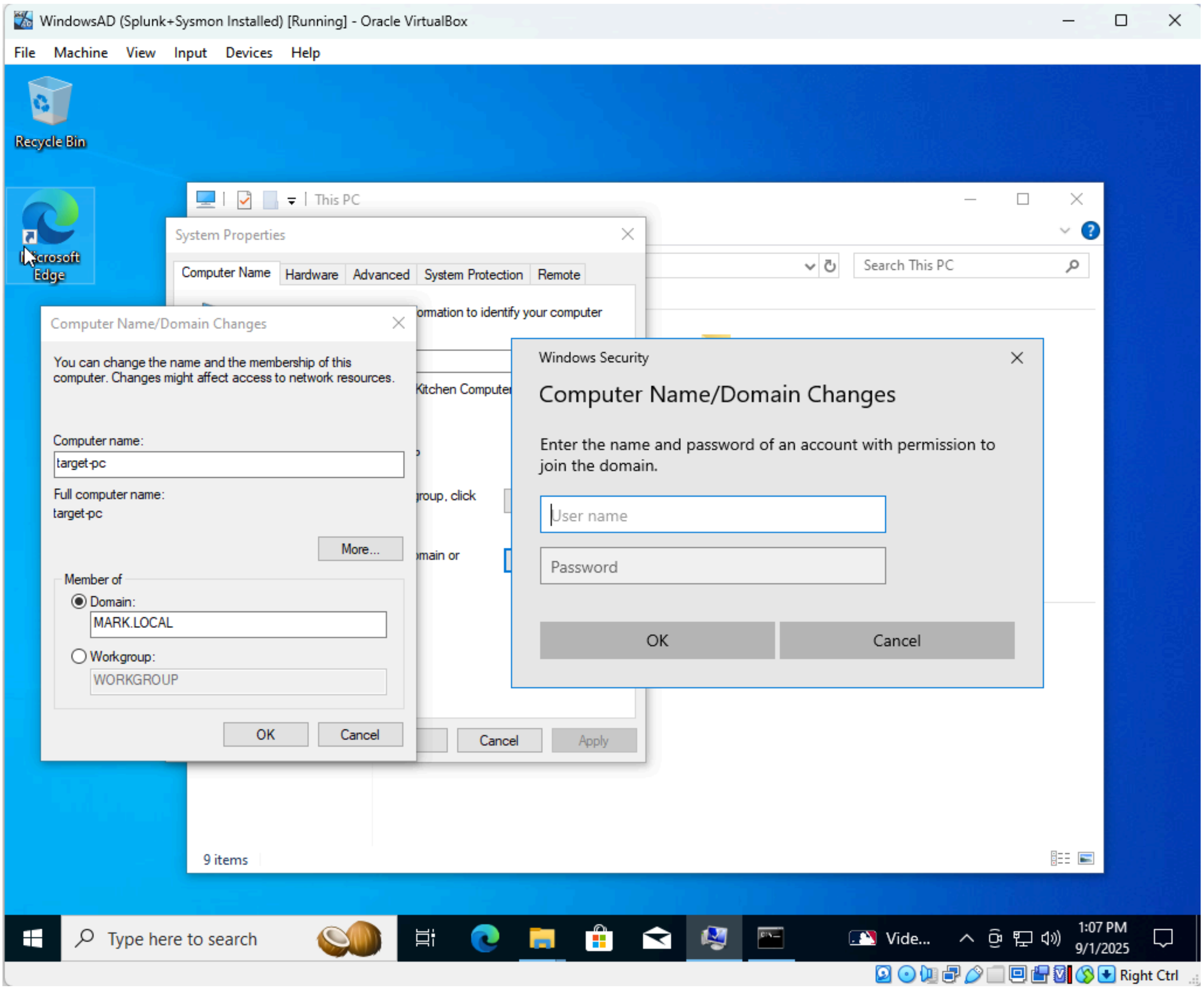
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

□ Validate settings upon exit

Advanced...

OK Cancel



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: target-pc

Full computer name: target-pc

More...

Member of

● Domain: MARK.LOCAL

○ Workgroup: WORKGROUP

OK Cancel

Windows Security

Computer Name/Domain Changes

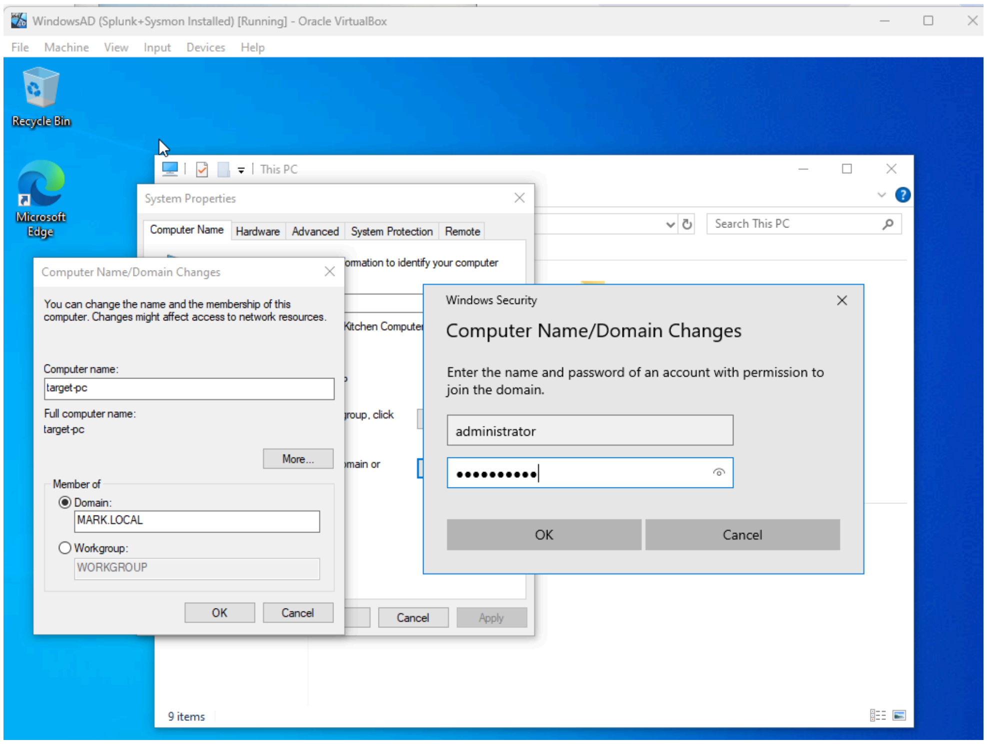
Enter the name and password of an account with permission to join the domain.

User name

Password

OK Cancel

- After changing the DNS server we are prompted with credentials instead of the previous error message



WindowsAD (Splunk+Sysmon Installed) [Running] - Oracle VirtualBox

System Properties

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: target-pc

Full computer name: target-pc

Member of

● Domain: MARK.LOCAL

○ Workgroup: WORKGROUP

Windows Security

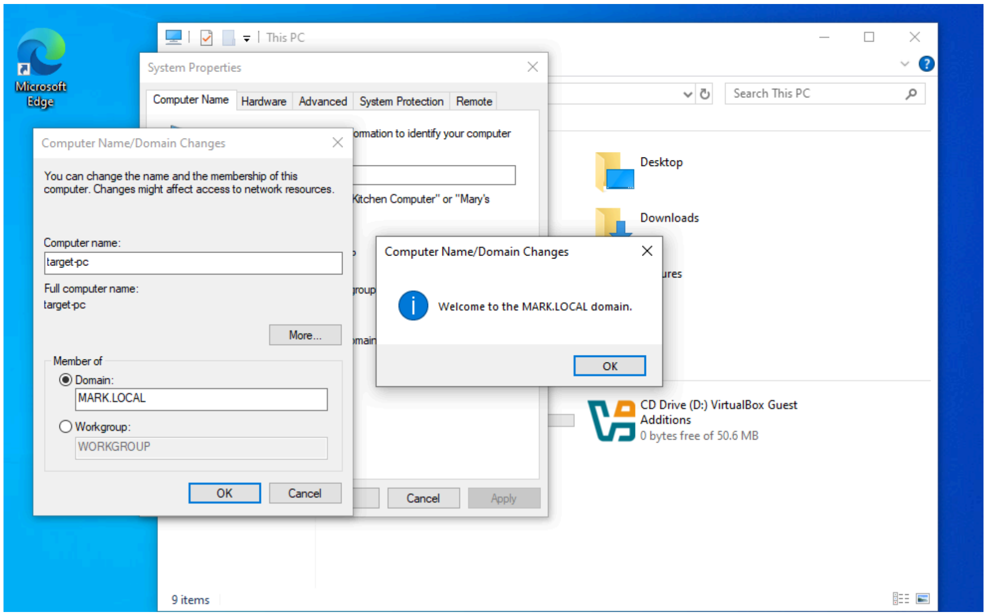
Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

administrator

••••••••••

- Use the account of the server to log in because it will have the proper permissions



System Properties

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: target-pc

Full computer name: target-pc

Member of

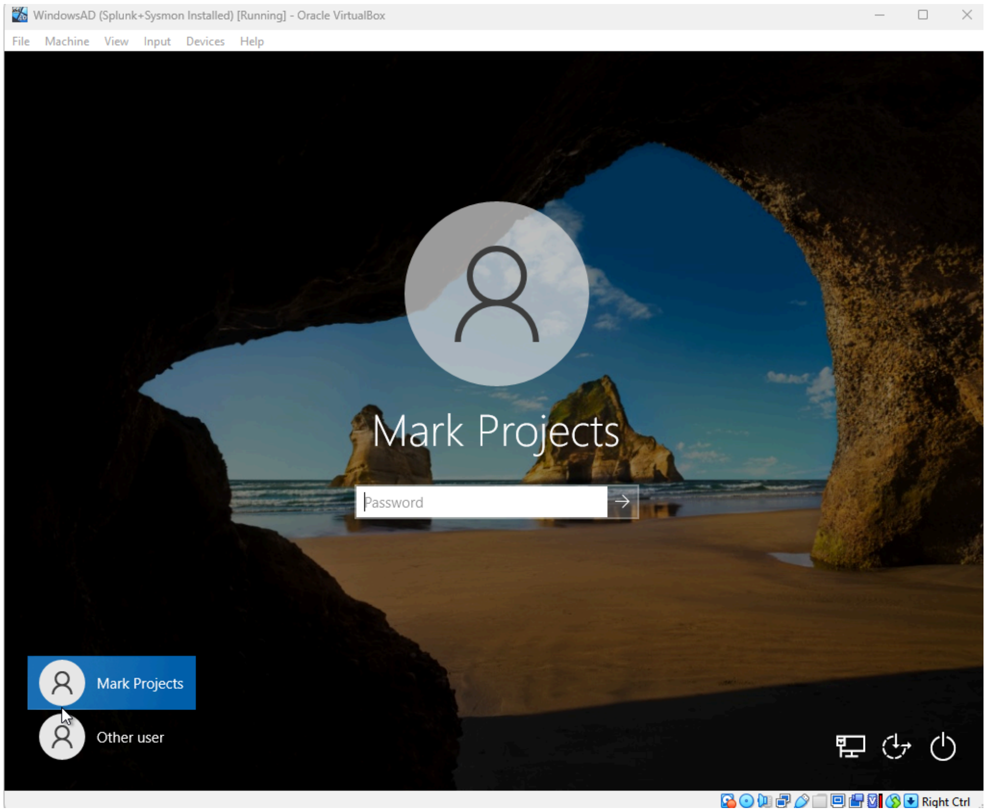
● Domain: MARK.LOCAL

○ Workgroup: WORKGROUP

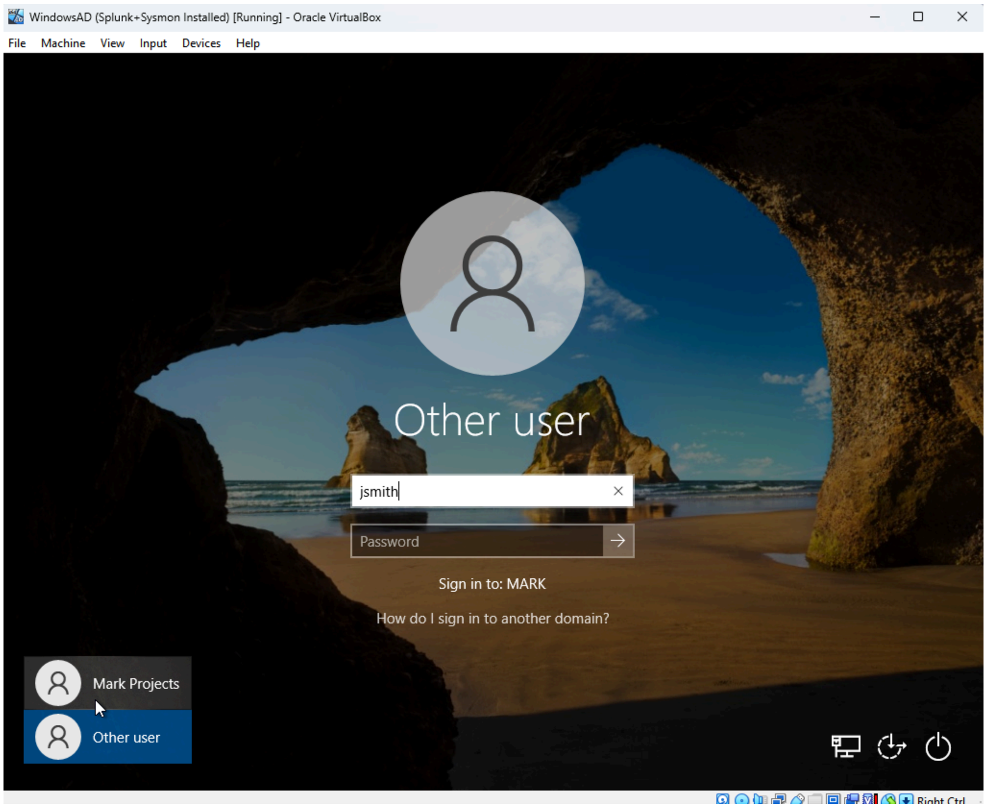
Computer Name/Domain Changes

Welcome to the MARK.LOCAL domain.

- It is now connected and we can log in with our newly created user after a restart



- I created a user named jenny smith in my active directory so I can click other user and log in with her credentials



jsmith

Password

Sign in to: MARK

How do I sign in to another domain?

- It should also be sign in to the ADDS name
- That is how we create a new user, join our computer to a new domain, and log in as a domain user
- I can now use this to adhere to my lab topology creating the necessary users

You may notice that the adminstrator option is gone but you can type (iny mcase)

- Mark\Administrator
- Password

to enter back into the ADDS