

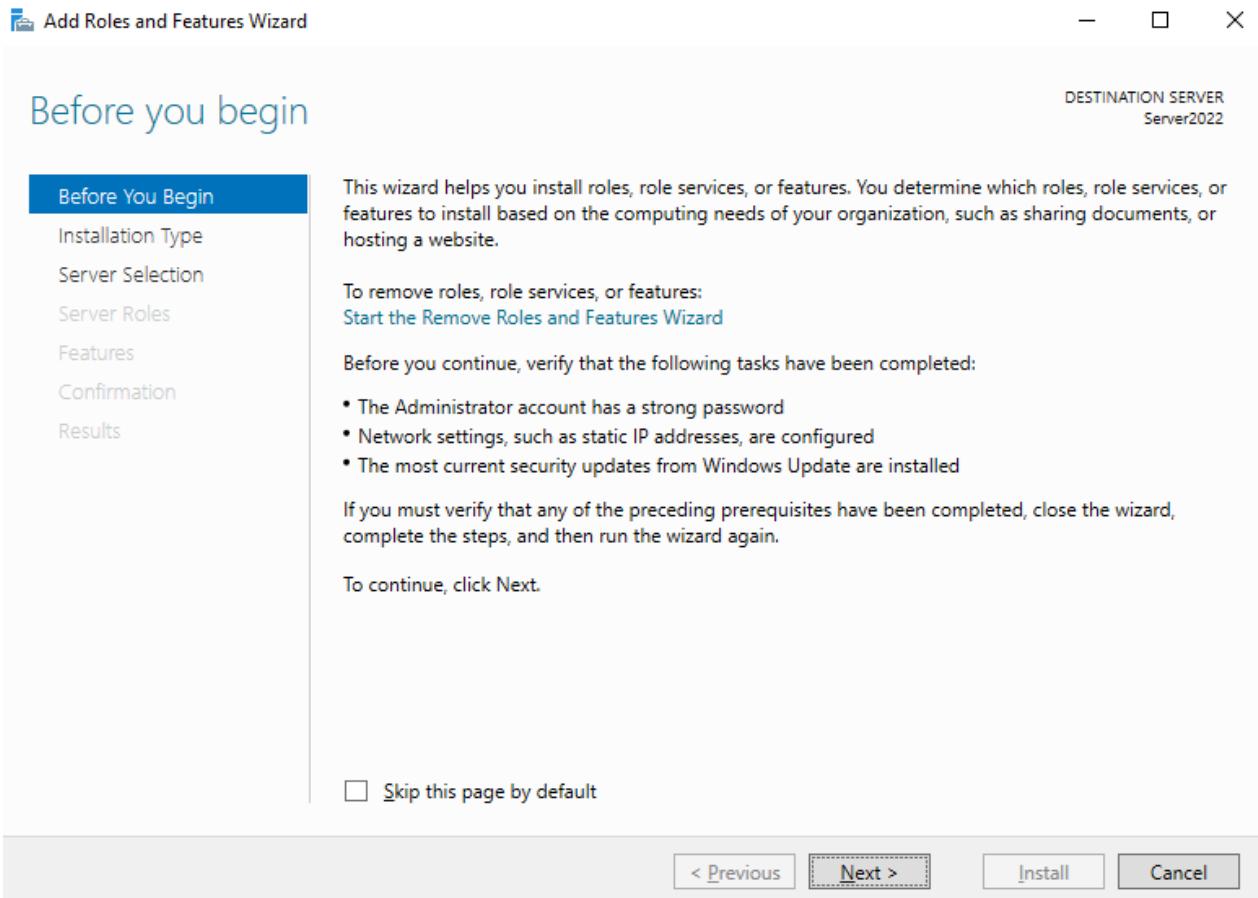
# Table of Contents

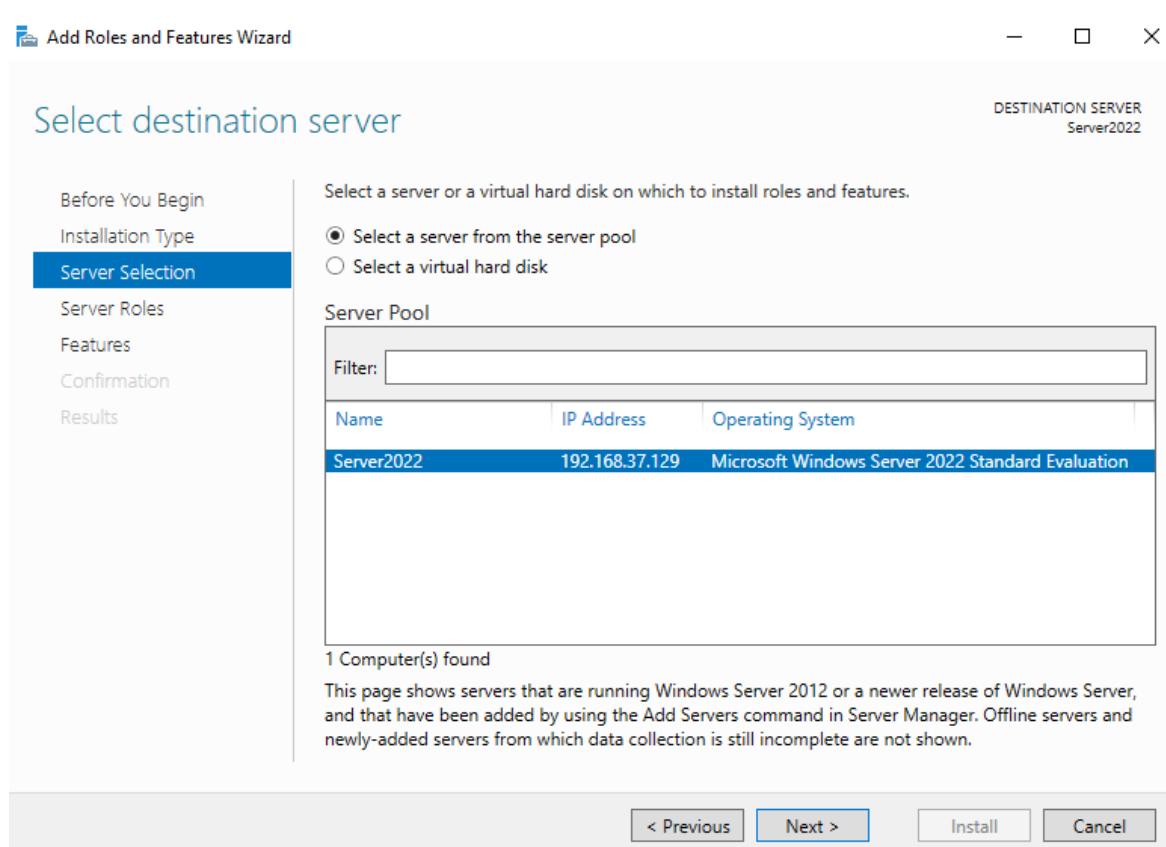
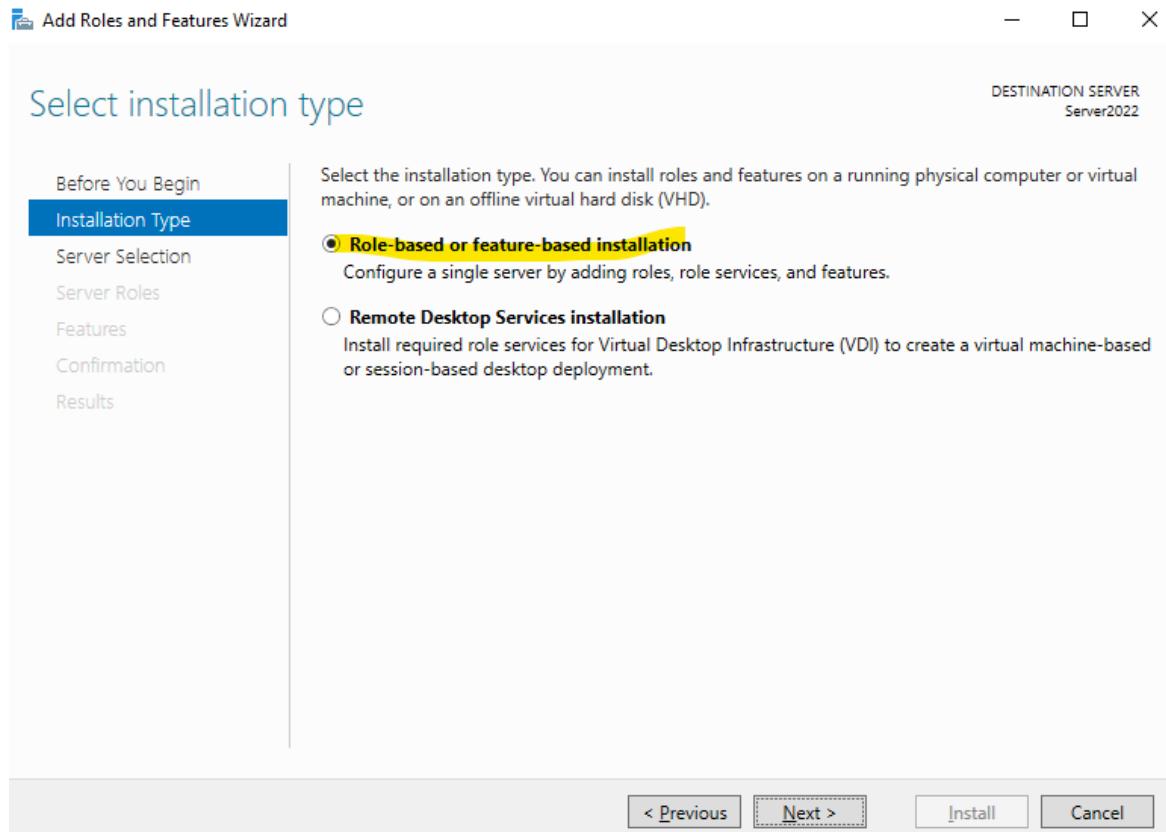
<b>Setting up VM and Active Directory .....</b>	<b>2</b>
<b>Creating Organizational Units and Users .....</b>	<b>51</b>
<b>Remote Connection.....</b>	<b>54</b>
<b>Implementing Group Policy Objects (GPOs).....</b>	<b>58</b>
<b>Creating Shared Folders, Security Groups, Access Permissions, and Network Drive Mapping .....</b>	<b>72</b>

## Setting up VM and Active Directory

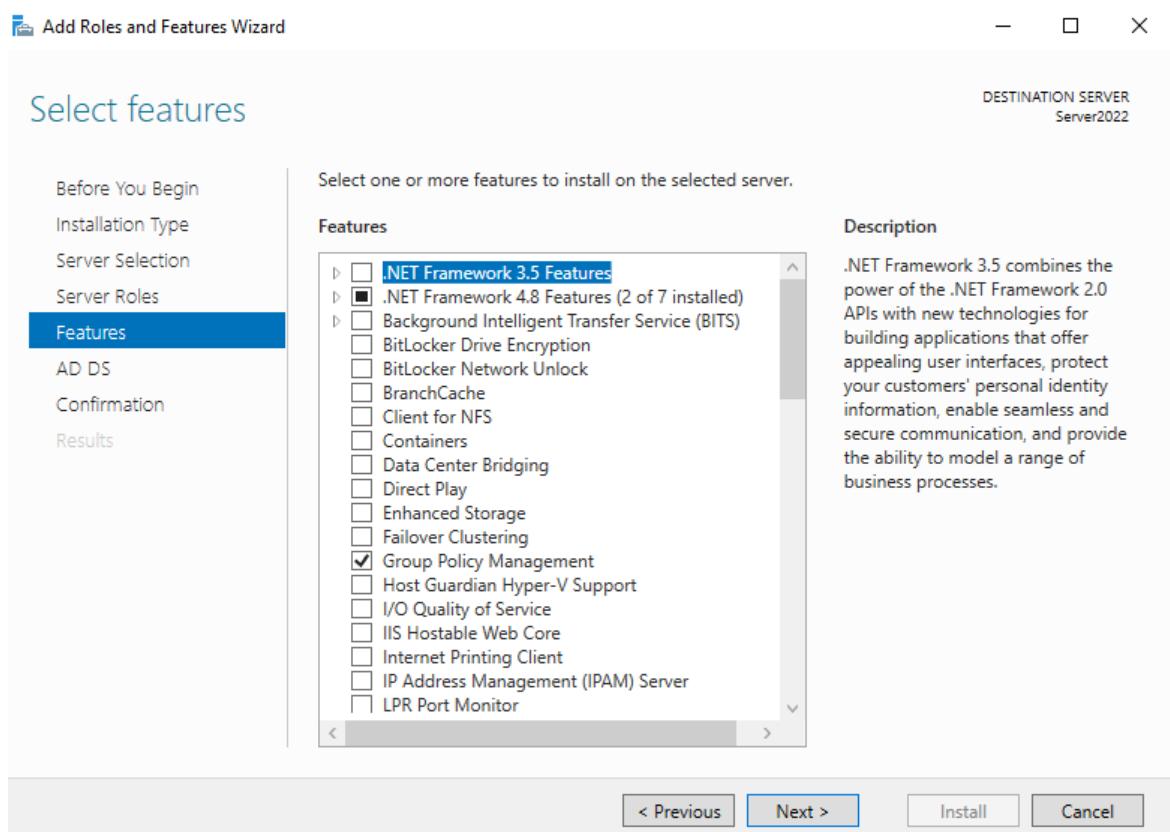
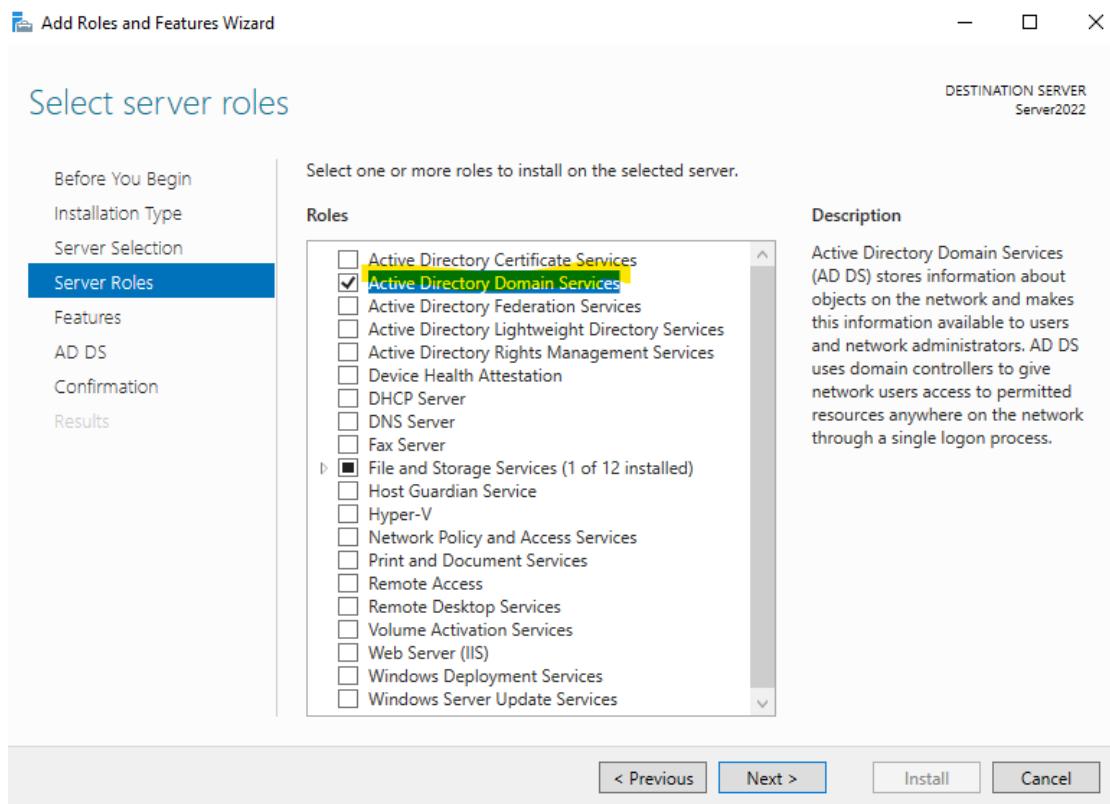
### Setting up Active Directory in Windows Server 2022

- Setting up creating Active Directory: Go to **Server Manager->click manage->click add roles and features** ->ensure your configurations matches the screenshots below





- Make sure to select **Active Directory Domain Services**



Add Roles and Features Wizard

## Active Directory Domain Services

DESTINATION SERVER  
Server2022

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
**AD DS**  
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:

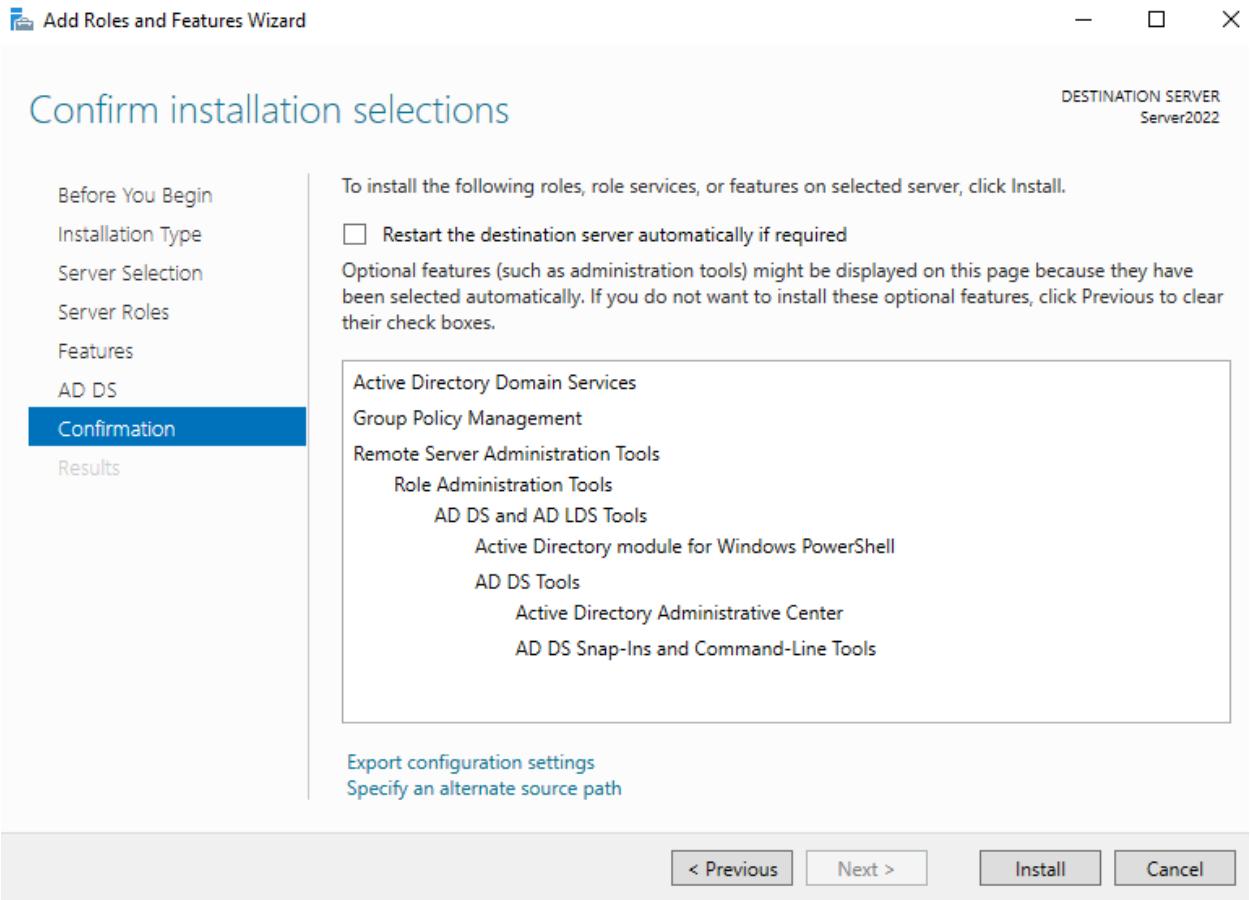
- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server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

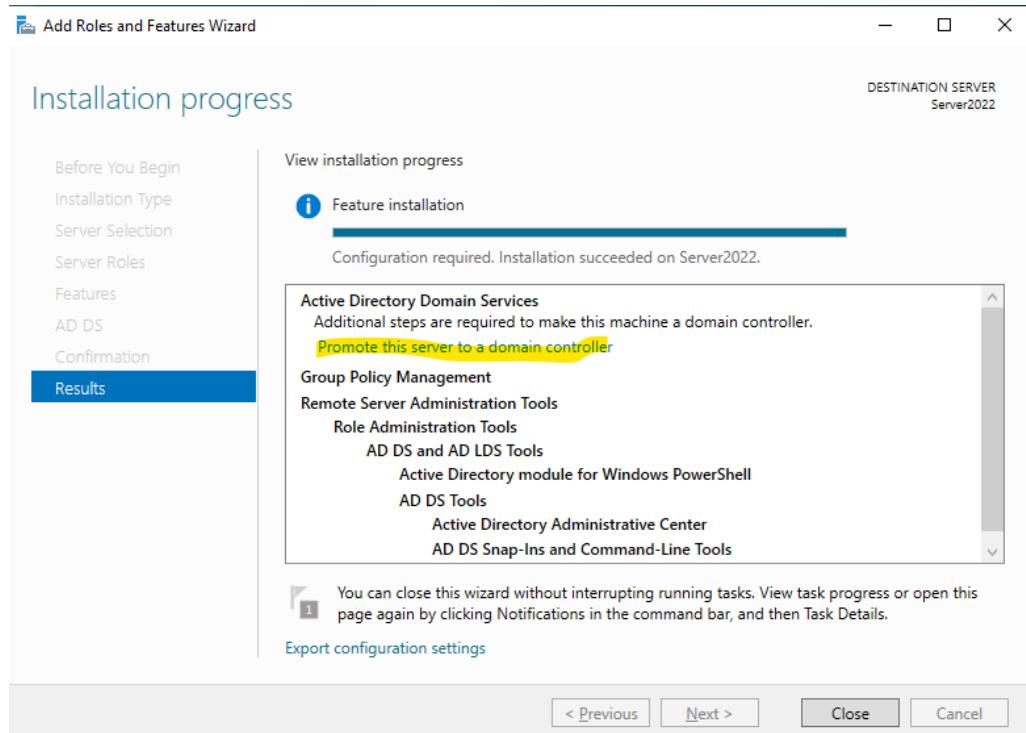
[Learn more about Azure Active Directory](#)  
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous    Next >    Install    Cancel

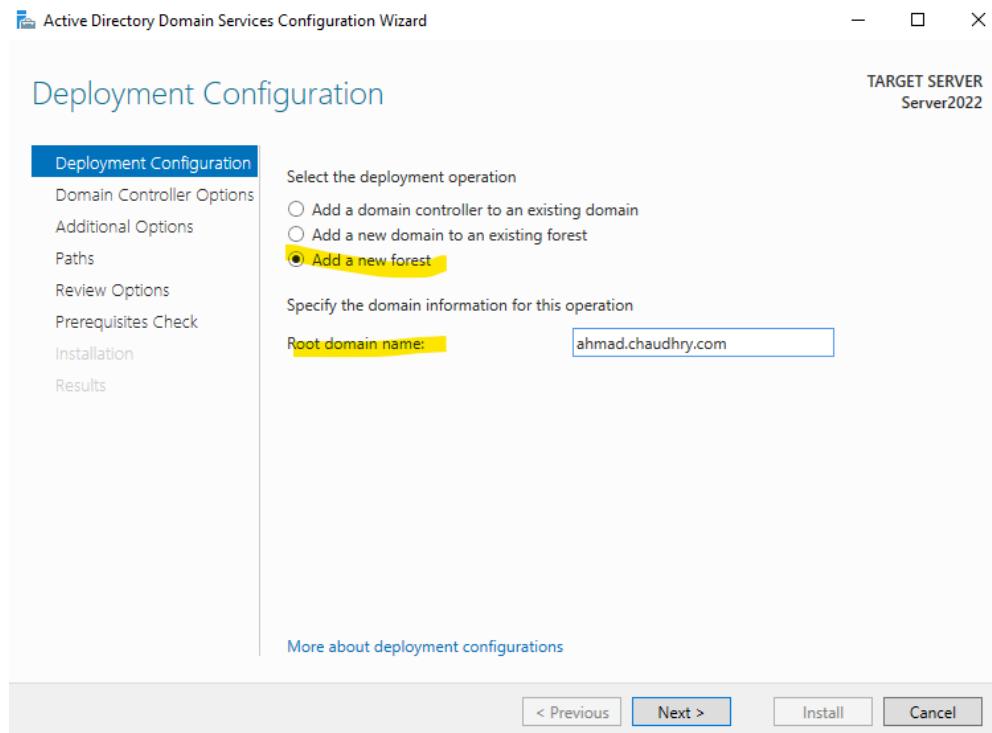


## Active Directory Domain Controller

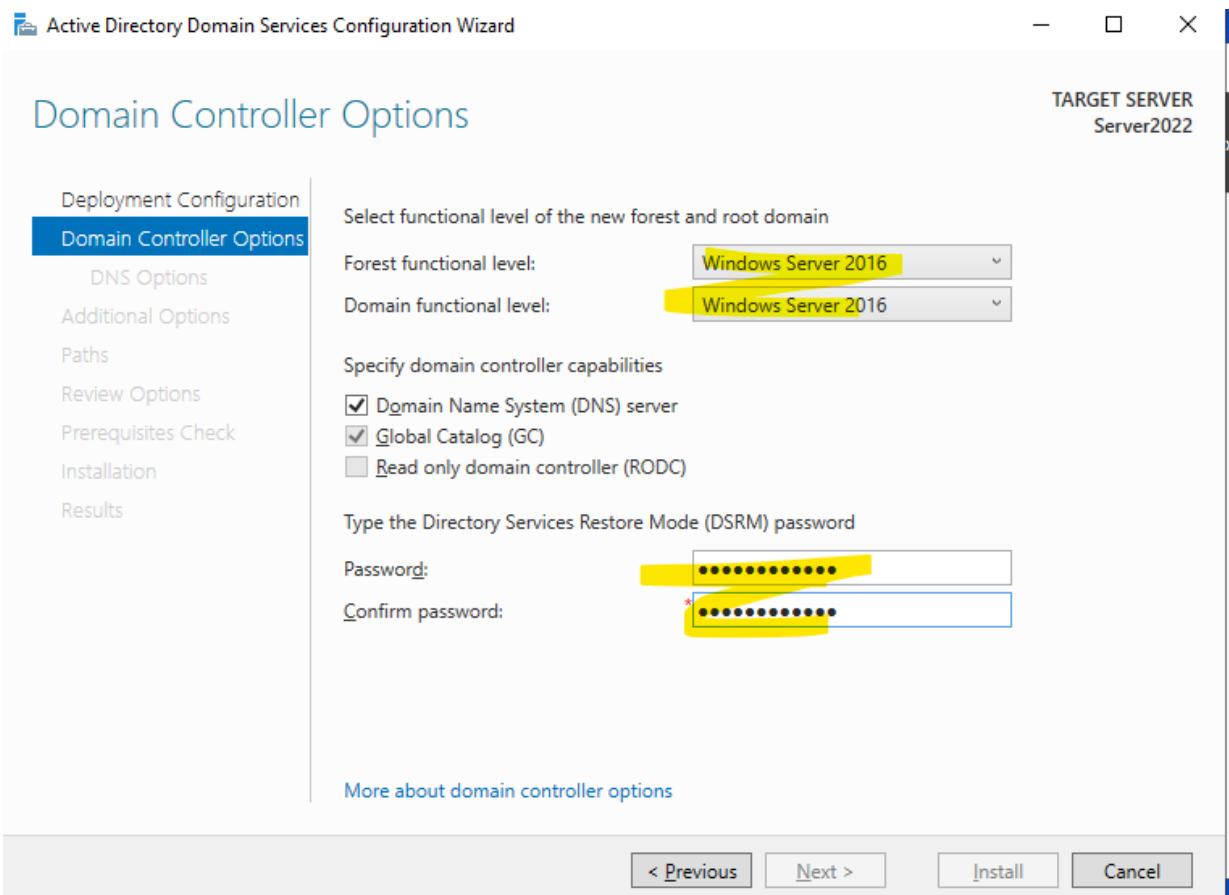
- So far, we have only created an Active Directory server, not a domain controller. We will complete that in the **Results** section
- Click **Promote this server to a domain controller**

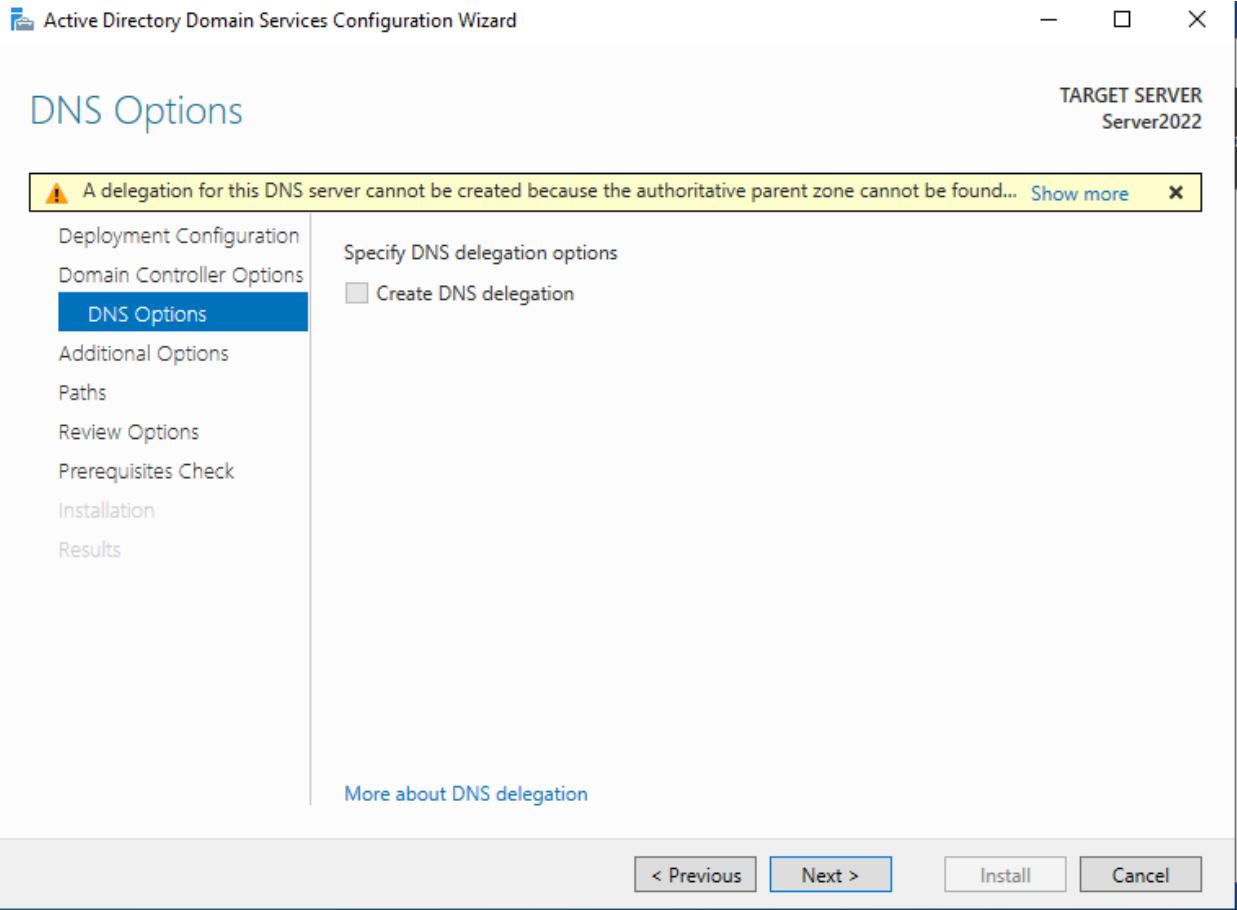


- Click **add a new forest** and enter the root domain name. Example, I named it "ahmad.chaudhry.com"

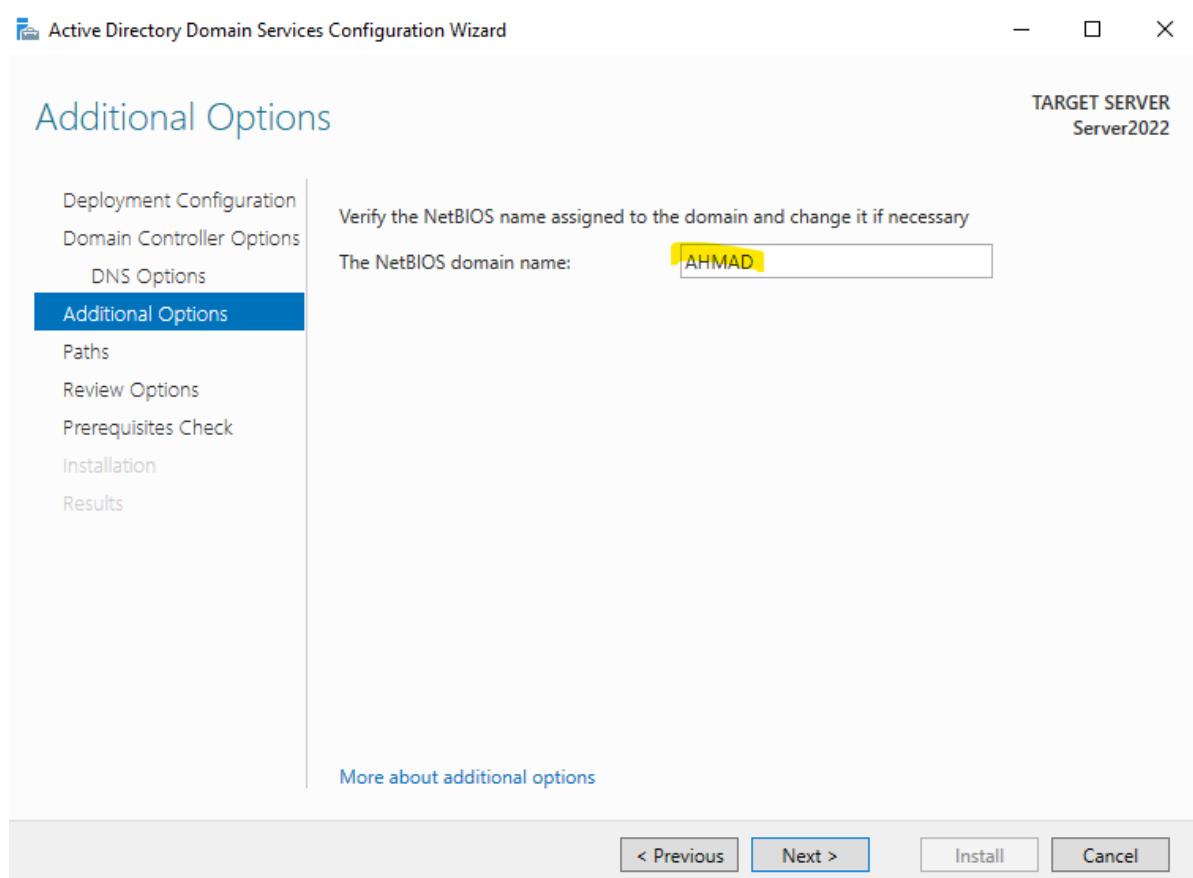


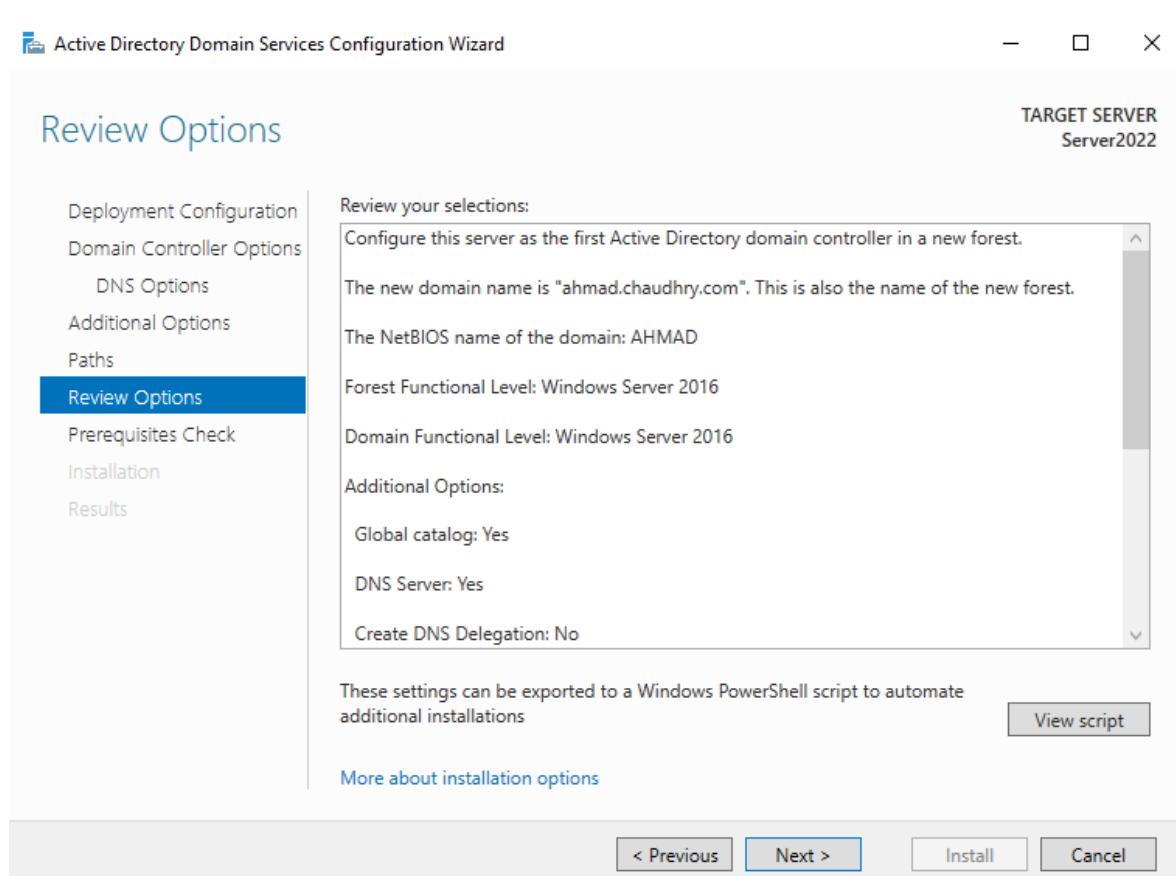
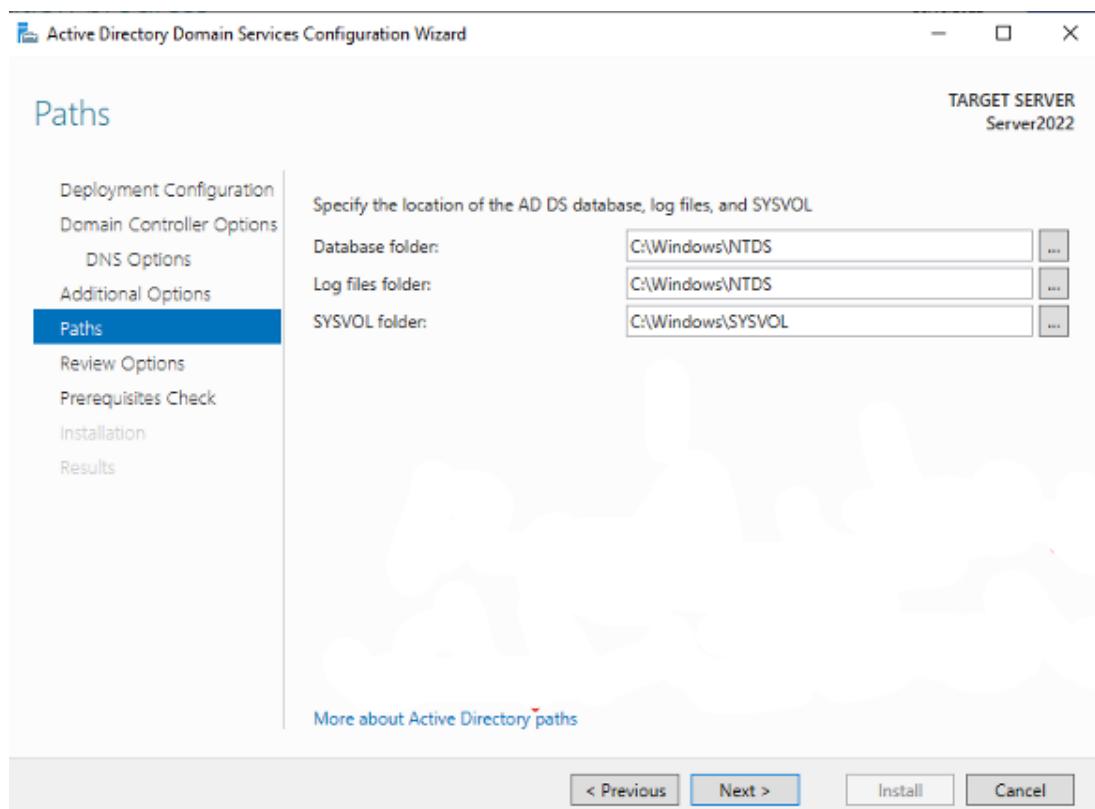
- Ensure your configurations matches the screenshots below



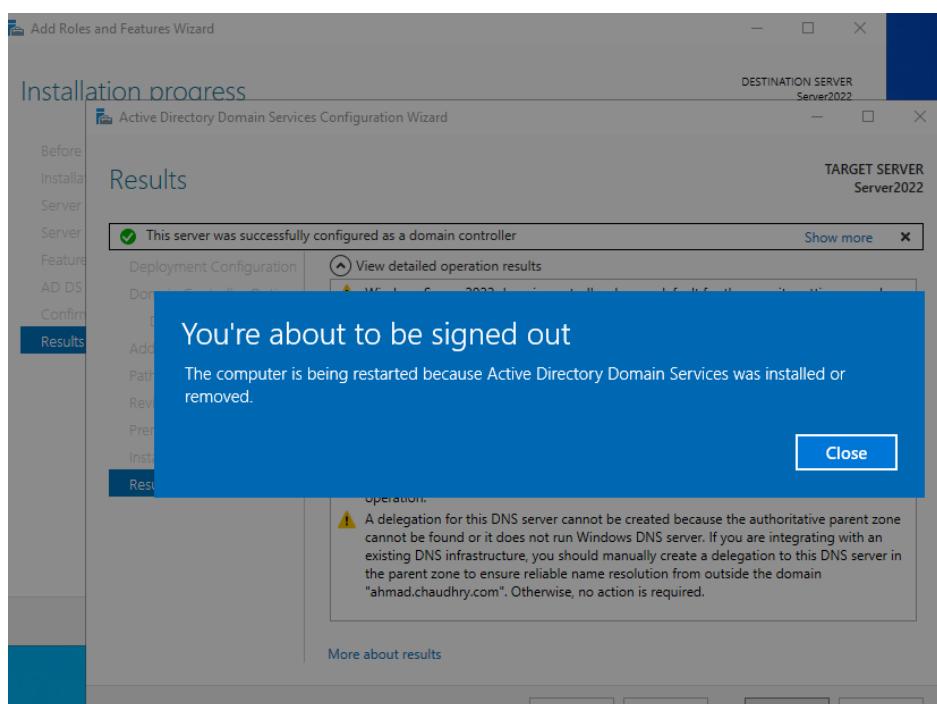
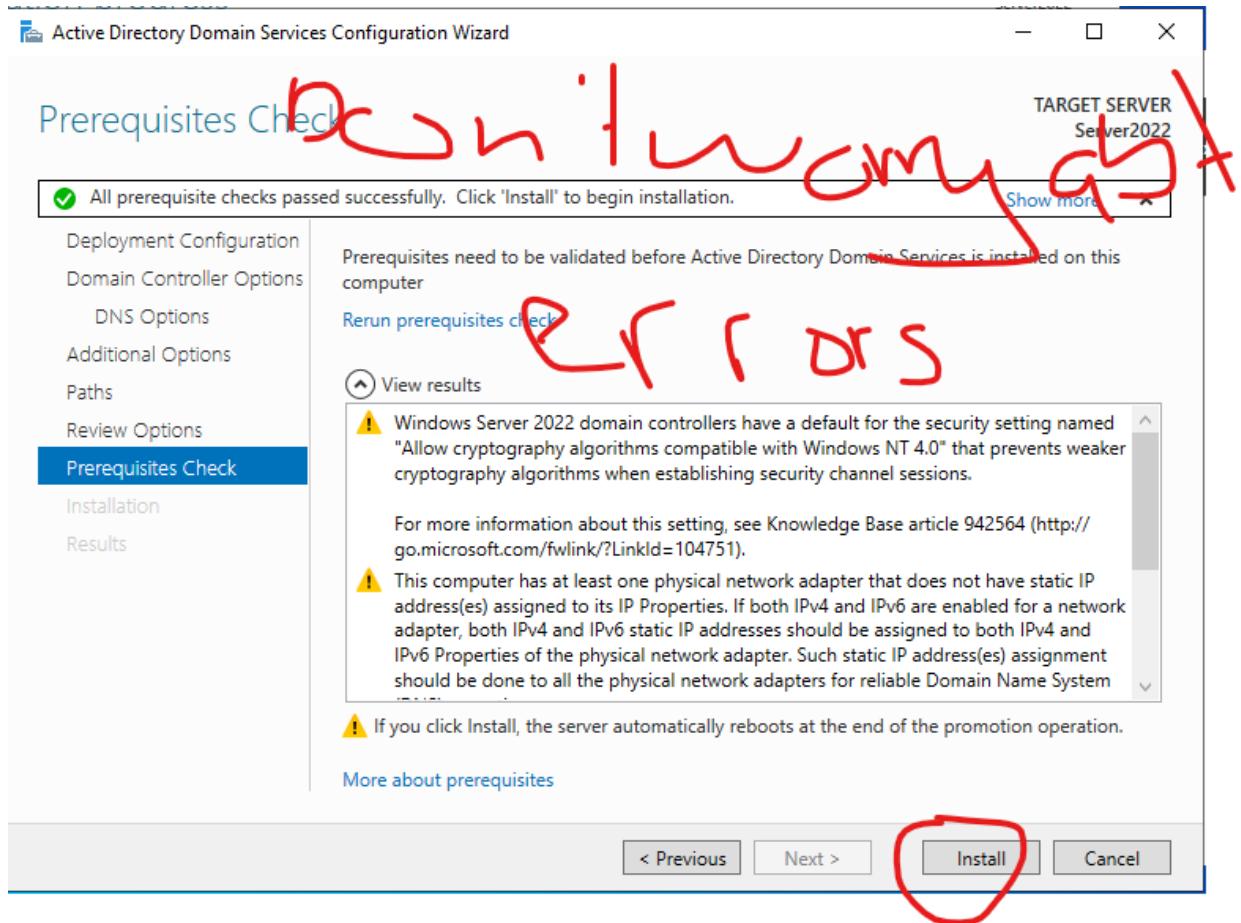


- The NetBIOS name will be populated automatically after a few seconds. In this case, it is Ahmad because the domain name is ahmad.chaudhry.com

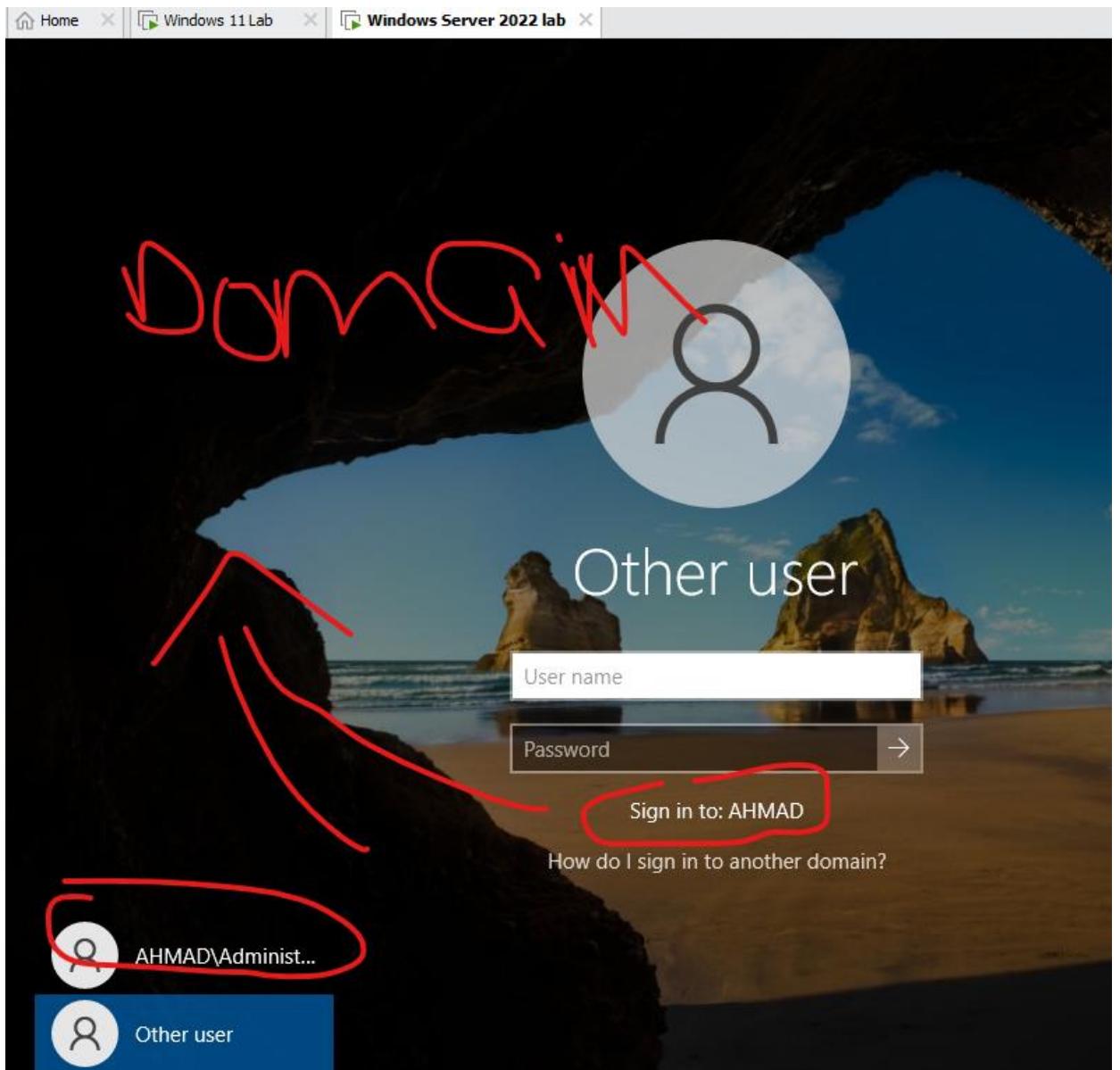




- o Don't worry about errors and click next

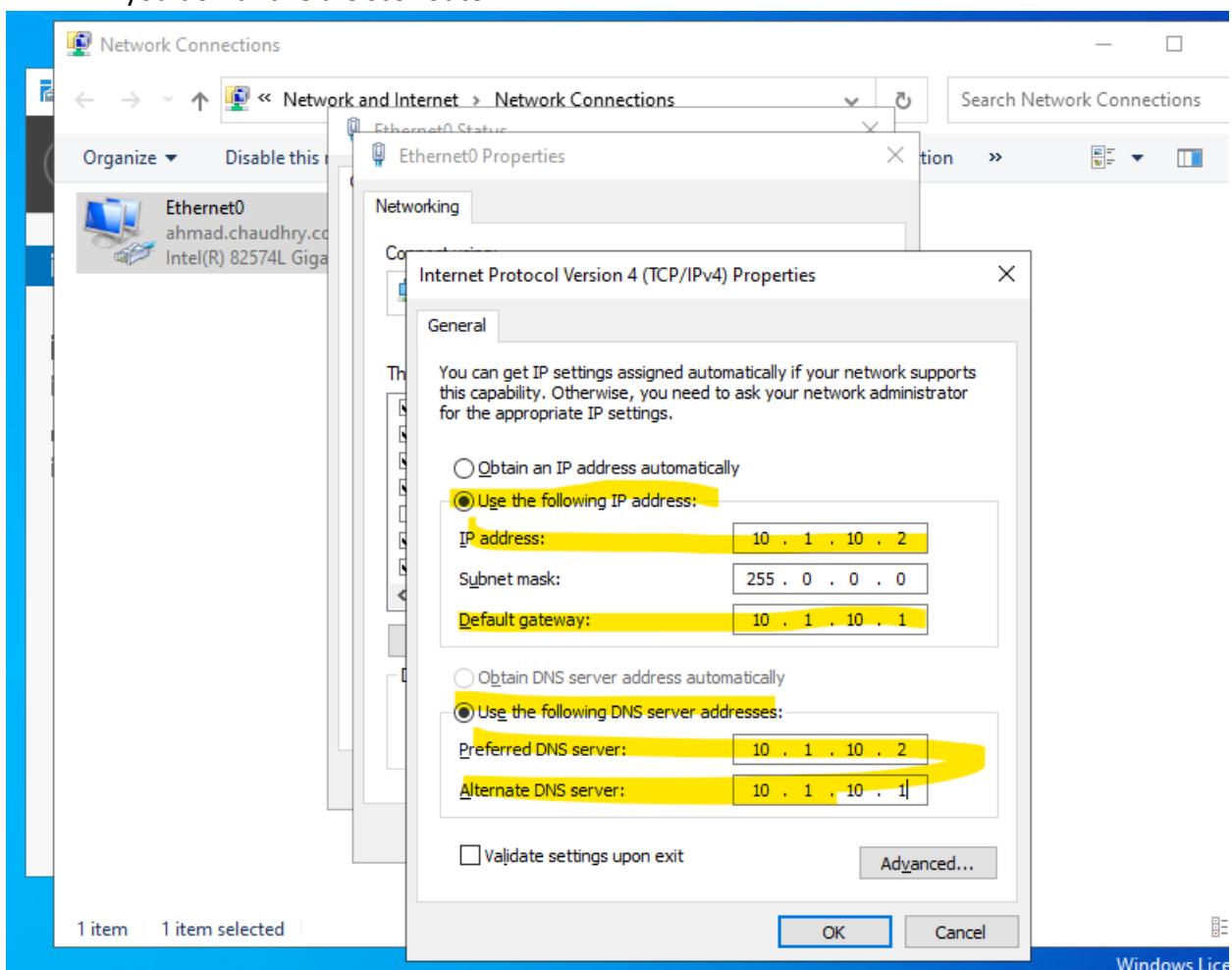


- You can confirm that the computer has joined the domain by checking the login screen. It shows **Sign in to: AHMAD**, and the username format appears as **AHMAD\Administrator**, which indicates the domain is active

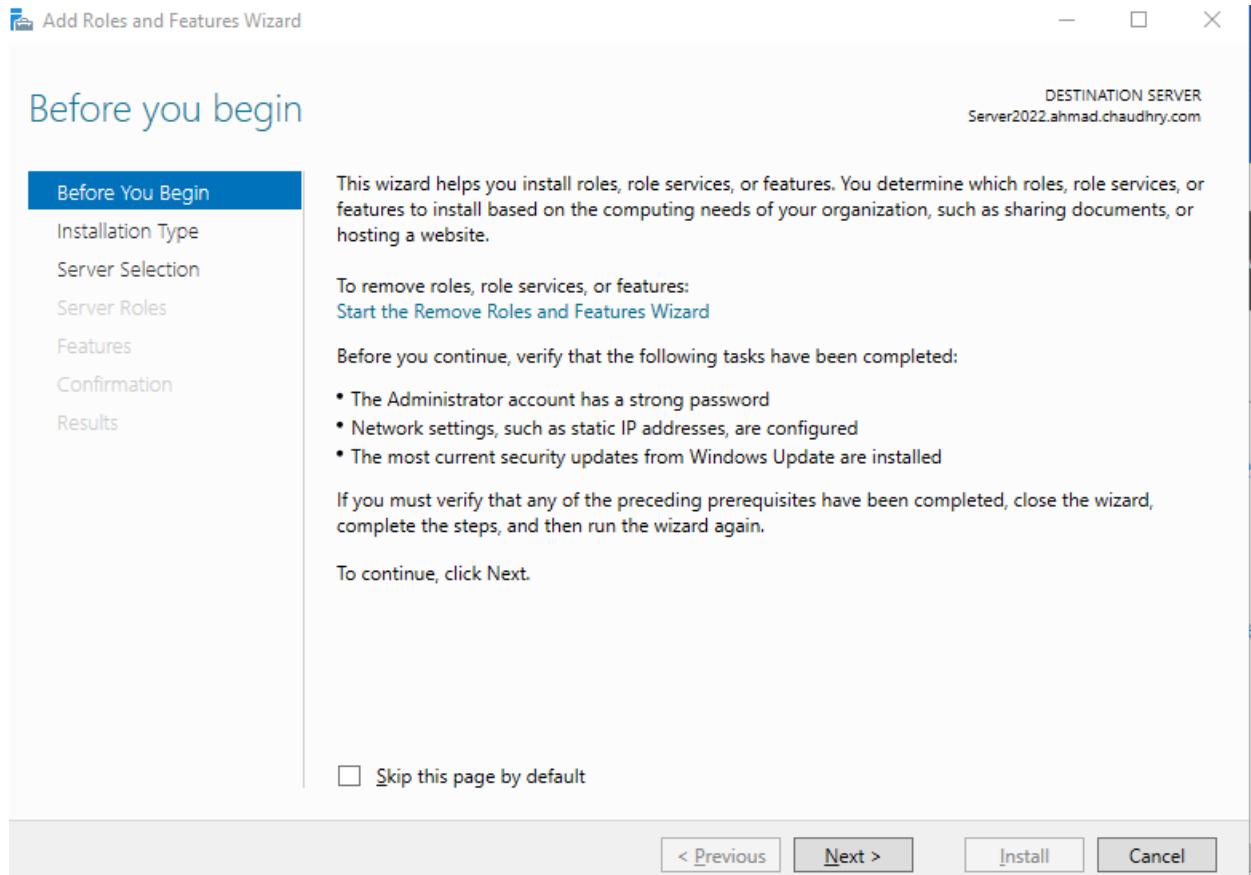


## DHCP and DNS configuration

- DNS: in Windows Server, go to **Control Panel → Network and Internet → View network status and tasks**. Then, click **Change adapter settings**, double-click **Ethernet**, and select **Properties**. Choose **Internet Protocol Version 4 (TCP/IPv4) Properties** and configure it with the IP address shown in the screenshot below
  - **Note:** You will not have internet access with this configuration. To restore internet access, select **Obtain an IP address automatically**. This is a workaround if you don't have a Cisco router



- Configure DHCP server: Windows Server: **Server Manager->Manager->Add roles and features** and configure to the following details:



## Select installation type

DESTINATION SERVER  
Server2022.ahmad.chaudhry.com

Before You Begin

**Installation Type**

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

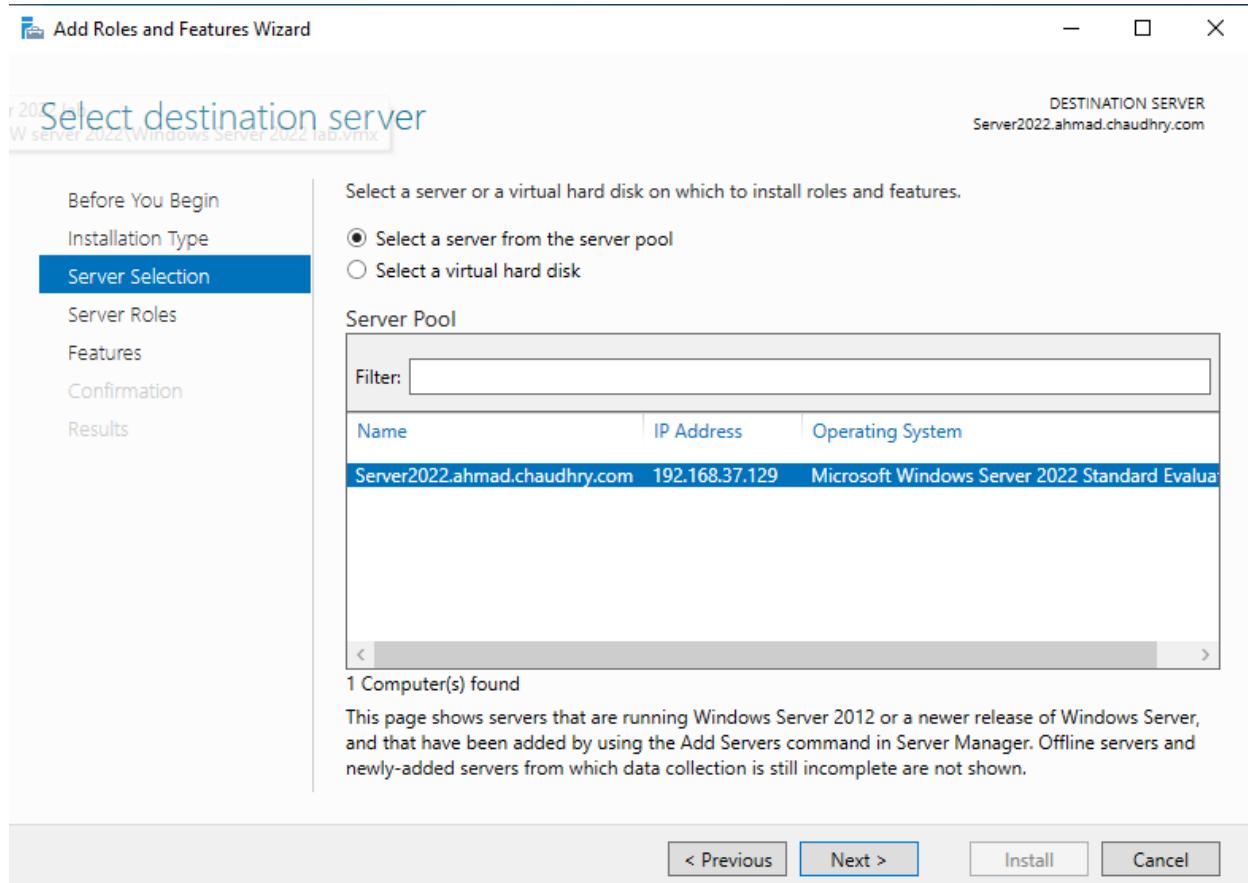
**Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

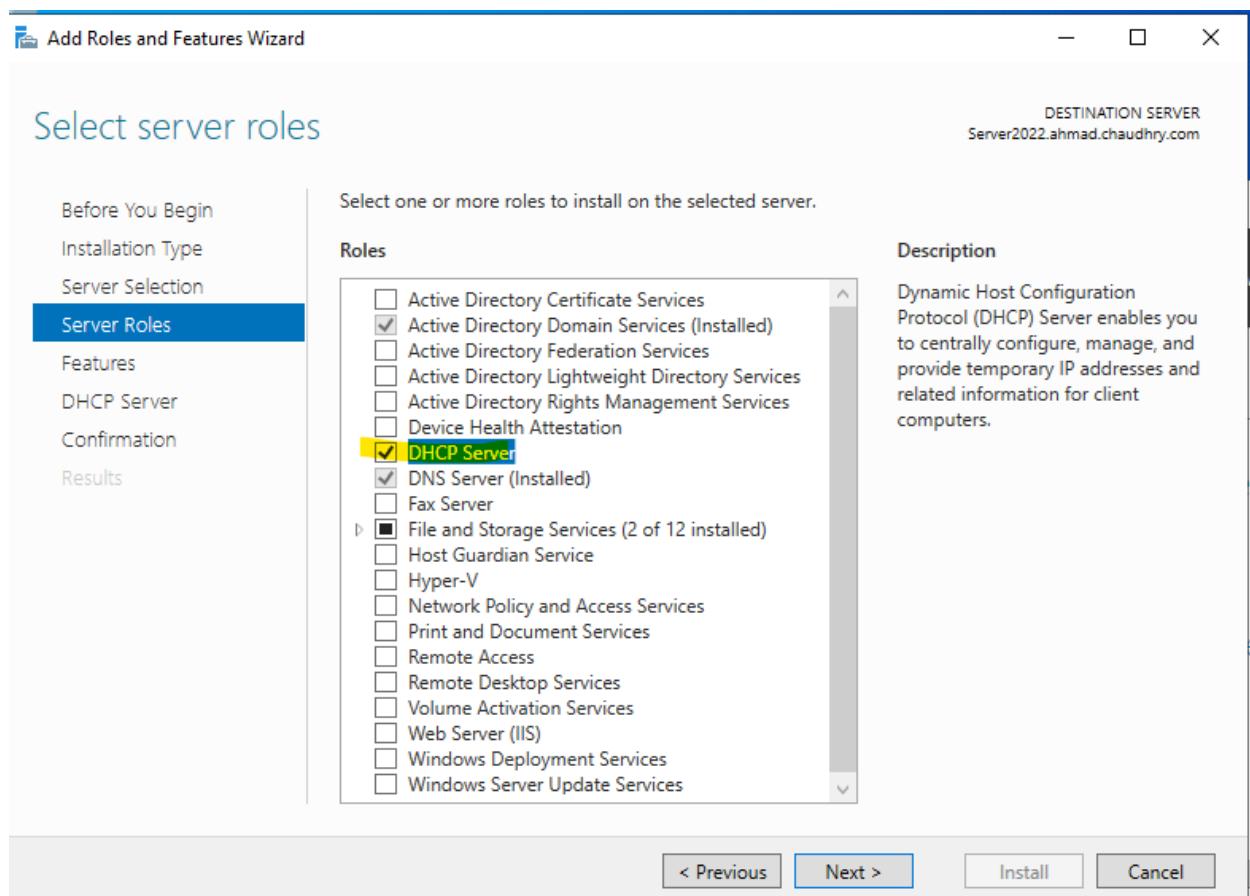
**Remote Desktop Services installation**

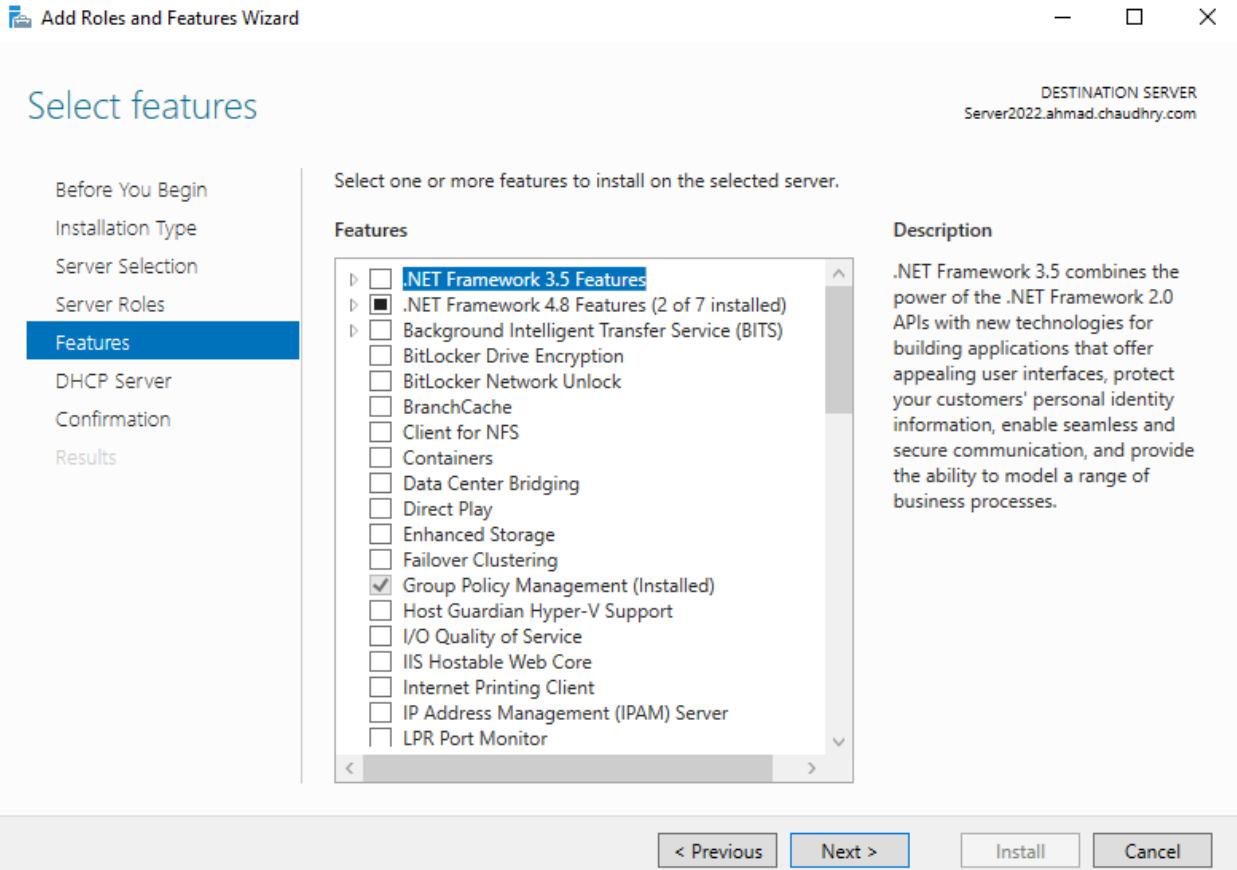
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

[< Previous](#)[Next >](#)[Install](#)[Cancel](#)



- o For the screenshot below, select **DHCP Server**. A box will appear — click **Add Features**. When another box appears, click **Continue**, and then click **Next**





## DHCP Server

DESTINATION SERVER  
Server2022.ahmad.chaudhry.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

**DHCP Server**

Confirmation

Results

The Dynamic Host Configuration Protocol allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients. Deploying a DHCP server on the network provides computers and other TCP/IP-based network devices with valid IP addresses and the additional configuration parameters these devices need, called DHCP options. This allows computers and devices to connect to other network resources, such as DNS servers, WINS servers, and routers.

Things to note:

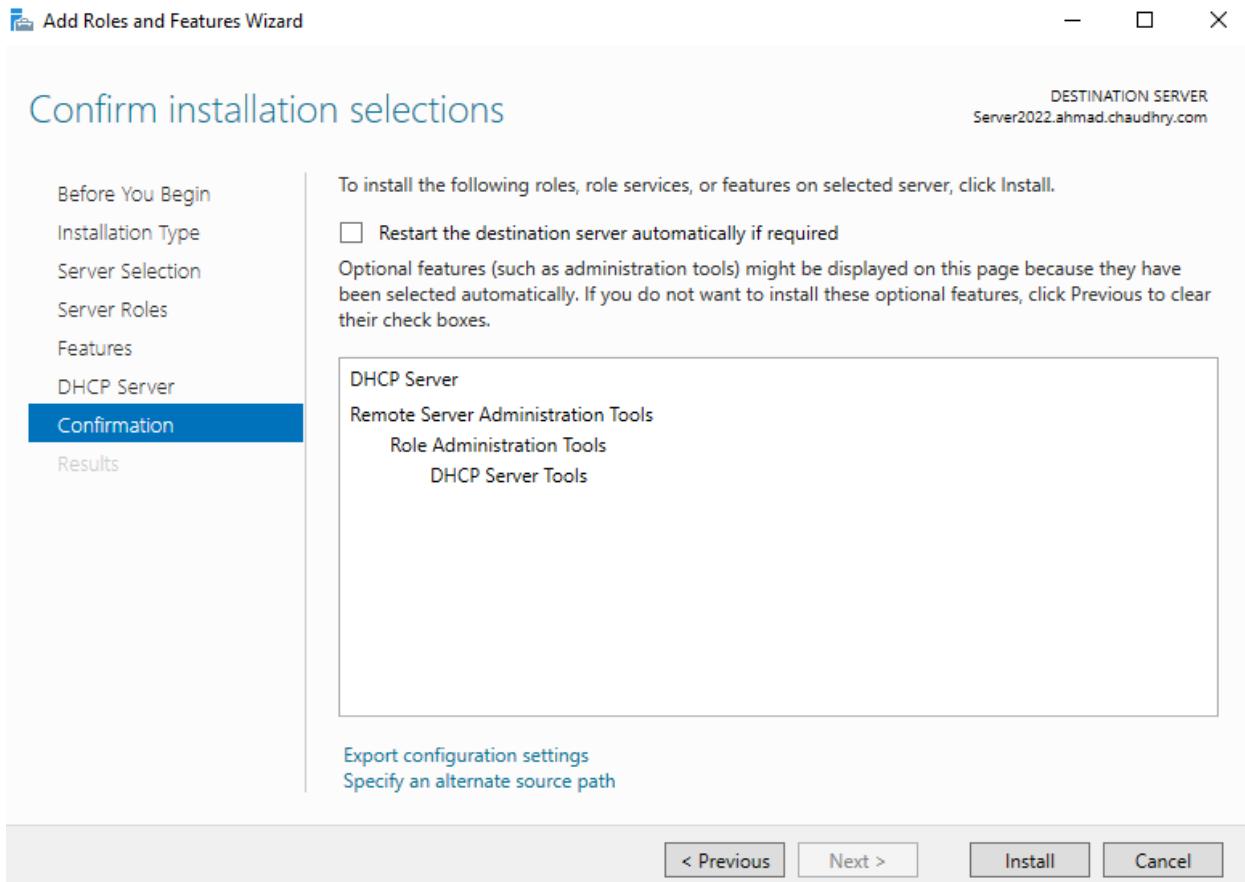
- You should configure at least one static IP address on this computer.
- Before you install DHCP Server, you should plan your subnets, scopes and exclusions. Store the plan in a safe place for later reference.

< Previous

Next >

Install

Cancel



## Installation progress

DESTINATIO  
Server2022.ahmad.chau

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
DHCP Server  
Confirmation  
**Results**

[View installation progress](#)

 **Feature installation**

Configuration required. Installation succeeded on Server2022.ahmad.chaudhry.com.

**DHCP Server**

[Launch the DHCP post-install wizard](#)  
[Complete DHCP configuration](#)

**Remote Server Administration Tools**

[Role Administration Tools](#)  
[DHCP Server Tools](#)

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

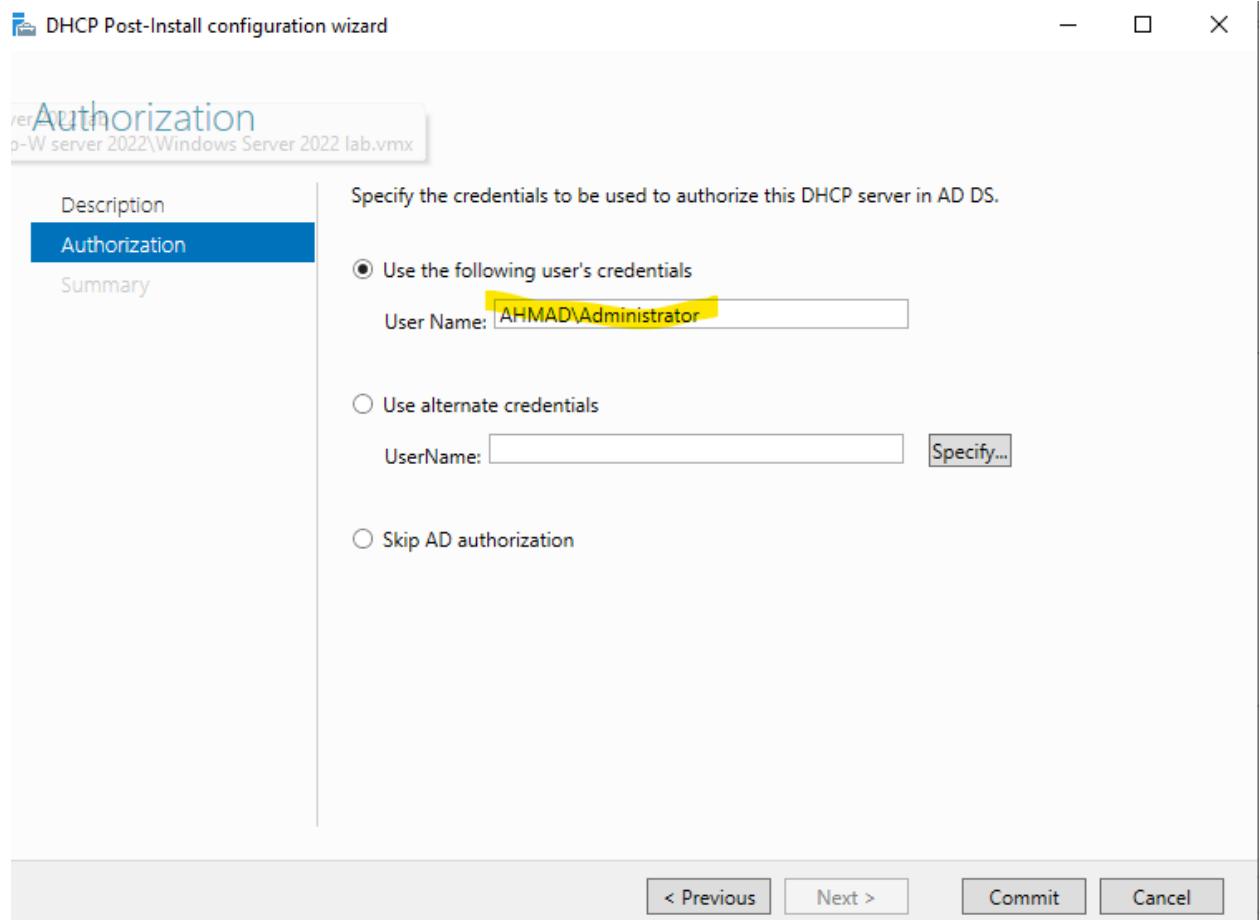
[Export configuration settings](#)

[< Previous](#)

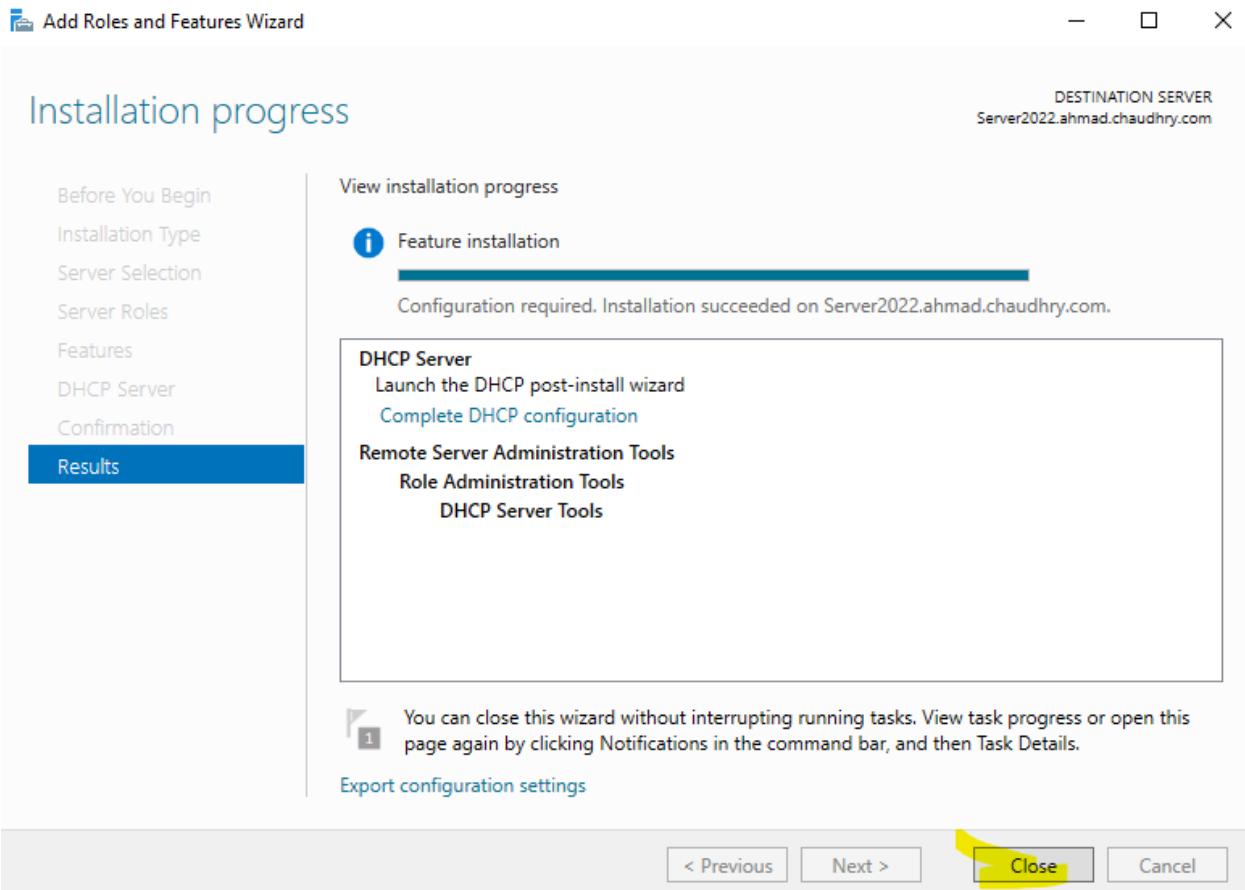
[Next >](#)

[Close](#)

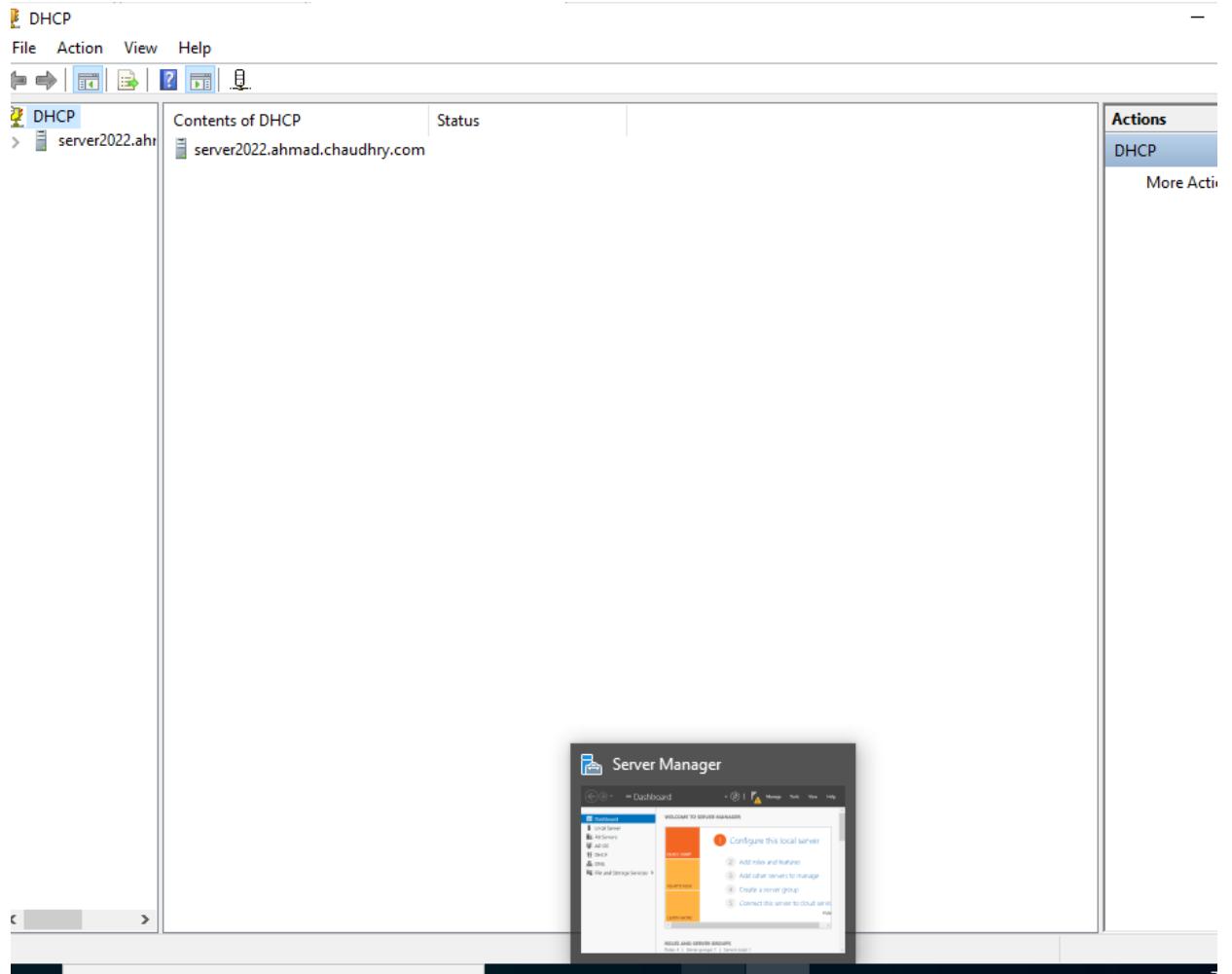
( )



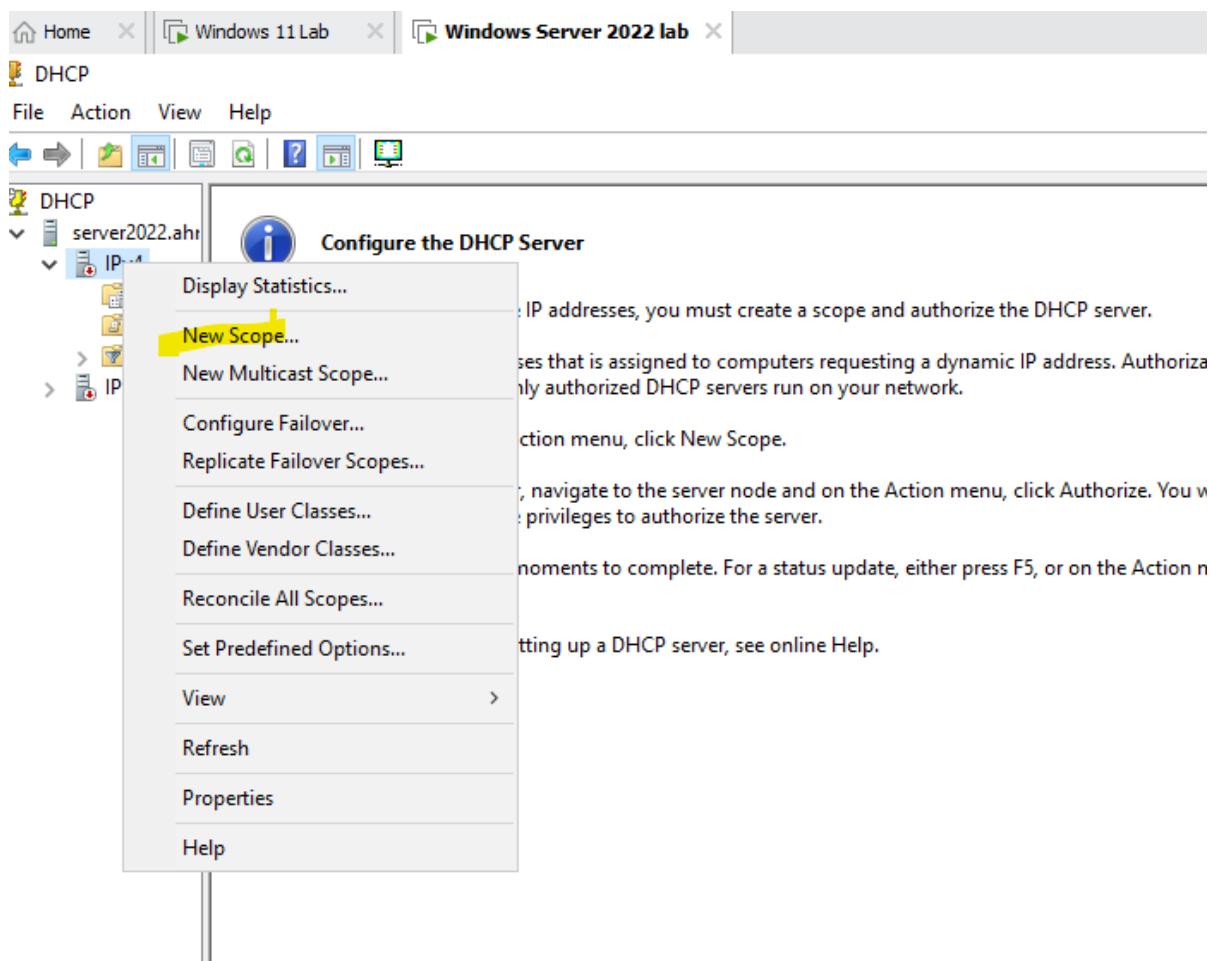
o click **close**



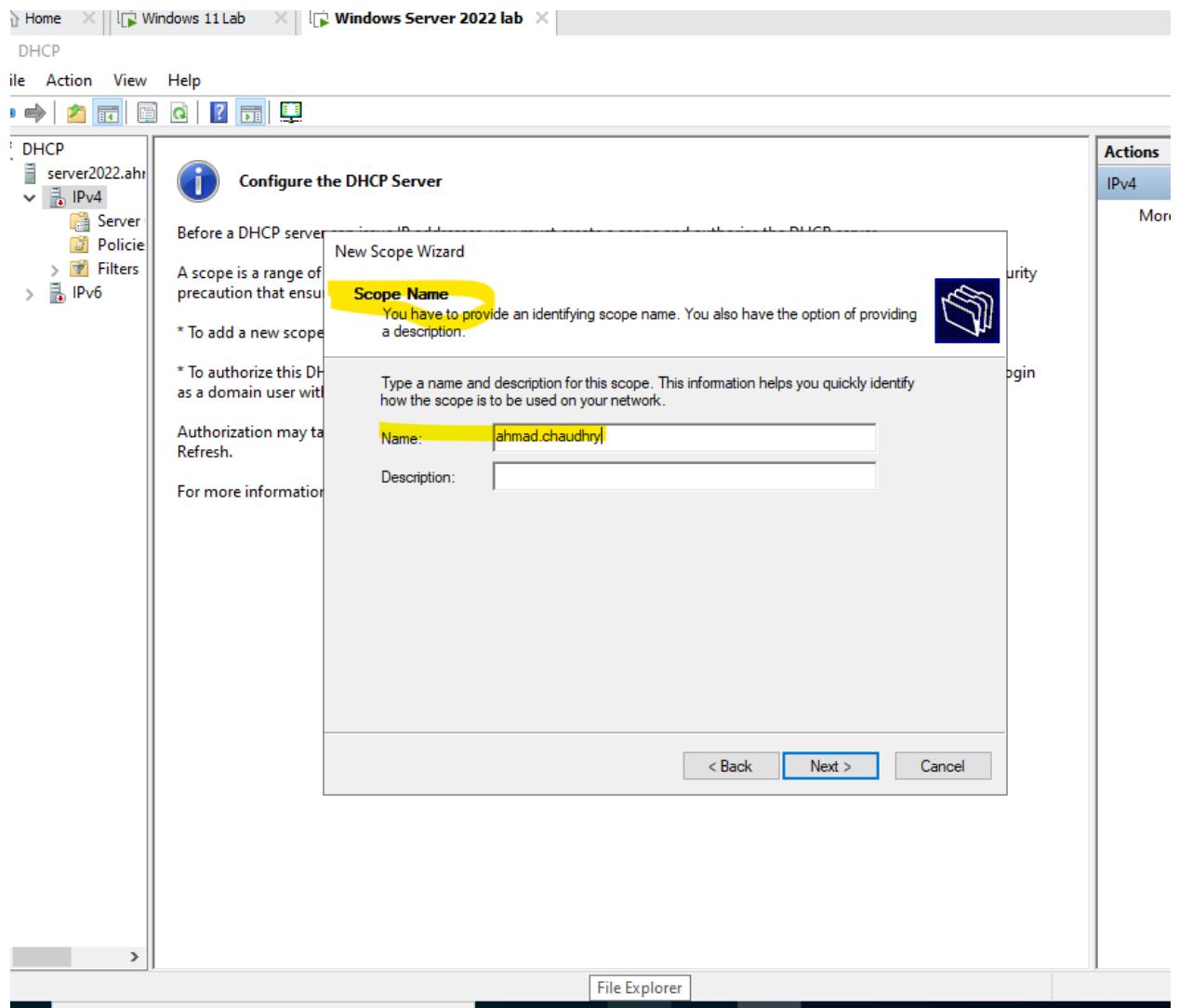
- Setting DHCP scope: **Windows Server->Server managers->Tools->DHCP** and you will see the following screen;

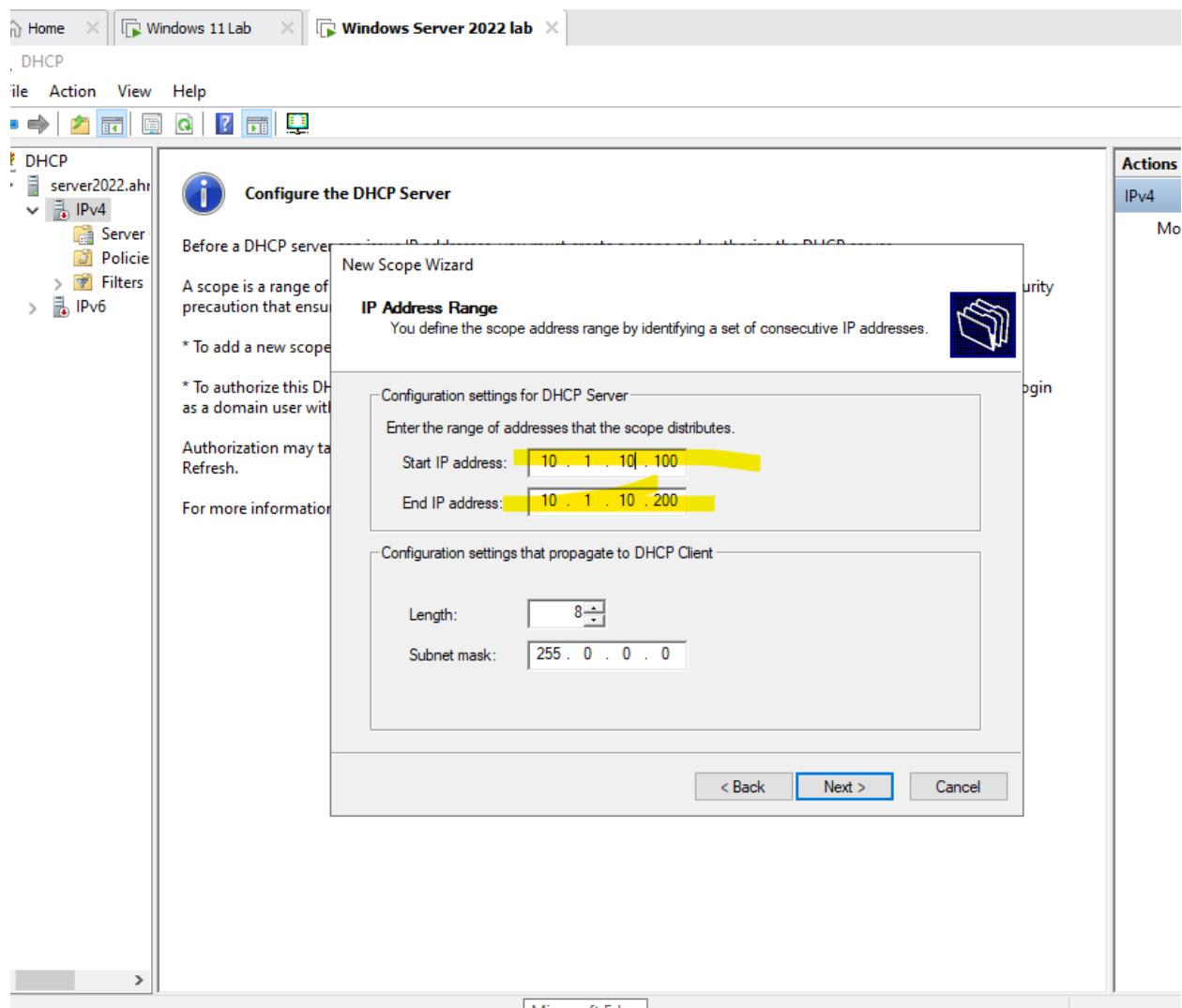


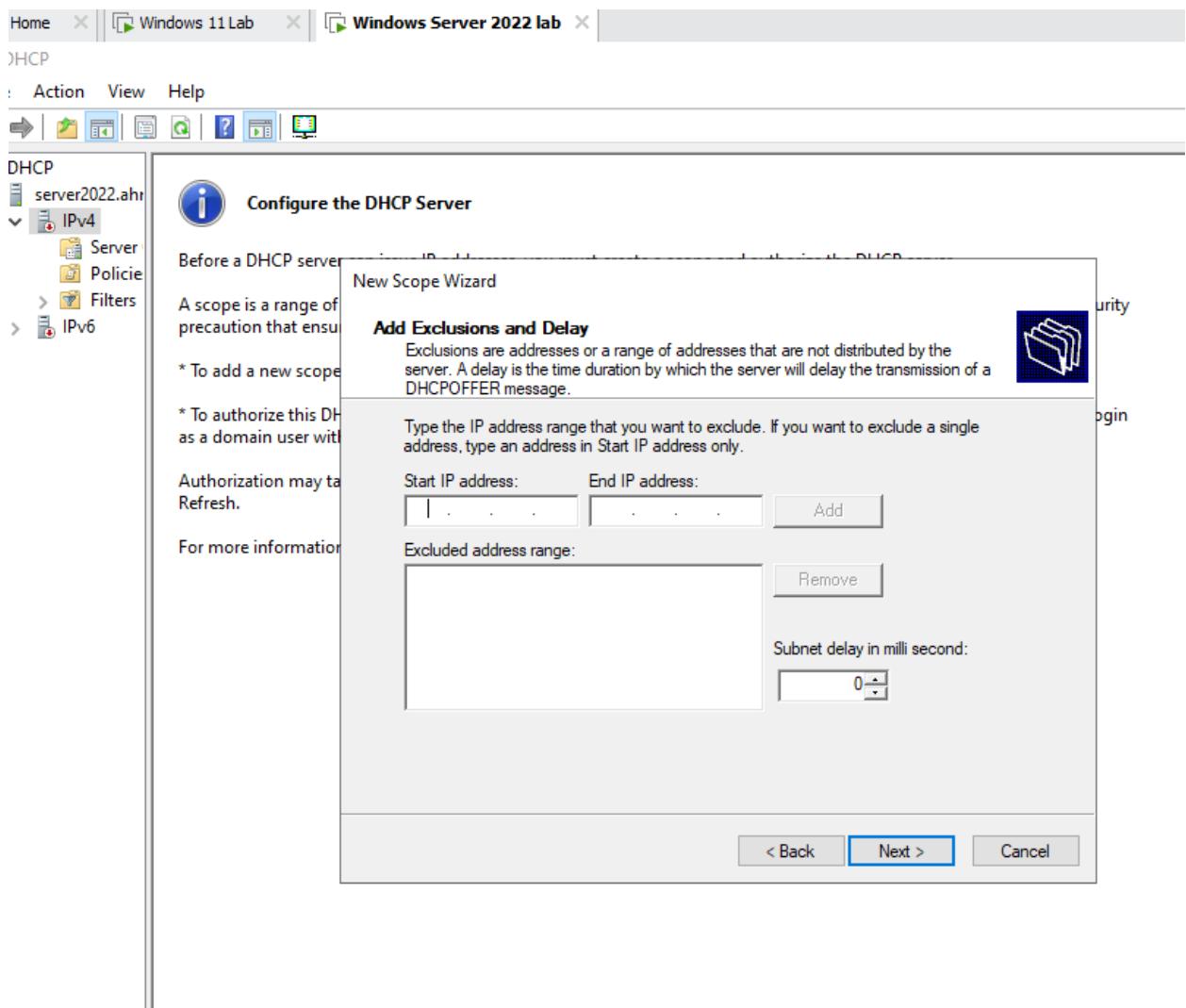
- Expand "server2022...."- and then, right click **IP4** and click **new scope**

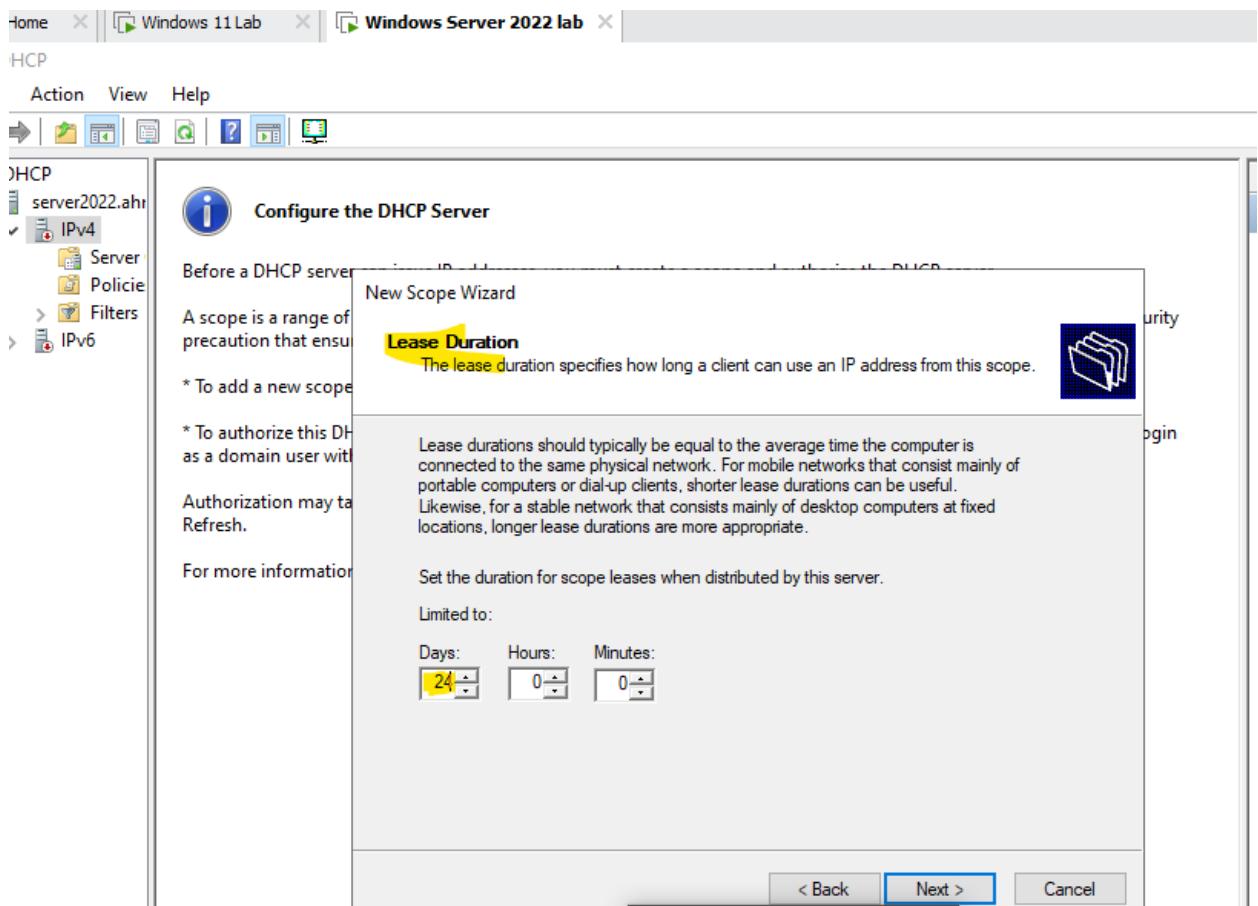


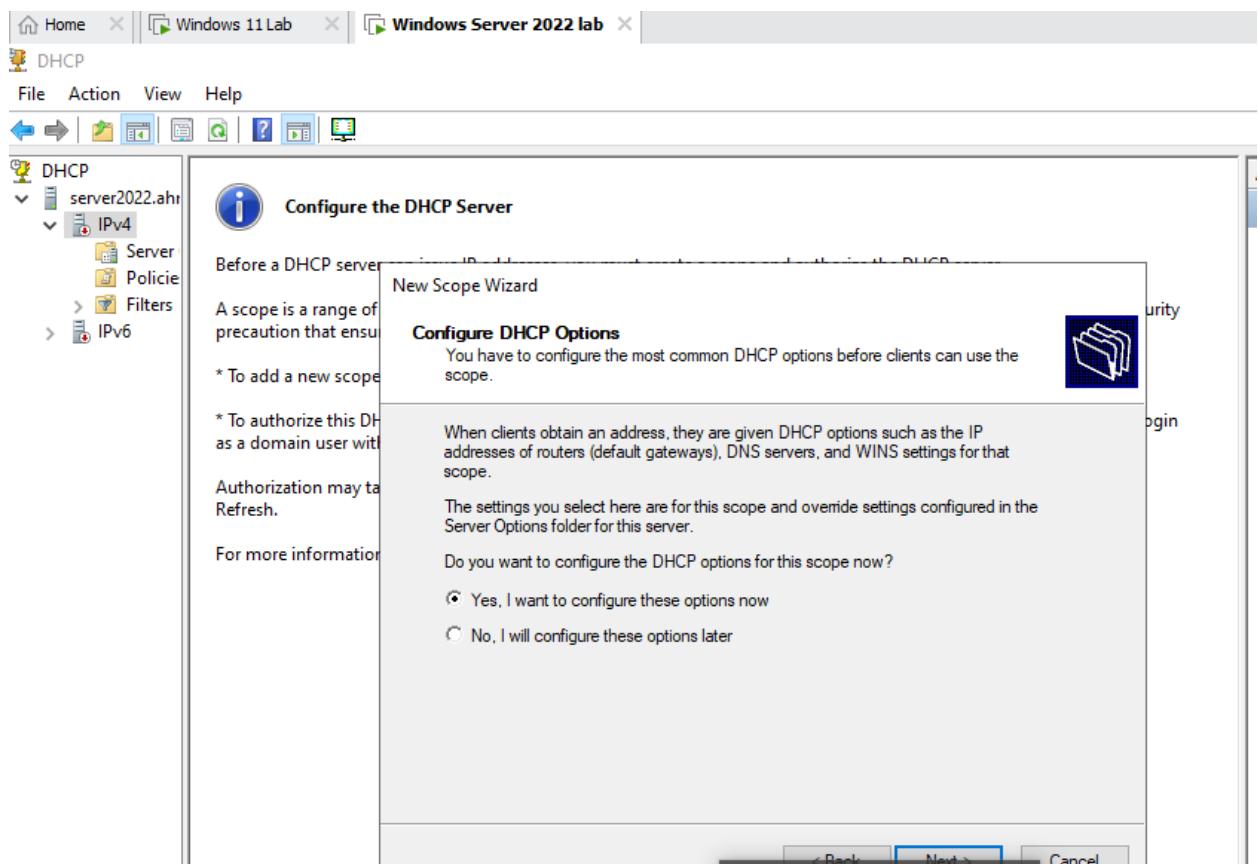
- Ensure your configuration is similar to the screenshots shown below.

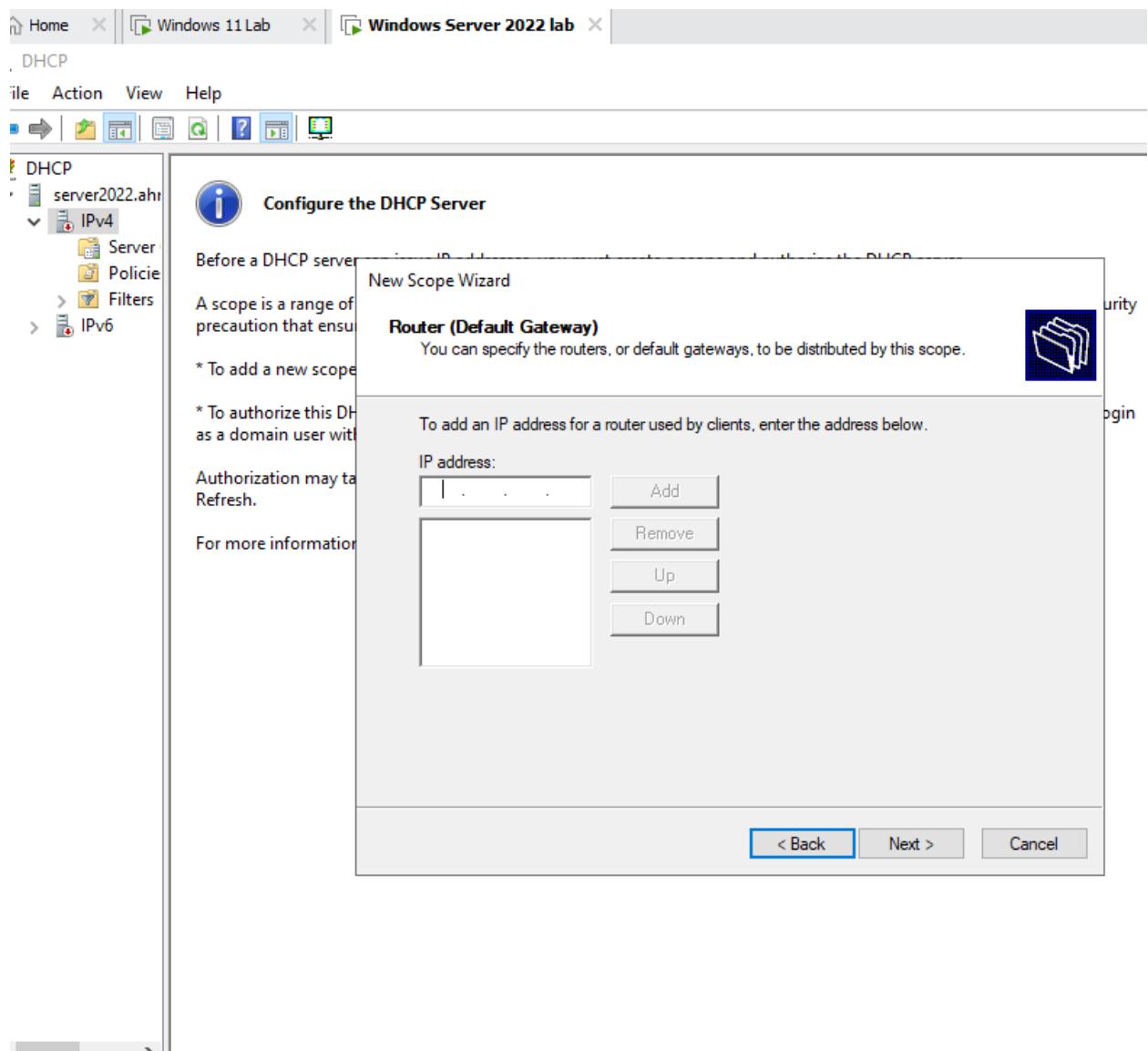


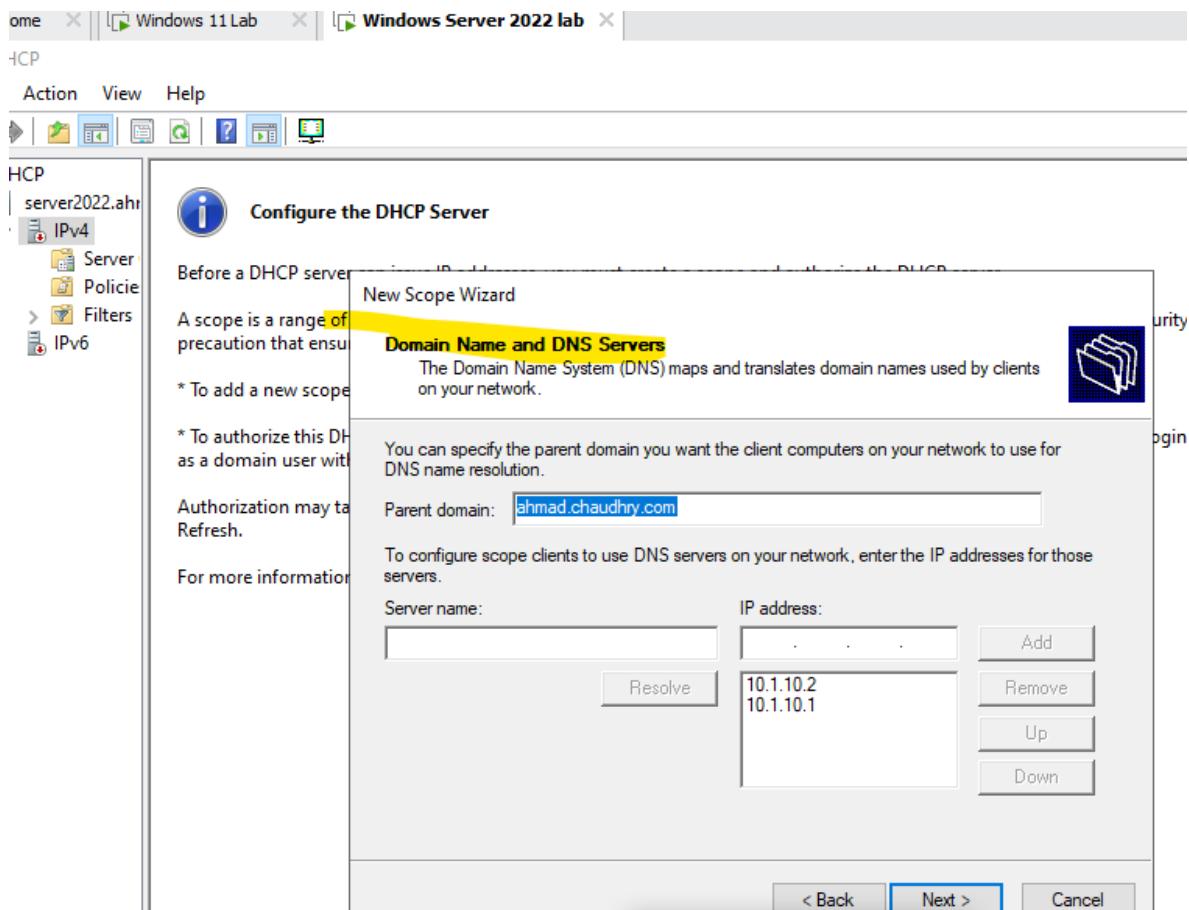


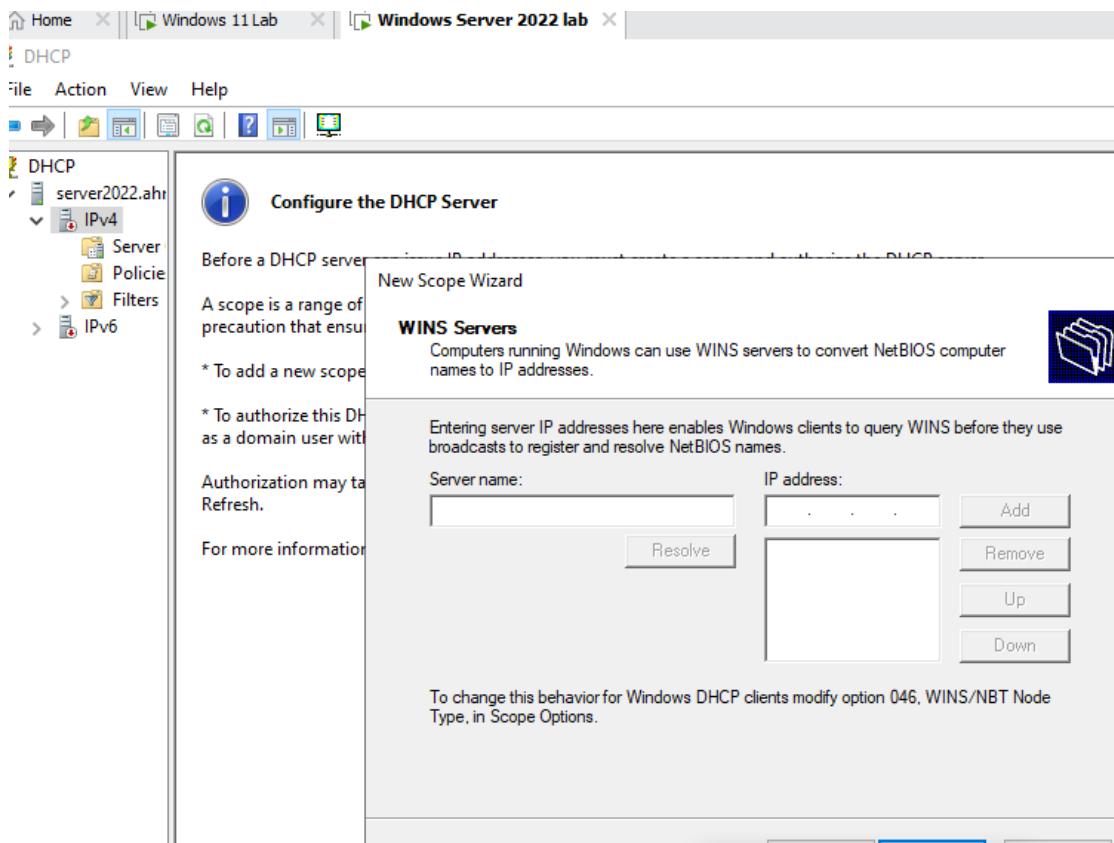


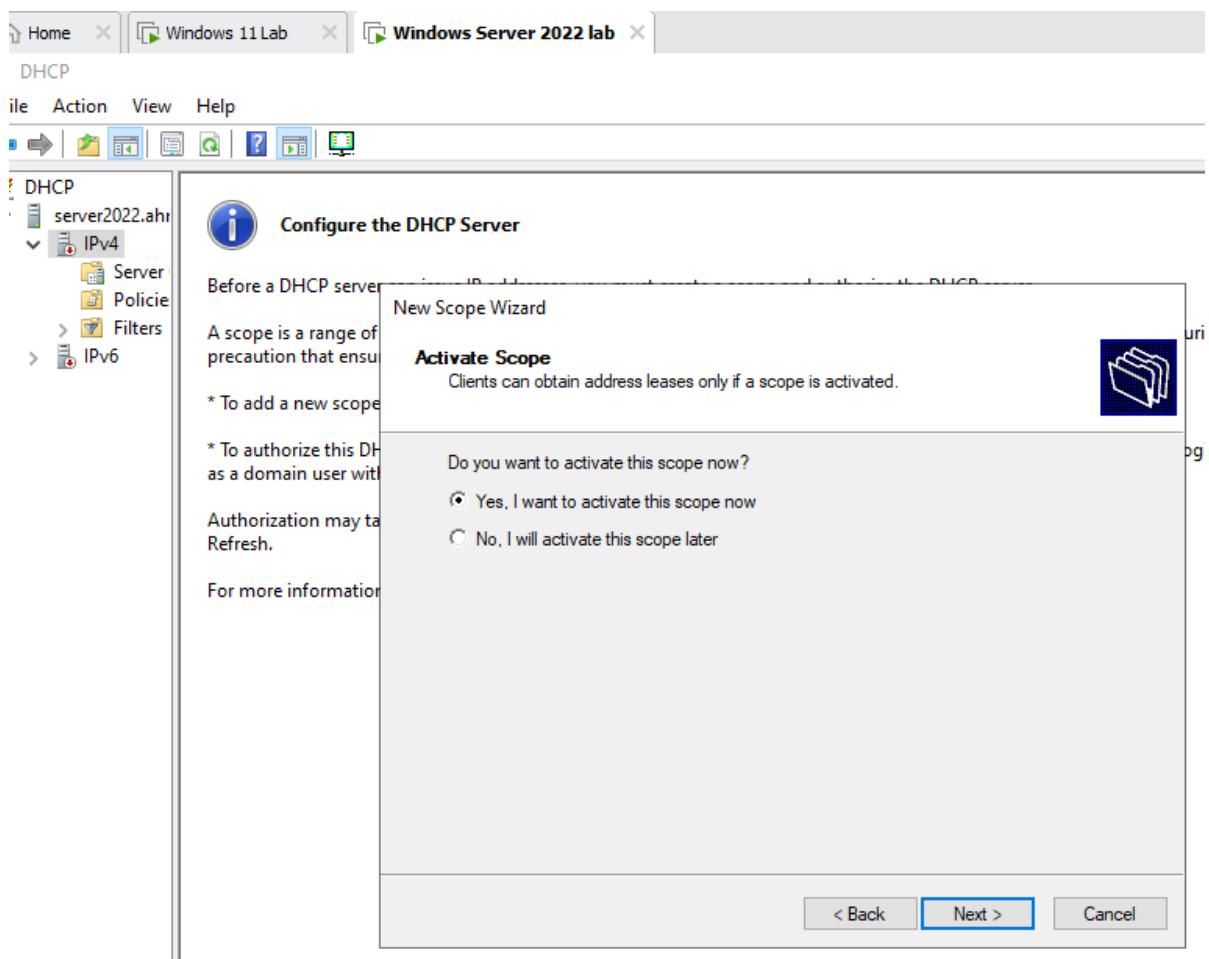




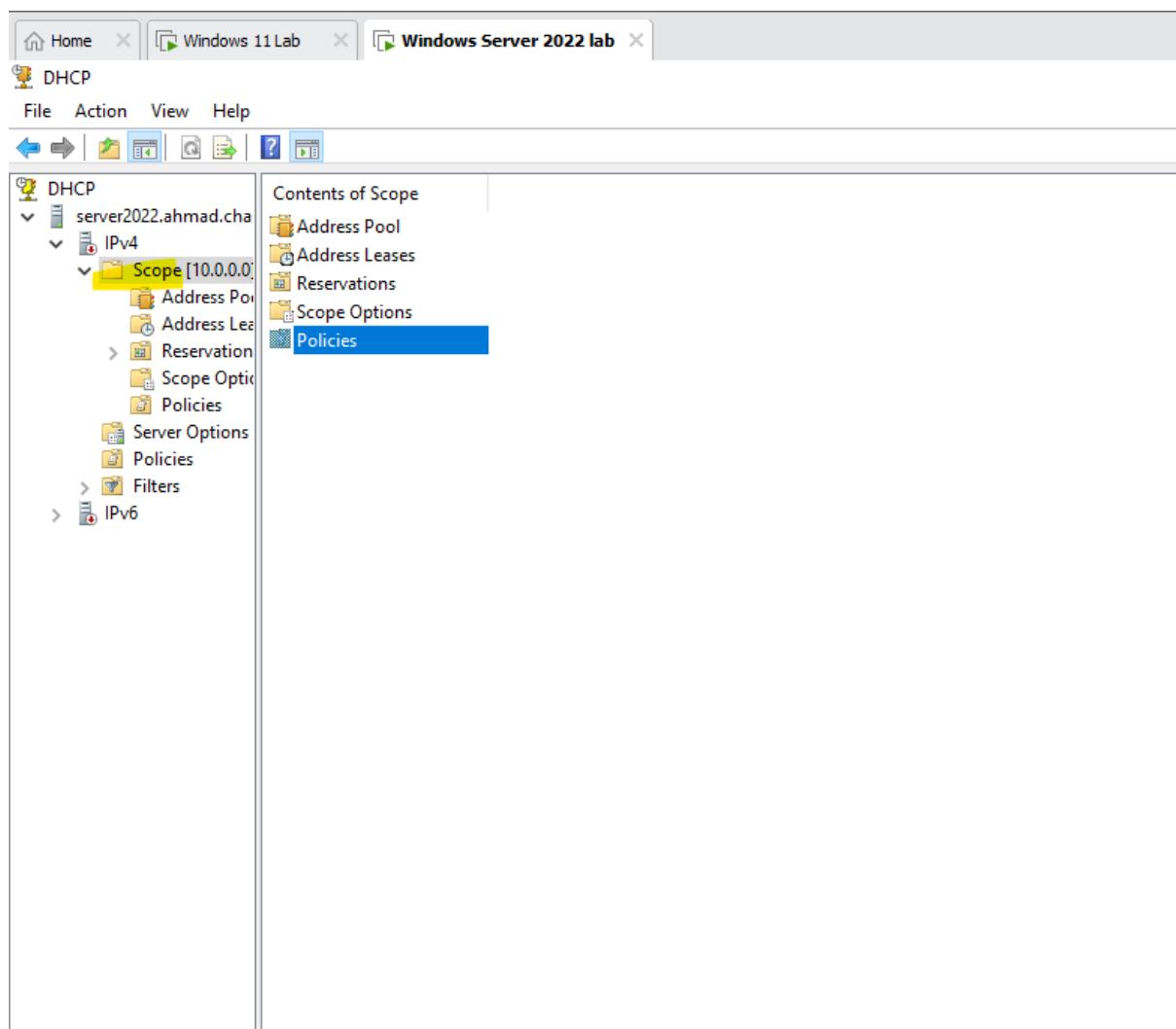




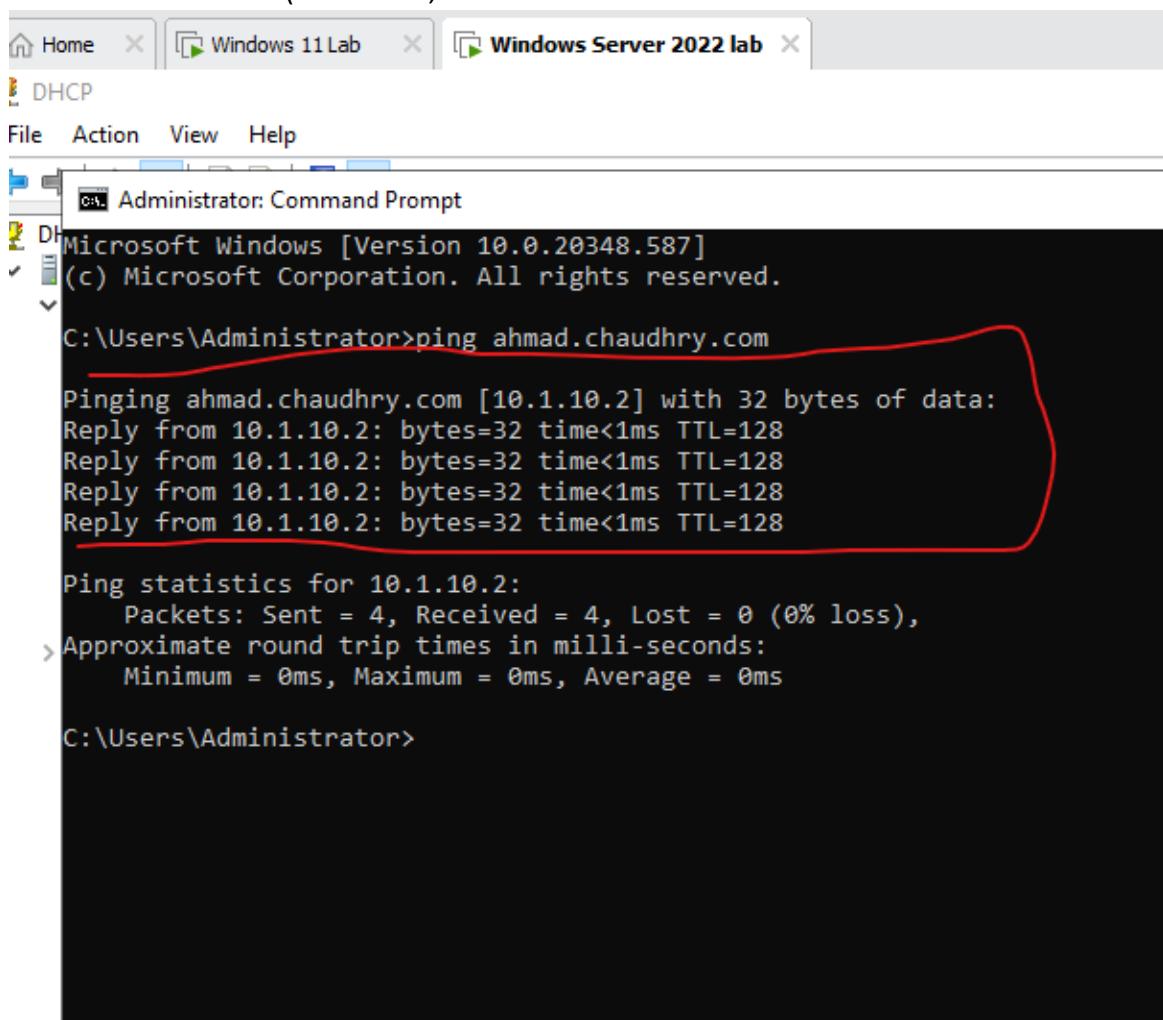




- Now, you will see the **Scope** in DHCP



- We will test whether our DNS and DHCP configurations are correct by pinging the domain name server (remember, the domain controller also functions as a server)



The screenshot shows a Windows Server 2022 Command Prompt window titled "Administrator: Command Prompt". The command entered is "ping ahmad.chaudhry.com". The output shows four successful replies from the target IP 10.1.10.2. A red box highlights the command and the reply section.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping ahmad.chaudhry.com

Pinging ahmad.chaudhry.com [10.1.10.2] with 32 bytes of data:
Reply from 10.1.10.2: bytes=32 time<1ms TTL=128

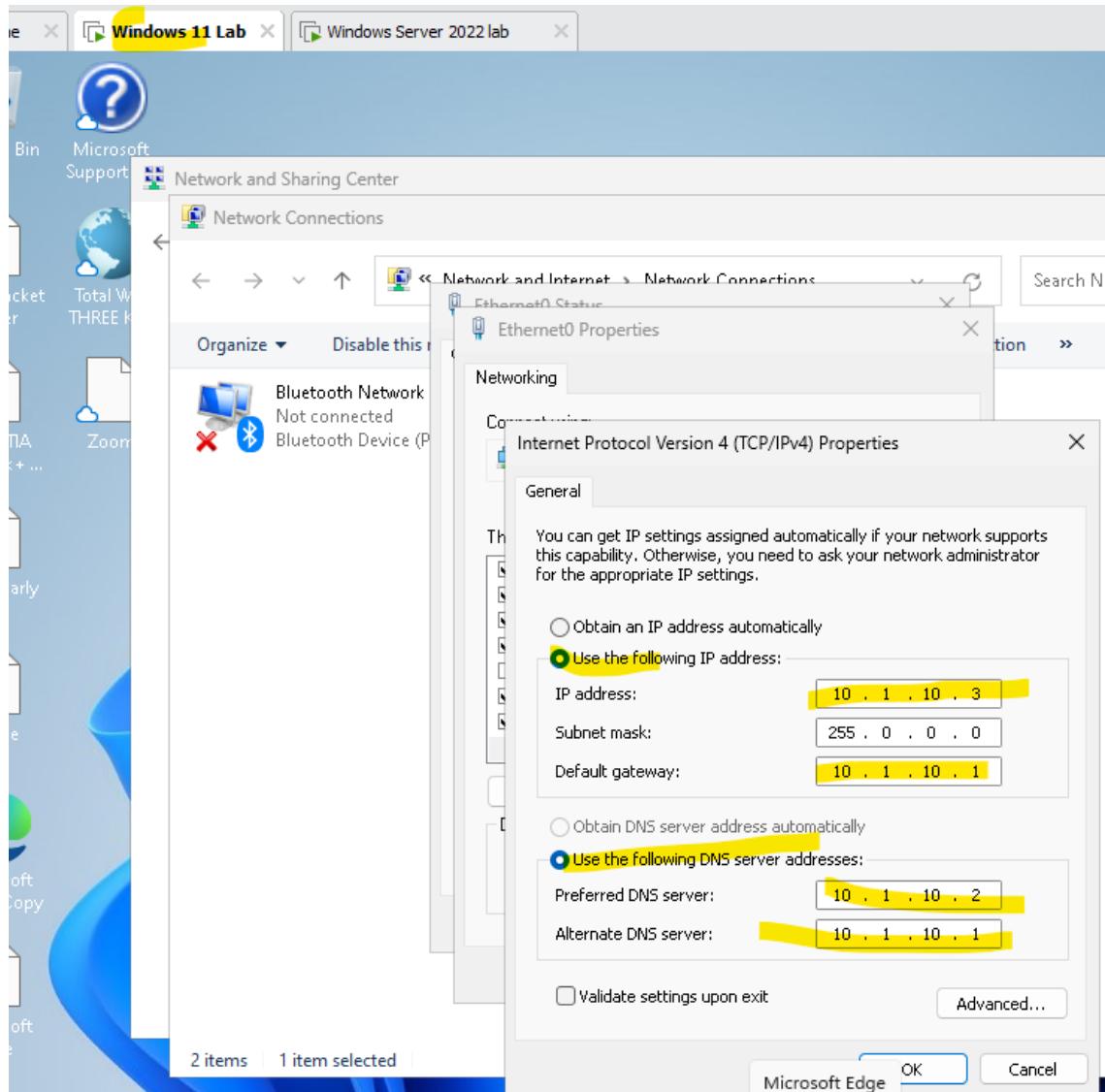
Ping statistics for 10.1.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

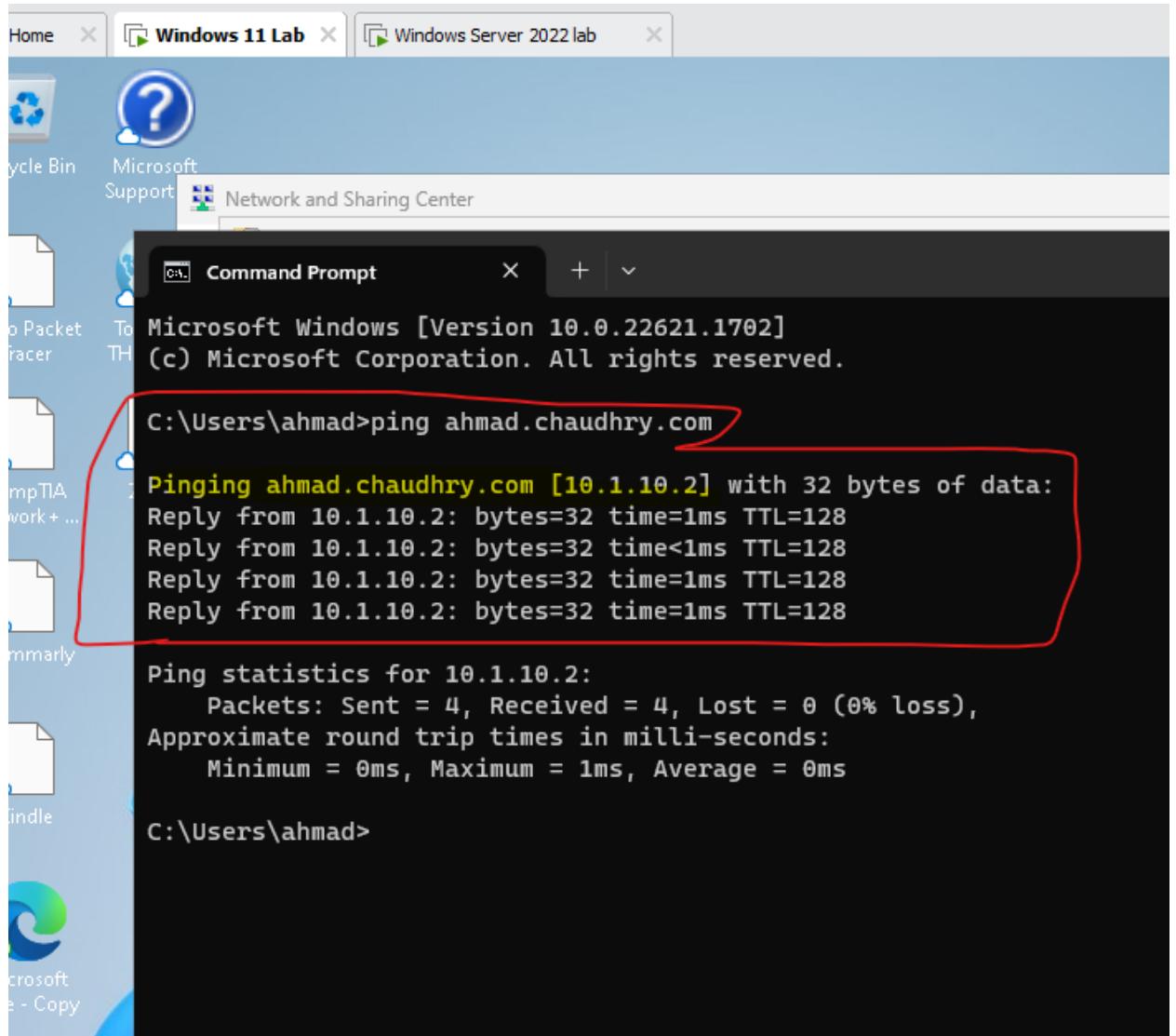
```

## Adding Windows 11 to the Active Directory Domain Server

- DNS: configure the following static IP address in Windows 11



- Test if it pings to the domain controller server



The screenshot shows a Windows 11 desktop environment. In the center, a Command Prompt window is open with the title "Command Prompt". The window displays the following text:

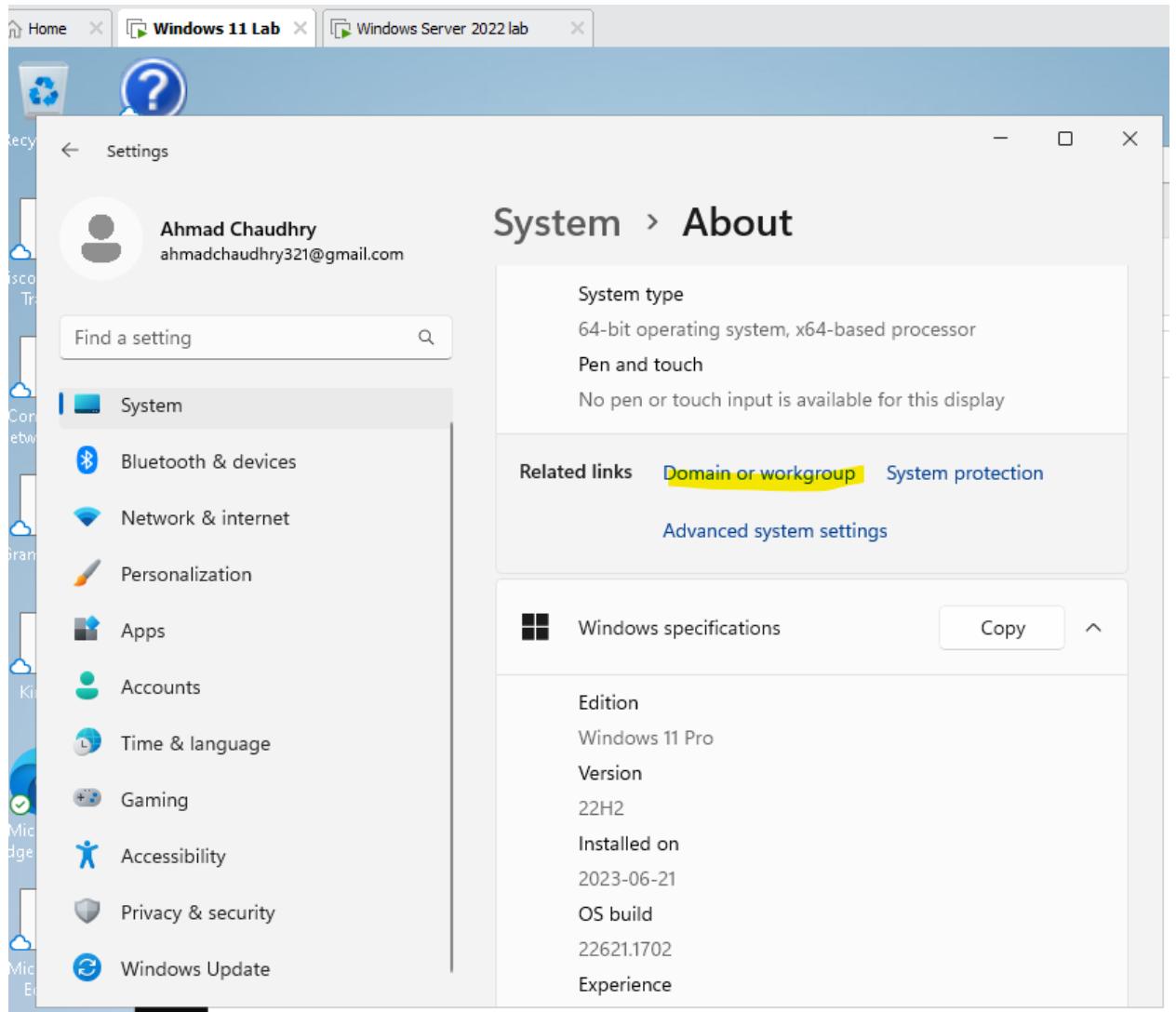
```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

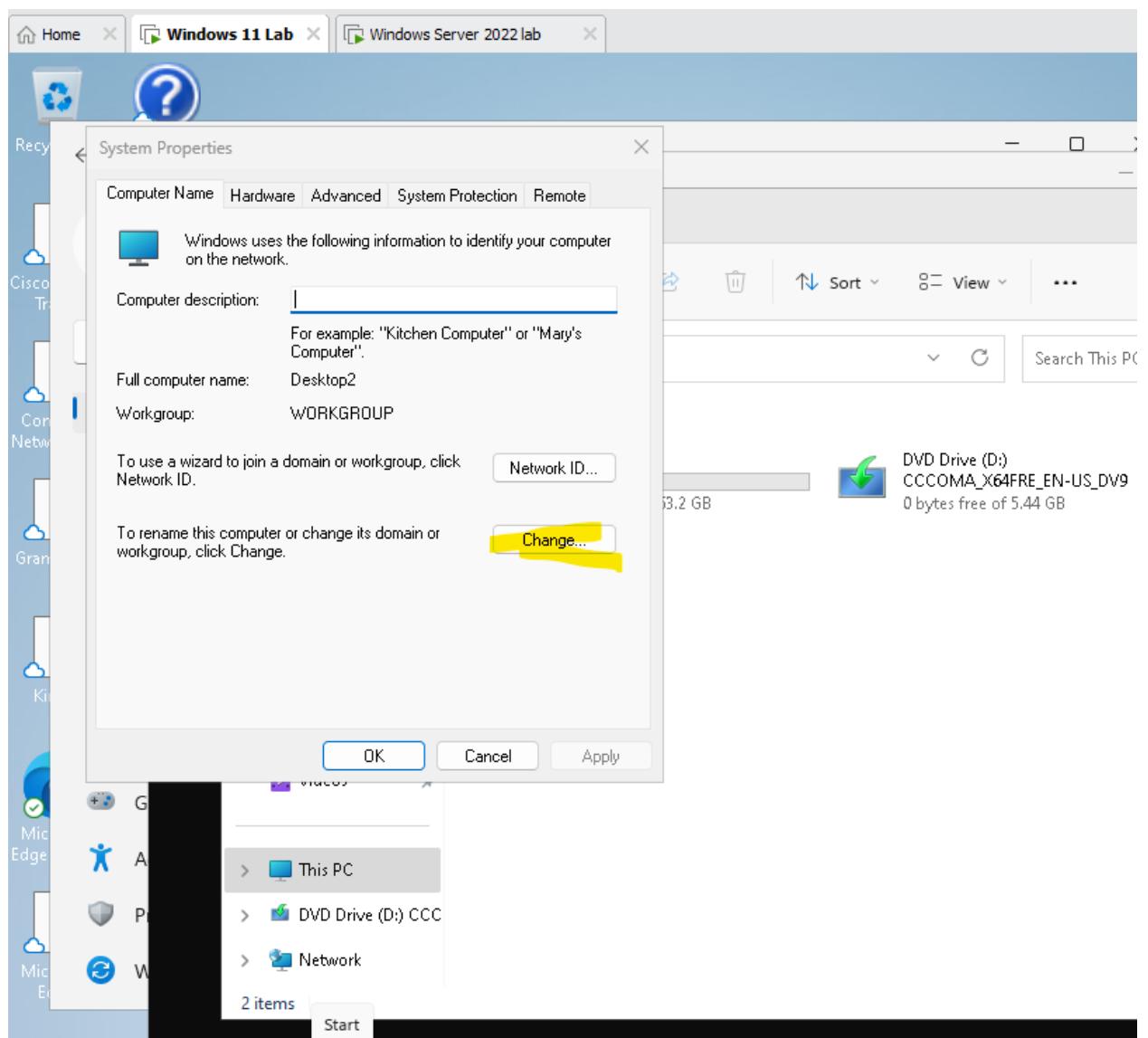
C:\Users\ahmad>ping ahmad.chaudhry.com
Pinging ahmad.chaudhry.com [10.1.10.2] with 32 bytes of data:
Reply from 10.1.10.2: bytes=32 time=1ms TTL=128
Reply from 10.1.10.2: bytes=32 time<1ms TTL=128
Reply from 10.1.10.2: bytes=32 time=1ms TTL=128
Reply from 10.1.10.2: bytes=32 time=1ms TTL=128

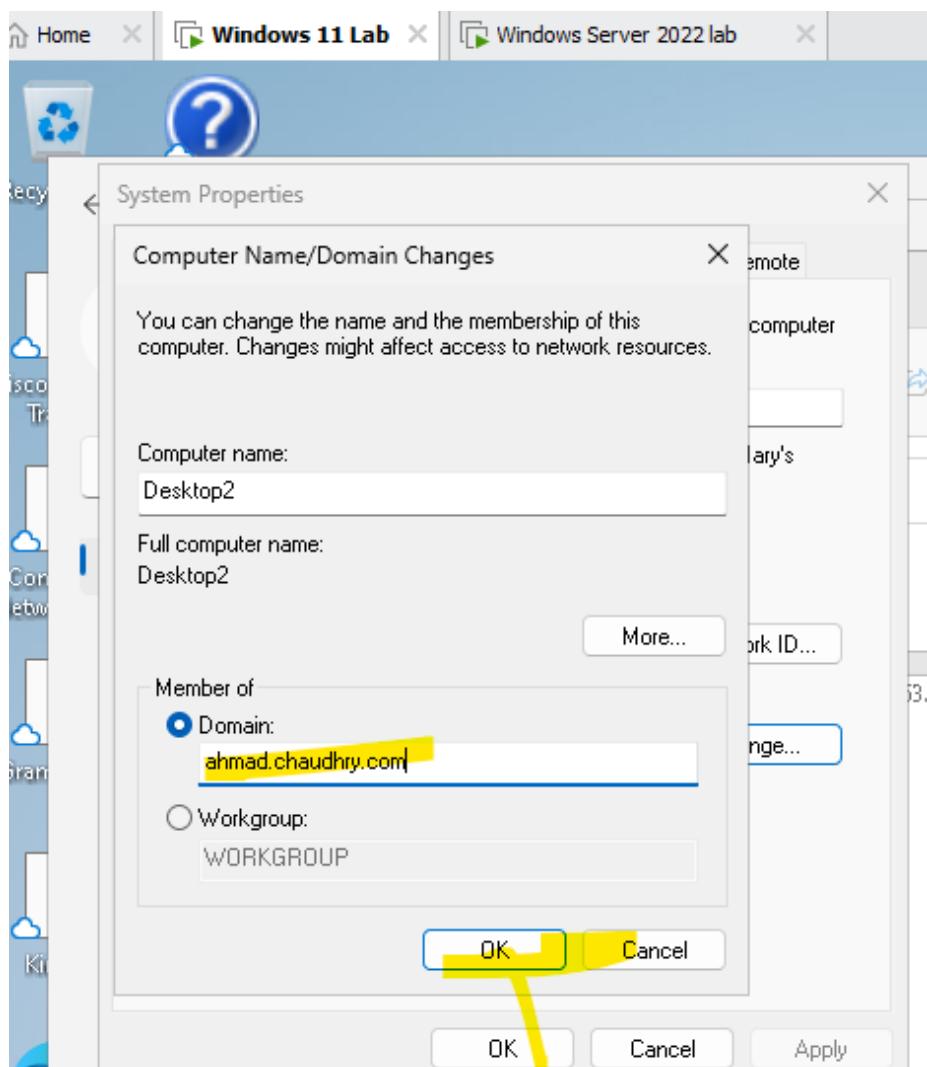
Ping statistics for 10.1.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

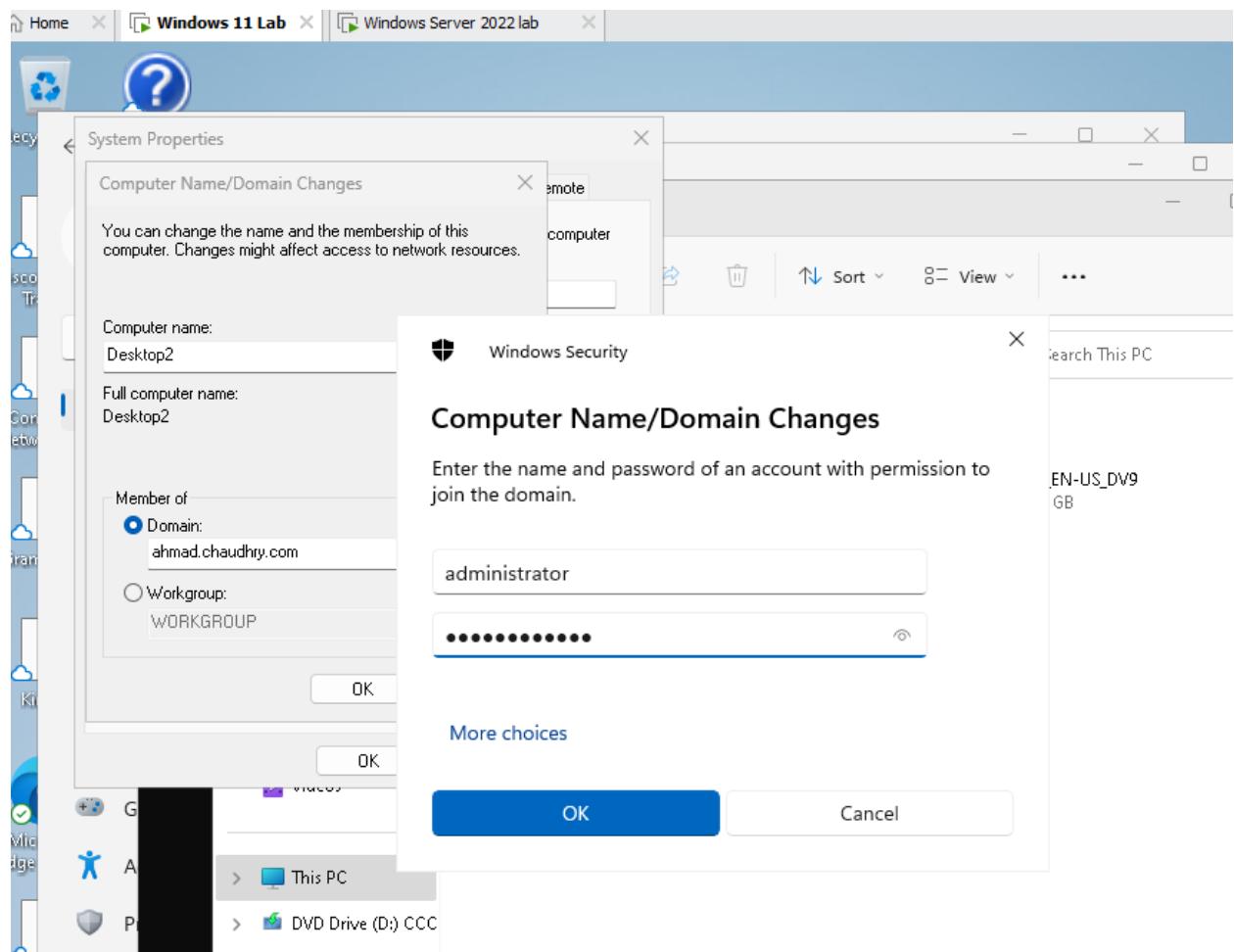
C:\Users\ahmad>
```

- To add PC to the domain: open **file explorer**->right click **this PC** ->**properties** and the settings window will appear. Scroll down and select **domain or workgroup** (1st screenshot)->click “**change...**” under the **computer name** tab (2nd screenshot). Enter the domain controller server name (3rd screenshot), then enter the administrator password (4th screenshot). A welcome message will appear, and you must restart the PC for changes to take effect



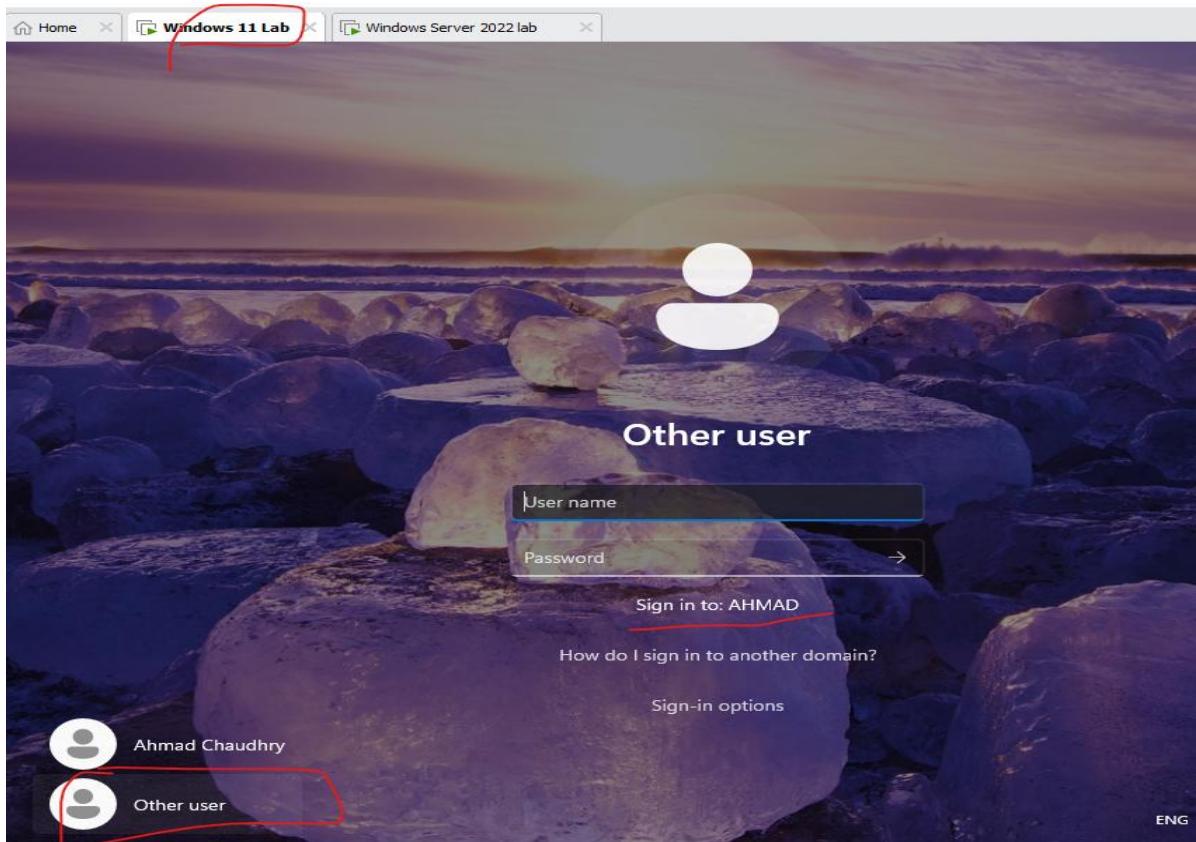




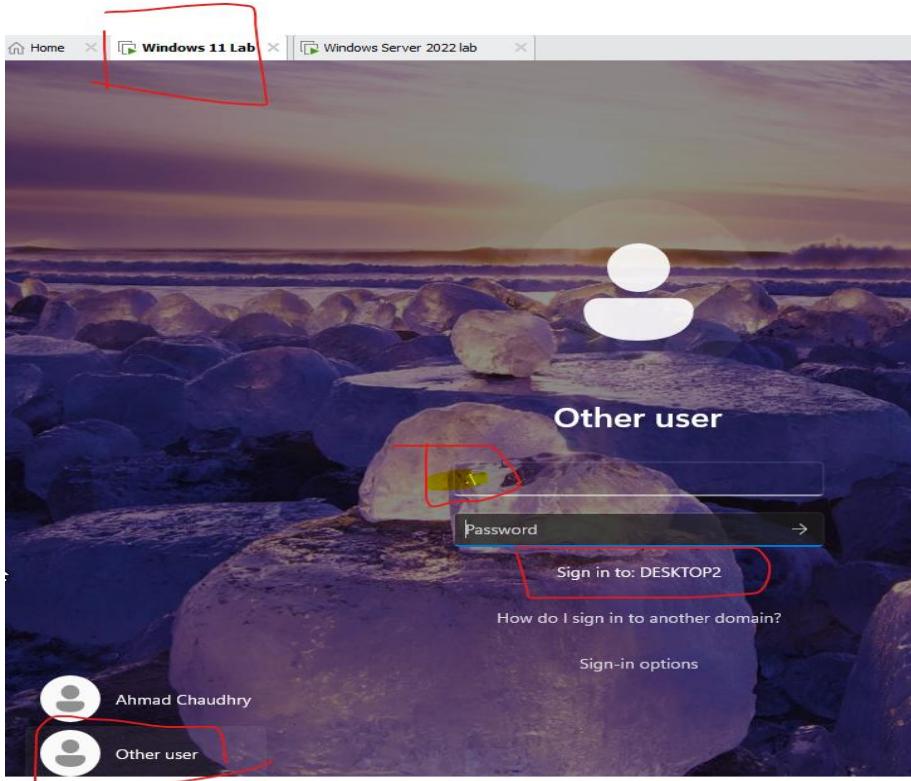


### Testing if the PC is entered in the domain correctly

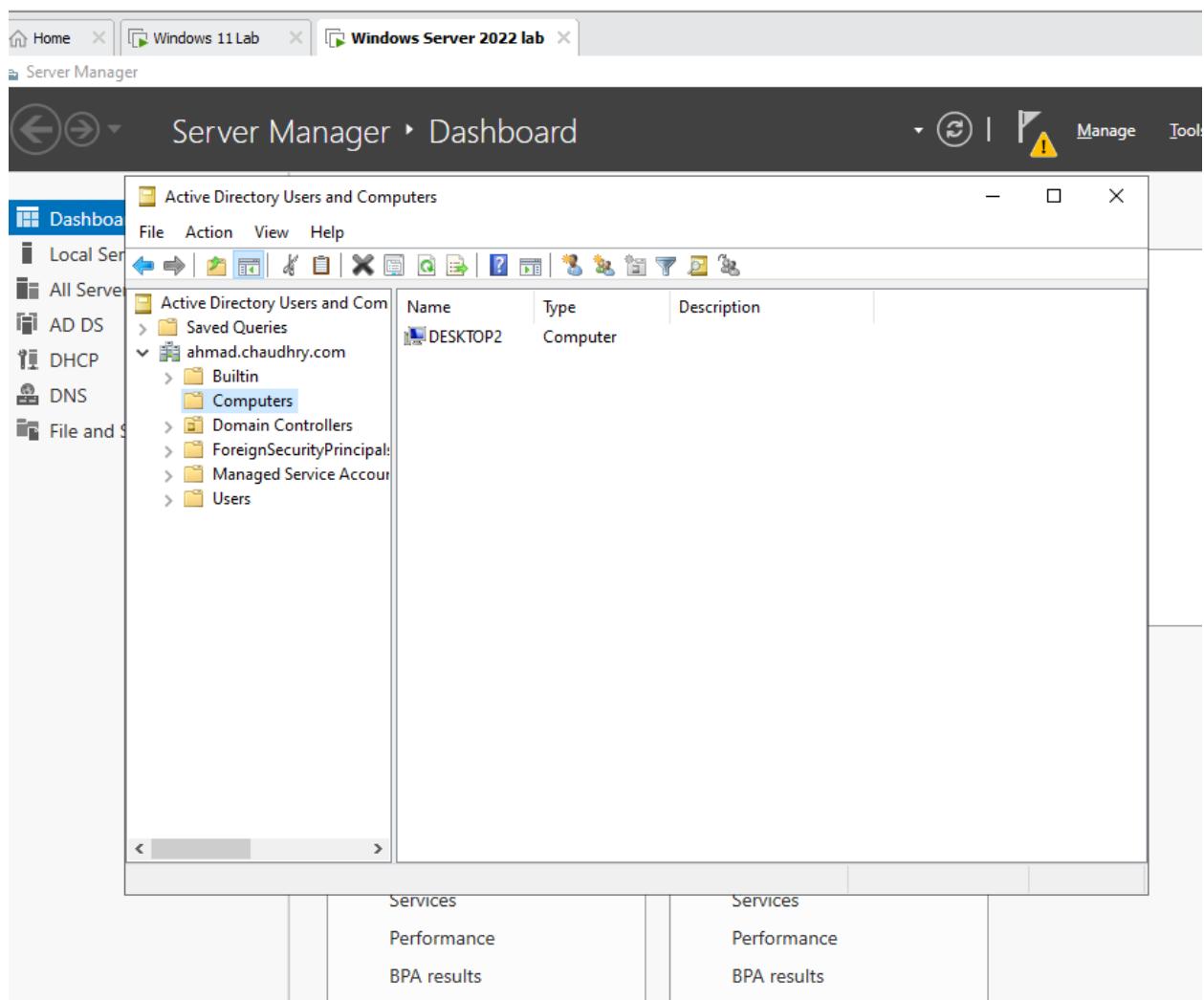
- Test 1;
  - Click **other user** on the Windows 11 Lab and you will see the domain name



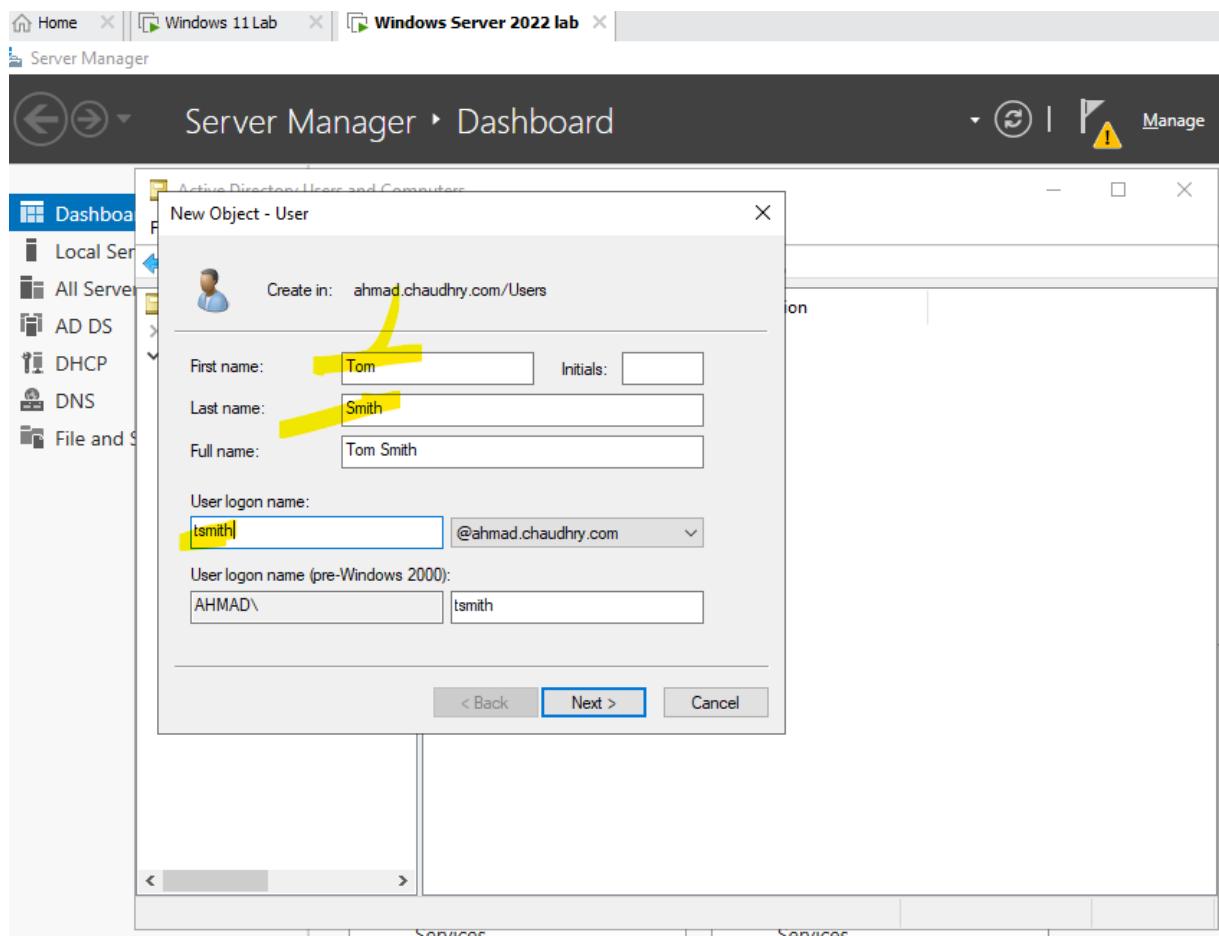
- Test 2
  - Click **other user** on the Windows 11 Lab screen. You will see the domain name and type "./" and your PC name will be displayed



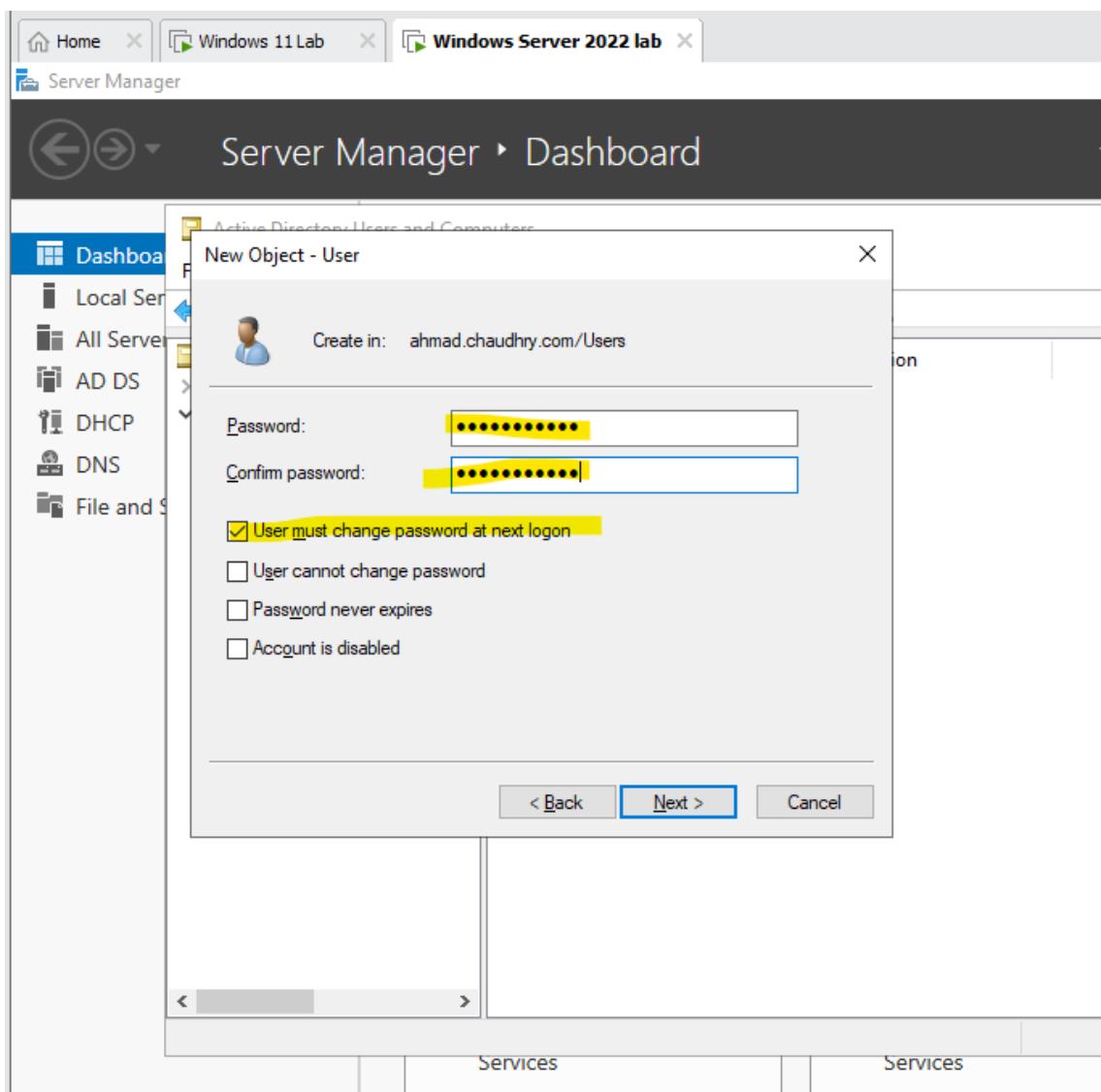
- Test 3
  - In Windows 2022 Server->go to **server manager**->**tools**->click **Active Directory users and computers**->click **domain controller**->**computers** and you will see the Windows 11 VM name (Desktop 2)



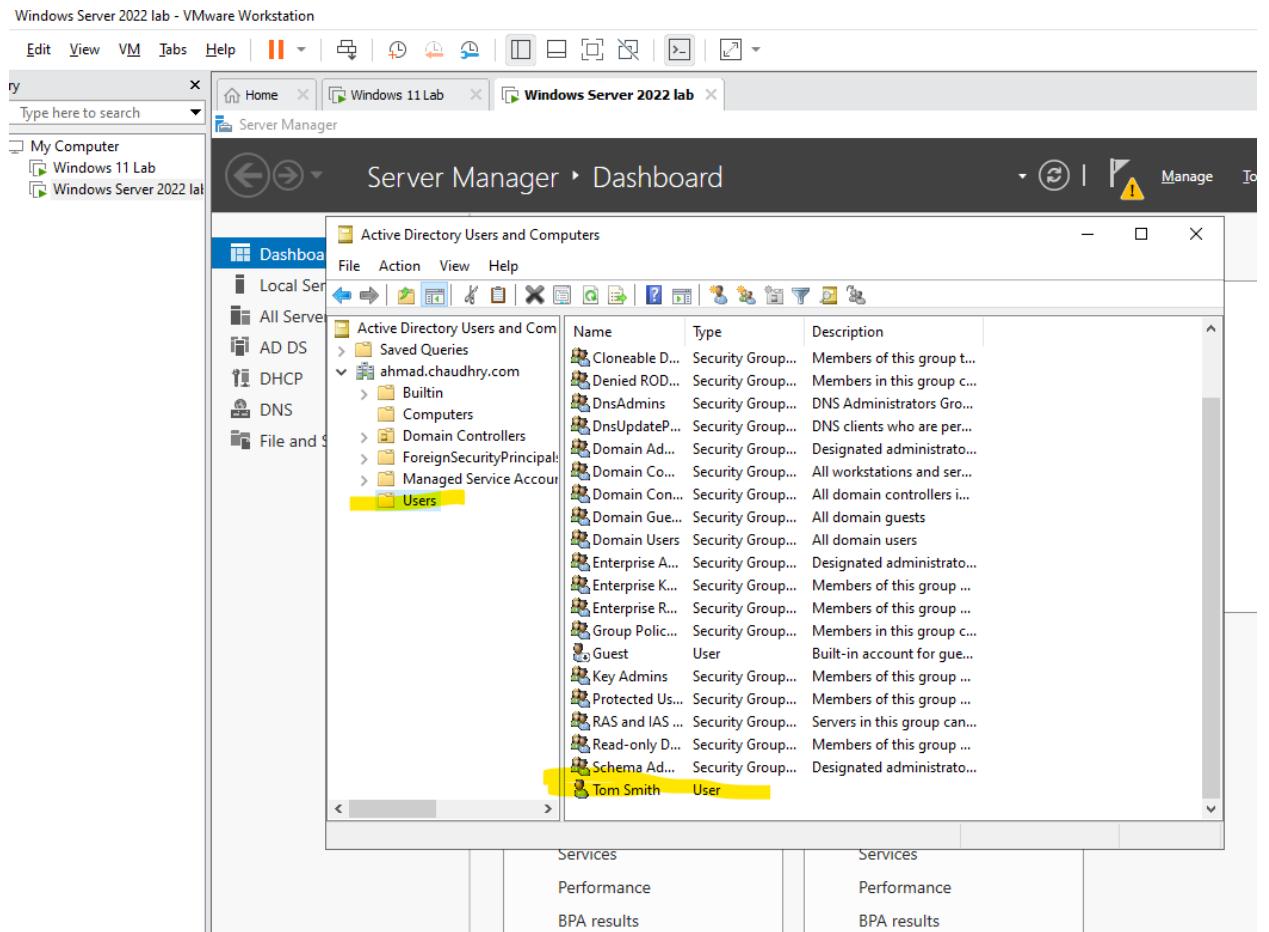
- Test 4
  - In Windows 2022 Server->go to **server manager->tools->click "Active Directory users and computers"**->right click **users->New->User** and create a user. Ex, we created Tom Smith



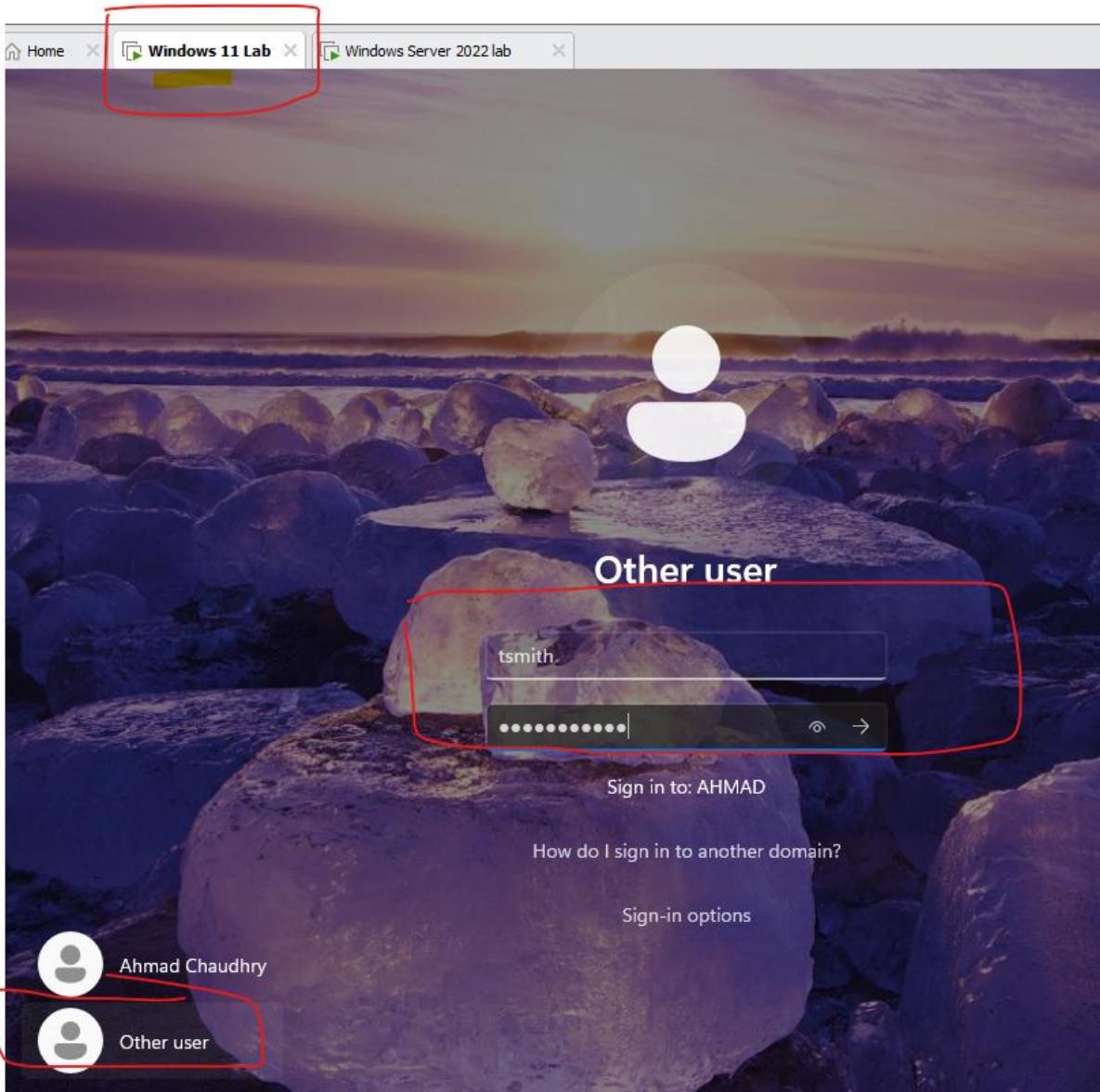
- Assign a password to the user



- You should see Tom Smith's account in **Users**



- On Windows 11 VM, go to the login screen and sign in with Tom Smith's credentials. When prompted, change the password

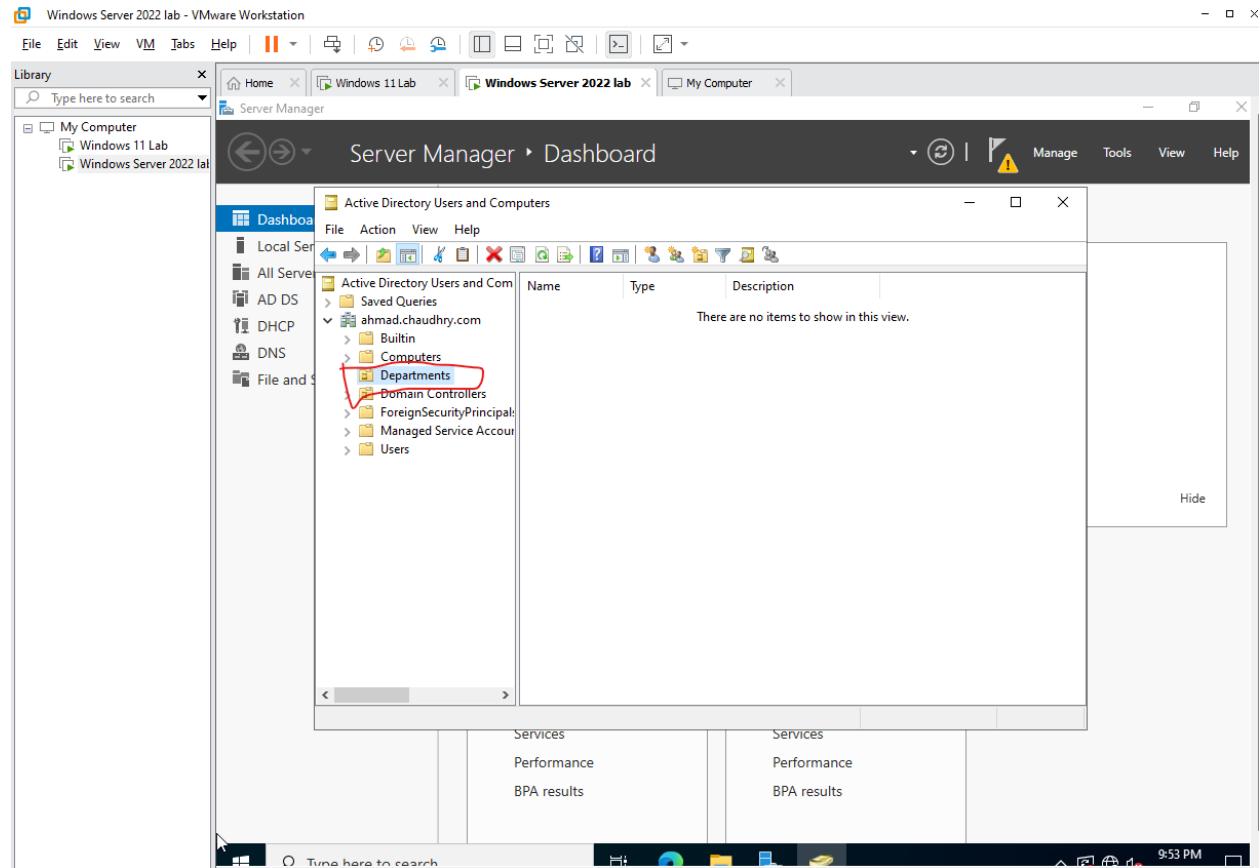


**Note:** The domain server must be **turned on** if you are trying to connect the Windows 11 VM to the domain

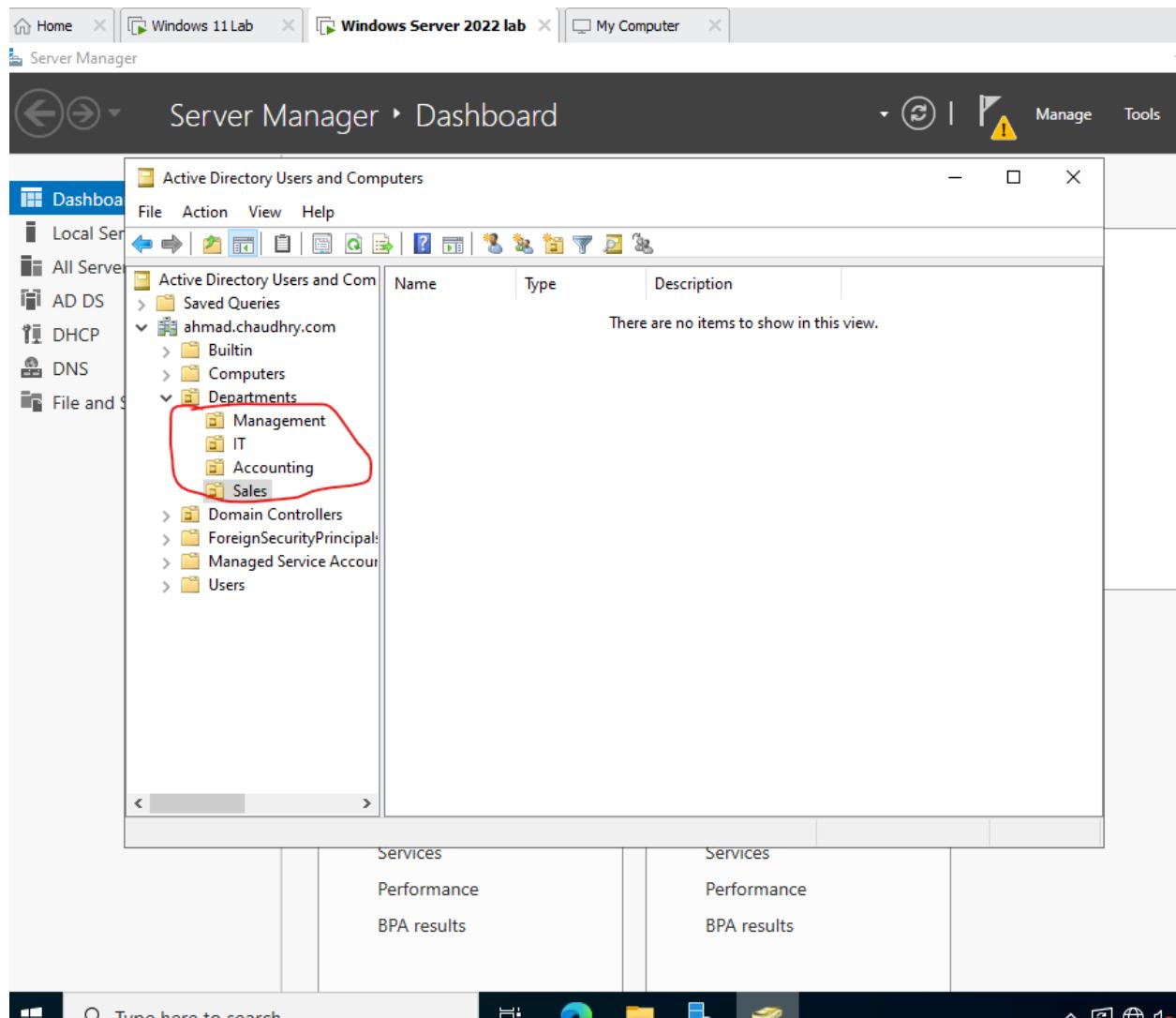
## Creating Organizational Units and Users

I created the department OU and four child OUs for the departments.

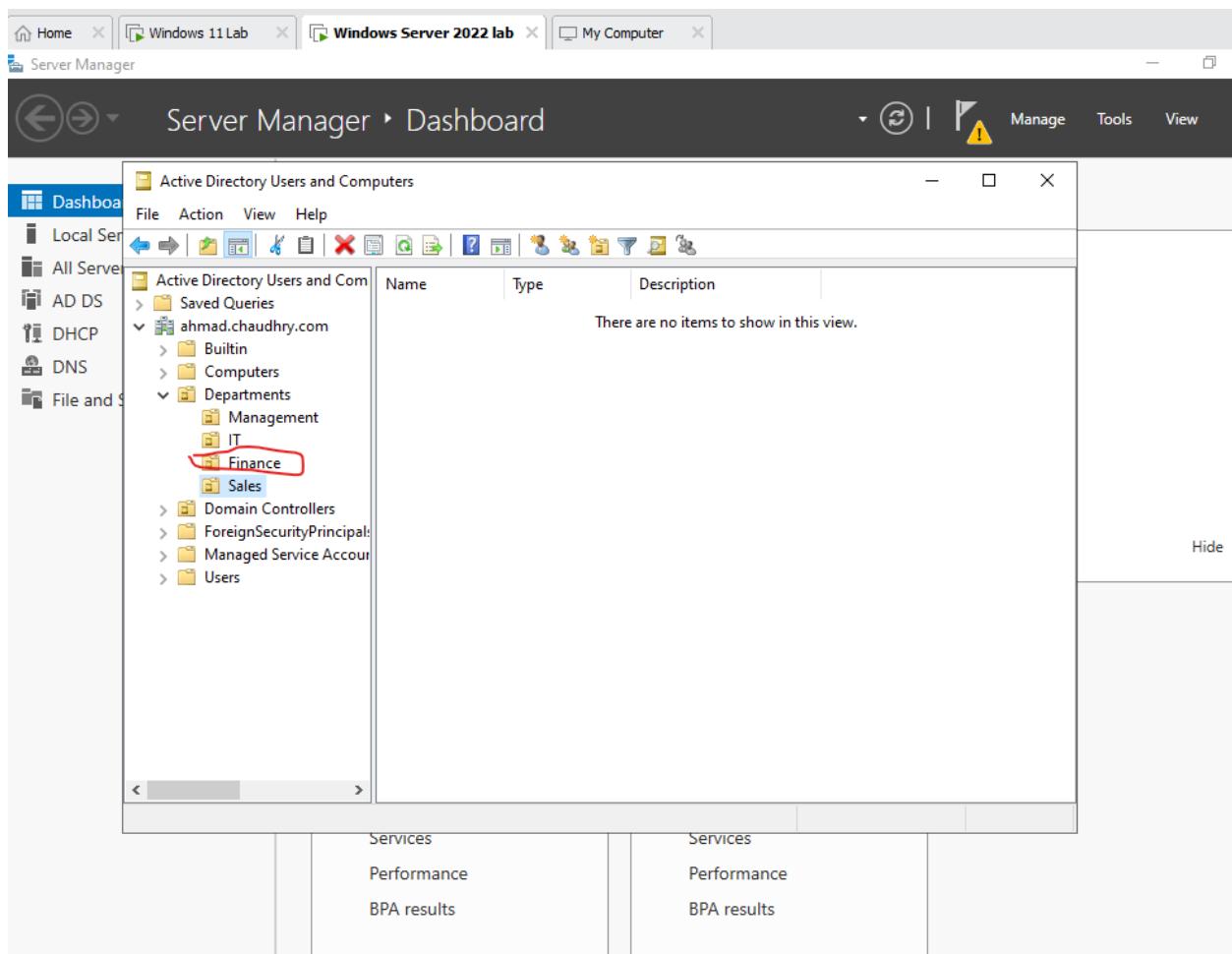
- Department OU: Server Manager->Tools->Active Directory Users and Computers->Right click **domain controller server** (ahmad.chaudhry.com) and click **New->Organizational Unit** and name it "departments"



- Create 4 departments or child OU: Right-click "Departments" OU->**New->Organizational Unit**-> and name them. See the screenshot below for the four different departments



- Rename "Accounting" child OU to "Finance"->Right click "Accounting" child OU and click **rename**-> name it to "**Finance**"

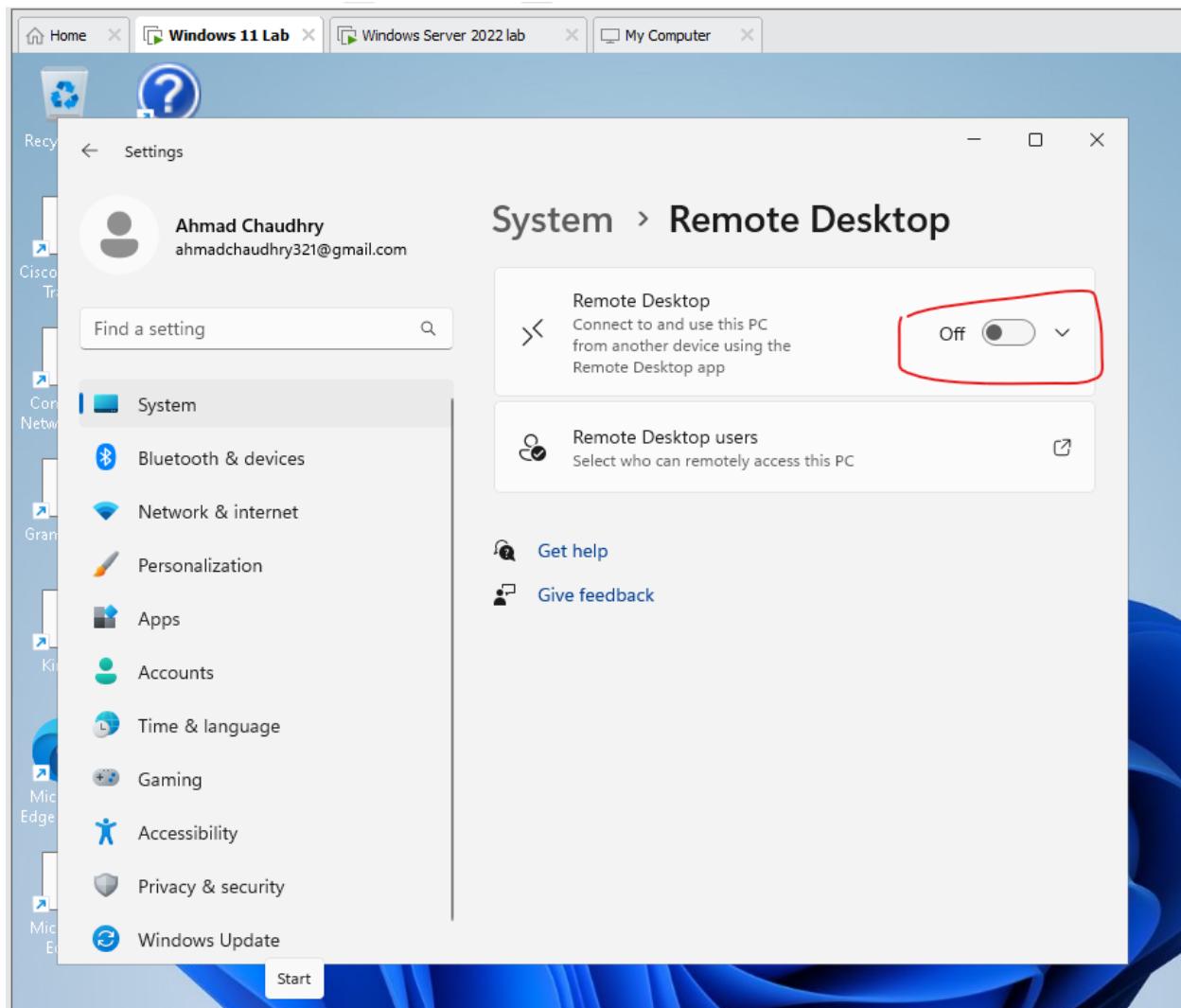


- I created users in each department. There are two ways to create a user:
  1. Right-click **department name->new**
  2. Or click **department name->new->click use**

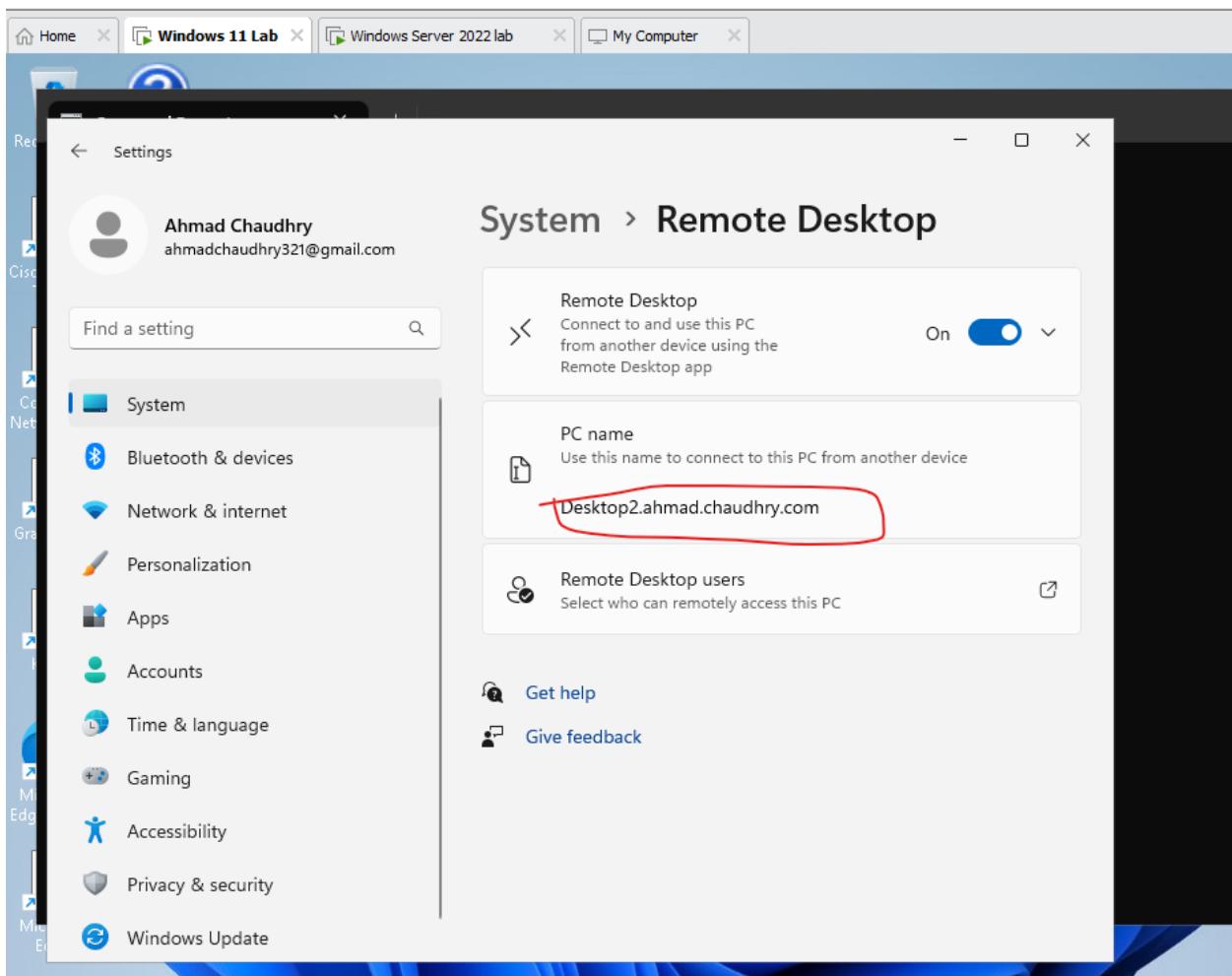
## Remote Connection

### RDP

- We will enable RDP on Windows 11 VM by doing the following:
  - Type "Settings" in the search bar->**System**->Scroll down and click "**Remote Desktop**"-> and enable by clicking the circle, as shown in the screenshot

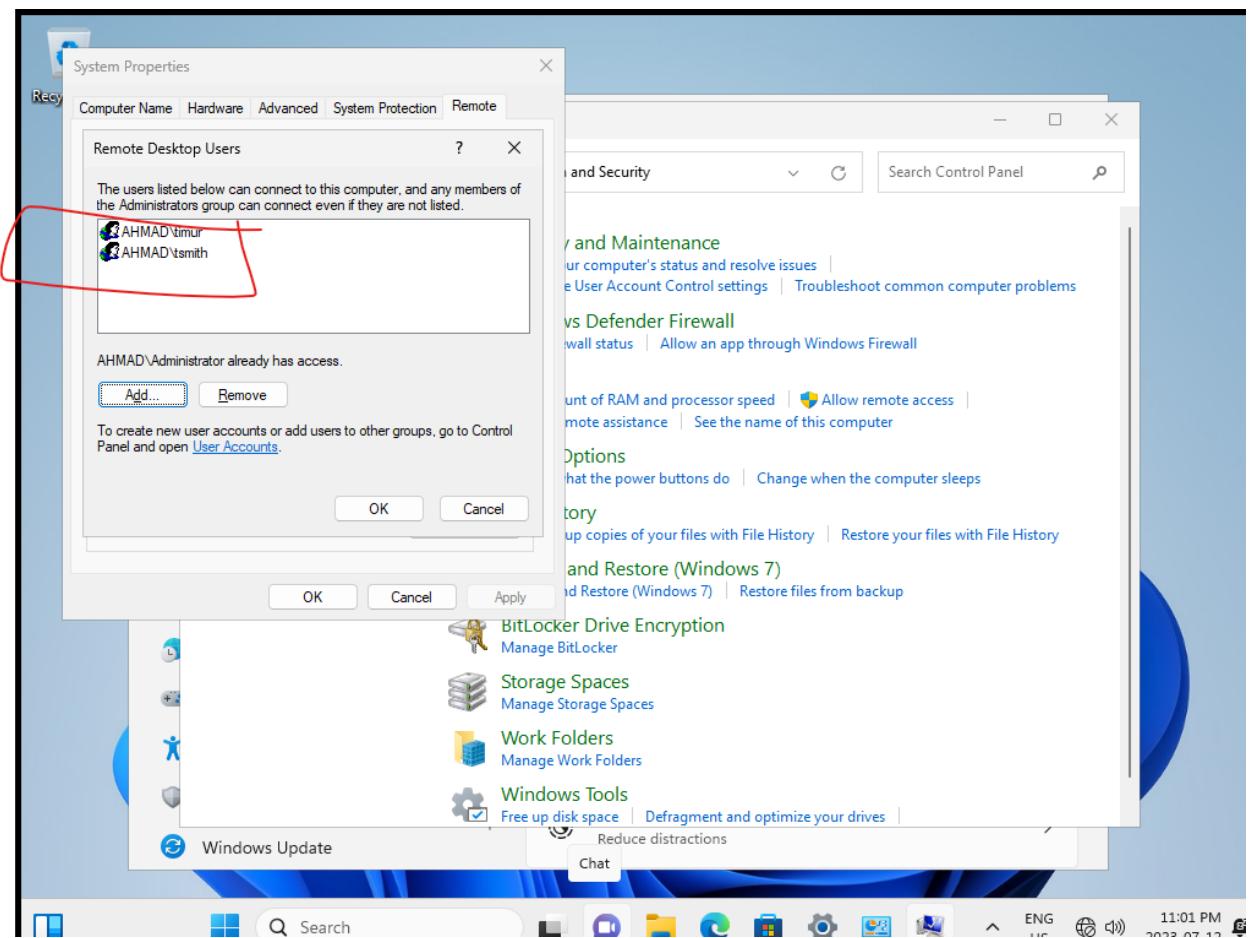


- You will receive the **Remote Desktop name**, which you can use to connect via RDP in Windows Server, or use the **IP address** (10.1.10.3 in this case):

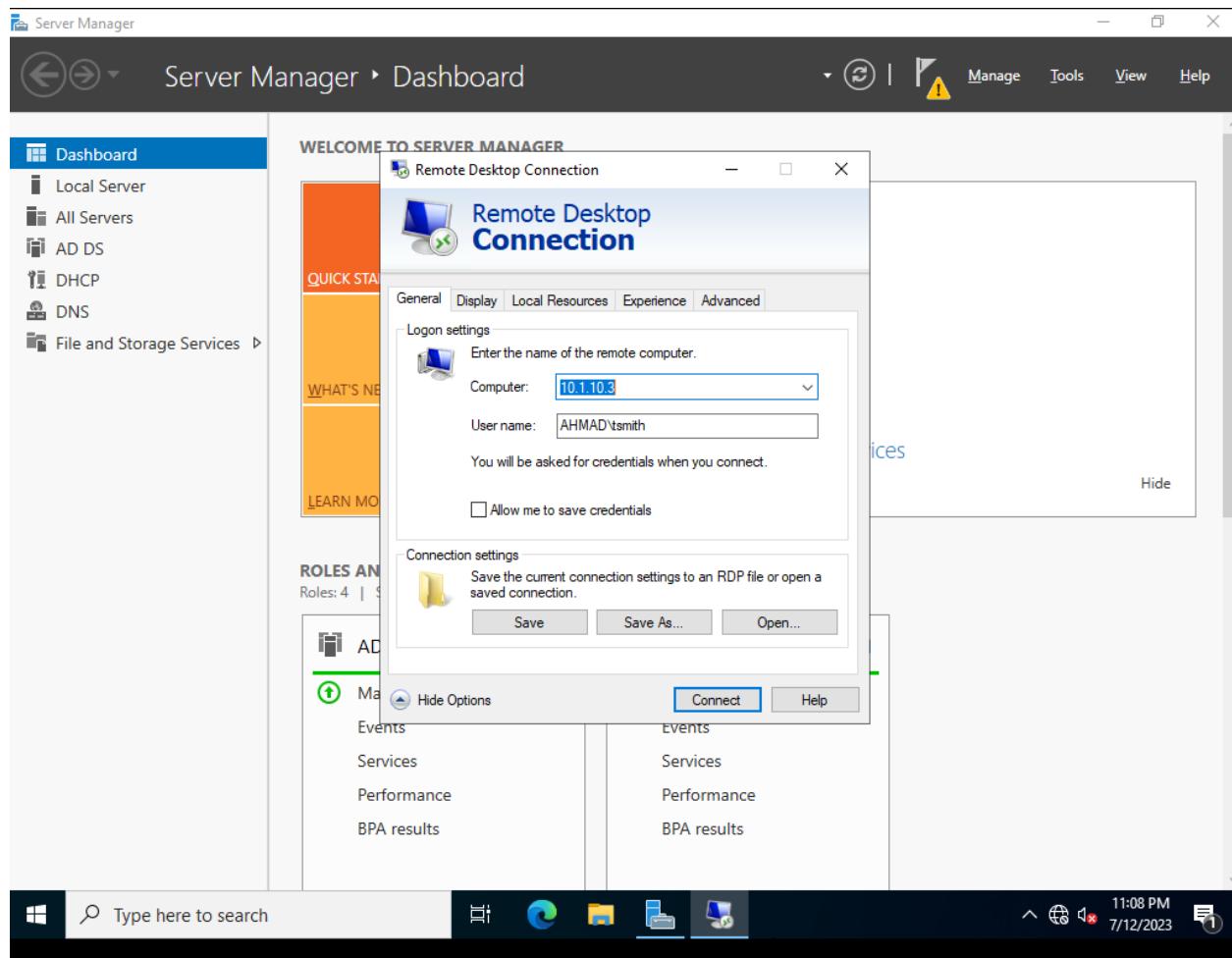


- You should now be able to log in to the remote desktop successfully
- Note:
  - You must **log in as the administrator** (Ahmad Chaudhry) in Windows 11 for this to work
  - When you log in via RDP, you will only log in as the **administrator**, not as a user.  
See below for instructions on how to log in as a user.
- Log in to Windows 11 as the administrator. Go to **Control Panel ->System and Security ->Allow Remote Access** ->click "Add remote users to this computer", and add the users

as shown in the screenshot



- Go to Windows Server->open **remote desktop connection**->click **more options**>enter the username (tsmith in this case)->enter password, and you will be logged in

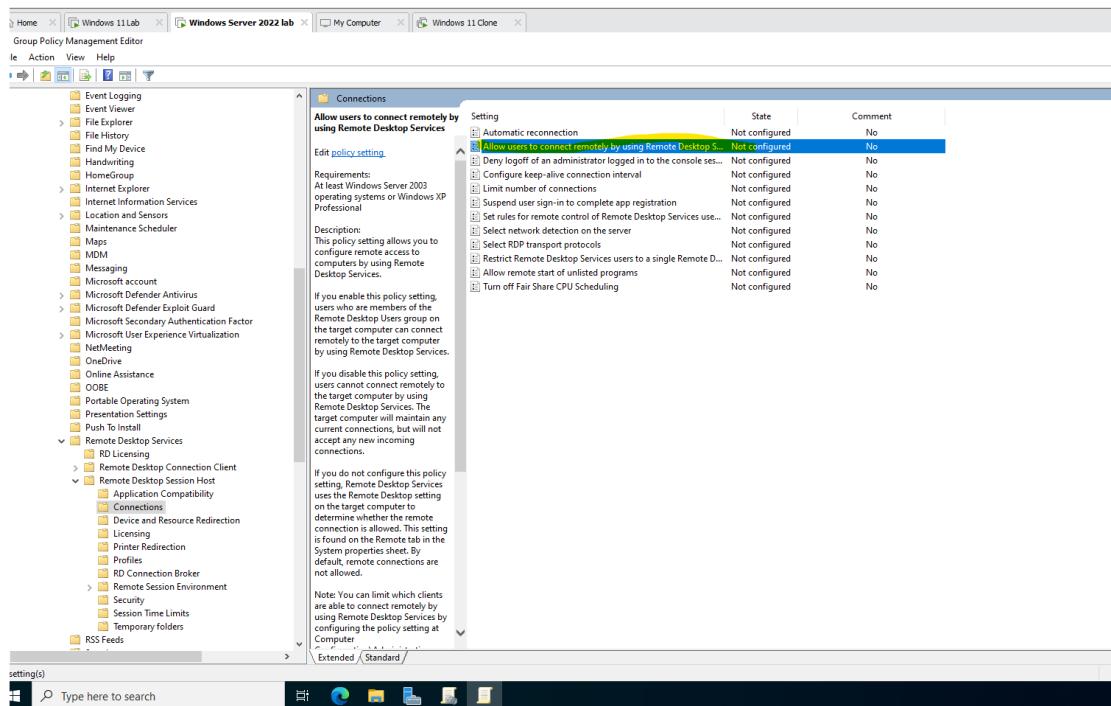


# Implementing Group Policy Objects (GPOs)

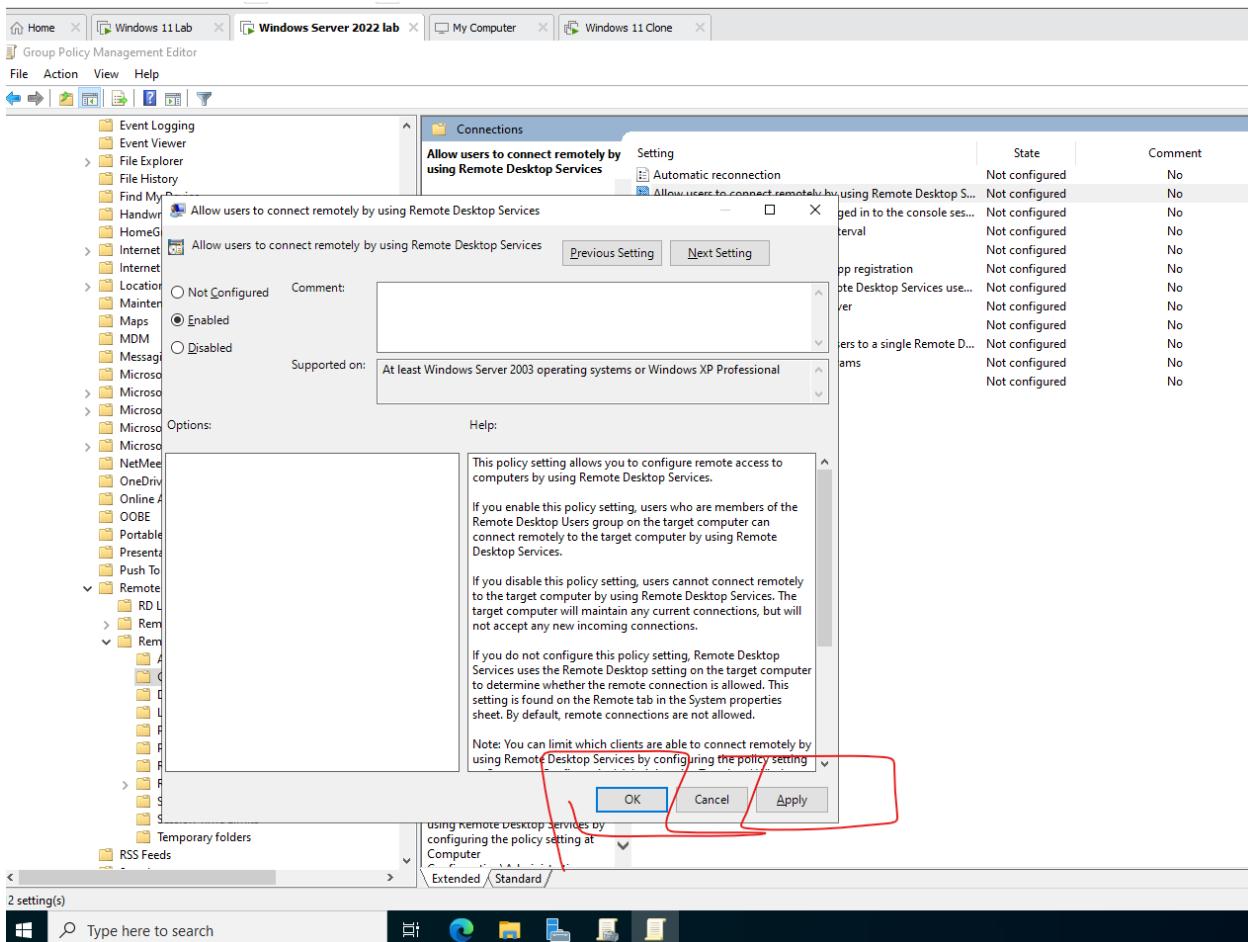
We will implement two GPOs-remote RDP and blocking users from the control panel

## Enable Remote RDP

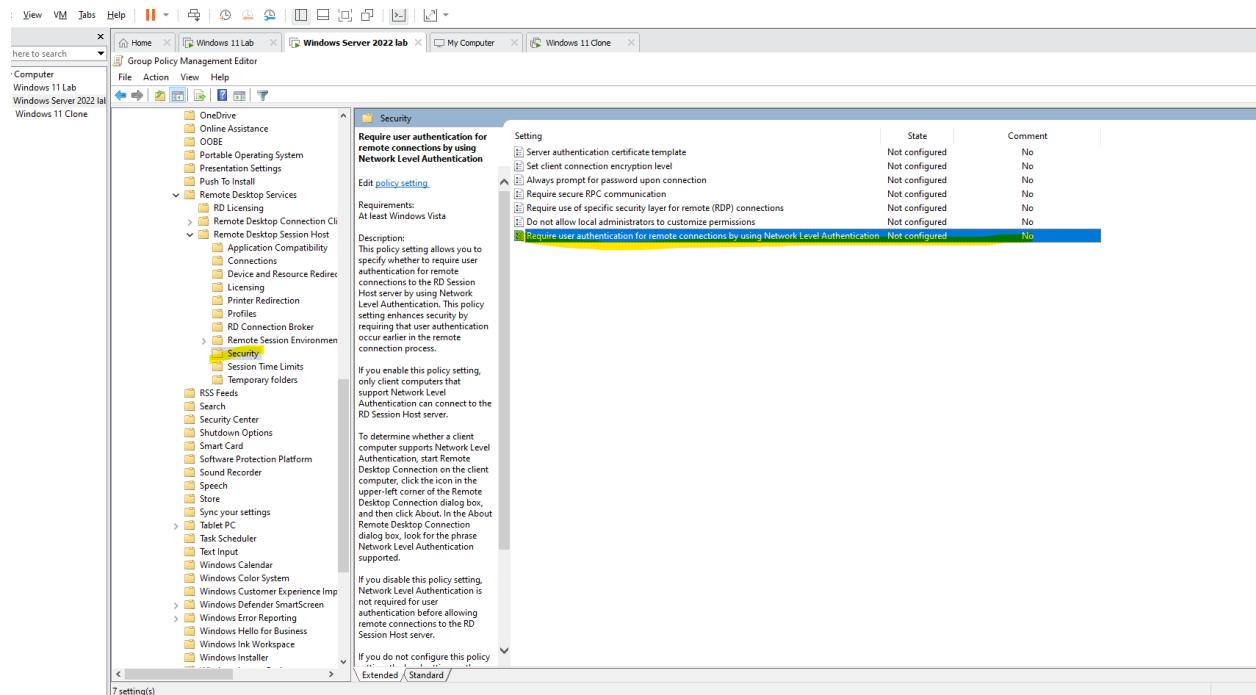
- Go to **sever manager->Tools->Group Policy Management->Right click Group Policy Objects->Select new and name it "RDP Policy"**
- Right click **RDP Policy->Edit->** and navigate to: **computer configuration/policies/administrative template/windows components/remote desktop services/remote desktop session host/connections**
- Select the policy as shown in the screenshot



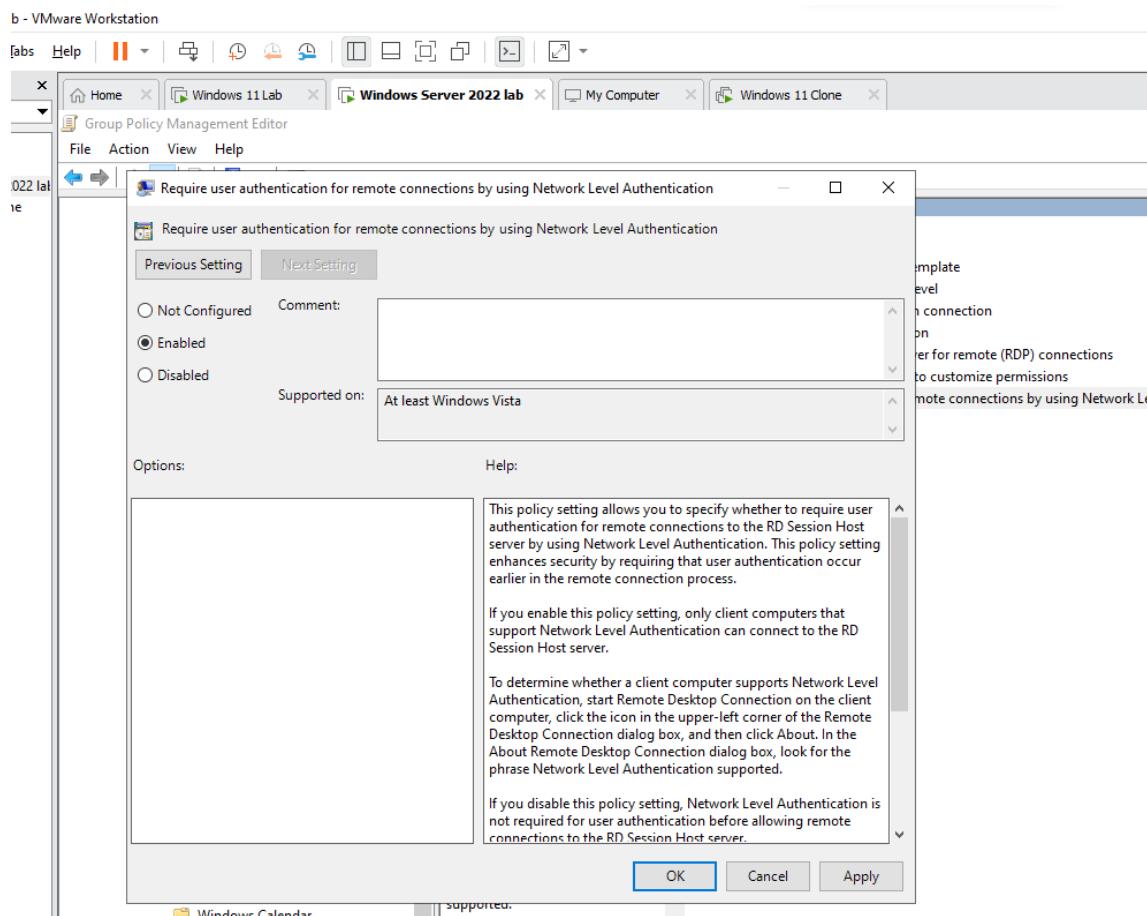
- Double click the **policy->enabled->apply->Ok**. This enables remote desktop services



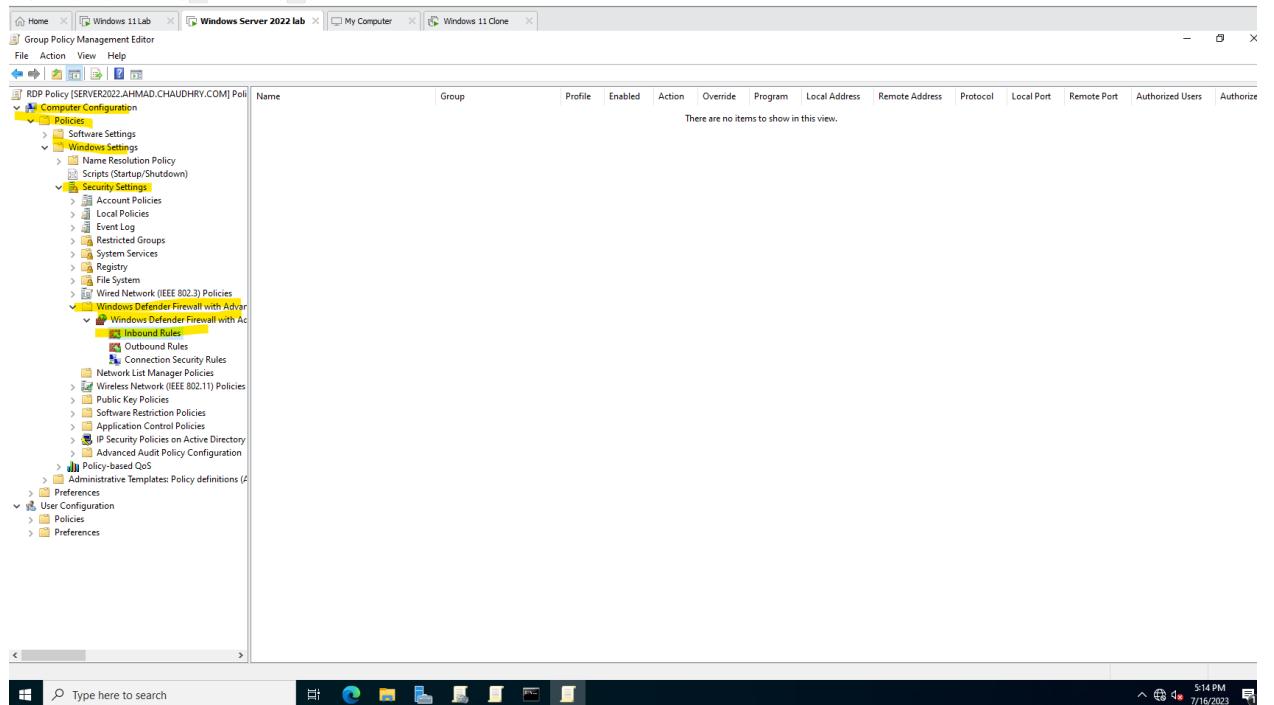
- Now we want to enable authentication
- The policy path is the same as the previous one, except click on **Security** instead of **Connections**, and select the highlighted policy as shown in the screenshot:



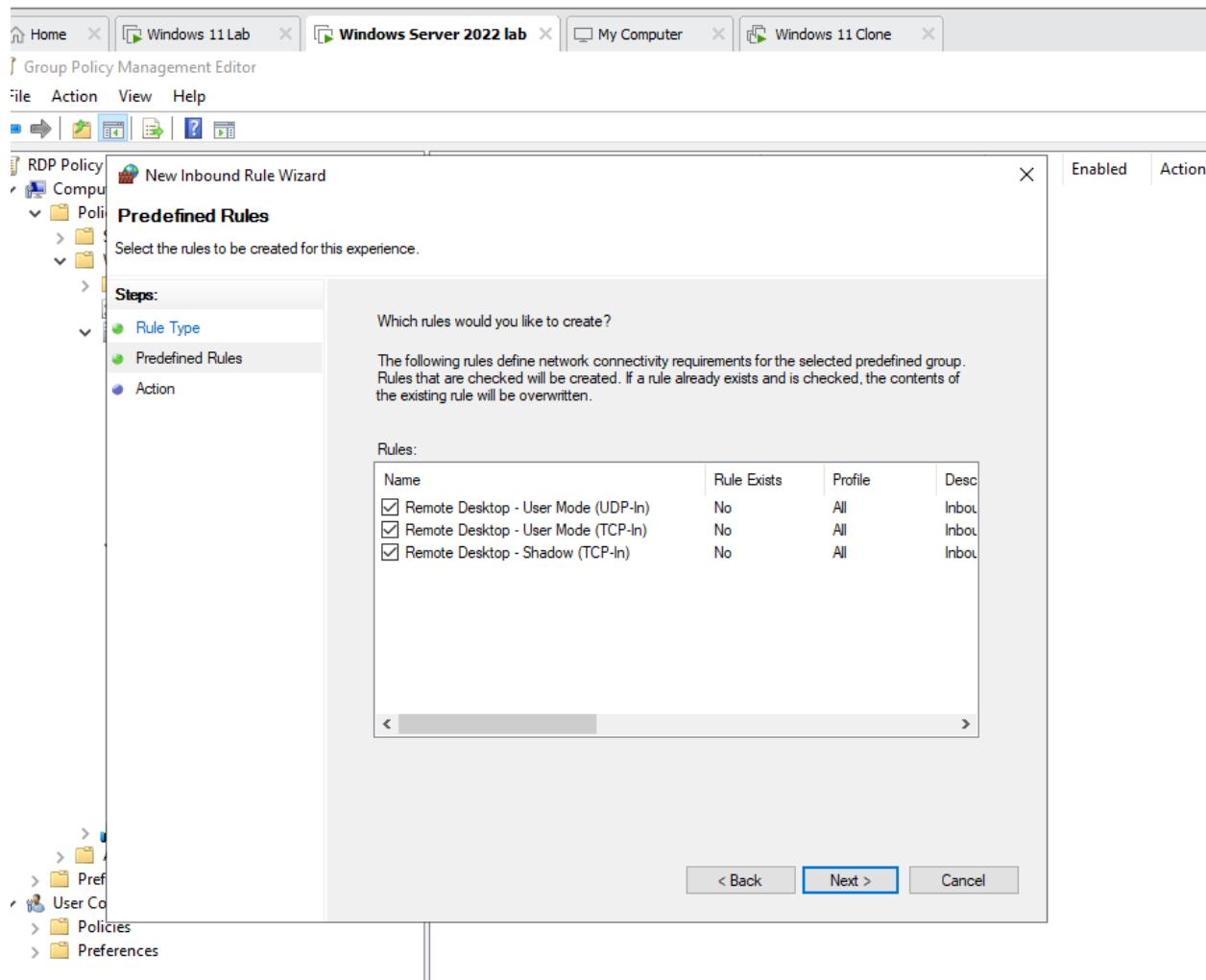
- Select enabled

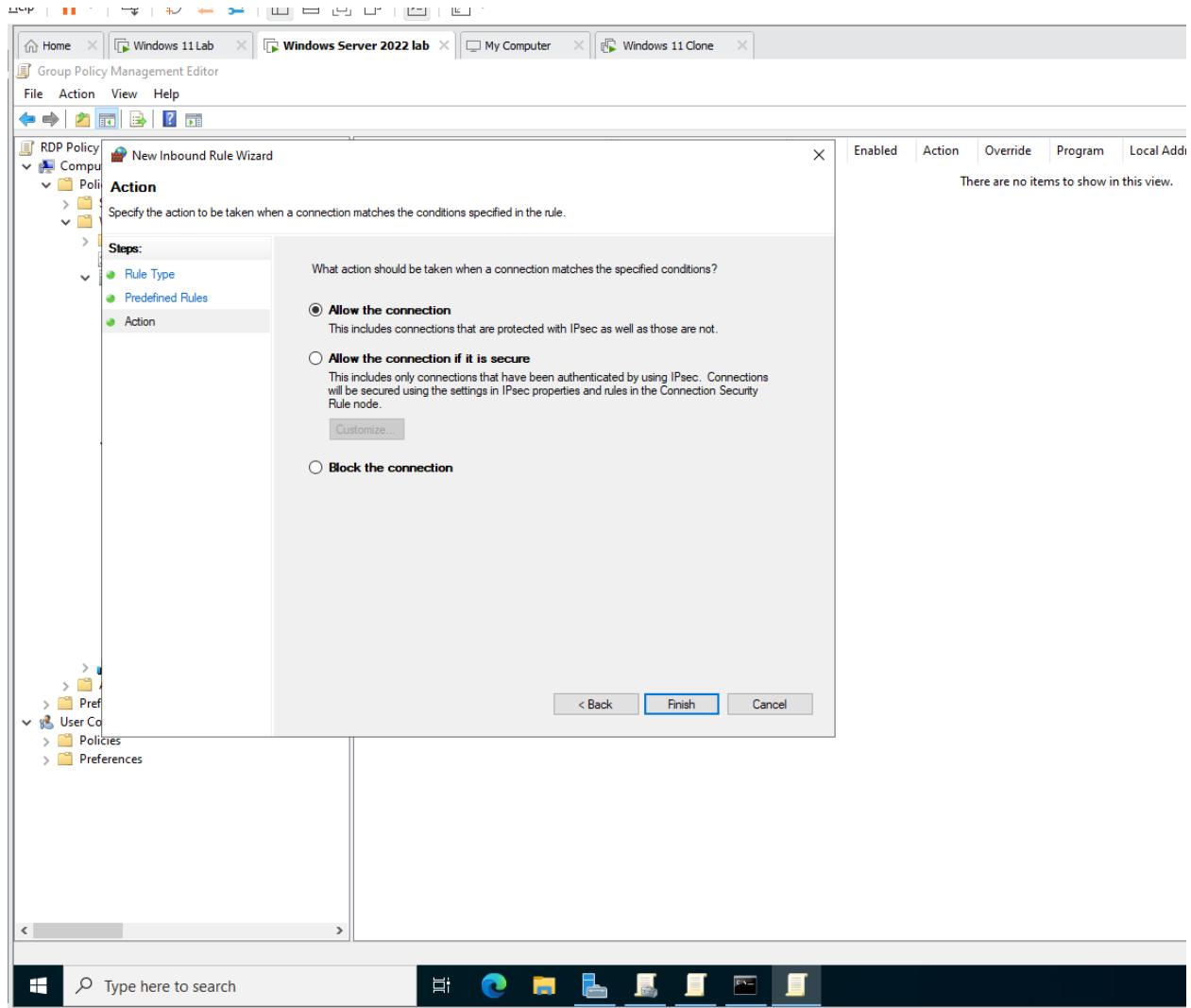


- We want to enable incoming traffic for Group Policy in the firewall. The file path and policy are shown below;

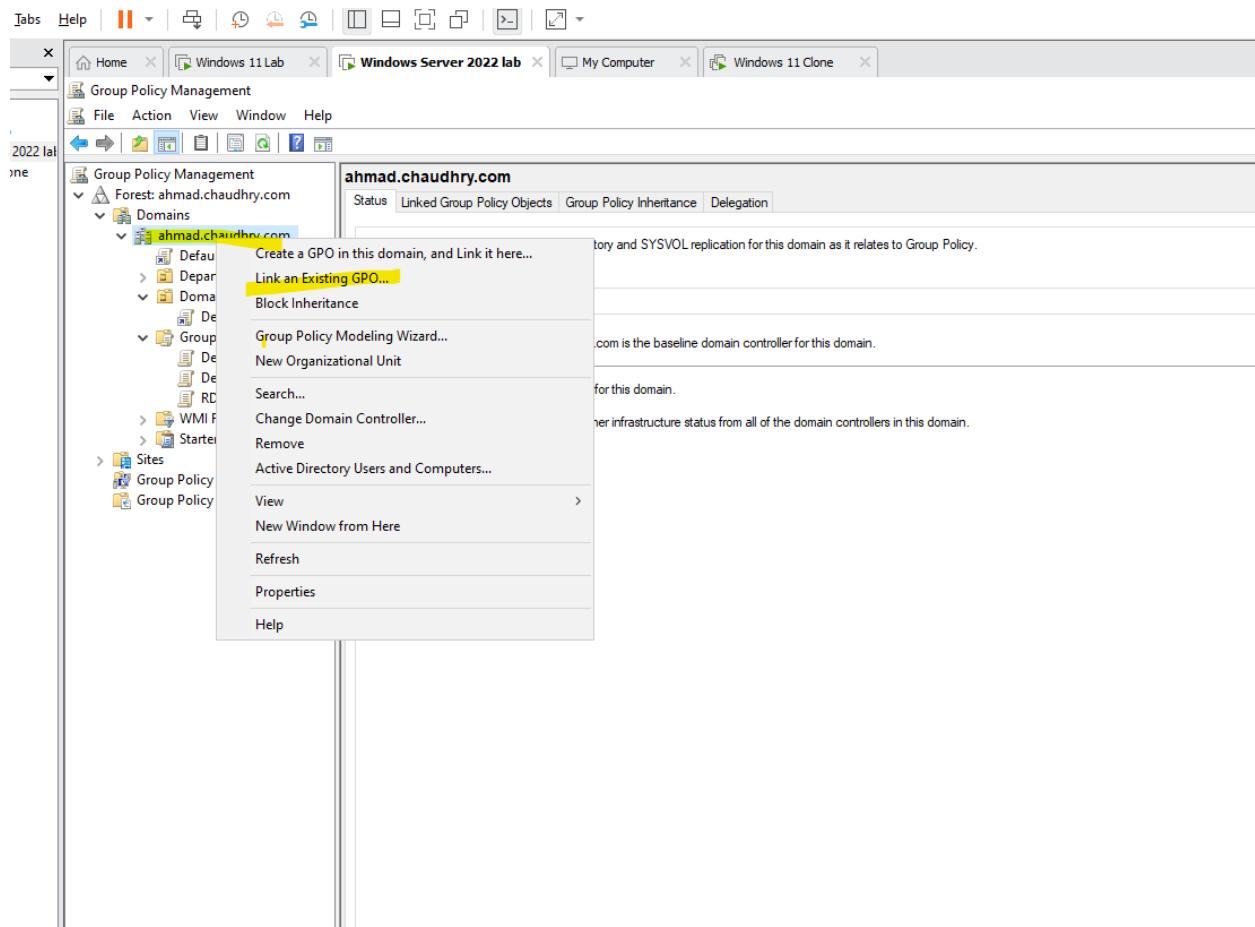


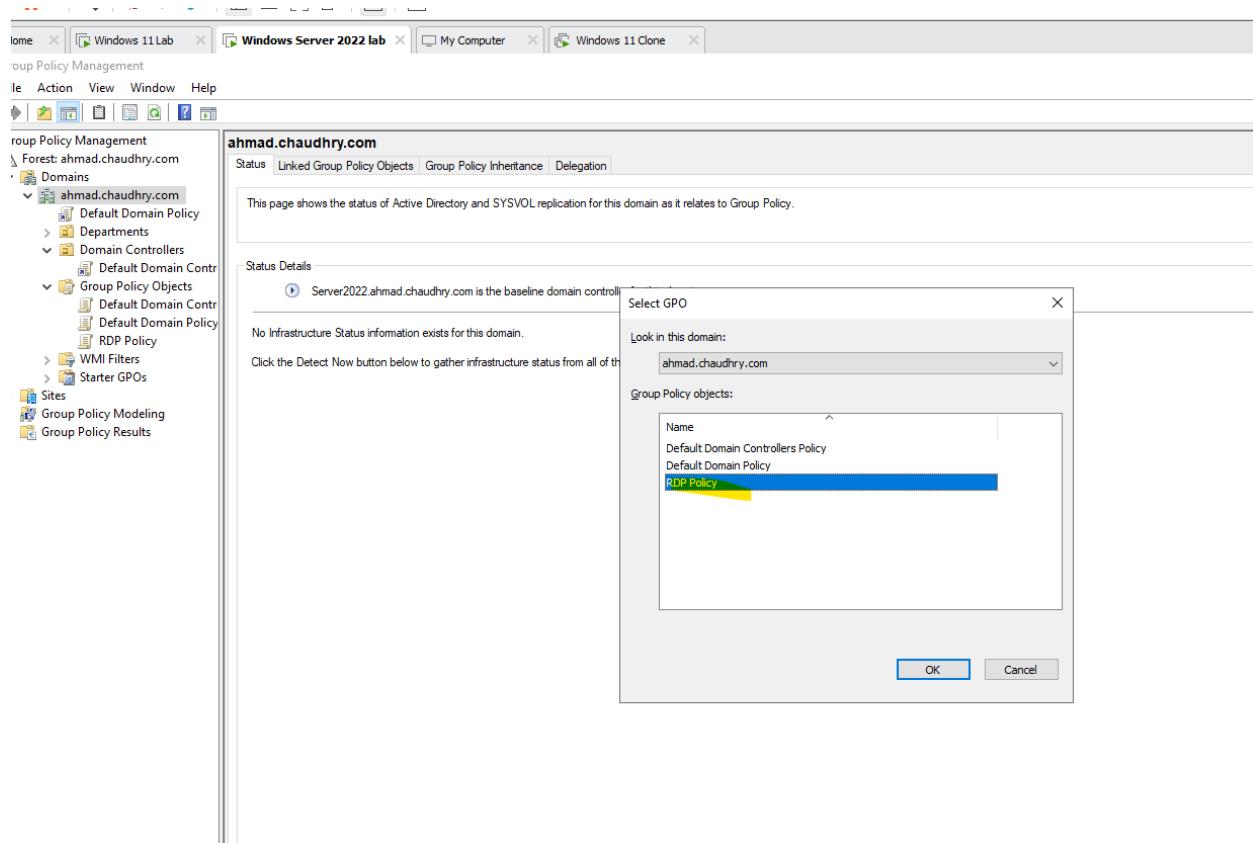
- Right click **inbound rules->new rules...>select predefined and select Remote Desktop from the dropdown and ensure the configuration matches the screenshot below;**





- Right click **domain->Link an existing GPO...->select RDP Policy**





- If you go to Windows Defender Firewall with Advanced Security, you will see the firewall rules we enabled earlier

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	No	Allow	No	%System...	Any	Any	TCP	3389	Any
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	No	Allow	No	%System...	Any	Any	TCP	3389	Any
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	No	Allow	No	%System...	Any	Any	UDP	3389	Any
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Any	UDP	3389	Any
Remote Desktop - (TCP-WS-In)	Remote Desktop (WebSocket)	All	No	Allow	No	System	Any	Any	TCP	3387	Any
Remote Desktop - (TCP-WS-In)	Remote Desktop (WebSocket)	All	No	Allow	No	System	Any	Any	TCP	3392	Any
Remote Event Log Management (NP-In)	Remote Event Log Manage...	All	No	Allow	No	System	Any	Any	TCP	445	Any
Remote Event Log Management (RPC)	Remote Event Log Manage...	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Event Log Management (RPC-EP...	Remote Event Log Manage...	All	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any
Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any
Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No	System	Any	Any	TCP	445	Any
Remote Service Management (RPC)	Remote Service Management	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Service Management (RPC-EPM...	Remote Service Management	All	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any
Inbound Rule for Remote Shutdown (RP...	Remote Shutdown	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Inbound Rule for Remote Shutdown (TCP...	Remote Shutdown	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Volume Management - Virtual Di...	Remote Volume Management	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Remote Volume Management - Virtual Di...	Remote Volume Management	All	No	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any
Remote Volume Management (RPC-EPM...	Remote Volume Management	All	No	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any
Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No	System	Any	Any	GRE	Any	Any
Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No	System	Any	Any	UDP	1701	Any
Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No	System	Any	Any	TCP	1723	Any
Secure Socket Tunneling Protocol (SSTP-L...	Secure Socket Tunneling Pr...	All	No	Allow	No	System	Any	Any	TCP	443	Any
SNMP Trap Service (UDP In)	SNMP Trap	Private...	No	Allow	No	%System...	Any	Local subnet	UDP	162	Any
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow	No	%System...	Any	Any	UDP	162	Any
Software Load Balancer Multiplexer (TCP...	Software Load Balancer	All	No	Allow	No	%System...	Any	Any	TCP	Any	Any
Start	Start	Domain	Yes	Allow	No	Any	Any	Any	Any	Any	Any
TPM Virtual Smart Card Management (D...	TPM Virtual Smart Card Ma...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	135	Any
TPM Virtual Smart Card Management (D...	TPM Virtual Smart Card Ma...	Domain	No	Allow	No	%System...	Any	Any	TCP	135	Any
TPM Virtual Smart Card Management (C...	TPM Virtual Smart Card Ma...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any
TPM Virtual Smart Card Management (C...	TPM Virtual Smart Card Ma...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any
Virtual Machine Monitoring (DCOM-In)	Virtual Machine Monitoring	All	No	Allow	No	%System...	Any	Any	TCP	135	Any
Virtual Machine Monitoring (Echo Reque...	Virtual Machine Monitoring	All	No	Allow	No	System	Any	Any	ICMPv4	Any	Any

- Open the command prompt, type "**gpupdate /force**" to force an immediate group policy update
- You should now see that RDP is enabled on the local server

The screenshot shows the Windows Server Manager interface for a server named "Server2022".

**Properties for Server2022:**

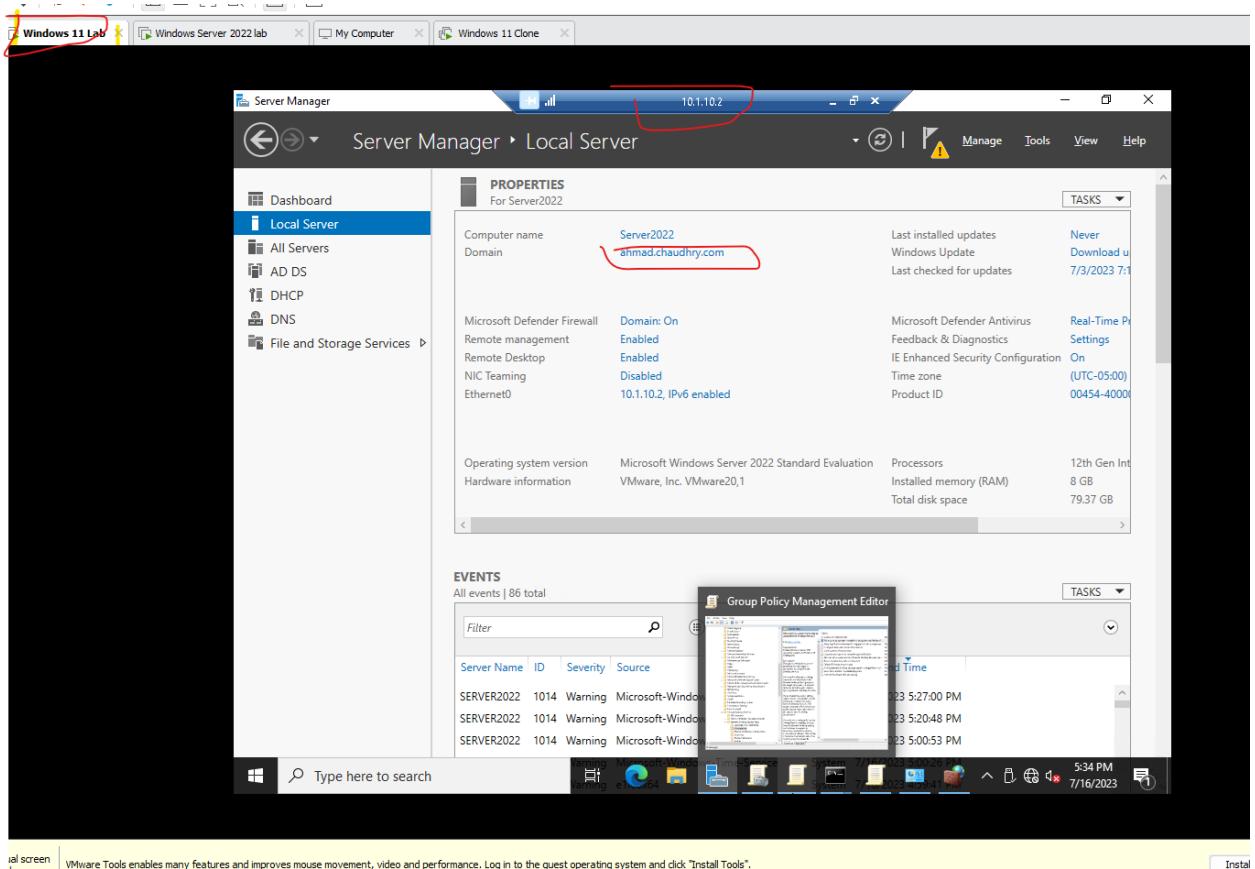
- Computer name: Server2022
- Domain: ahmad.chaudhry.com
- Microsoft Defender Firewall: Domain: On, Enabled
- Remote management: Enabled
- Remote Desktop: Enabled
- NIC Teaming: Disabled
- Ethernet0: 10.1.10.2, IPv6 enabled
- Operating system version: Microsoft Windows Server 2022 Standard Evaluation
- Hardware information: VMware, Inc. VMware20,1
- Processor: (not explicitly listed)
- Installed memory (RAM): (not explicitly listed)
- Total disk space: (not explicitly listed)

**Events:**

All events | 85 total

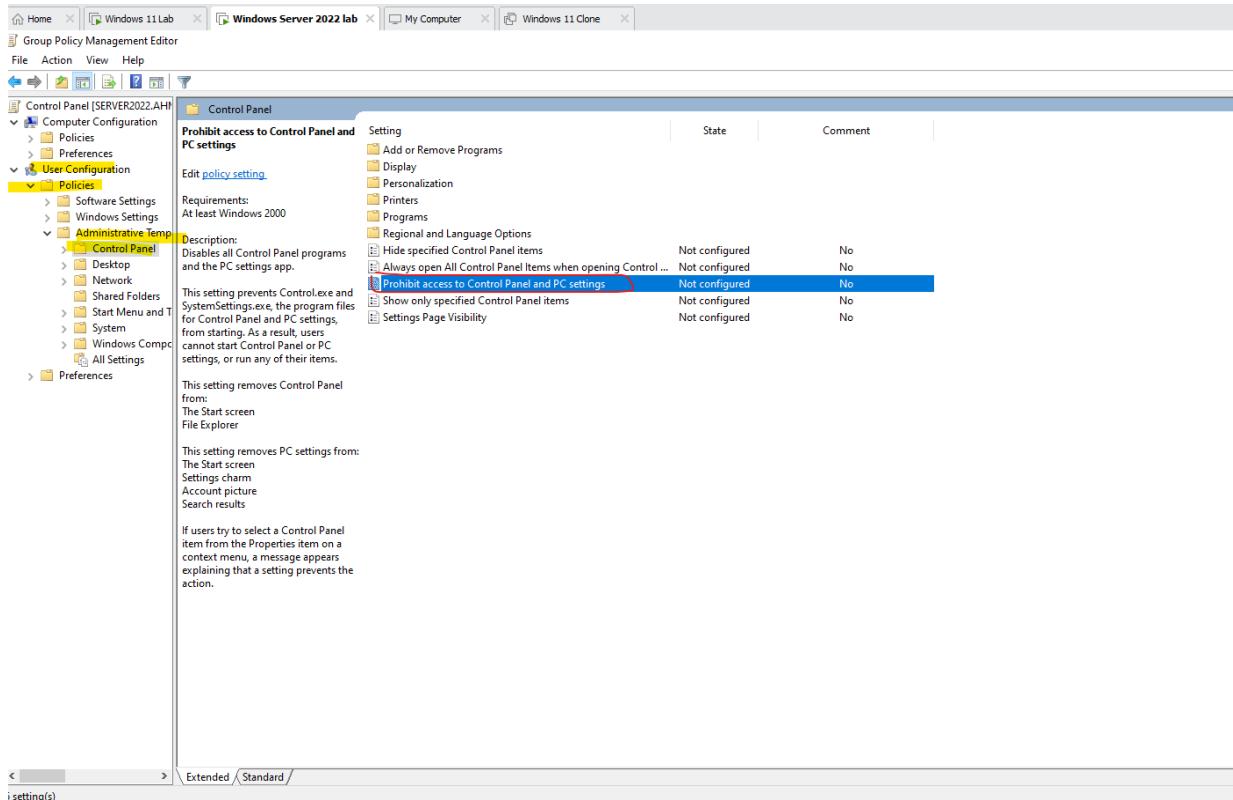
Server Name	ID	Severity	Source	Log	Date and Time
SFRVFR2022	1014	Warning	Microsoft-Windows-DNS Client Events	System	7/16/2023 5:20:48 PM

- Test the policy by doing the following:
  - Go to **Windows 11 Lab**->Open **RDP** ->Enter **Windows Server 2022 IP address** as per the above screenshot->Enter the password (log in as administrator)
- You are now connected remotely

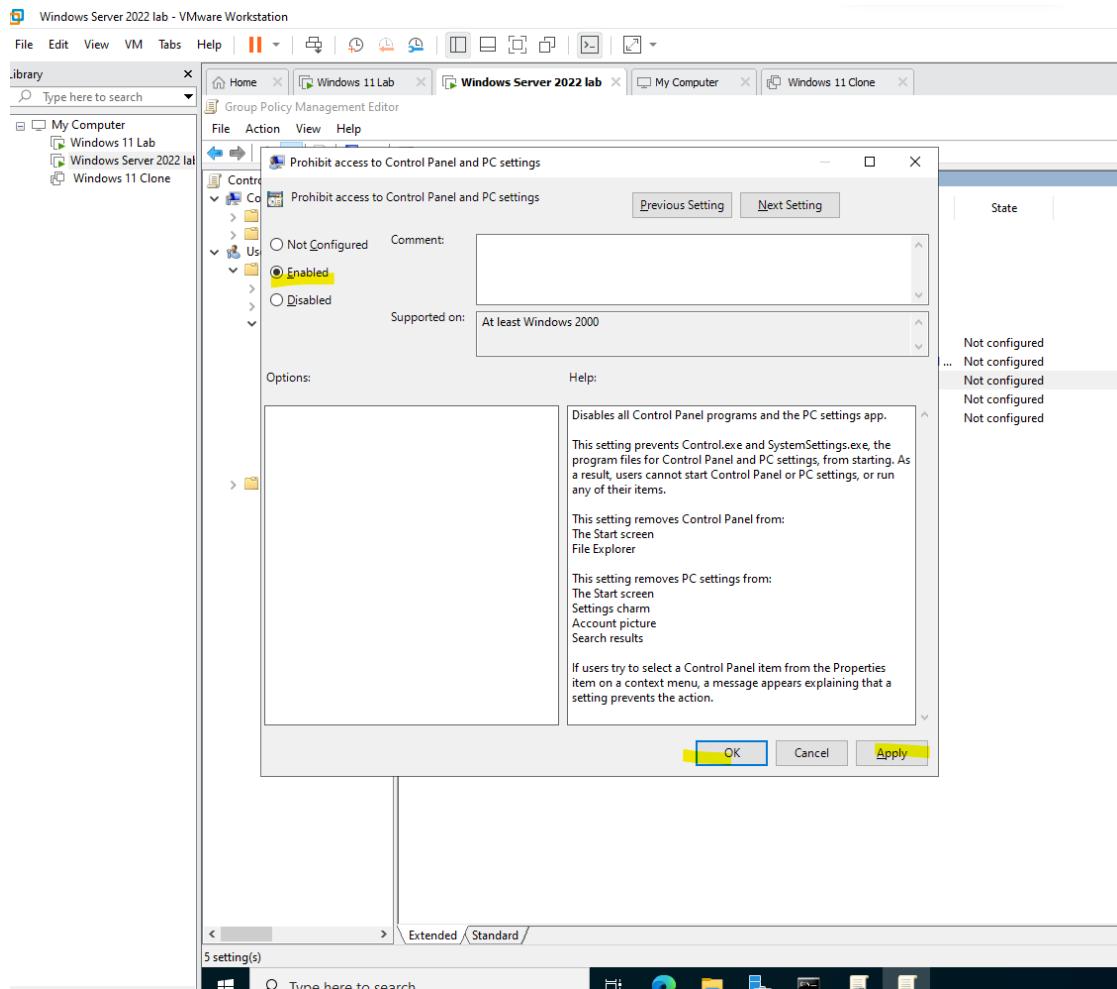


## Blocking users from the Control Panel

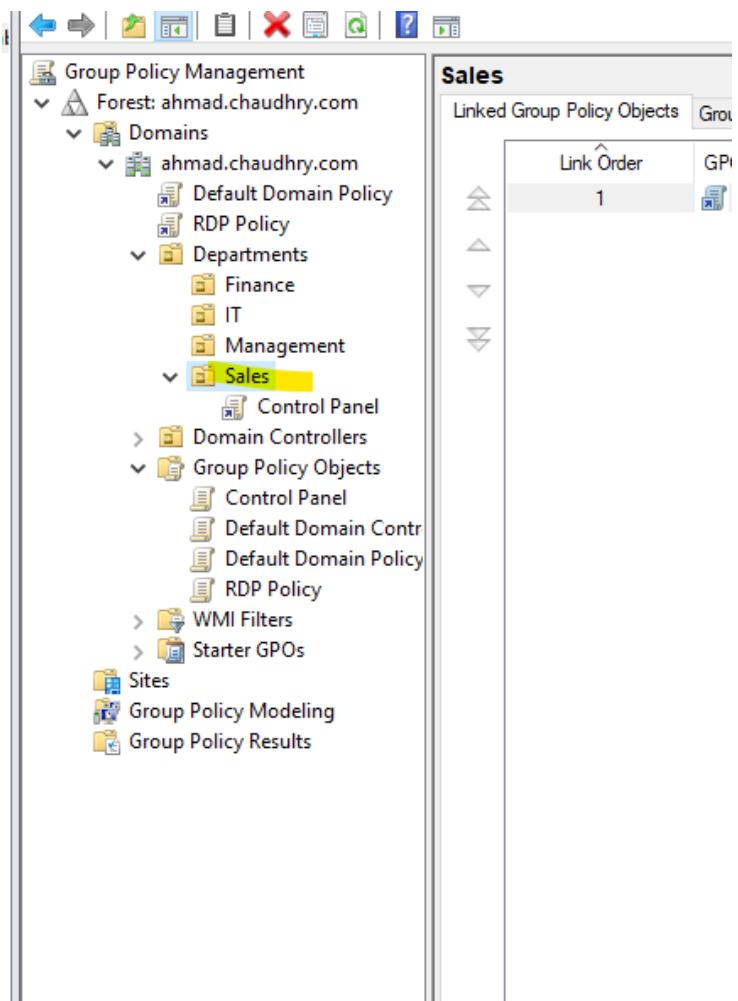
- Go to Server Manager->Group Policy Object->New->Name it **Control Panel**
- Right click "Control Panel"->Select **Edit...**-> navigate to the path shown in the screenshot and select "**Prohibit access...**"



- Double click the **policy->enabled->apply->Ok**

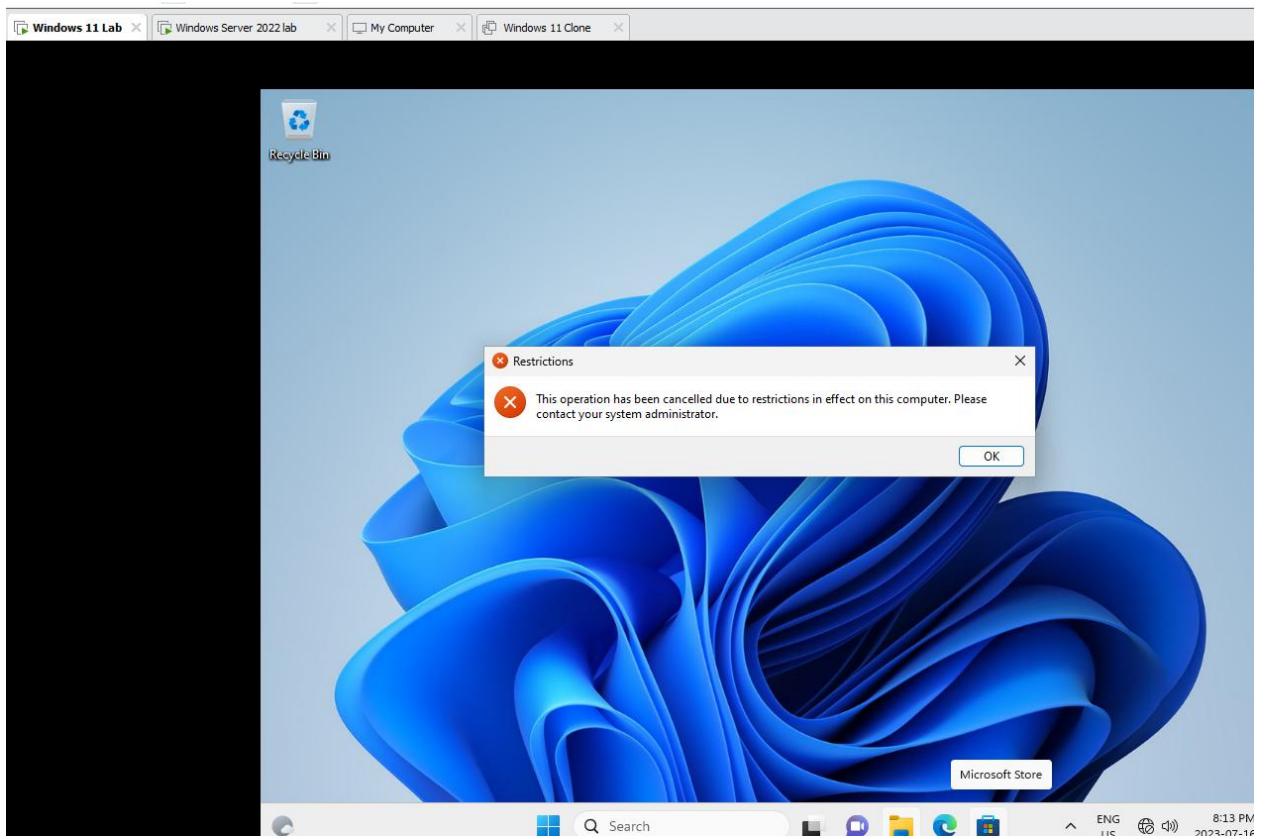


- We will apply it to the sales department: Right click sales->click "Linked an existing GPO..." -> select **control panel**



- Open the command prompt, type "**gpupdate /force**" to force an immediate group policy update

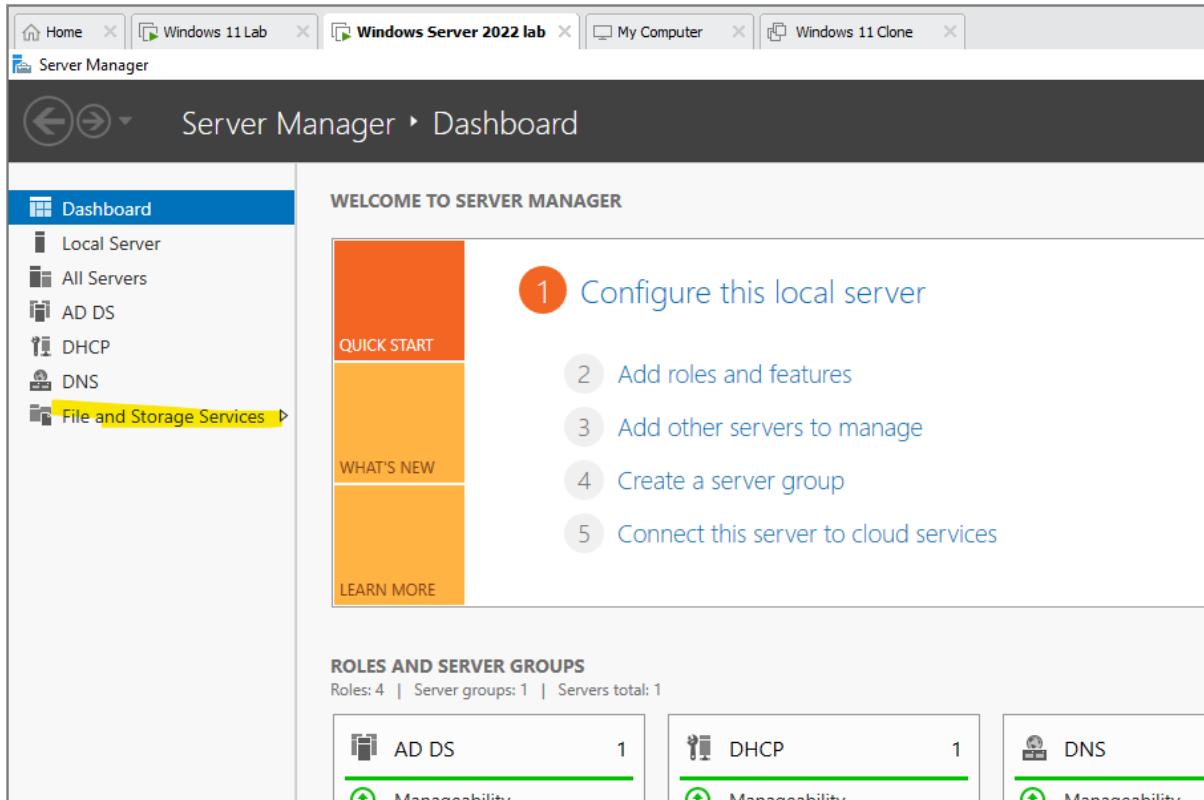
- Test it by logging in as one of the users from the **Sales department** and opening the **Control Panel**. You should see the following error



## Creating Shared Folders, Security Groups, Access Permissions, and Network Drive Mapping

We will create shared folders

- Go to Server Manager->File and Storage Services



- Go to Shares->Right click and select "New Share..."

The screenshot shows the Windows Server Manager interface under the 'File and Storage Services' section, specifically the 'Shares' tab. On the left, a navigation pane lists 'Servers', 'Volumes', 'Disks', 'Storage Pools', **Shares**, 'iSCSI', and 'Work Folders'. The 'Shares' option is selected. The main area displays a 'SHARES' table with two entries:

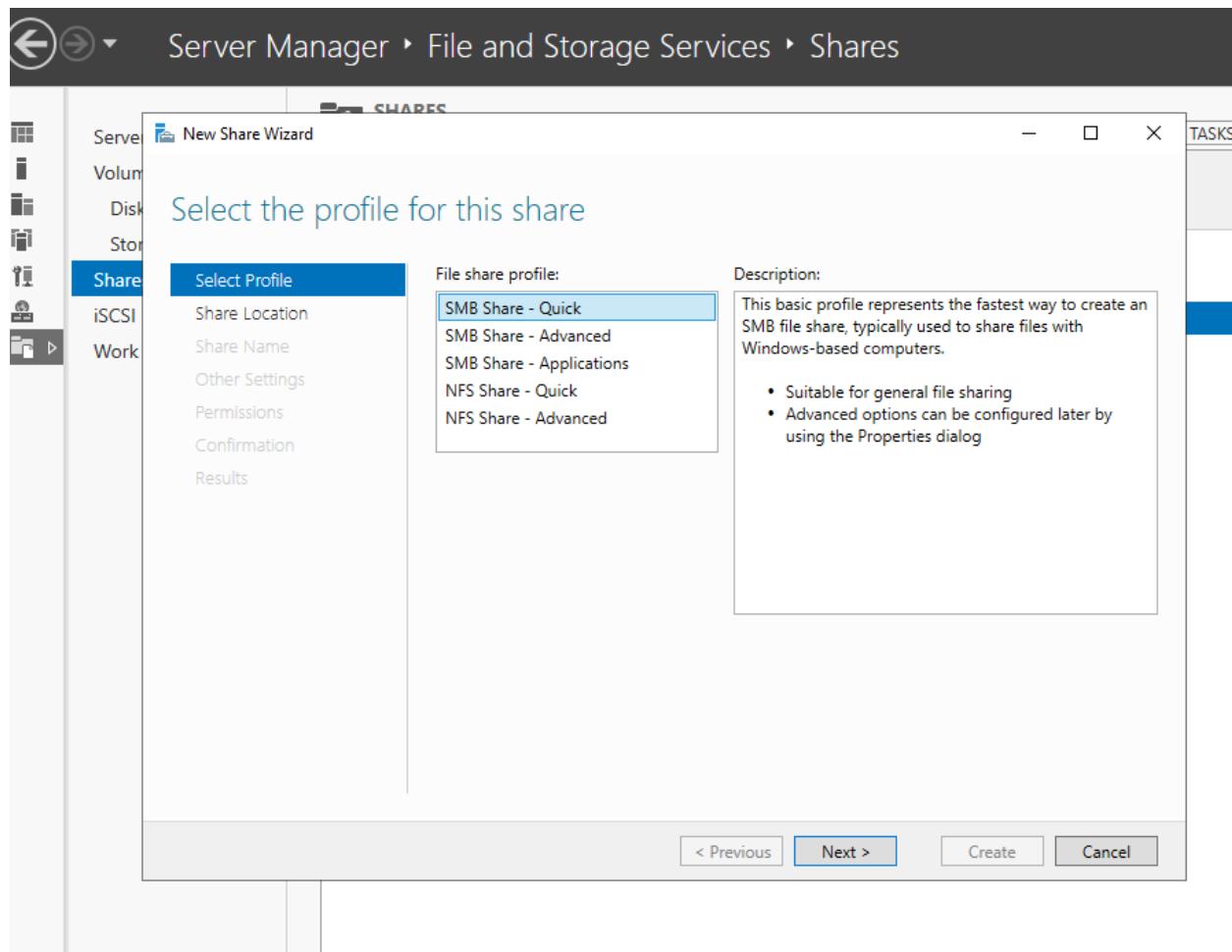
Share	Local Path	Protocol	Availability Type
NETLOGON	C:\Windows\SYSVOL\sysvol\ahma...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

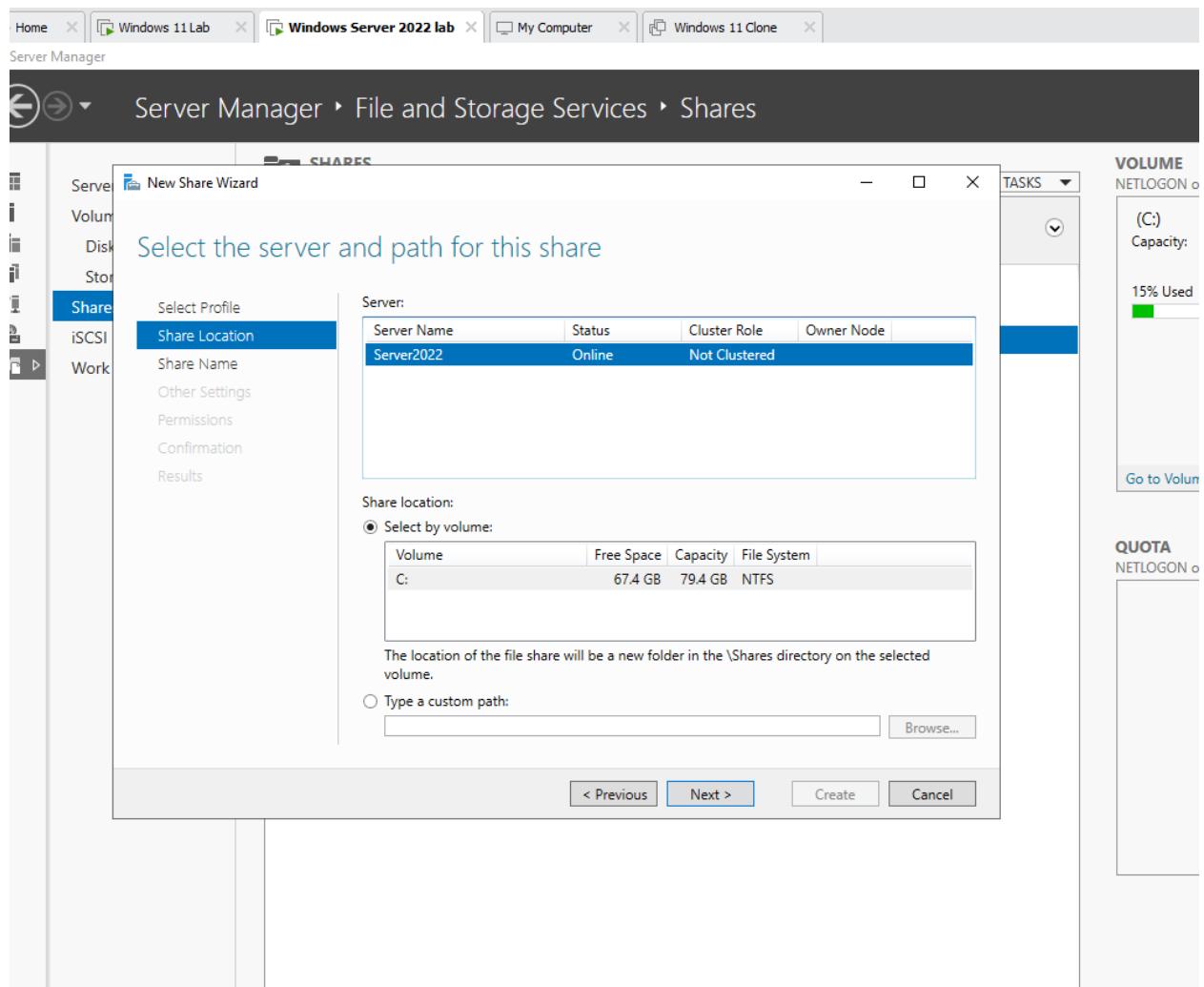
Below the table are 'New Share...' and 'Refresh' buttons. To the right, there are sections for 'VOLUME' (NETLOGON on Server2022) and 'QUOTA' (NETLOGON on Server2022). The volume section shows:

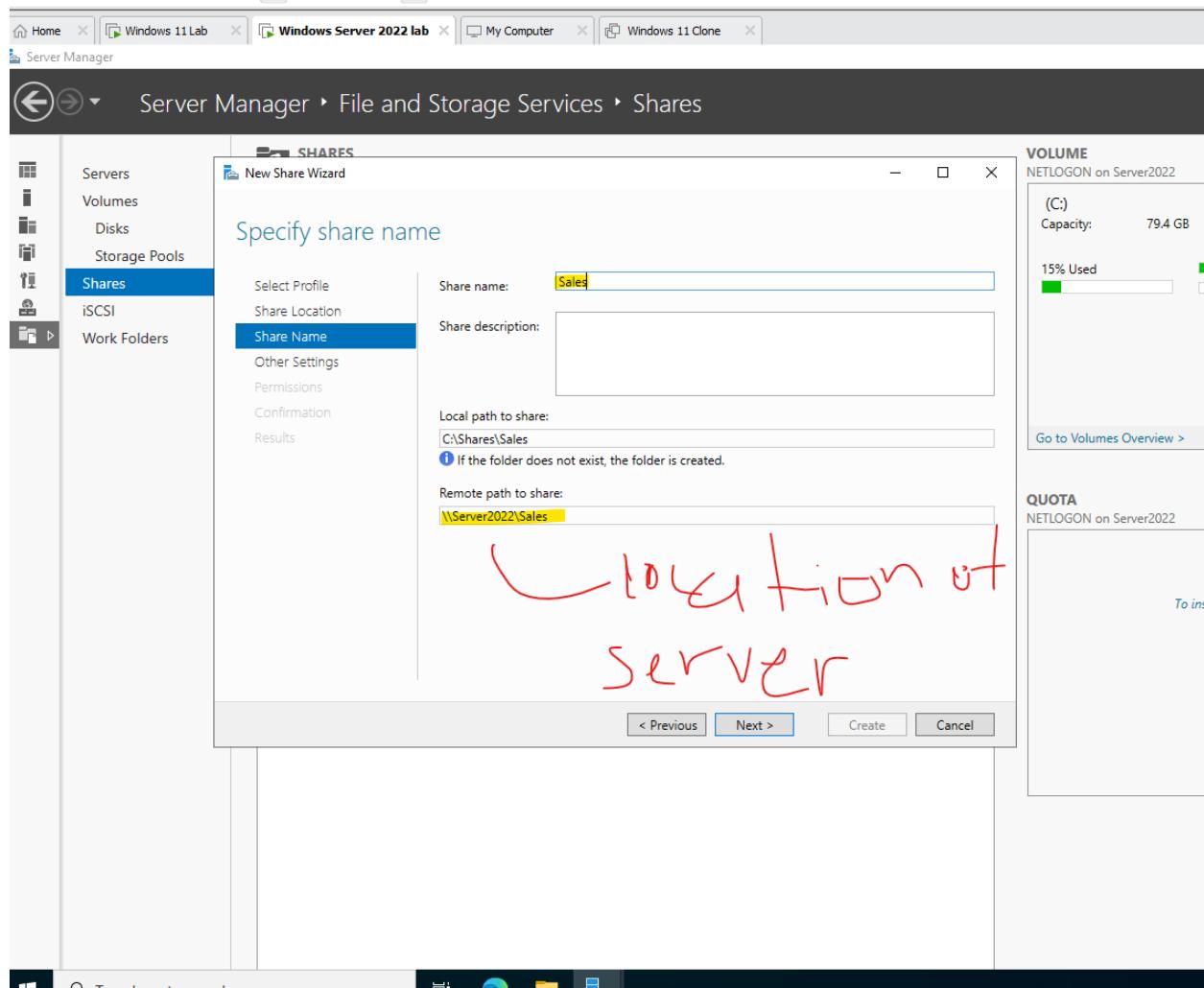
- (C): Capacity: 79.4 GB
- 15% Used: 11.9 GB Used Space
- 85% Free: 67.4 GB Free Space

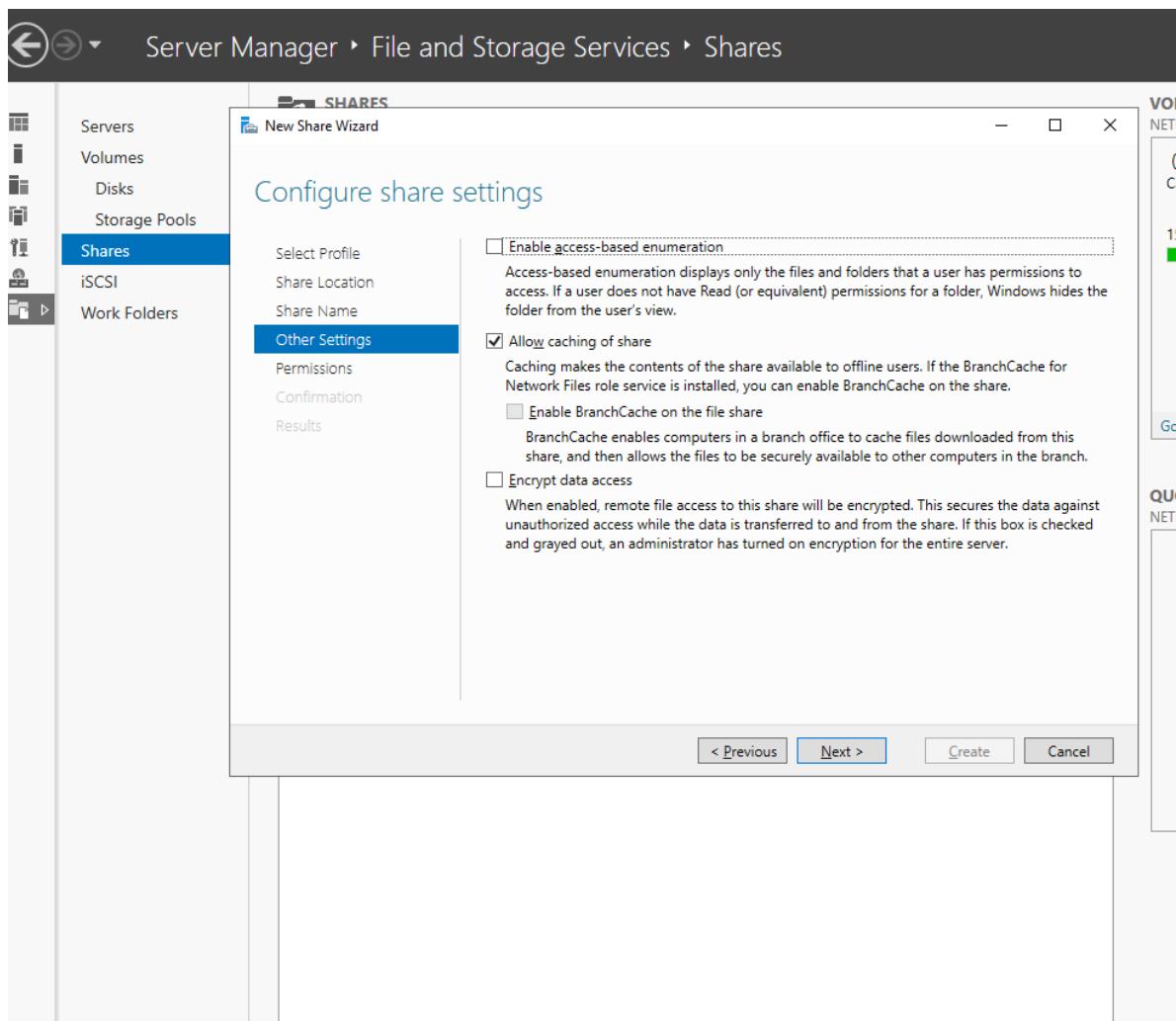
At the bottom, a search bar says 'Type here to search' and has a placeholder 'pointer inside or press Ctrl+G.'

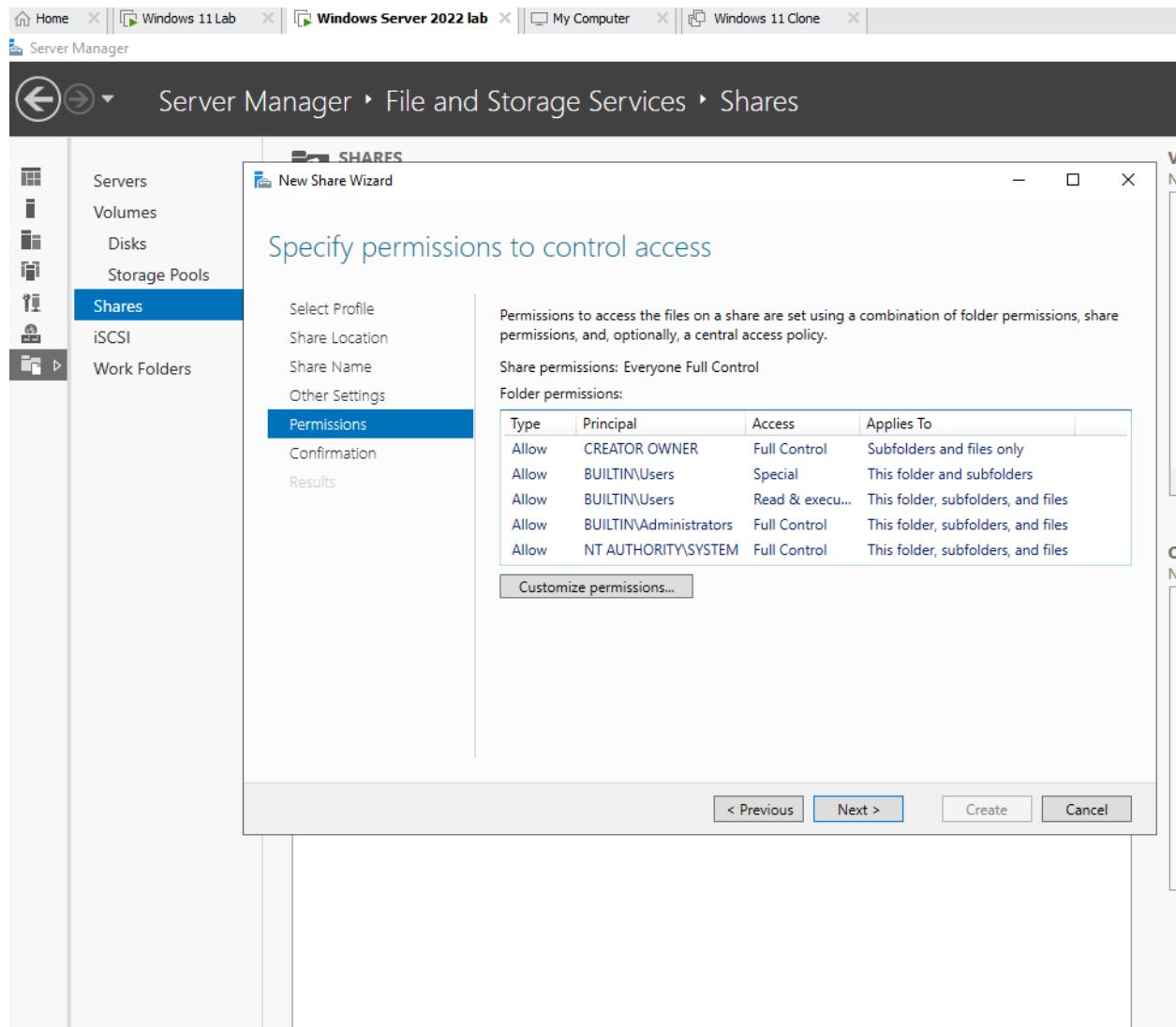
- Ensure the configurations match those shown in the screenshots below:

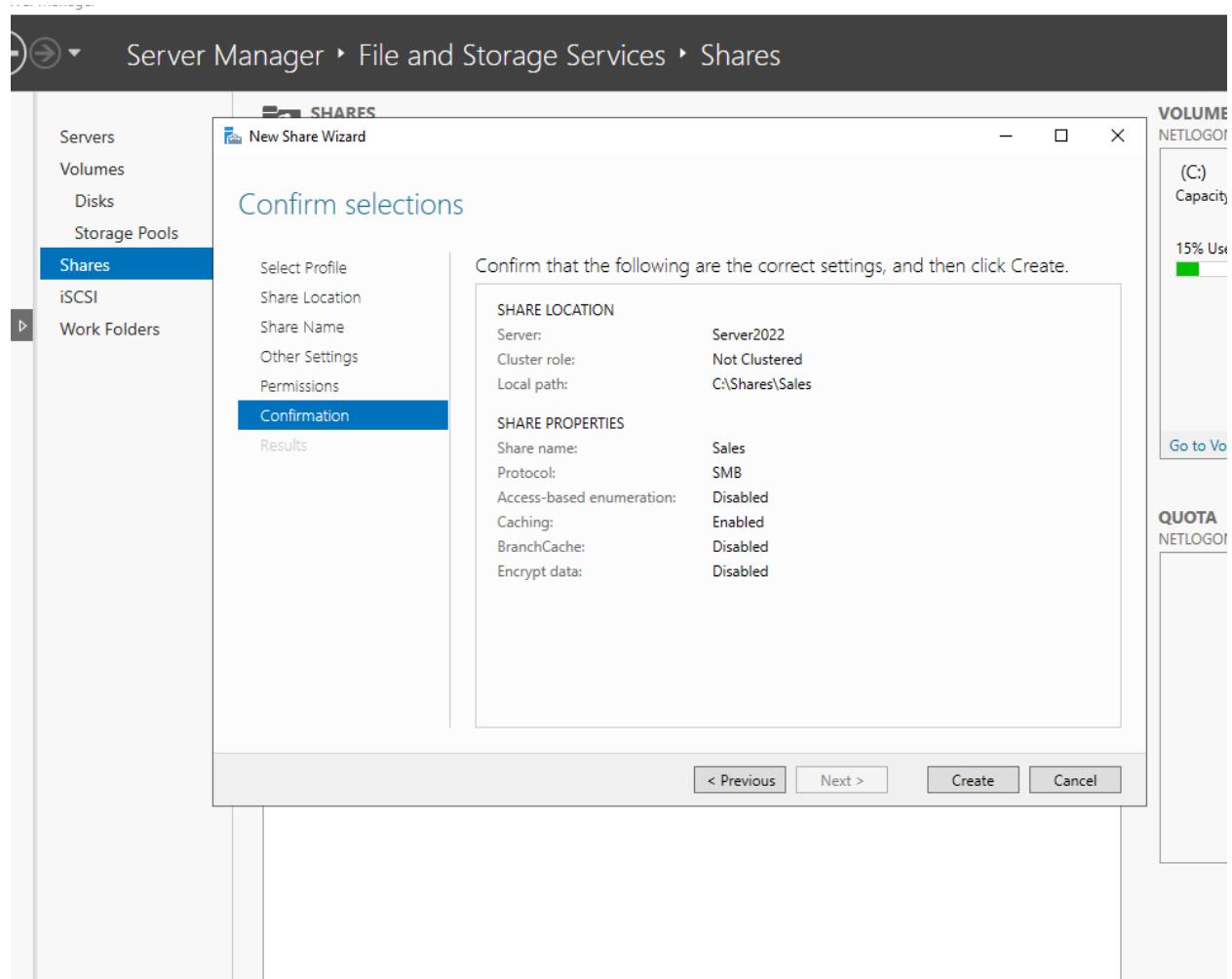


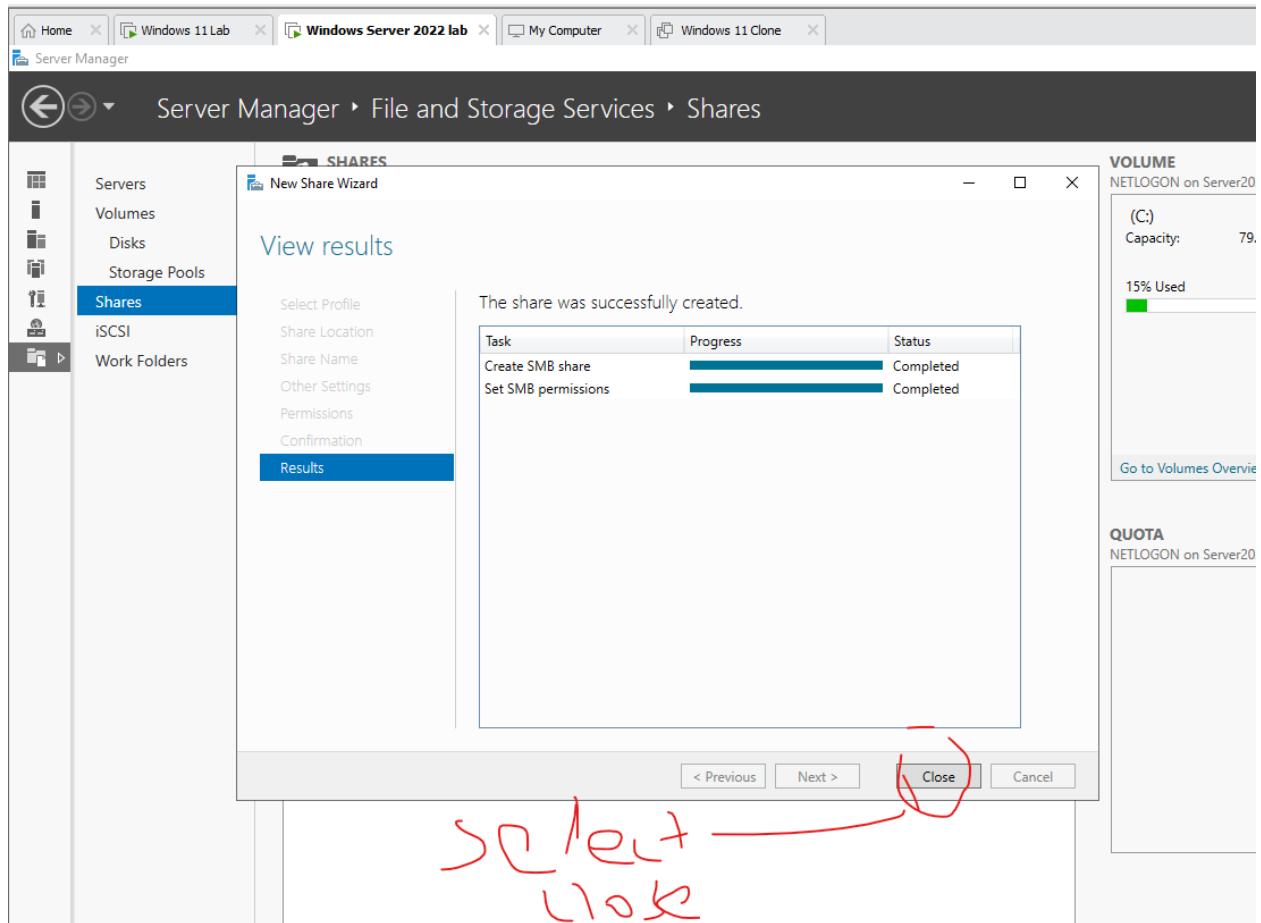












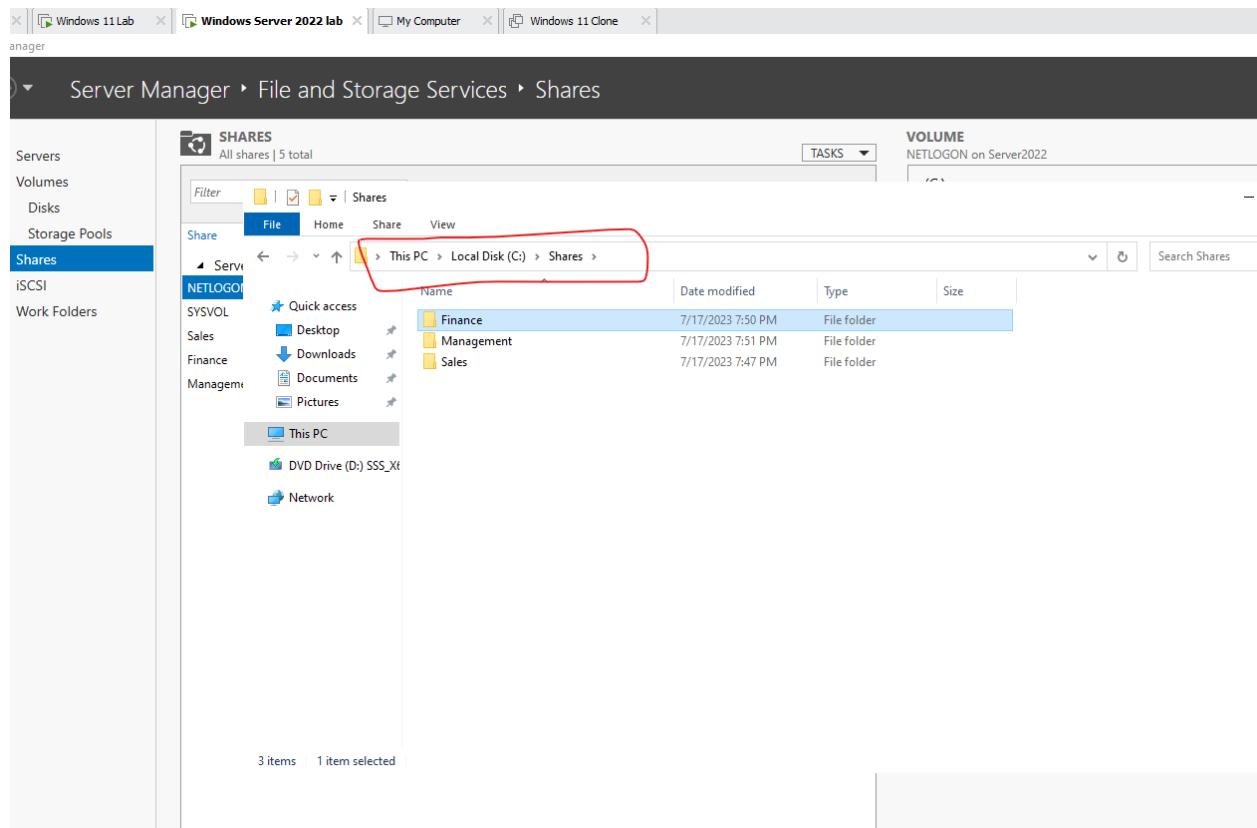
- Repeat the same steps for **Finance** and **Management**; you should then have **three shared folders**

Server Manager ▶ File and Storage Services ▶ Shares

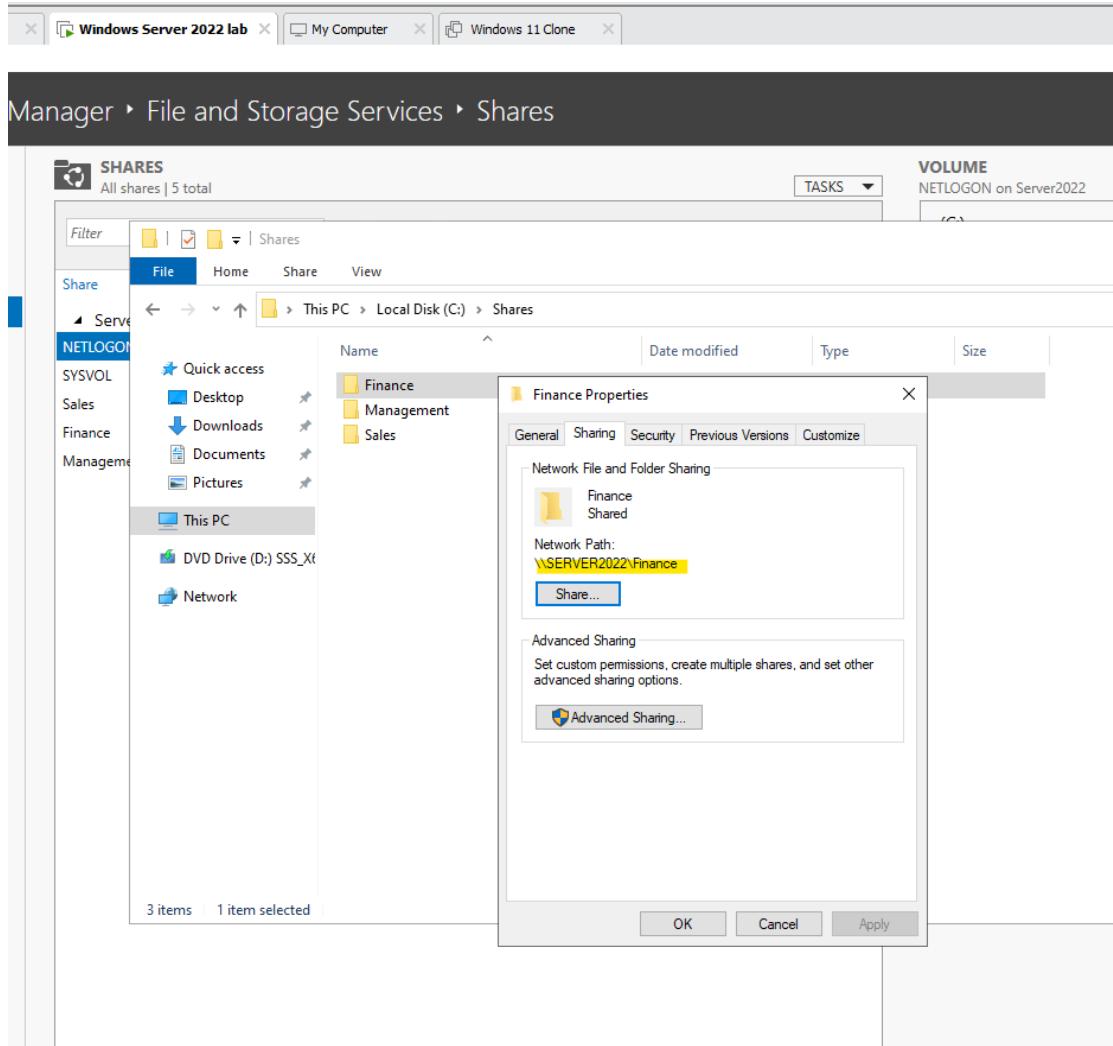
Share	Local Path	Protocol	Availability Type
NETLOGON	C:\Windows\SYSVOL\sysvol\ahma...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered
Sales	C:\Shares\Sales	SMB	Not Clustered
Finance	C:\Shares\Finance	SMB	Not Clustered
Management	C:\Shares\Management	SMB	Not Clustered

**VOLUME**  
NETLOGON on Server2022  
(C:) Capacity: 79.4 GB  
15% Used

**QUOTA**  
NETLOGON on Server2022  
To in

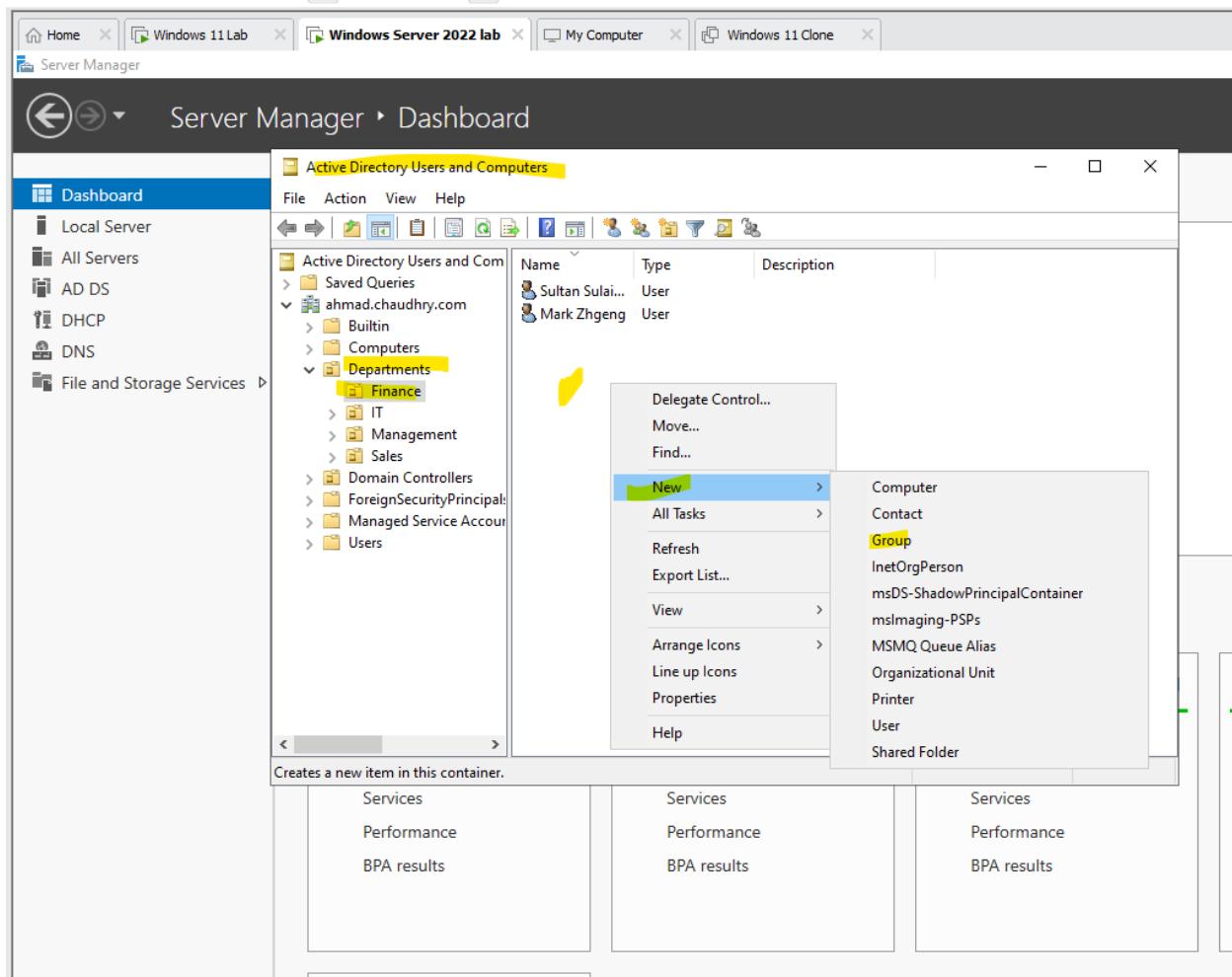


- If you look at the properties of one of the folders, you will see that it is configured to be shared

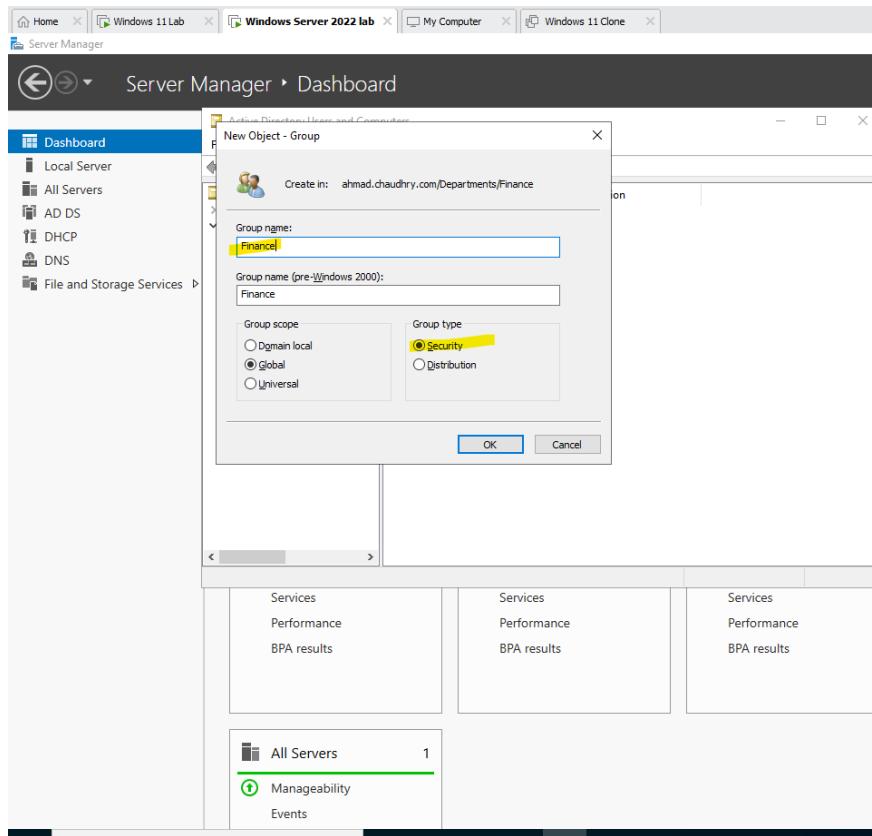


## We will create a security group

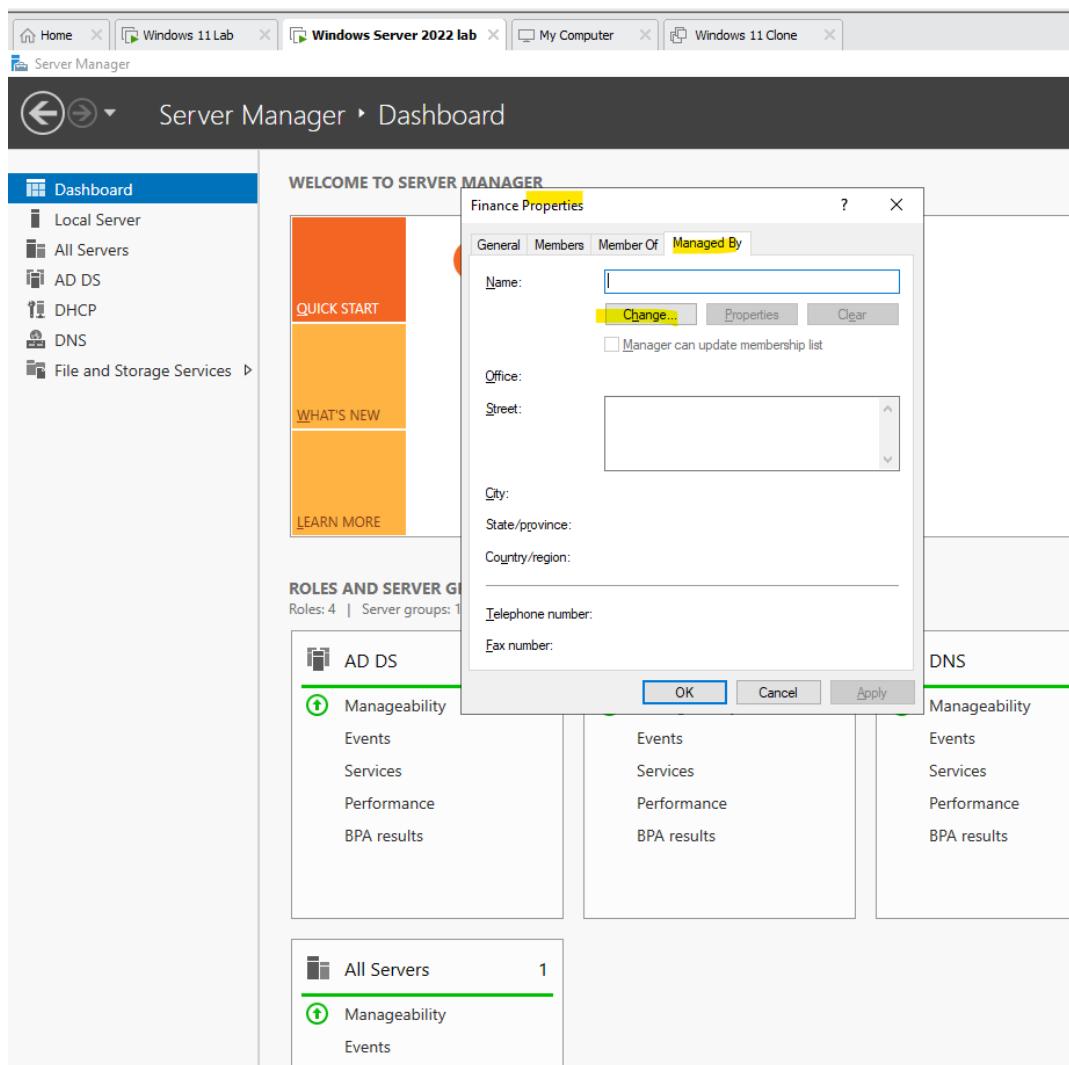
- In a job environment, there are 2 ways to provide access to folders:
  - By creating a security group, so only its members can access the folder
  - By granting **direct access** to specific users
- To create a security group for Finance, go to **Server Manager->Tools->Departments->Finance->** right click and select **new->Group**



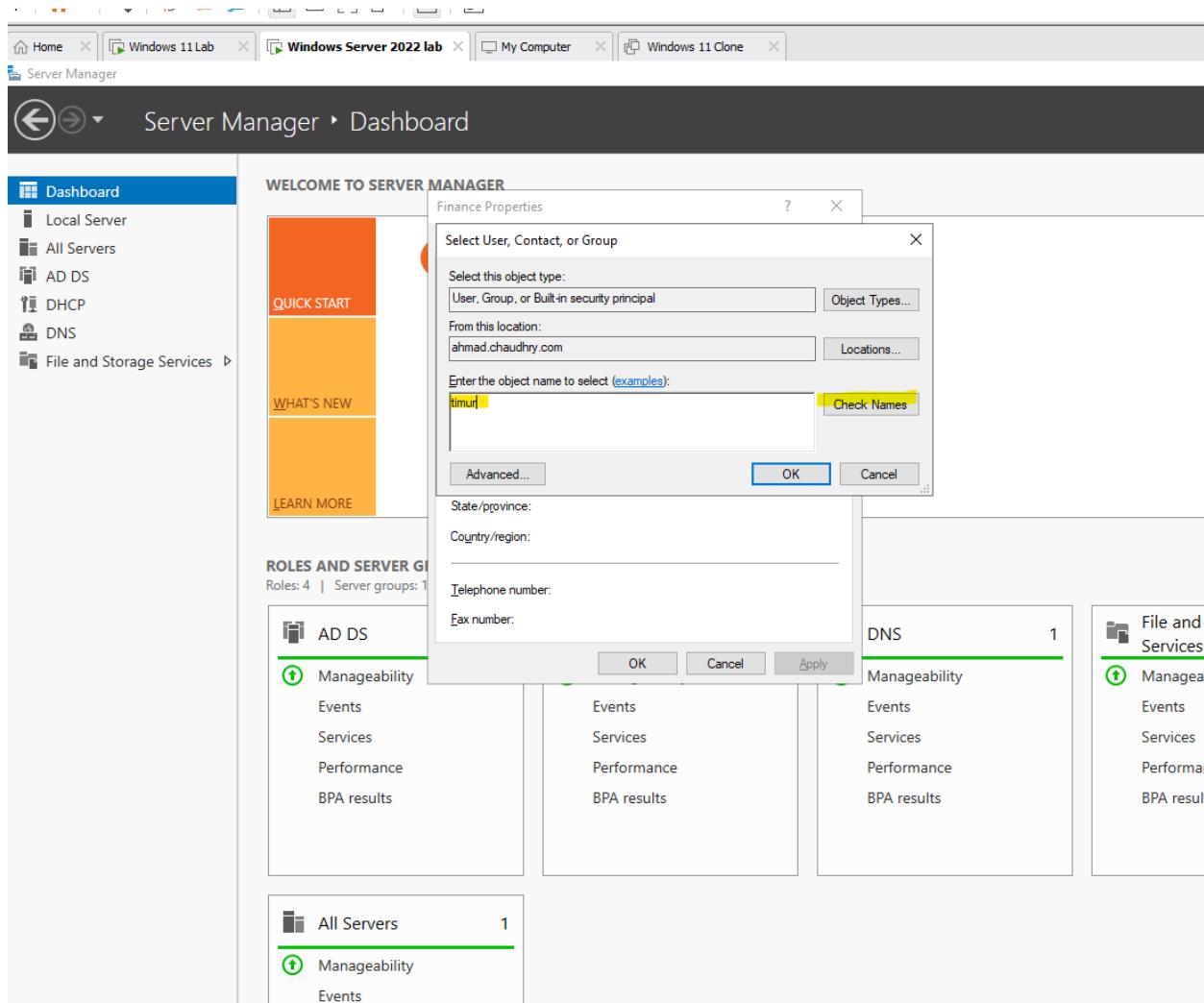
- Provide a name for the group and choose **Security** for the group type



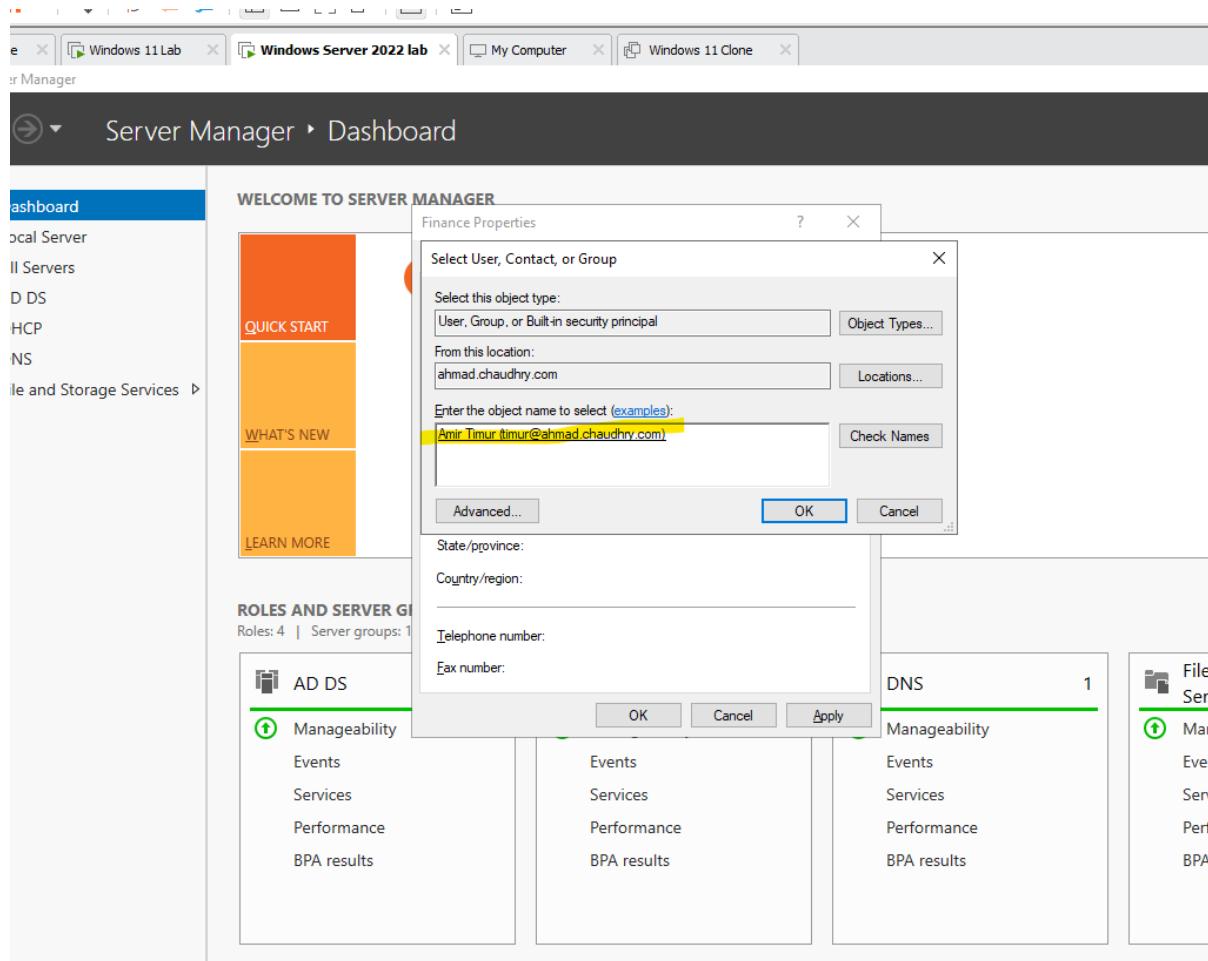
- Now, double-click the **Finance** security group. This is where you can manage permissions. For example, at Company Inc, **I.T** and **Shanon** have access. Here, I added **Timur** from I.T by doing the following:
  - Go to the **Managed by** tab and click "change..."



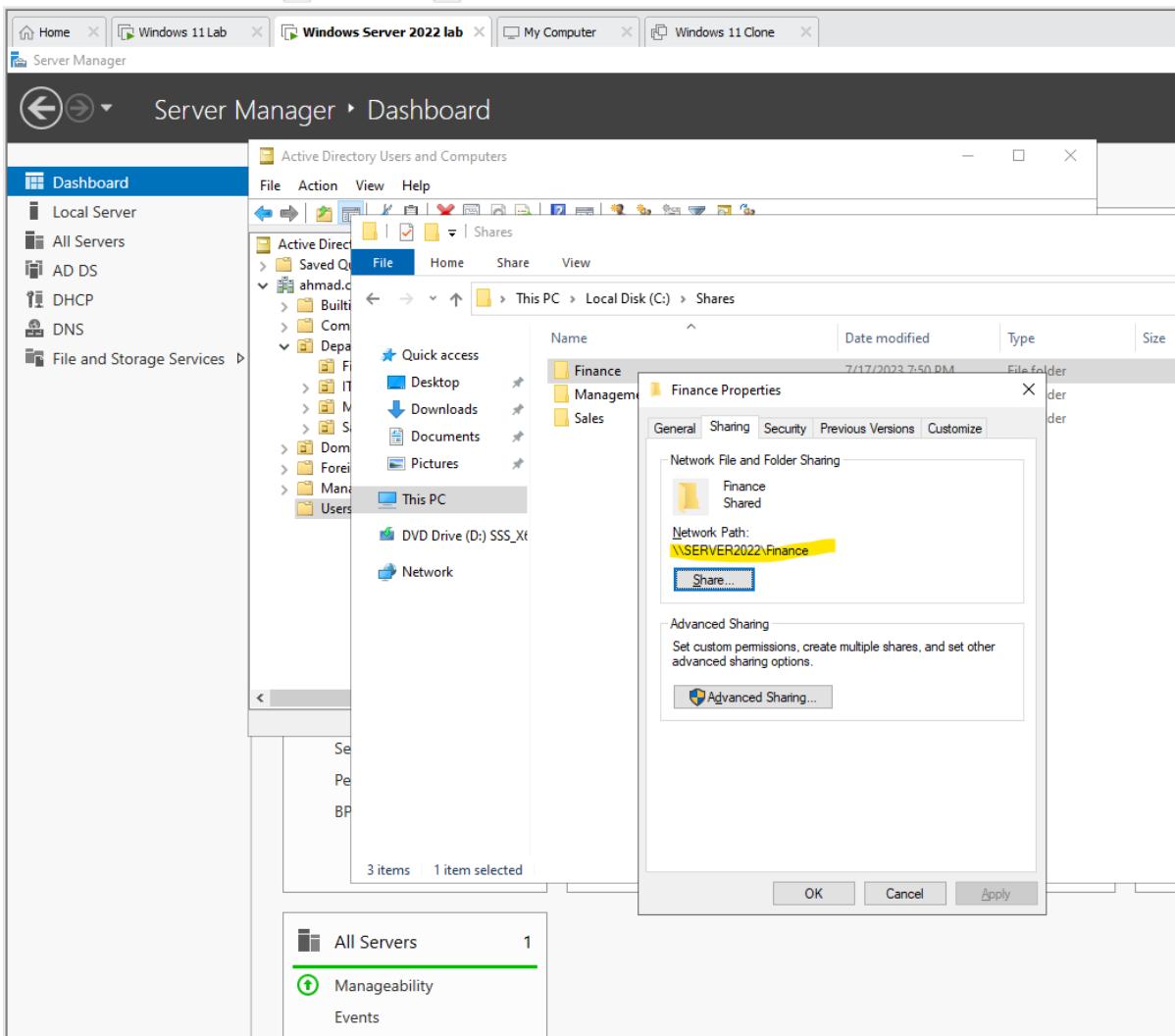
- Type "Timur" and then click **check names**



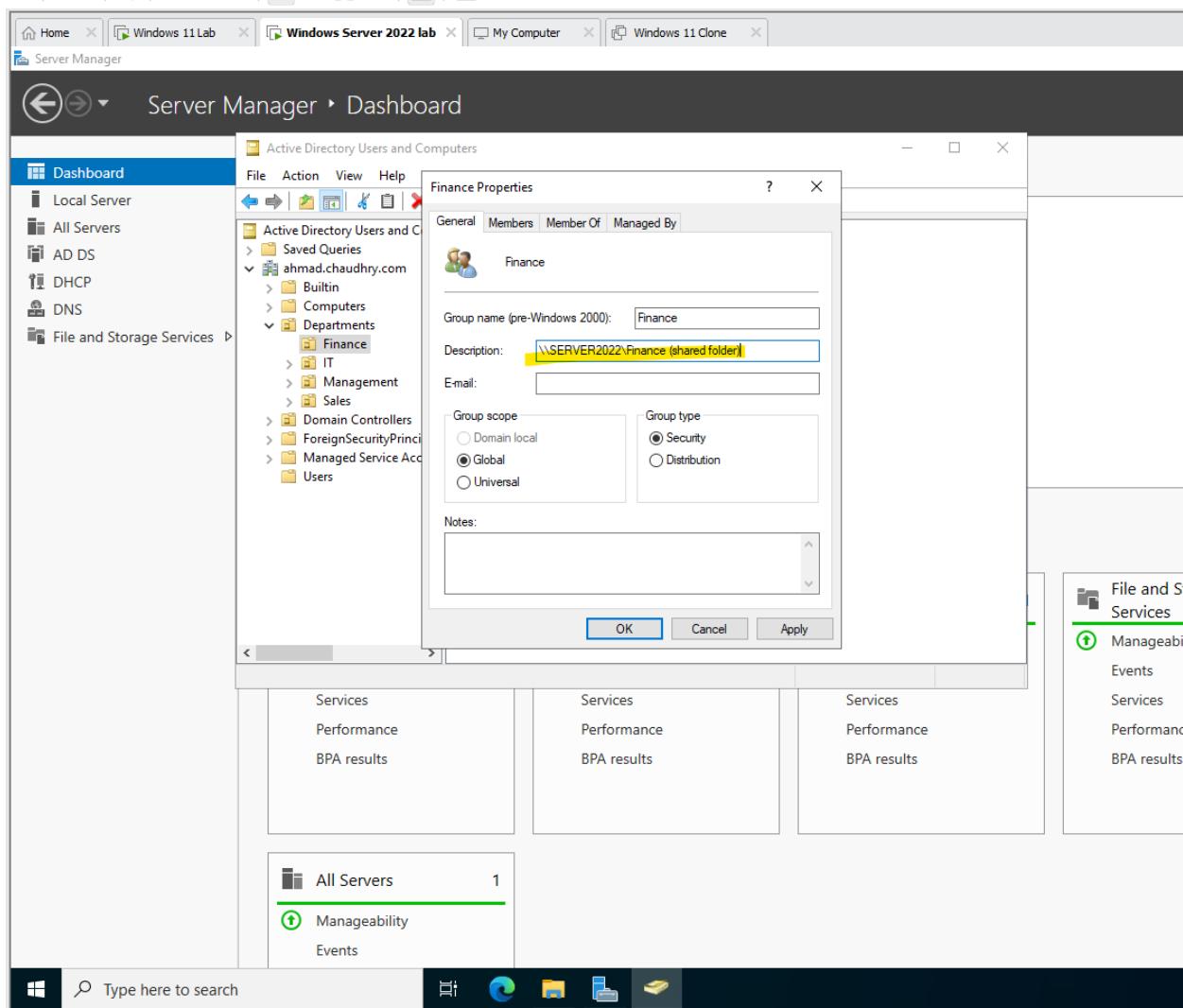
- Select the correct name:



- Create a **Management** security group by following the same steps as described earlier
- Add description to the finance security group. Right-click the **finance** shared folder->**properties->Sharing tab** and copy the **network path**



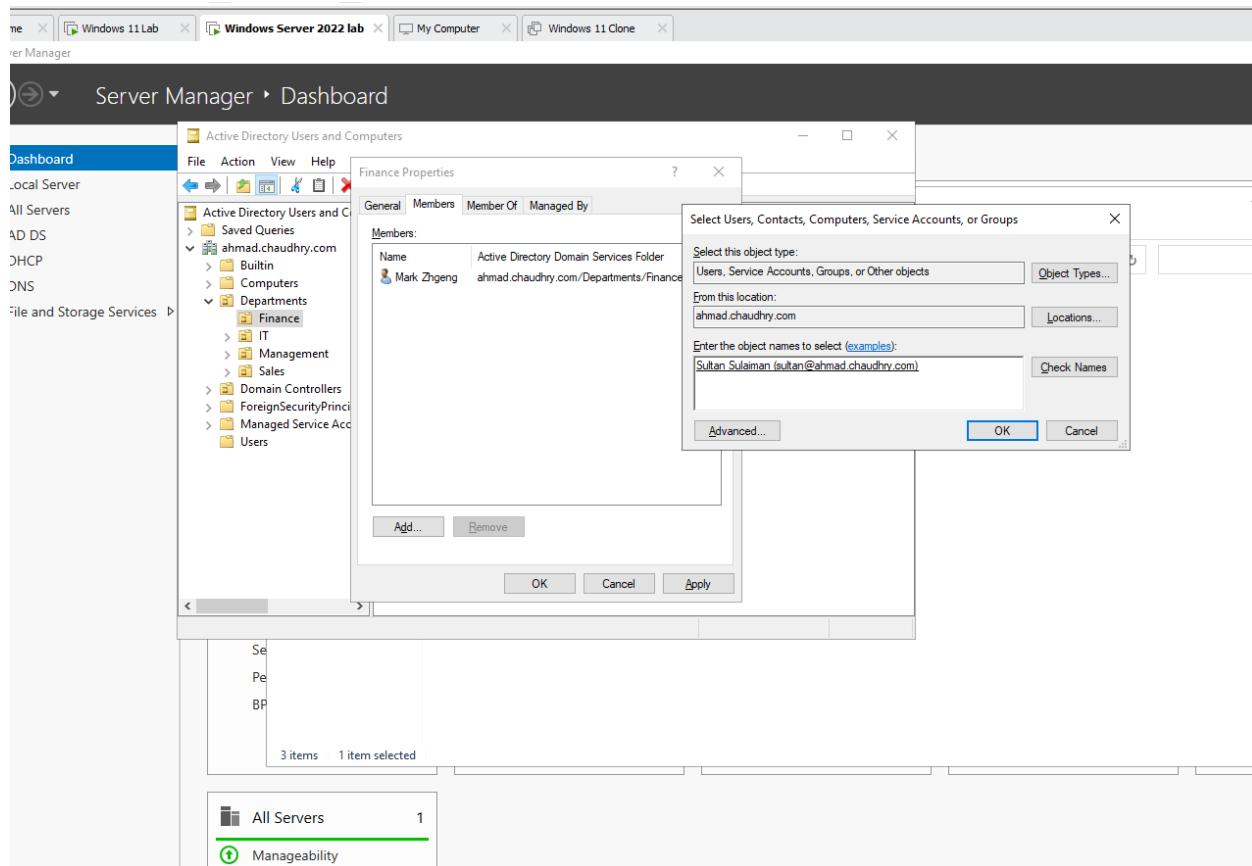
- Double-click the Finance security group and paste the **network path** in the **description** section and add “**(shared folder)**” at the end



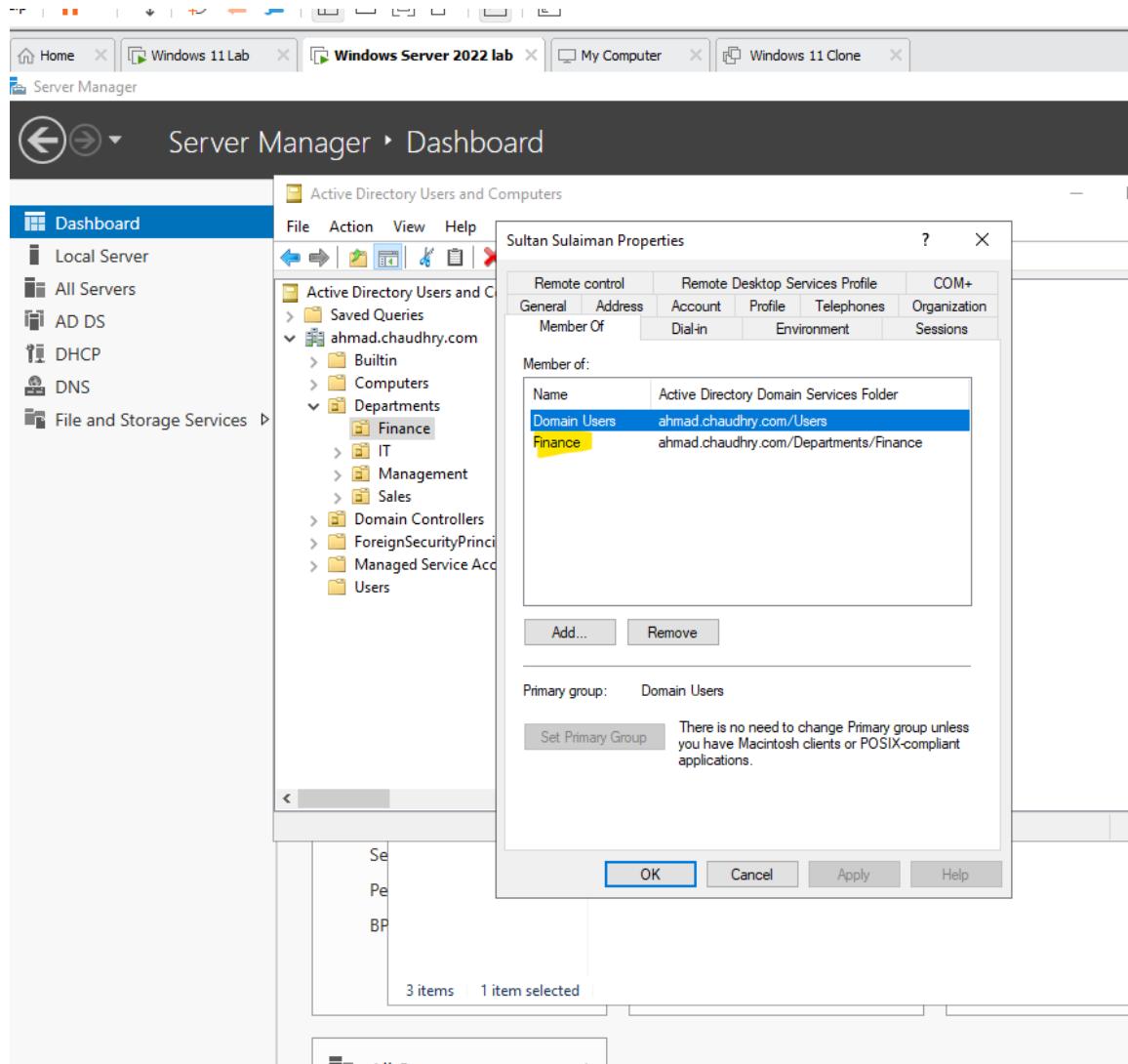
- Perform the same actions for the **management** security group

We will add members to the finance security group

- Double click **finance** security group-> click **members** tab->select **add...**->and add names



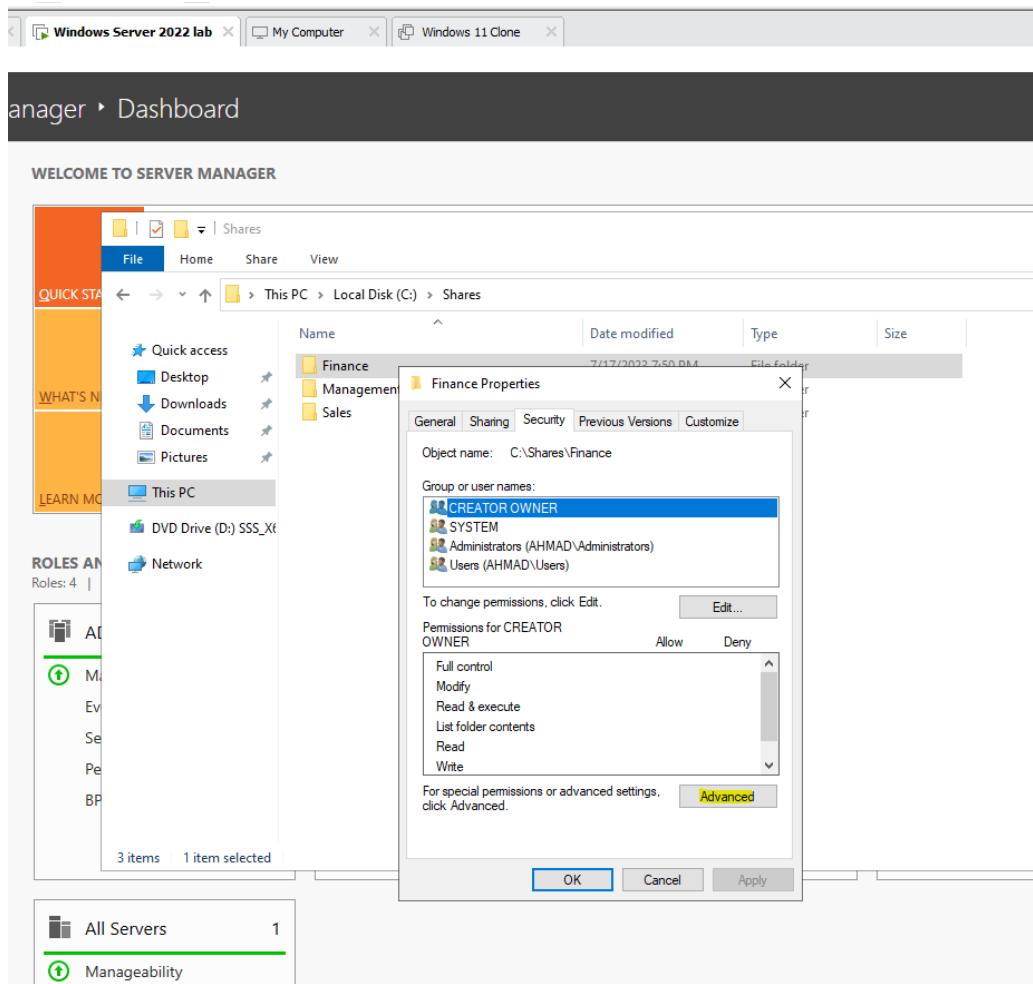
- To confirm it's configured correctly, go to one of the users (ex Sultan Sulaiman)->Select "member of" and you will be able to see it



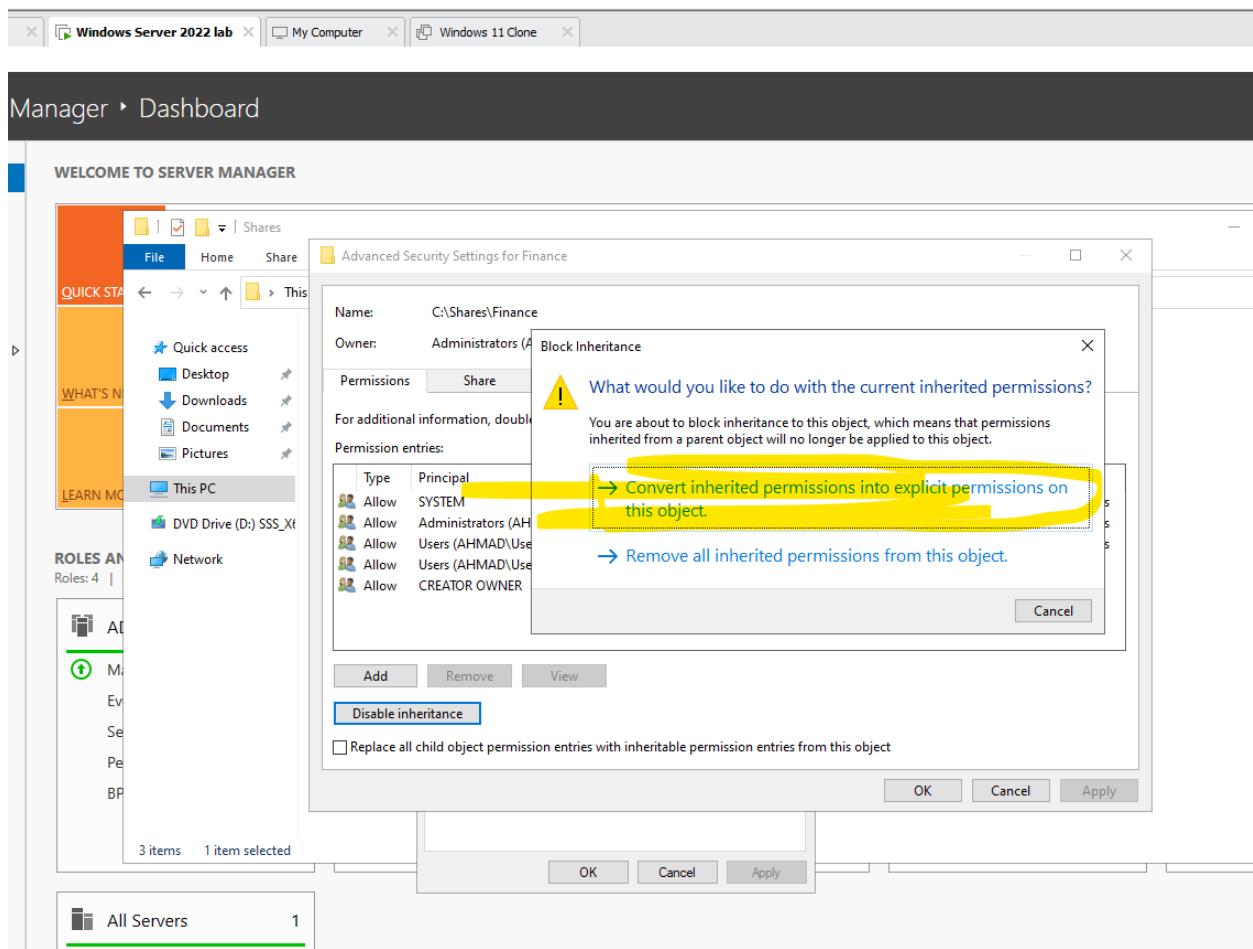
- Follow the same procedure for management and sales department

### We will set up permission for the folder

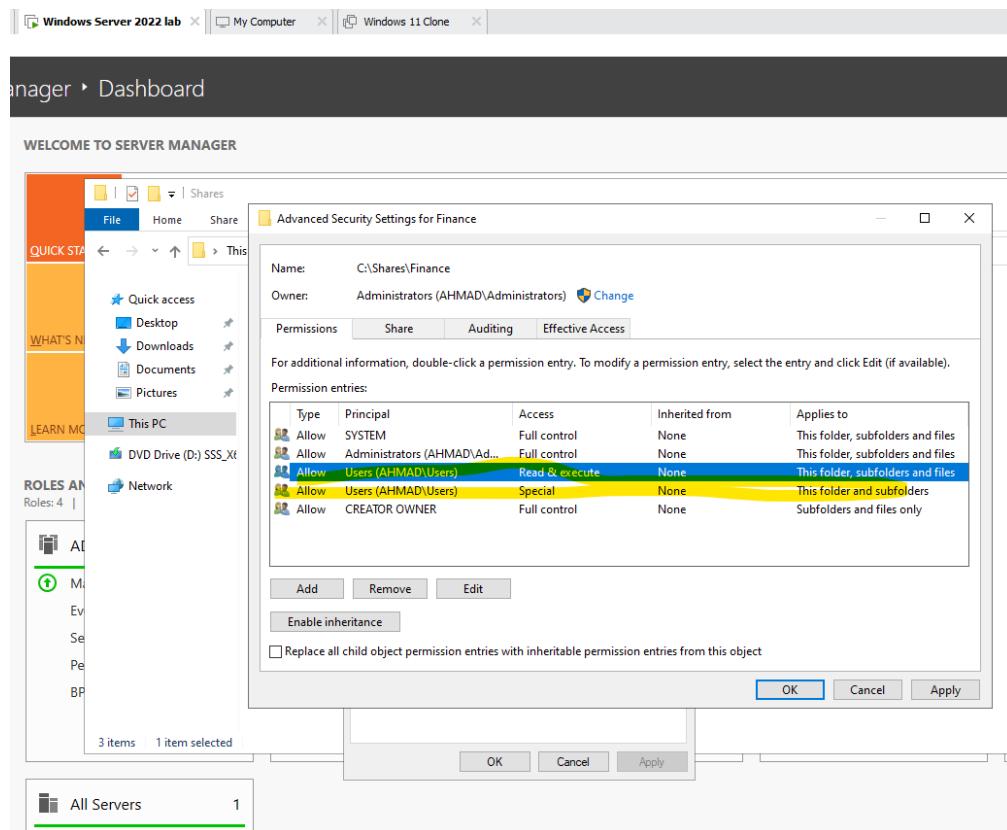
- Go to properties of **finance** folder->**security tab**->**advanced**



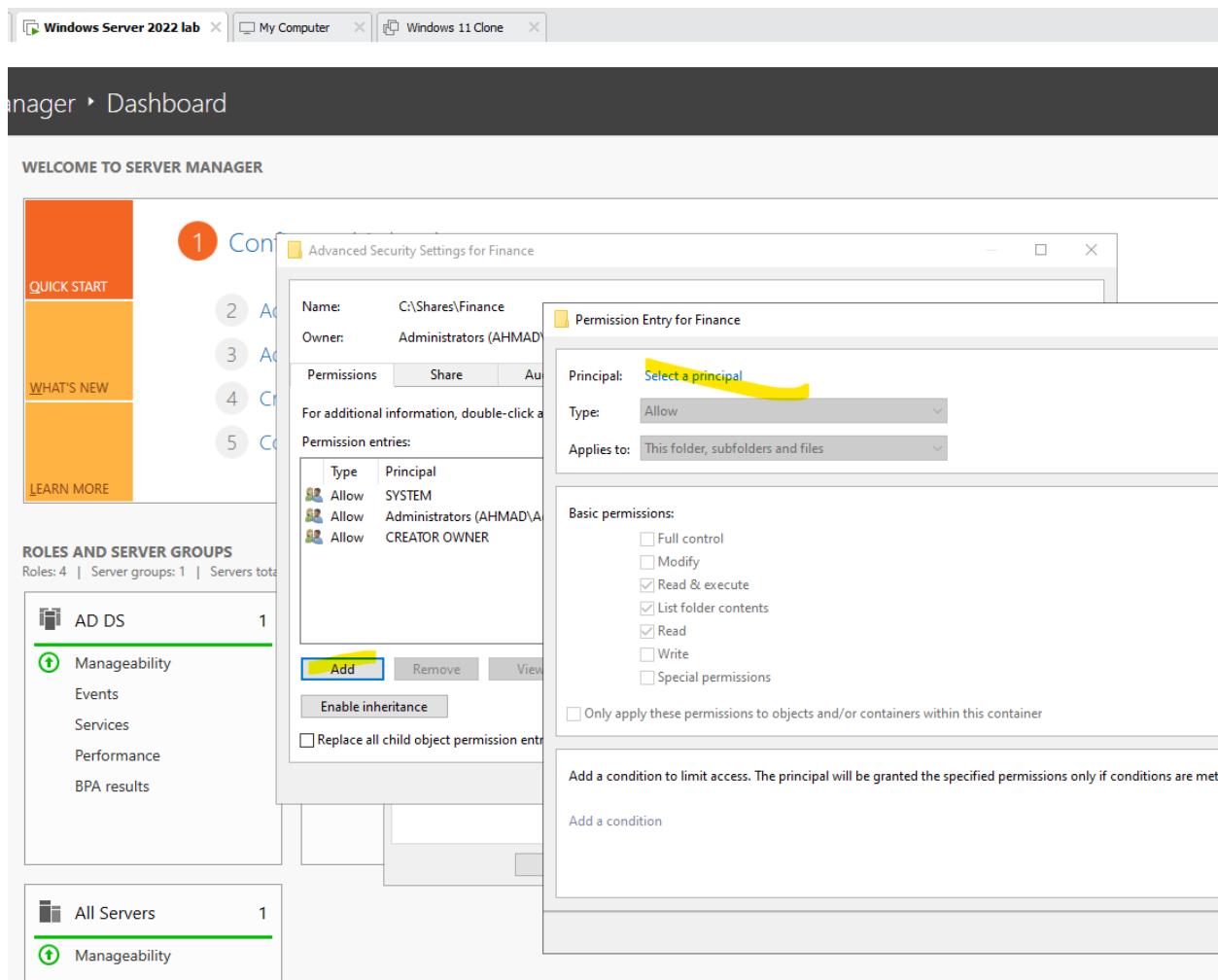
- In the **permission** tab->click **disable inheritance** and select the highlight option shown in the screenshot



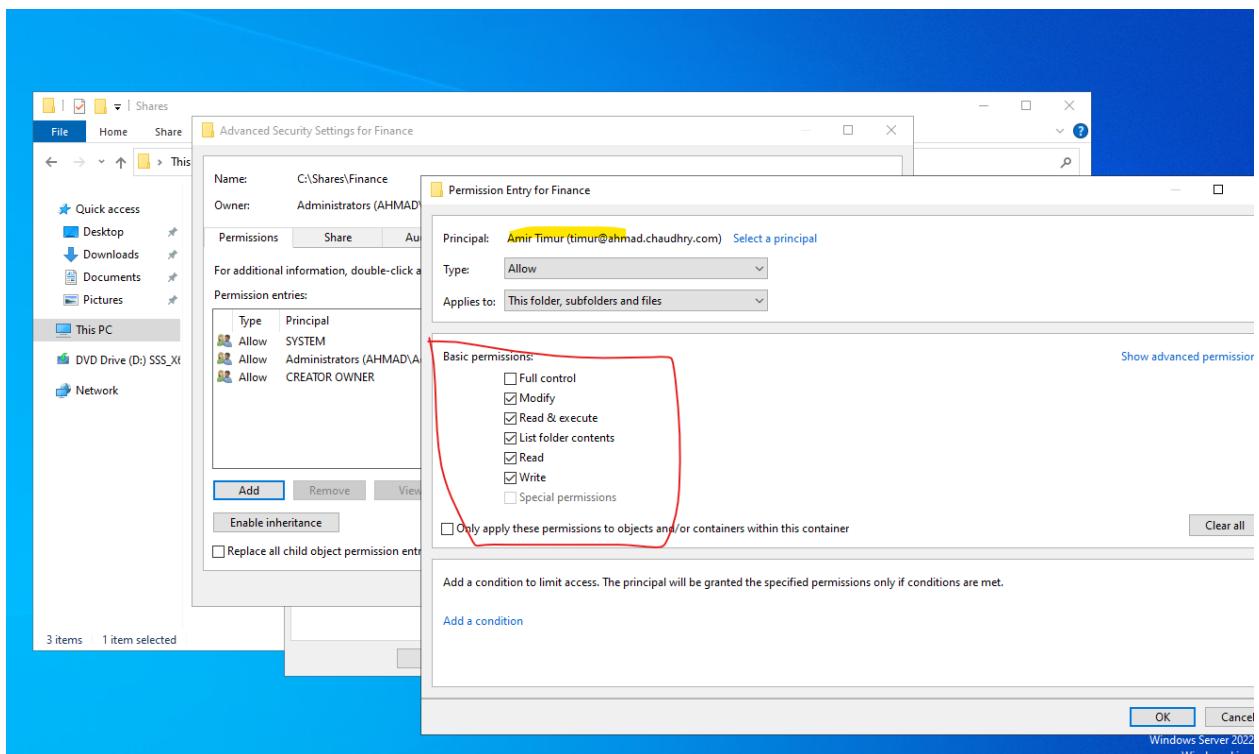
- These are added users and we will remove "**Users**", highlighted in yellow in the screenshot



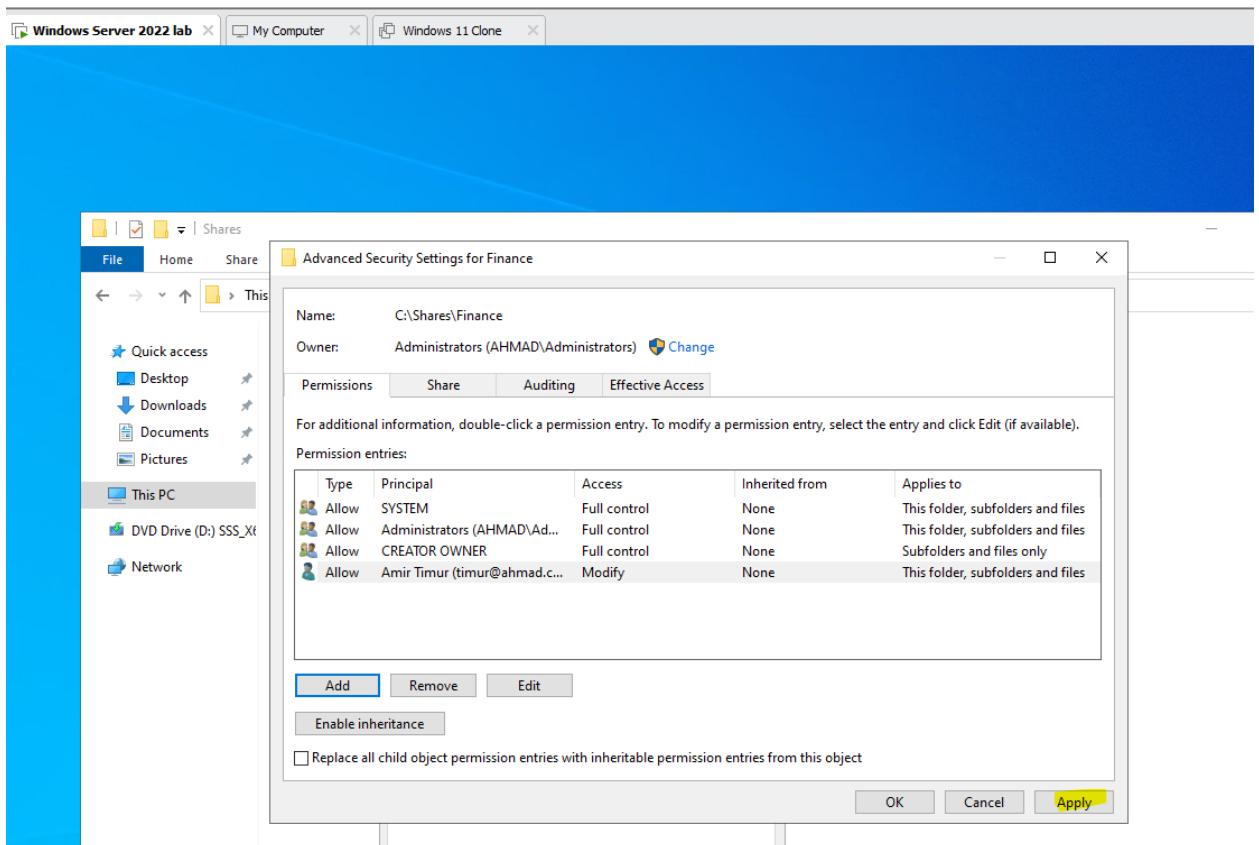
- Click add -> Select a Principle



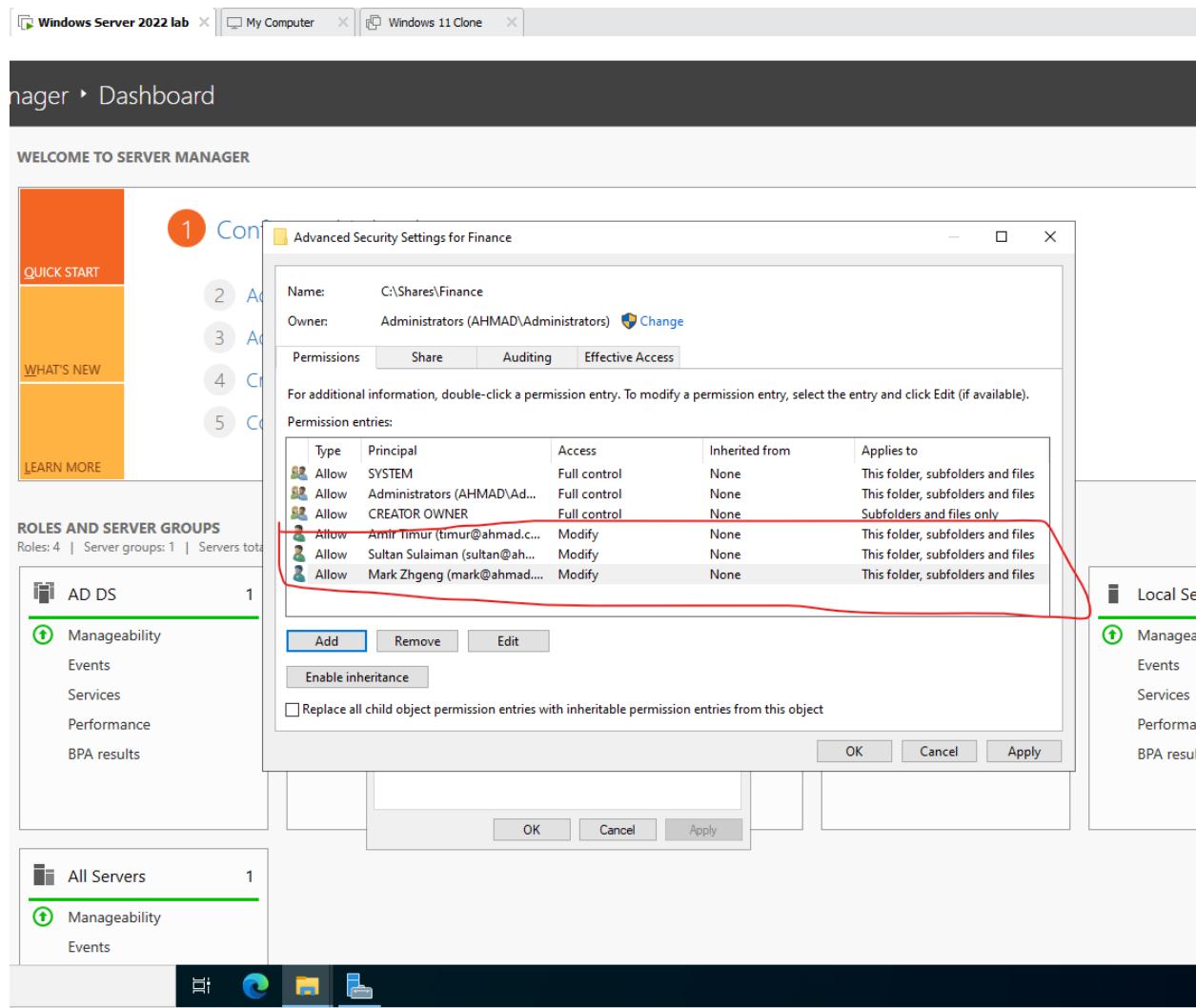
- Add Timur, an I.T. employee who manages folder access and ensures it has the following permissions:



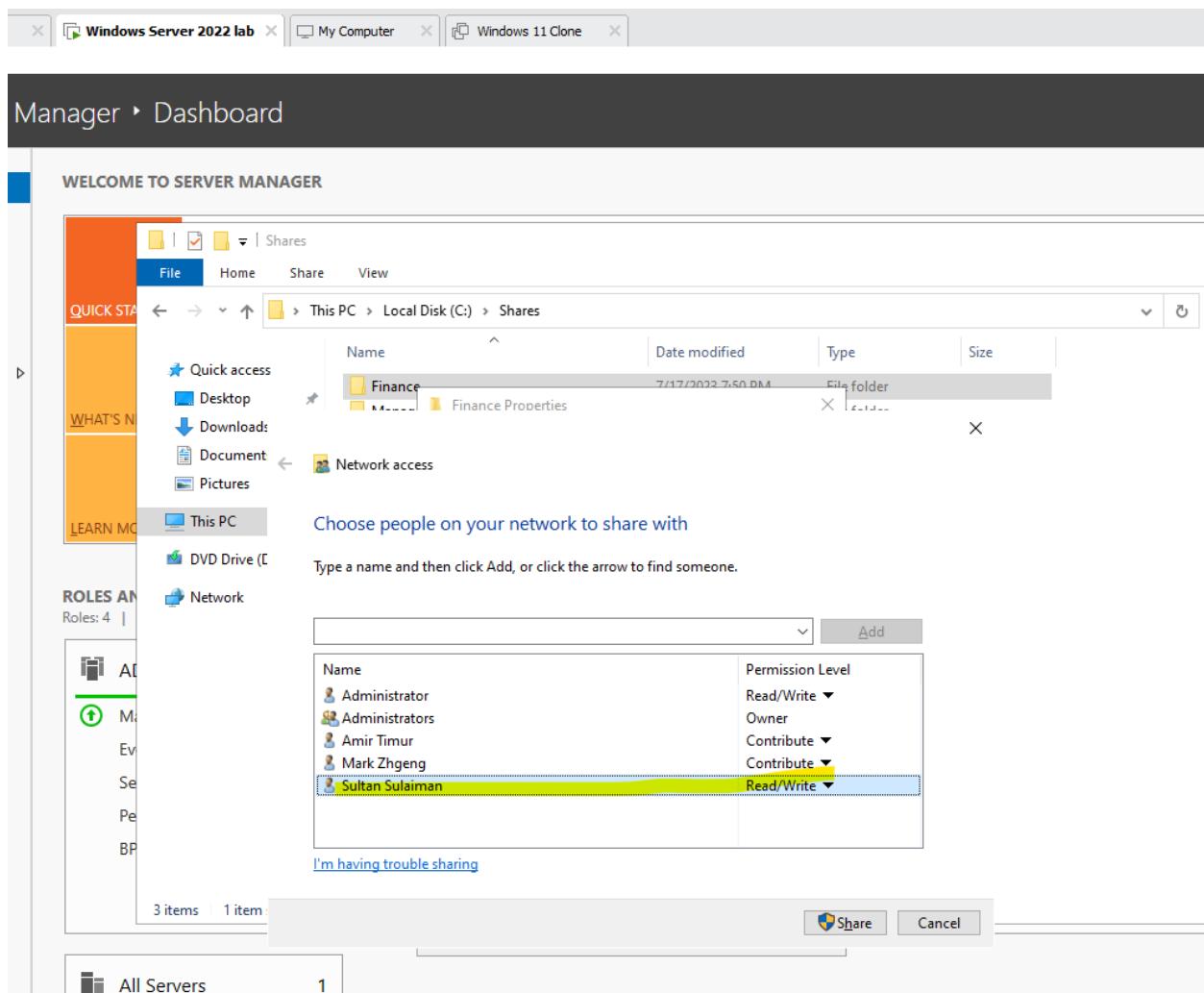
- Click apply



- Now, add users in the finance department for this folder:



- Right click **Finance** shared folder->Select the "**Sharing**" tab->select "**Share...**">Select one of the finance users (Sultan in this case)->and select "**Read/Write**"



- Select Share

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
Amir Timur	Contribute ▾
Mark Zheng	Contribute ▾
Sultan Sulaiman	Read/Write ▾

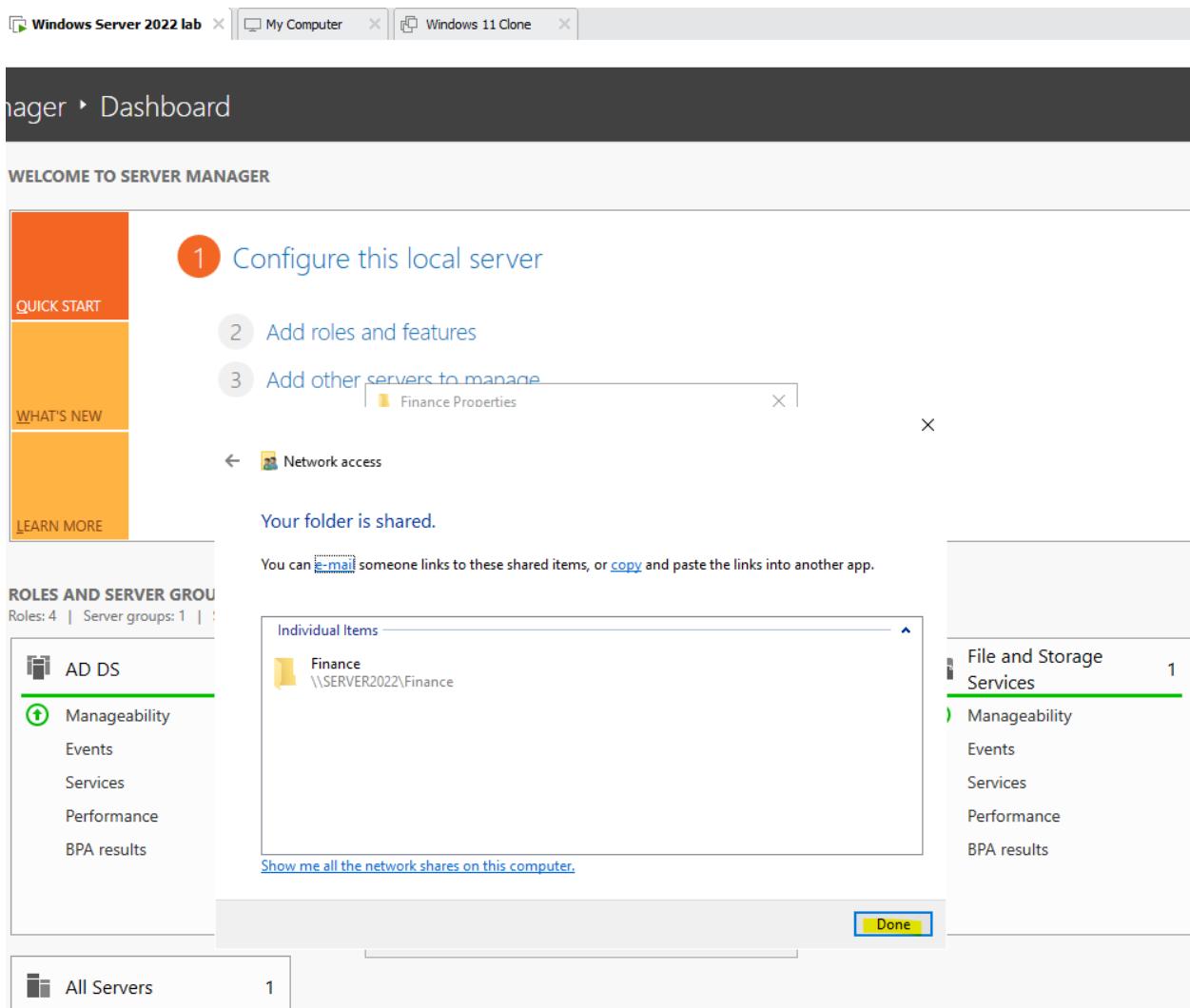
I'm having trouble sharing

Share Cancel

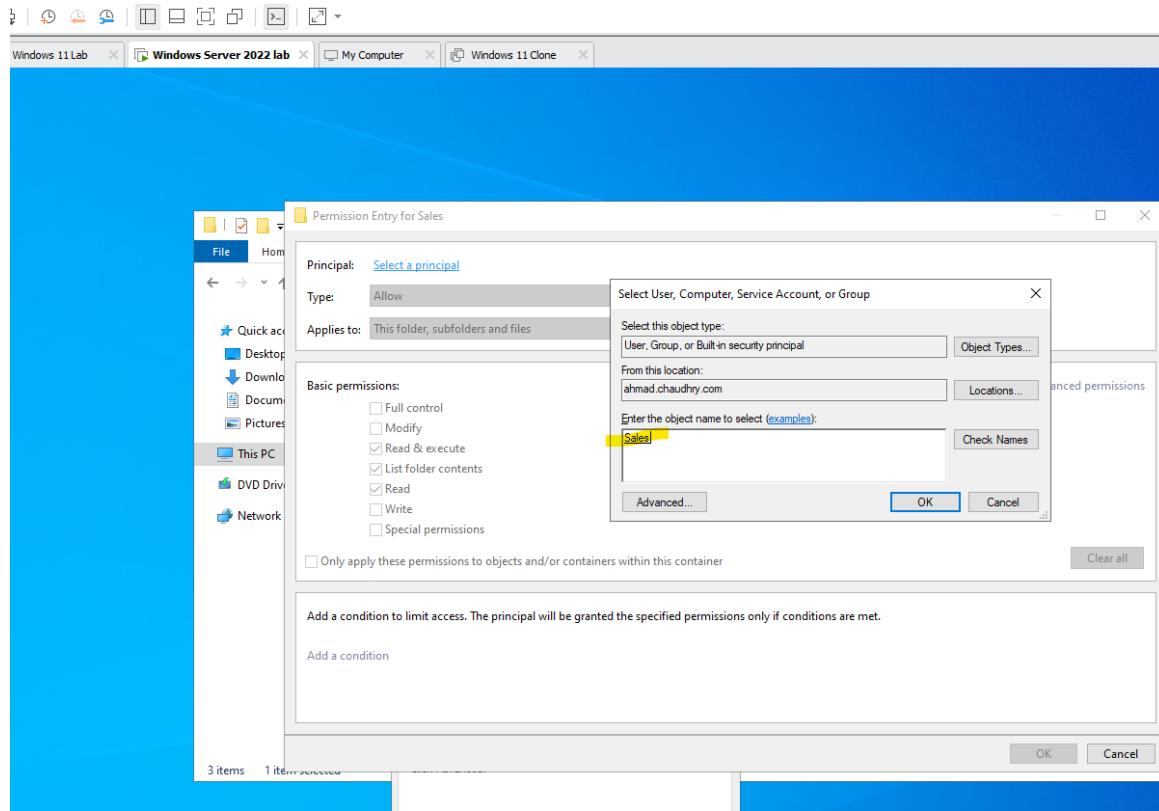
File and St Services

All Servers 1

- Select done



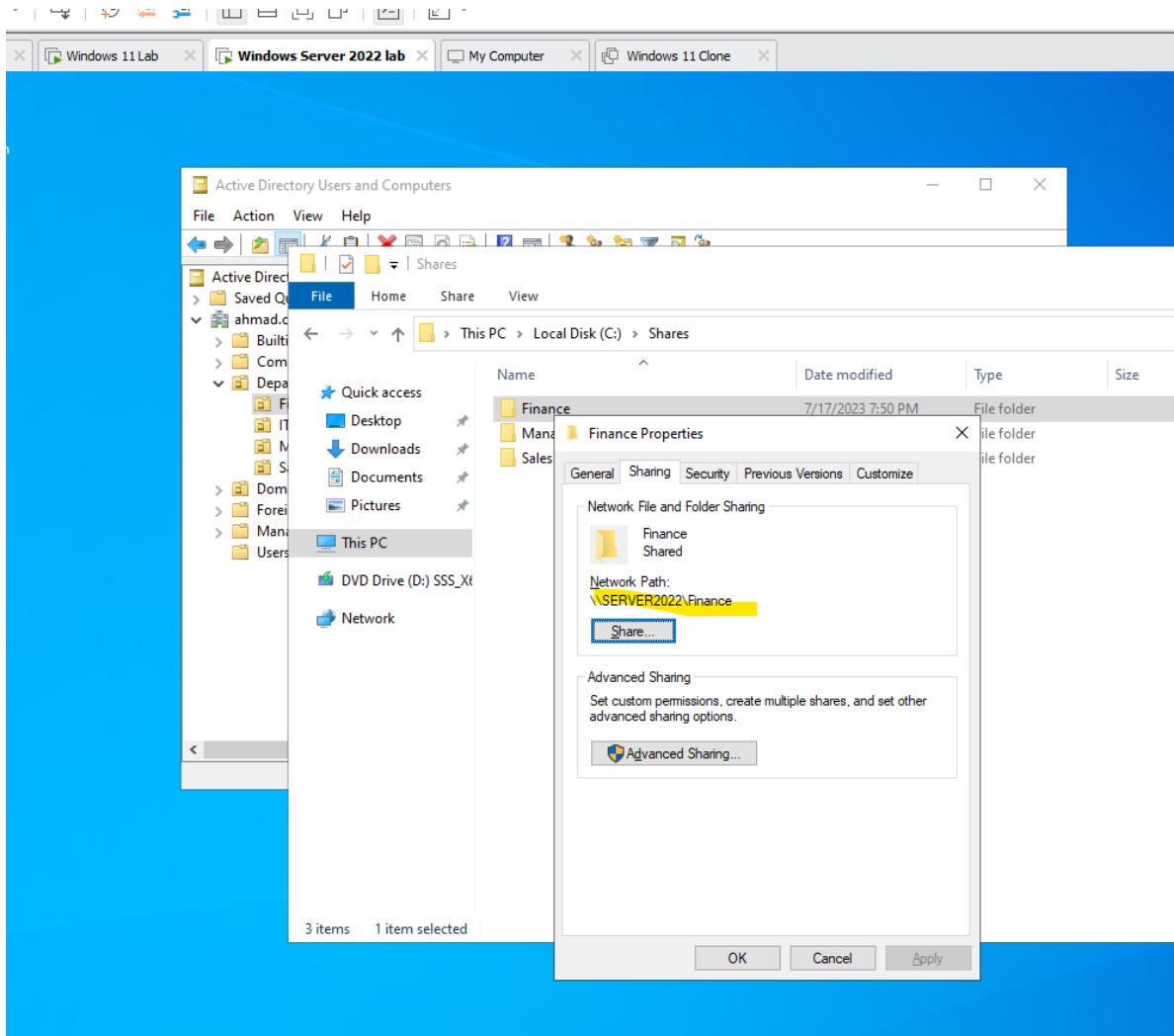
- Perform the same action for Mark
- Follow the exact procedure for the Management folder, add Tom Smith as a user and set his permission level to **Read/Write**
- So far, we have covered how to grant permission for each specific user and not a security group
- We will grant permission to the Sales Department using the Sales security group:
  - The process is the same, except select the security group instead of an individual user.
  - Ensure the permission level is set to Read/Write.



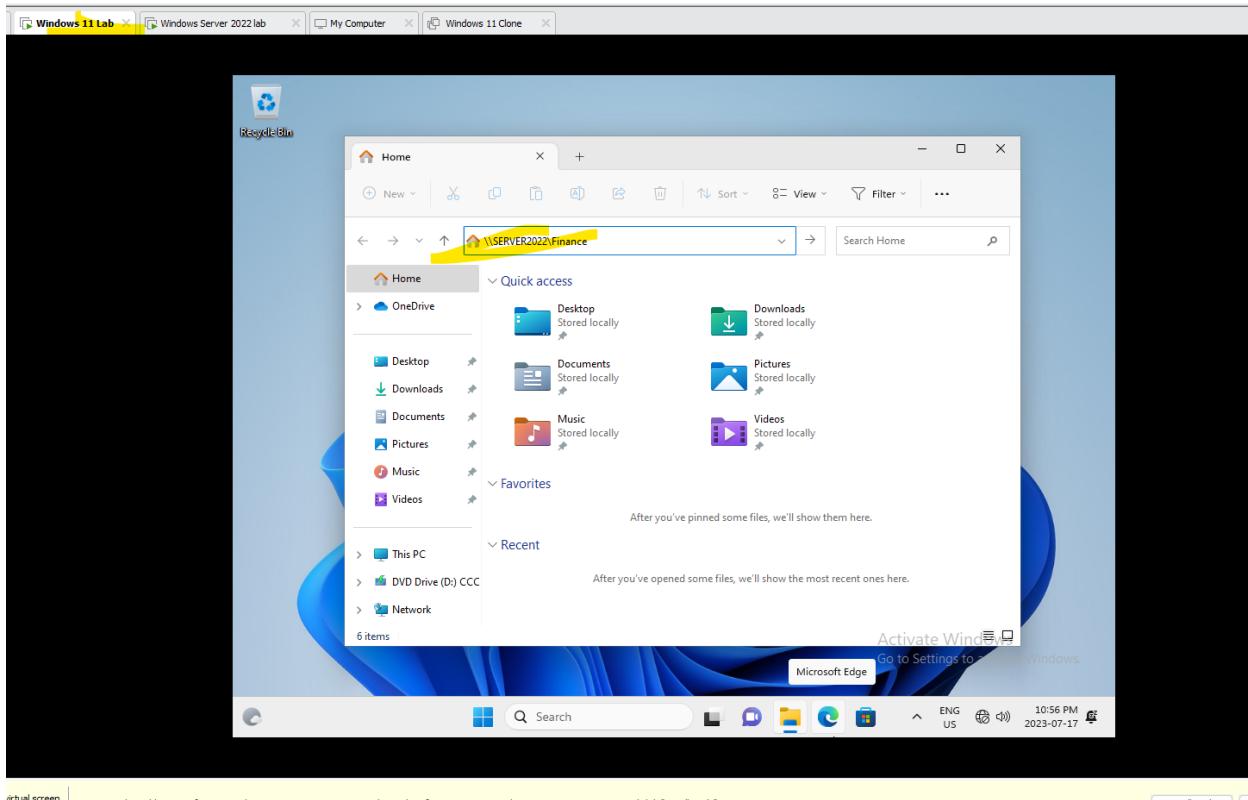
## How to map the network shared

### First Method to Map a Network Drive

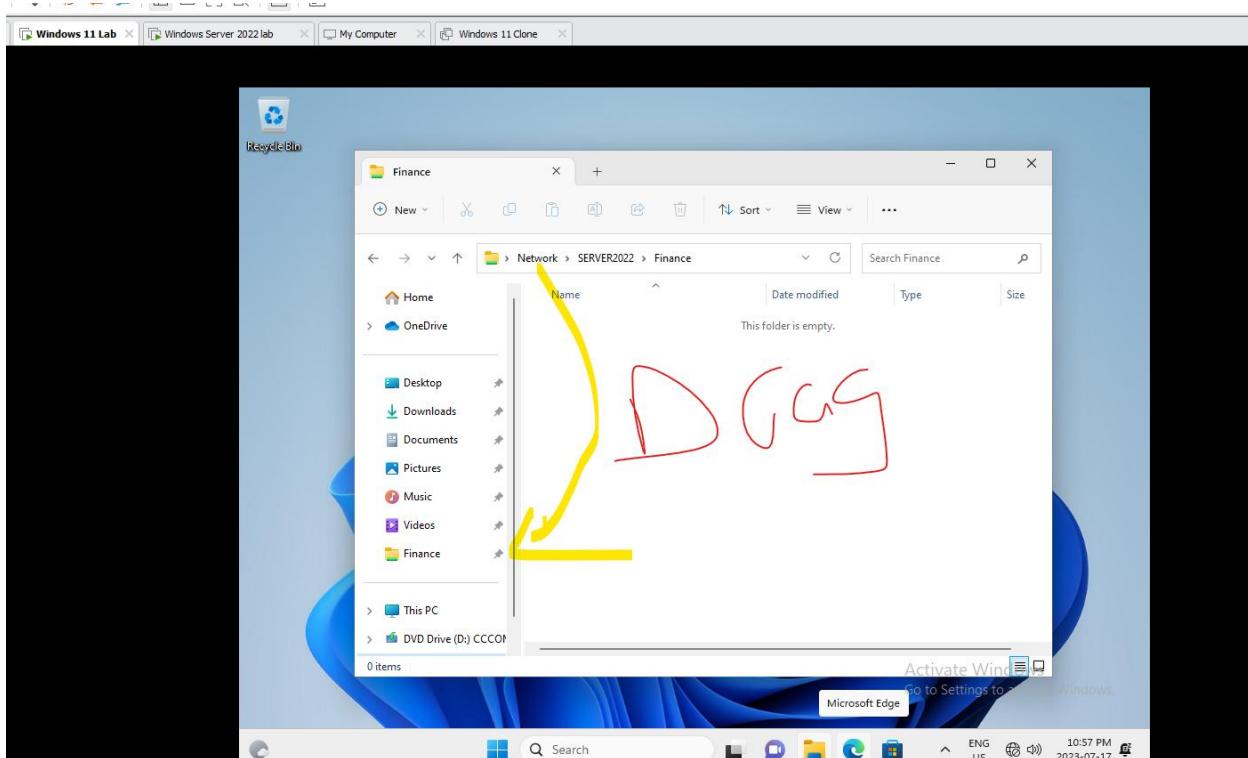
- Log in as Sultan Soliman from Finance in the Windows 11 Lab
- In Windows Server 2022, copy the finance shared folder network path



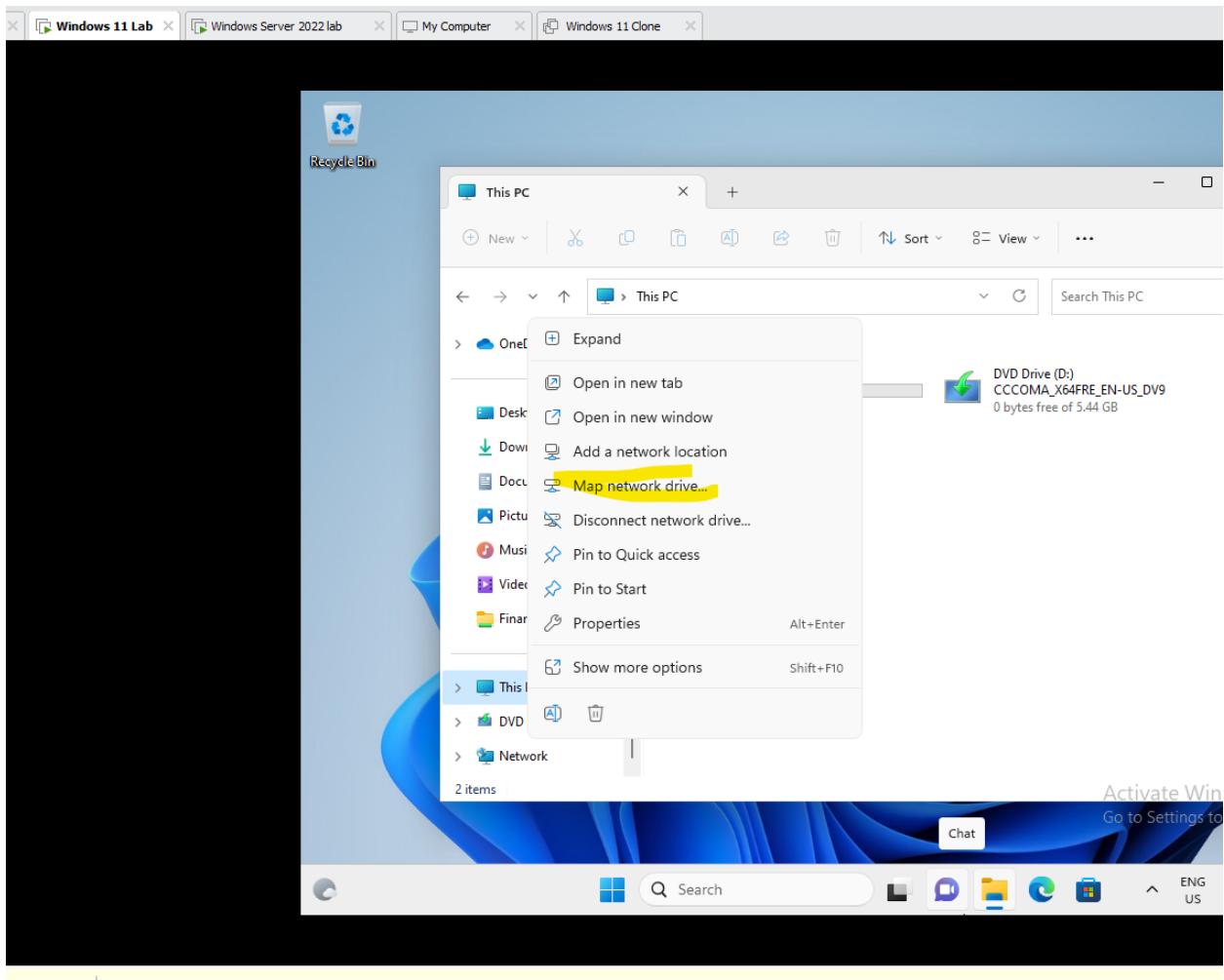
- Windows 11: In the file explorer, type the file path



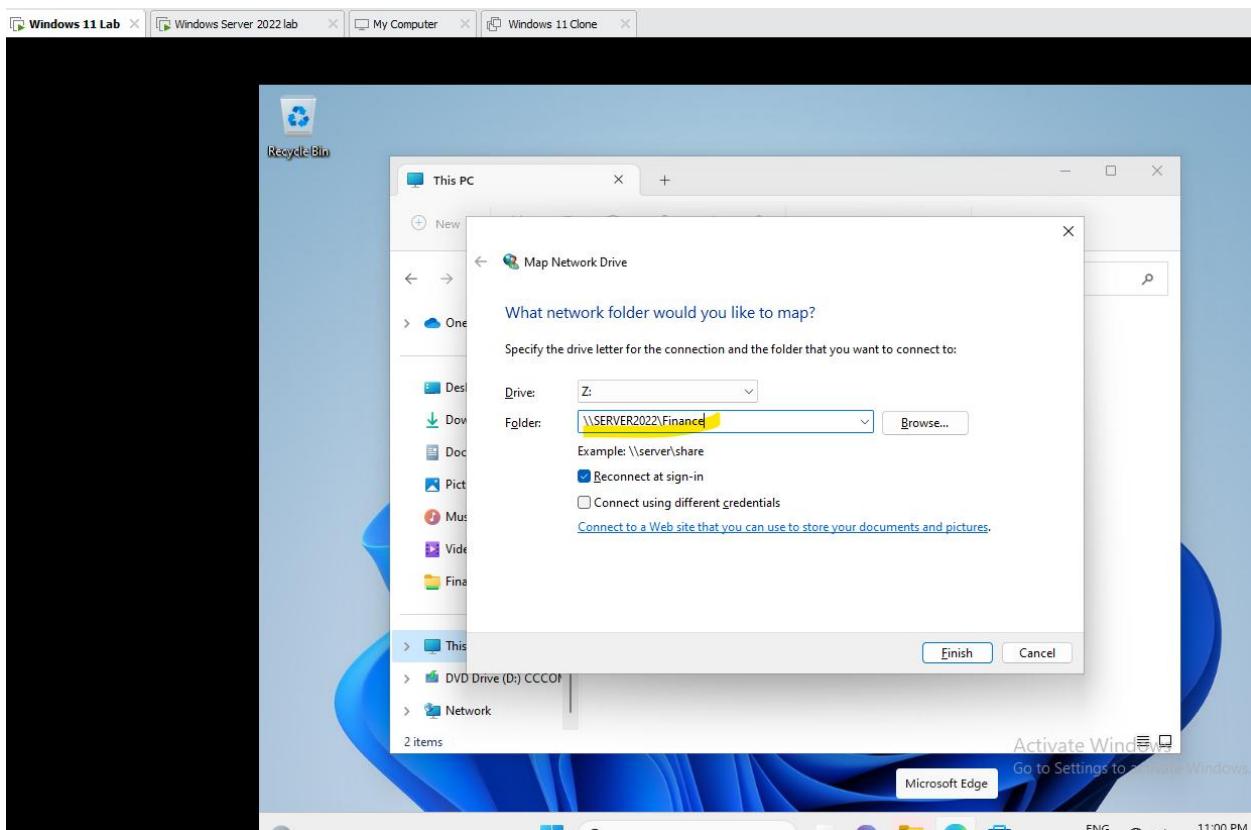
- Drag it to the right side to create a quick link



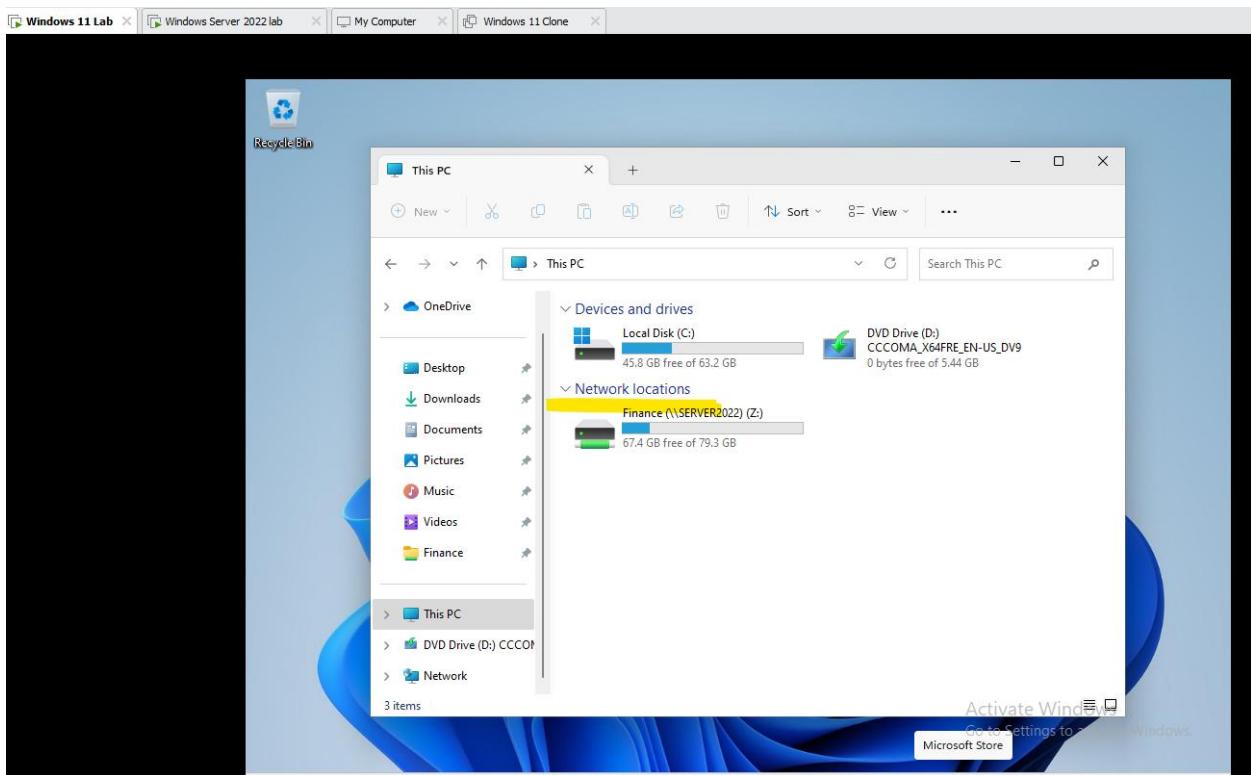
- To map network drive: copy the file path-> right click "This PC"->select "Map network drive..."



- Paste the file path
  - Enable "**reconnect at sign-in**", which ensures the drive connects automatically each time the user logs in



- You can see the drive now

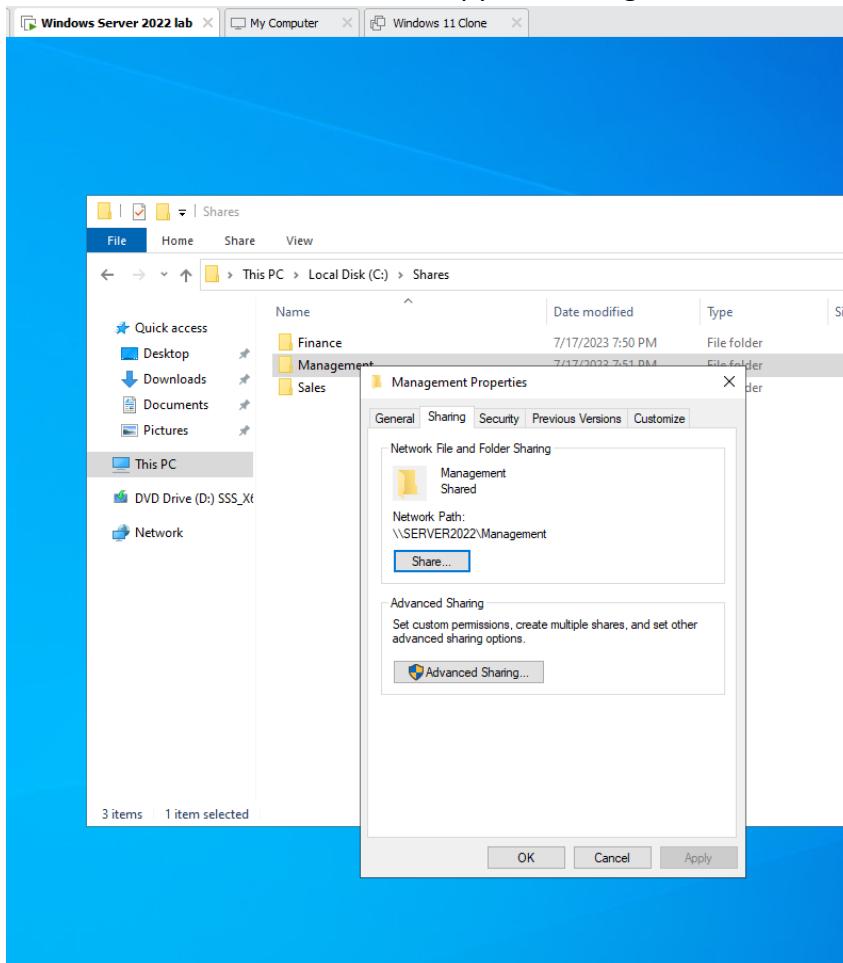


- The drive is currently mapped via a security group, but it's also possible to grant a single user access to a specific folder
- Up to this point, we have only mapped the drive, without creating folders for individual users

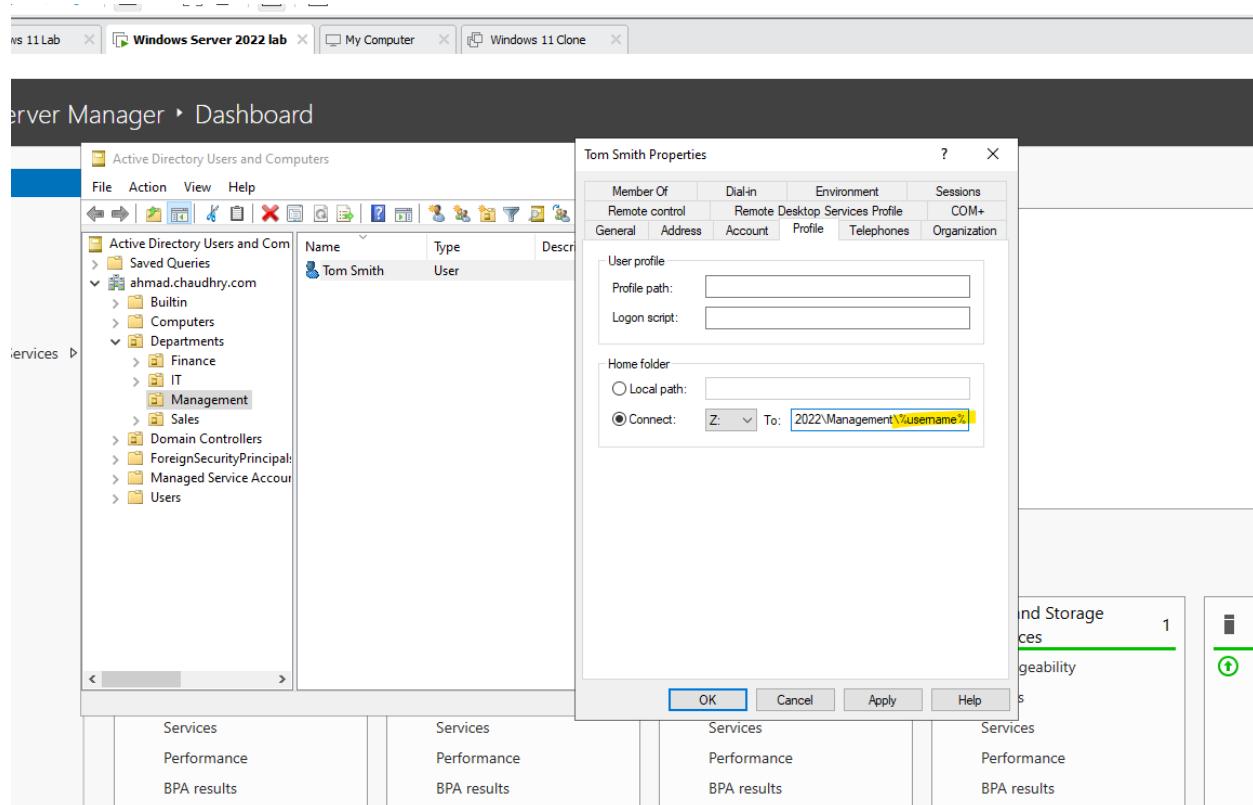
### Second Method to Map a Network Drive

We will map the drive via Active Directory for management and the user folder

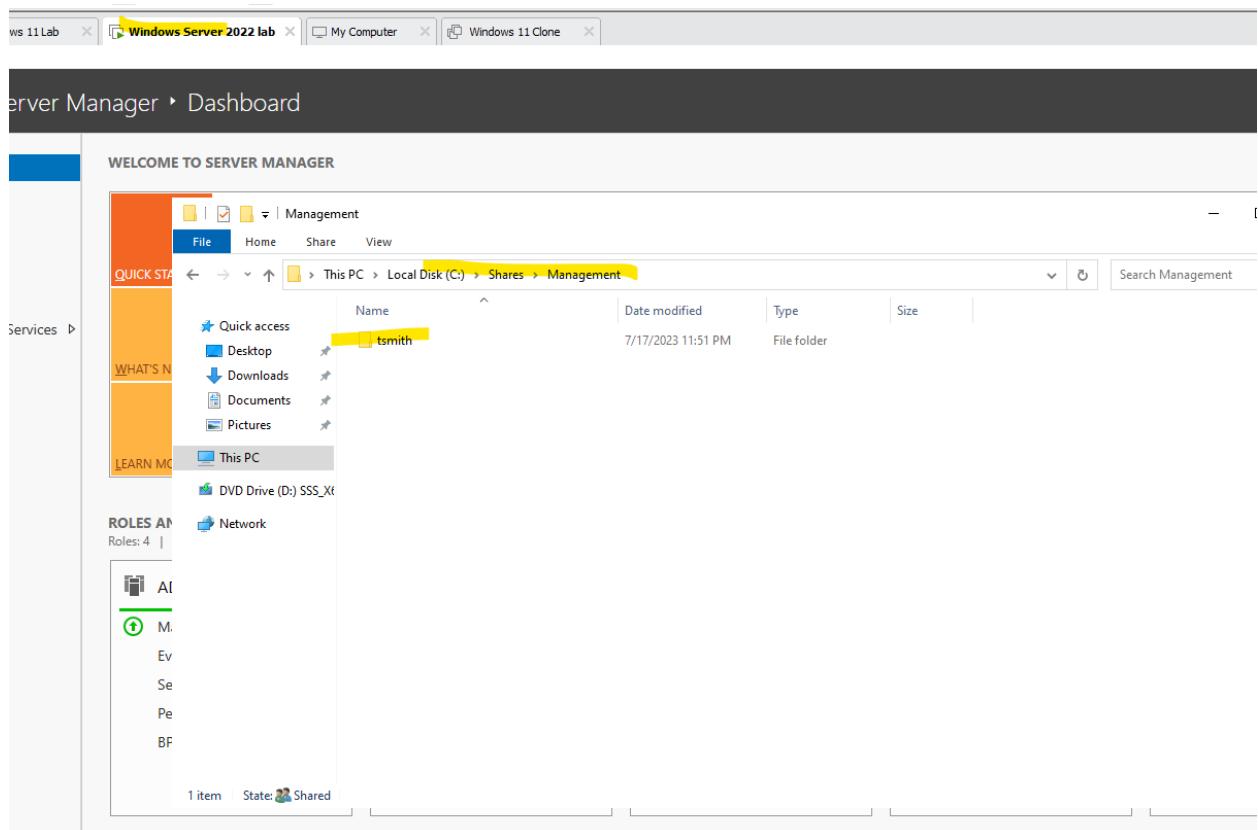
- In Windows 2022 Server, copy the management shared folder network path



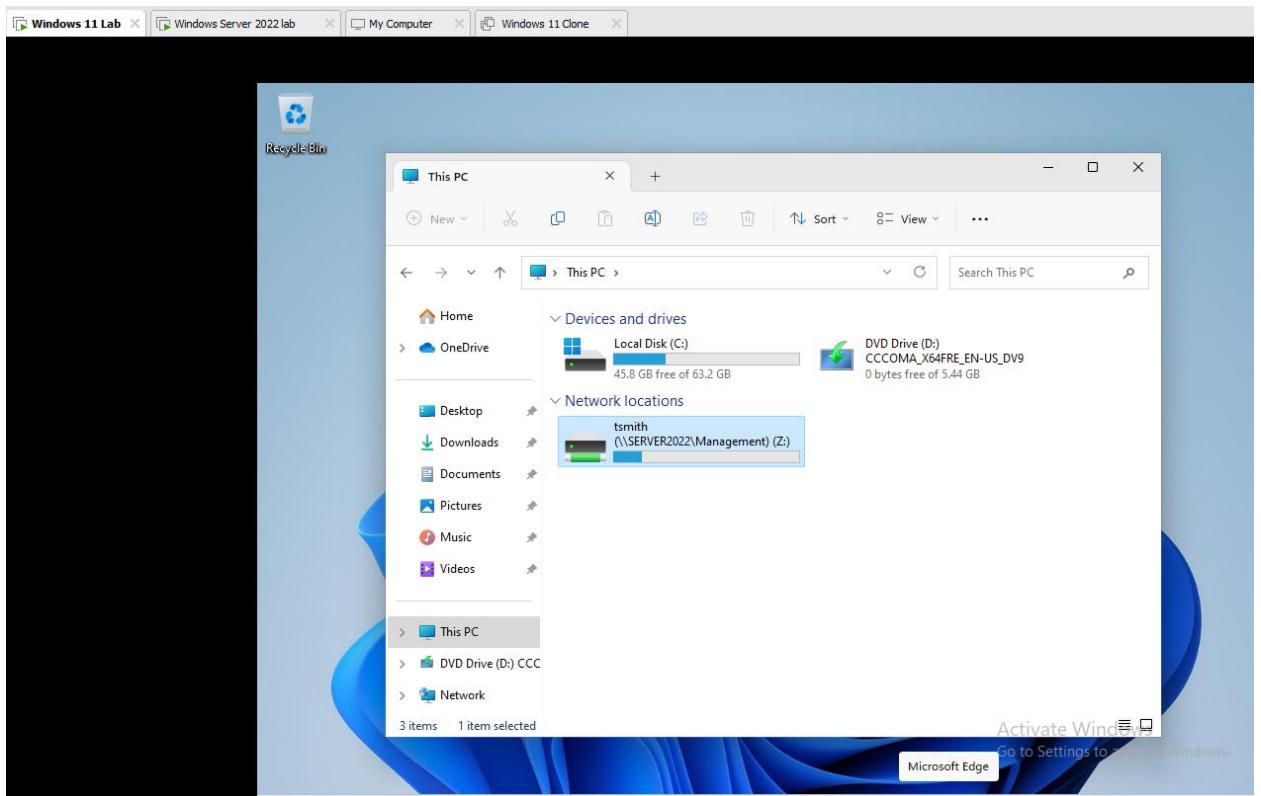
- Go to **Server Manager->Active directory users and computers->**go to **Tom Smith's** properties-> Select the **Profile** tab->and paste it the **connect** field but add **\%username%** at the end



- The shared folder will now display a folder named using **Tom's username**

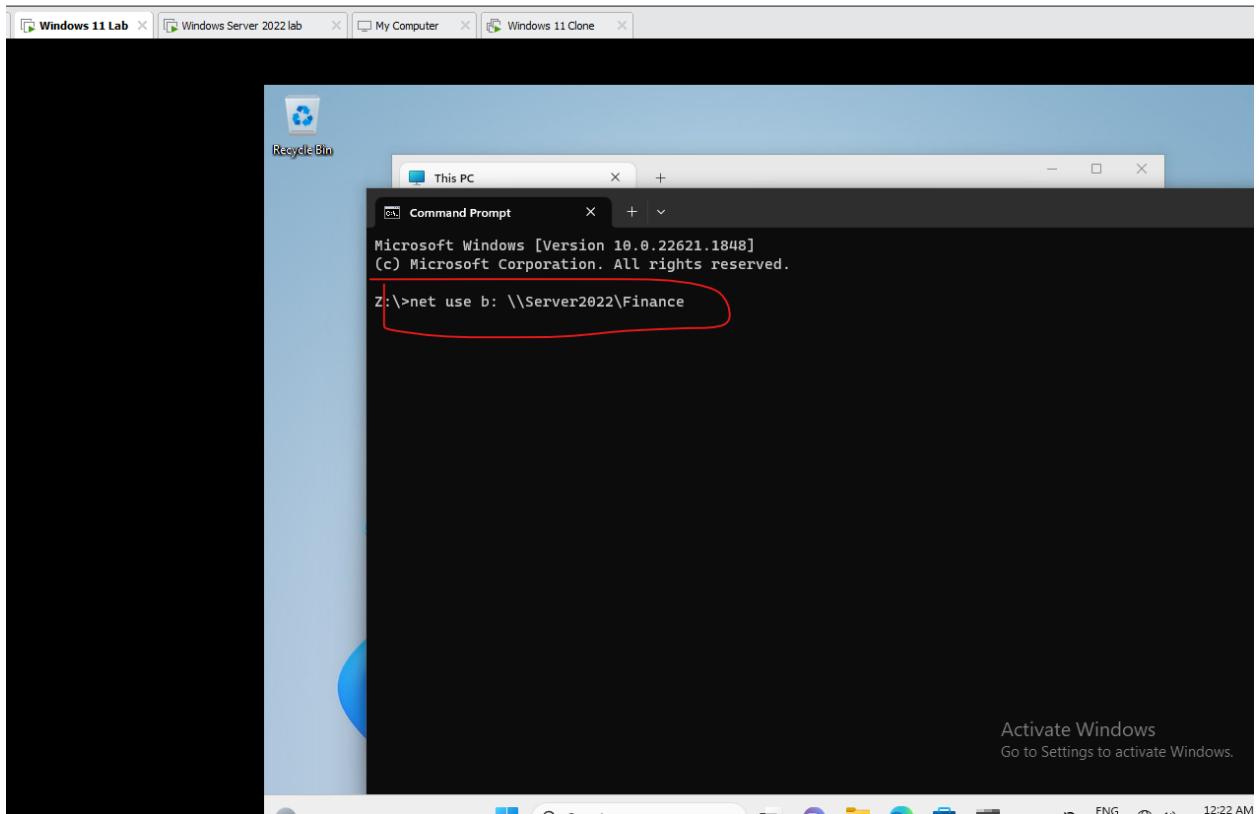


- Log in as **Tom**, and you will see that the network drive has been created for you

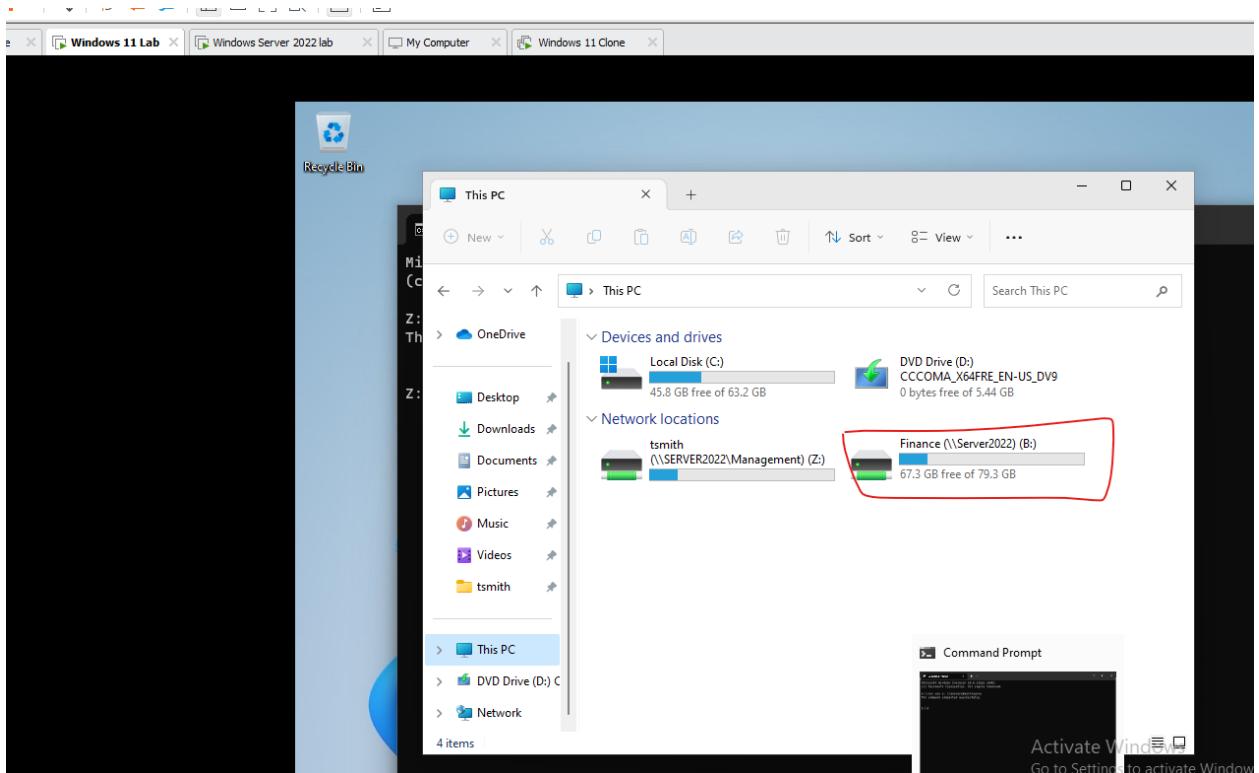


### Third Method to Map a Network Drive

- You can map a network drive via command prompt by typing **net use drive letter: \\servername\sharename**
  - Refer to the screenshot below

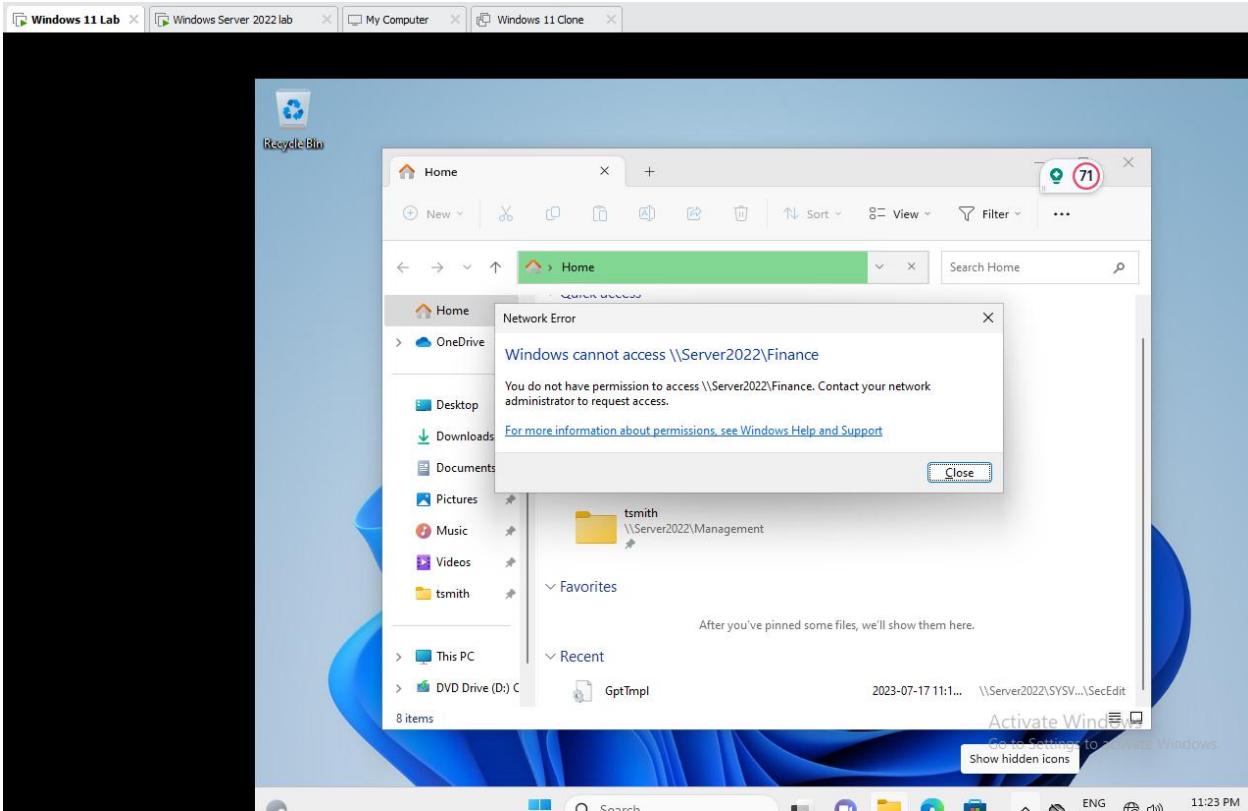


- You should see the network map now

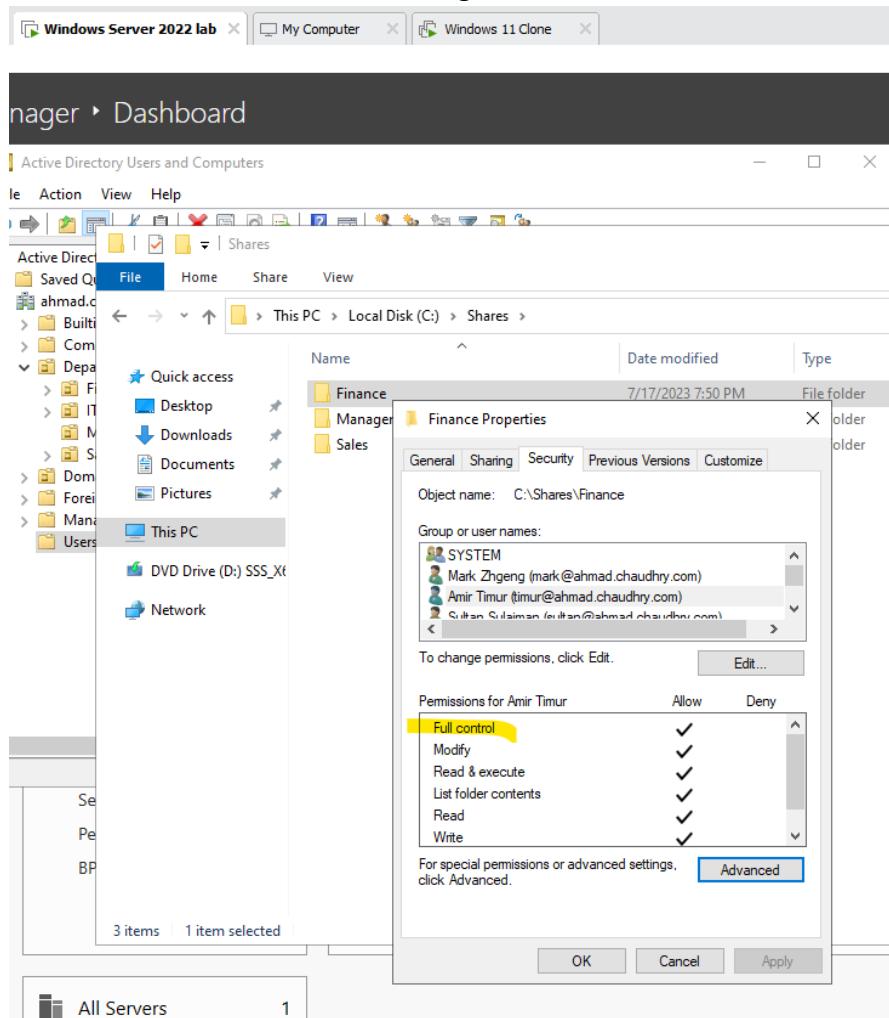


**Verify whether users from one department can access another department's resources, then assign permissions as needed**

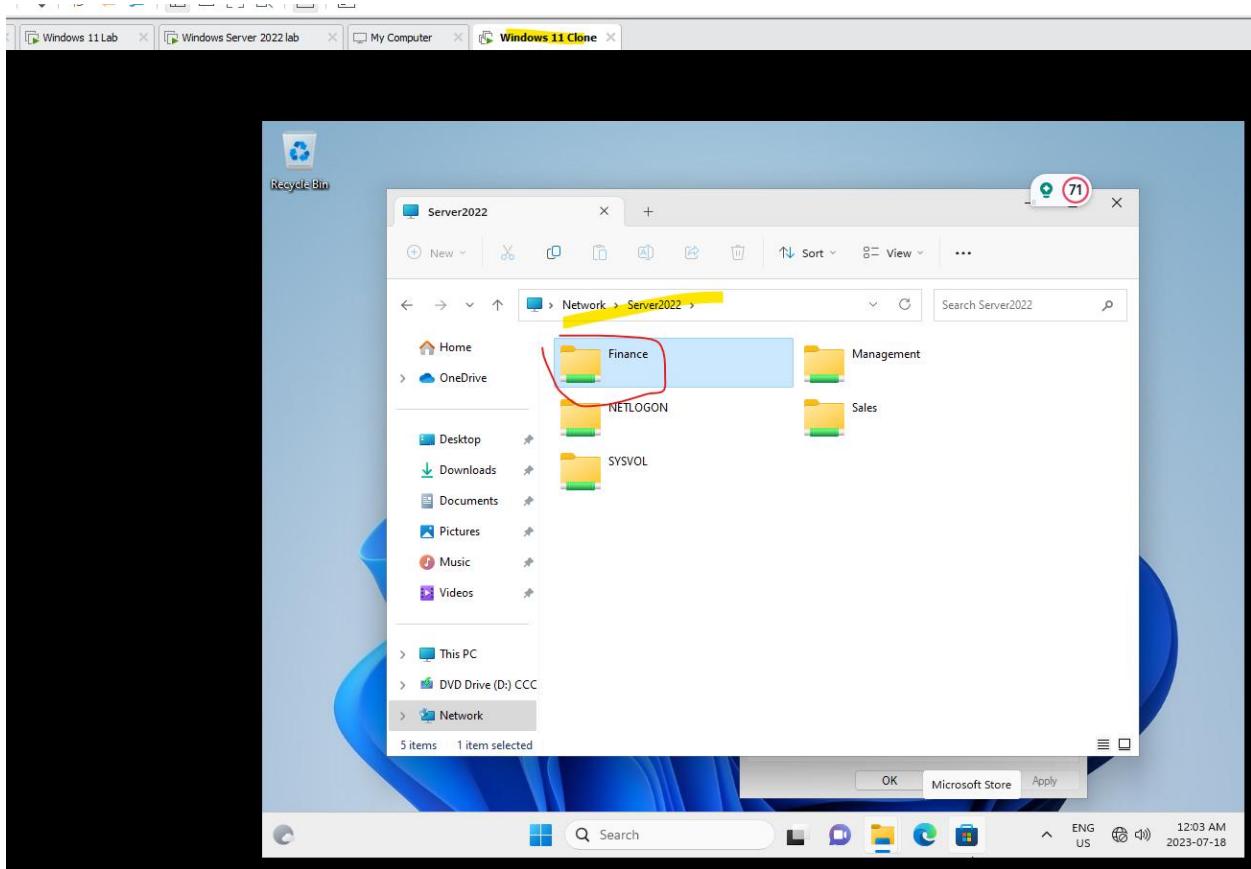
- I log in as Tom from Management to see if I can access Finance, which I could not



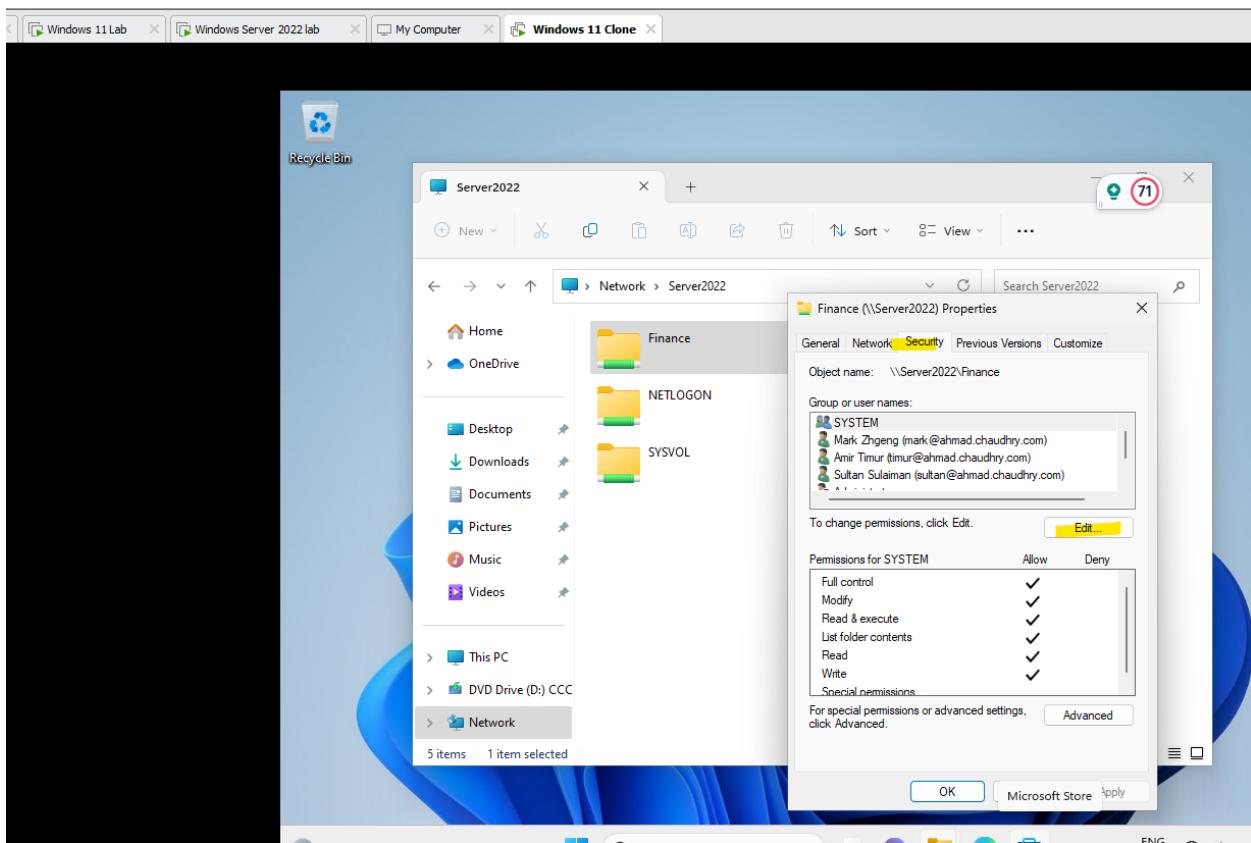
- Ensure that **Timur** has **Full Control** for the **Finance** shared folder on Windows Server 2022. I hadn't set this earlier during the lab, so I had to edit it



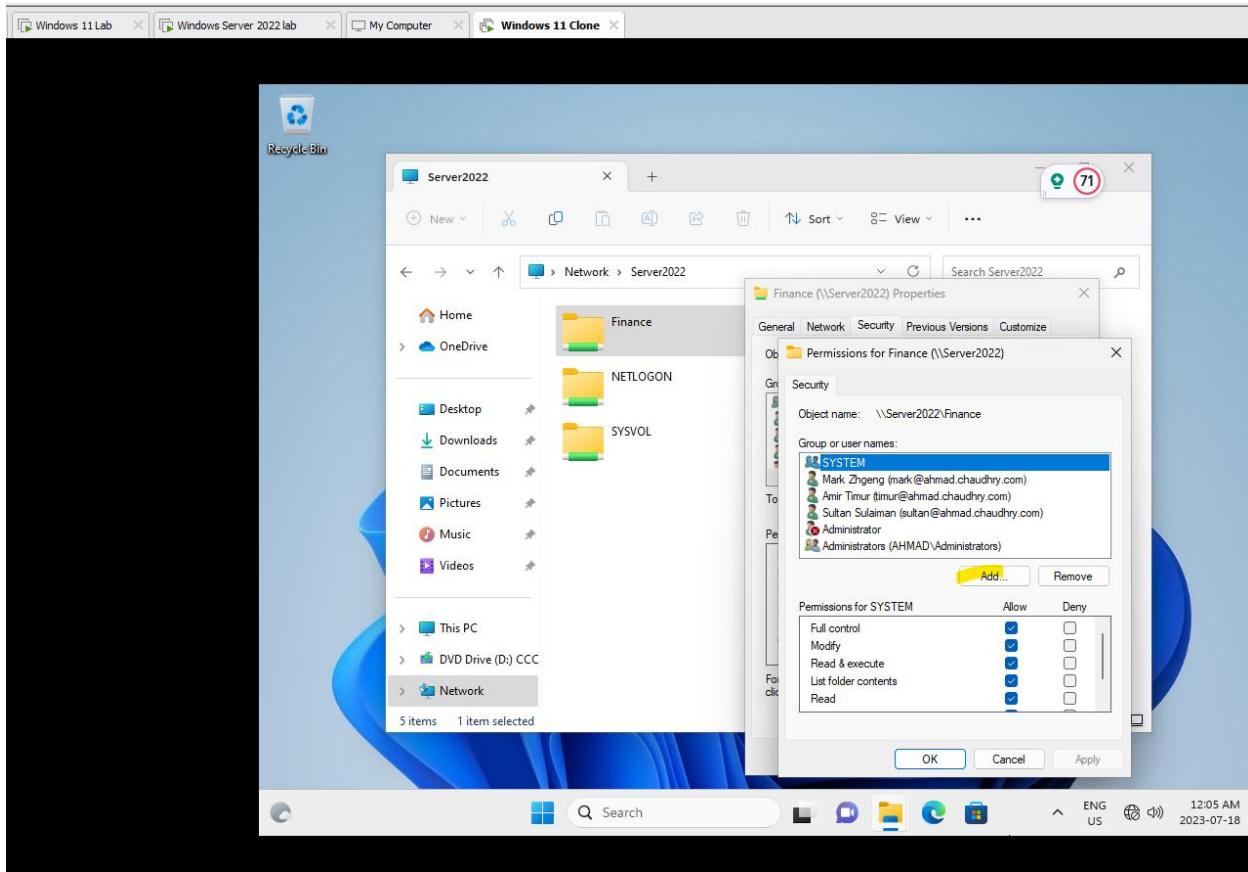
- I log in as Amir Timur (I.T person) and enter the finance shared folder file path



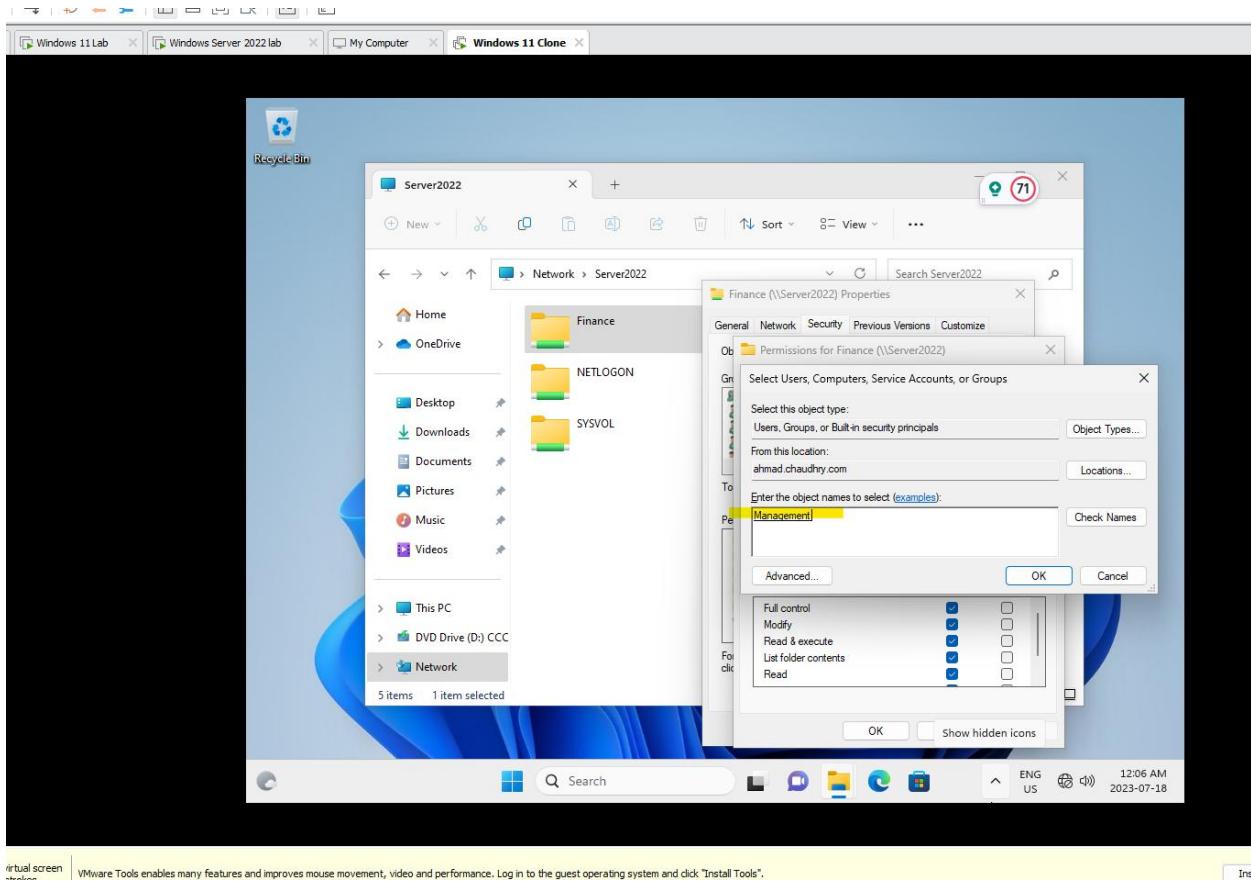
- Right click **finance** folder->Select **properties**->go to **security** tab->select **edit**



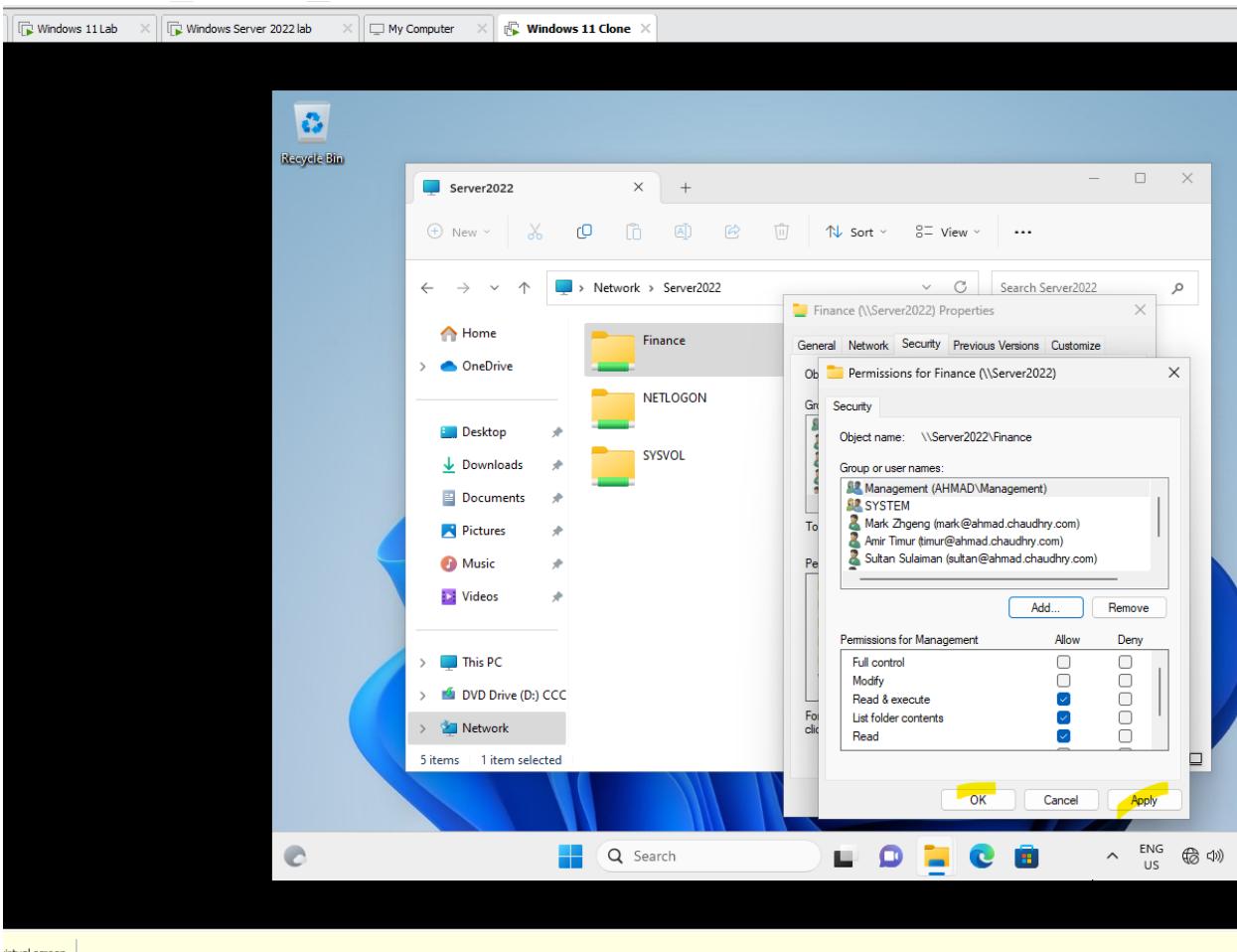
- Select add



- I entered the management security group (you can also add a user instead of a security group)



- Click apply and ok



- Now, log in as Tom Smith and paste the network path for Finance and it should work

