

Identity and Access Management Lab: Active Directory, DNS, and Least Privilege File Sharing

Jemmy Roque

Summary

In this tutorial, I used VirtualBox to create a functional Windows domain lab. I set up a Windows Server virtual machine as the lab.local domain's Domain Controller and used nslookup to confirm DNS resolution. To keep students and help desk users apart, I made an Active Directory structure using Organizational Units, user accounts, and security groups. After that, I set up VirtualBox networking so the Windows 10 client virtual machine could connect to the domain controller and join the client. I used LAB\student1 and LAB\helpdesk1 to verify domain logins after the client joined.

I set up share permissions, applied NTFS permissions using the relevant security groups, and created shared folders on the server to show file services and access control. I verified that students could access the Students share while being blocked from the Helpdesk share and that Helpdesk users could access the Helpdesk share by testing access from the Windows 10 client. Identity, DNS, domain join, and file sharing with least privilege access are all covered in this straightforward but realistic enterprise-style Windows Server lab.

Part A: Prep the server

Step 1: Rename the server

Open Server Manager

Click Local Server

Click the computer name

Click Change

Set: Computer name: DC1

Restart when prompted

The screenshot shows the Server Manager interface for a local server named 'DC1'. The left sidebar has 'Local Server' selected. The main area displays the 'PROPERTIES' for the server, including the computer name 'DC1' and workgroup 'WORKGROUP'. The 'EVENTS' section shows a single warning event from the Microsoft-Windows-AppModel-State log.

Step 2: Set a static IP address

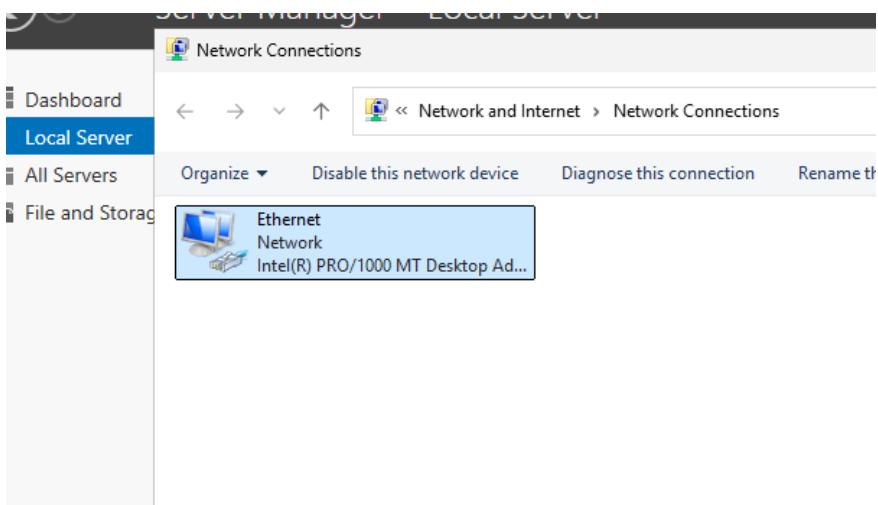
Server Manager → Local Server

Click the Ethernet link

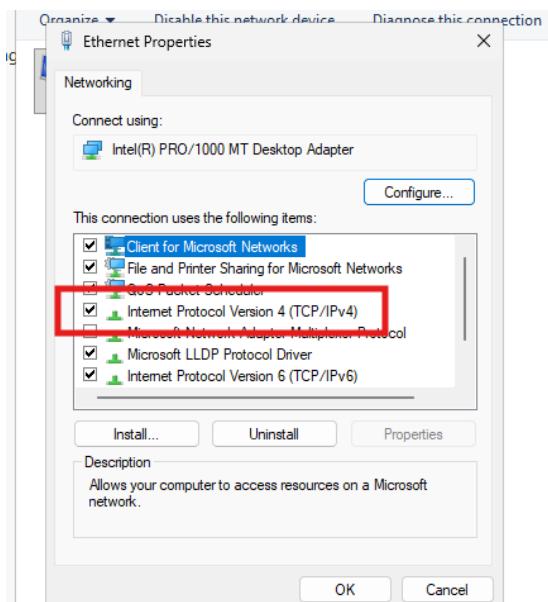
The screenshot shows the Server Manager interface for a local server named 'DC1'. The left sidebar has 'Local Server' selected. The main area displays the 'PROPERTIES' for the server, including the computer name 'DC1' and workgroup 'WORKGROUP'. The 'Network adapter' section shows the 'Ethernet' adapter with the note 'IPv4 address assigned by DHCP, IPv6 enabled'. The 'EVENTS' section shows a single warning event from the Microsoft-Windows-AppModel-State log.

Click Change adapter options

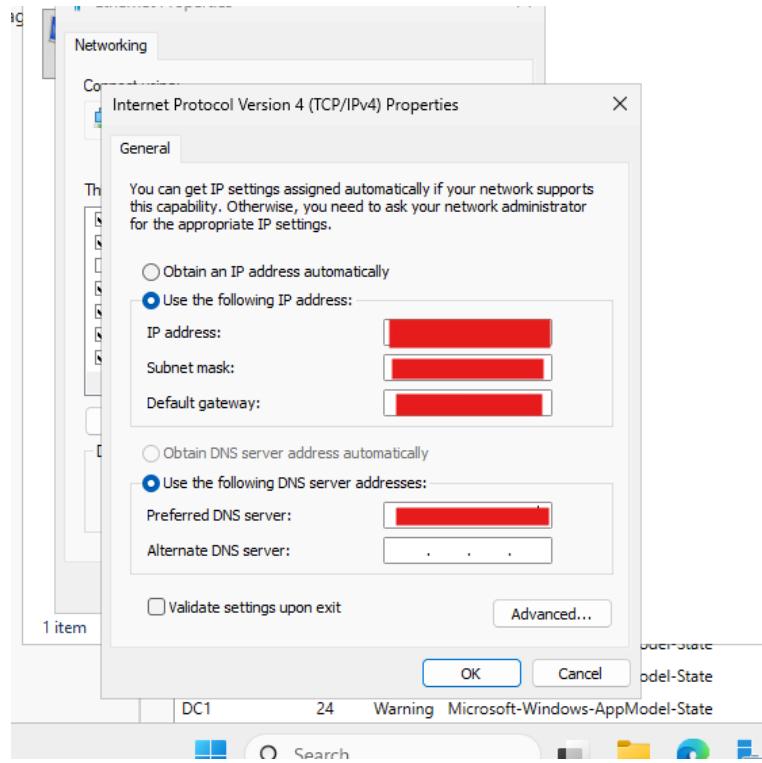
Right click your **Ethernet adapter** → **Properties**



Double click Internet Protocol Version 4 (TCP/IPv4)



Select Use the following IP address



Example values you can use if your VM is on a typical home NAT network:

IP address: 192.168.1.50

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

Preferred DNS server: 192.168.1.50 (this server will become DNS)

Alternate DNS server: leave blank for now

Click **OK** → **Close**

Double check if it's working by using ipconfig /all

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

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

PS C:\WINDOWS\system32> ipconfig /all

Windows IP Configuration

    Host Name . . . . .
    Primary Dns Suffix . . .
    Node Type . . . . .
    IP Routing Enabled. . . .
    WINS Proxy Enabled. . . .
    DNS Suffix Search List. . . .

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . .
    Description . . . . .
    Physical Address. . . . .
    DHCP Enabled. . . . .
    Autoconfiguration Enabled . .
    IPv6 Address. . . . .
    Link-local IPv6 Address . .
    IPv4 Address. . . . .
    Subnet Mask . . . . .
    Lease Obtained. . . . .
    Lease Expires . . . . :
```

For a quick test if its working

Open **Command Prompt** Run these commands:

Ipconfig /all

Ping 10.0.2.2

Ping 8.8.8.8

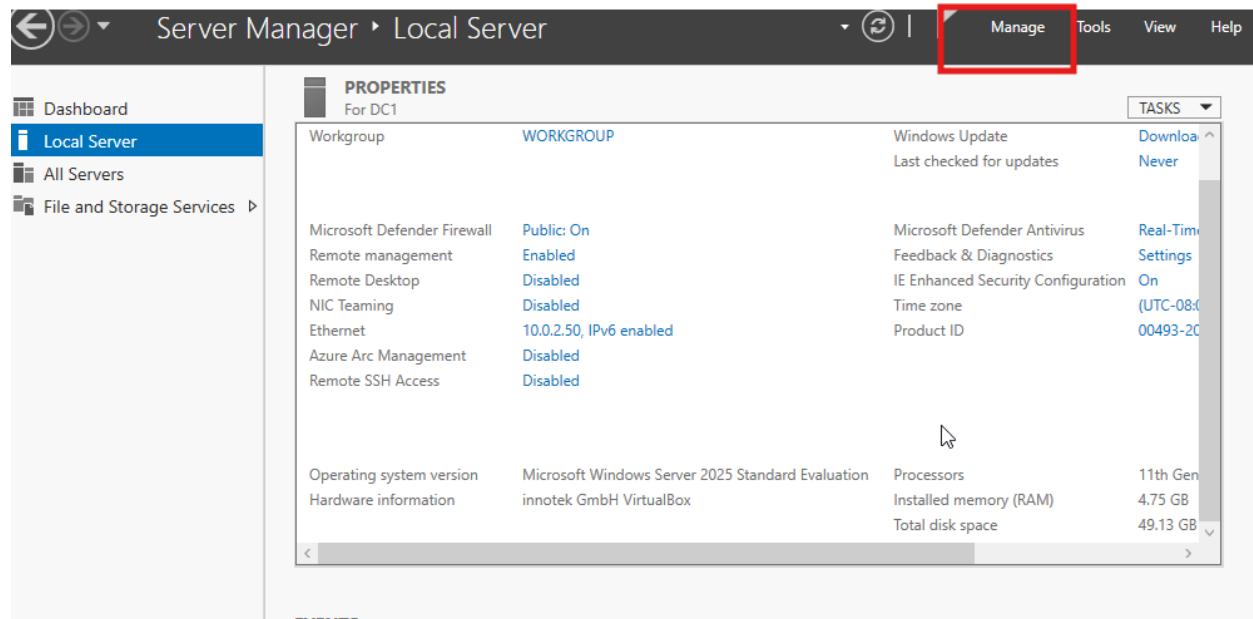
```
PS C:\WINDOWS\system32> ping 10.0.2.2

Pinging 10.0.2.2 with 32 bytes of data:
Reply from 10.0.2.2: bytes=32 time<1ms TTL=255
Reply from 10.0.2.2: bytes=32 time=1ms TTL=255
Reply from 10.0.2.2: bytes=32 time=1ms TTL=255
Reply from 10.0.2.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

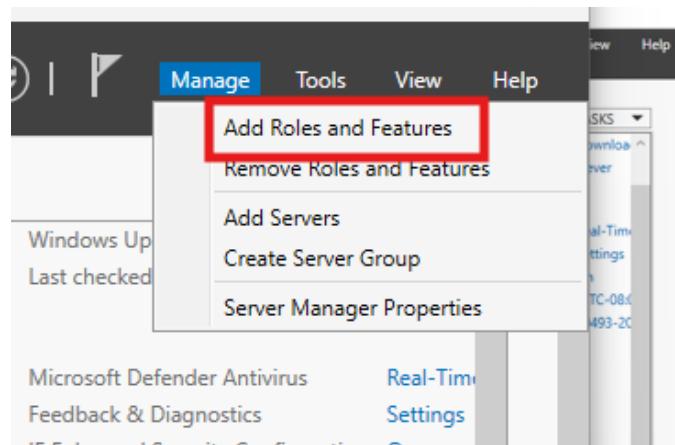
Step 3: Install AD DS and DNS roles

Open **Server Manager** → Click **Manage** (top right)



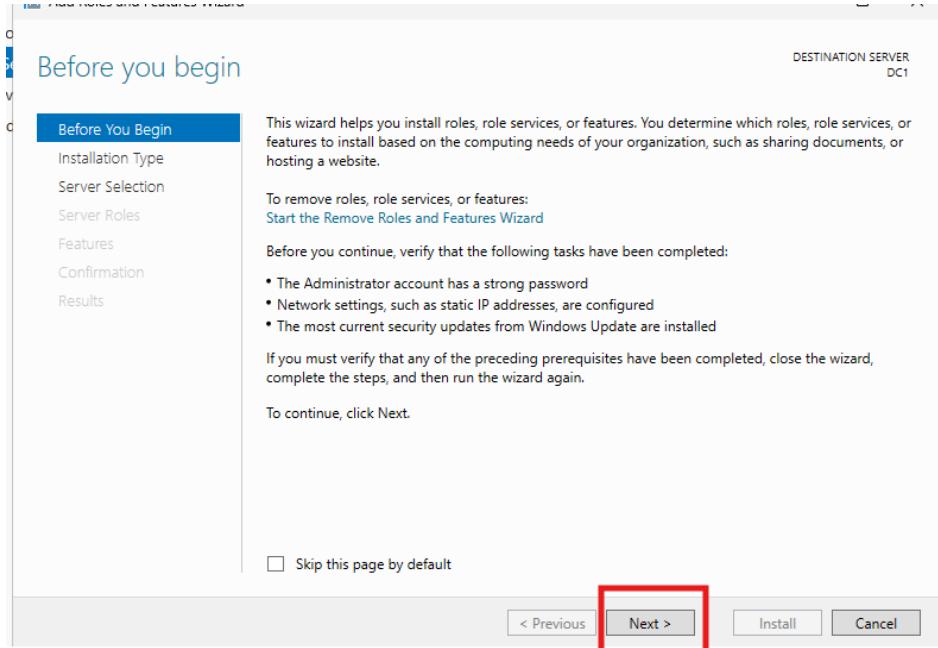
The screenshot shows the Windows Server Manager interface for a local server named 'DC1'. The 'Local Server' tab is selected in the navigation pane. The main area displays the 'PROPERTIES' for the server, including system information like Workgroup (WORKGROUP), operating system version (Windows Server 2025 Standard Evaluation), and hardware details (Processor: 11th Gen, RAM: 4.75 GB, Disk Space: 49.13 GB). The 'Manage' button in the top right corner is highlighted with a red box.

Click **Add Roles and Features**

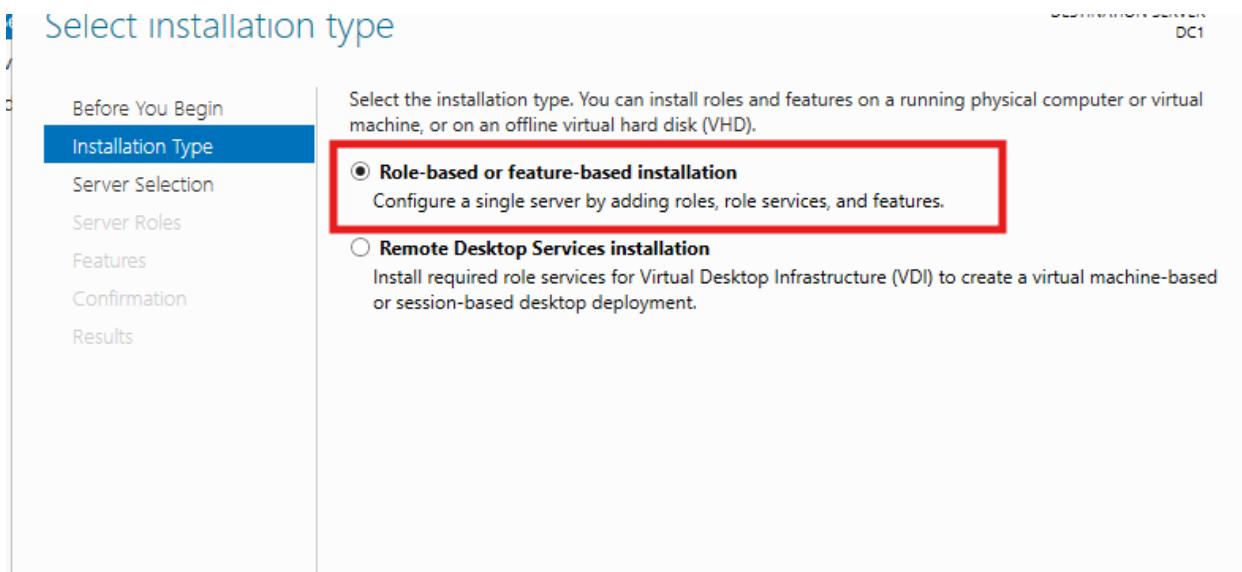


The screenshot shows the 'Manage' ribbon in the Server Manager. The 'Add Roles and Features' option is highlighted with a red box. Other options visible in the ribbon include Tools, View, and Help. Below the ribbon, there are status messages about Windows Update and various system services.

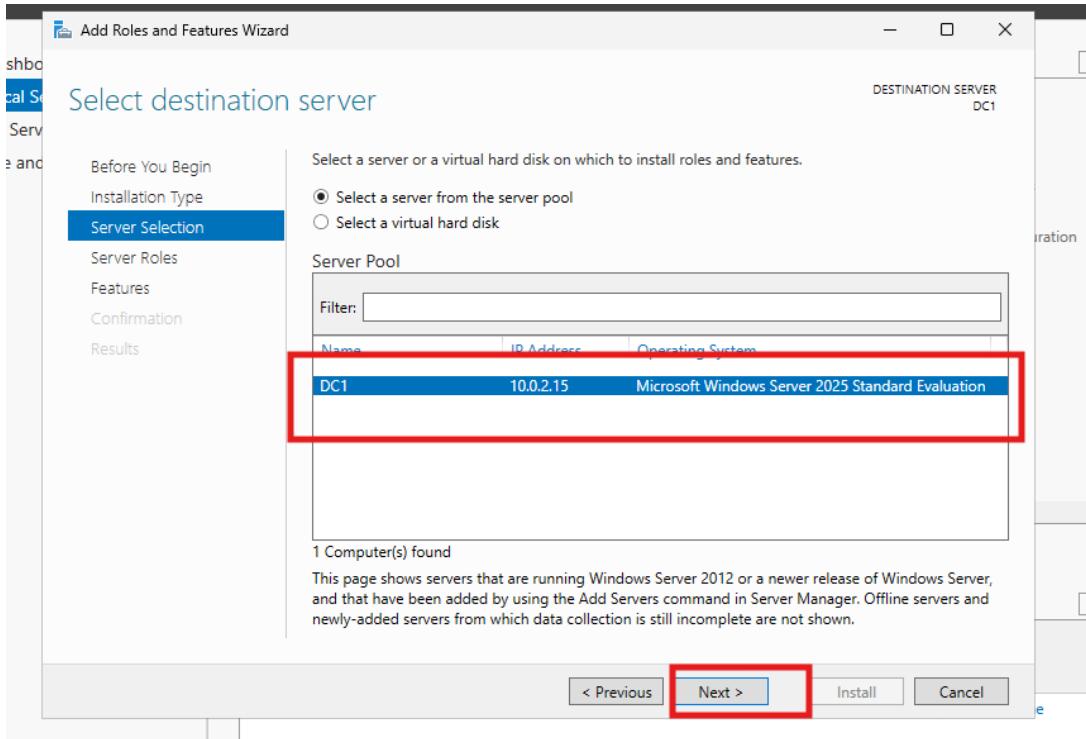
Click Next



Select Role based or feature based installation → Next



Select your server (DC1) → Next

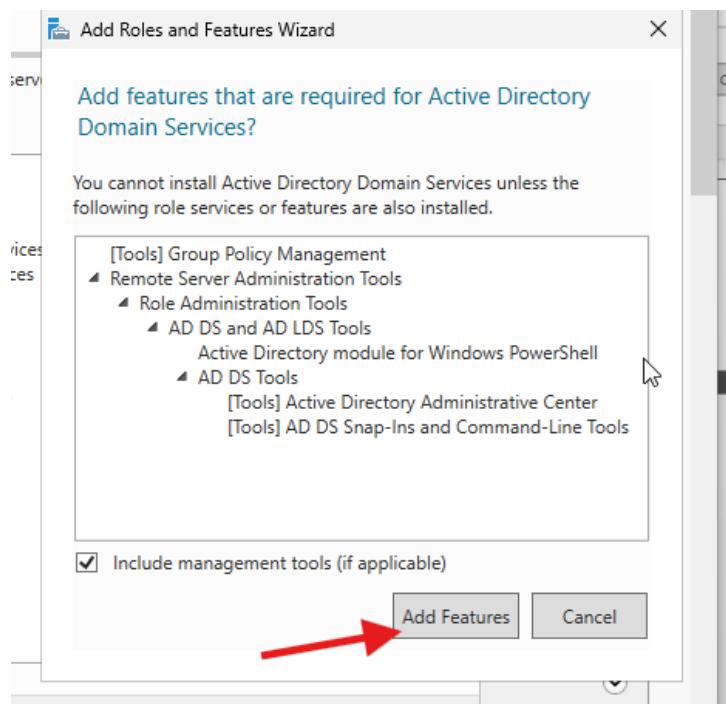


On Server Roles, check:

Active Directory Domain Services

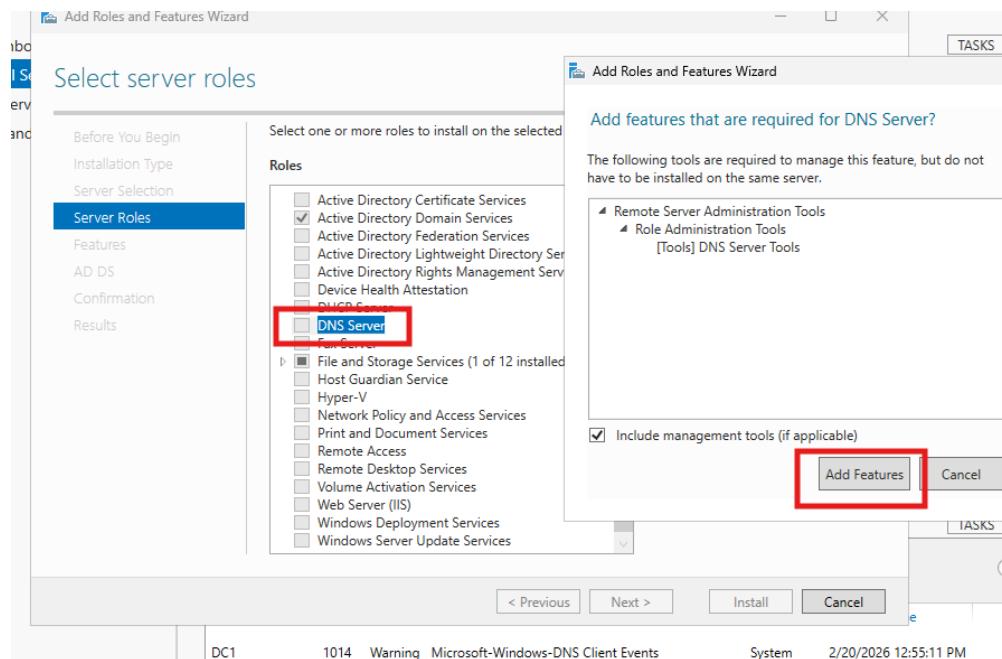
The screenshot shows the 'Select server roles' step of the 'Add Roles and Features Wizard'. The 'Server Roles' tab is active. 'Active Directory Domain Services' is checked and highlighted with a red box. The 'Add Features' button is visible at the bottom right.

When it prompts, click **Add Features**

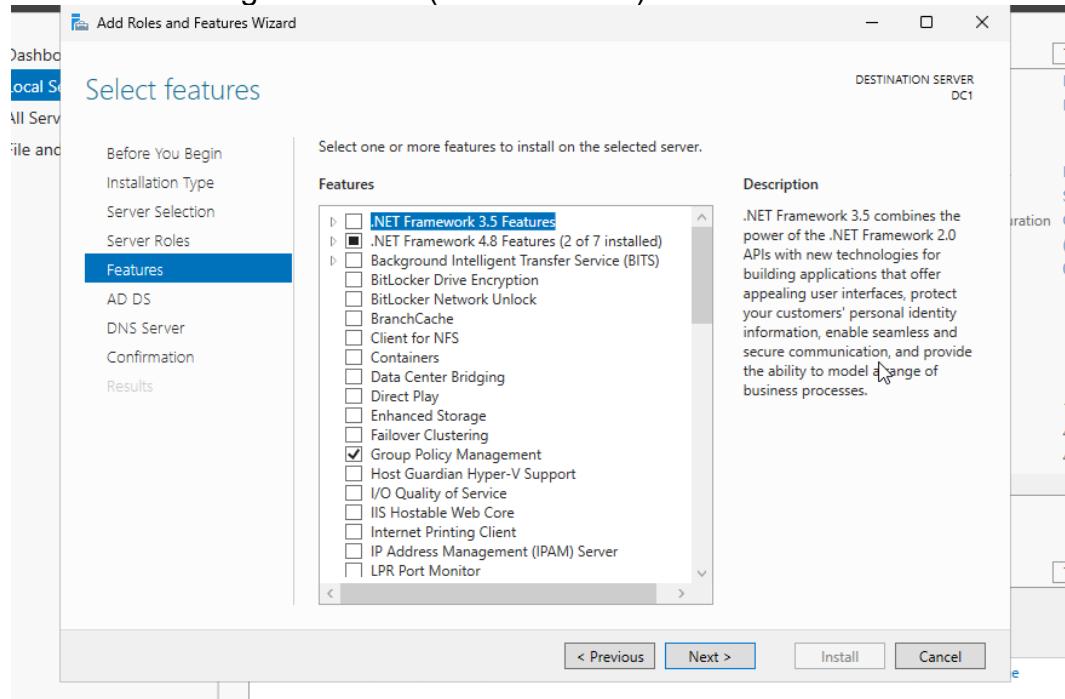


DNS Server

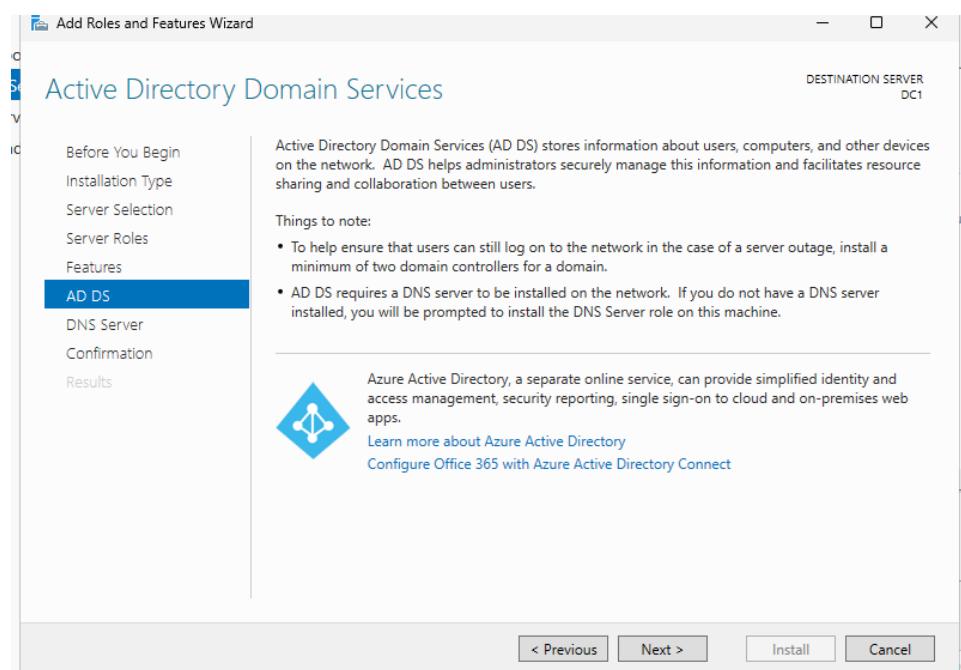
Click **Add Features** if prompted



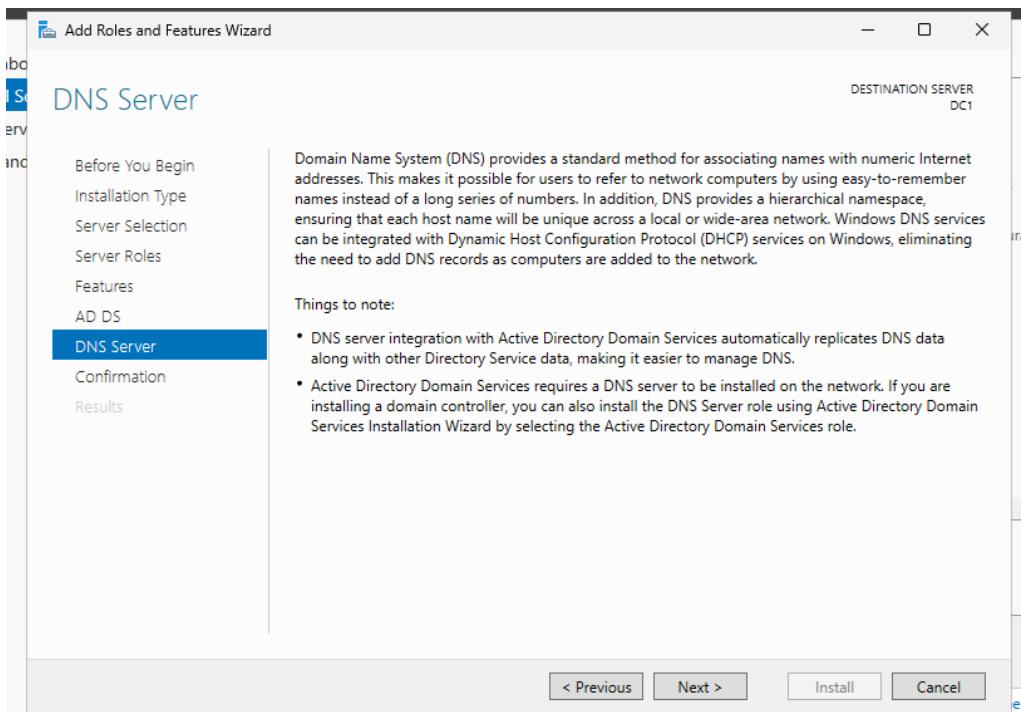
Click **Next** through **Features** (leave defaults)



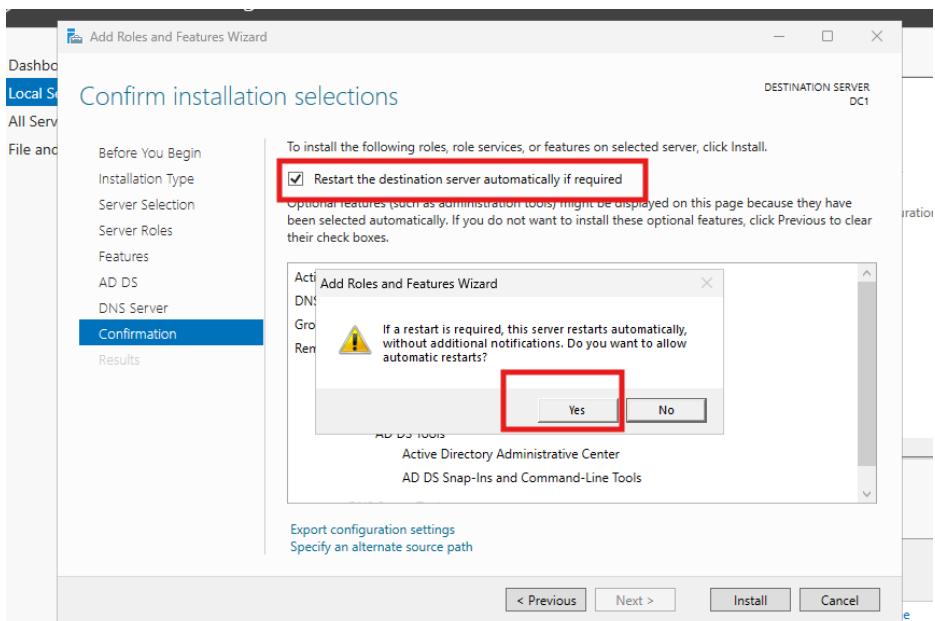
Click **Next** on the **AD DS** page



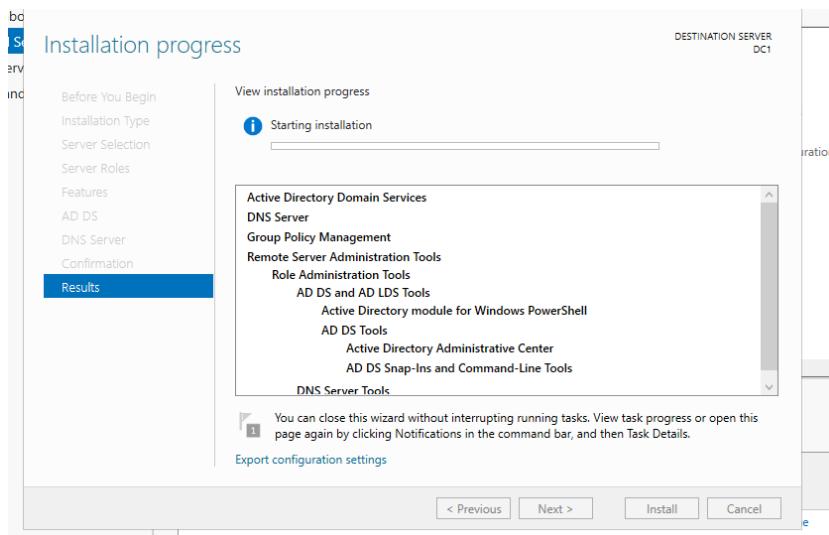
Click **Next** on the DNS page



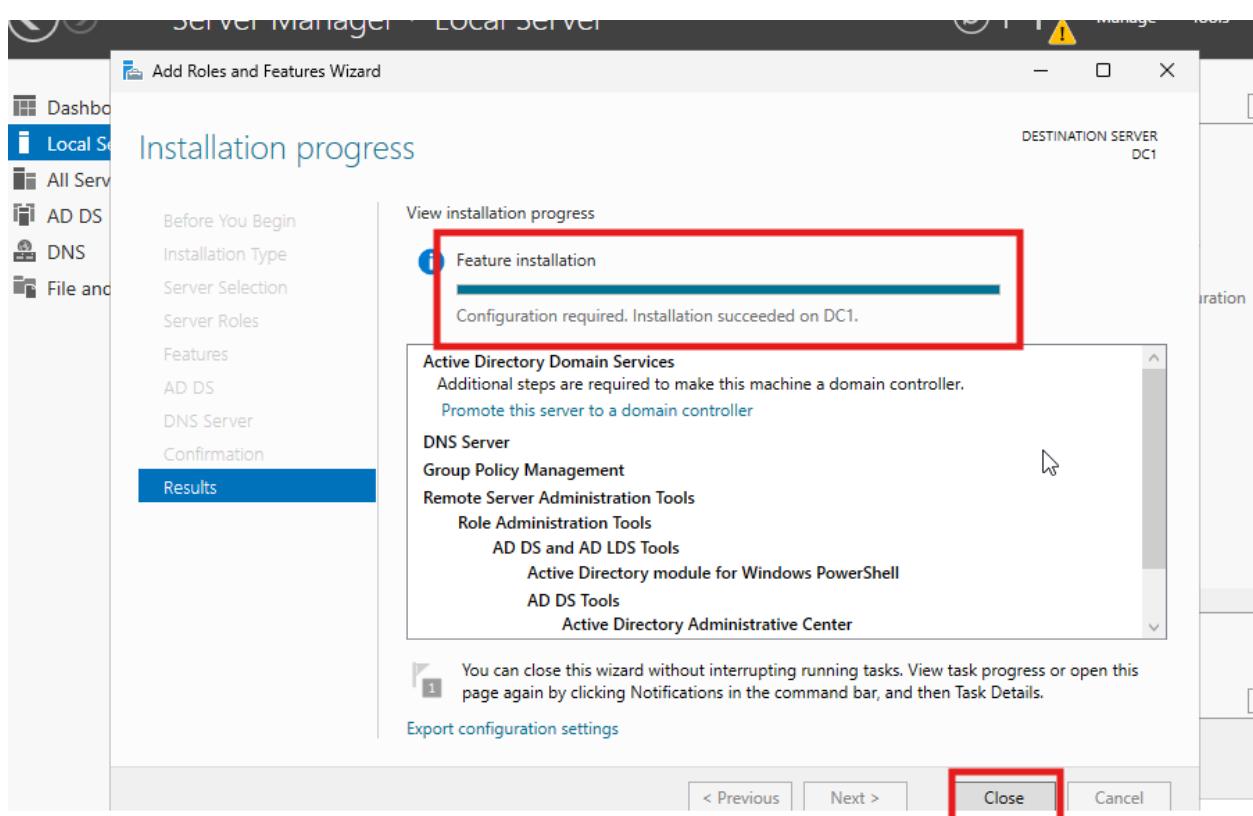
On Confirmation, check **Restart the destination server automatically if required**



Click **Install**

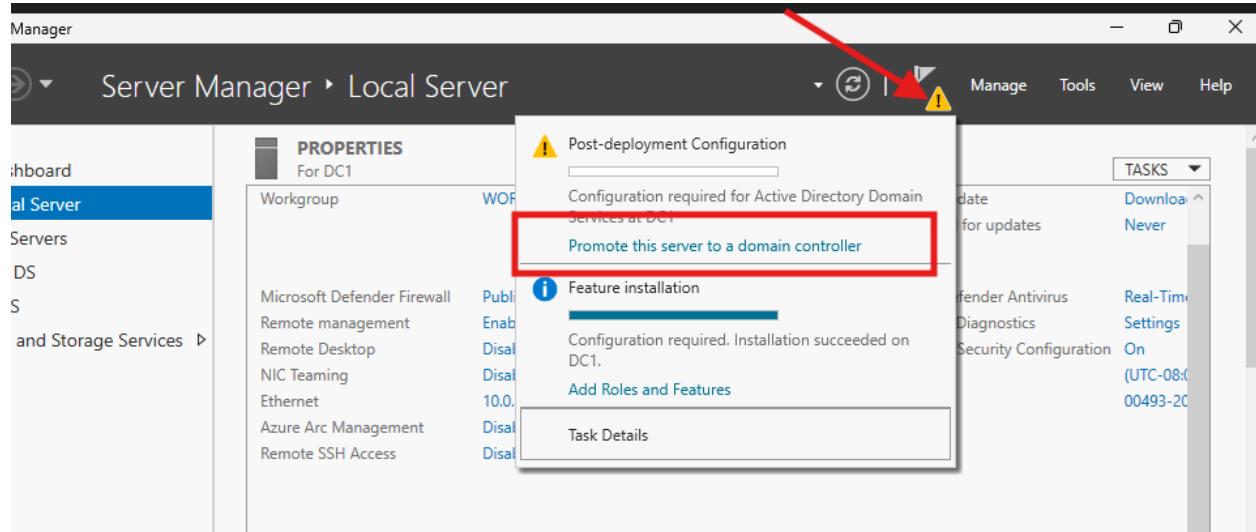


Confirmation Installation successfully showing and press **Close**.



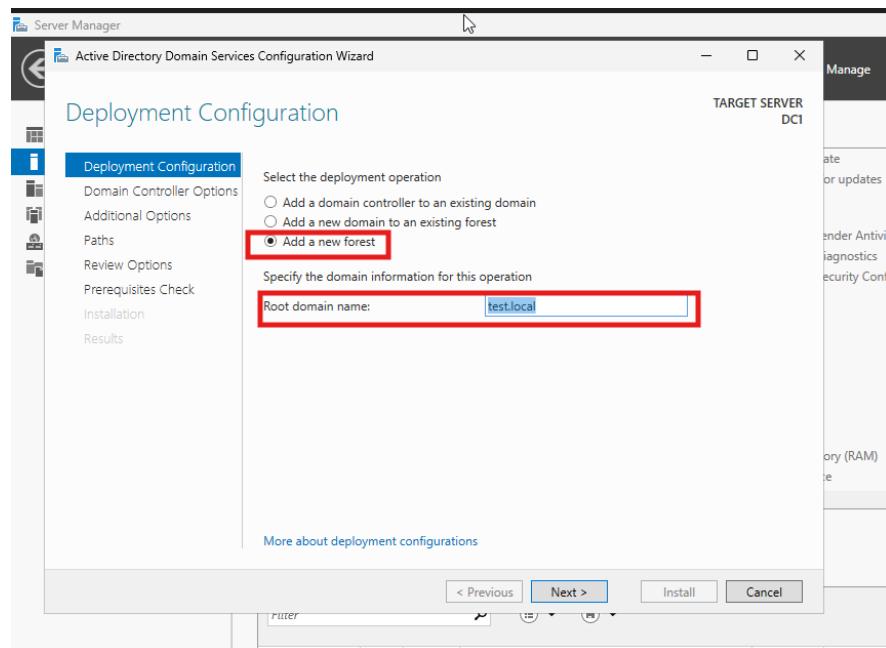
Step 4: Promote to Domain Controller

Click the blue link: Promote this server to a domain controller



Choose: Add a new forest

Root domain name: lab.local

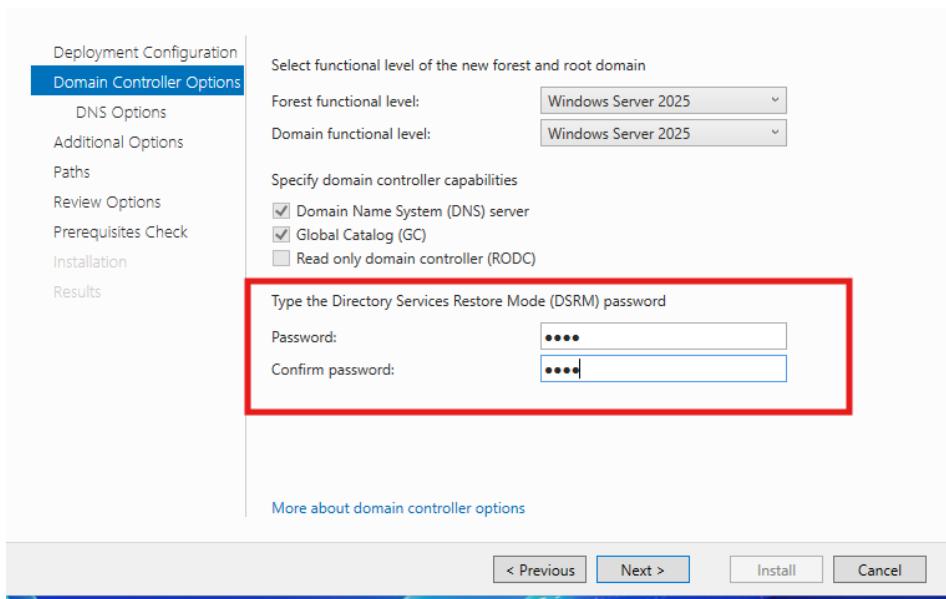


Click Next

On Domain Controller Options:

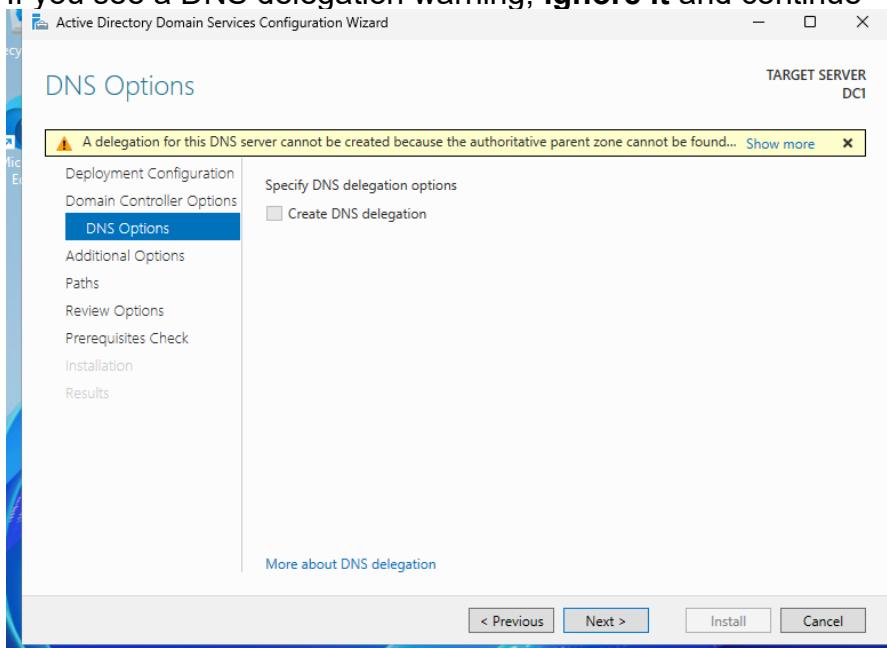
Leave defaults checked (DNS and GC should be checked)

Set the DSRM password (write it down)

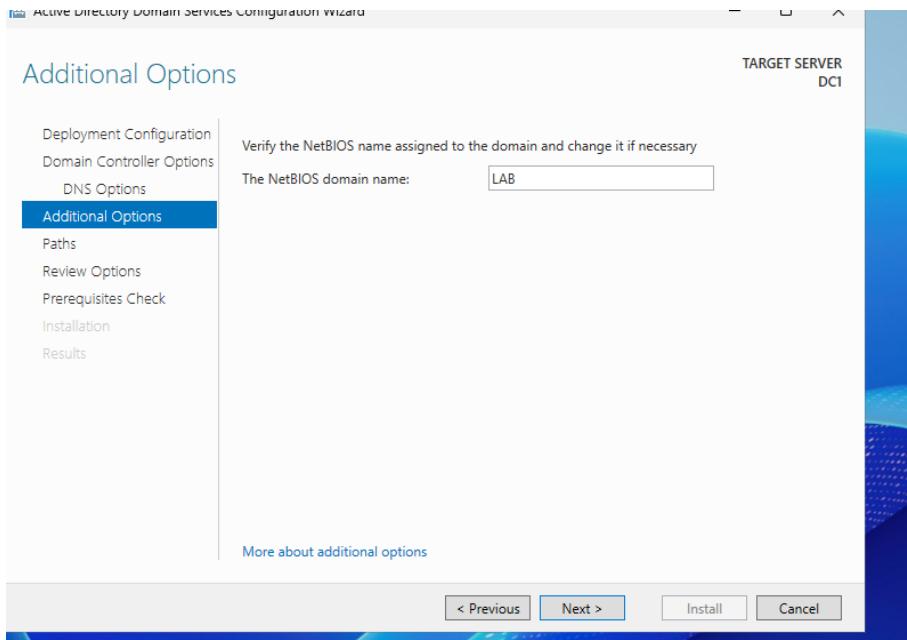


Click Next through the rest

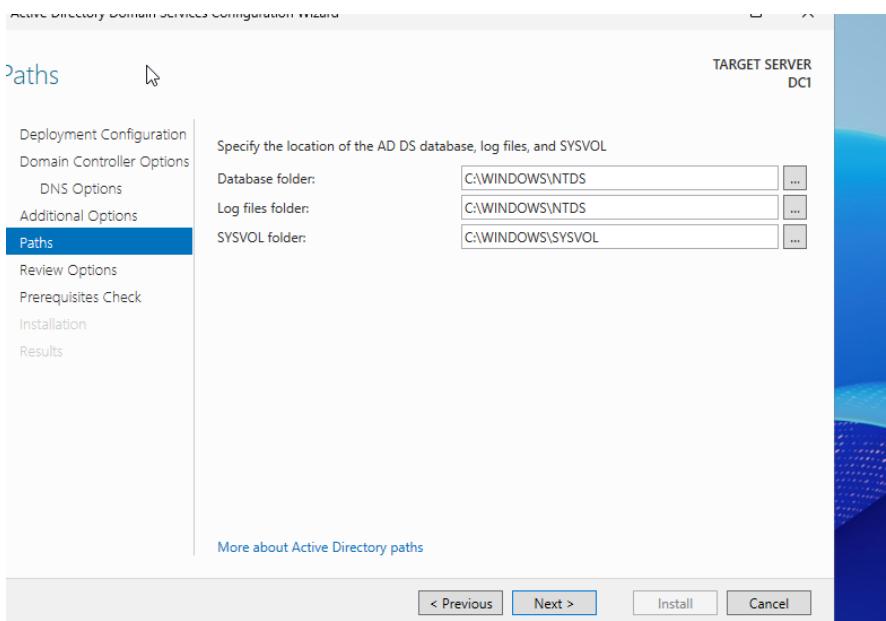
If you see a DNS delegation warning, ignore it and continue



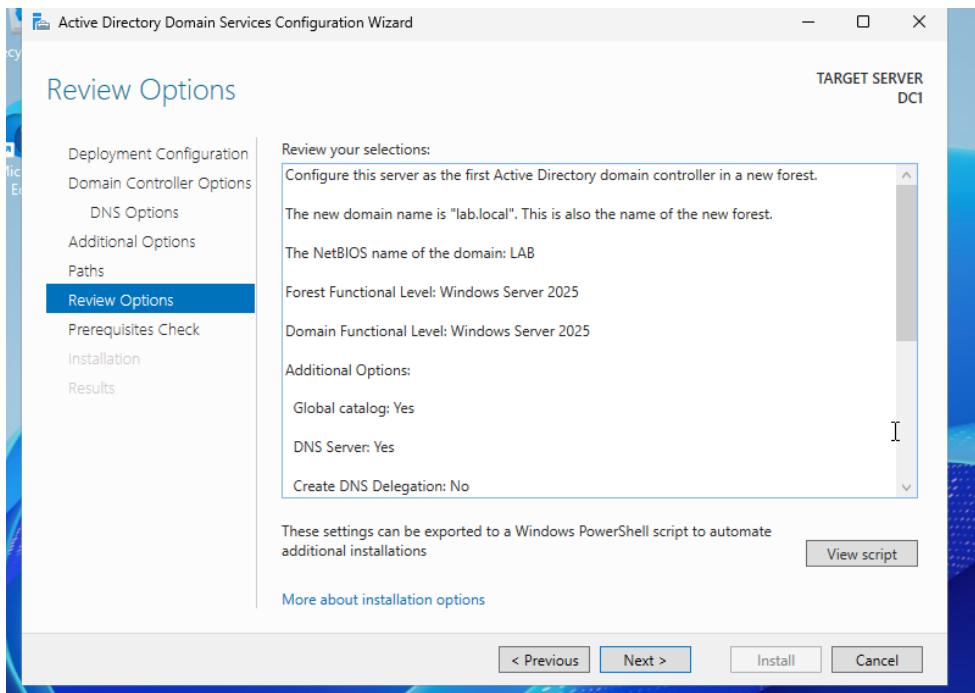
Additional Options it will be Auto fill as LAB, click Next.



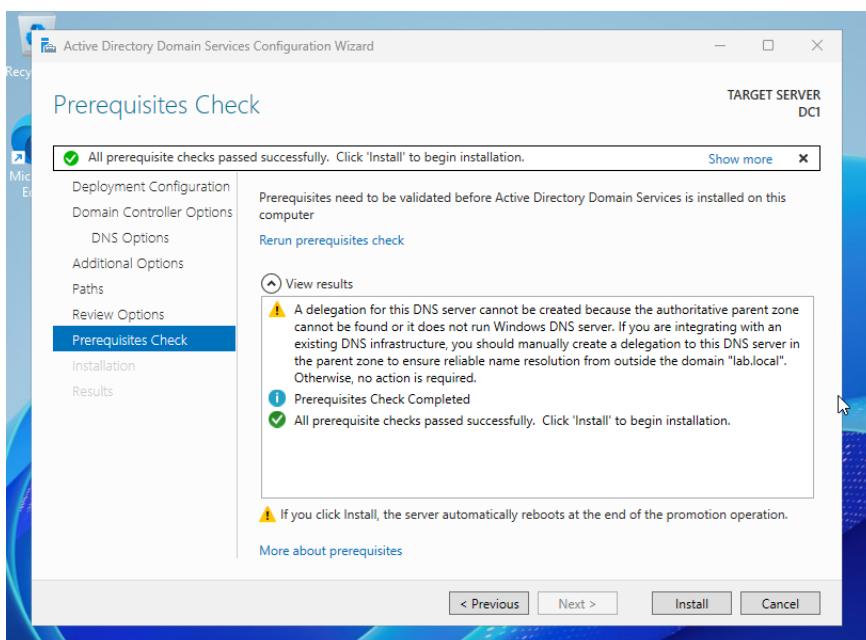
Path Leave defaults, Click Next.



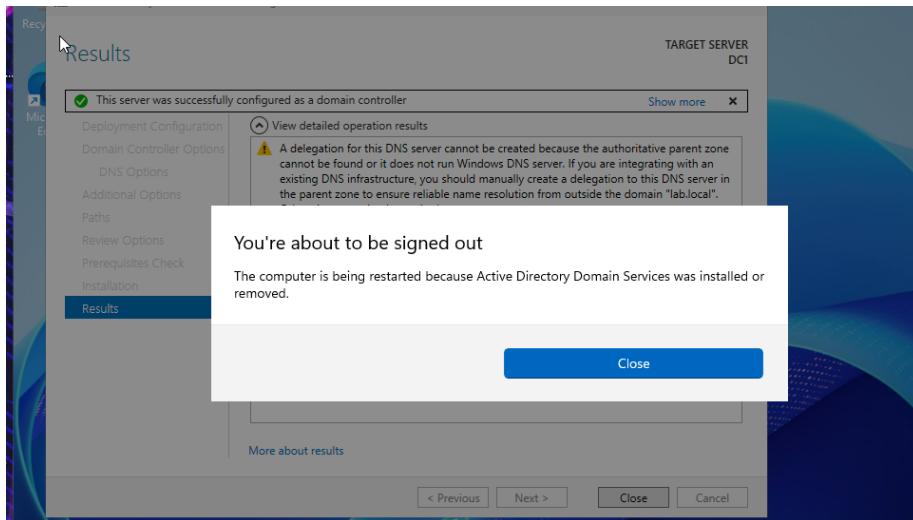
Review Options Click Next.



Click Install



It will restart automatically



Important DNS note for internet

Before you click Install, make sure your NIC DNS is set to:

Preferred DNS: 8.8.8.8 (temporary, so you can still resolve names during setup)

After the server reboots and you log in as the domain admin, change DNS back to:

Preferred DNS: 10.0.2.50

Alternate DNS: blank

Soon as it finishes, it will reboot on its own. After the reboot, check these 3 things in order.

Open Command prompt as Administrator.

Ipconfig

nslookup lab.local

nslookup dc1.lab.local

```
C:\Windows\System32>nslookup lab.local
Server: UnKnown
Address: ::1

Name: [REDACTED].local
Address: [REDACTED]

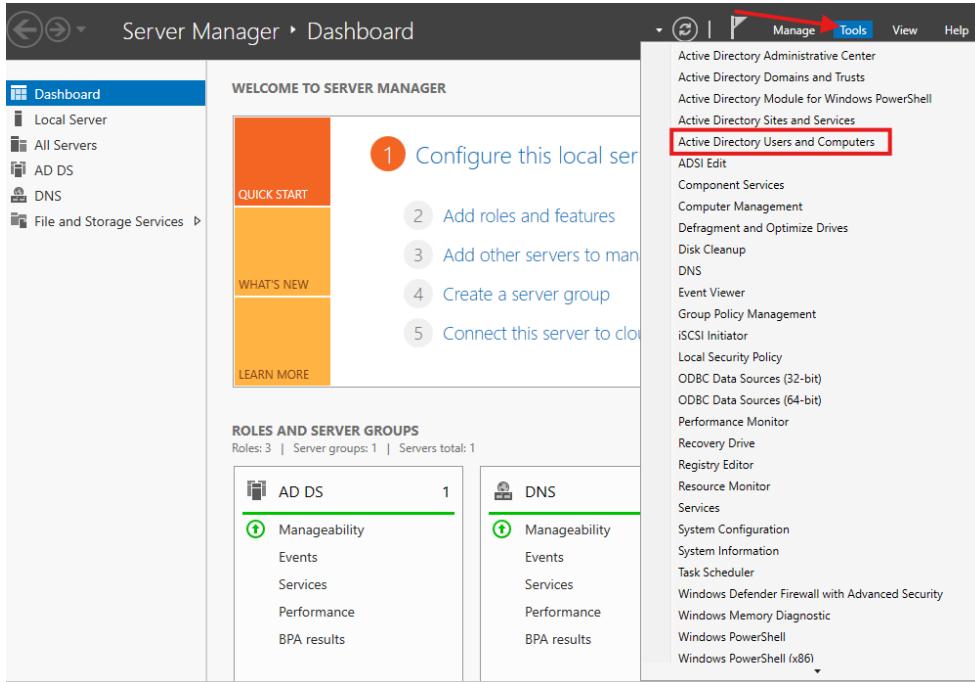
C:\Windows\System32>nslookup dc1.lab.local
Server: UnKnown
Address: ::1

Name: [REDACTED].local
Address: [REDACTED]
```

Step 5: Create OUs, users, and groups in AD

A) Server Manager Tools (top right) → Open the Tool

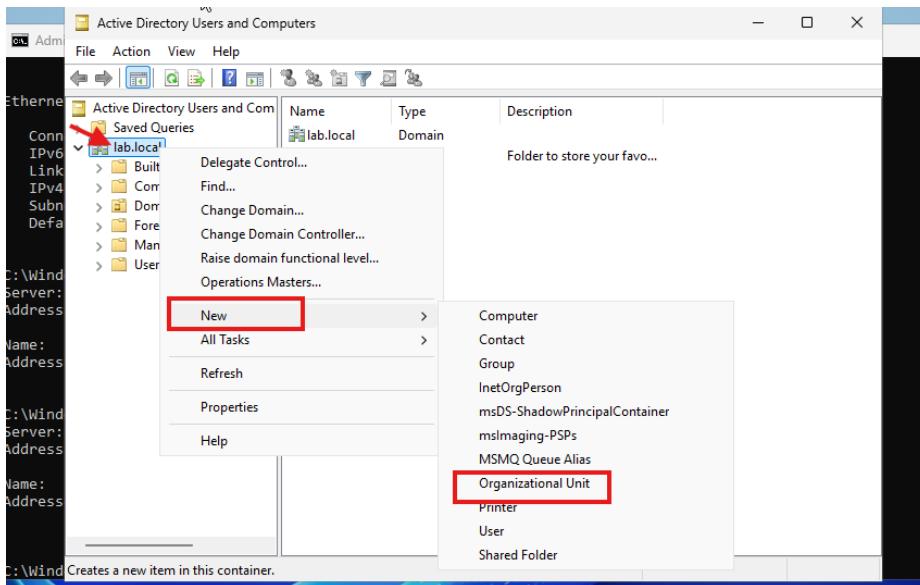
Click Active Directory Users and Computers



B) Create Organizational Units (OUs)

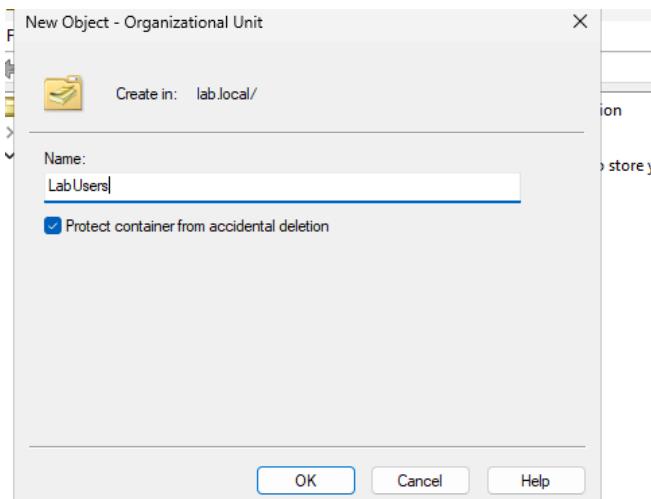
In the left pane, expand lab.local

Right click lab.local → New → Organizational Unit



Create these OUs (one by one):

LabUsers



LabComputers

LabGroups

Active Directory Users and Computers

lab.local

Users

LabUsers

LabComputers

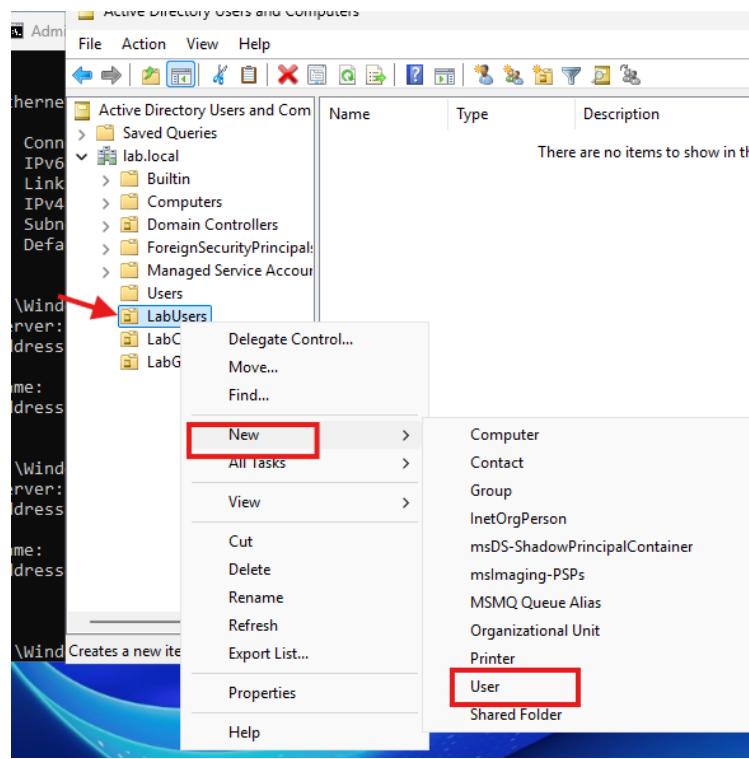
LabGroups

There are no items to show in this view.

ADUC showing all three OUs under lab.local.

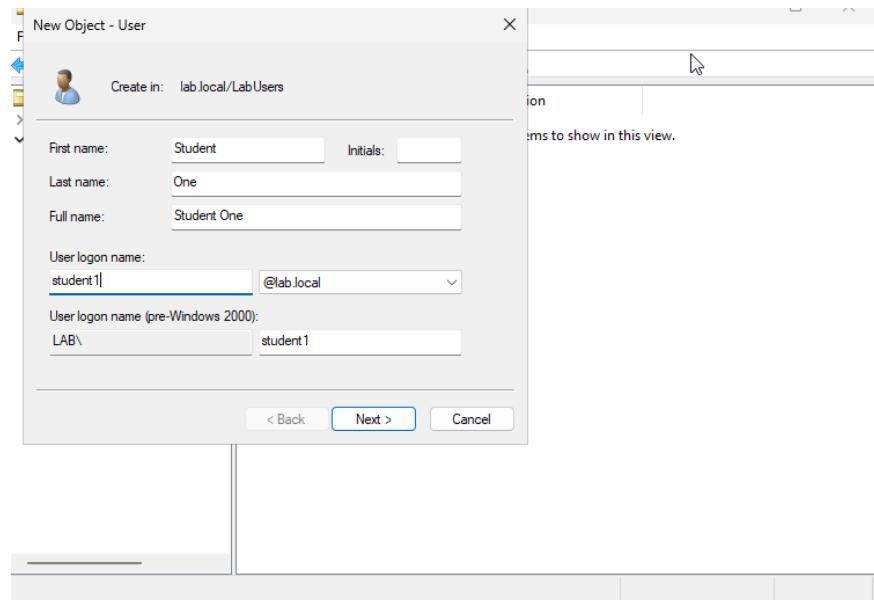
C) Create users

Click LabUsers Right click inside the blank area → New → User



Create these users:

student1 (Display name: Student One)



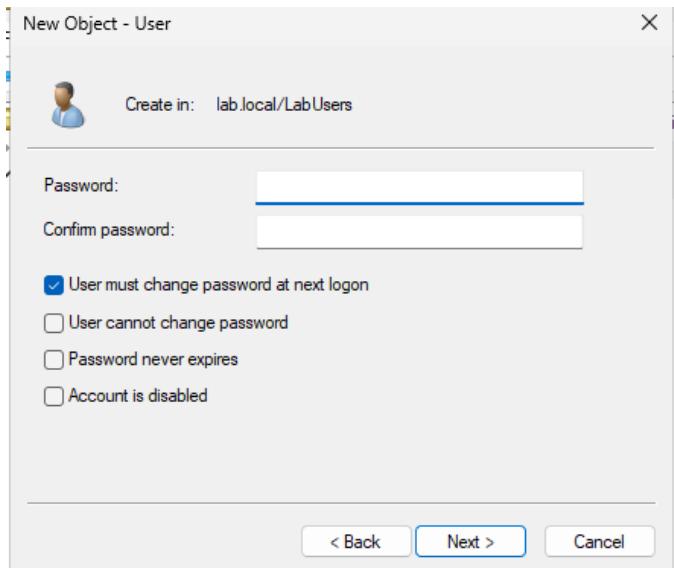
Users must change password at next logon

During the password screen:

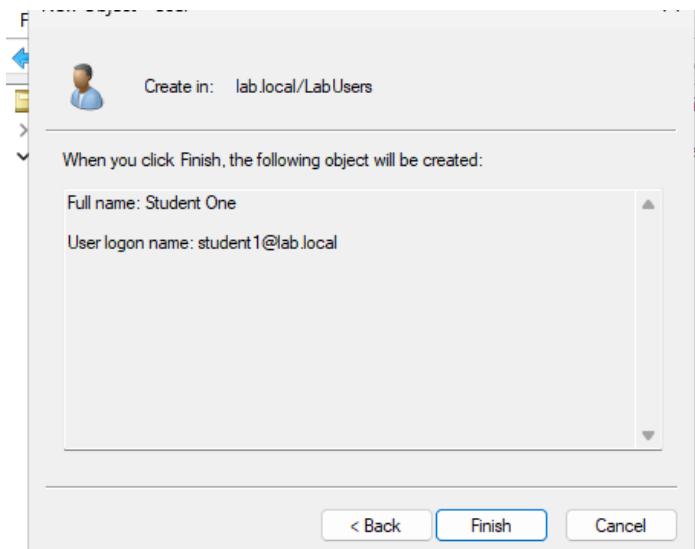
Set a password you will remember

Check Password never expires (lab only)

Users must change password at next logon



Double check your Username and logon name and Click **Finish**.



Repeat the same process with the other User **helpdesk1**

helpdesk1 (Display name: Help Desk One)

The screenshot shows the Active Directory Users and Computers interface. The left pane displays the navigation tree with the 'LabUsers' folder selected under 'lab.local'. The right pane lists two users: 'HelpDesk One' (User) and 'Student One' (User). The 'HelpDesk One' row is highlighted.

LabUsers OU showing the two users.

D) Create security groups

Click LabGroups Right click → New → Group

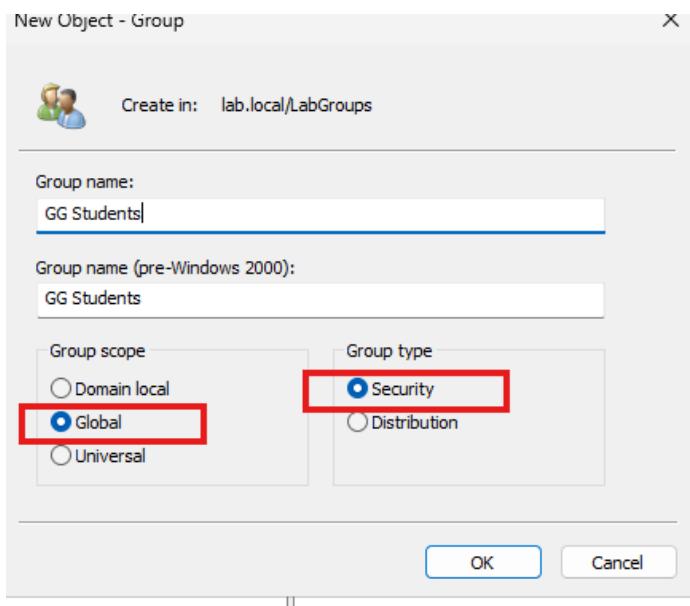
Create:

The screenshot shows the Active Directory Users and Computers interface. The left pane displays the navigation tree with the 'LabGroups' folder selected under 'lab.local'. A red arrow points to the 'LabGroups' folder. A context menu is open over the 'LabGroups' folder, with the 'New' option highlighted. A secondary context menu is displayed, also with the 'Group' option highlighted. The message 'There are no items to show in this view.' is visible in the center of the right pane.

Group name: GG Students

Group scope: Global

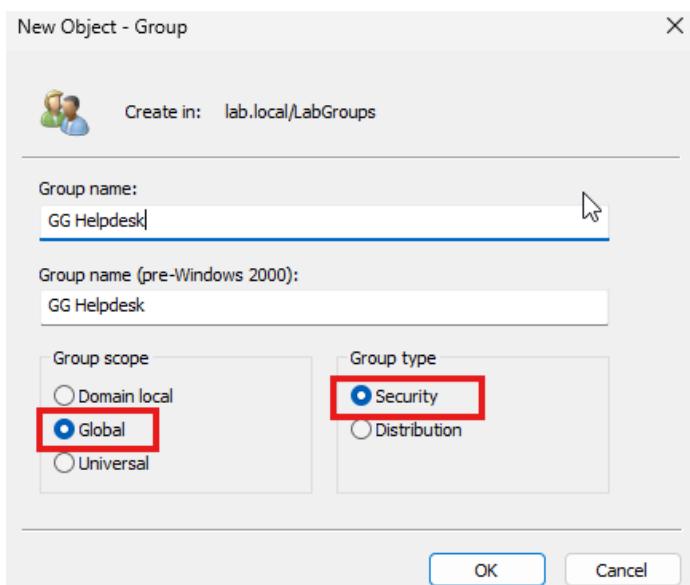
Group type: Security



Group name: GG Helpdesk

Group scope: Global

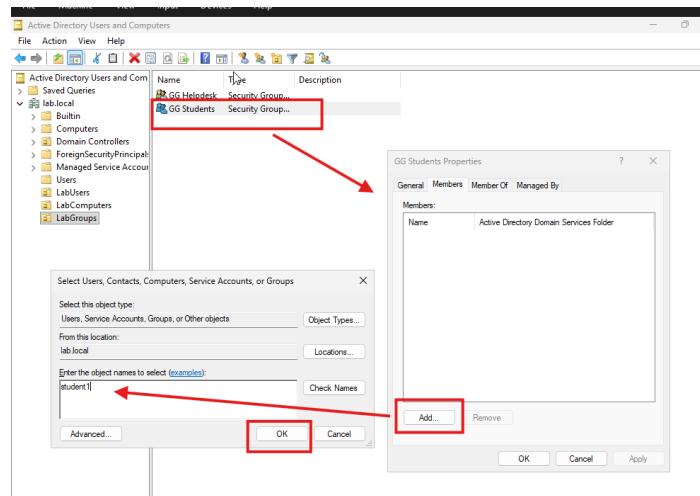
Group type: Security



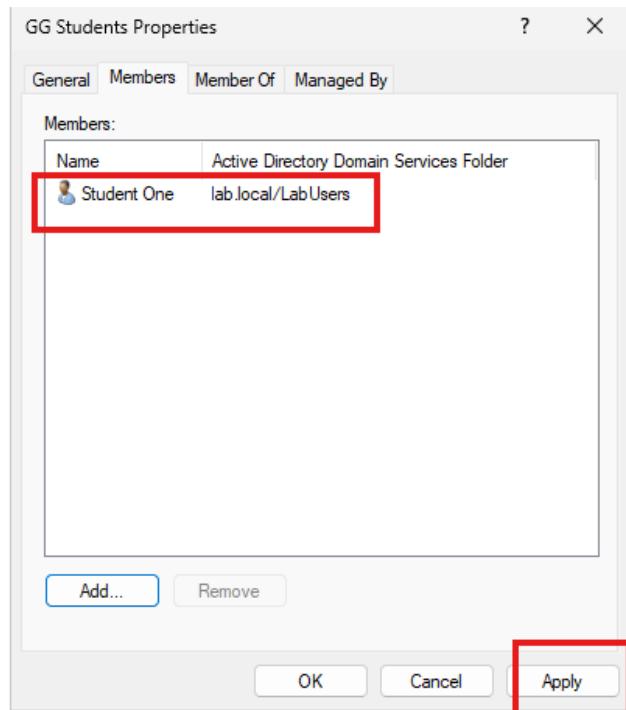
E) Add users to groups

Double click GG Students → Members tab → Add

Add: student1

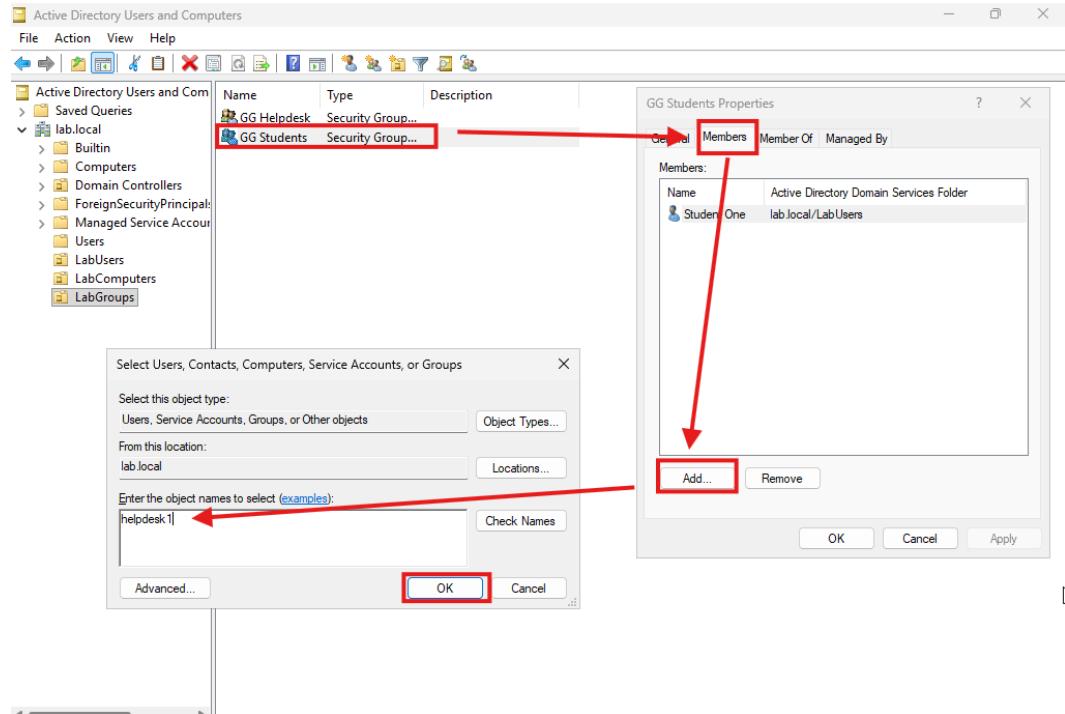


Confirm Student One is added and Click **Apply**.

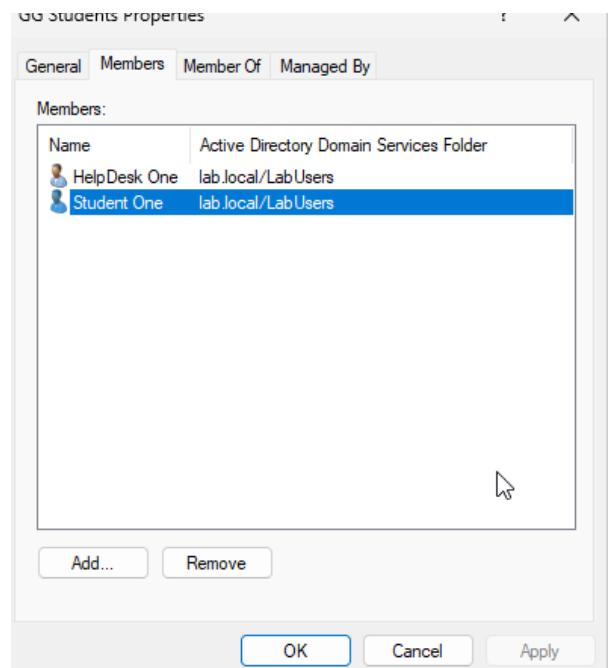


Double click **GG Helpdesk** → **Members tab** → **Add**

Add: helpdesk1



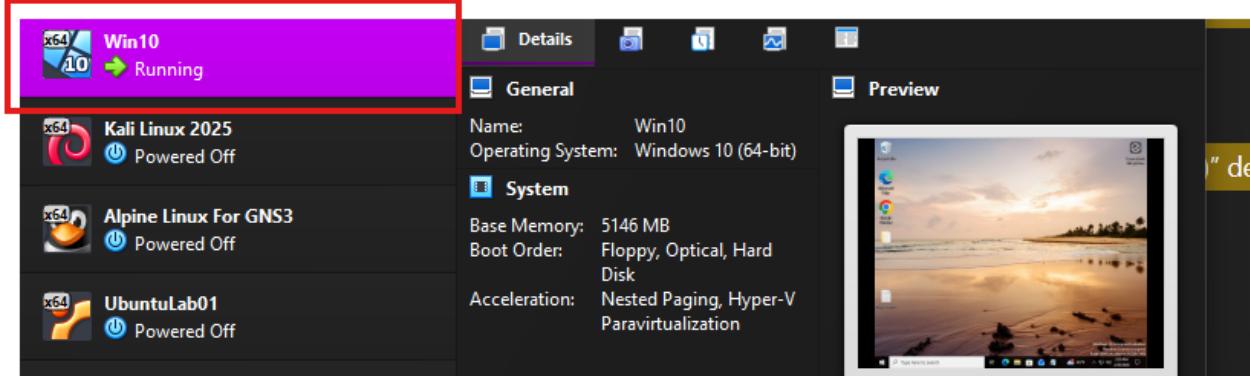
One group's Members tab showing the user added.



Step 6: Join your other VM to the domain (lab.local)

Put both VMs on the same VirtualBox NAT Network

A. In VirtualBox, create or confirm the NAT Network

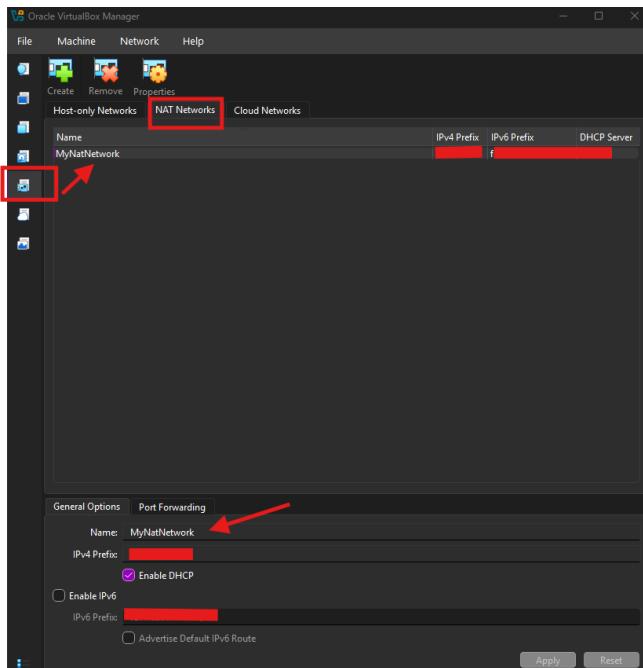


VirtualBox Manager

File → Tools → Network Manager

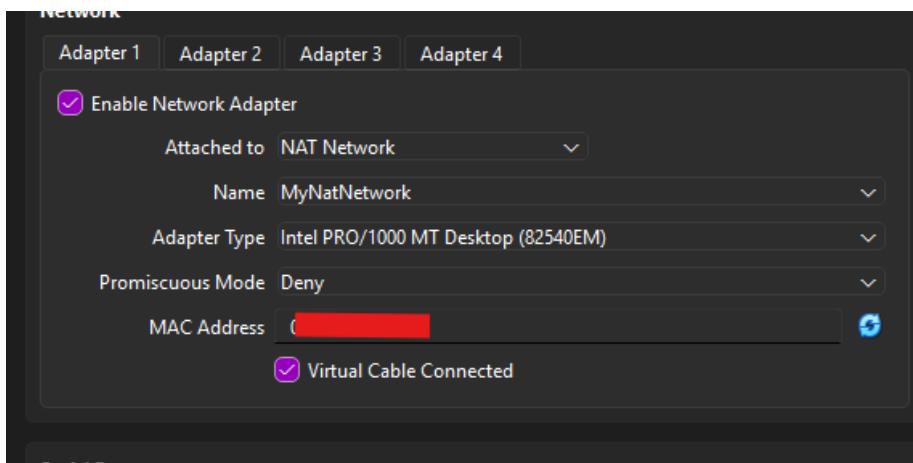
Click the **NAT Networks** tab

Confirm you see: **MyNatNetwork** (DHCP enabled)



B. Attach BOTH VMs to MyNatNetwork

Do this for your Domain Controller VM (WinServer2016 or Server 2025) and your Win10 VM.



Power off the VM

Settings → Network → Adapter 1

Attached to: **NAT Network**

Name: **MyNatNetwork**

OK

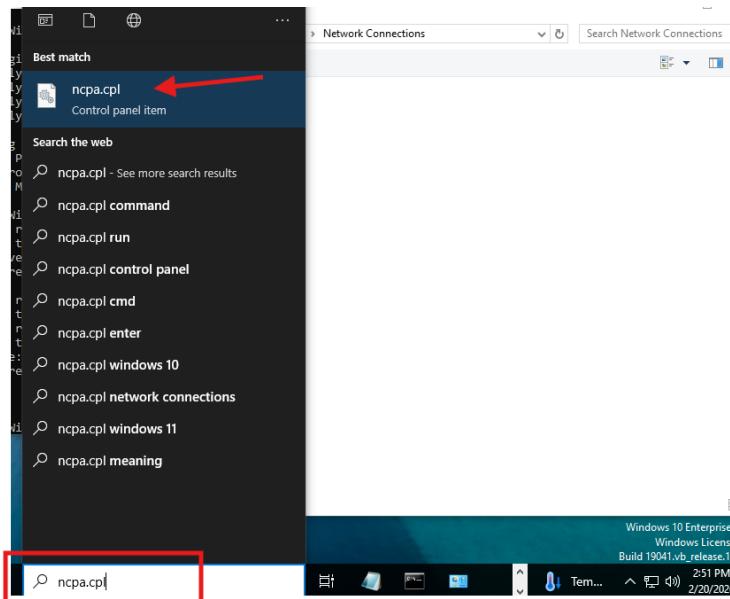
Start the Domain Controller first, then start Win10

Make Windows 10 use the Domain Controller for DNS

On the Win10 VM

Press **Windows + R**

Type **ncpa.cpl** and press **Enter**

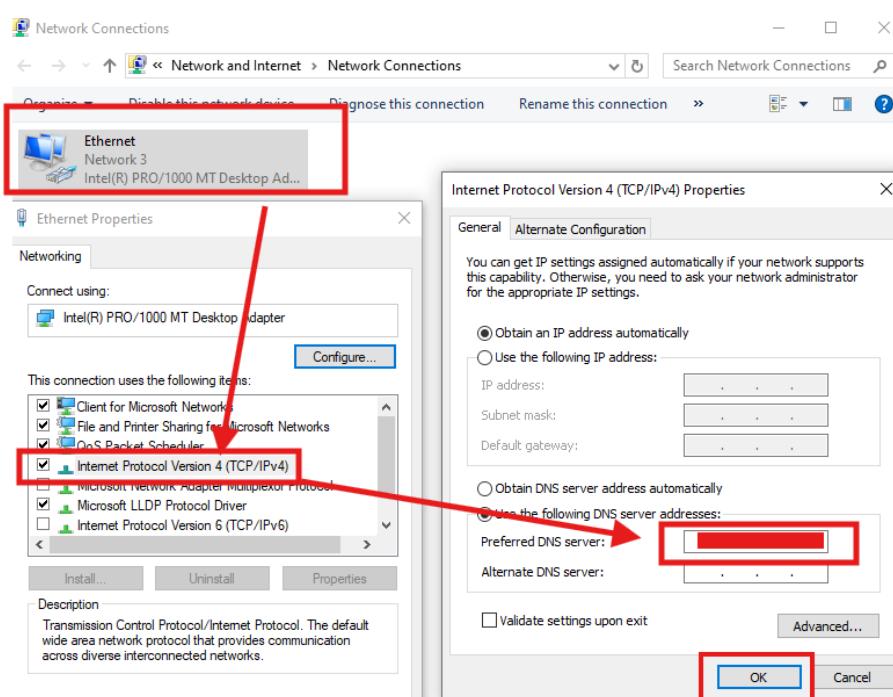


Right click **Ethernet** → **Properties**

Double click **Internet Protocol Version 4 (TCP/IPv4)**

Keep this **on**

Obtain an IP address automatically



Set this to

Use the following DNS server addresses

Preferred DNS server: 10.0.*.* ← your DNS server from your Window Server 2025 or 2016.

Alternate DNS server: blank

Click **OK**, then **Close**

Quick check in Command Prompt

ping 10.*.*.*

nslookup lab.local

```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.1]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10[REDACTED]

Pinging 10[REDACTED] with 32 bytes of data:
Reply from 10[REDACTED]: bytes=32 time=1ms TTL=128
Reply from 10[REDACTED]: bytes=32 time<1ms TTL=128
Reply from 10[REDACTED]: bytes=32 time=1ms TTL=128
Reply from 10[REDACTED]: bytes=32 time<1ms TTL=128

Ping statistics for 10[REDACTED]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>nslookup lab.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address: 10[REDACTED]

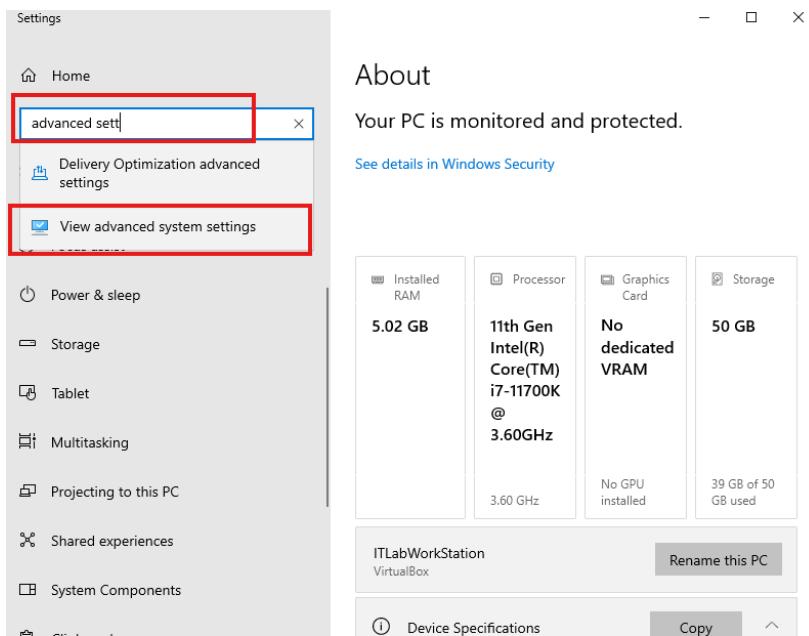
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Name:  lab.local
Address: 10[REDACTED]

C:\Windows\system32>
```

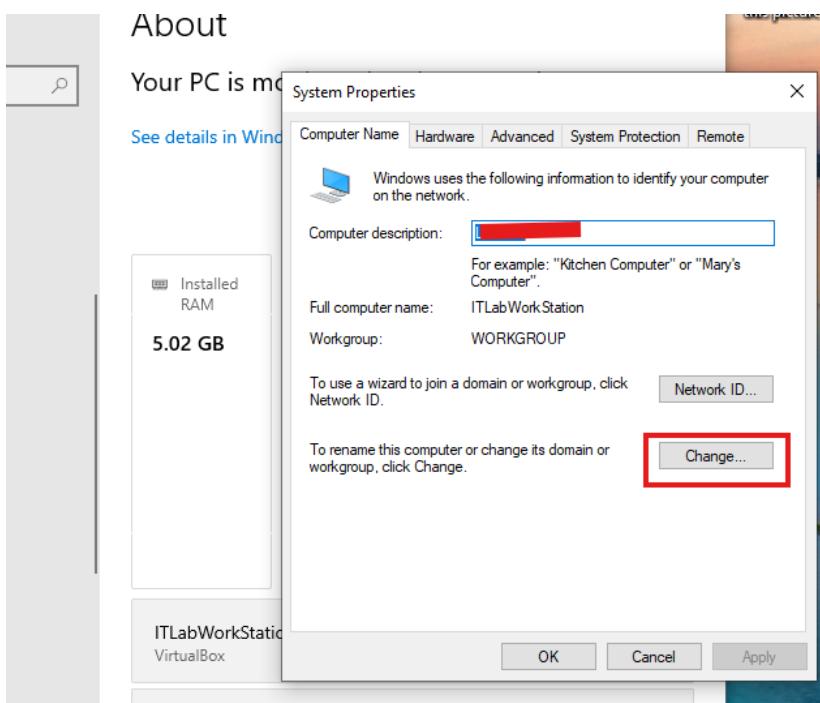
Join the domain

Right click **This PC** → **Properties**

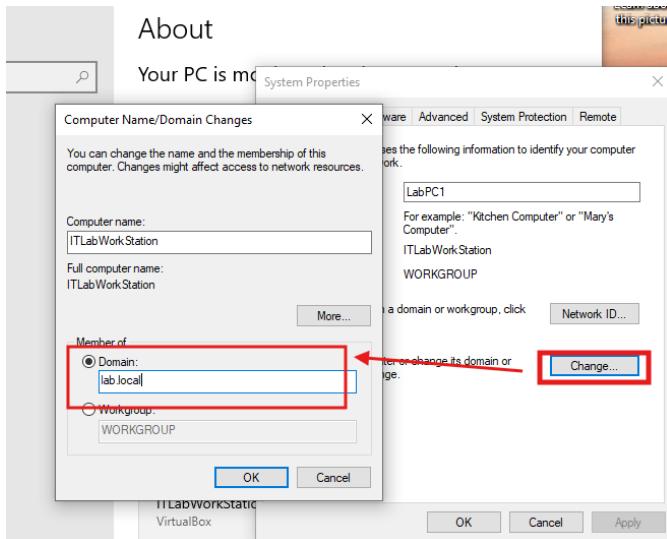
Click **Advanced system settings**



Computer Name tab → Change



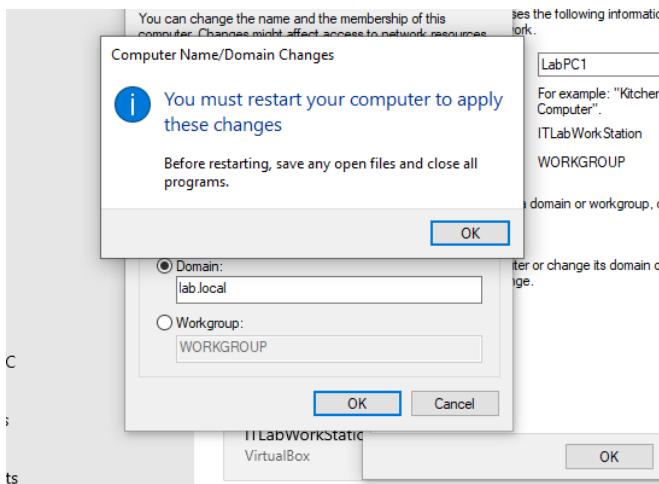
Select Domain and type: lab.local



When prompted, enter

Username: LAB\Administrator (your Window Server 2025 / 2016 log in)

Password: your DC Administrator password (Your Window server 2025/2016 password)



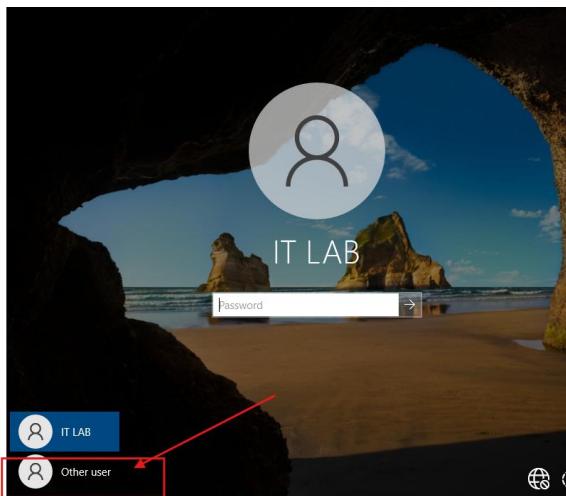
Click OK

When you see "Welcome to the lab.local domain", click OK

Restart the Win10 VM

Log in with a domain user after rebooting

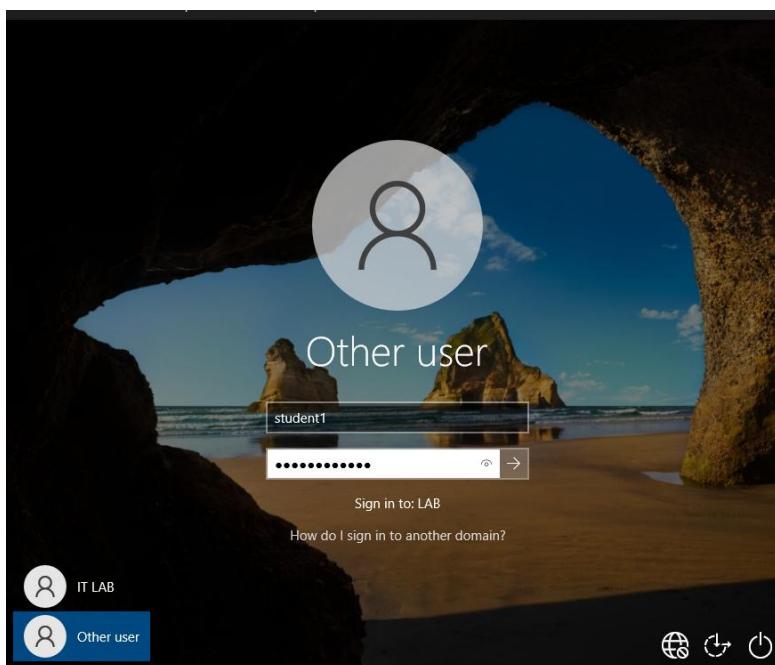
On the login screen, click **Other user**



Sign in as

LAB\student1

or student1@lab.local



Enter the password you created

If a message appears asking you to change your password, create a new password and continue logging in.

Final verification on Win10

Open Command Prompt and run

ipconfig /all (DNS should show 10.0.2.50)

```
C:\Users\student1>ipconfig /all
Windows IP Configuration

Host Name . . . . . : ITLabWorkStation
Primary Dns Suffix . . . . . : lab.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : lab.local
                                         attlocal.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : attlocal.net
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : [REDACTED]
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 10[REDACTED] (Preferred)
Subnet Mask . . . . . : [REDACTED]
Lease Obtained. . . . . : Friday, February 20, [REDACTED] 3:07:46 PM
Lease Expires . . . . . : Friday, February 20, [REDACTED] 3:17:47 PM
Default Gateway . . . . . : 10[REDACTED]
DHCP Server . . . . . : 10[REDACTED]
DNS Servers . . . . . : 10[REDACTED]
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\student1>
```

nslookup lab.local

```
C:\Users\student1>nslookup lab.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10[REDACTED]

Name:      lab.local
Address:   10.[REDACTED]

C:\Users\student1>
```

ping dc1.lab.local

```
C:\Users\student1>ping dc1.lab.local

Pinging dc1.lab.local [10] with 32 bytes of data:
Reply from 10[REDACTED] bytes=32 time<1ms TTL=128
Reply from 10[REDACTED] bytes=32 time=1ms TTL=128
Reply from 10[REDACTED] bytes=32 time=1ms TTL=128
Reply from 10[REDACTED] bytes=32 time=1ms TTL=128

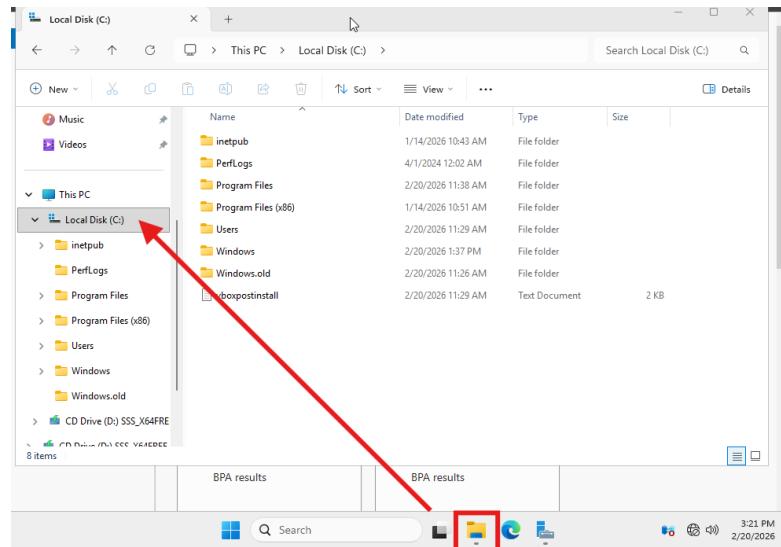
Ping statistics for 10[REDACTED]
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\student1>
```

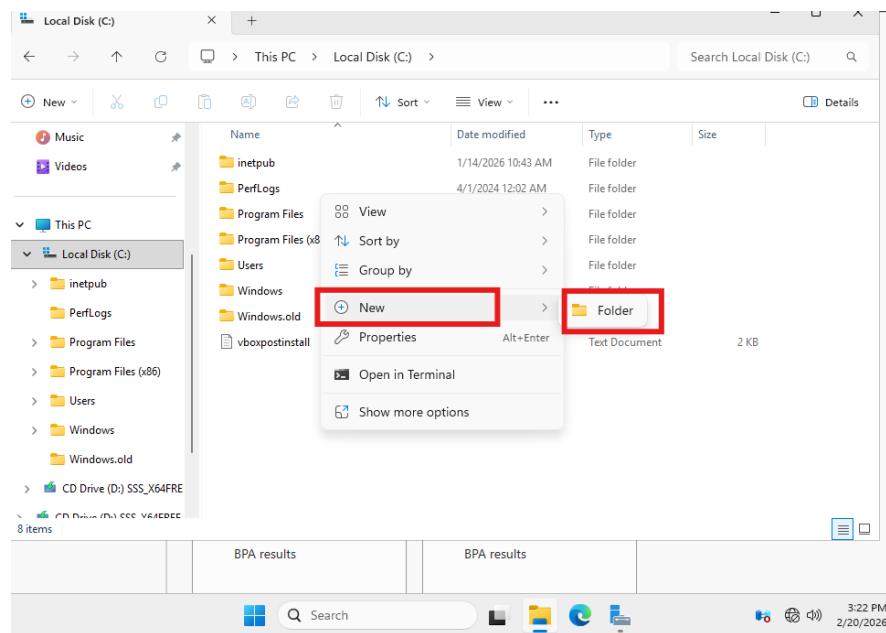
Step 7A: File Share plus NTFS permissions (test with your domain users)

Goal: Create a shared folder on the server and control access using groups, then verify from the Win10 client.

A) Create folders on the Domain Controller



On the server (DC1):

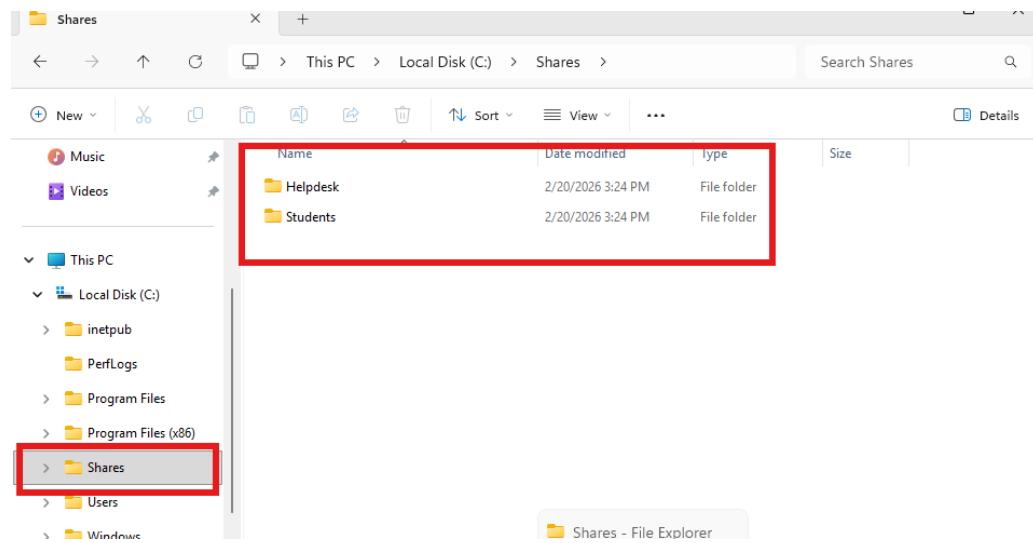


Create a folder: C:\Shares

Inside it, create:

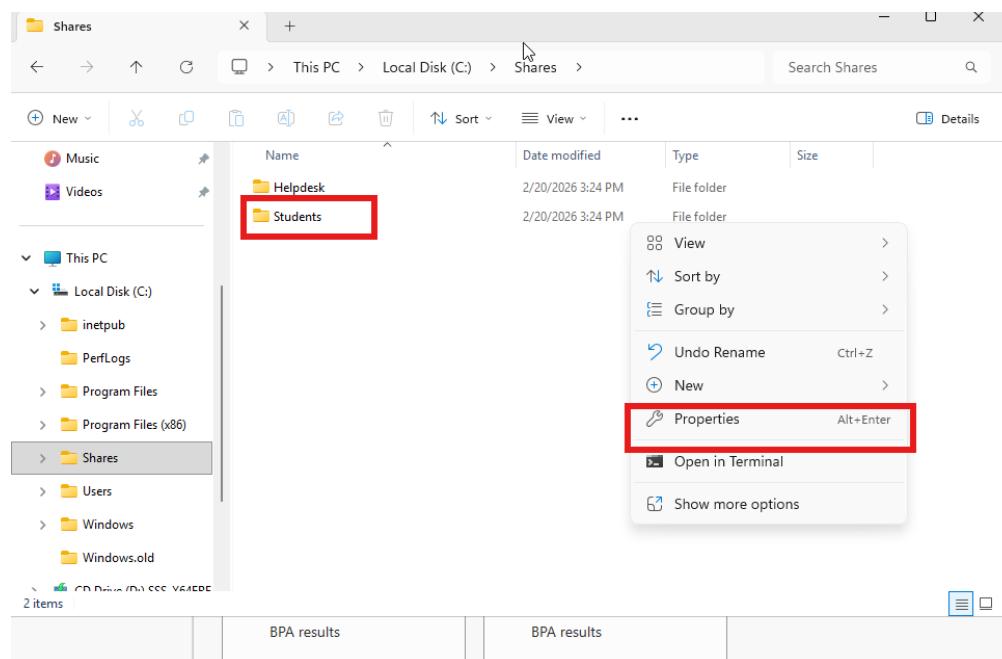
C:\Shares\Students

C:\Shares\Helpdesk

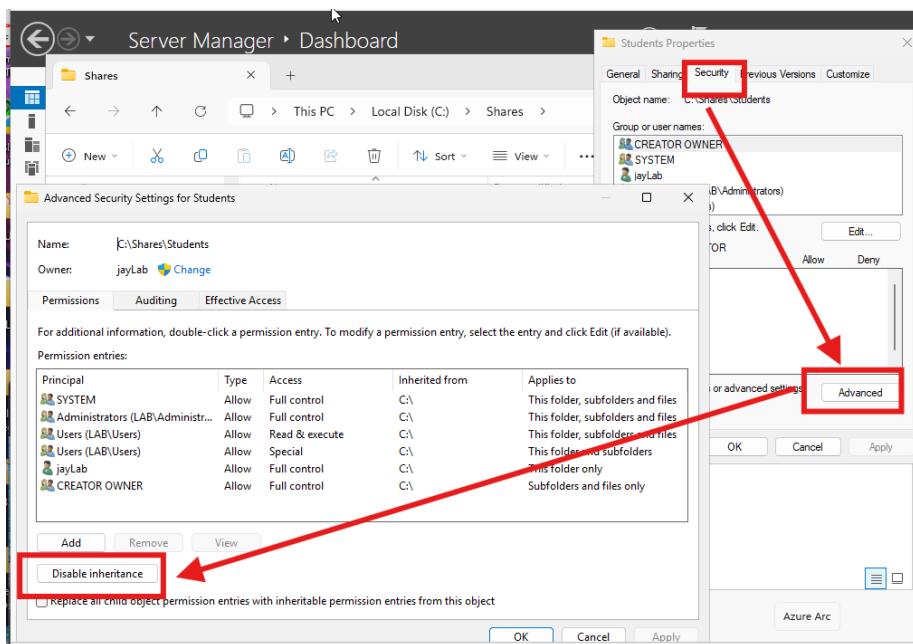


B) Set NTFS permissions (Security tab)

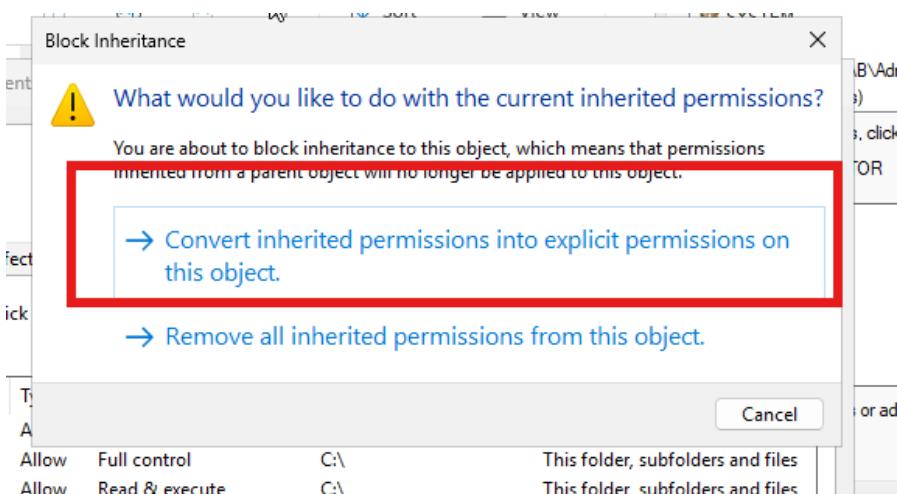
Right click C:\Shares\Students → Properties → Security → Advanced



Click Disable inheritance



Choose Convert inherited permissions

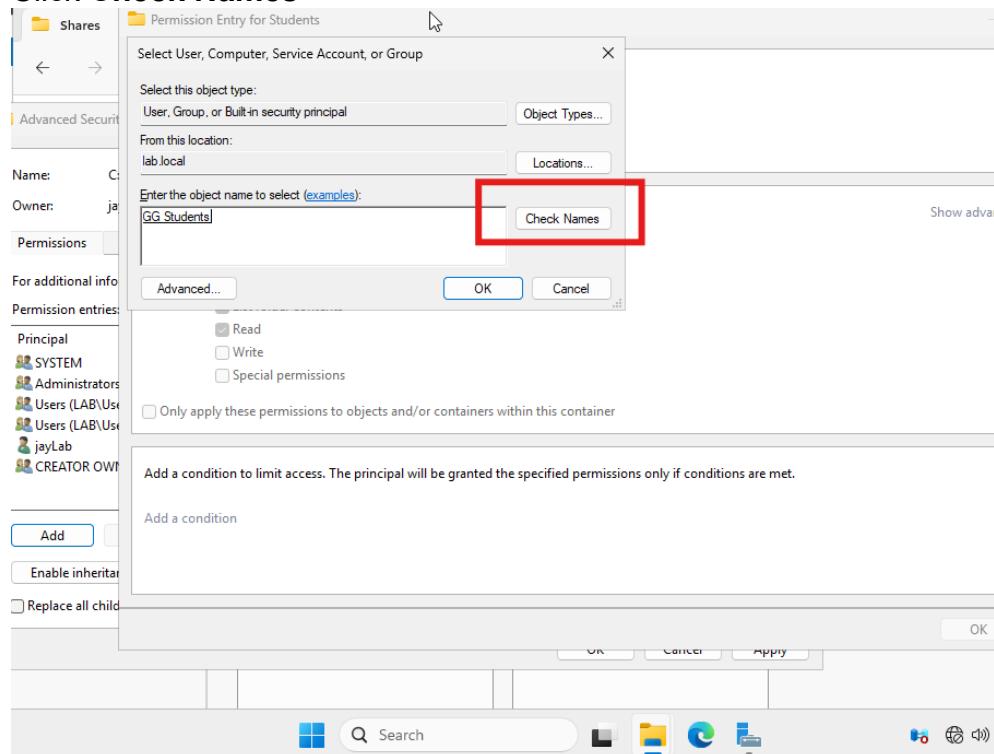


Remove groups you do not want (example Users) but keep.

Type the group name, then verify it:

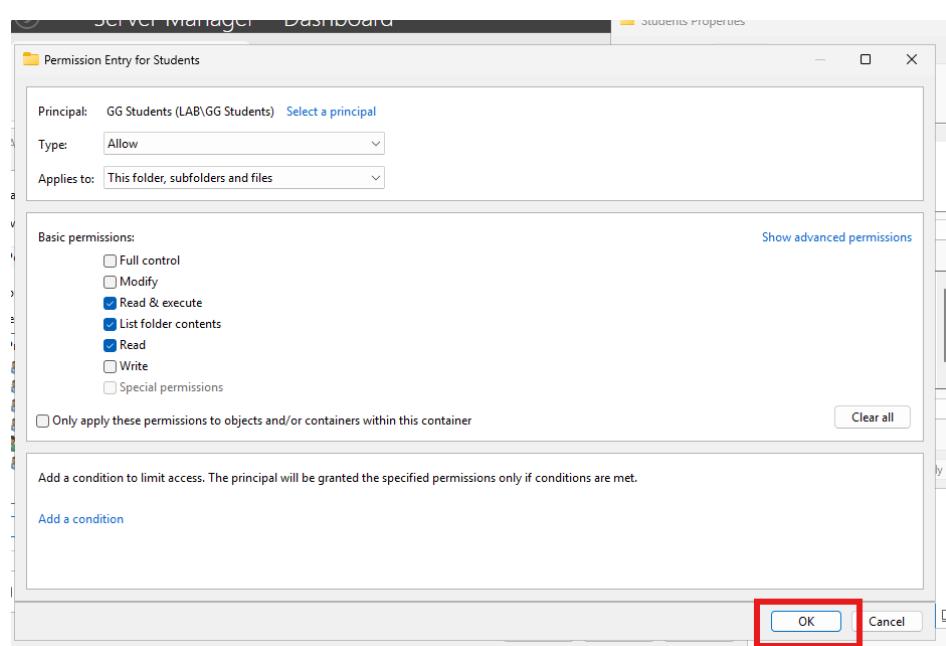
In Enter the object name to select, type **GG Students**

Click **Check Names**



If it changes to LAB\GG Students (or becomes underlined), click **OK**

On the next screen, select Modify permissions, then click **OK** and **Apply**



Make sure these remain:

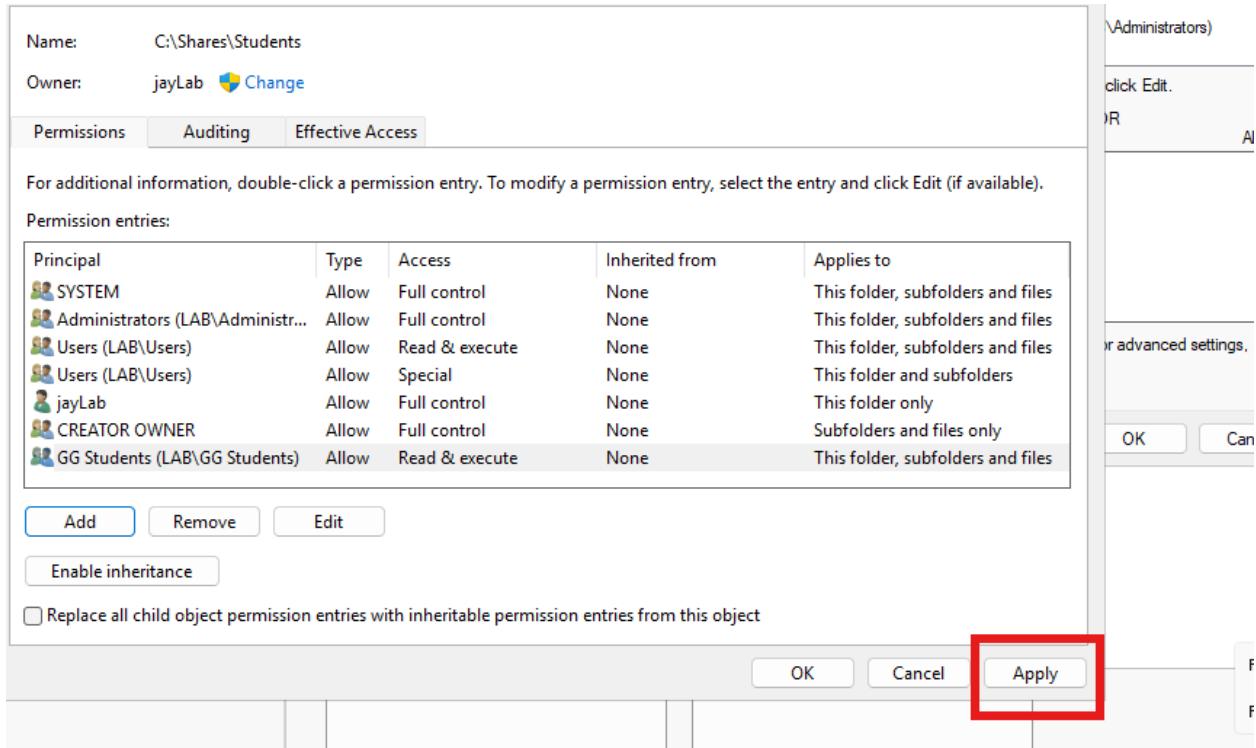
SYSTEM (Full control)

Administrators (Full control)

GG Students (Modify)

Click **Apply** (bottom right)

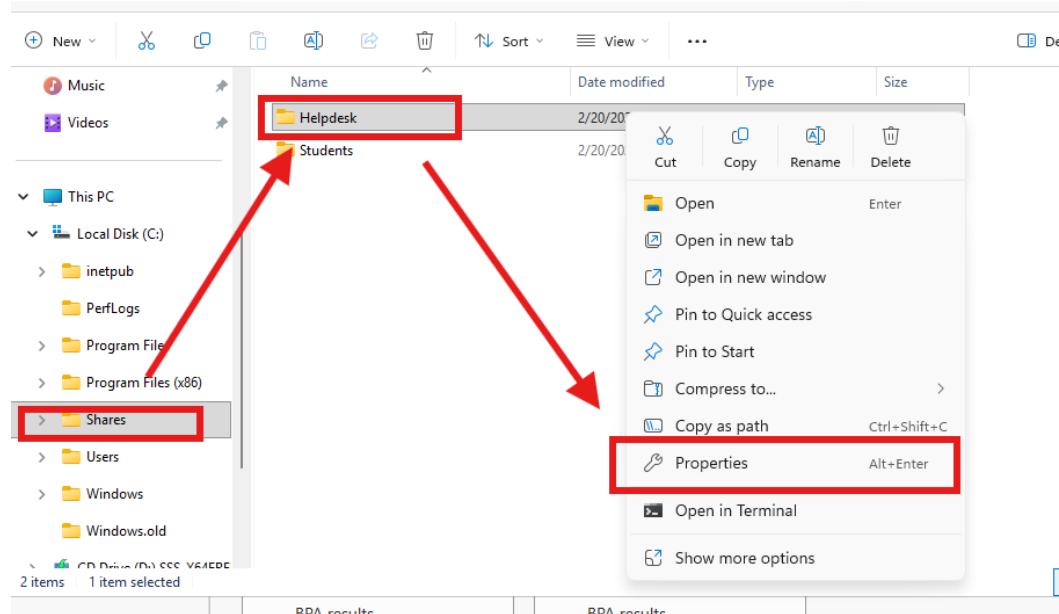
Click **OK** to close



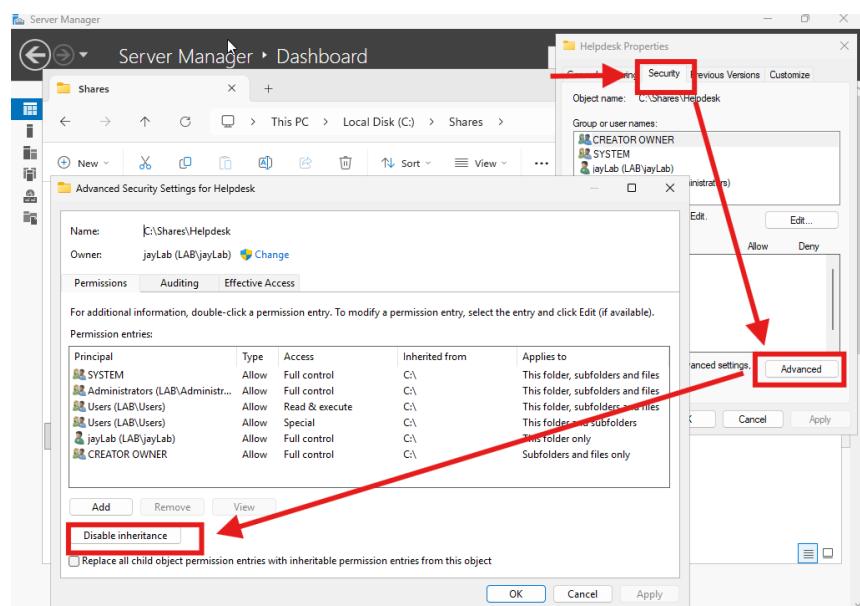
Step 7B: Helpdesk / Students NTFS permissions

On the server:

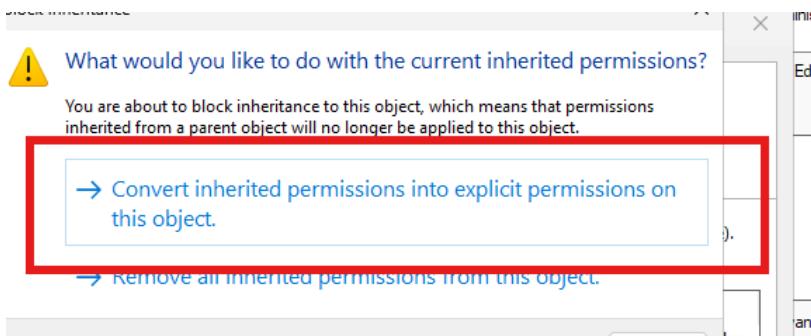
Right click C:\Shares\Helpdesk → Properties



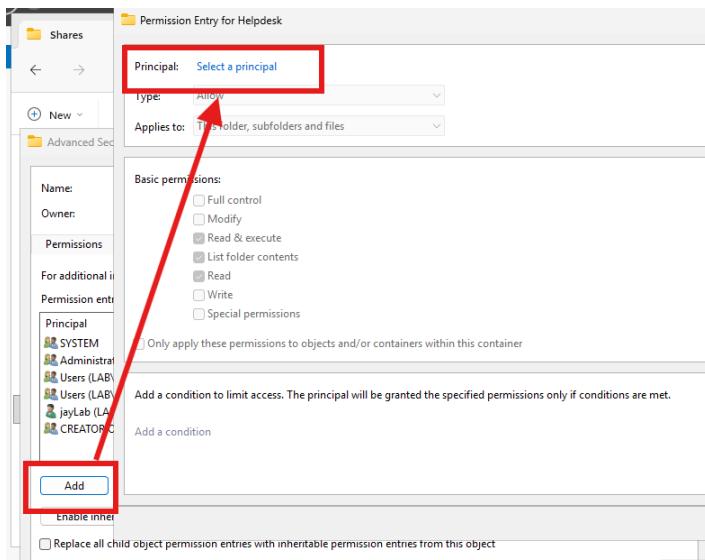
Security tab → Advanced



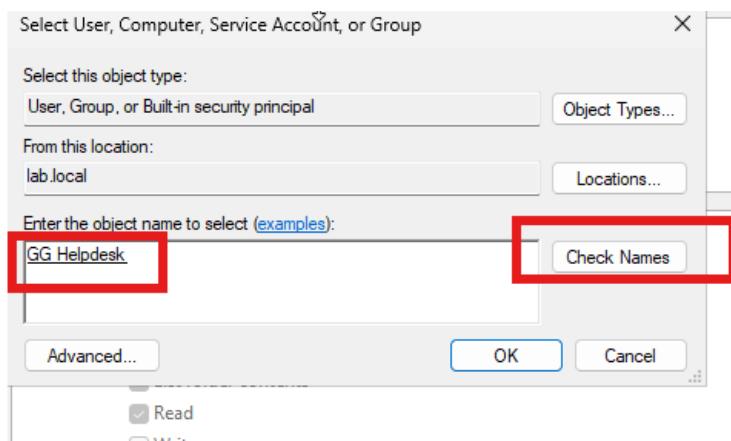
Click Disable inheritance → choose Convert

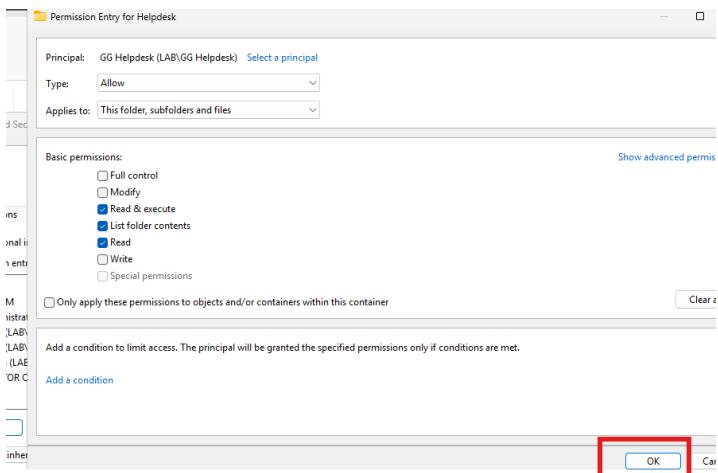


Click Add → Select a principal



Type GG Helpdesk → Check Names → OK





Set permissions to Modify

Click OK → Apply

Optional cleanup:

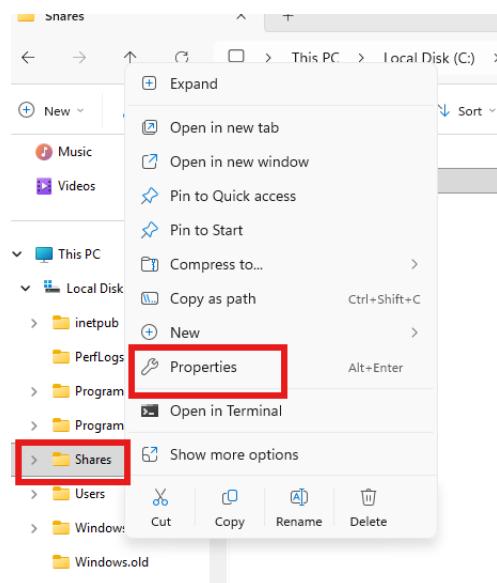
Remove Users (LAB\Users) if it is listed

Keep SYSTEM and Administrators

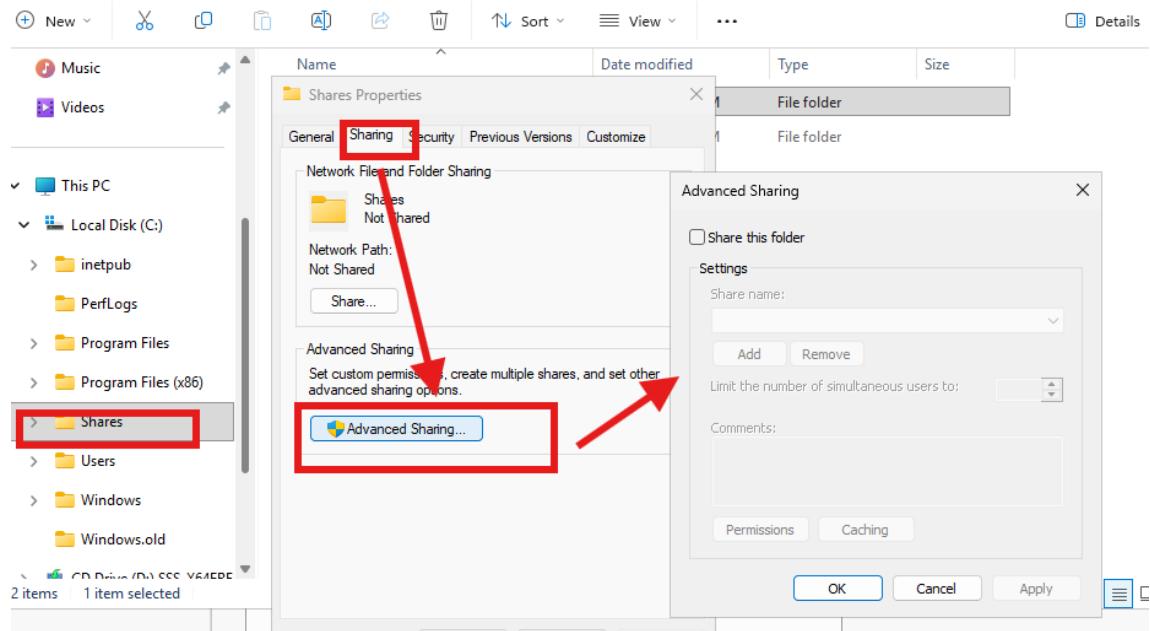
Step 7C: Share Students and Helpdesk

We will do Students first, then Helpdesk:

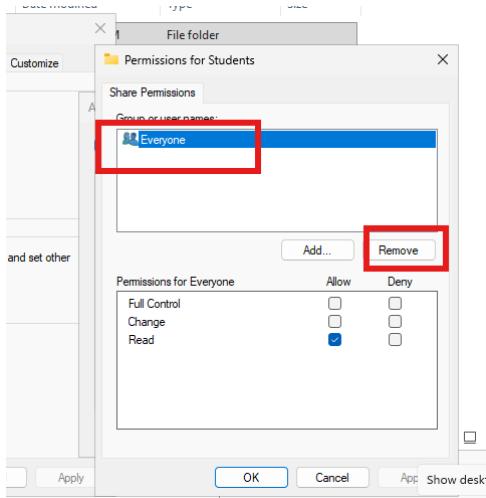
Properties →



Sharing → Advanced Sharing → Share this folder



Remove Everyone

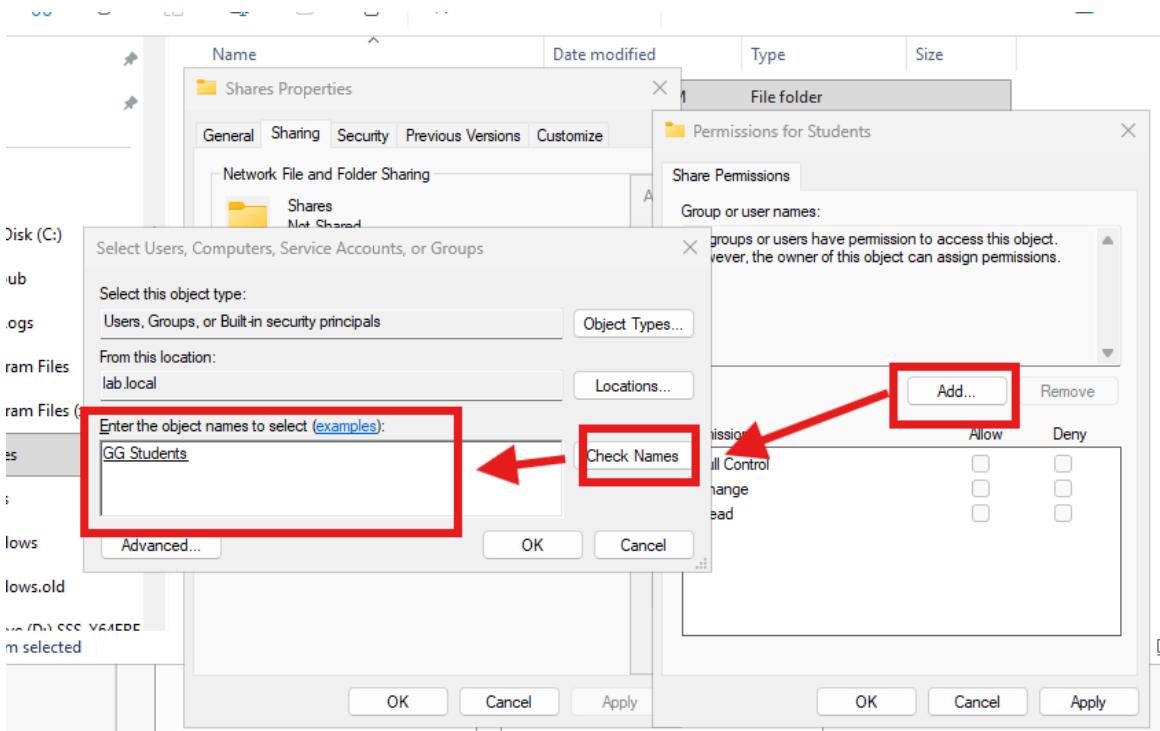


Add the correct group (Change, Read)

Click Add...

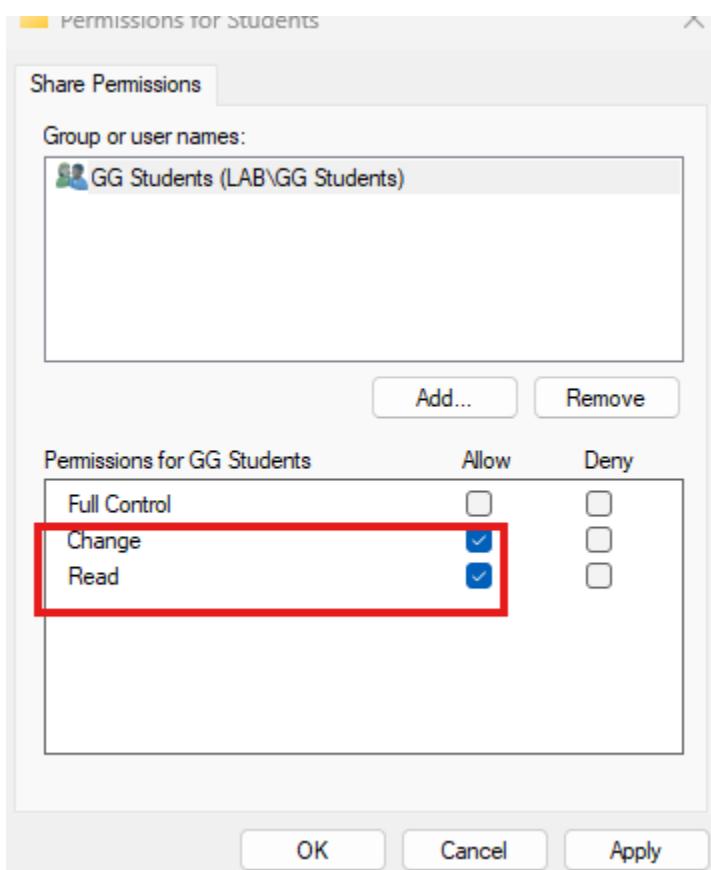
Type: **GG Students**

Click **Check Names** → **OK**



With GG Students selected, allow:

- Change
- Read



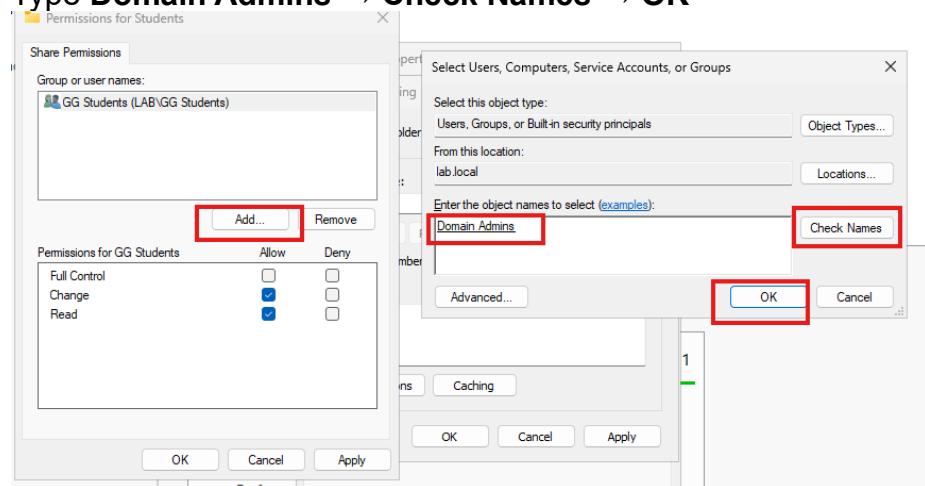
Then you will be back in the Permissions window:

Select **GG Students**

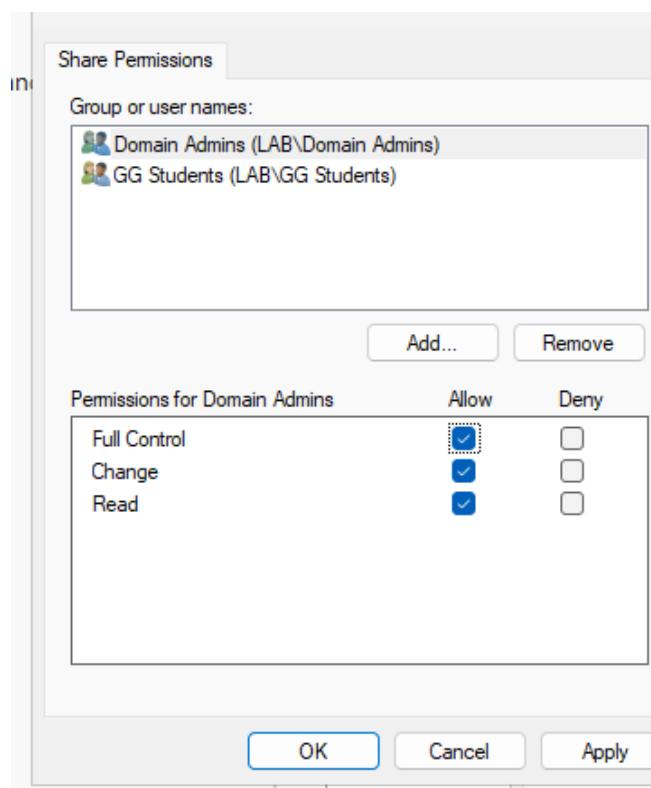
Check **Allow: Change** and **Allow: Read**

Click **Add...** again

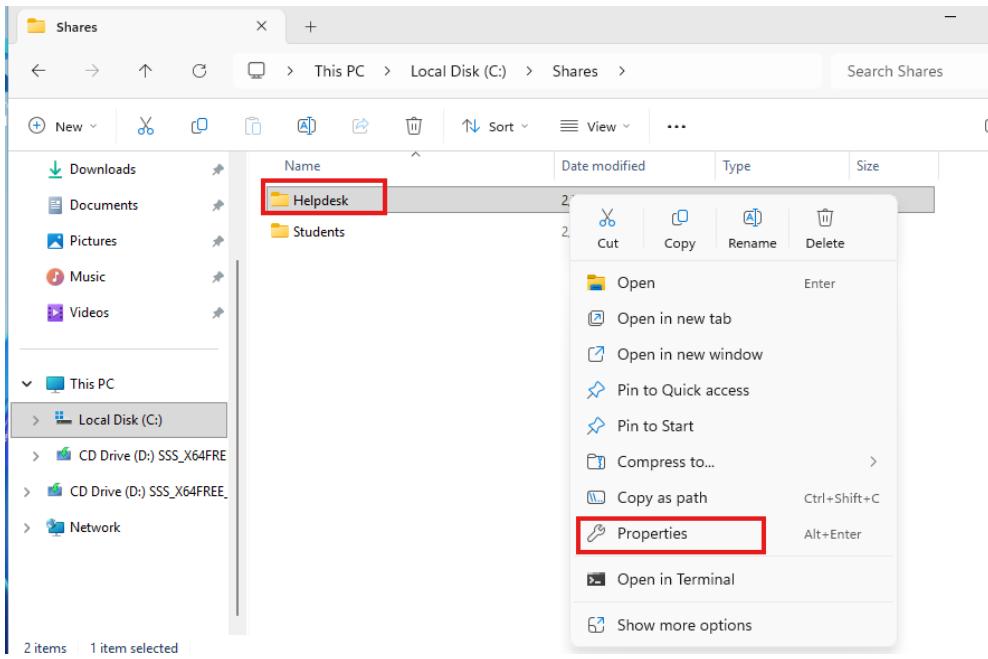
Type **Domain Admins** → **Check Names** → **OK**



Select **Domain Admins** and check **Allow: Full Control**



Click OK → Apply → OK

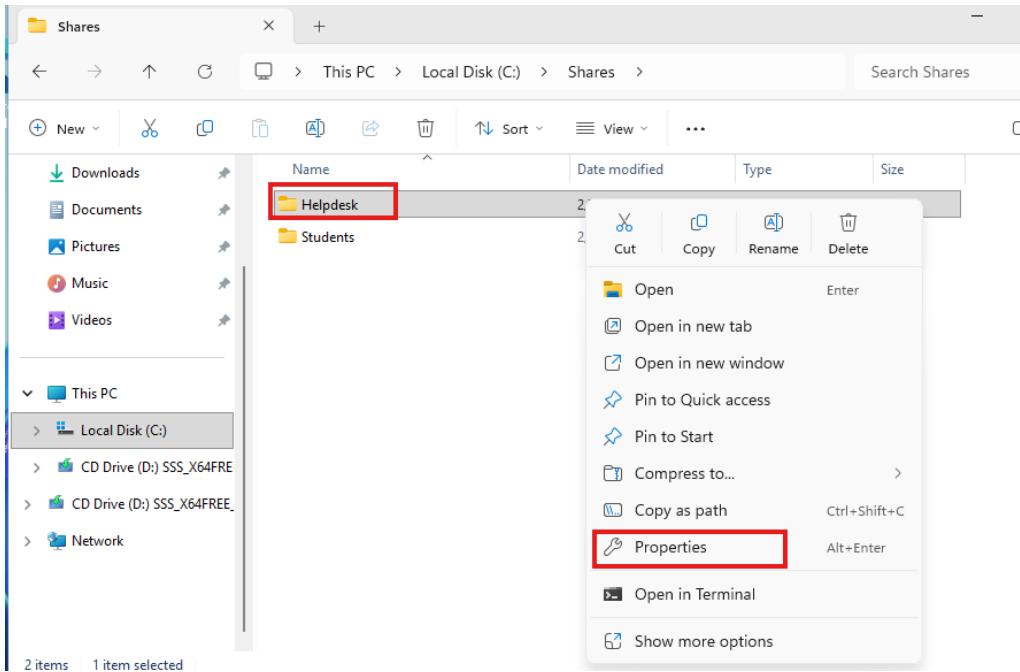


Step 7C Helpdesk Sharefolder

On Windows Server:

Go to C:\Shares

Right click Helpdesk → Properties



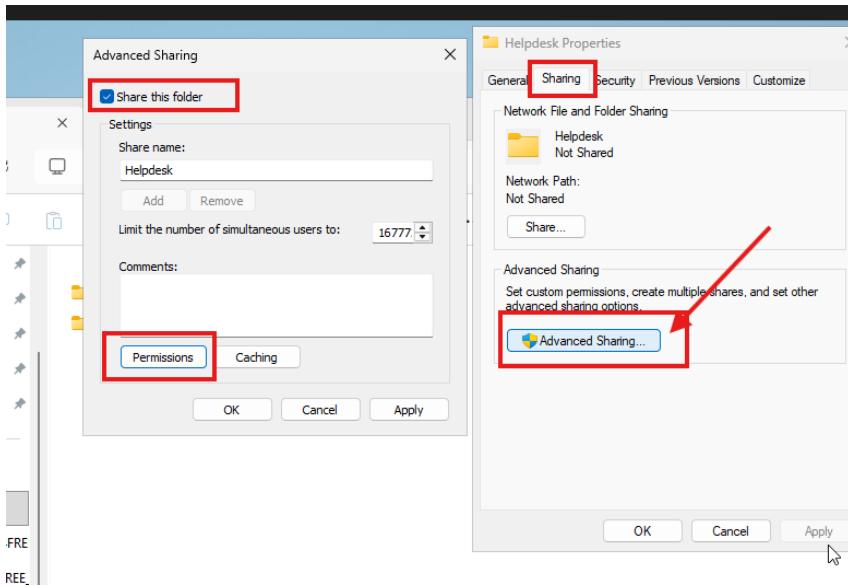
Click Sharing tab

Click Advanced Sharing

Check Share this folder

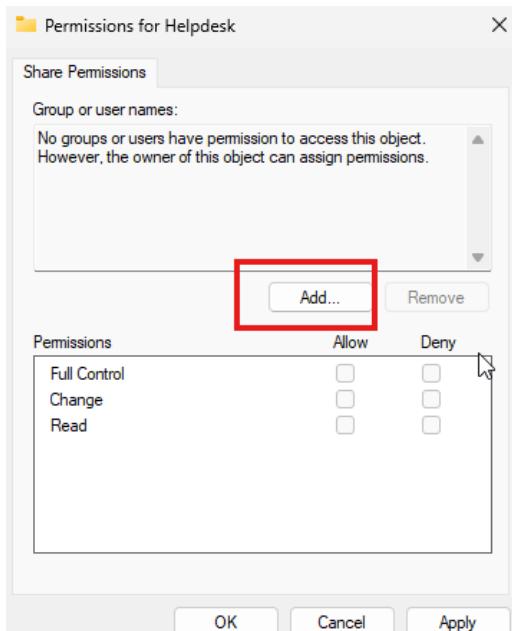
Share name: Helpdesk

Click Permissions

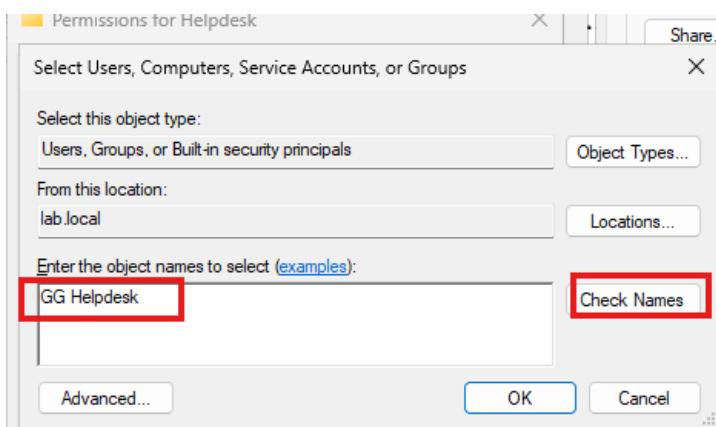


Select Everyone → Remove

Click Add

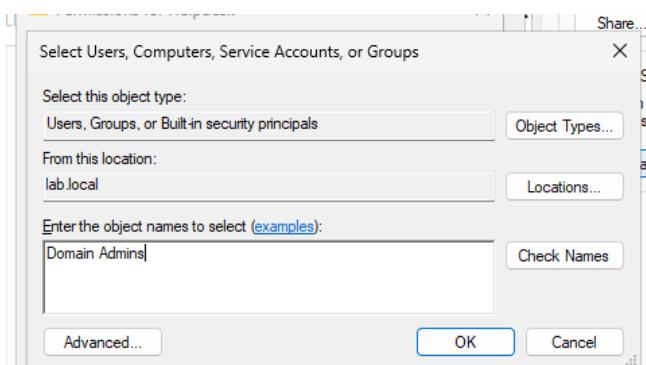


Type **GG Helpdesk** → **Check Names** → **OK**

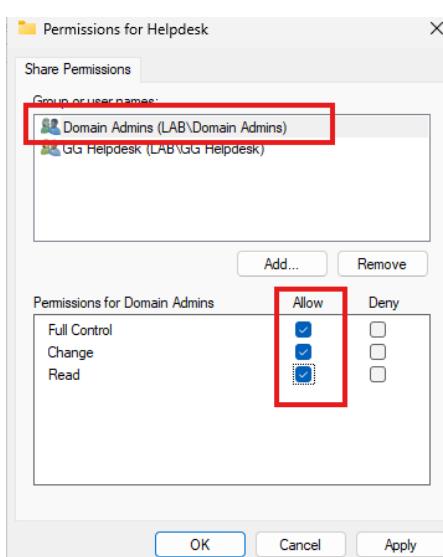


Select **GG Helpdesk** → Allow **Change** and **Read**

Click **Add Type Domain Admins** (or Administrators) → **Check Names** → **OK**



Select **Domain Admins/Administrators** → Allow **Full Control**



Click **OK** → **Apply** → **OK**

Appendix

Appendix A: Lab Environment

- Host platform: Oracle VirtualBox
- Server VM: Windows Server (Domain Controller)
- Client VM: Windows 10
- VirtualBox network mode used for VM to VM communication: NAT Network
- NAT Network name: MyNatNetwork
- Domain name: lab.local

Appendix B: IP and DNS Settings

- Domain Controller
- IPv4 address: 10.*.*.*
- Subnet mask: 255.255.255.0
- Default gateway: 10.*.*.*
- Preferred DNS: 10.*.*.*
- Windows 10 client
- IP addressing: DHCP
- Preferred DNS: 10.*.*.*
- DNS forwarders on Domain Controller
- 8.8.8.8
- 1.1.1.1

Appendix C: Active Directory Objects Created

- Organizational Units
- LabUsers
- LabGroups
- LabComputers
- Users
- student1
- helpdesk1
- Security Groups
- GG Students
- GG Helpdesk
- Membership
- student1 is a member of GG Students
- helpdesk1 is a member of GG Helpdesk

Appendix D: Shares Created

- Folders on server
- C:\Shares\Students
- C:\Shares\Helpdes
- Share names
- Students
- Helpdesk
- UNC paths used for testing

Appendix E: Permissions Summary

- NTFS permissions
- Students folder: GG Students has Modify
- Helpdesk folder: GG Helpdesk has Modify
- SYSTEM and Administrators retained for full control
- Share permissions
- Students share: GG Students has Change and Read, Domain Admins or Administrators has Full Control
- Helpdesk share: GG Helpdesk has Change and Read, Domain Admins or Administrators has Full Control

Appendix F: Validation Commands Used

- On server or client
- ipconfig
- ipconfig /all
- nslookup lab.local
- nslookup dc1.lab.local
- ping 10.0.2.50
- ping dc1.lab.local

Appendix G: Suggested Screenshots to Include

- VirtualBox NAT Network showing MyNatNetwork
- Server showing domain and DNS tools available
- ADUC showing OUs, users, and groups
- Domain join confirmation on Windows 10
- NTFS permissions for Students and Helpdesk folders
- Advanced Sharing permissions for Students and Helpdesk shares
- Win10 successful access to correct share and denied access to the other share