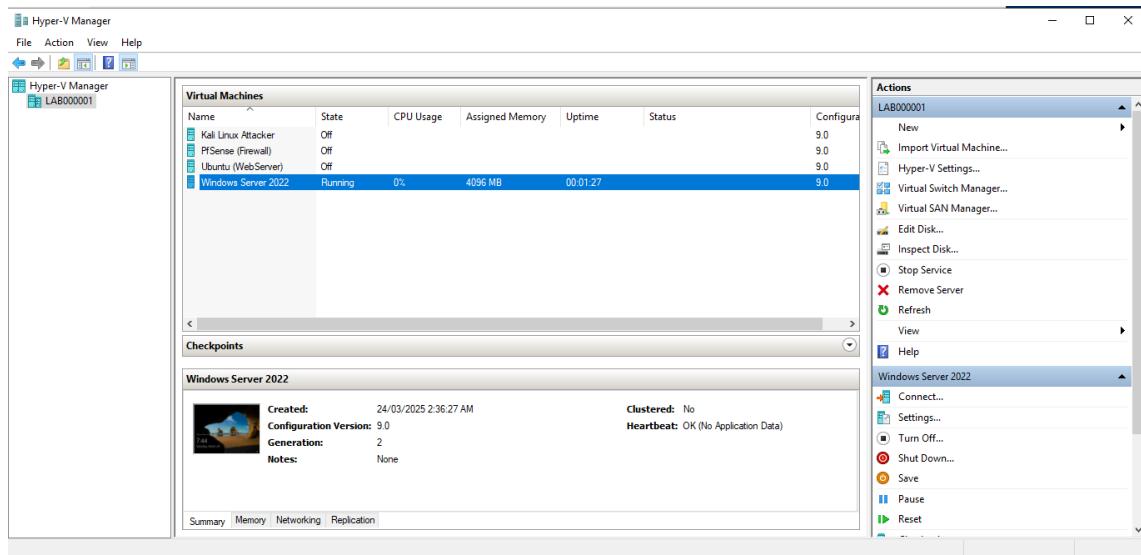


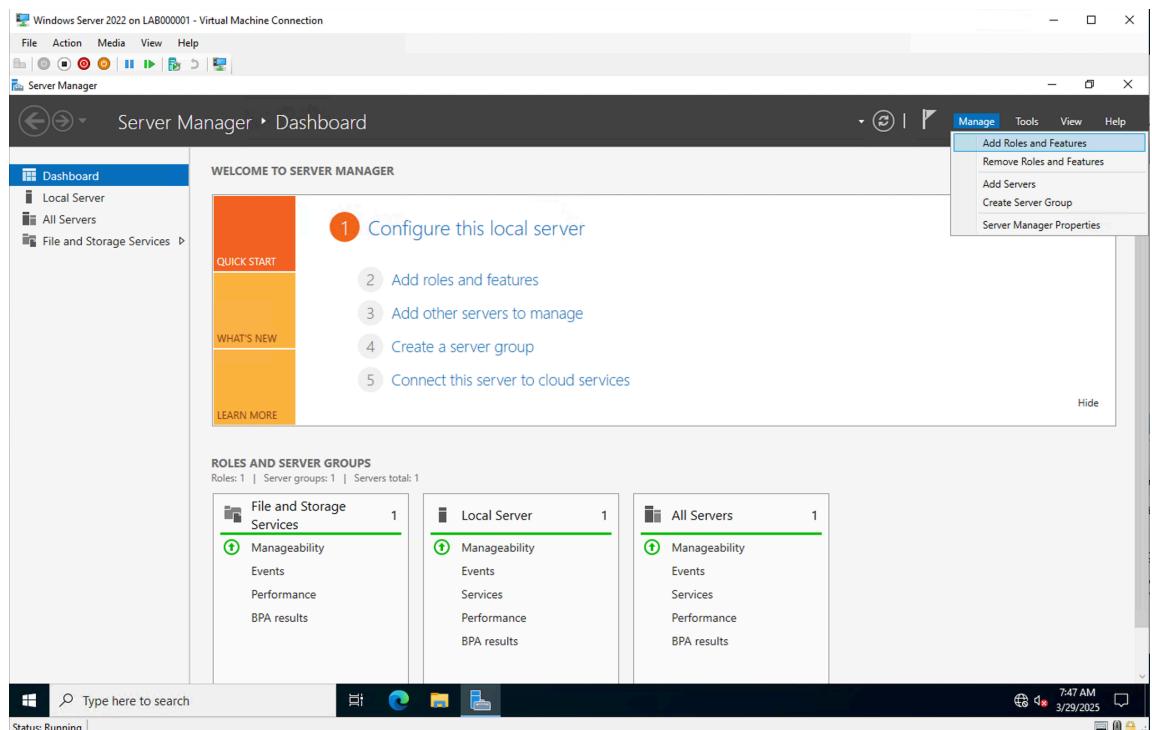
Implementing Basic Configurations in Windows Server 2022 – AD DS, Group Policies and SMB File Sharing

Open Hyper-V and Start the Windows Server 2022 VM by clicking “Connect”

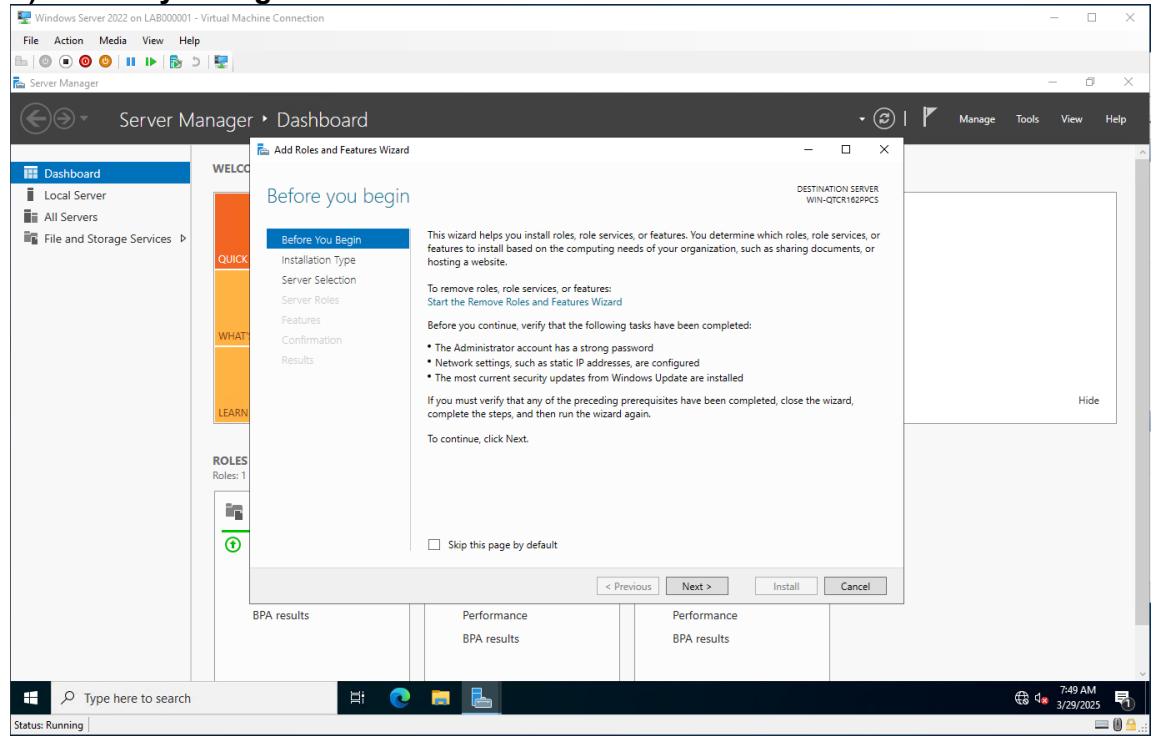


1. Install Active Directory Domain Services (AD DS):

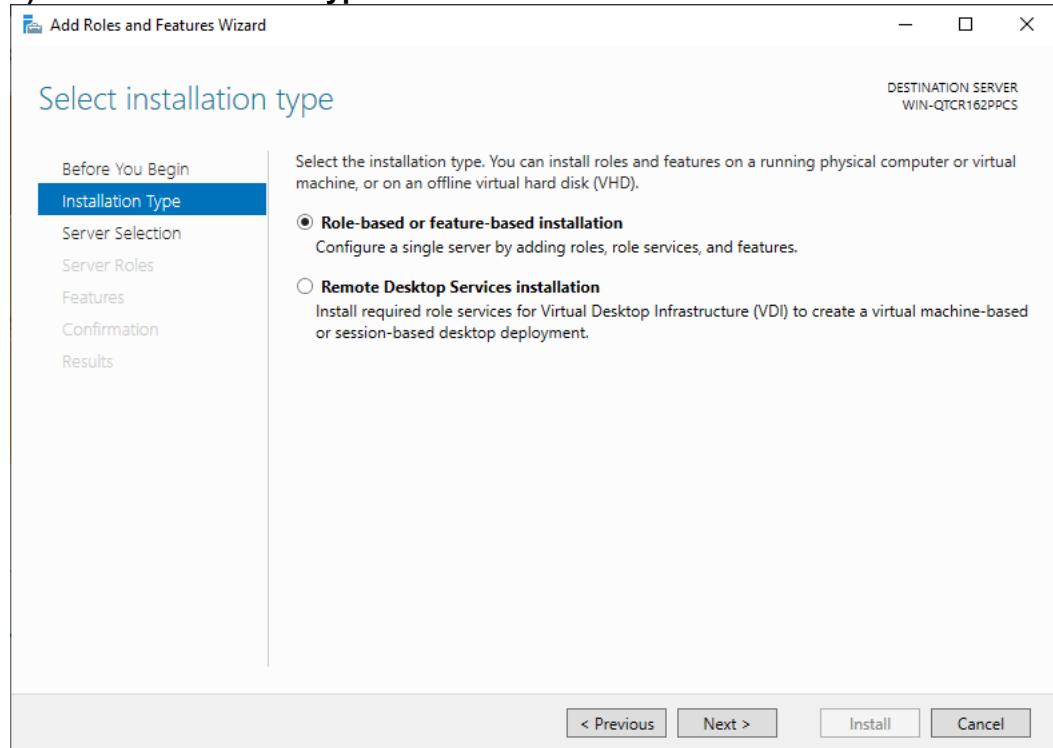
- In Server Manager,
Click **Manage** on top right > **Add Roles and Features** OR
Click on **Add roles and features** in the **Dashboard**



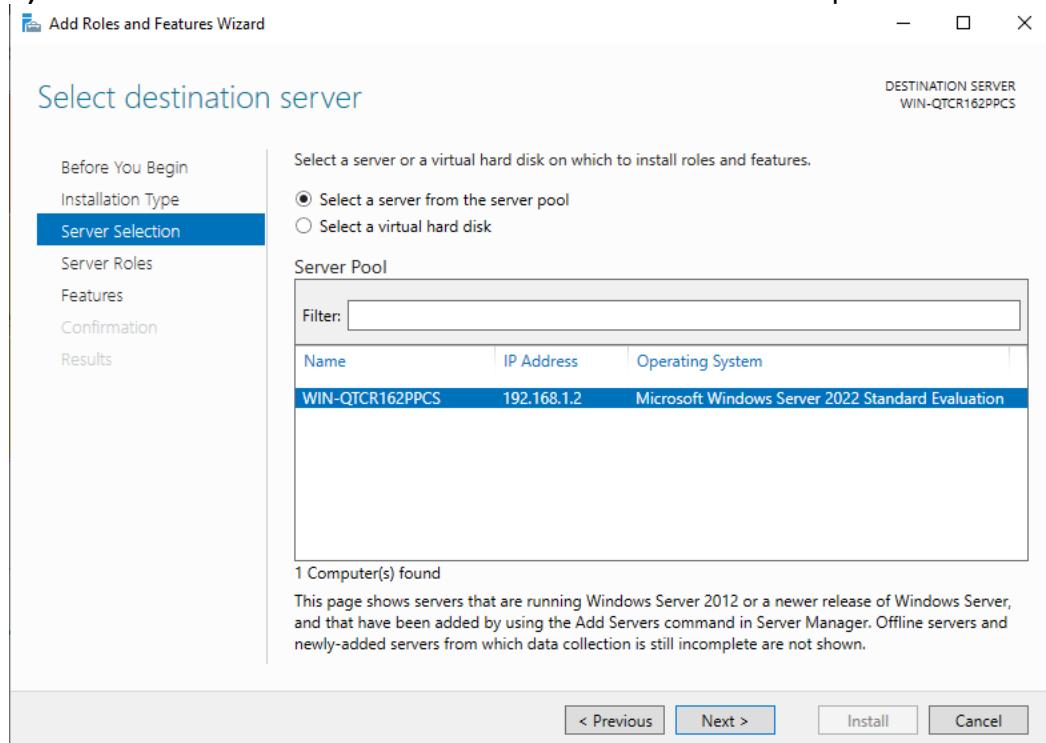
b) Before you begin > Next



c) Select installation type: Role-based or feature-based installation > Next

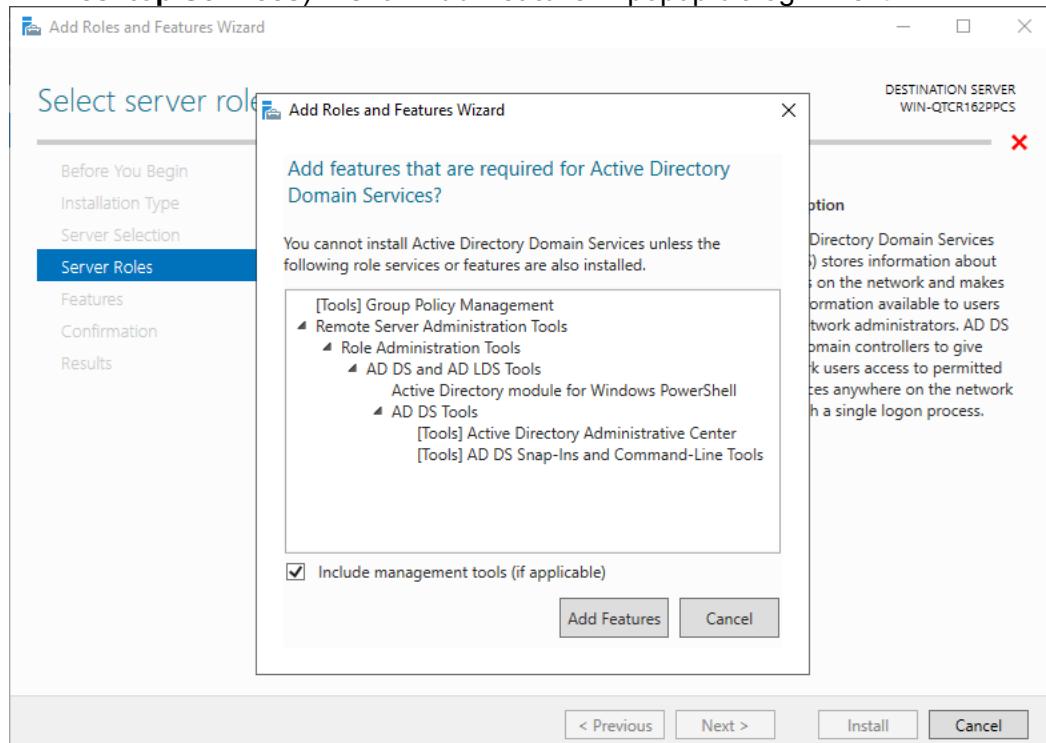


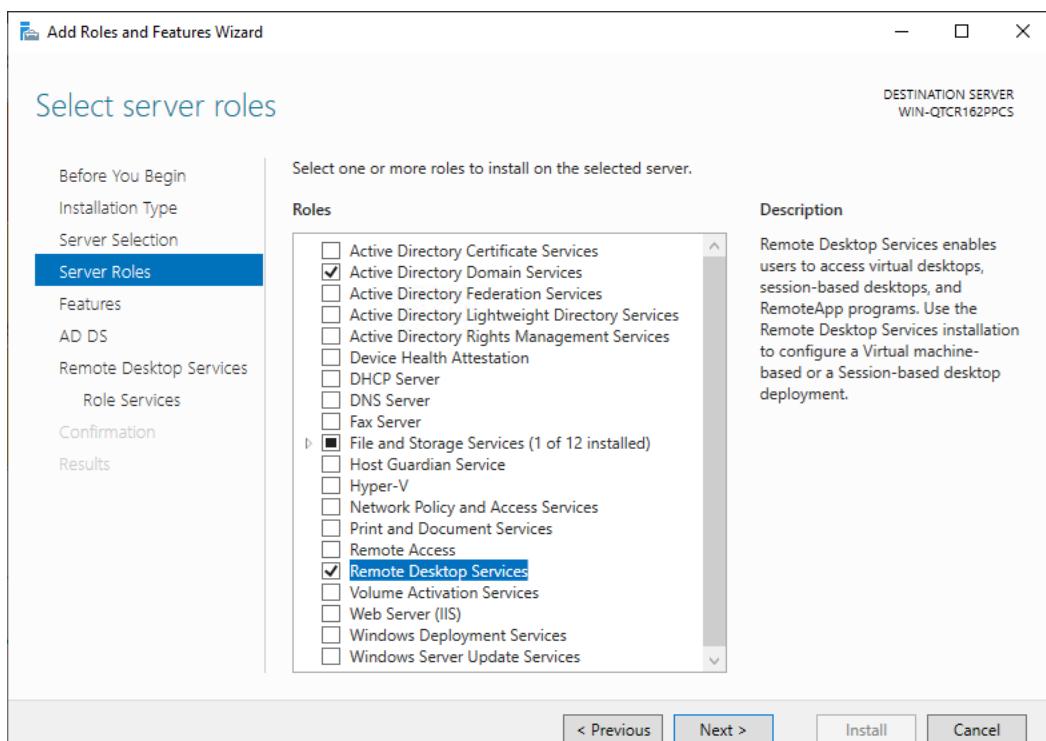
d) **Select destination server:** Select a server from the server pool > Next



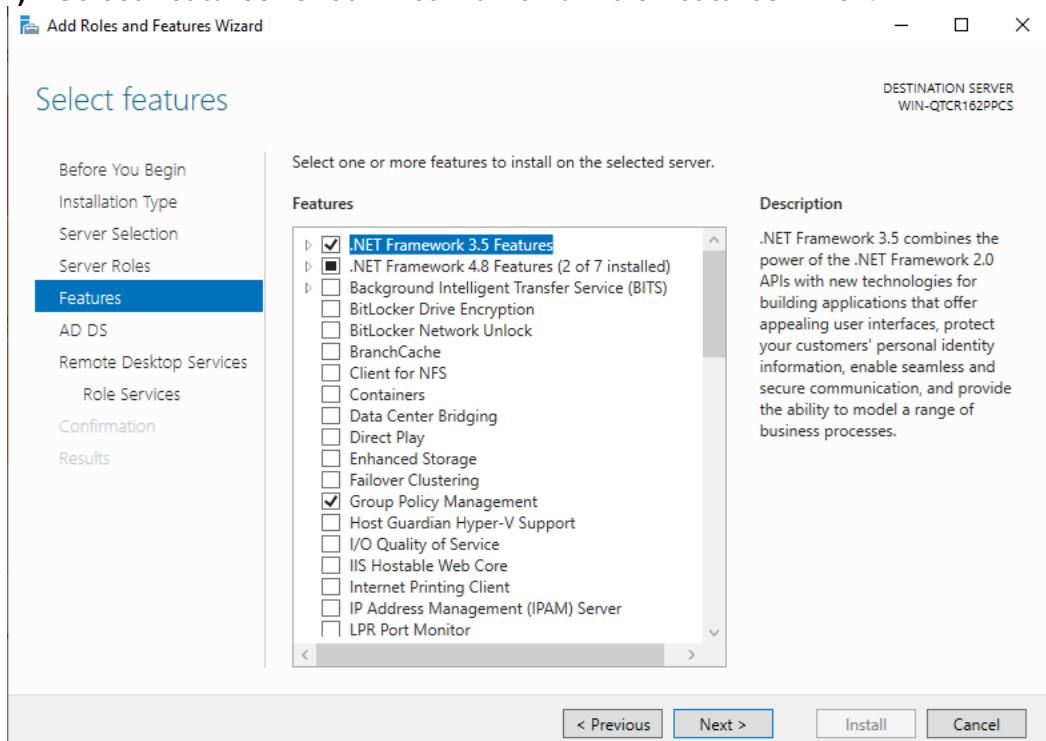
e) **Select server roles:**

Check **Active Directory Domain Services (Optional: Check Remote Desktop Services)** > Click **Add Feature** in popup dialog > Next





f) Select Features: Check .Net Framework 3.5 Features > Next



g) Active Directory Domain Services > Next

Add Roles and Features Wizard

Active Directory Domain Services

DESTINATION SERVER
WIN-QTCR162PPCS

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Remote Desktop Services
Role Services
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous Next > Install Cancel

If you also selected Remote Desktop Services with AD DS,
Remote Desktop Services > Next

Add Roles and Features Wizard

Remote Desktop Services

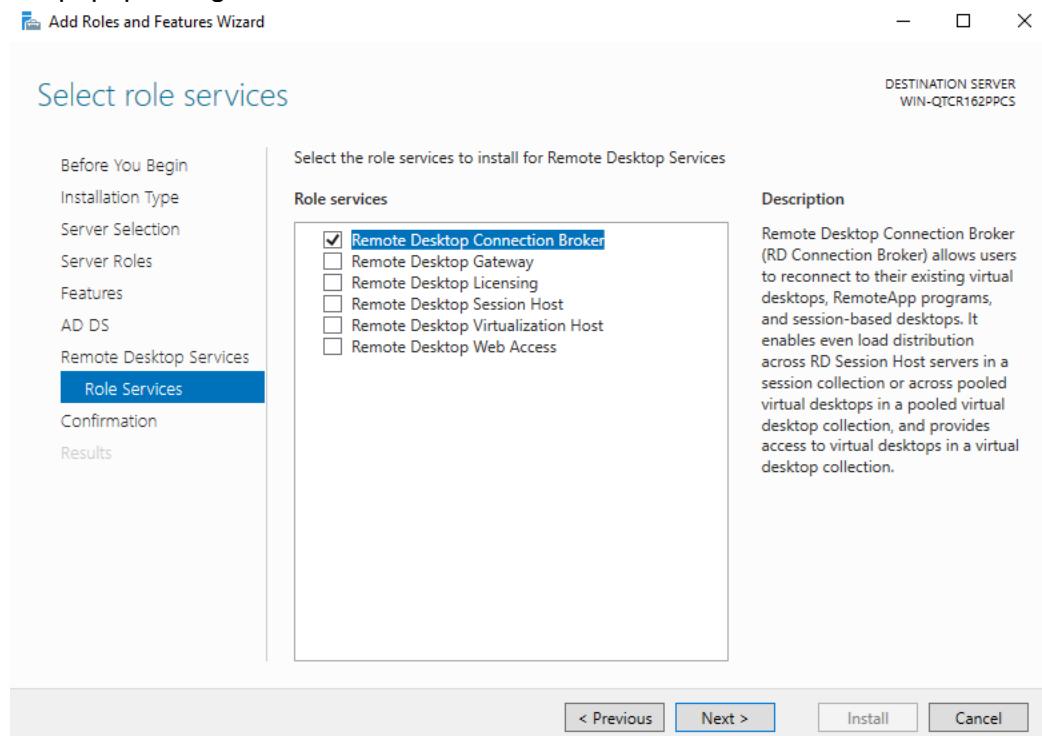
DESTINATION SERVER
WIN-QTCR162PPCS

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Remote Desktop Services
Role Services
Confirmation
Results

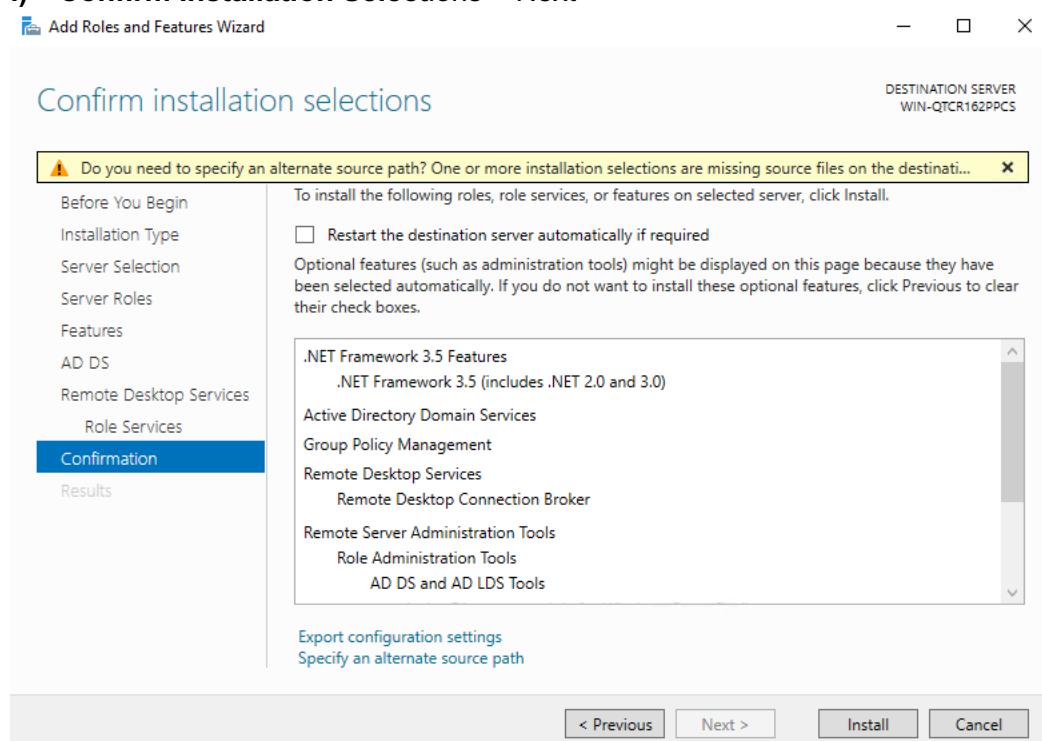
Remote Desktop Services provides technologies that enable users to connect to virtual desktops, RemoteApp programs, and session-based desktops. With Remote Desktop Services, users can access remote connections from within a corporate network or from the Internet.

< Previous Next > Install Cancel

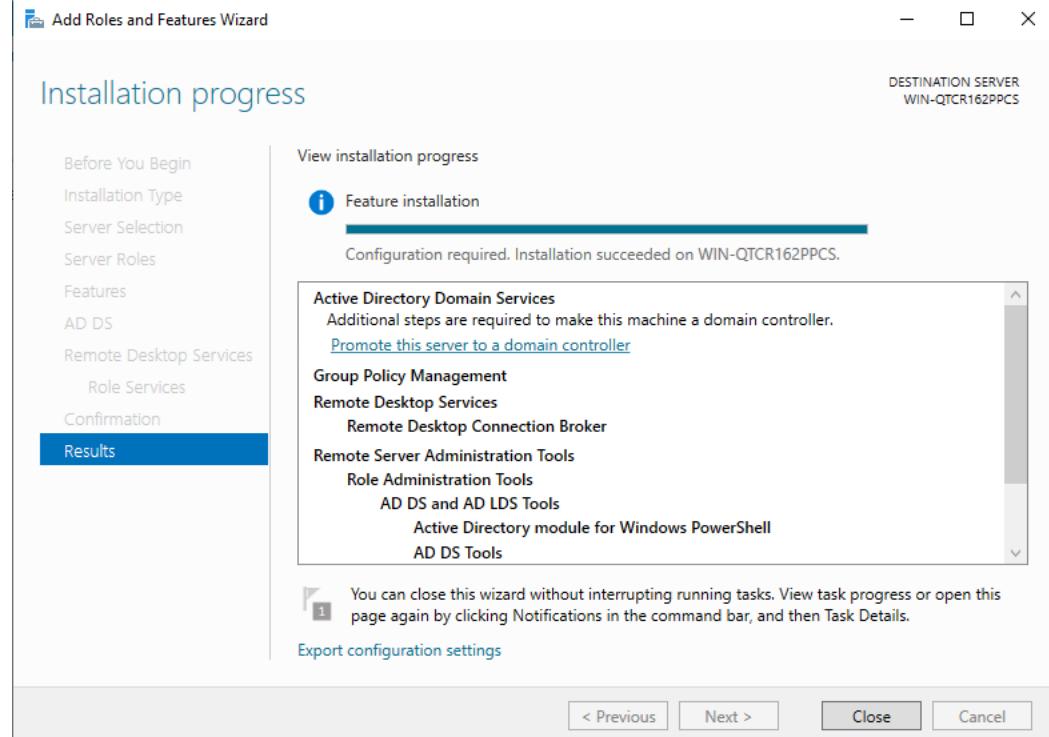
- h) Check Remote Desktop Connection Broken > Click Add Feature in popup dialog > Next**



- i) Confirm Installation Selections > Next**

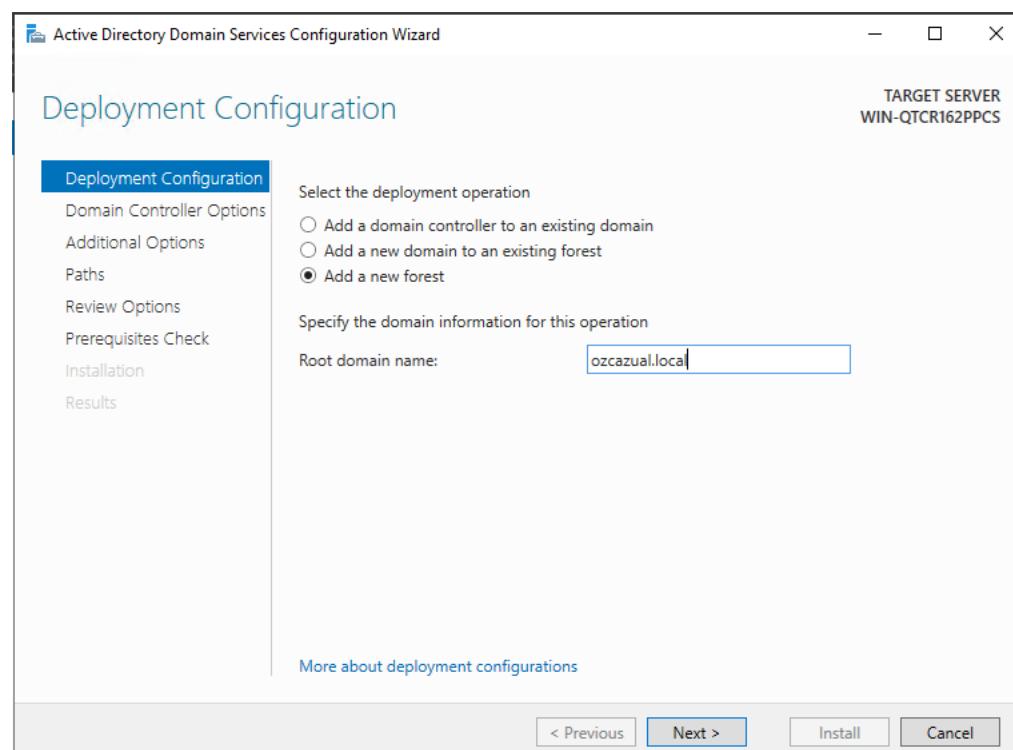


j) Installation Progress: Feature Installation Complete > Close



2. Promote Server to Domain Controller

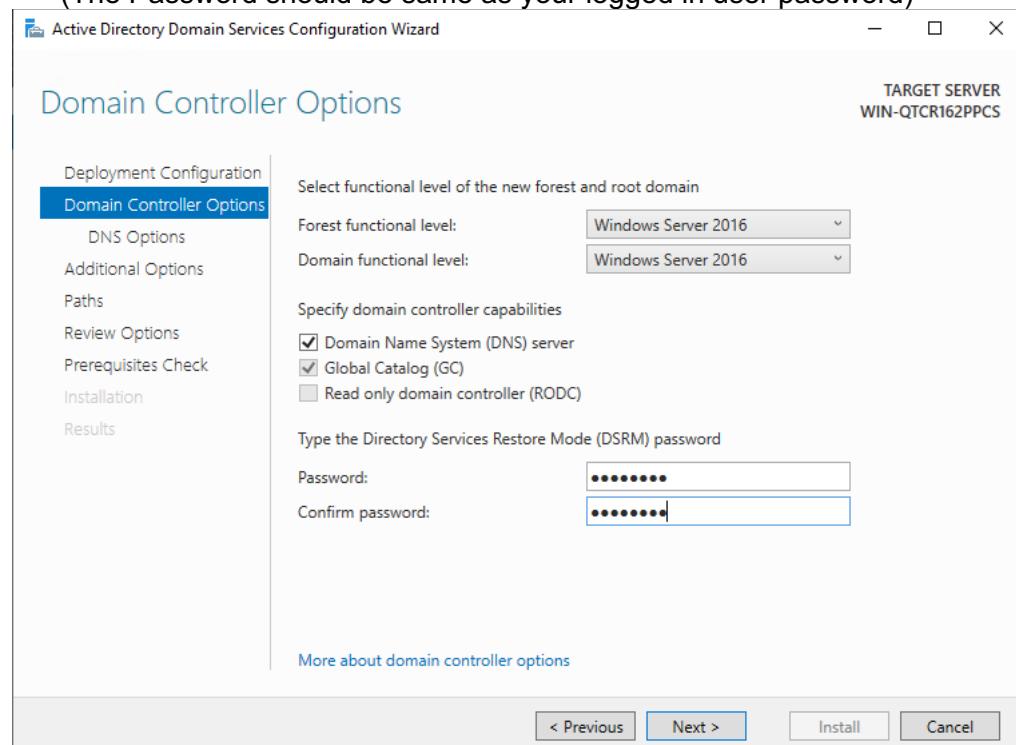
- a) Click on the Flag icon on top right > Promote this server to a domain controller
In the Active Directory Domain Wizard,
Deployment Configuration: Select Add a new forest
Root domain name: [domain_name].local > Next



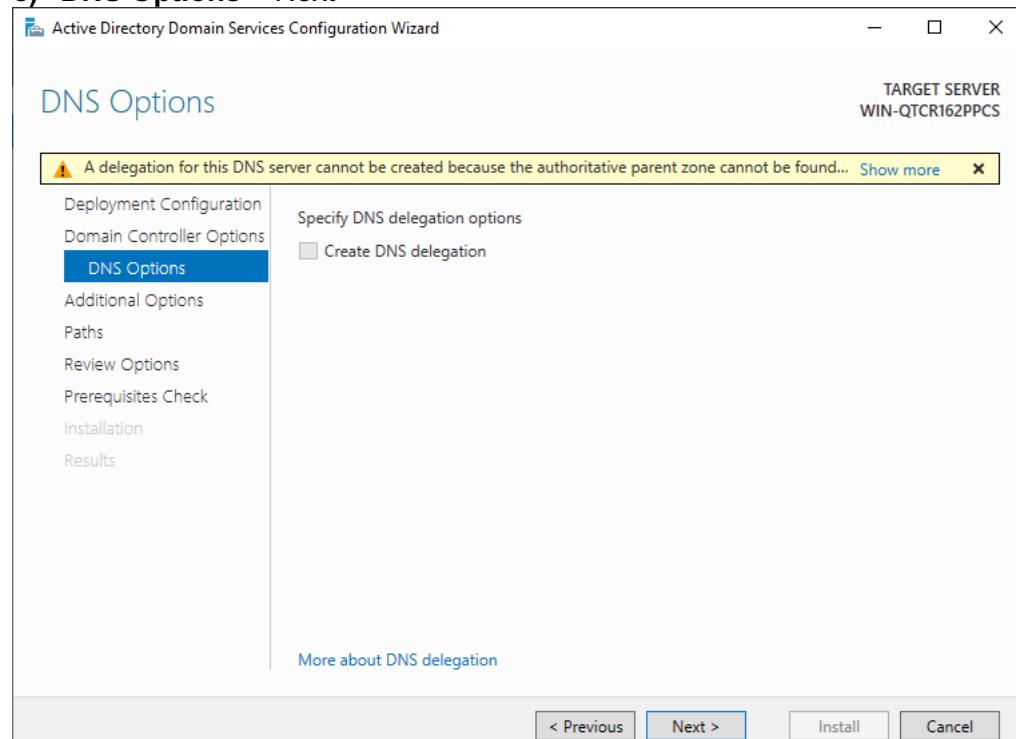
b) Domain Controller Options:

Password: [your_password] > Next

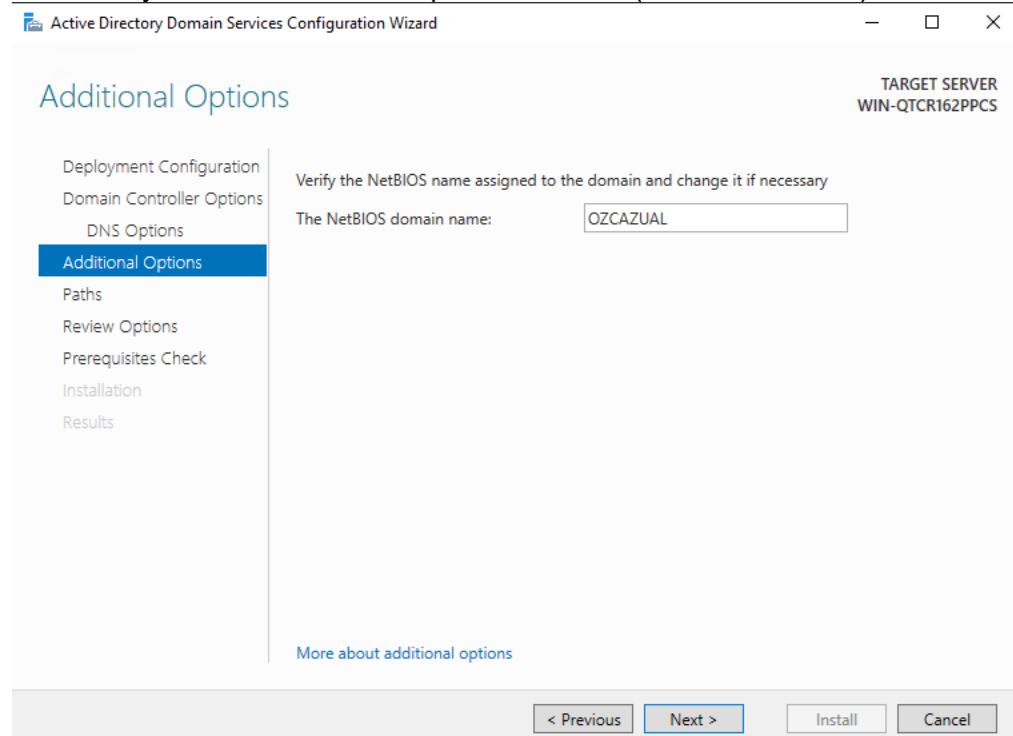
(The Password should be same as your logged in user password)



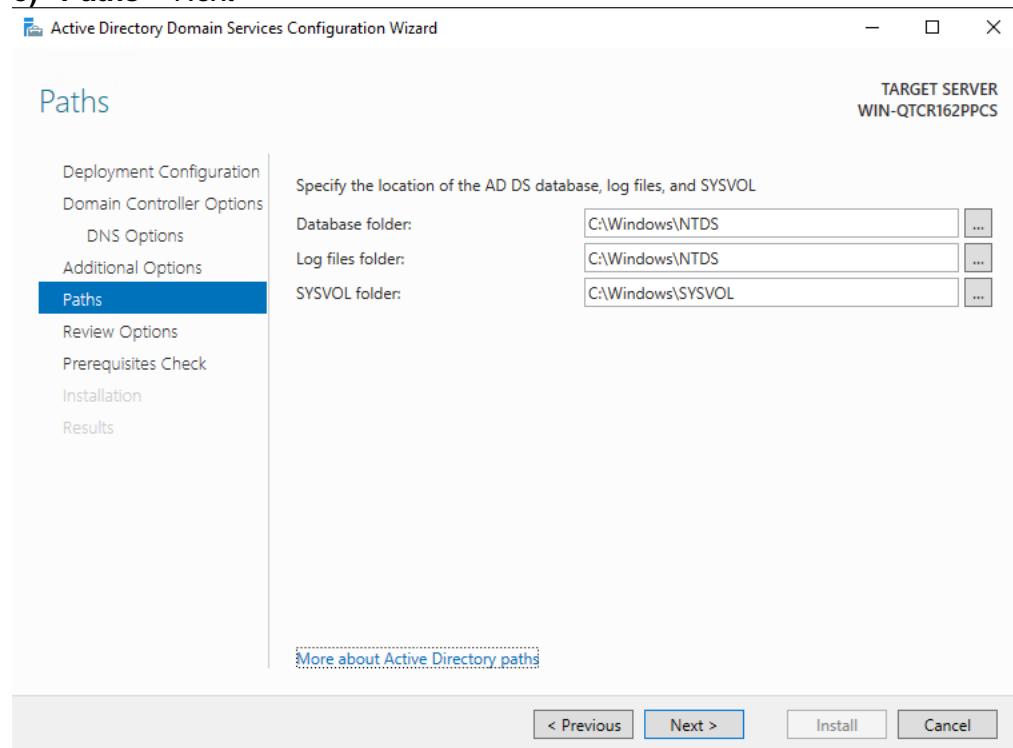
c) DNS Options > Next



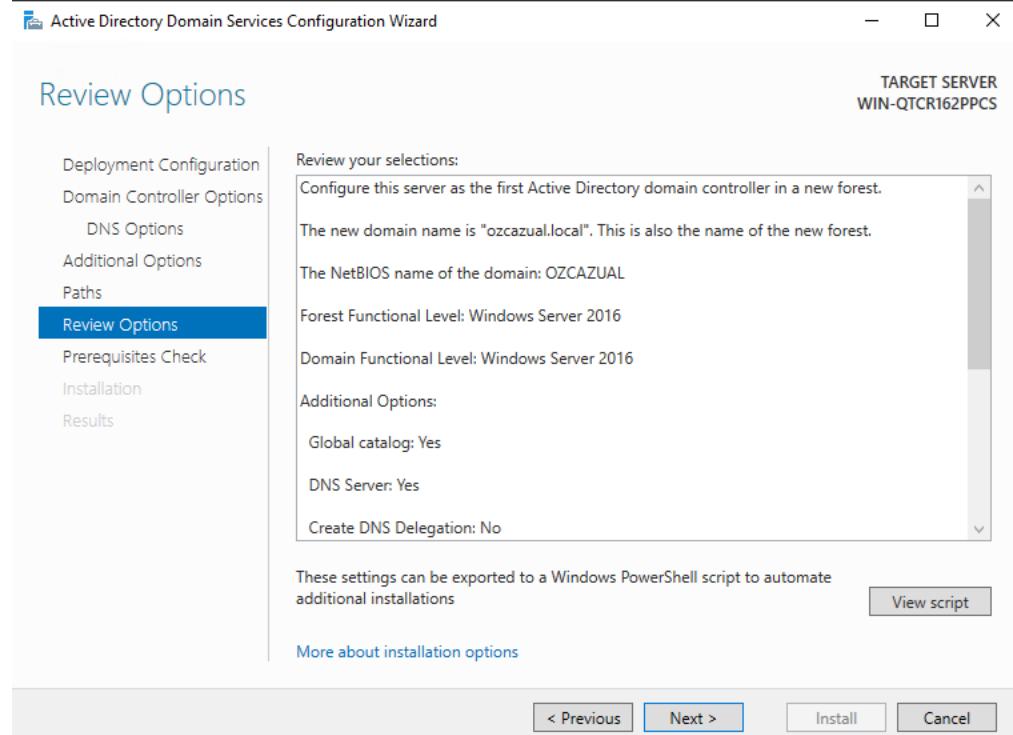
- d) **Additional Options:** Check the NetBIOS domain name matches the .local forest you created at first step in this wizard (Case-Insensitive) > Next



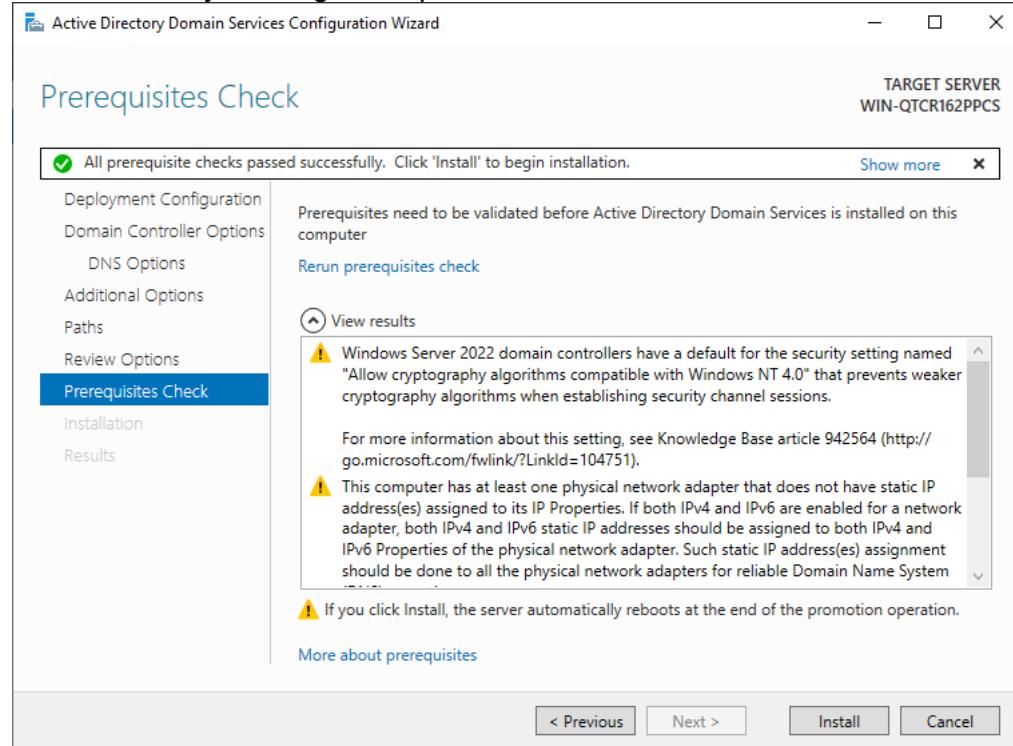
- e) **Paths** > Next



f) Review Options > Next

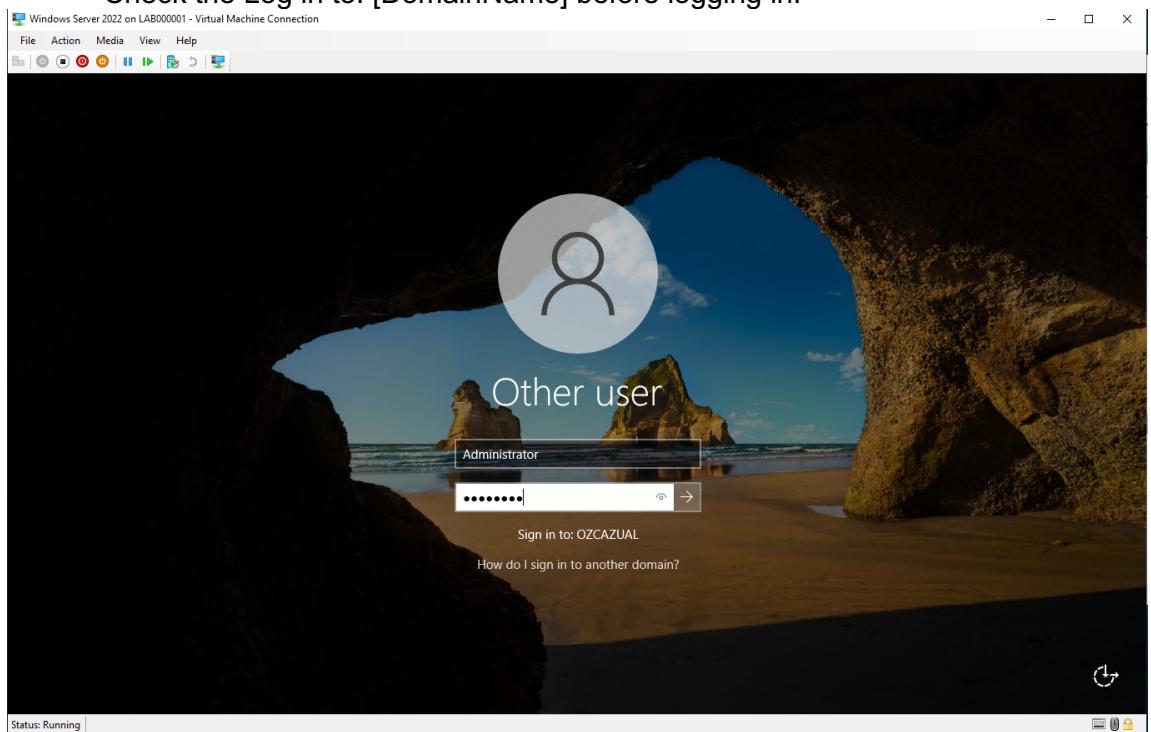


g) Prerequisites Check: Click **Install** only if see All prerequisite check passed successfully message on top

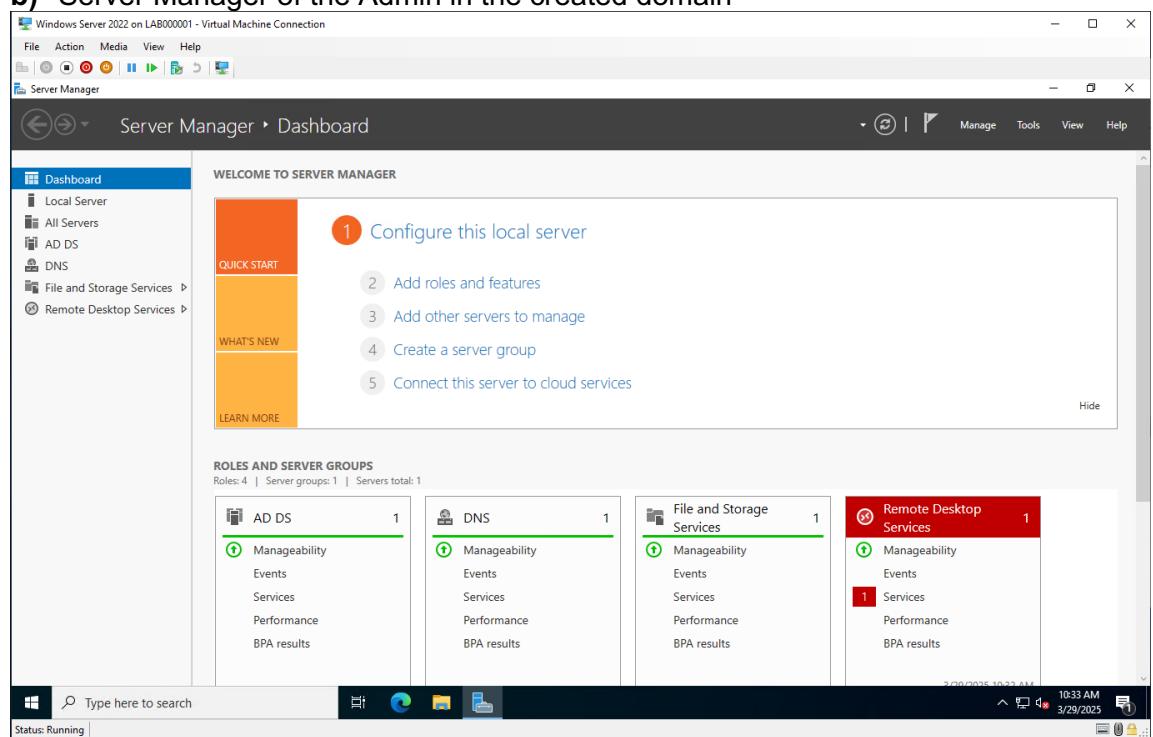


3. Post Installation Configuration

- a) After Installation, the server reboots and asks for login.
Check the Log in to: [DomainName] before logging in.

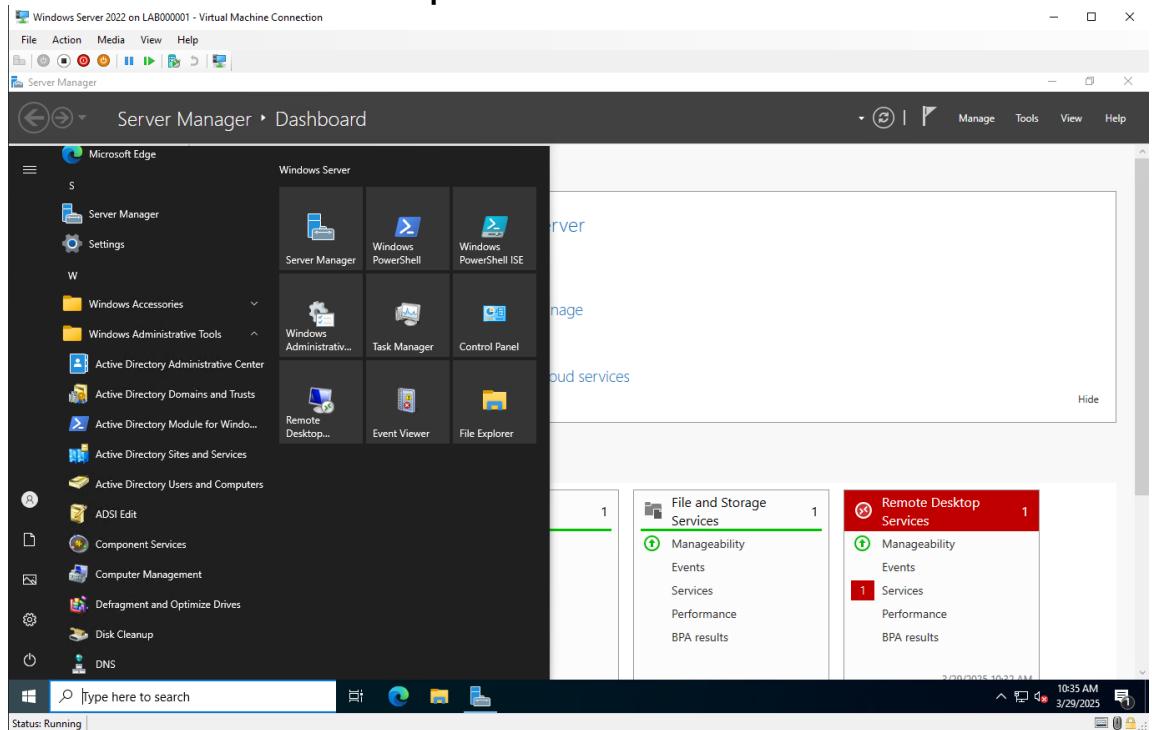


- b) Server Manager of the Admin in the created domain



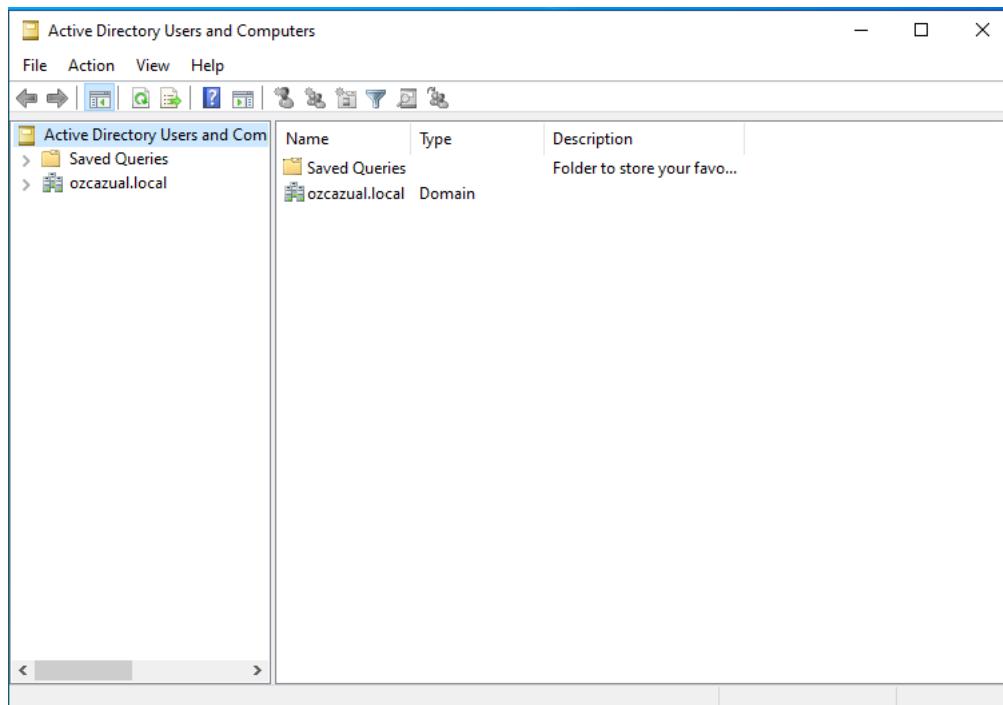
4. Verify AD DS Installation

Check the installed packages under **Start > Windows Administrative Tools**
You will find **Administrative Center, Domains & Trusts, Module, Sites & Services and Users & Computers**.



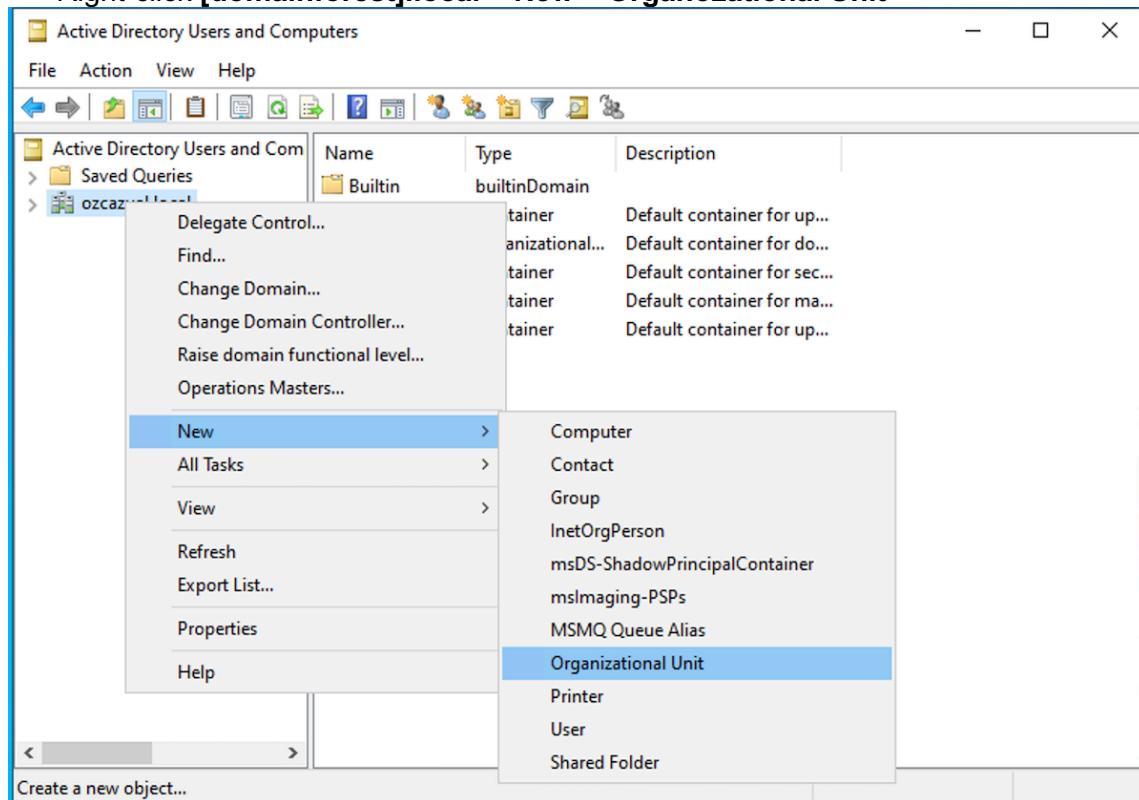
5. Configuring AD DS for User Authentication

- Go to **Start > Windows Administrative Tools > Active Directory Users and Computers**

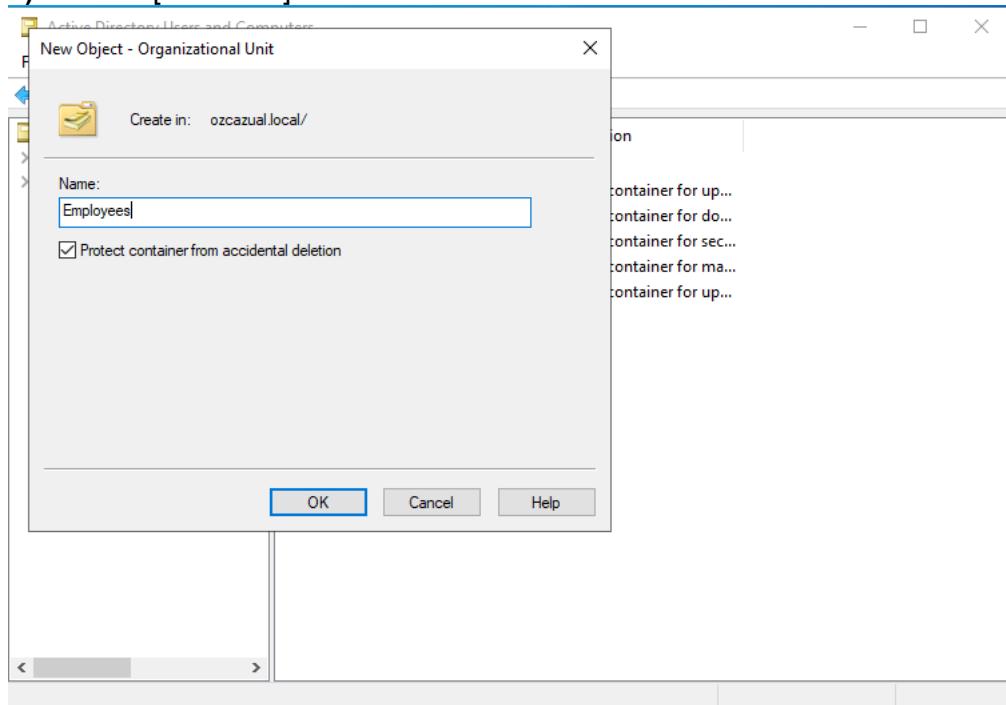


b) Create Organizational Units:

Right-click [domainforest].local > New > Organizational Unit



c) Name: [OUName] > OK



d) Created OUs: Employees, IT Team, Remote Staff, Servers

The screenshot shows the 'Active Directory Users and Computers' window. The left pane displays a tree view of the 'ozcazial.local' domain with several organizational units (OUs) listed: 'Builtin', 'Computers', 'Domain Con...', 'ForeignSecu...', 'Managed Se...', 'Users', 'Employees', 'IT Team', 'Remote Staff', and 'Servers'. The 'Employees' OU is selected. The right pane is a table with columns 'Name', 'Type', and 'Description'. It lists the following entries:

Name	Type	Description
Builtin	builtinDomain	Default container for up...
Computers	Container	Default container for do...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
Employees	Organizational...	
IT Team	Organizational...	
Remote Staff	Organizational...	
Servers	Organizational...	

**e) Create Users in OUs:
Right-click [OUName] > New > User**

The screenshot shows the 'Active Directory Users and Computers' window. The left pane displays the same tree view as before. The 'Employees' OU is selected and has a context menu open. The menu includes options like 'Delegate Control...', 'Move...', 'Find...', 'New' (which is expanded to show 'Computer', 'Contact', 'Group', etc.), 'All Tasks', 'View', 'Cut', 'Delete', 'Rename', 'Refresh', 'Export List...', 'Properties', and 'Help'. The 'User' option under the 'New' submenu is highlighted.

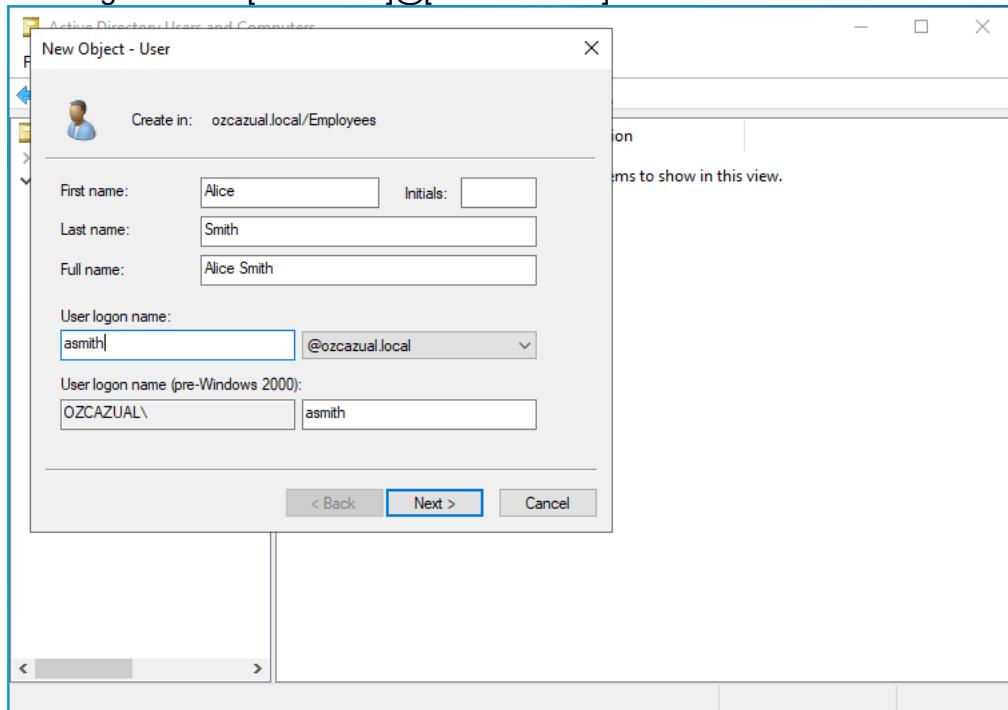
f) Create User:

First name: [UserFirstName]

Last name: [UserLastName]

Full name: (Fills automatically after First name and Last name fields are filled)

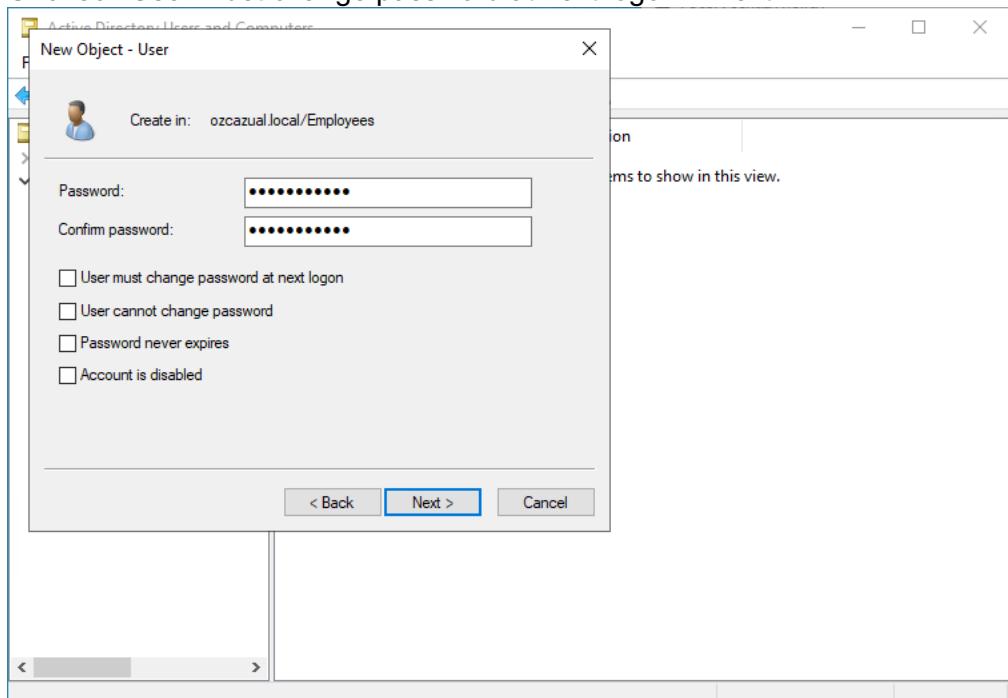
User logon name: [username]@[domainname].local > Next



g) Create Password:

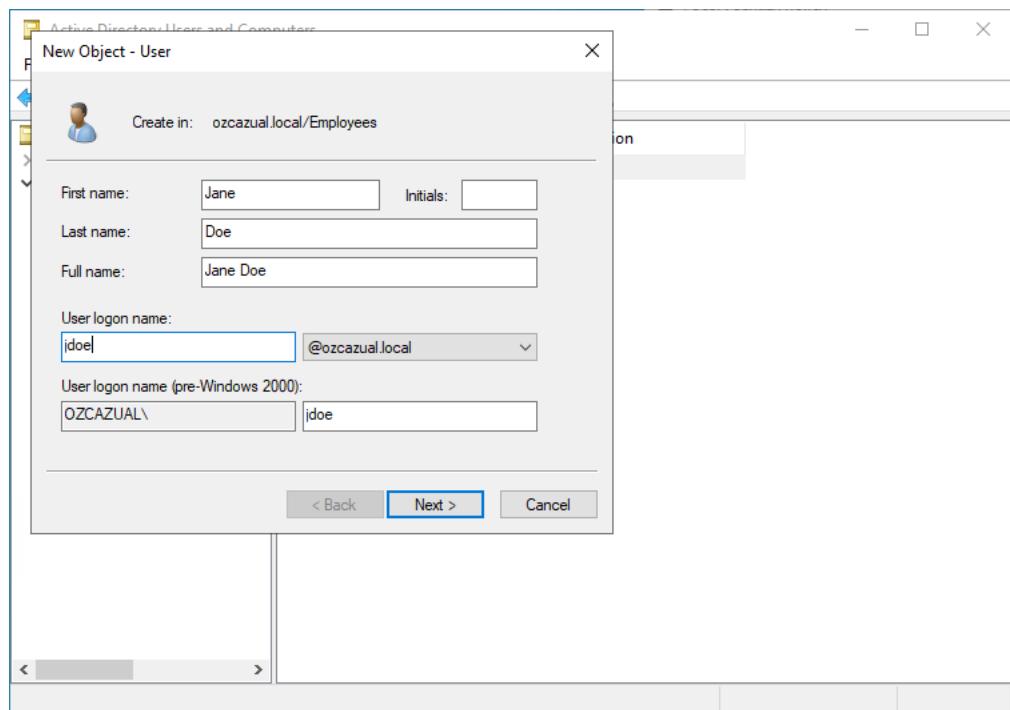
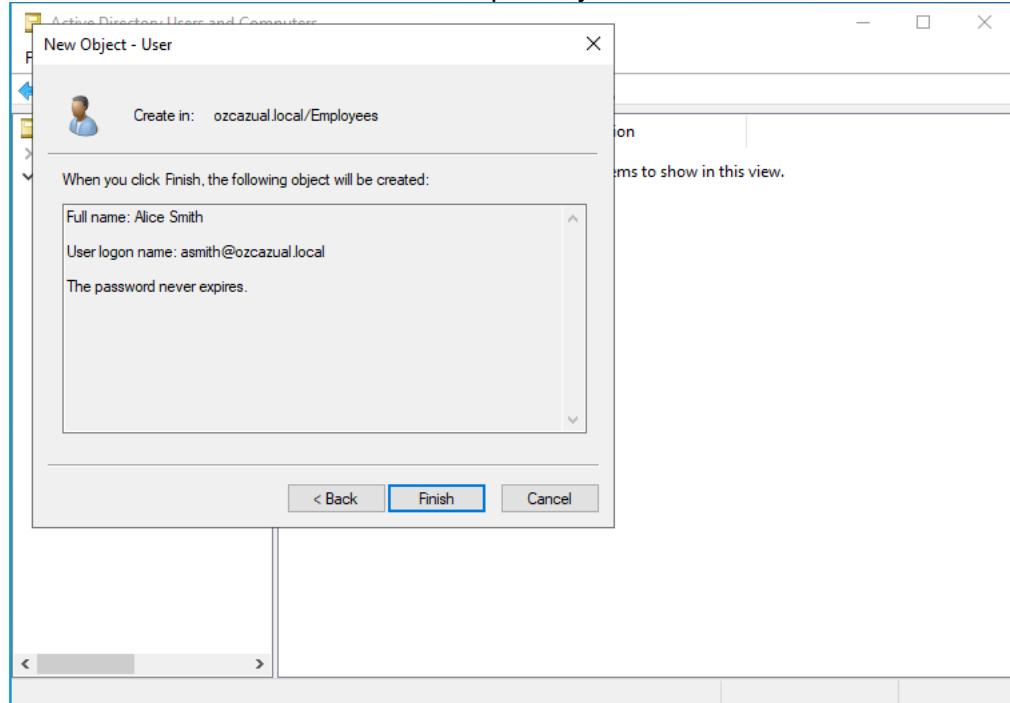
Password: [ypur_Password]

Uncheck User must change password at next logon > Next



As0zcemp001

h) Check the user information and the options you have chosen > Finish



New Object - User

Create in: ozcazual.local/Employees

Password: Confirm password:

User must change password at next logon
 User cannot change password
 Password never expires
 Account is disabled

< Back Next > Cancel

Jd0zcemp002

New Object - User

Create in: ozcazual.local/Employees

When you click Finish, the following object will be created:

Full name: Jane Doe
User logon name: jdoe@ozcazual.local

< Back Finish Cancel

New Object - User

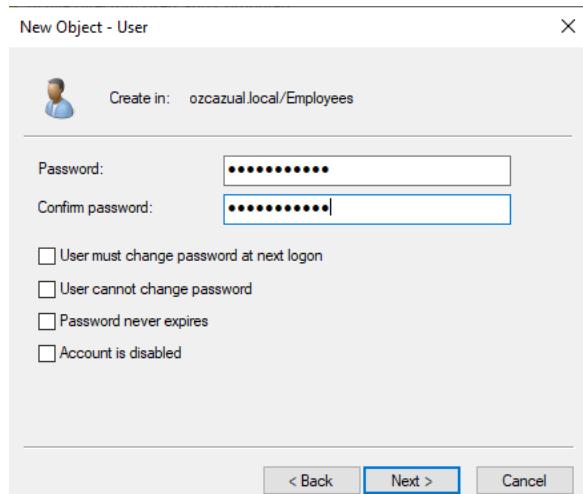
Create in: ozcazual.local/Employees

First name: Matt Initials:
Last name: Wilson
Full name: Matt Wilson

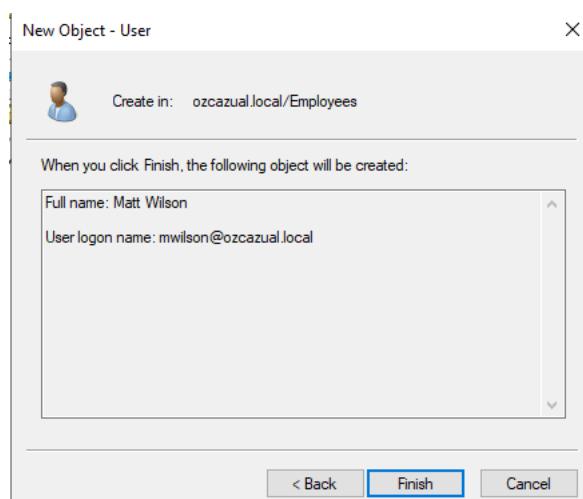
User logon name:
mwilson @ozcazual.local

User logon name (pre-Windows 2000):
OZCAZUAL\ mwilson

< Back Next > Cancel



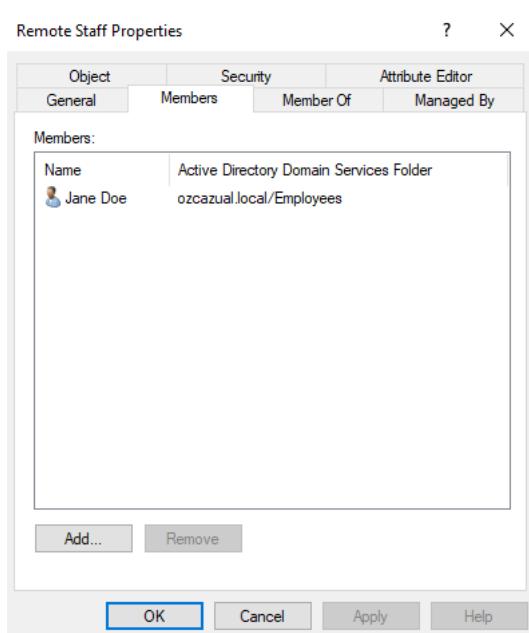
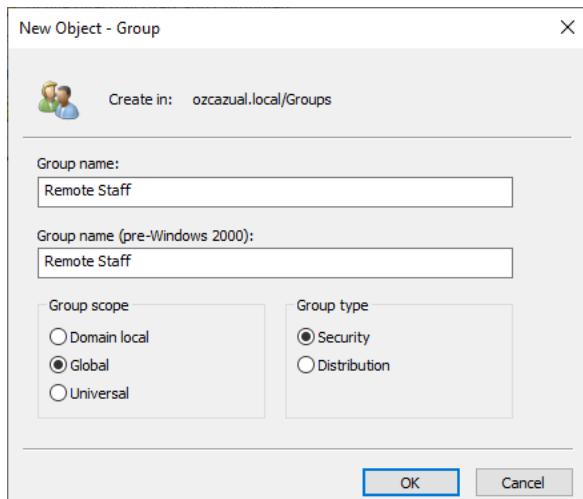
Mw0zceemp003

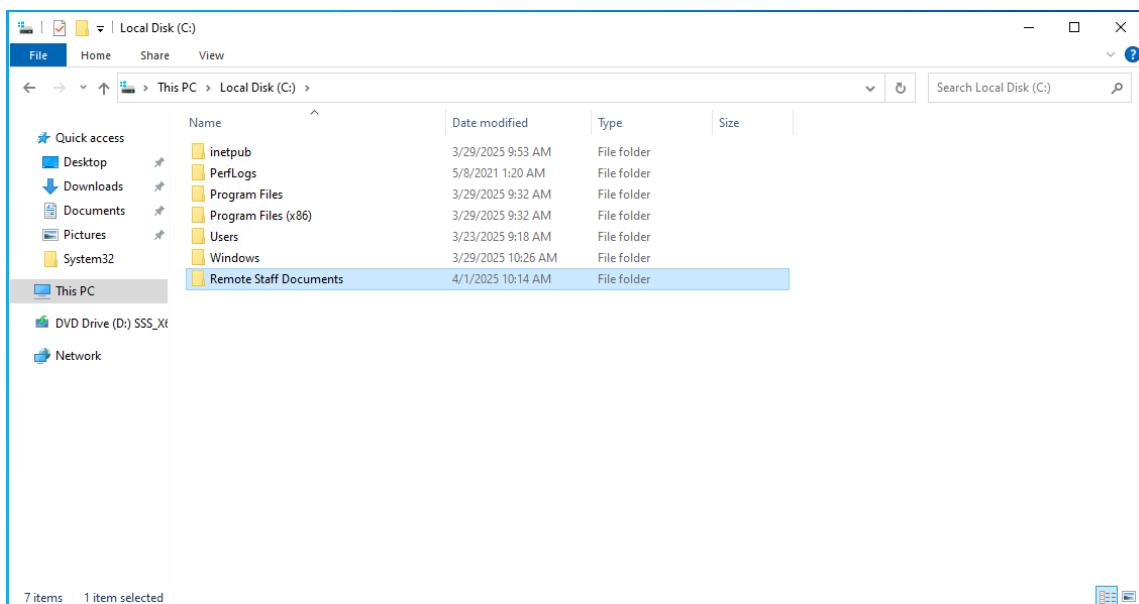
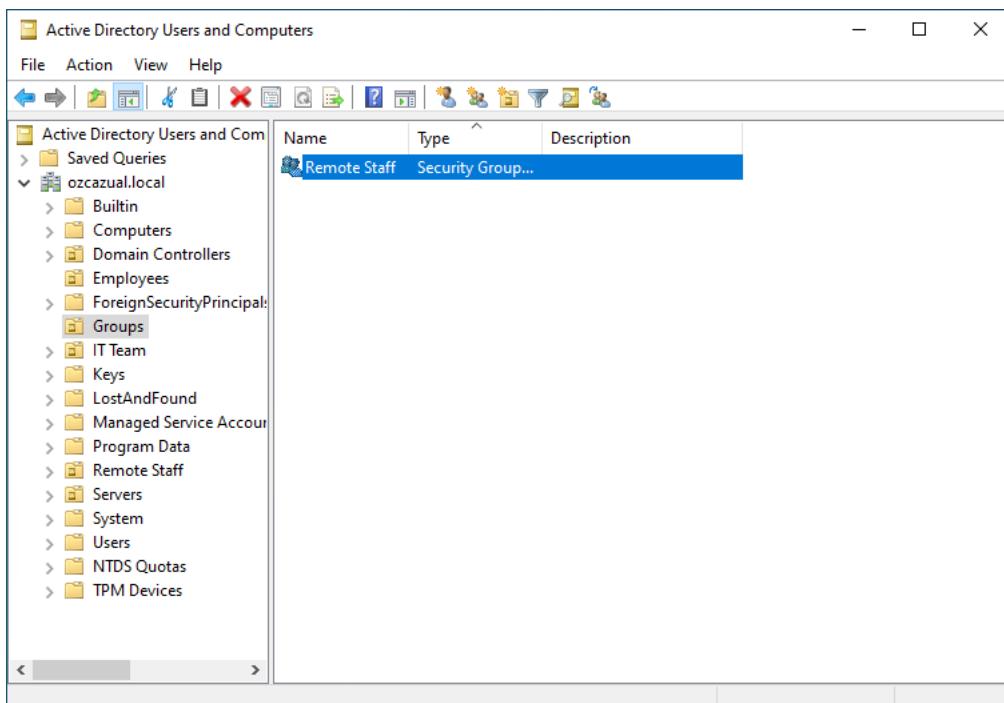


i) List of users created in one OU:

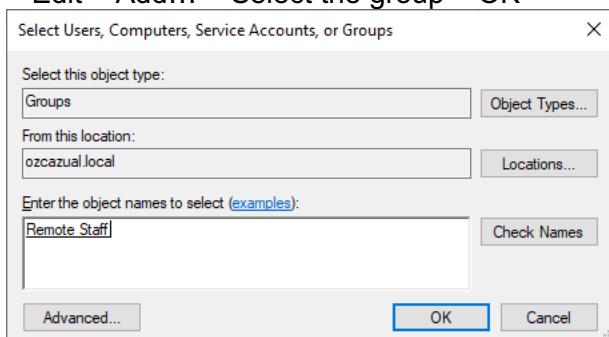
Active Directory Users and Computers			
File Action View Help			
Active Directory Users and Computers	Name	Type	Description
Saved Queries			
ozcazual.local			
Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipal			
Managed Service Account			
Users			
Employees	Alice Smith	User	
IT Team	Jane Doe	User	
Remote Staff			
Servers	Matt Wilson	User	

6. Create a Group Security Policy

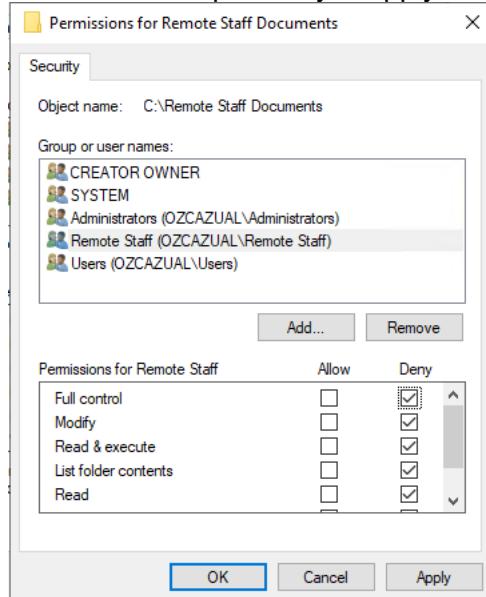




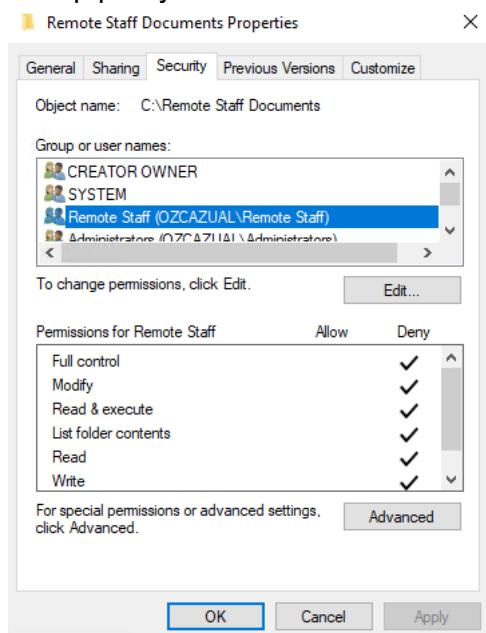
Right-click Remote Staff Documents > Properties > Security tab > Group or user names > Edit > Add... > Select the group > OK



Select the Group > Deny > Apply > OK

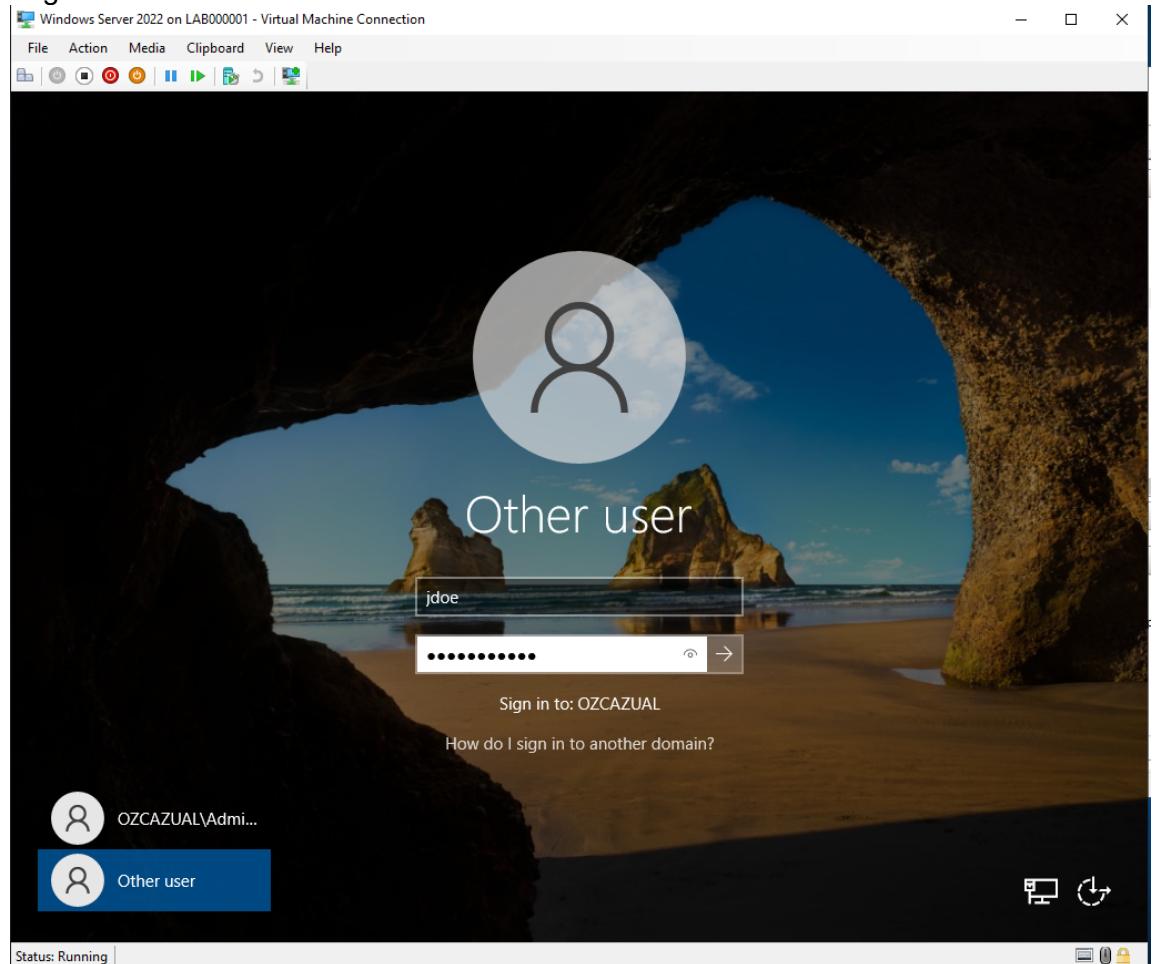


Group policy for the document

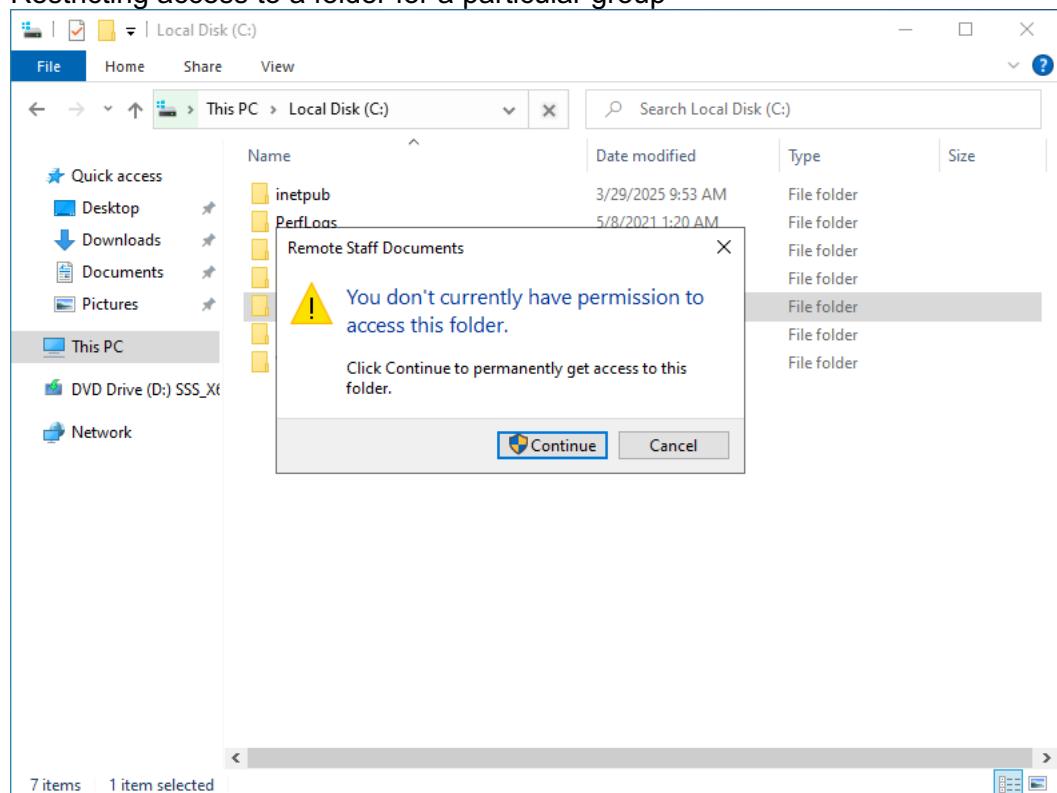


7. Test Access Privileges

Log in as a user of the domain



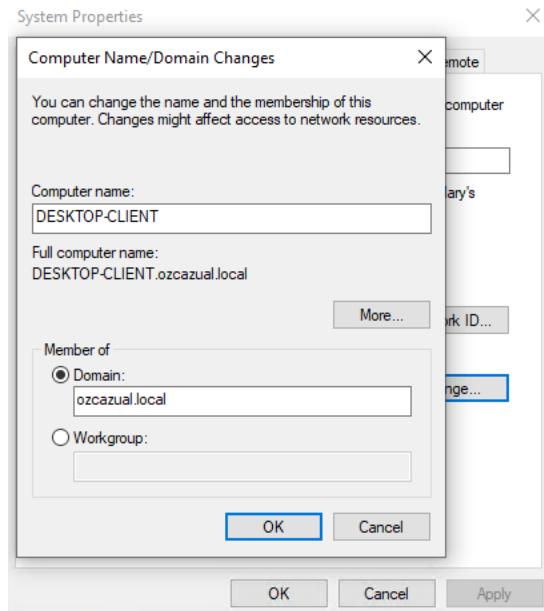
Restricting access to a folder for a particular group



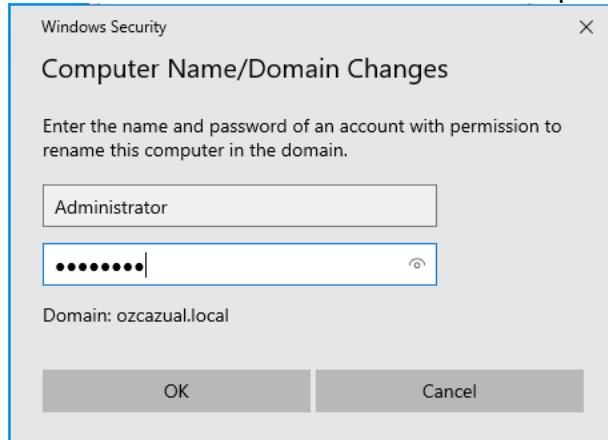
Test Login from a Client Machine

1. Join a client machine (Windows 10/11) to the domain:

- Open **System Properties** (sysdm.cpl)
- Click **Change...** > Select Domain
- Enter **Domain Name (domainname.local)** and click **OK**



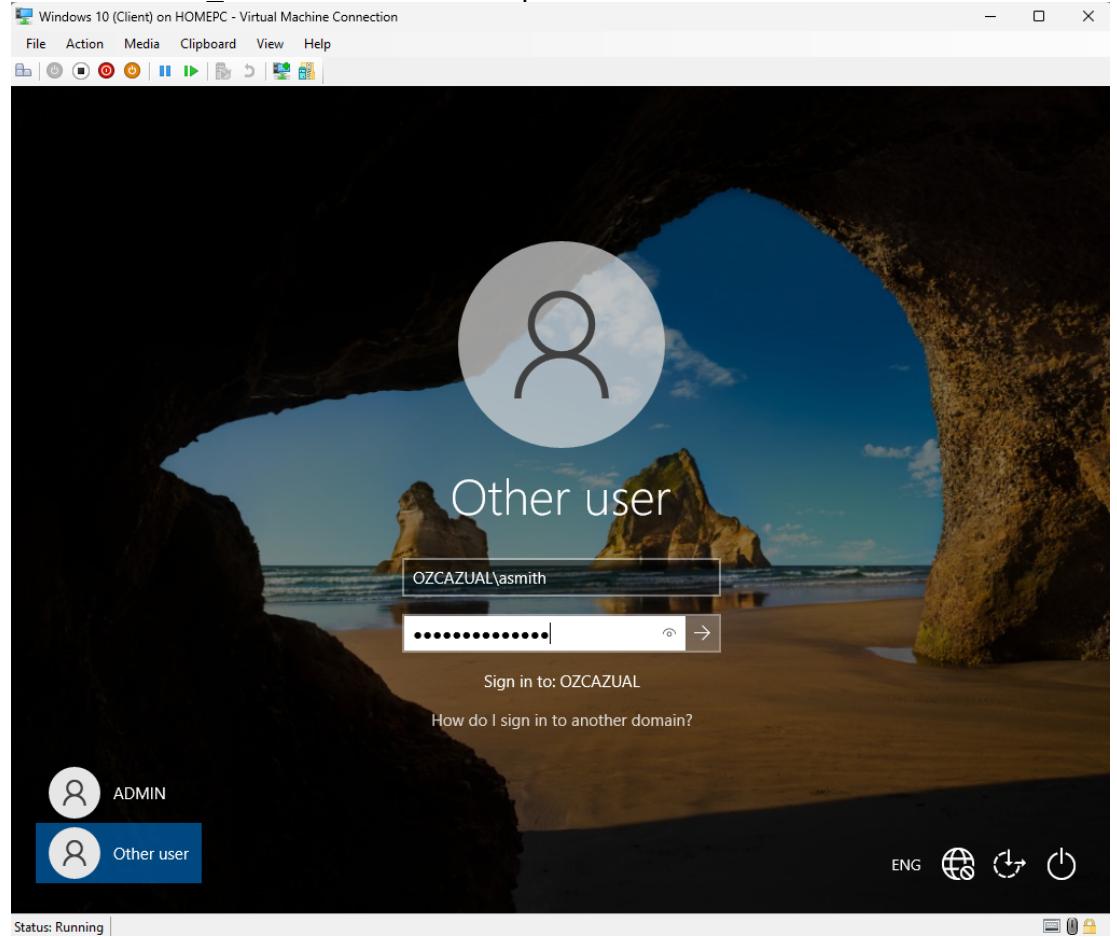
- Provide **Administrator credentials** when prompted



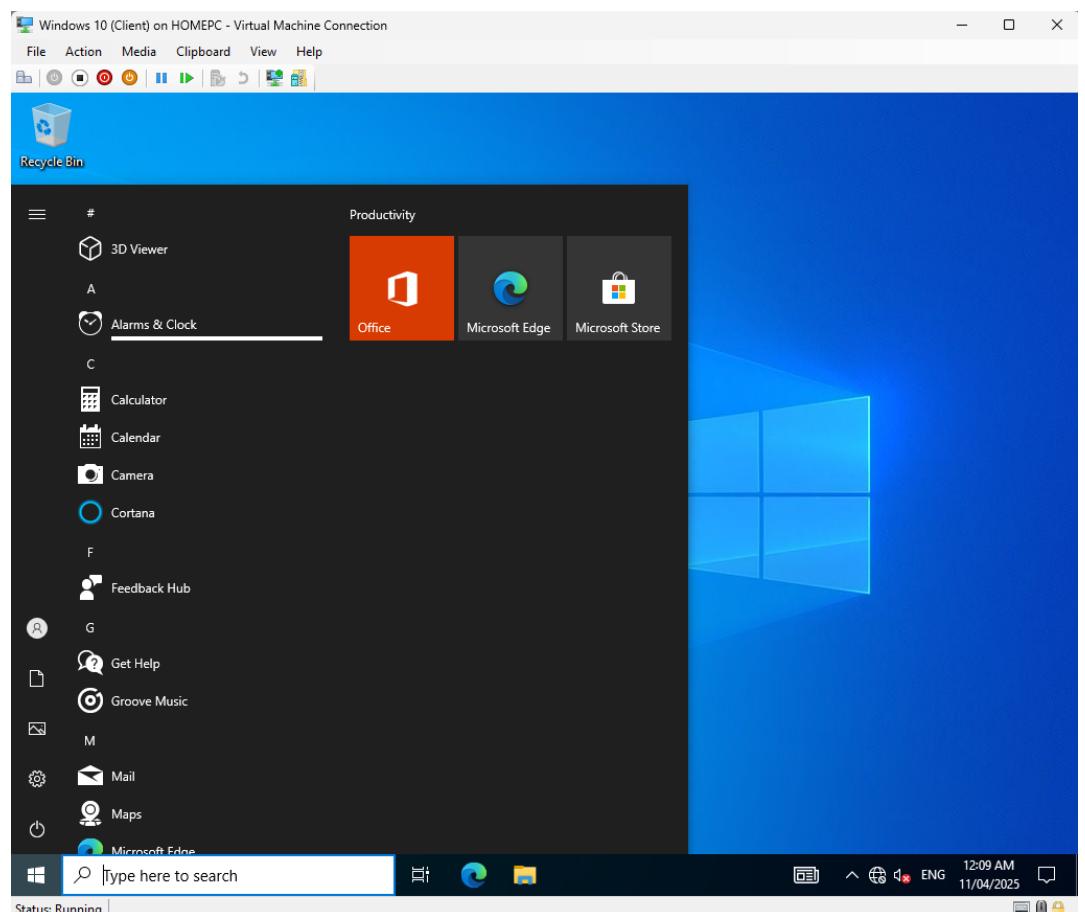
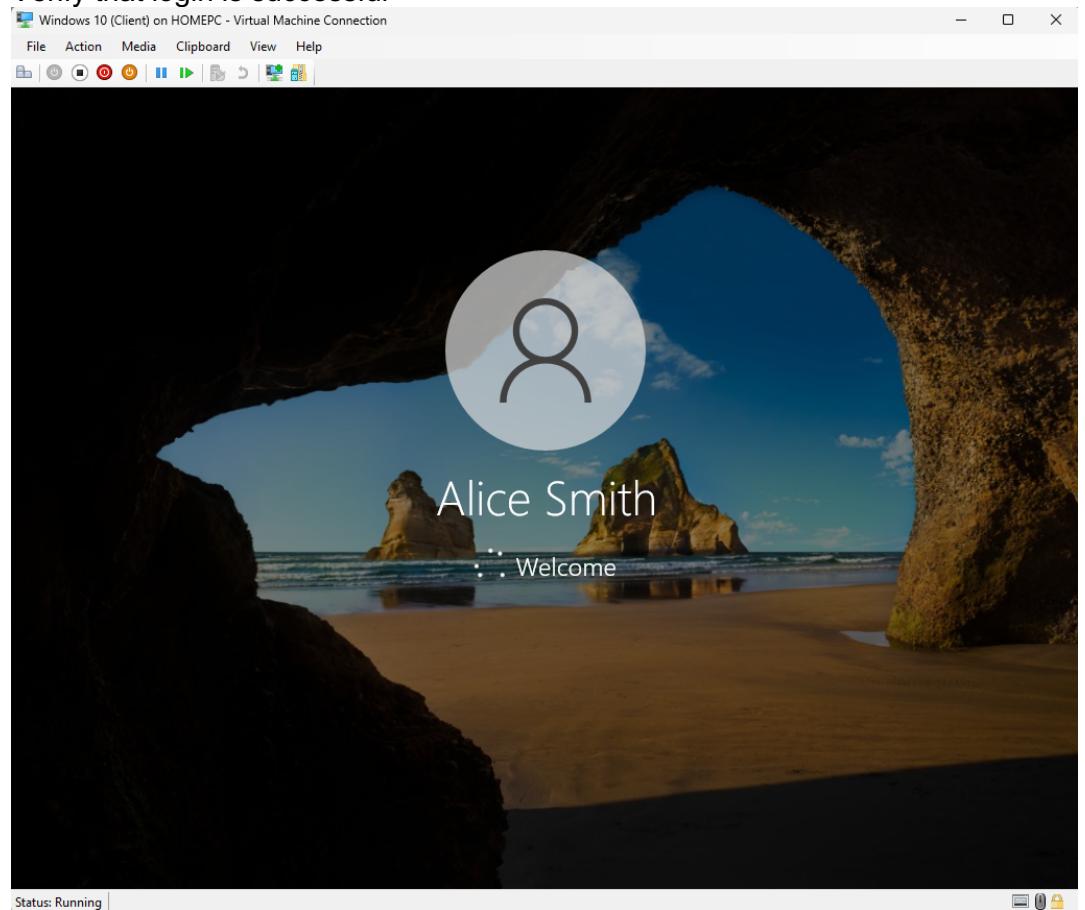
- Restart the client machine

2. Login as a domain user:

- On the client machine (Windows 10), press Ctrl + Alt + Del
- Click **Switch User > Other User**
- Enter DOMAIN_NAME\UserName and password



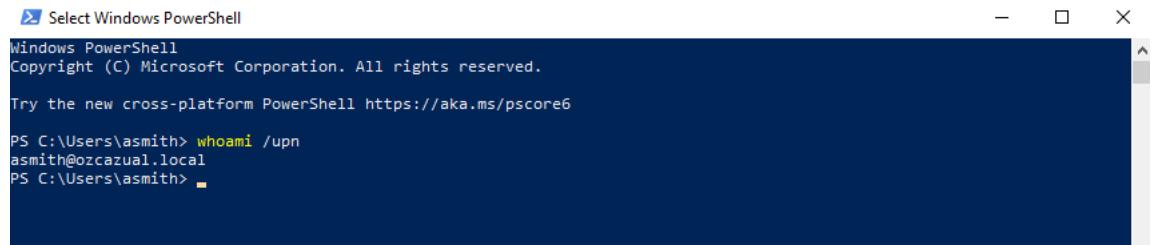
- Verify that login is successful



3. **Check user details using PowerShell:**
On the **Windows 10 (Client) machine**, run:

```
powershell  
whoami /upn
```

It should return the user's UPN (User Principal Name) from AD DS.



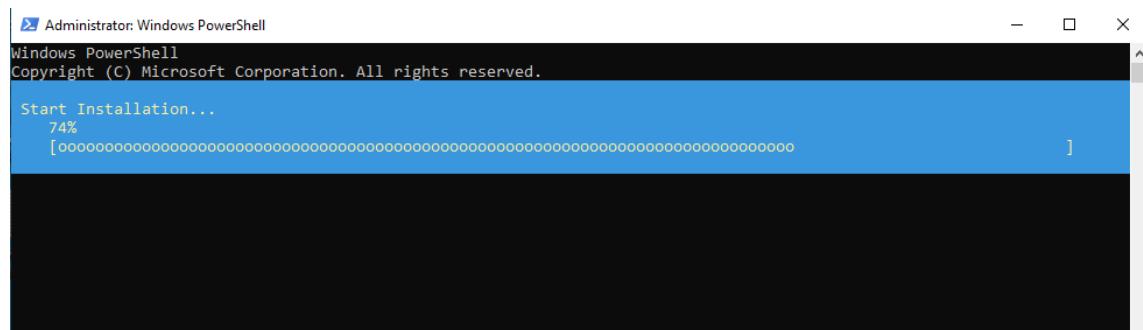
```
Select Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
PS C:\Users\asmith> whoami /upn  
asmith@ozcazual.local  
PS C:\Users\asmith>
```

Detailed SMB file sharing configuration in Windows Server

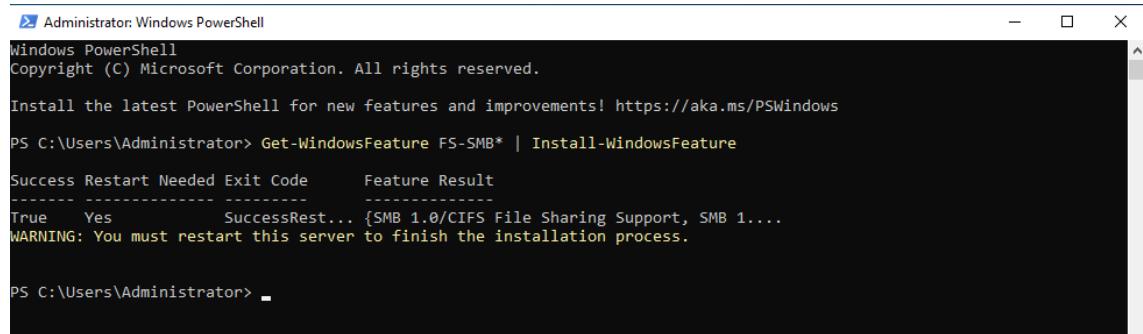
Install and Enable SMB:

Open Powershell (as Administrator)

```
Get-WindowsFeature FS-SMB* | Install-WindowsFeature
```



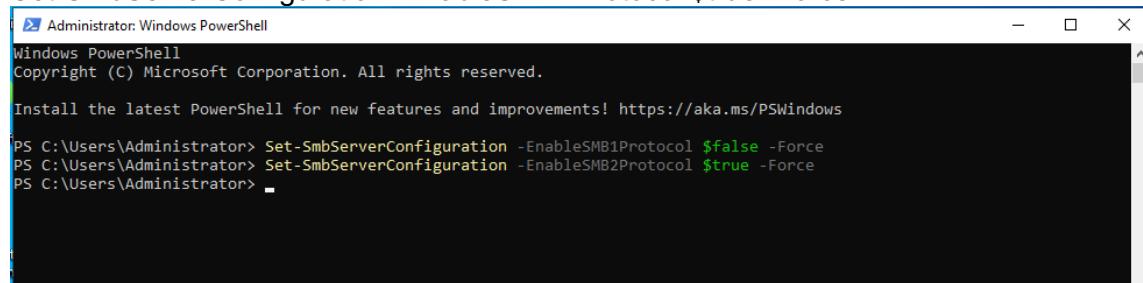
```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Start Installation...  
74%  
[oooooooooooooooooooooooooooooooooooooooooooooooooooo]
```



```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
PS C:\Users\Administrator> Get-WindowsFeature FS-SMB* | Install-WindowsFeature  
Success Restart Needed Exit Code Feature Result  
----- ----- ----- -----  
True Yes SuccessRest... {SMB 1.0/CIFS File Sharing Support, SMB 1....  
WARNING: You must restart this server to finish the installation process.  
PS C:\Users\Administrator>
```

Ensure SMBv2 and SMBv3 are enabled

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force  
Set-SmbServerConfiguration -EnableSMB2Protocol $true -Force
```



```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
PS C:\Users\Administrator> Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force  
PS C:\Users\Administrator> Set-SmbServerConfiguration -EnableSMB2Protocol $true -Force  
PS C:\Users\Administrator>
```

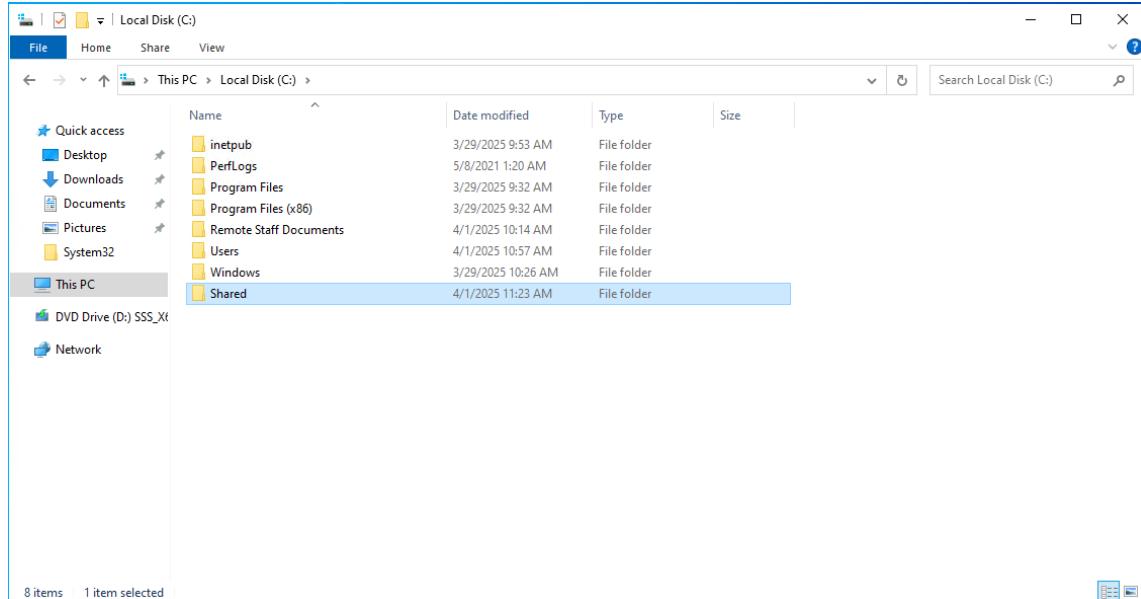
Ensure SMB is running

Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol

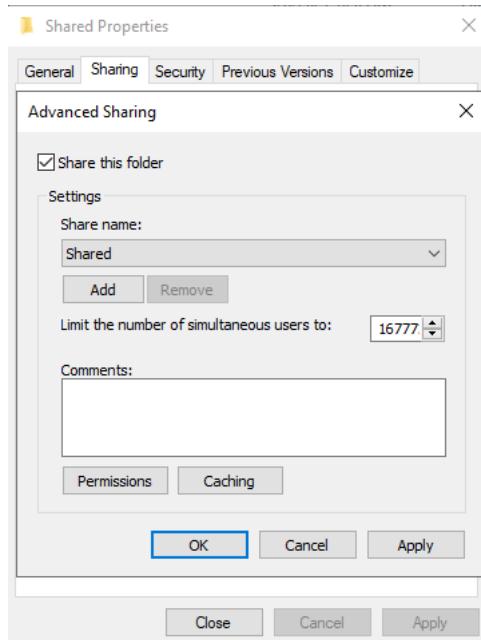
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
EnableSMB1Protocol EnableSMB2Protocol
-----
False          True

PS C:\Users\Administrator>
```

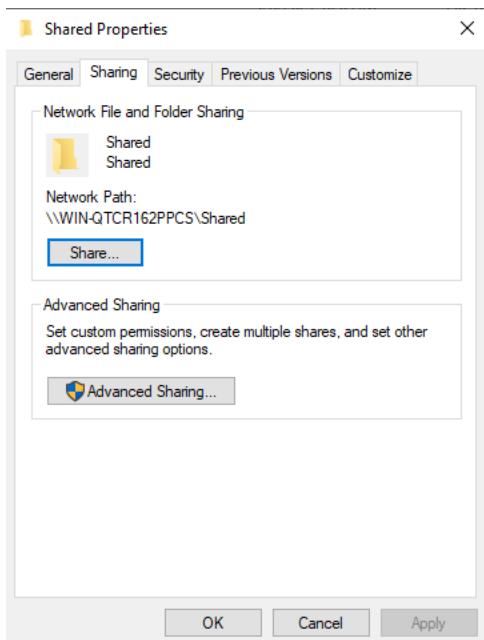
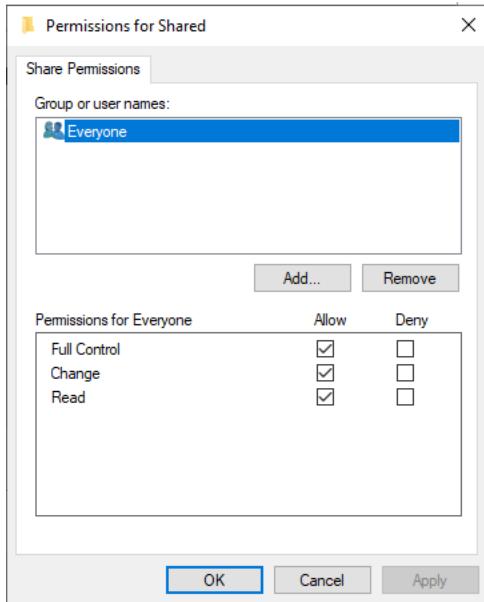
Create a Shared Folder:
Create a folder to share



Right-click > Properties > Sharing tab > Advanced Sharing
Check Share this folder

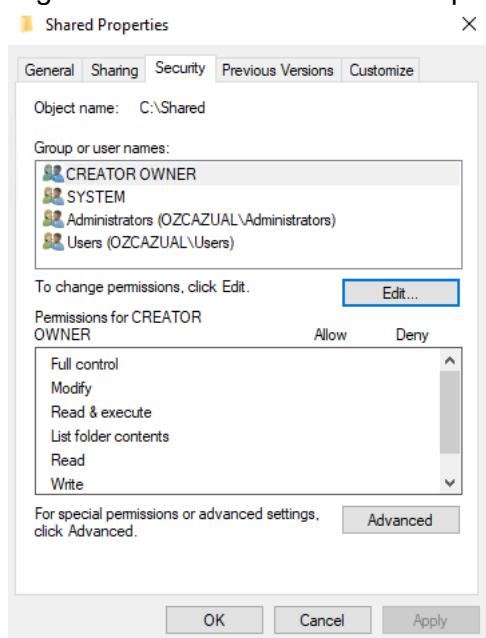


Click Permissions > Set:
Everyone: Full Control > OK > Apply > OK

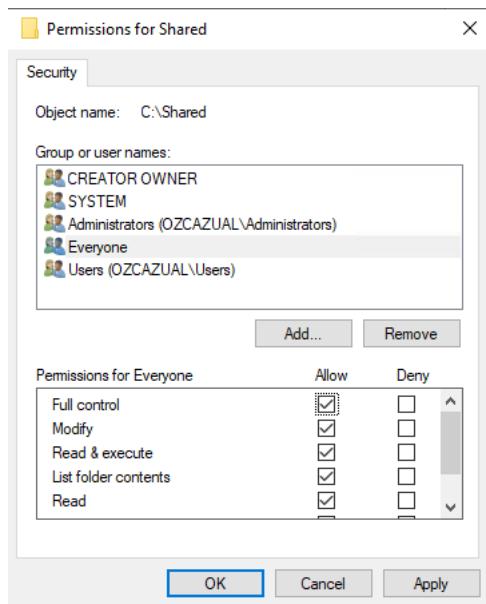
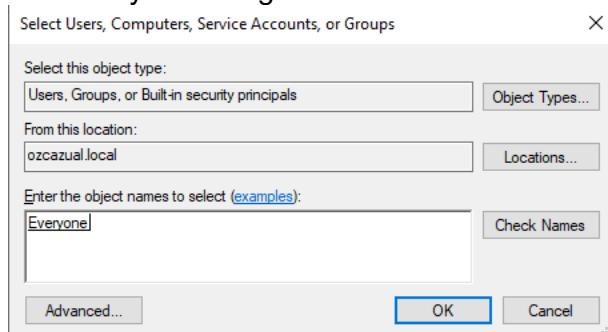


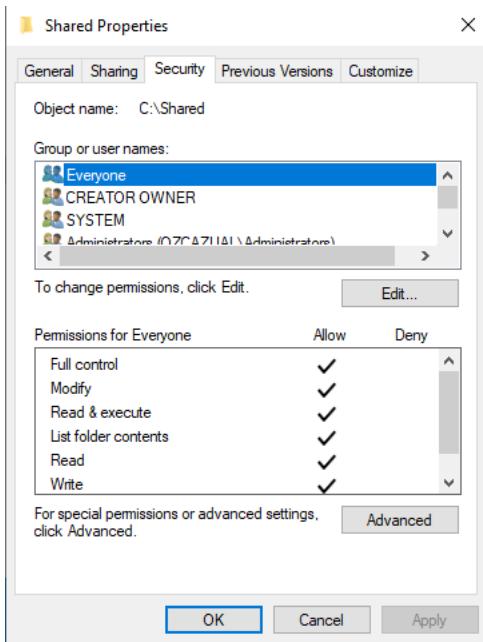
Set NTFS Permissions (Temporary Full Access)

Right-click the shared folder > Properties > Security tab > Edit... > Add...



Add Everyone and give Full Control





Open SMB Ports in Windows Firewall

Open Windows Defender Firewall > Advanced Settings

Go to Inbound Rules > Find File and Printer Sharing (SMB-In) > Enable the rule

Name	Group	Profile	Enabled
Distributed Transaction Coordinator (RPC-EPM...	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
<input checked="" type="checkbox"/> DNS (TCP, Incoming)	DNS Service	All	Yes
<input checked="" type="checkbox"/> DNS (UDP, Incoming)	DNS Service	All	Yes
<input checked="" type="checkbox"/> RPC (TCP, Incoming)	DNS Service	All	Yes
<input checked="" type="checkbox"/> RPC Endpoint Mapper (TCP, Incoming)	DNS Service	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (Echo Request - ICMPv4...	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (Echo Request - ICMPv6...	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (Spooler Service - RPC-E...	File and Printer Sharing	All	Yes
<input checked="" type="checkbox"/> File and Printer Sharing (SMB-QUIC-In)	File and Printer Sharing over...	All	No
<input checked="" type="checkbox"/> File and Printer Sharing over SMBDirect (IWARP...	File and Printer Sharing over...	All	No
<input checked="" type="checkbox"/> File Replication (RPC)	File Replication	All	Yes
<input checked="" type="checkbox"/> File Replication (RPC-EPMAP)	File Replication	All	Yes
<input checked="" type="checkbox"/> File Server Remote Management (DCOM-In)	File Server Remote Manage...	All	Yes
<input checked="" type="checkbox"/> File Server Remote Management (SMB-In)	File Server Remote Manage...	All	Yes
<input checked="" type="checkbox"/> File Server Remote Management (WMI-In)	File Server Remote Manage...	All	Yes
iSCSI Service (TCP-In)	iSCSI Service	All	No
<input checked="" type="checkbox"/> Kerberos Key Distribution Center - PCR (TCP-In)	Kerberos Key Distribution C...	All	Yes
<input checked="" type="checkbox"/> Kerberos Key Distribution Center - PCR (UDP-In)	Kerberos Key Distribution C...	All	Yes
<input checked="" type="checkbox"/> Kerberos Key Distribution Center (TCP-In)	Kerberos Key Distribution C...	All	Yes
<input checked="" type="checkbox"/> Kerberos Key Distribution Center (UDP-In)	Kerberos Key Distribution C...	All	Yes
Key Management Service (TCP-In)	Key Management Service	All	No
mDNS (UDP-In)	mDNS	Private	Yes

Access the Share from Another Machine

On a Windows Client Machine:

Open Run (Win + R)

Type: <\\<WindowsServer-IP>\Shared>

Enter credentials (if prompted)

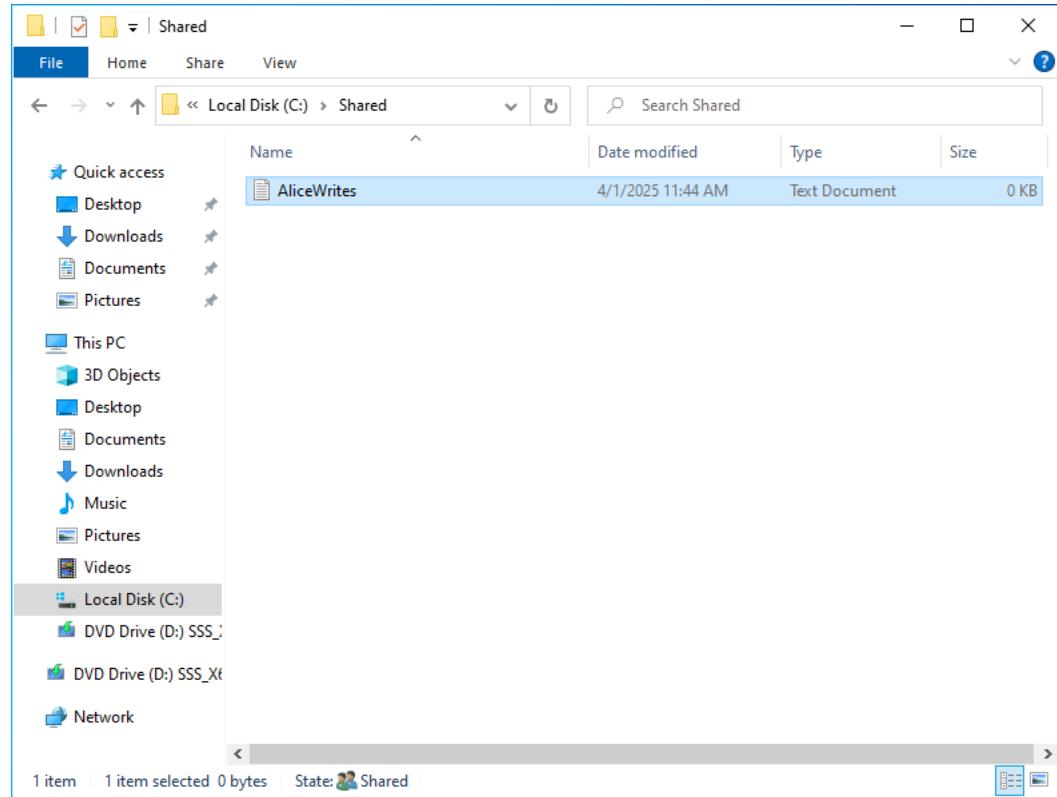
Try copying, modifying and deleting files to confirm it works.

OR

If checking on the same machine,

Log in as a user

Access shared folder and make changes either by navigating to the path or by typing in address bar: \\localhost\[sharedFolderName] > Enter



Can also access through PowerShell with using either of these commands:

net share
(Gives a listing of shared folders)

dir \\localhost\[sharedFolderName]

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\asmith> net share

Share name   Resource          Remark
-----   -----
C$        C:\                 Default share
IPC$       IPC                Remote IPC
ADMIN$     C:\Windows         Remote Admin
NETLOGON   C:\Windows\SYSVOL\sysvol\ozcazial.local\SCRIPTS
           Logon server share
Shared      C:\Shared          Logon server share
SYSVOL    C:\Windows\SYSVOL\sysvol      Logon server share
The command completed successfully.

PS C:\Users\asmith> dir \\localhost\shared

Directory: \\localhost\shared

Mode          LastWriteTime      Length Name
----          -----          -----
-a---  4/1/2025 11:44 AM          0 AliceWrites.txt
```