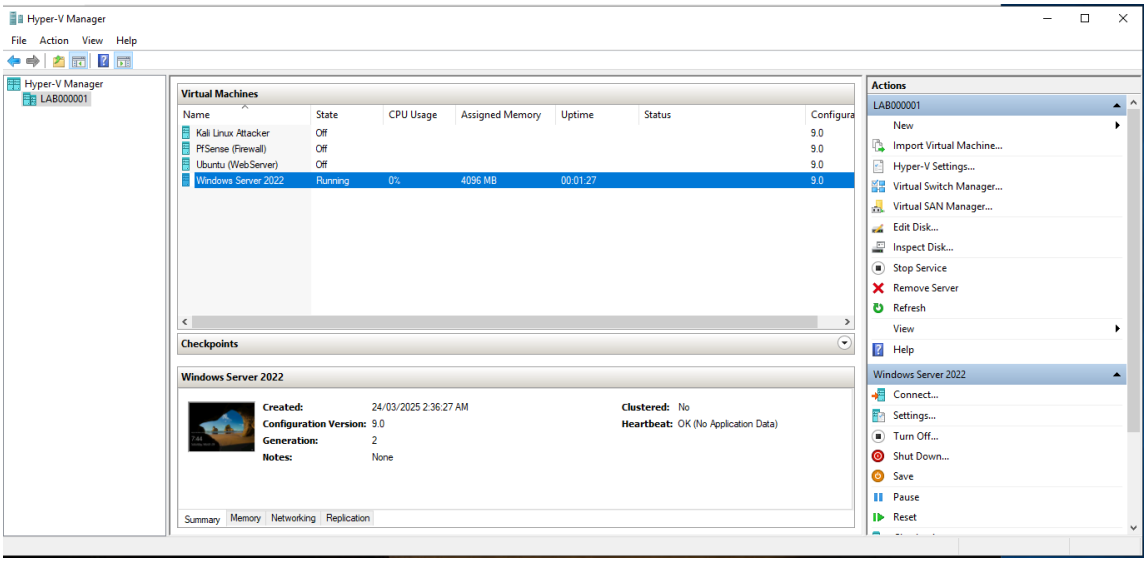
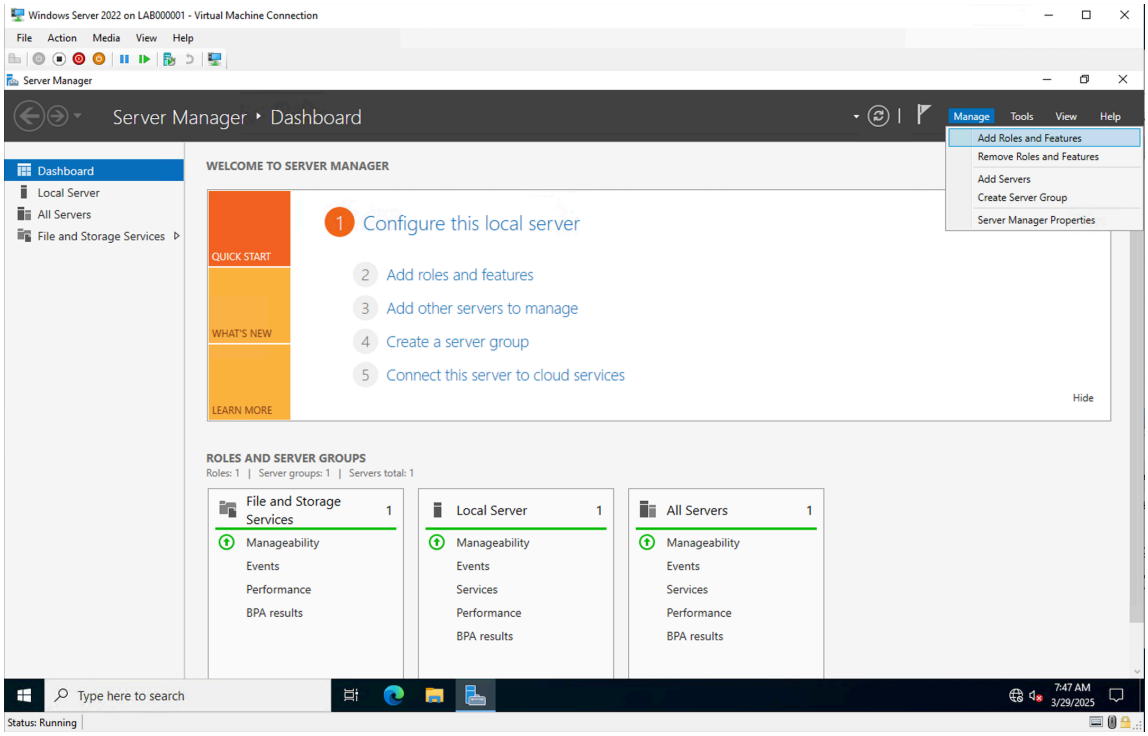
Implementing Basic Configurations in Windows Server 2022 – AD DS, Group Policies and SMB File Sharing

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

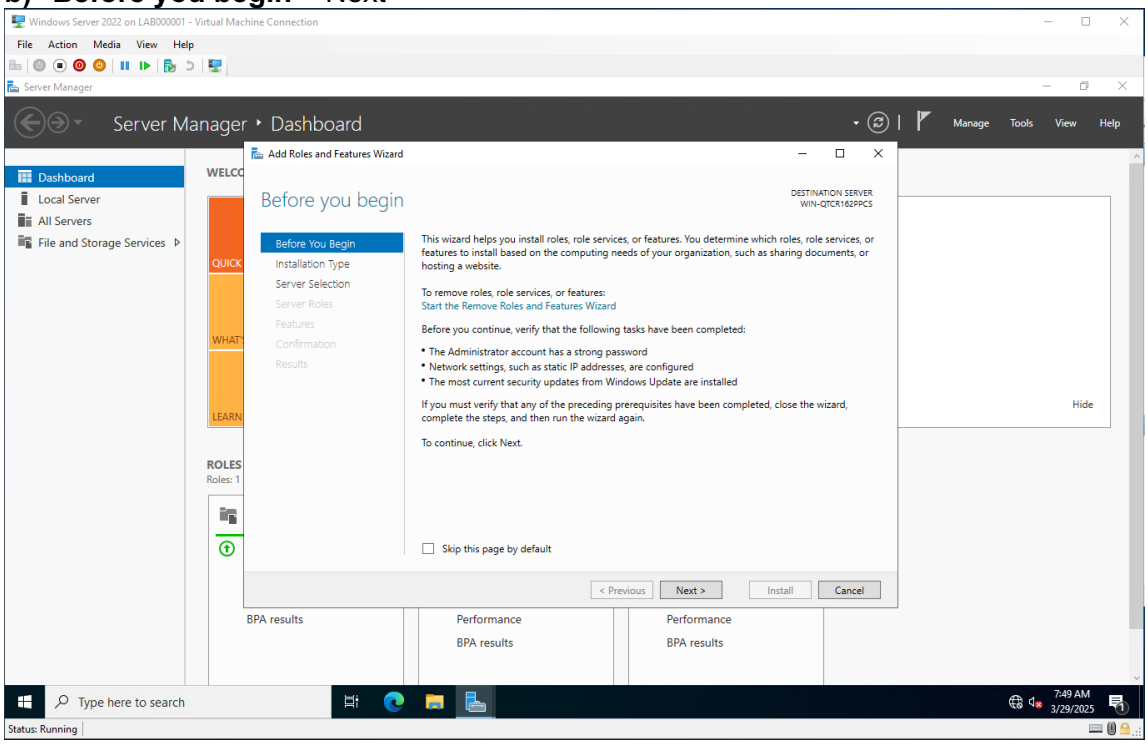


1. Install Active Directory Domain Services (AD DS):

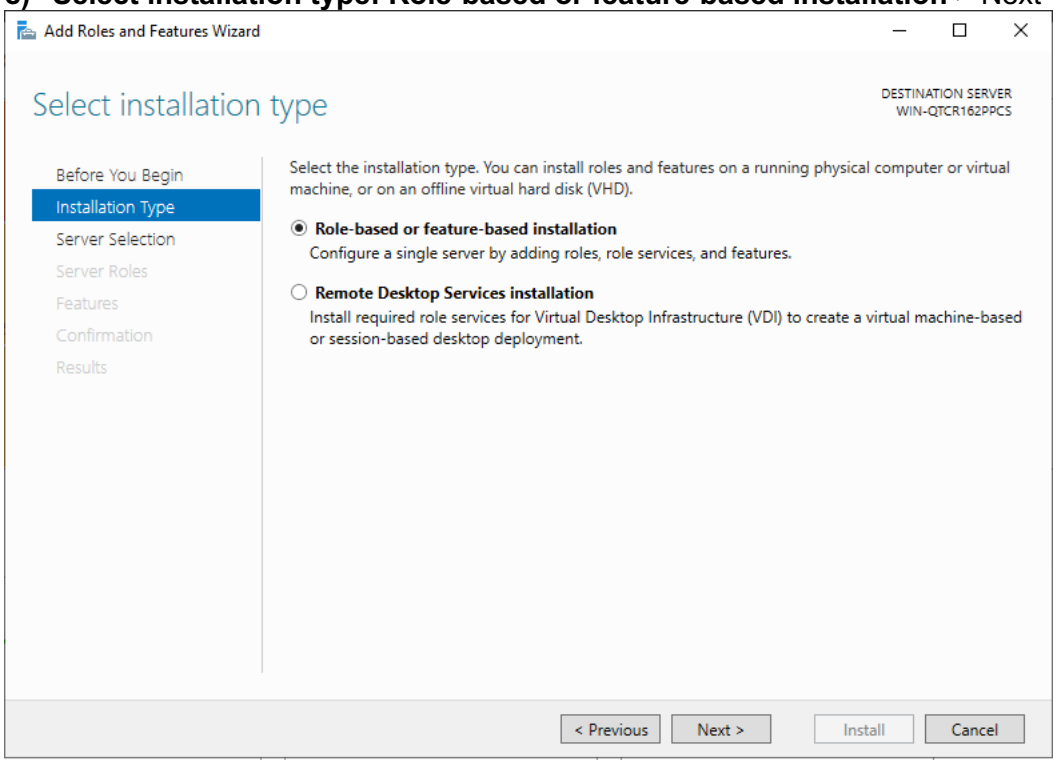
a) In Server Manager,
Click **Manage** on top right > **Add Roles and Features** OR
Click on **Add roles and features** in the **Dashboard**



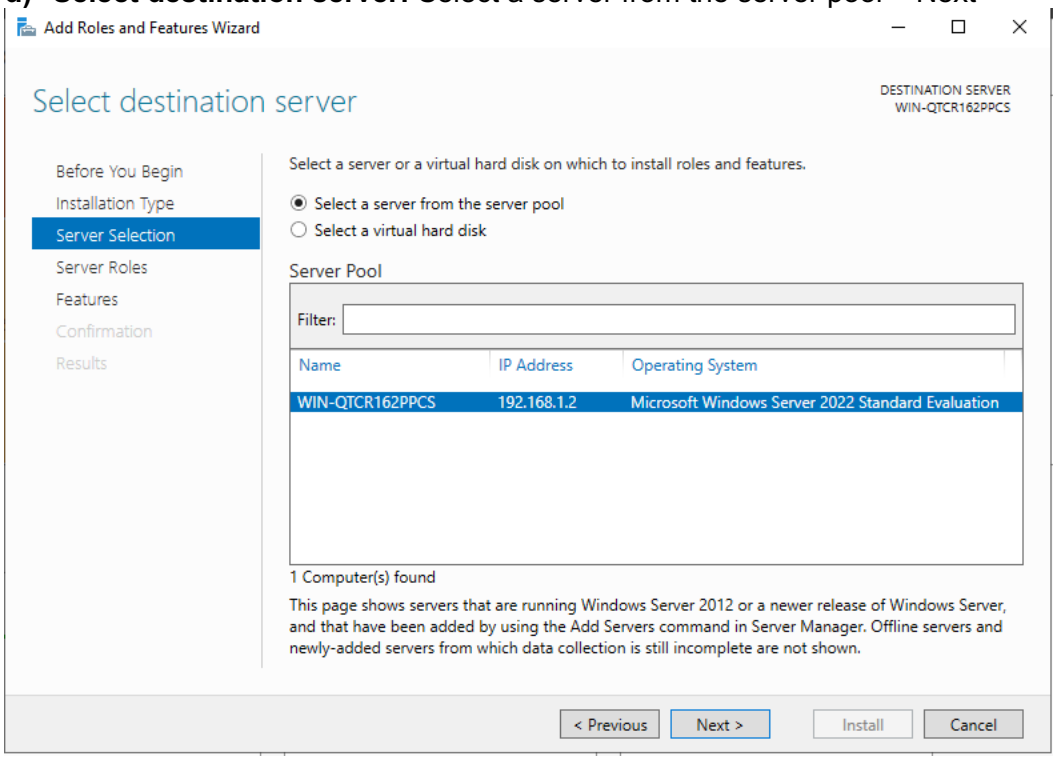
b) Before you begin > Next



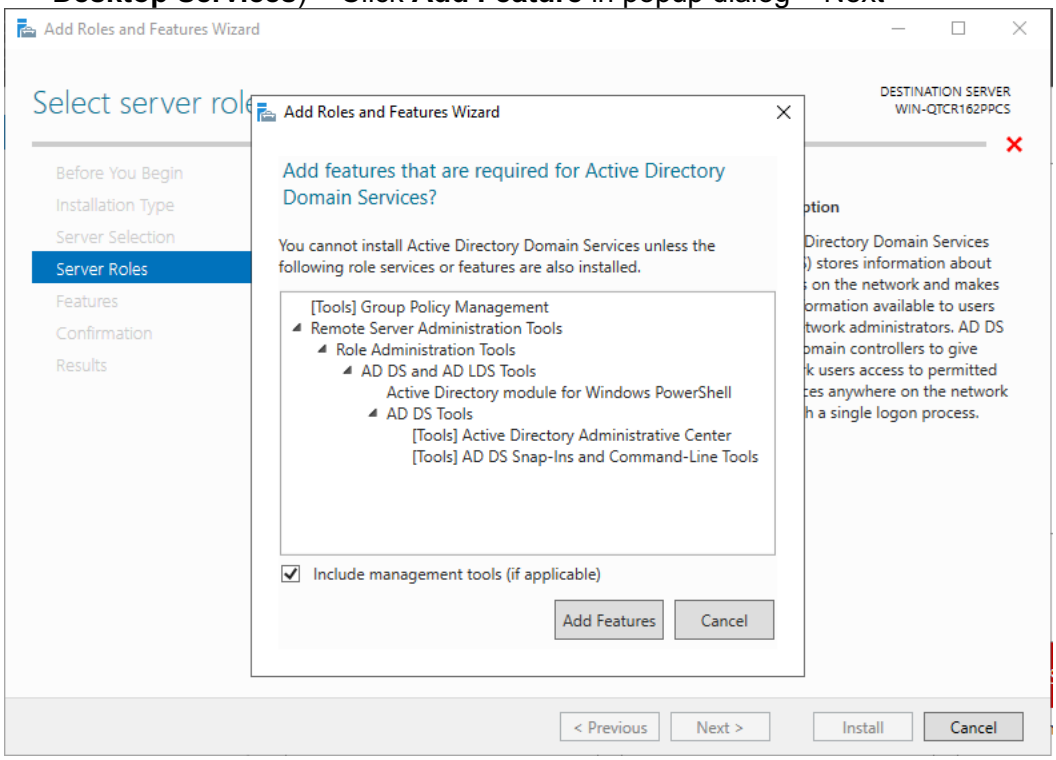
c) Select installation type: Role-based or feature-based installation > Next

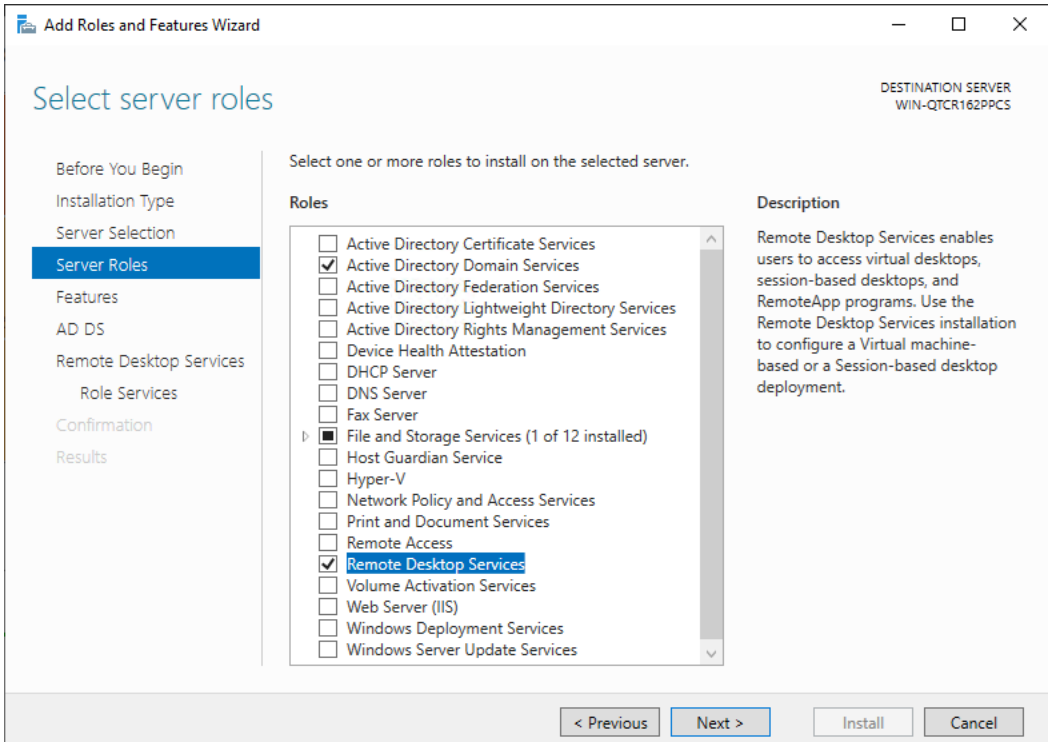


d) Select destination server: Select a server from the server pool > Next

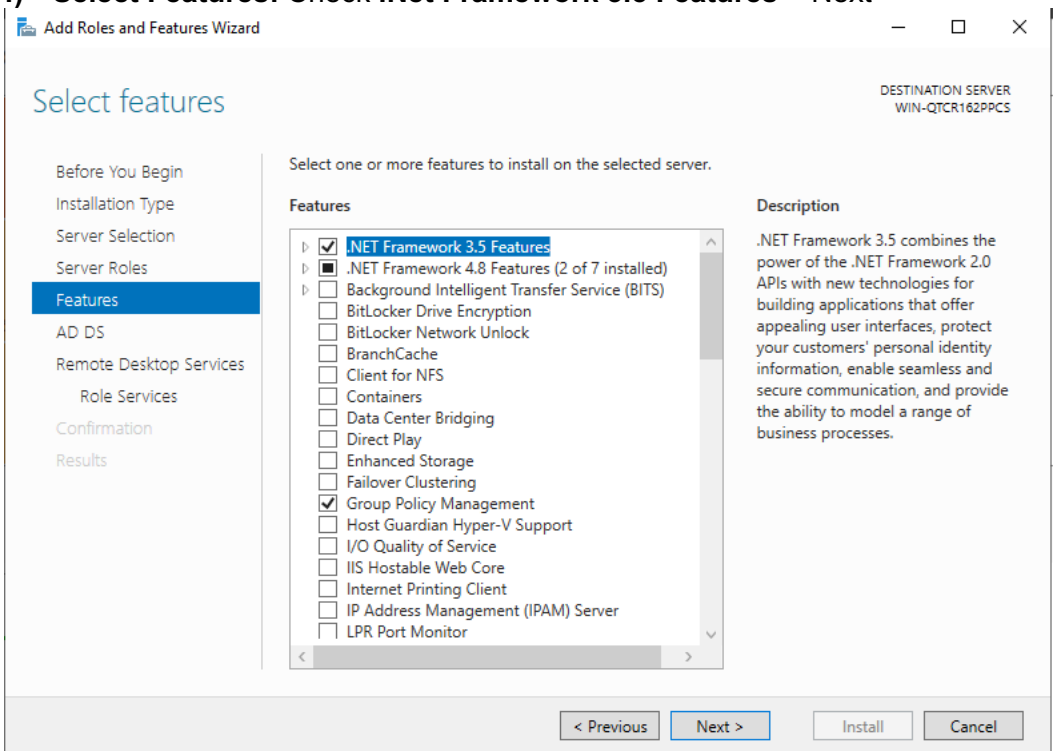


e) Select server roles:
Check **Active Directory Domain Services** (**Optional**: Check **Remote Desktop Services**) > Click **Add Feature** in popup dialog > Next

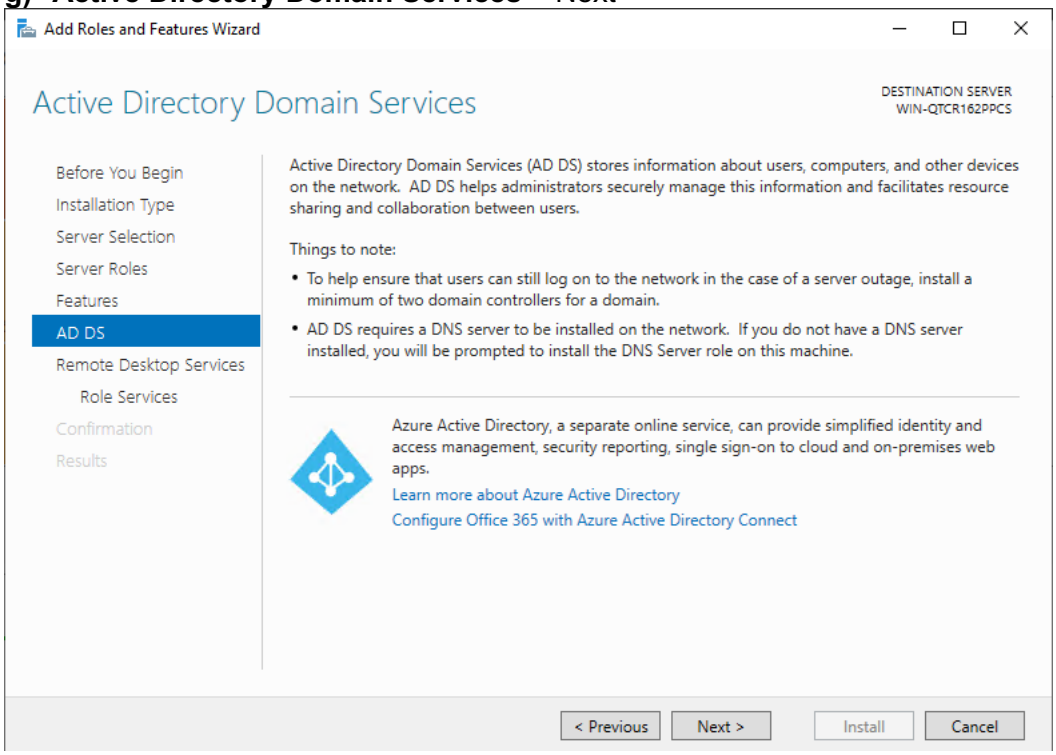




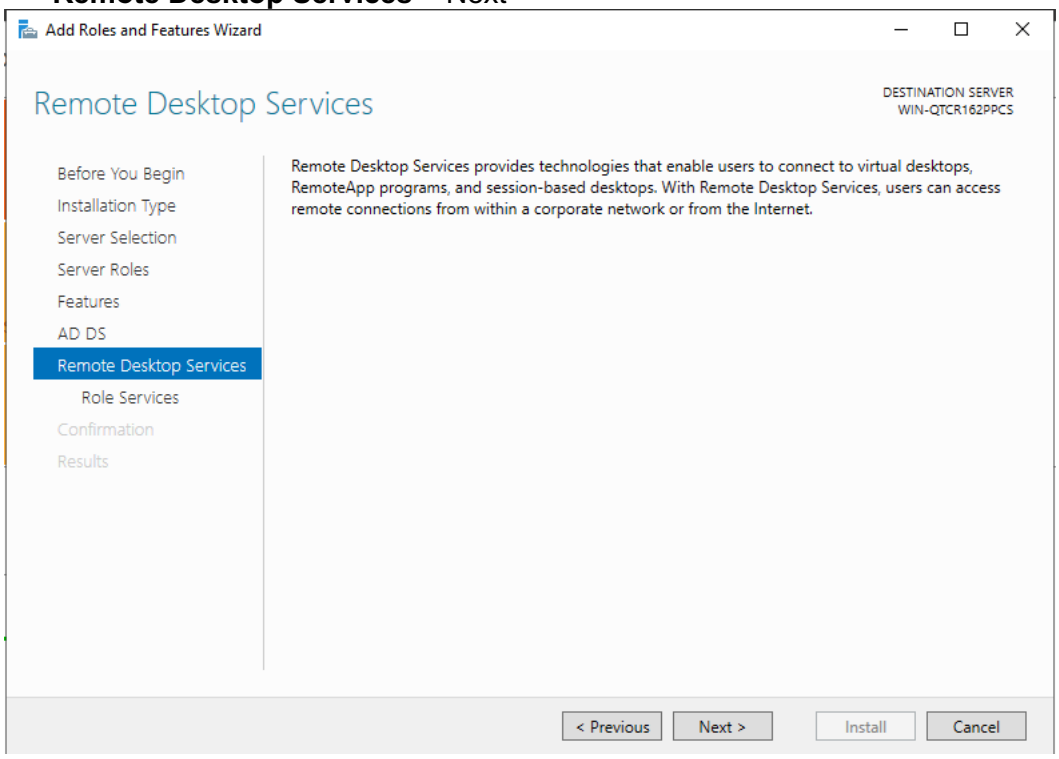
f) Select Features: Check **.Net Framework 3.5 Features** > Next



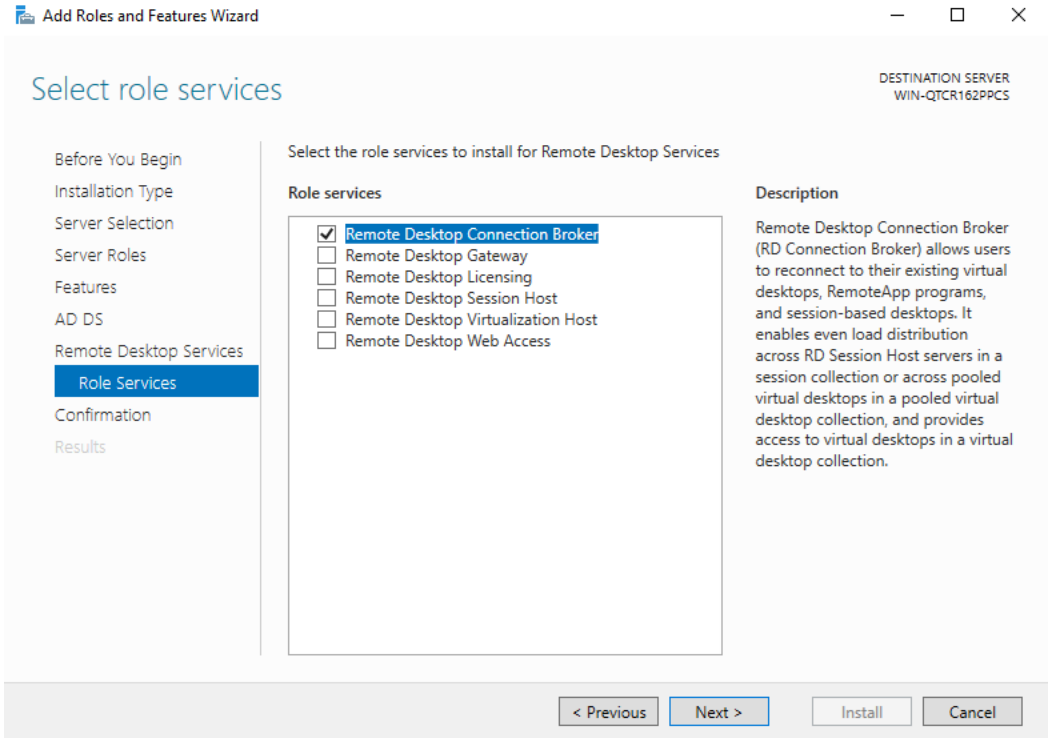
g) **Active Directory Domain Services** > Next



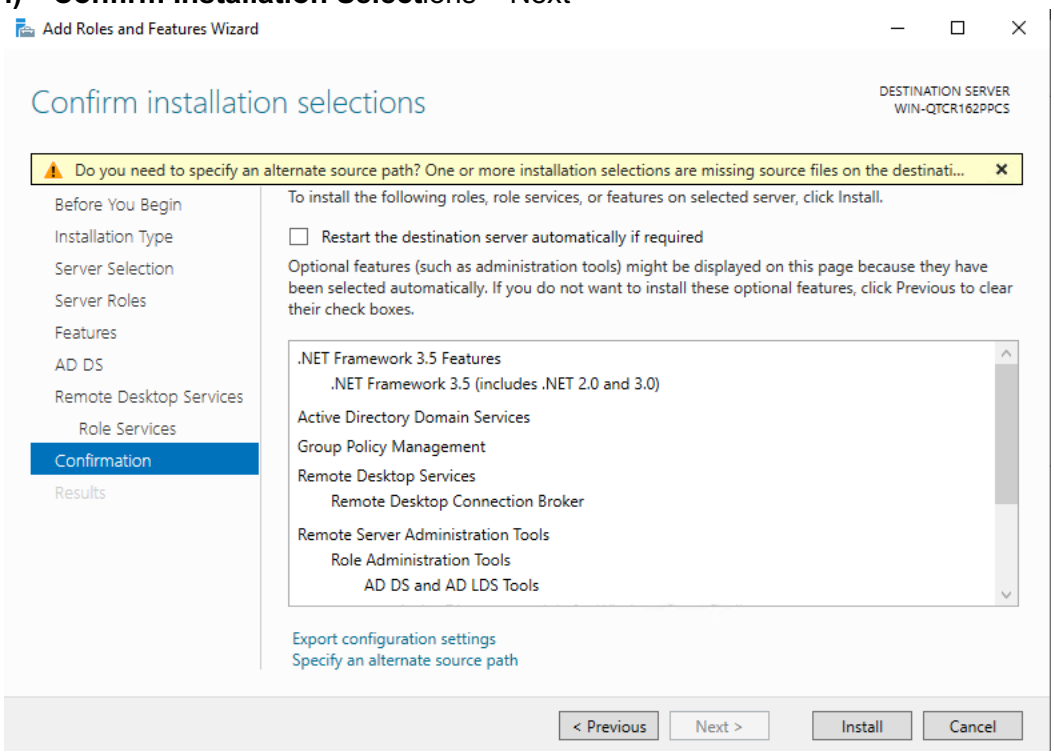
If you also selected Remote Desktop Services with AD DS,
Remote Desktop Services > Next



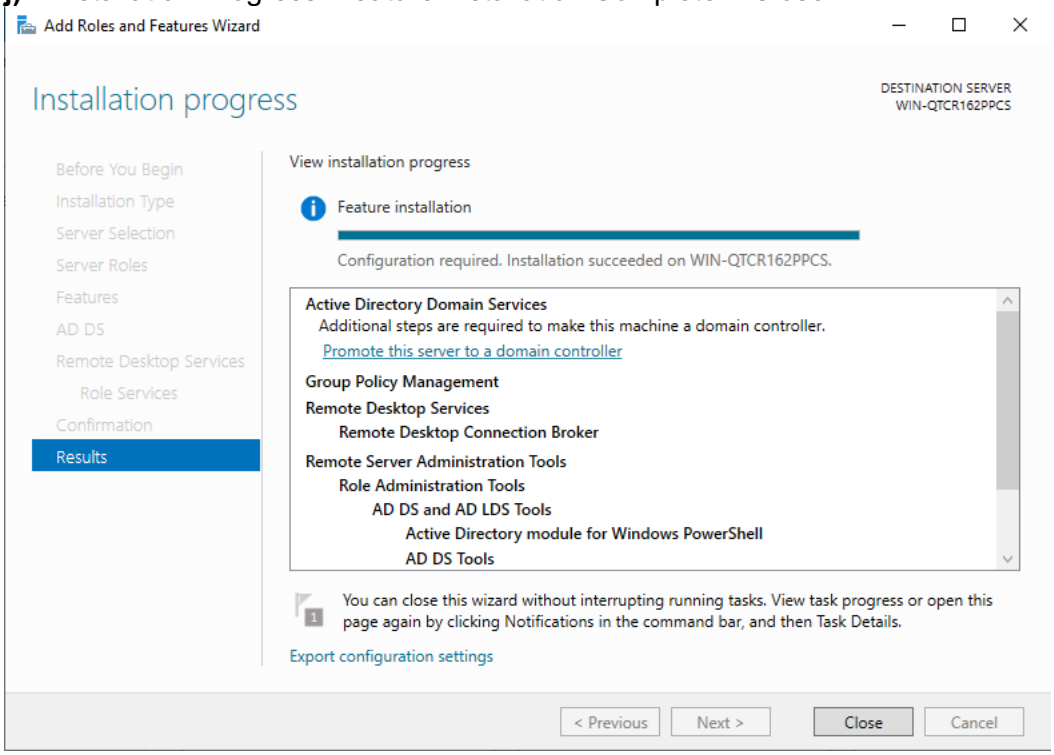
h) Check **Remote Desktop Connection Broken** > Click **Add Feature** in popup dialog > Next



i) **Confirm Installation Selections** > Next

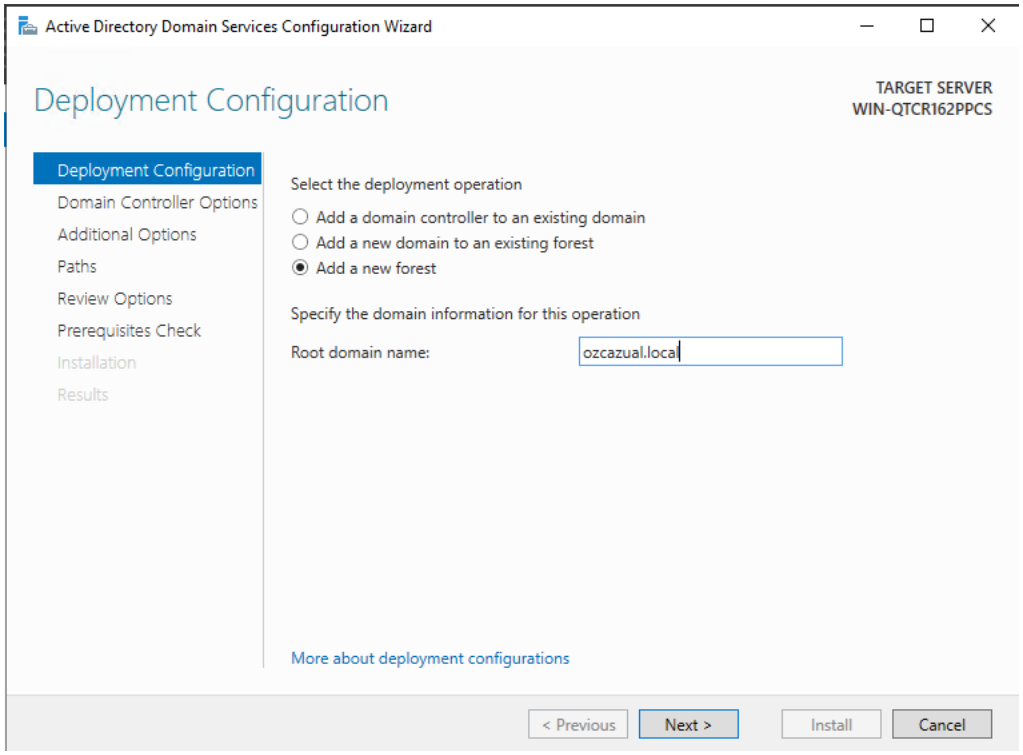


j) Installation Progress: Feature Installation Complete > Close

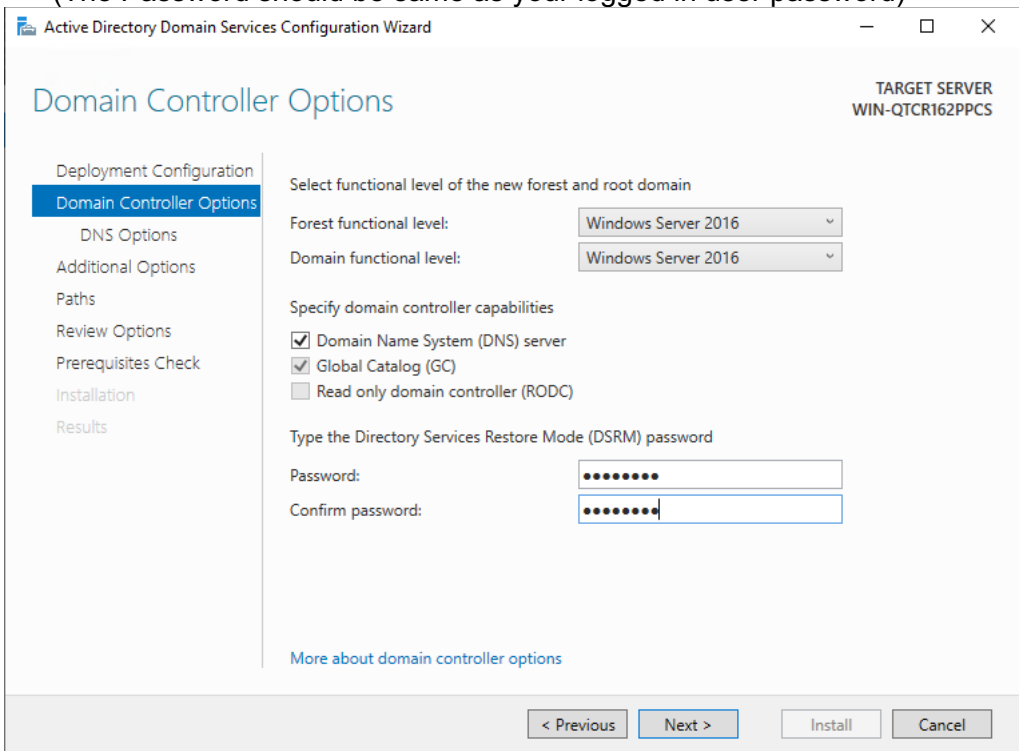


2. Promote Server to Domain Controller

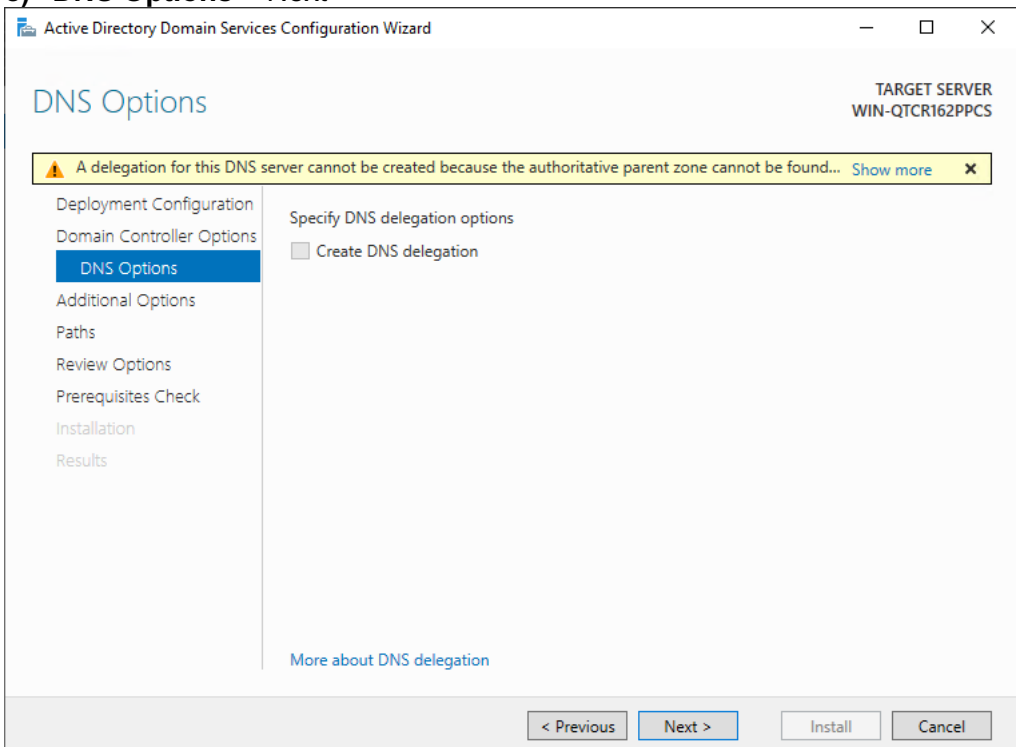
a) Click on the **Flag icon on top right** > **Promote this server to a domain controller**
In the **Active Directory Domain Wizard,**
Deployment Configuration: Select **Add a new forest**
Root domain name: **[domain_name].local** > Next



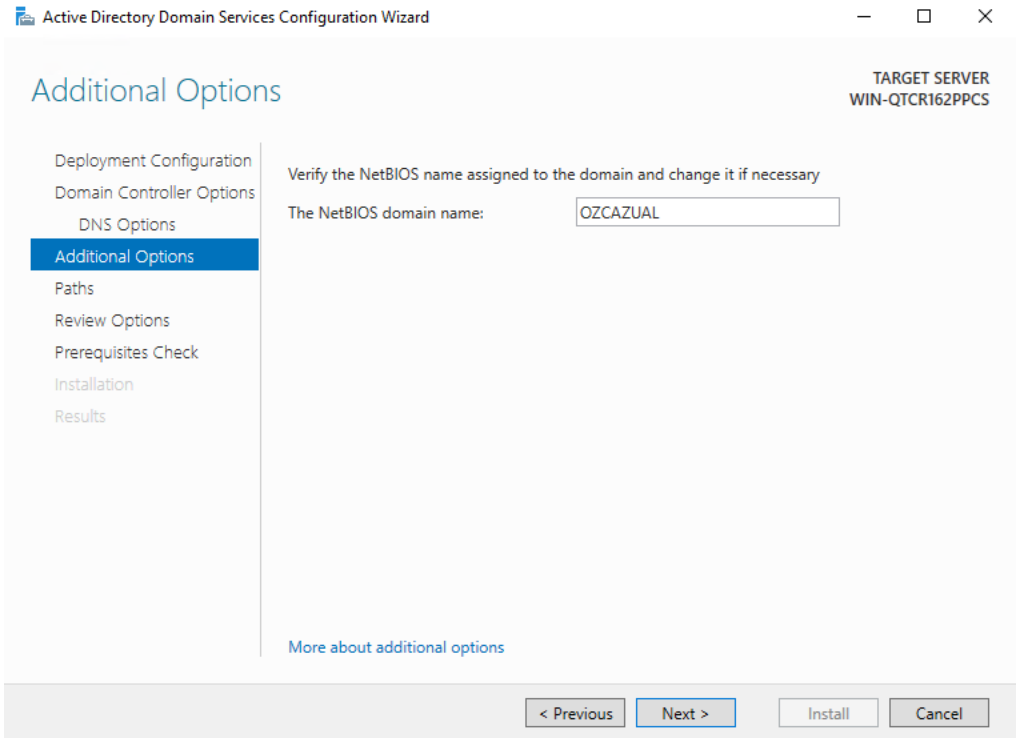
b) Domain Controller Options:
Password: **[your_password]** > Next
(The Password should be same as your logged in user password)



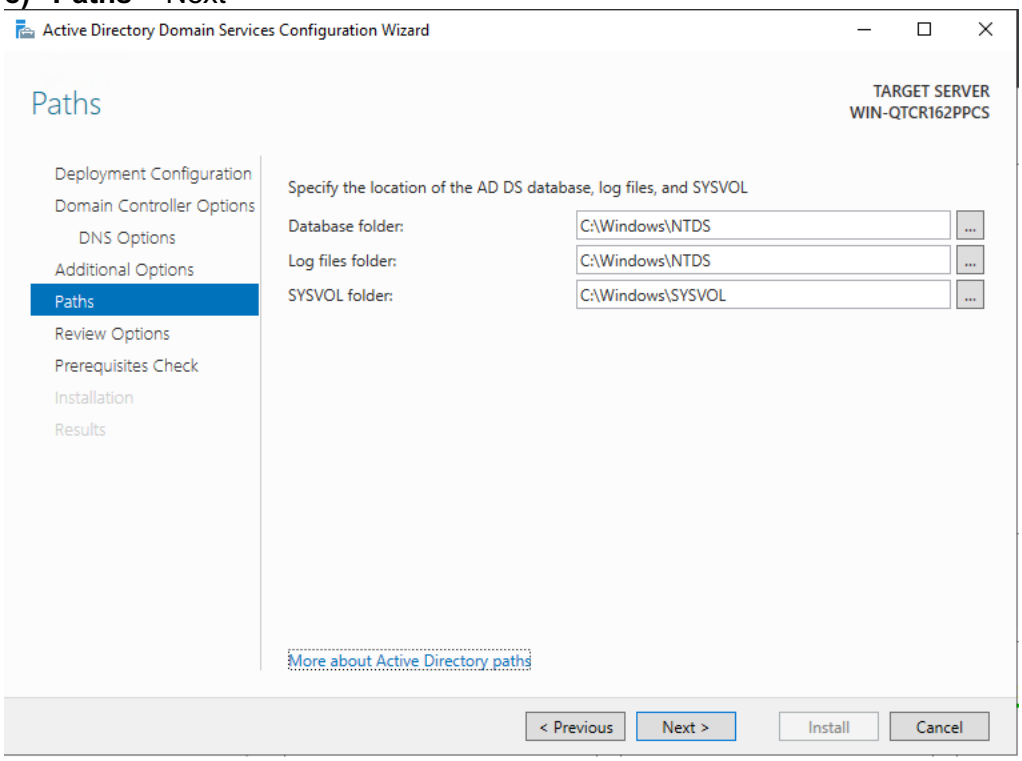
c) DNS Options > Next



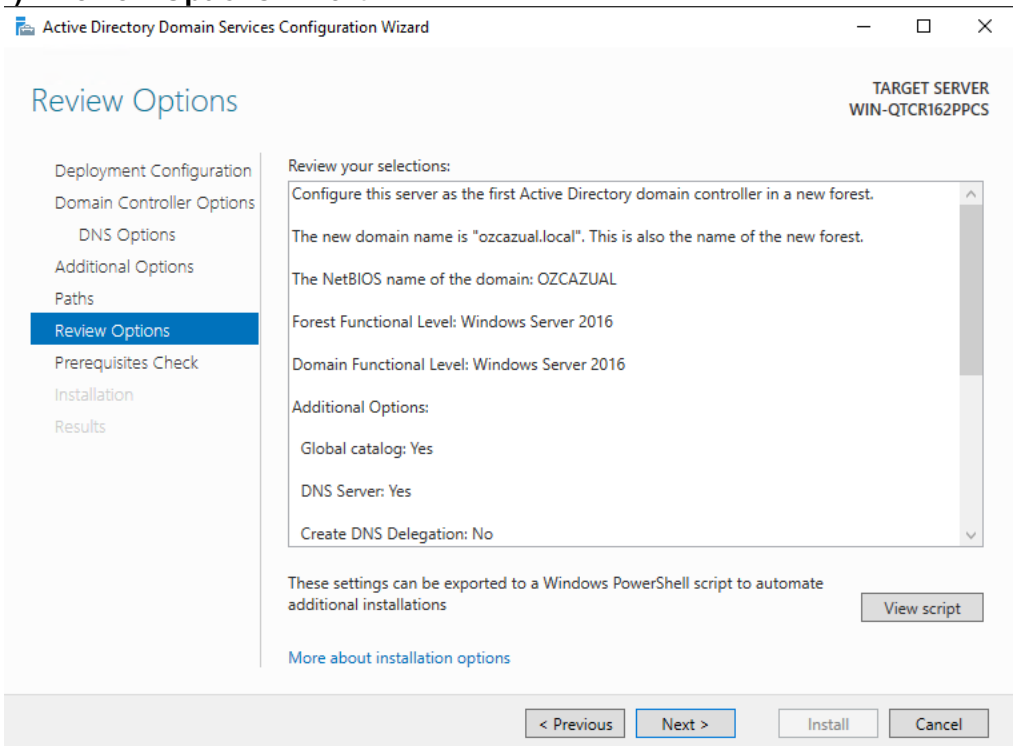
d) Additional Options: Check the NetBIOS domain name matches the .local forest you created at first step in this wizard (Case-Insensitive) > Next



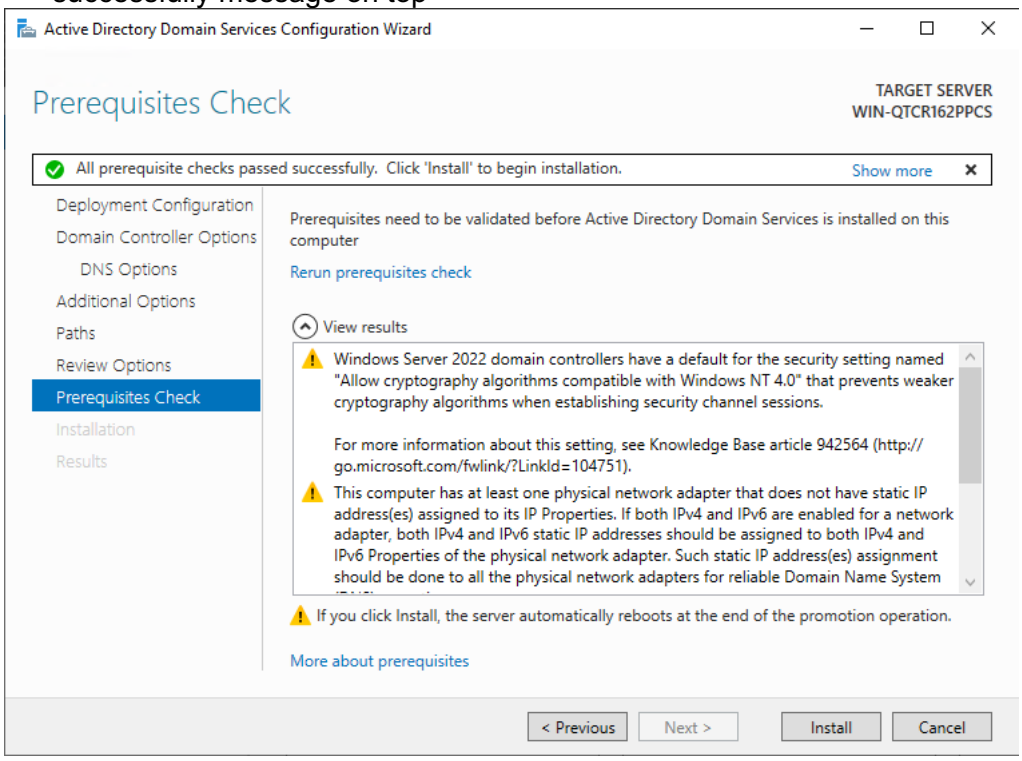
e) Paths > Next



f) Review Options > Next

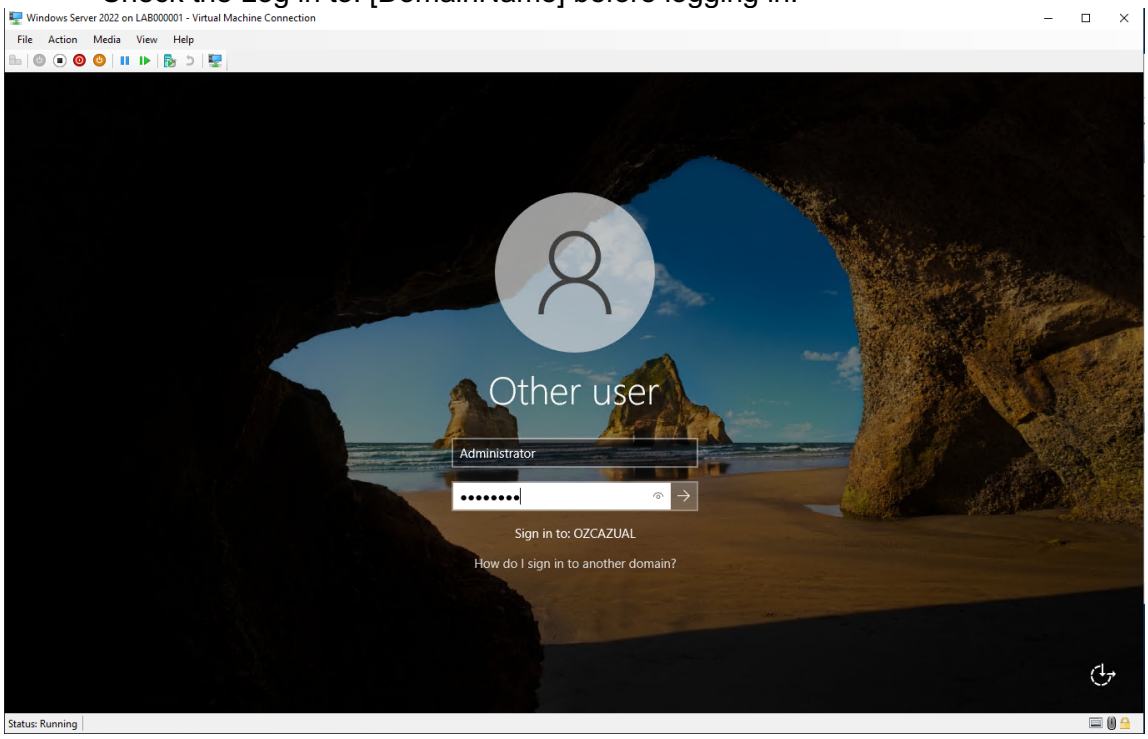


g) Prerequisites Check: Click **Install** only if see All prerequisite check passed successfully message on top

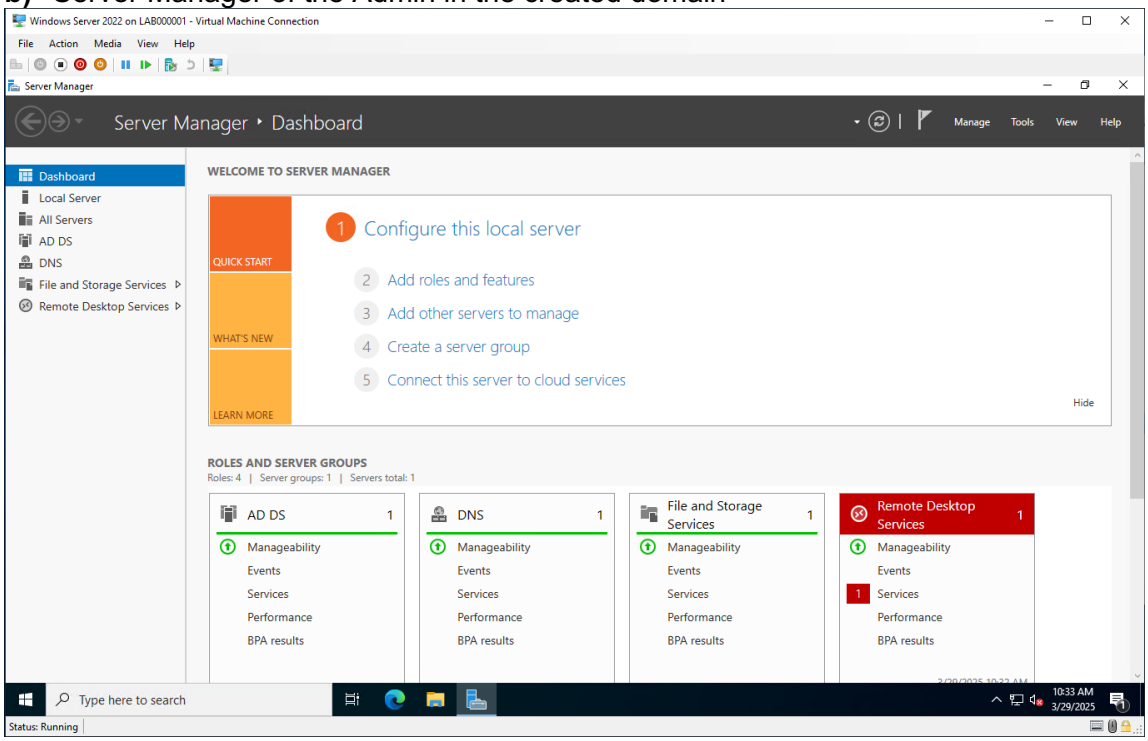


3. Post Installation Configuration

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

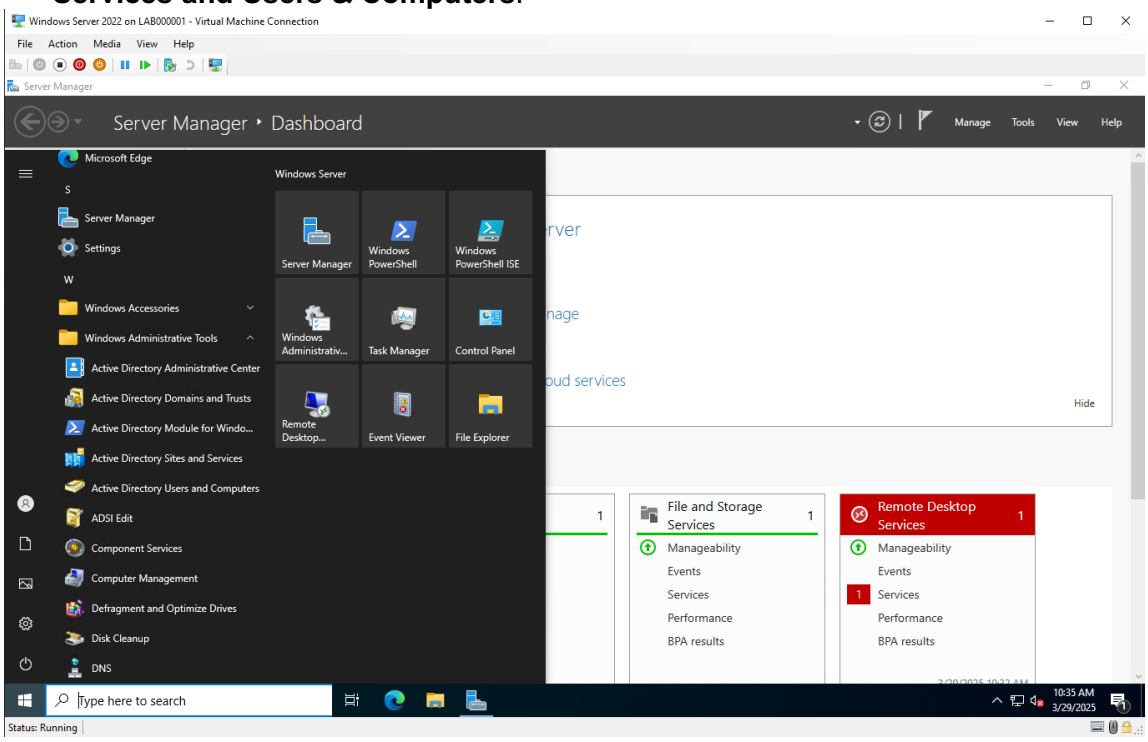


b) Server Manager of the Admin in the created domain



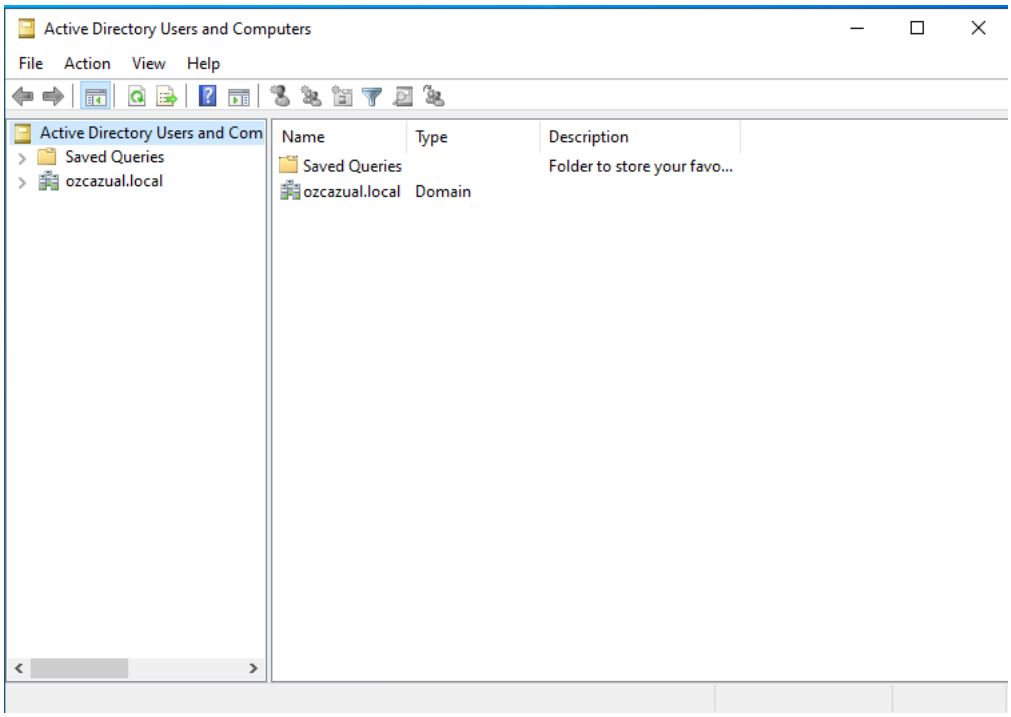
4. Verify AD DS Installation

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

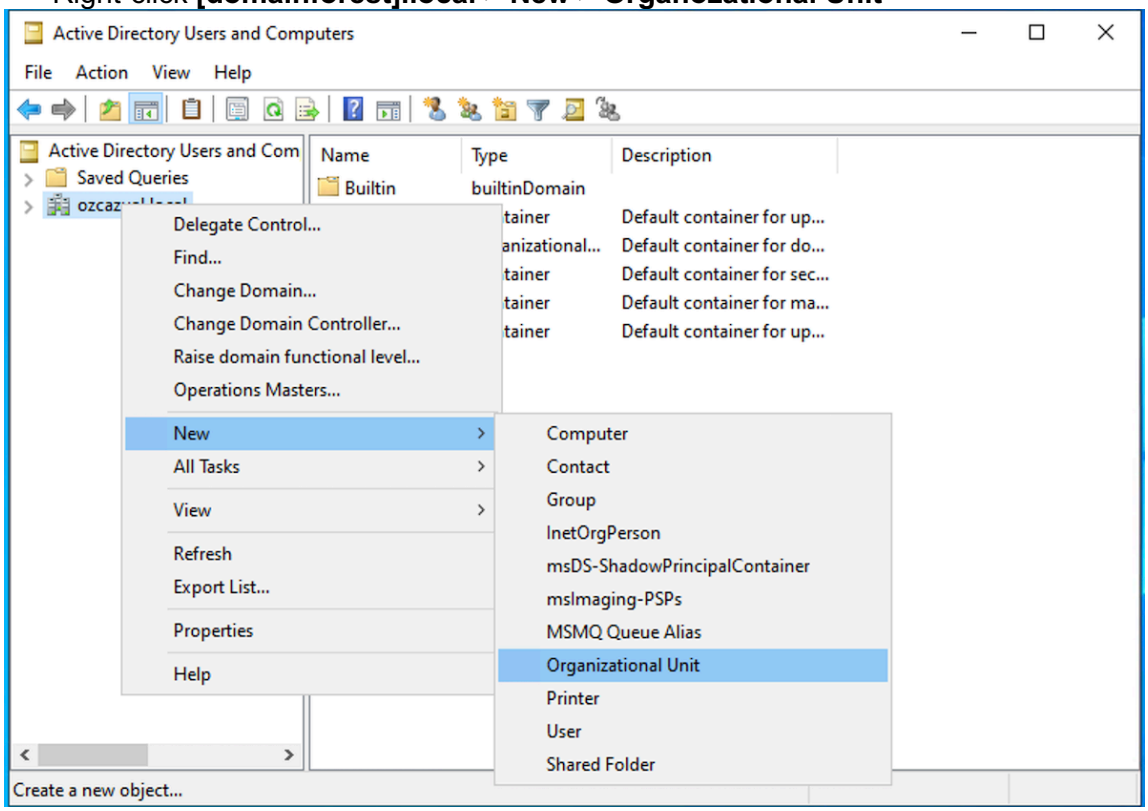


5. Configuring AD DS for User Authentication

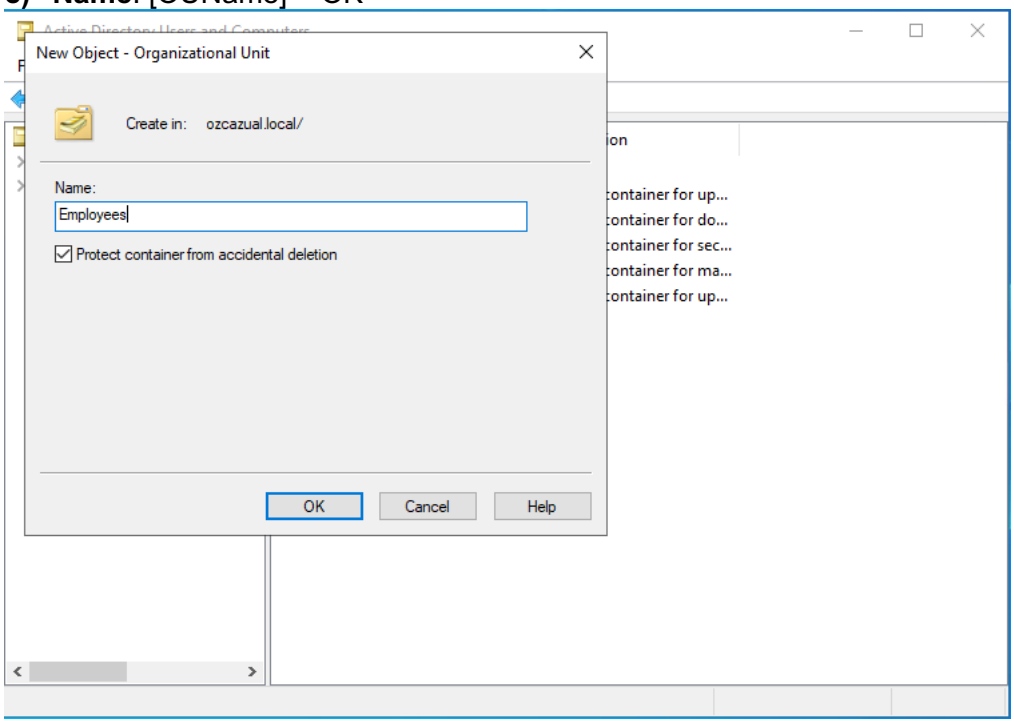
a) Go to **Start > Windows Administrative Tools > Active Directory Users and Computers**



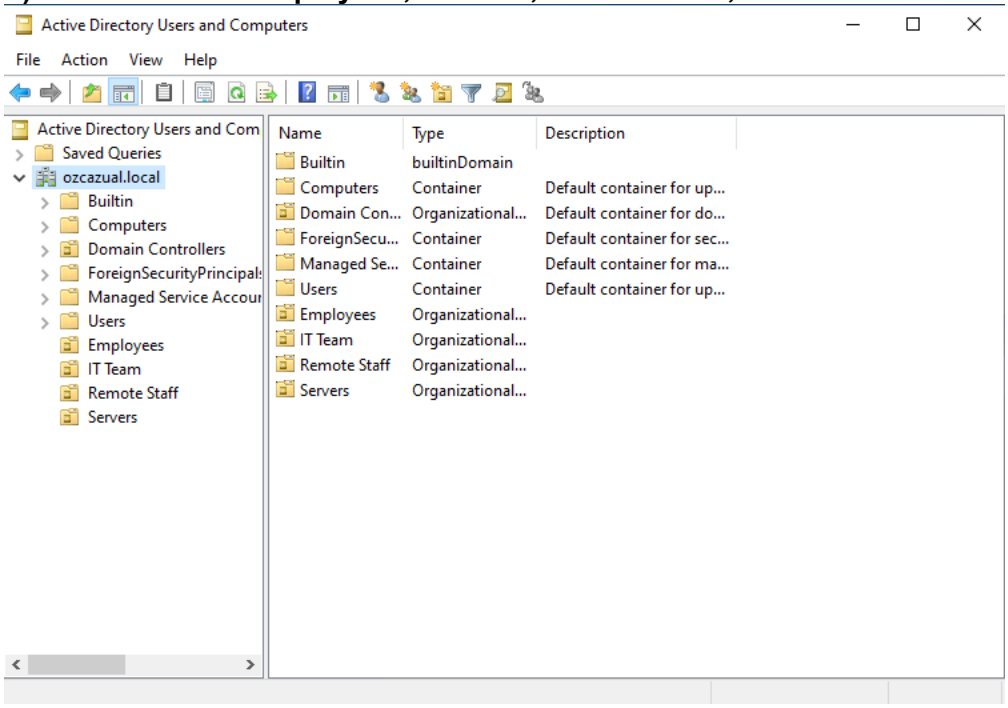
b) Create Organizational Units:
Right-click **[domainforest].local > New > Organozational Unit**



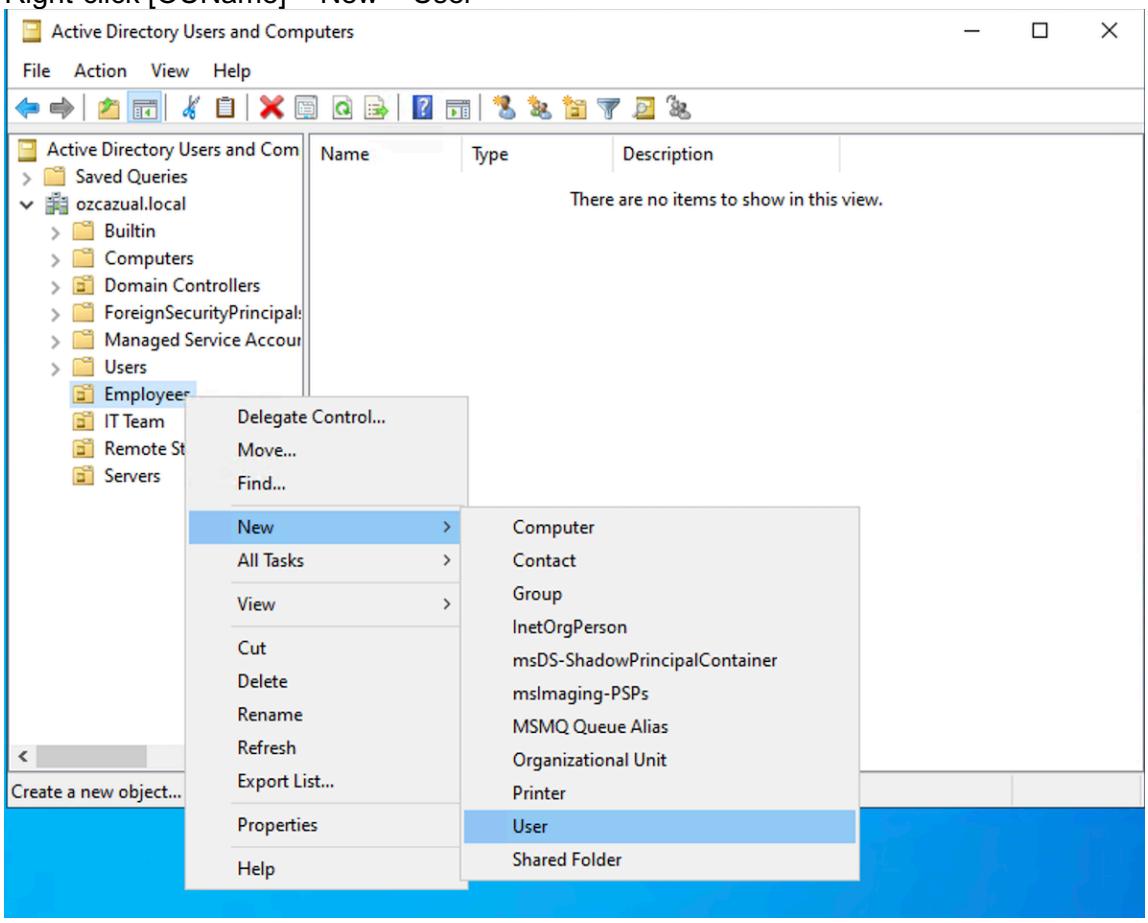
c) Name: [OUName] > OK



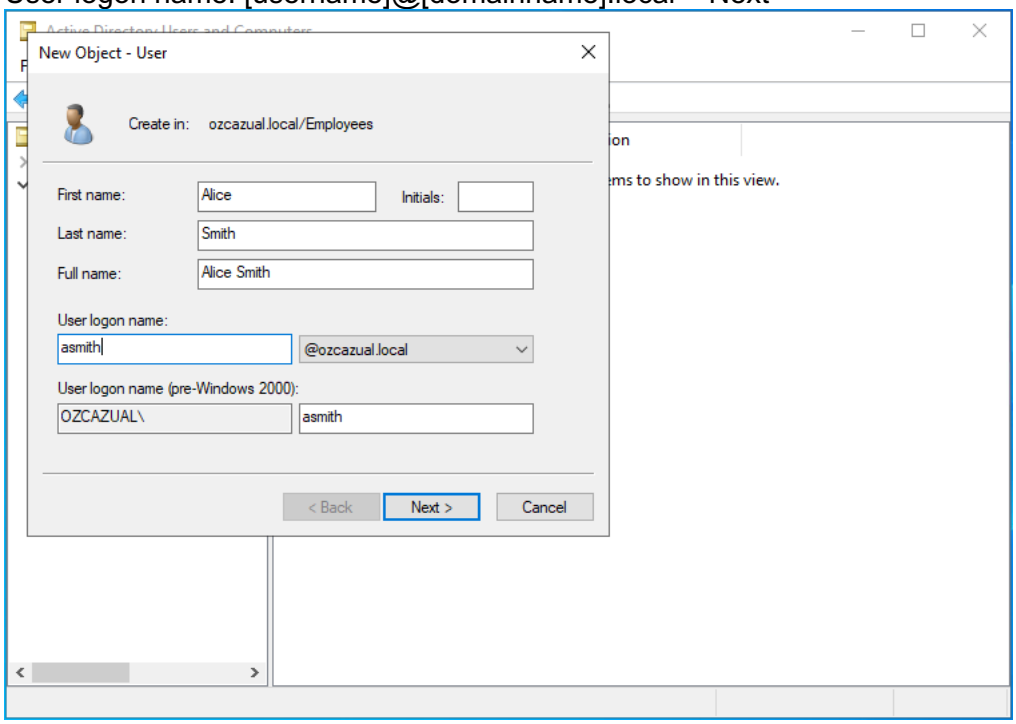
d) Created OUs: Employees, IT Team, Remote Staff, Servers



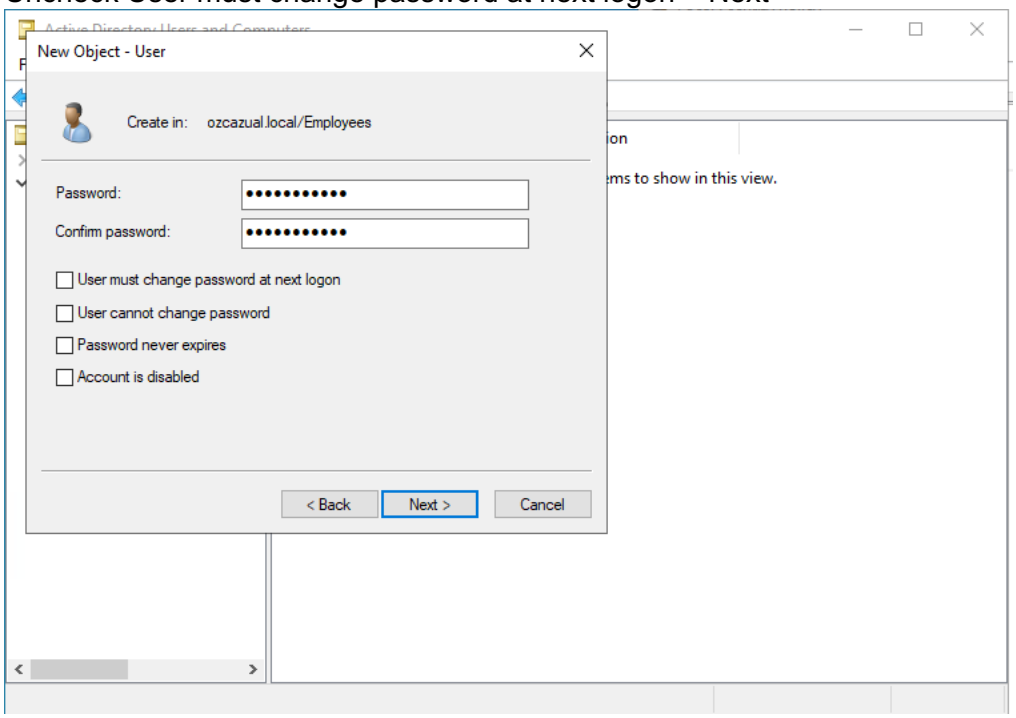
e) Create Users in OUs:
Right-click [OUName] > New > User



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

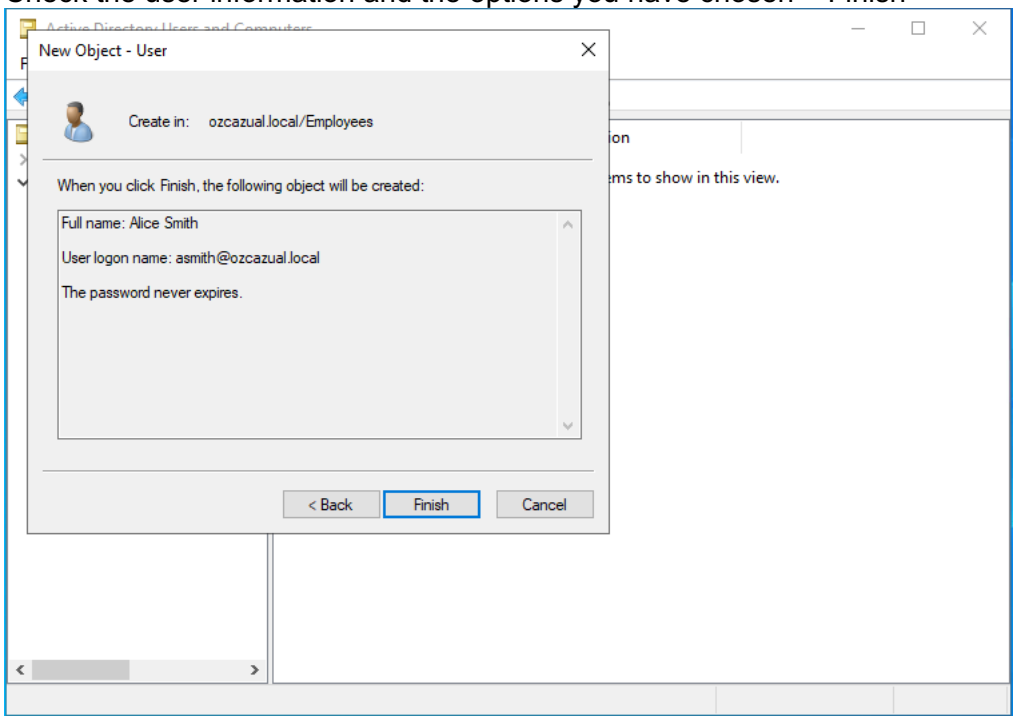


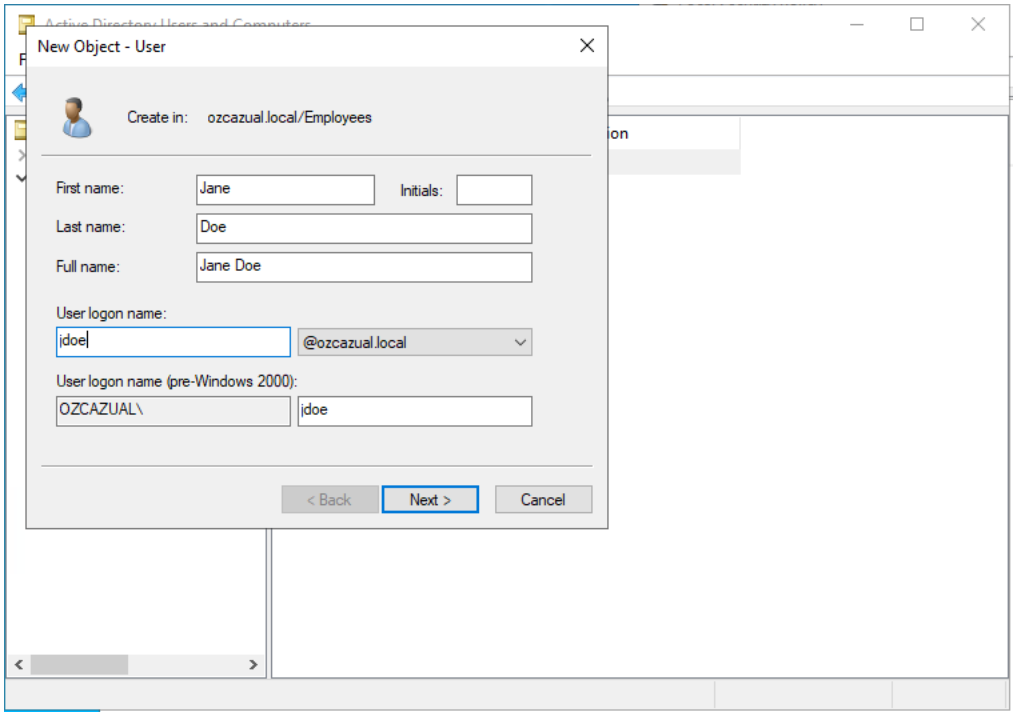
g) Create Password:
Password: [ypur_Password]
Uncheck User must change password at next logon > Next

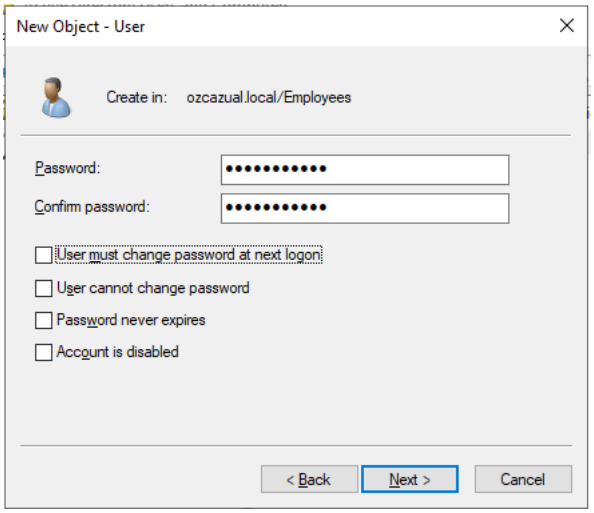


As0zcemp001

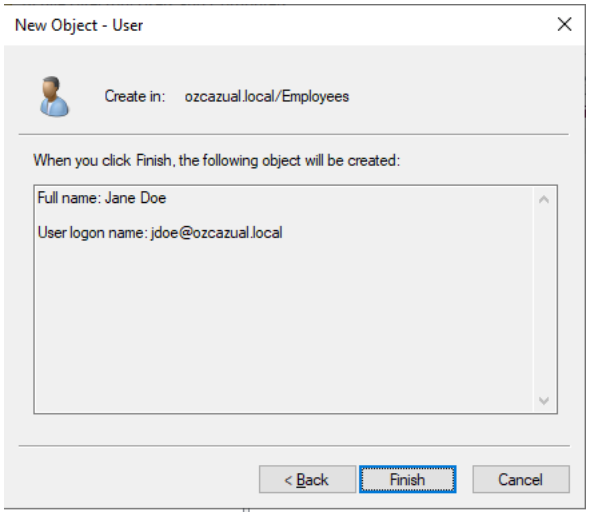
h) Check the user information and the options you have chosen > Finish

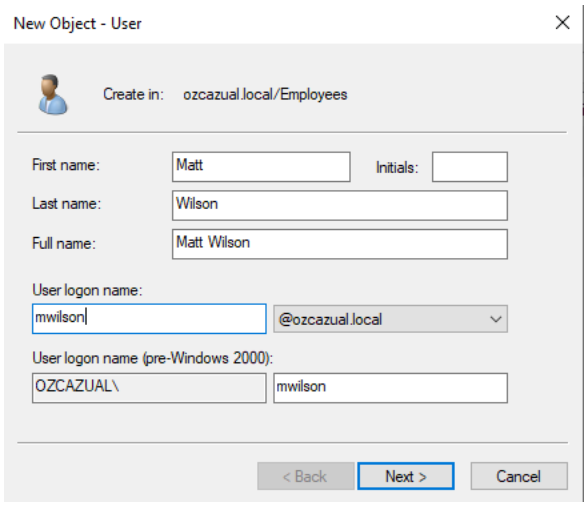


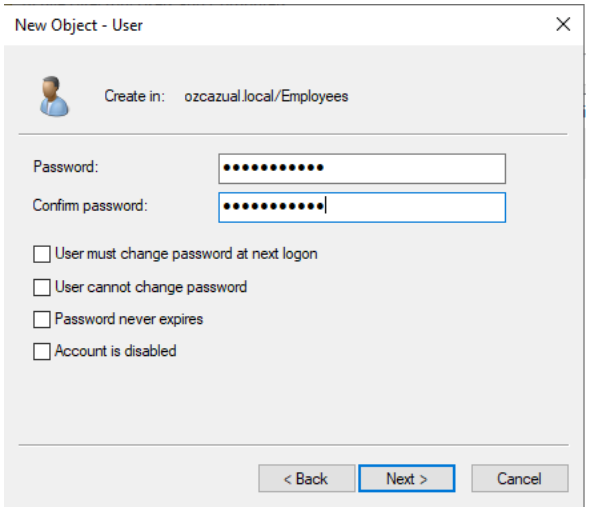




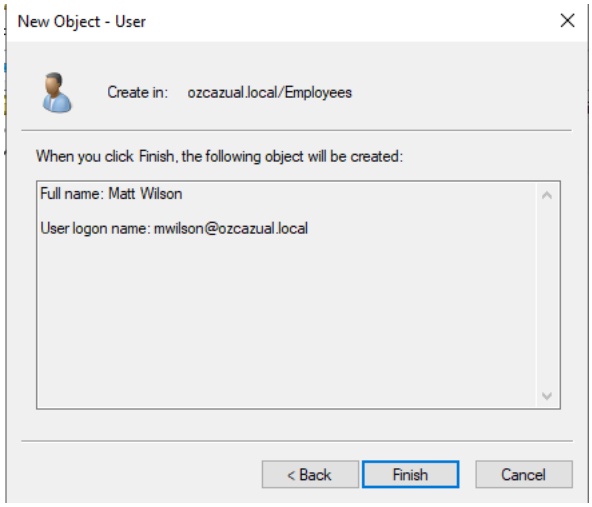
Jd0zcemp002



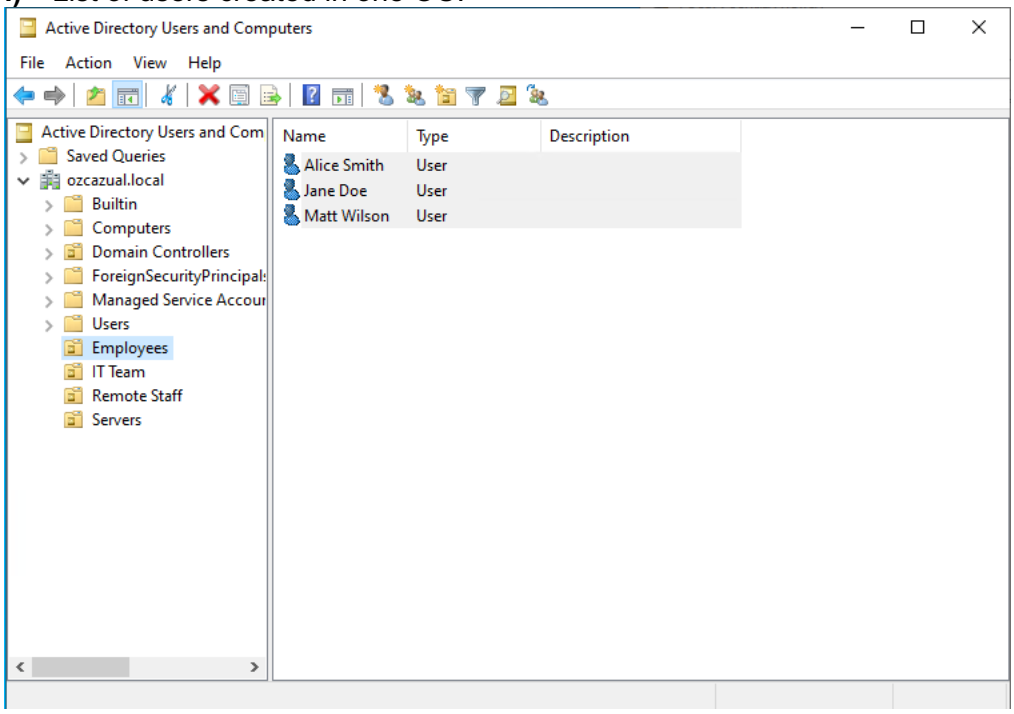




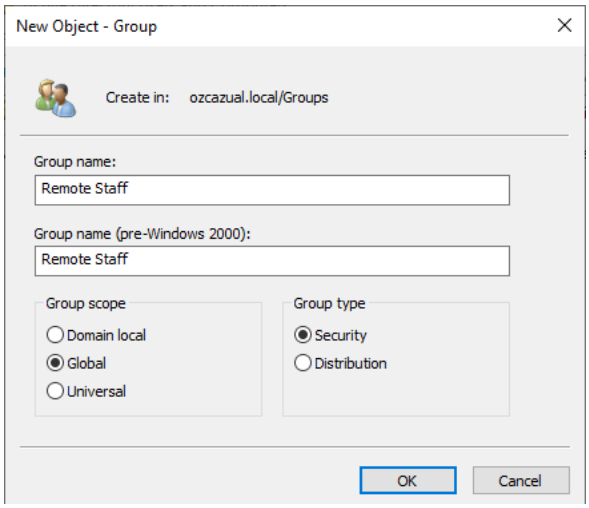
Mw0zcemp003

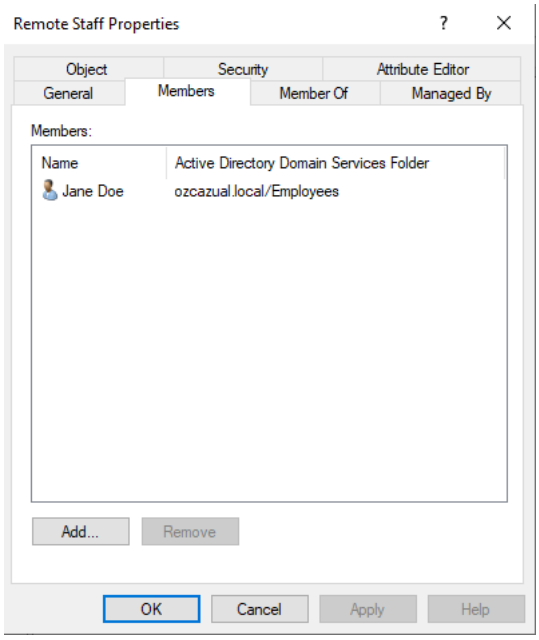


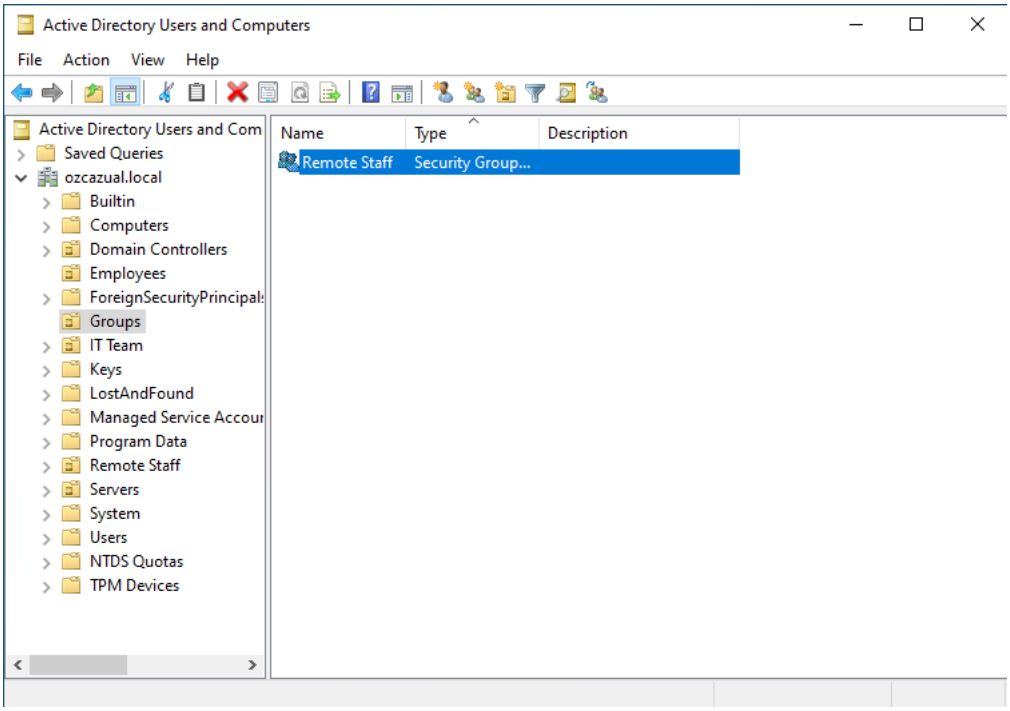
i) List of users created in one OU:

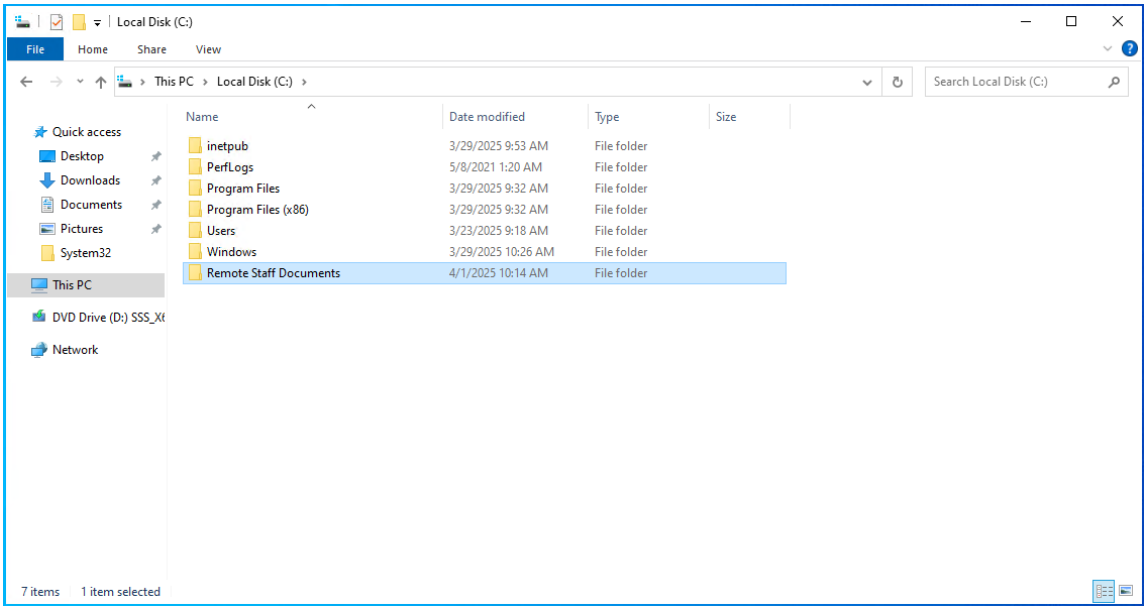


6. Create a Group Security Policy

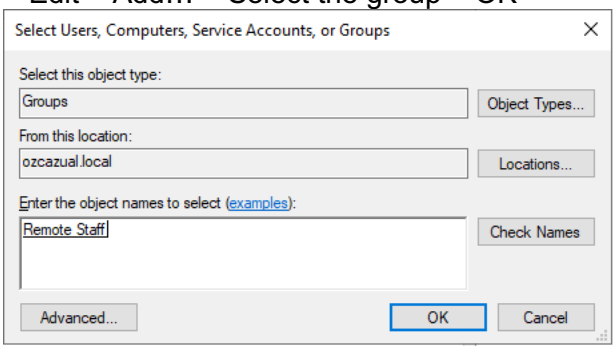




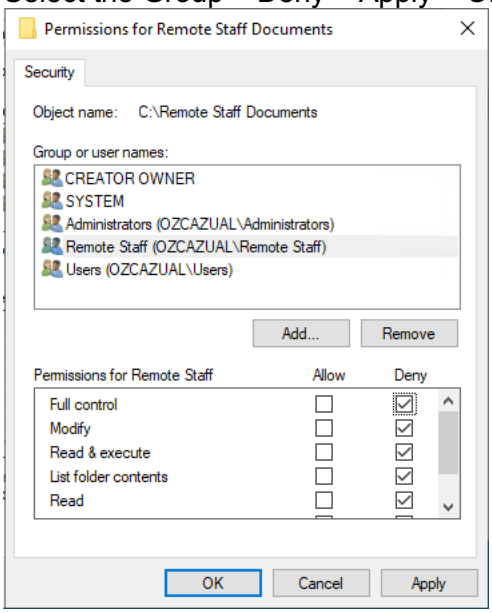




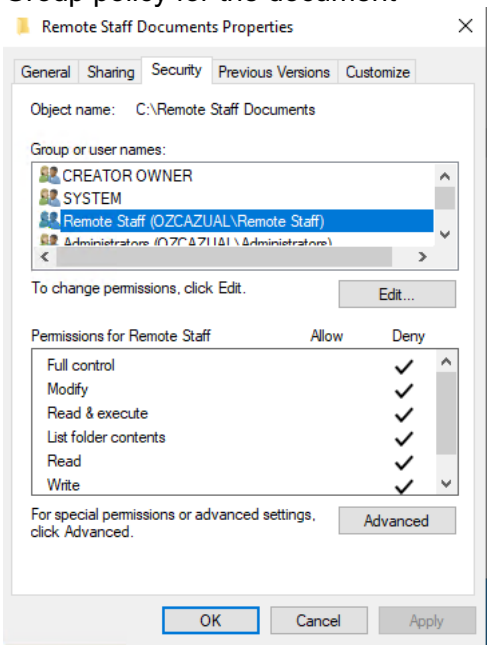
Right-click Remote Staff Documents > Properties > Security tab > Group or user names > Edit > Add… > Select the group > OK



Select the Group > Deny > Apply > OK

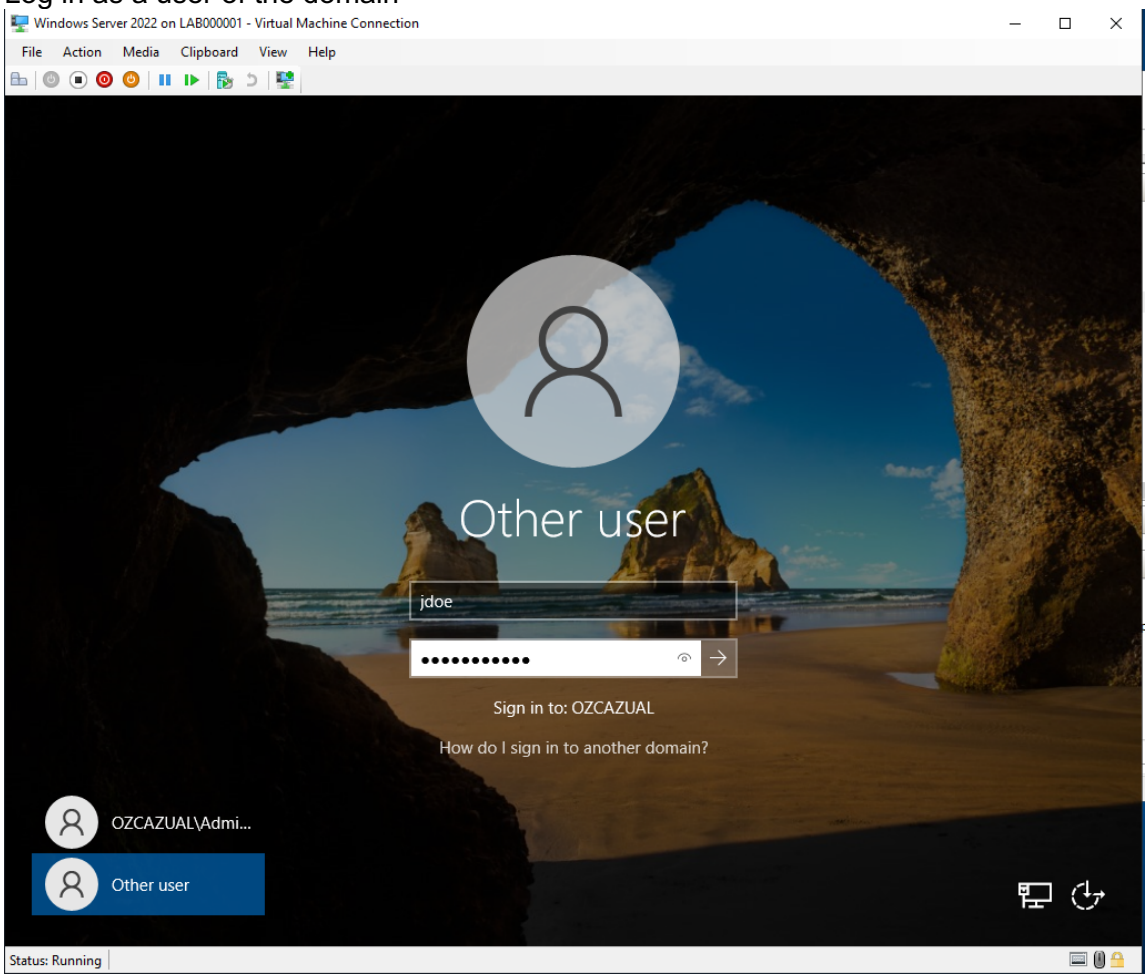


Group policy for the document

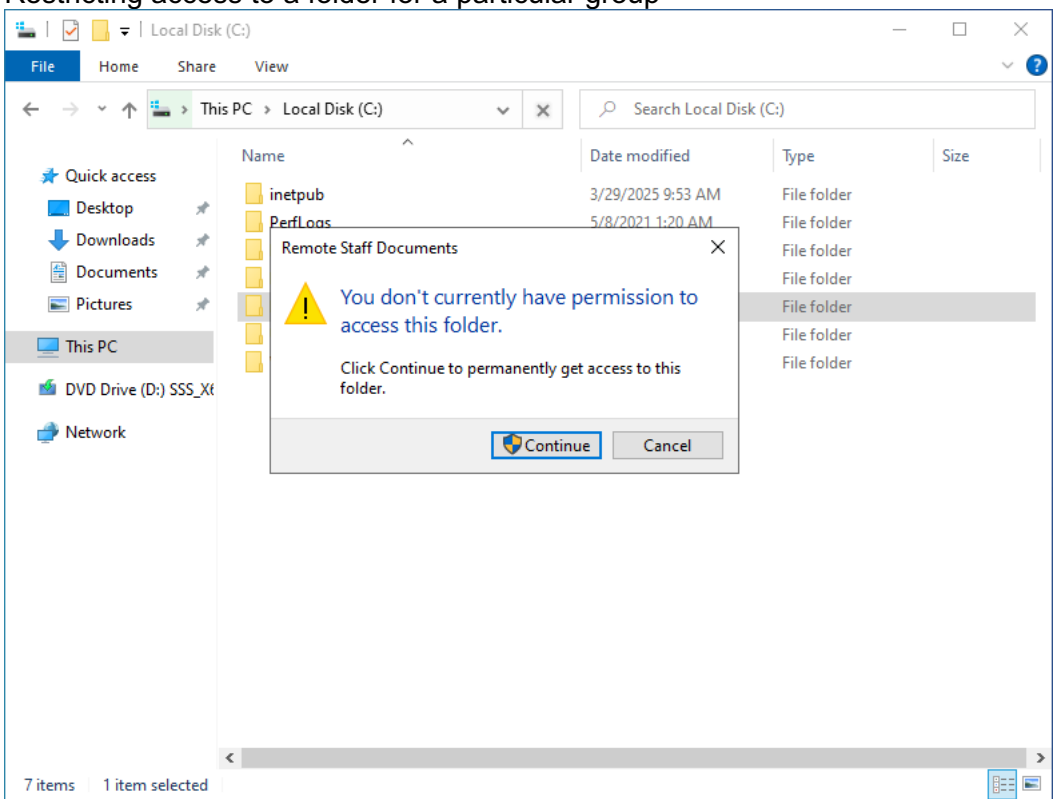


7. Test Access Privileges

Log in as a user of the domain

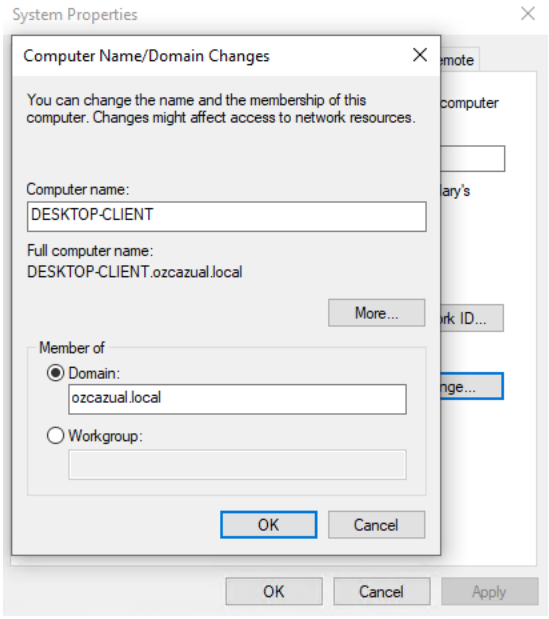


Restricting access to a folder for a particular group

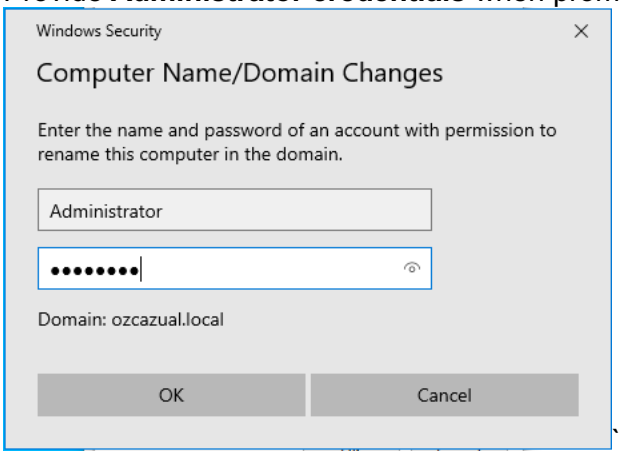


Test Login from a Client Machine

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**

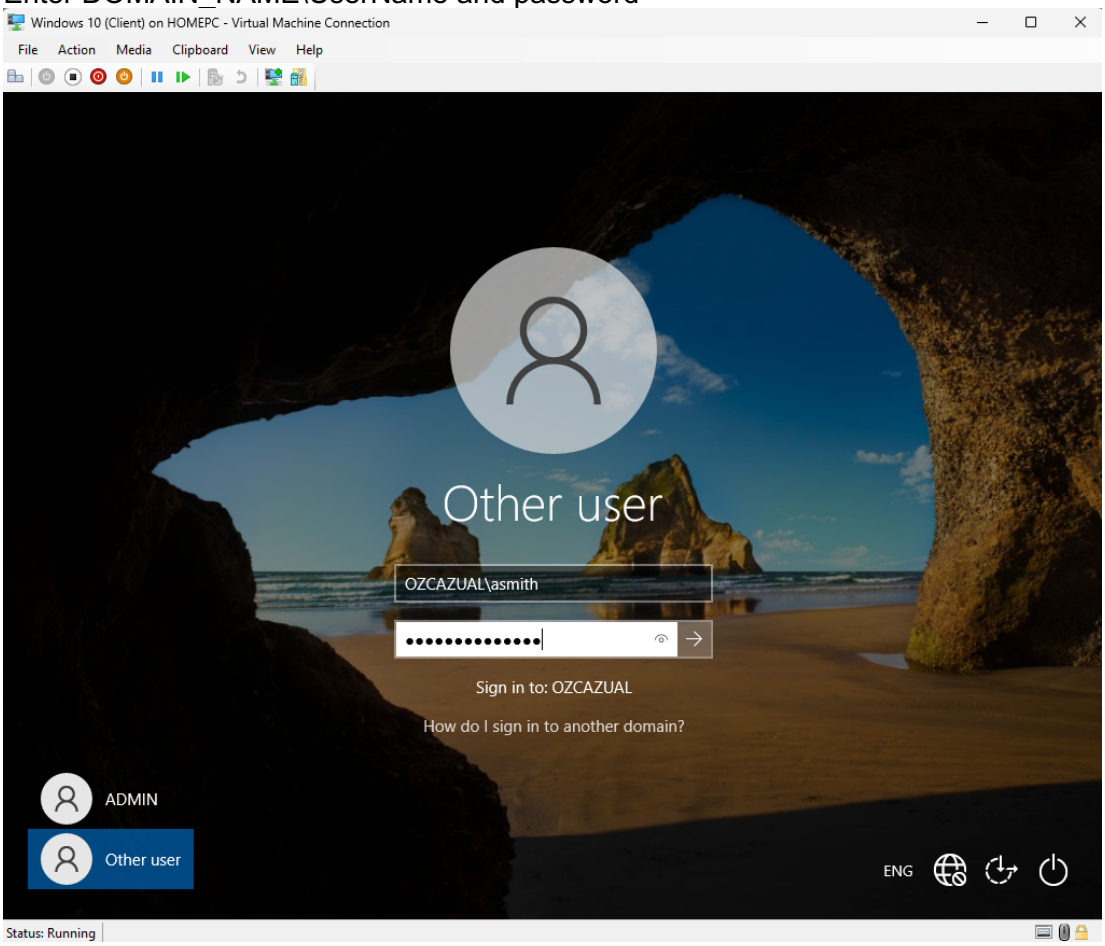


    - Provide **Administrator credentials** when prompted

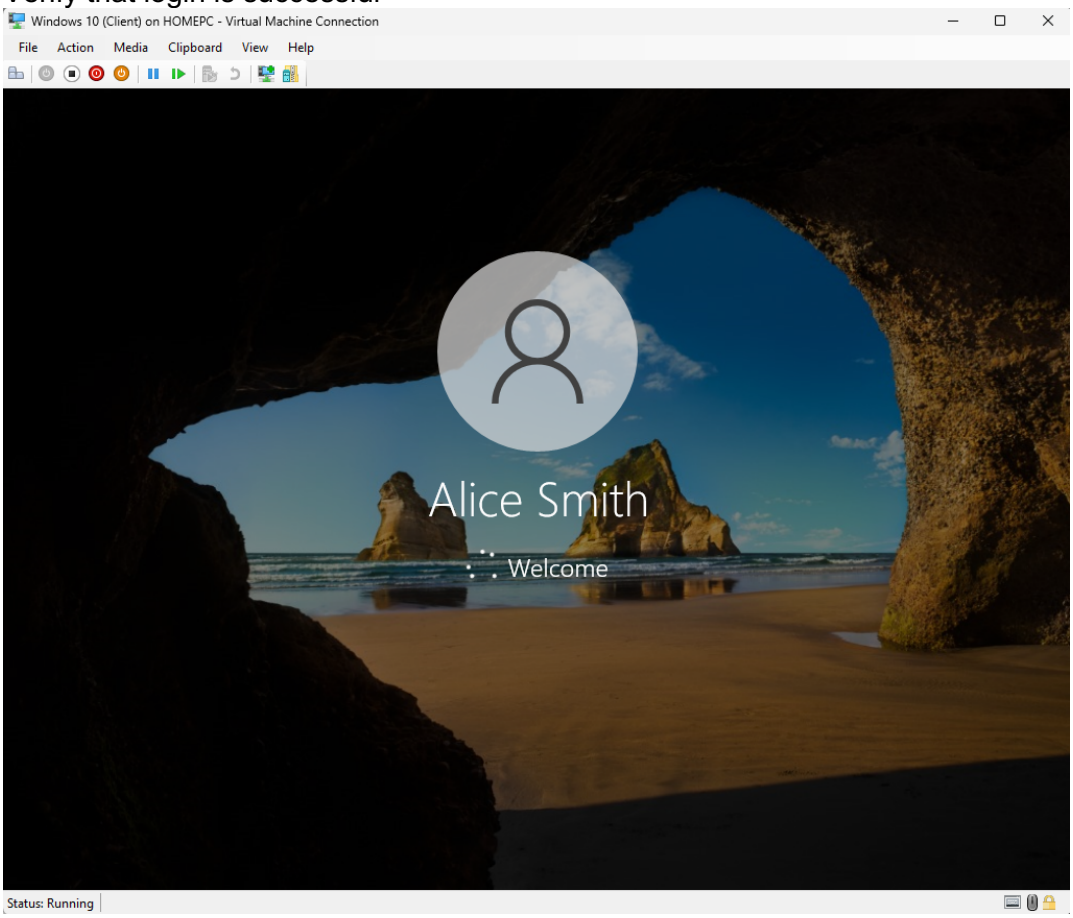


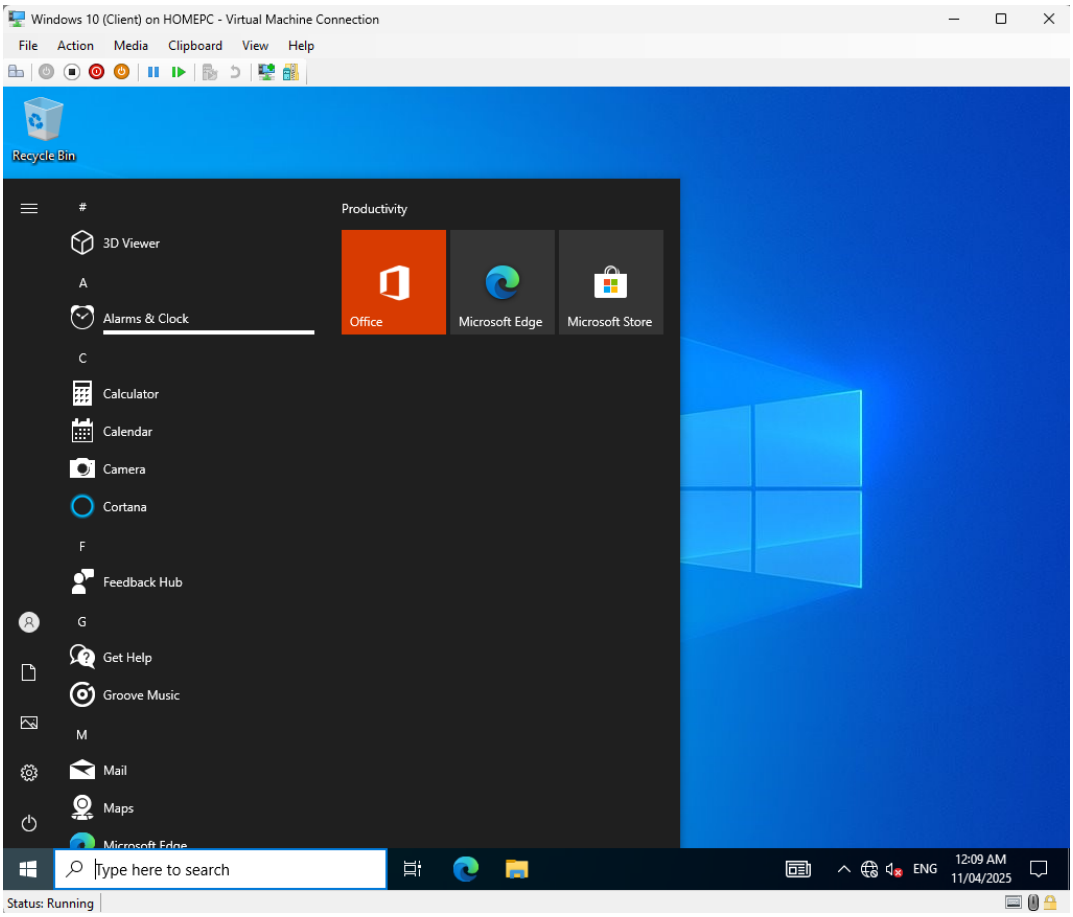
    - Restart the client machine

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

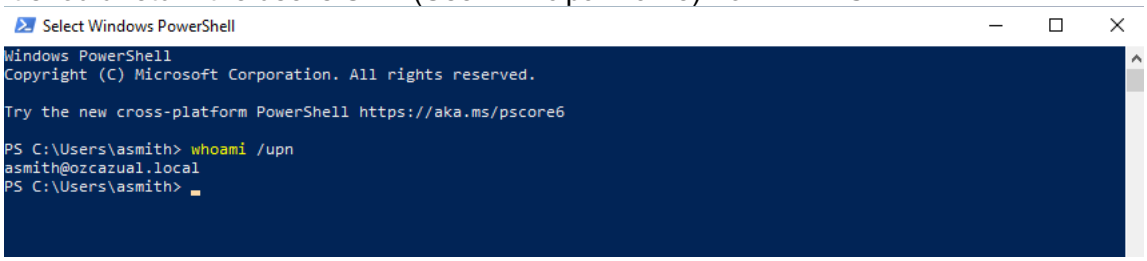


- Verify that login is successful



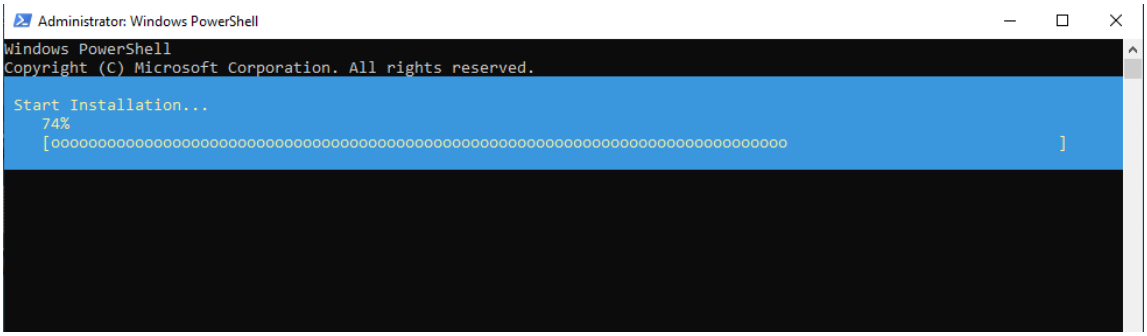


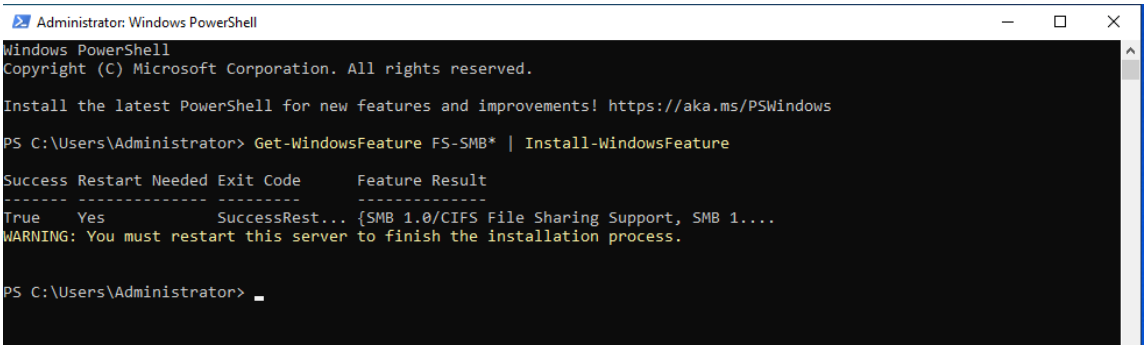
3. **Check user details using PowerShell:**
   On the **Windows 10 (Client) machine**, run:
   powershell
   `whoami /upn`
   It should return the user's UPN (User Principal Name) from AD DS.



Detailed SMB file sharing configuration in Windows Server
Install and Enable SMB:
Open Powershell (as Administrator)

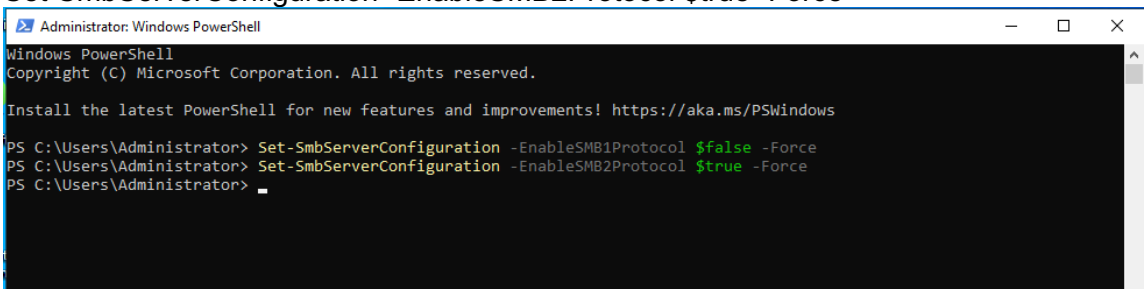
Get-WindowsFeature FS-SMB* | Install-WindowsFeature





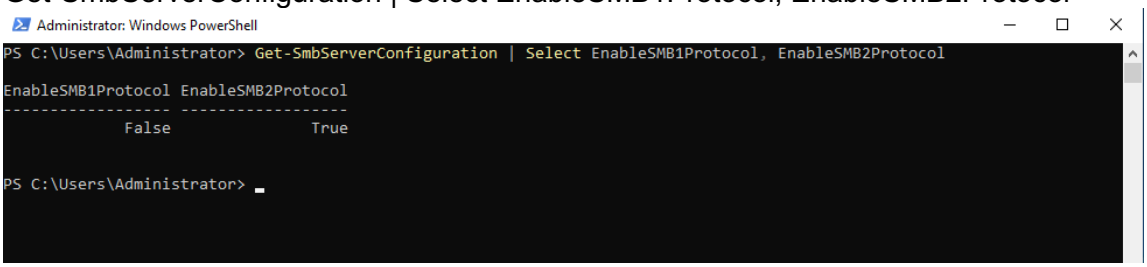
Ensure SMBv2 and SMBv3 are enabled

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

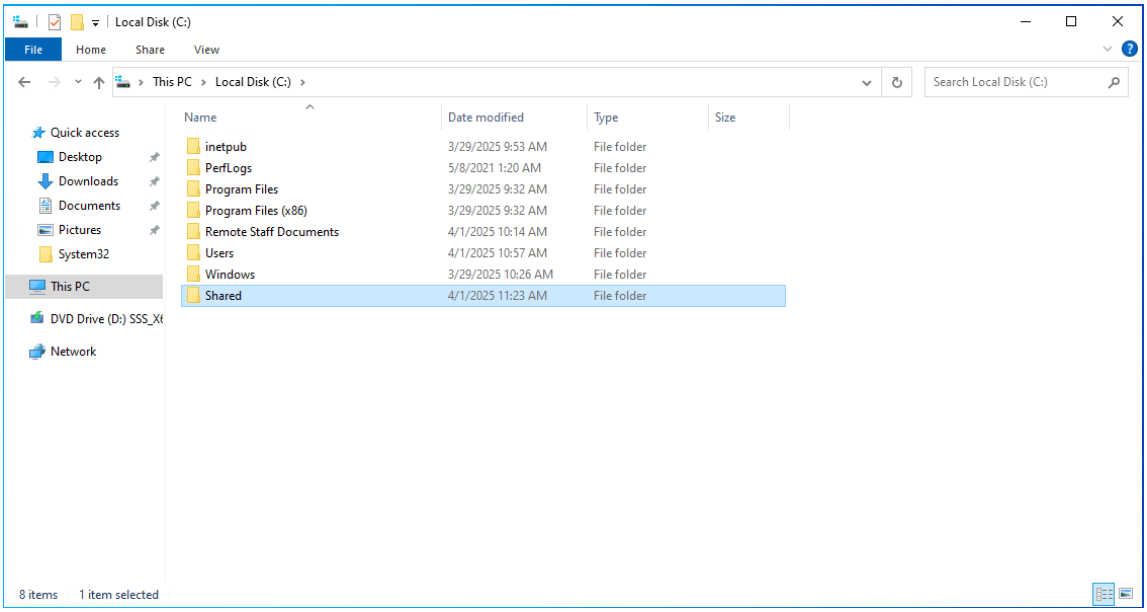


Ensure SMB is running

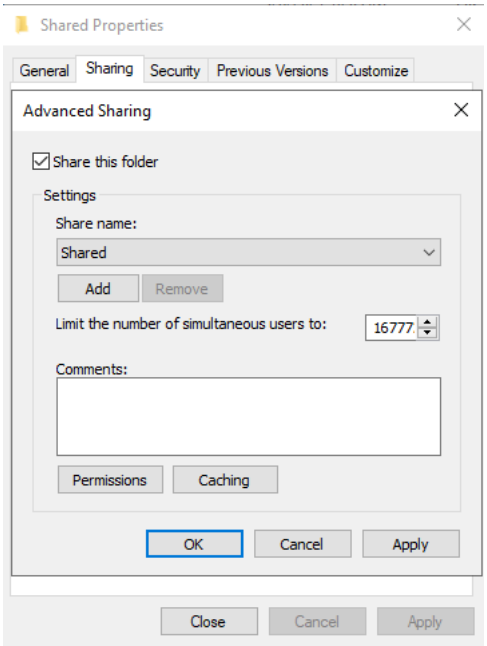
Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol



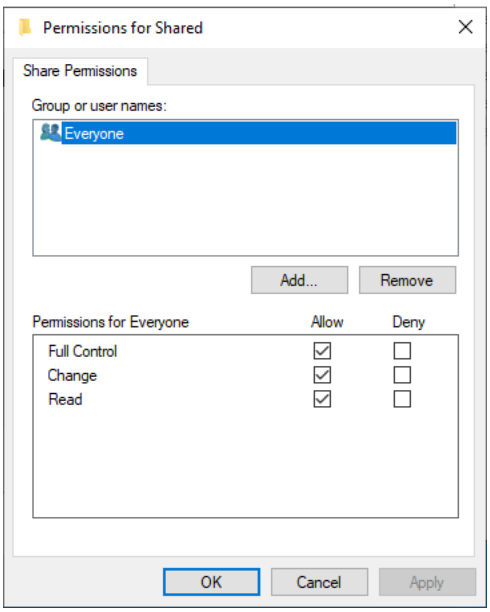
Create a Shared Folder:
Create a folder to share

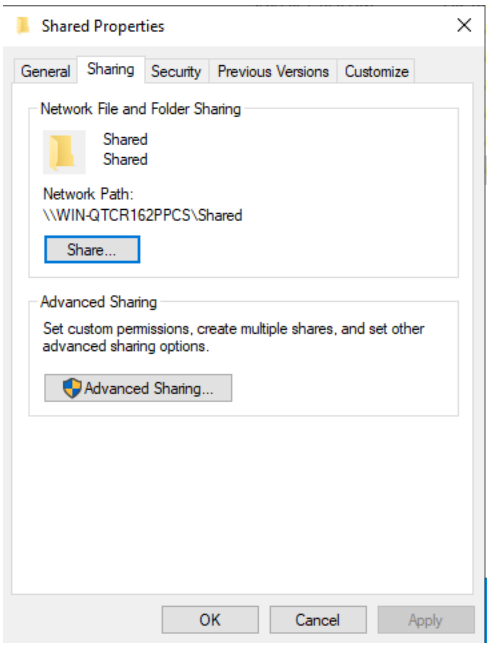


Right-click > Properties > Sharing tab > Advanced Sharing
Check Share this folder

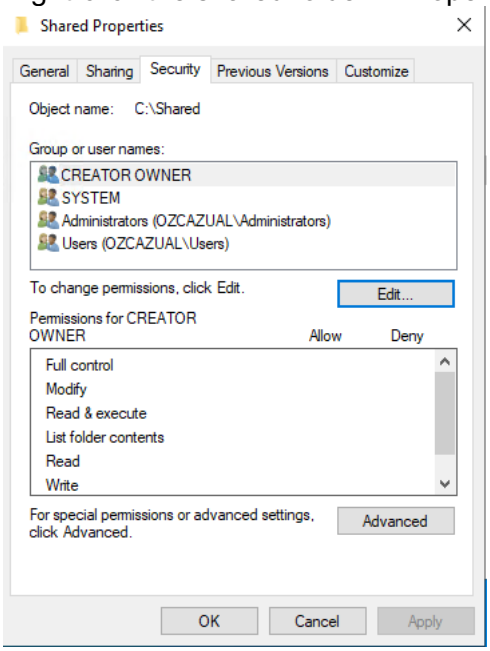


Click Permissions > Set:
Everyone: Full Control > OK > Apply > OK

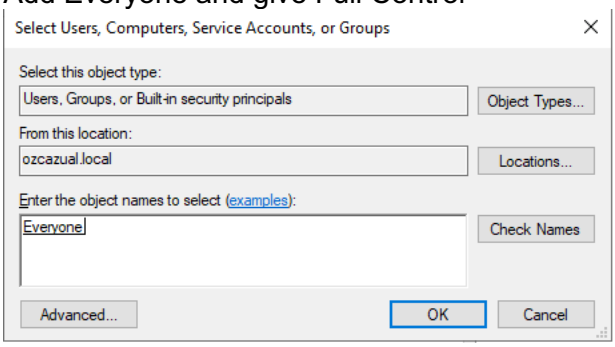

Permissions for Shared
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

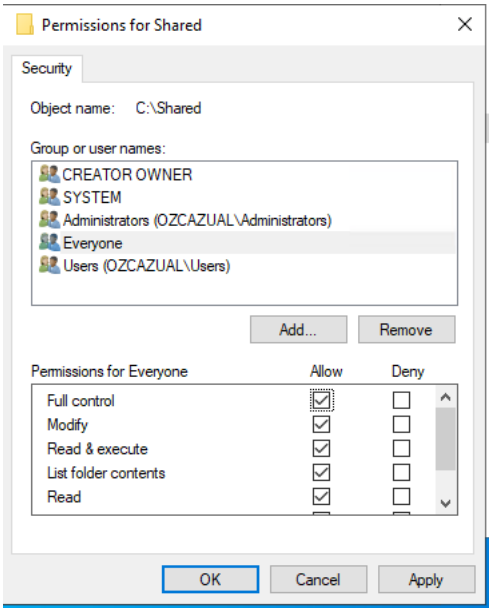

Shared Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Shared
Shared
Network Path:
\\WIN-QTCR162PPCS\Shared
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
OK
Cancel
Apply

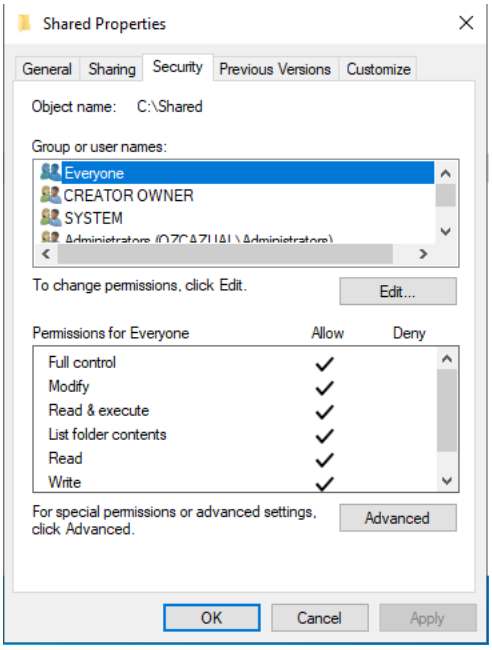
Set NTFS Permissions (Temporary Full Access)
Right-click the shared folder > Properties > Security tab > Edit… > Add…



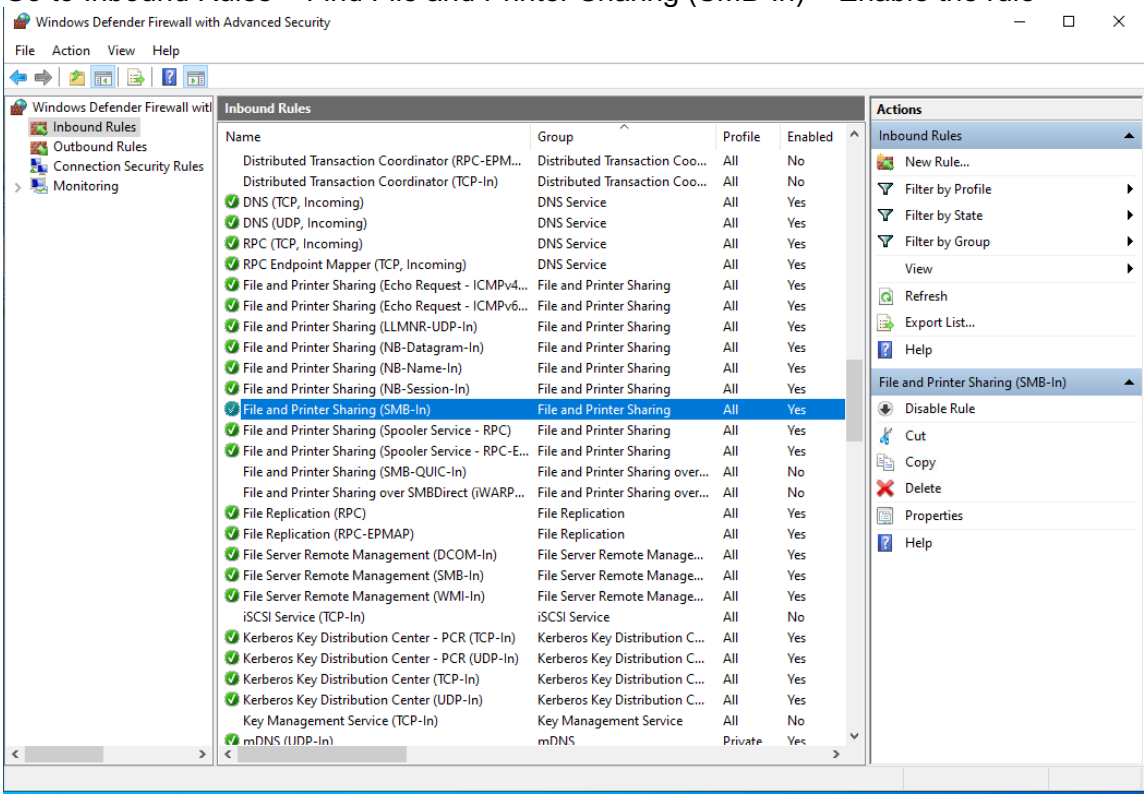
Add Everyone and give Full Control







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

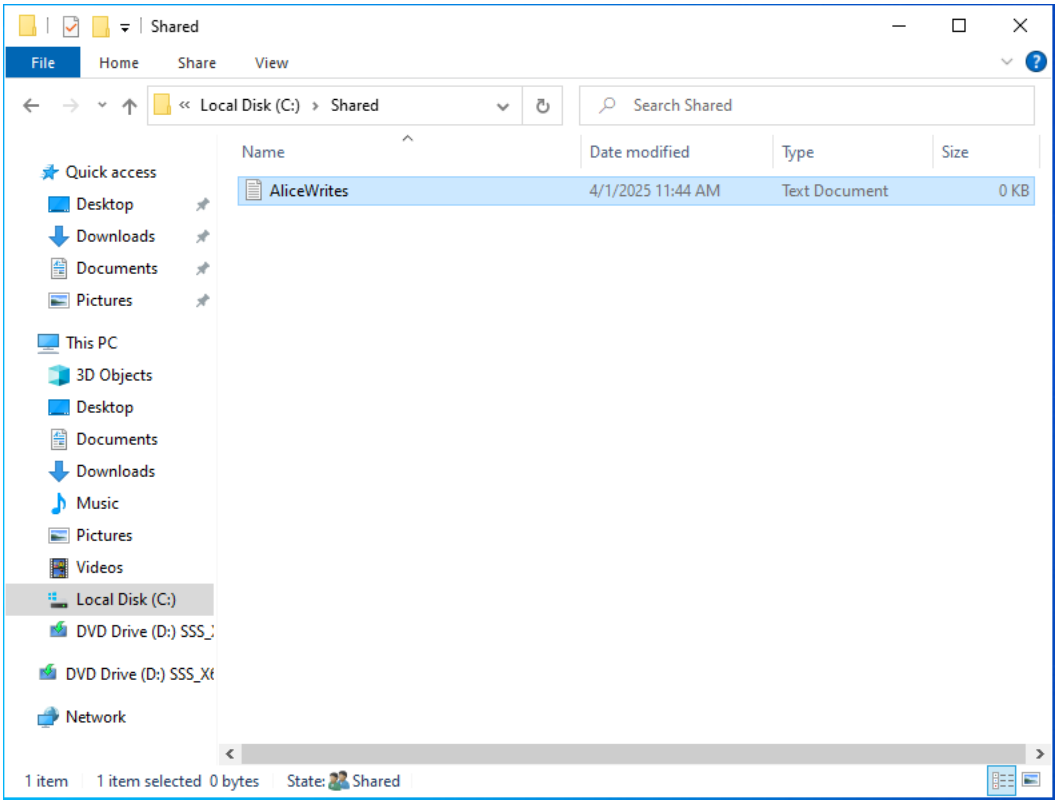


Access the Share from Another Machine
On a Windows Client Machine:
Open Run (Win + R)
Type: \\<WindowsServer-IP>\Shared
Enter credentials (if prompted)
Try copying, modifying and deleting files to confirm it works.

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]