

8/5/2025

Lab 5

Managing Group Accounts in Active
Directory



Mohammed, Laetitia, 0931512

NETWORK INSTALLATION AND ADMINISTRATION II

Contents

Task 1: Create and Manage Security Groups.....	1
Task 2: Add Members to Groups	2
Task 3: Create Organizational Units (OUs) and Domain Local Groups.....	4
Task 4: Create a Local Group and Manage Membership	7
Task 5: Share and Set Permissions on SRV12.....	10
Task 6: Test HR Share Access from ClientX.....	13
Task 7: Remove a User from a Group and Delete a User	15
Task 8: Create IT OU and Configure Groups on DC312 and DC112	17
Task 9: Share and Set Permissions for IT Global Share.....	22
Task 10: Test IT Share Access from ClientX	24
Task 11: Change Group Scope.....	26

Objective

This lab will help you practice managing Active Directory groups using Active Directory Administrative Center (ADAC) and PowerShell. You will perform tasks related to group creation, membership management, delegation, and permission assignments.

Task 1: Create and Manage Security Groups

Create a Global Security Group (**GG_HR_Admins**) in the **HR** OU using **ADAC**.

Create a Global Security Group (**GG_IT_Admins**) in the **IT** OU using **PowerShell**.

Create Group: GG_HR_Admin

Group	Group name: <input type="text" value="GG_HR_Admin"/>		E-mail: <input type="text"/>
Managed By	Group (SamAccountName...): <input type="text" value="GG_HR_Admin"/>		Create in: OU=HR,DC=vlabs12,DC=com
Member Of	Group type: <input checked="" type="radio"/> Security <input type="radio"/> Distribution		Description: <input type="text"/>
Members	Group scope: <input checked="" type="radio"/> Global <input type="radio"/> Domain local <input type="radio"/> Universal		Notes: <input type="text"/>
Password Settings	<input type="checkbox"/> Protect from accidental deletion		

Managed By

Managed by: <input type="text"/> <input type="button" value="Edit..."/> <input type="button" value="Clear"/>	Office: <input type="text"/>
<input type="checkbox"/> Manager can update membership list	Address: <input type="text"/>
Phone numbers:	Street: <input type="text"/>
Main: <input type="text"/>	City: <input type="text"/>
Mobile: <input type="text"/>	Country/Region: <input type="text"/>
Fax: <input type="text"/>	

New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"GG_IT_Admins" -Path:"OU=IT,DC=vlabs12,DC=com" -SamAccountName:"GG_IT_Admins"

Get-ADGroup -Filter {Name -eq "GG_it_Admins"} | Select DistinguishedName

```
PS C:\Users\Administrator.DC112> New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"GG_IT_Admins" -Path:"OU=IT,DC=vlabs12,DC=com" -SamAccountName:"GG_IT_Admins"
PS C:\Users\Administrator.DC112> Get-ADGroup -Filter {Name -eq "GG_it_Admins"} | Select DistinguishedName
DistinguishedName
-----
CN=GG_IT_Admins,OU=IT,DC=vlabs12,DC=com
PS C:\Users\Administrator.DC112>
```

Task 2: Add Members to Groups

Add **Emma Morel (e.morel)** and **Lucas Bernard (l.bernard)** to **GG_HR_Admins** using **PowerShell**.

Add **Chloe Girard (c.girard)** and **Sophie Lambert (s.lambert)** to **GG_IT_Admins** using **PowerShell**.

Add-ADGroupMember -Identity "GG_HR_Admins" -Members "e.morel"

Add-ADGroupMember -Identity "GG_HR_Admins" -Members "l.bernard"

Get-ADGroupMember -Identity "GG_HR_Admins"

```
PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "GG_HR_Admins" -Members "e.morel"
PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "GG_HR_Admins" -Members "l.bernard"
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "GG_HR_Admins"

distinguishedName : CN=Emma Morel,OU=HR,DC=vlabs12,DC=com
name               : Emma Morel
objectClass        : user
objectGUID         : 3a31d06c-840b-4ff6-bbcd-c3dae2c89fc3
SamAccountName     : e.morel
SID                : S-1-5-21-1463046243-3978224867-743297864-1111

distinguishedName : CN=Lucas Bernard,OU=HR,DC=vlabs12,DC=com
name               : Lucas Bernard
objectClass        : user
objectGUID         : ee95857e-4238-445e-b05e-a6187b340eb0
SamAccountName     : l.bernard
SID                : S-1-5-21-1463046243-3978224867-743297864-1113

PS C:\Users\Administrator.DC112> _
```

Add-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard"

Add-ADGroupMember -Identity "GG_IT_Admins" -Members "s.lambert"

Get-ADGroupMember -Identity "GG_IT_Admins"

```

PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard"
PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "GG_IT_Admins" -Members "s.lambert"
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "GG_IT_Admins"

distinguishedName : CN=Sophie Lambert,OU=IT,DC=vlabs12,DC=com
name              : Sophie Lambert
objectClass       : user
objectGUID        : 5885a491-c0db-4e89-8f9a-f841e7b00f51
SamAccountName    : s.lambert
SID               : S-1-5-21-1463046243-3978224867-743297864-1109

distinguishedName : CN=Chloe Girard,OU=IT,DC=vlabs12,DC=com
name              : Chloe Girard
objectClass       : user
objectGUID        : 6565678e-60b9-4eec-a008-1c6bbb71e686
SamAccountName    : c.girard
SID               : S-1-5-21-1463046243-3978224867-743297864-1115

```

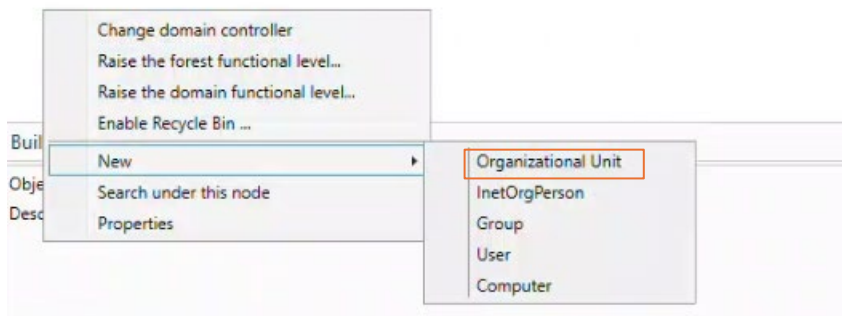
Task 3: Create Organizational Units (OUs) and Domain Local Groups

Create an **OU** named **Shared Resources** in **vlabs12.com** domain using **ADAC**.

Create a **Domain Local Group (DLG_HR_Share)** in **Shared Resources** using **ADAC**.

Create a **Domain Local Group (DLG_IT_Share)** in **Shared Resources** using **PowerShell**.

Create Shared Resources by right-clicking → New → Organizational Unit (OU)



Create Organizational Unit: Shared Resources

Organizational Unit
Managed By

Name: * Shared Resources

Address:
Street

City State/Province Zip/Postal code

Country/Region:

Managed By

Managed by:

Phone numbers:
Main:
Mobile:
Fax:

In Shared Resources, create the Domain Local Group → DLG_HR_Share

Active Directory Administrative Center ▸ vlabs12 (local) ▸ Shared Resources

Directory... < Shared Resources (0)

Filter

Name Type Description

New

Delete

Move...

Search under this node

Properties

Organizational Unit

InetOrgPerson

Group

User

Computer

Make sure to select “Domain Local”

Create Group: DLG_HR_Share

Group

Managed By

Member Of

Members

Password Settings

Group

Group name: * DLG_HR_Share

Group (SamAccountName... * DLG_HR_Share

Group type:

☒ Security

☐ Distribution

☐ Protect from accidental deletion

Group scope:

☒ Domain local

☐ Global

☐ Universal

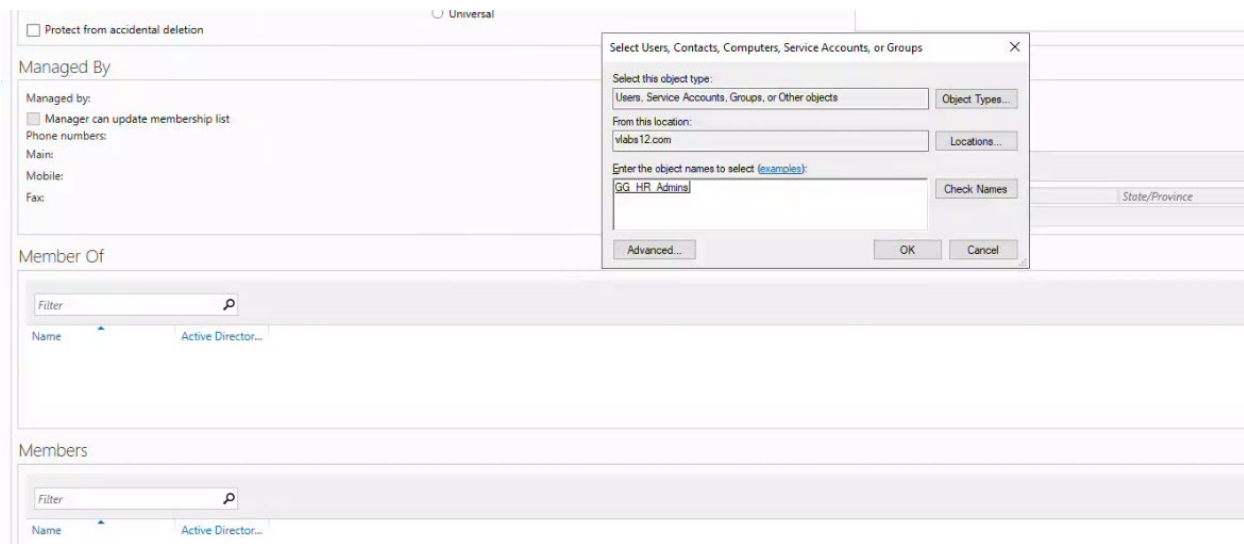
E-mail:

Create in: OU=Shared Resources,DC=vlabs12,DC=

Description:

Notes:

Click on Add in the Members section and add GG_HR_Admins



Repeat for the IT groups in Powershell using the commands below

New-ADGroup -Name "DLG_IT_Share" -SamAccountName "DLG_IT_Share" -GroupCategory Security -GroupScope DomainLocal -Path "OU=Shared Resources,DC=vlabs12,DC=com"

Get-ADGroup -Identity "DLG_IT_Share"

```
PS C:\Users\Administrator.DC112> New-ADGroup -Name "DLG_IT_Share" -SamAccountName "DLG_IT_Share" -GroupCategory Security -GroupScope DomainLocal -Path "OU=Shared Resources,DC=vlabs12,DC=com"
PS C:\Users\Administrator.DC112> Get-ADGroup -Identity "DLG_IT_Share"

DistinguishedName : CN=DLG_IT_Share,OU=Shared Resources,DC=vlabs12,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : DLG_IT_Share
ObjectClass       : group
ObjectGUID        : 140e23ec-5091-4c3d-b4ee-5caf922e7794
SamAccountName    : DLG_IT_Share
SID               : S-1-5-21-1463046243-3978224867-743297864-1120

PS C:\Users\Administrator.DC112>
```

Add-ADGroupMember -Identity "DLG_IT_Share" -Members "GG_IT_Admins"

Get-ADGroupMember -Identity "DLG_IT_Share"

```
PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "DLG_IT_Share" -Members "GG_IT_Admins"
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "DLG_IT_Share"

distinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs12,DC=com
name               : GG_IT_Admins
objectClass        : group
objectGUID         : f17e7bce-fdd1-4443-ba67-23a1449d6aec
SamAccountName     : GG_IT_Admins
SID                : S-1-5-21-1463046243-3978224867-743297864-1117

PS C:\Users\Administrator.DC112>
```

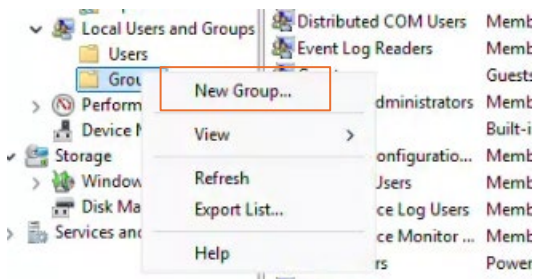
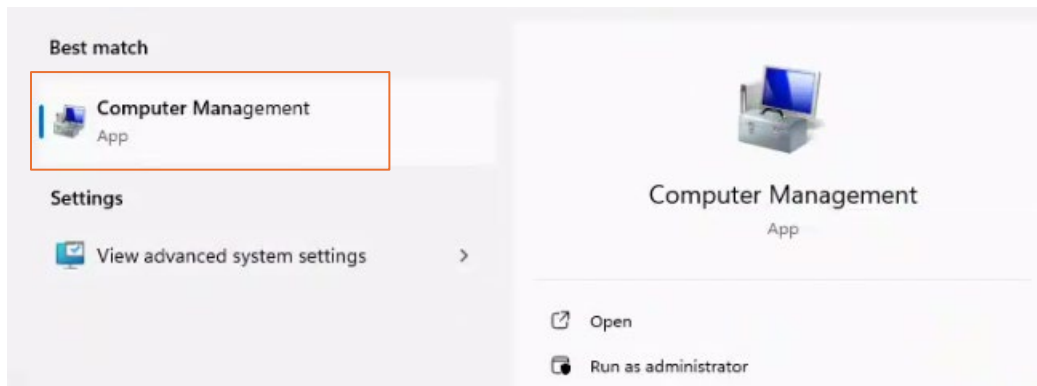
Task 4: Create a Local Group and Manage Membership

On **SRV12**, create a **Local Group (LG_HR_Files)** using **GUI**.

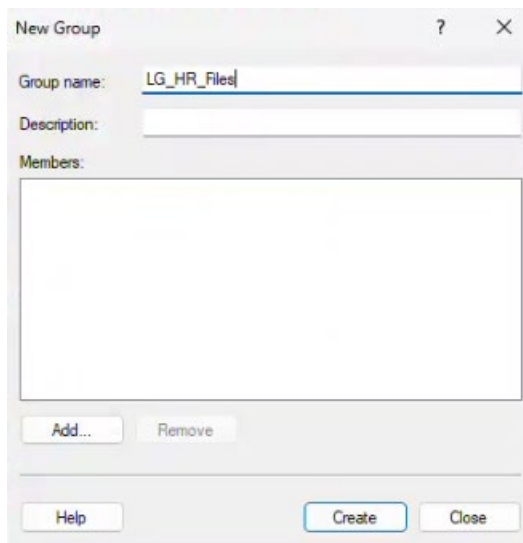
Add **DLG_HR_Share** group into **LG_HR_Files** group using **GUI**.

Verify the membership of **LG_HR_Files** group using **PowerShell**.

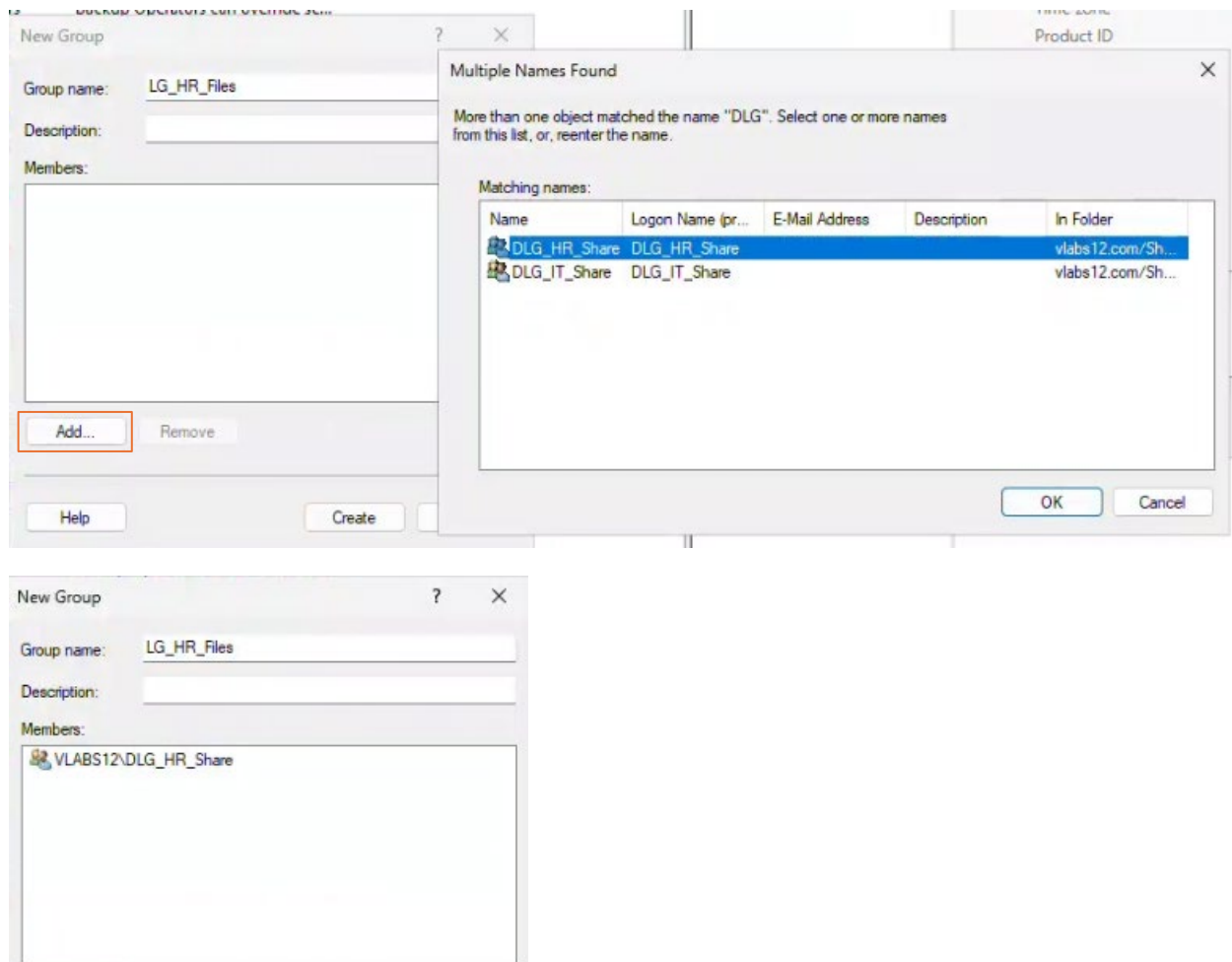
Go to Computer Management → Local Users and Groups. Right click and select New Group.



Create LG_HR_Files and then Add



Add the group DLG_HR_Share



Get-LocalGroupMember -Group "LG_HR_Files"

```
PS C:\Users\Administrator.VLABS12> Get-LocalGroupMember -Group "LG_HR_Files"

ObjectClass Name                PrincipalSource
-----
Group        VLABS12\DLG_HR_Share ActiveDirectory

PS C:\Users\Administrator.VLABS12> |
```

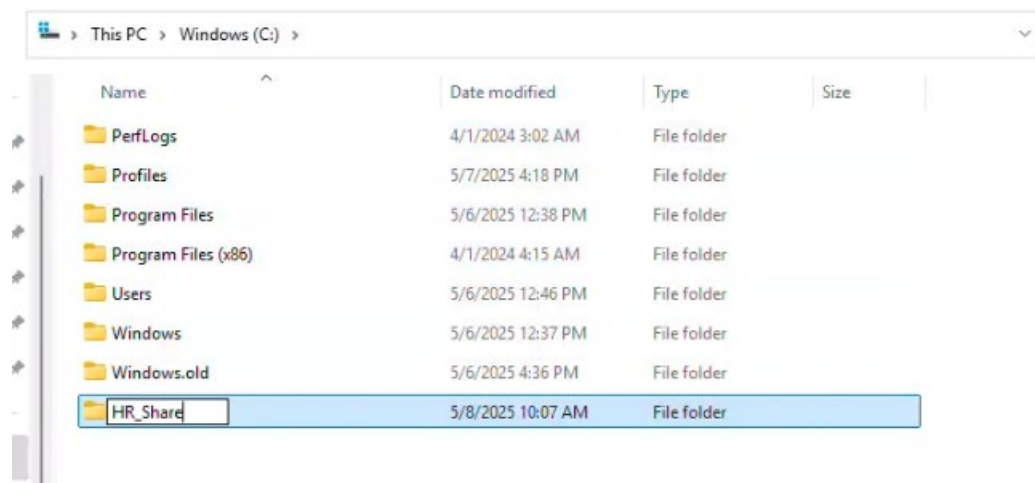
Task 5: Share and Set Permissions on SRV12

On **SRV12**, create and share a folder **C:\HR_Share** using **GUI**.

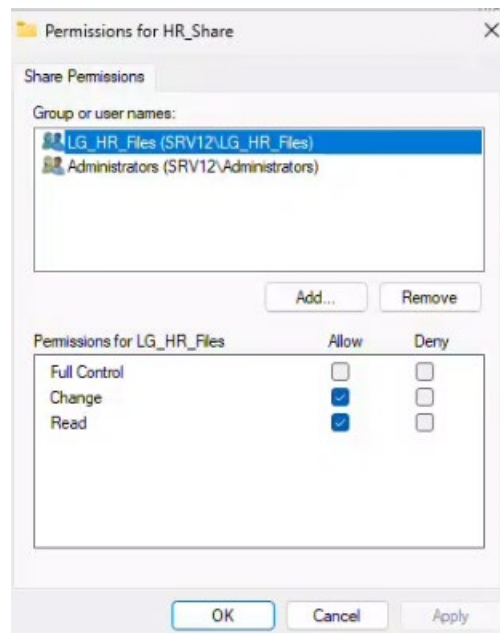
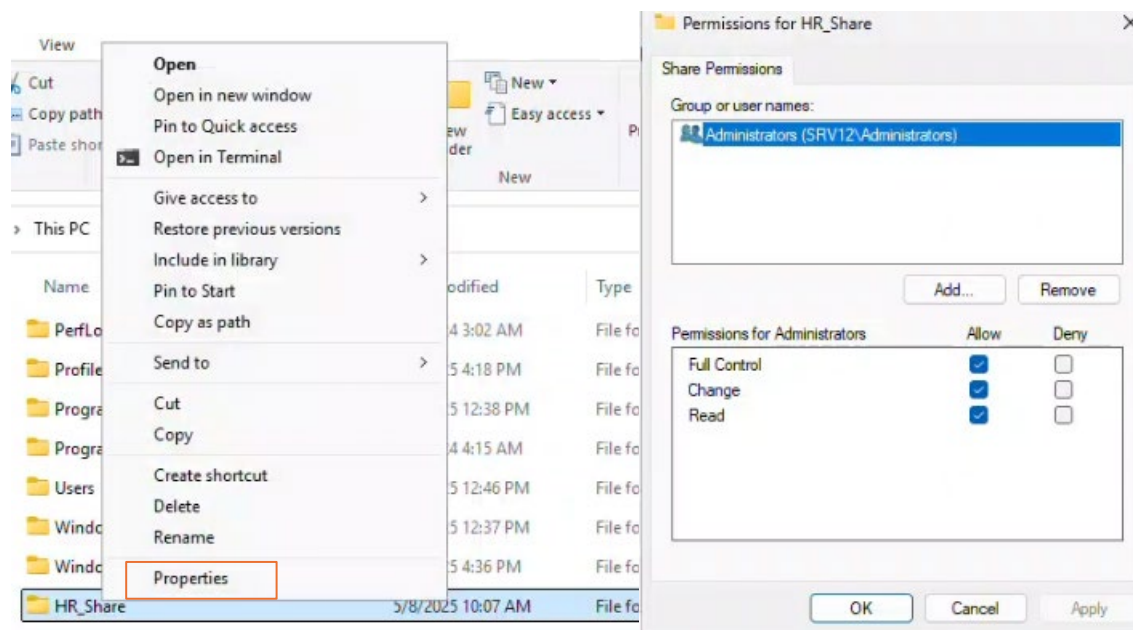
Assign **Change** permissions (Read/Write) to **LG_HR_Files** group, and remove the **Everyone** group using **GUI**.

Verify the share and permissions using **PowerShell**.

On the C: drive, right click and create the new folder HR_Share that we will use as our shared folder



Right-click and select Properties → Share and edit the permissions for specific groups. We want to give LG_HR_Files “change” permissions and we also want to remove “Everybody”

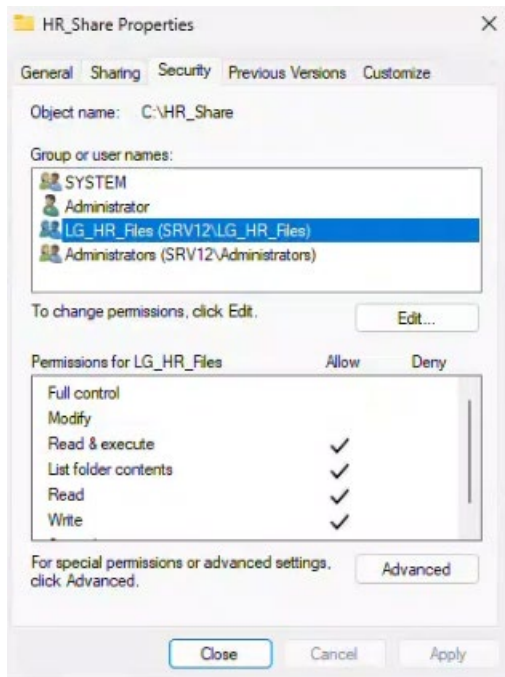


	Add
Name	Permission Level
Administrator	Read/Write ▼
Administrators	Owner
LG_HR_Files	Read/Write ▼

[I'm having trouble sharing](#)



In the Security tab, go to Edit and make sure the group, administrator and SYSTEM all have correct permissions.



Verify with PowerShell using the commands below

Get-SmbShare -Name "HR_Share"

Get-SmbShareAccess -Name "HR_Share"

Get-Acl -Path "C:\HR_Share" | Format-List

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

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

```
PS C:\Users\Administrator.VLABS12> Get-LocalGroupMember -Group "LG_HR_Files"
```

ObjectClass	Name	PrincipalSource
Group	VLABS12\DLG_HR_Share	ActiveDirectory

```
PS C:\Users\Administrator.VLABS12> Get-SmbShare -Name "HR_Share"
```

Name	ScopeName	Path	Description
HR_Share	*	C:\HR_Share	

```
PS C:\Users\Administrator.VLABS12> Get-SmbShareAccess -Name "HR_Share"
```

Name	ScopeName	AccountName	AccessControlType	AccessRight
HR_Share	*	BUILTIN\Administrators	Allow	Full

```
PS C:\Users\Administrator.VLABS12> Get-Acl -Path "C:\HR_Share" | Format-List
```

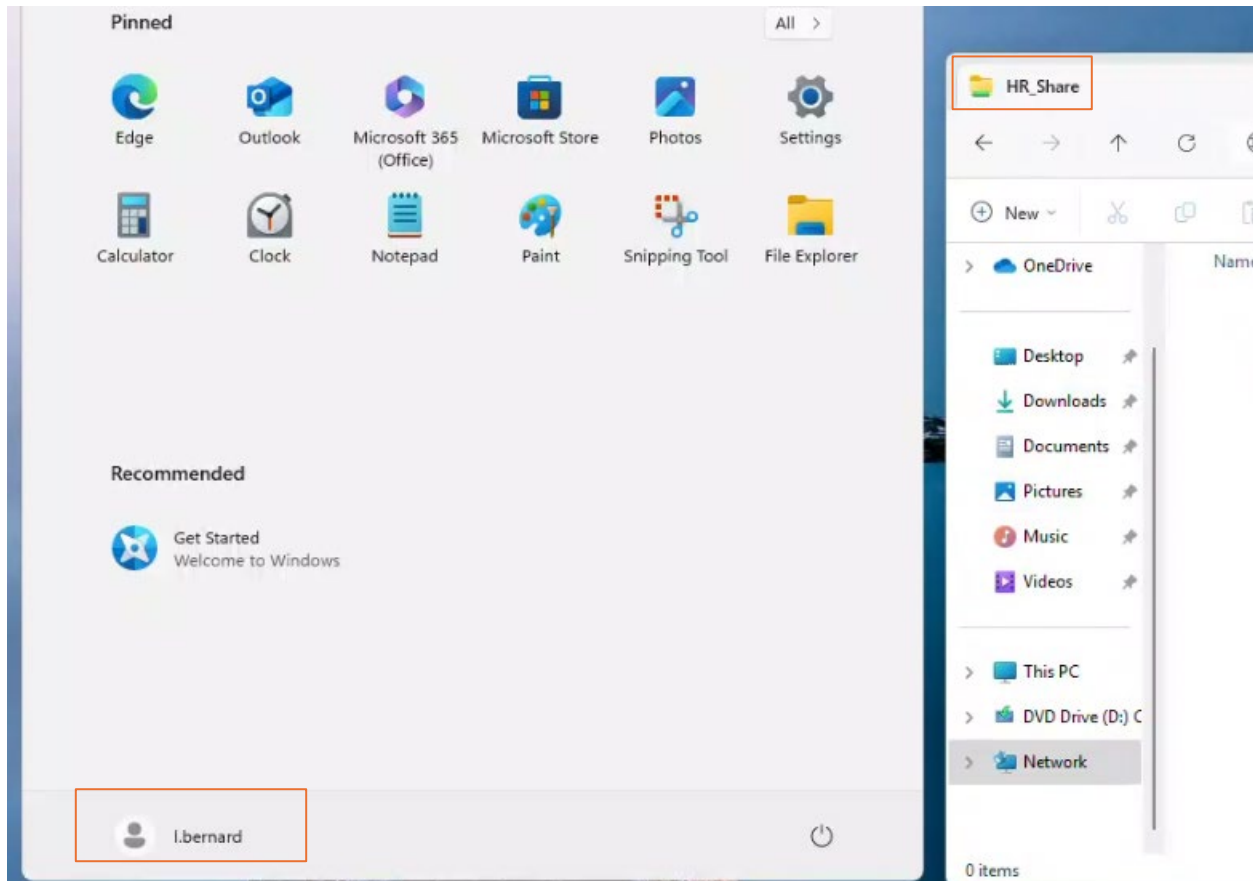
```
Path      : Microsoft.PowerShell.Core\FileSystem::C:\HR_Share
Owner     : BUILTIN\Administrators
Group     : VLABS12\Domain Users
Access    : NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators Allow FullControl
           SRV12\LG_HR_Files Allow Write, Read, Synchronize
           VLABS12\Administrator Allow FullControl
Audit     :
Sddl      : O:BAG:DUD:PAI(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICI;0x12019f;;;S-1-5-21-363679278-1750503931-45209311-1000)(A;OICI;FA;;;S-1-5-21-1463046243-397822
PS C:\Users\Administrator.VLABS12>
```

Task 6: Test HR Share Access from ClientX

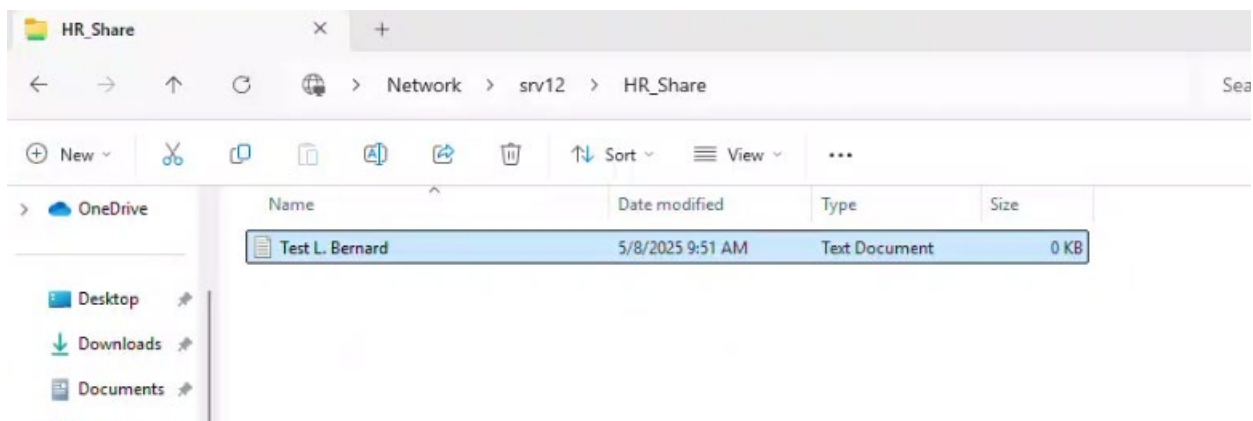
Log in as **Lucas Bernard** (l.bernard) on **Windows 11 (ClientX)**.

Access the shared folder **\\SRVXX\HR_Share\$** and verify permissions by creating and deleting files in this share.

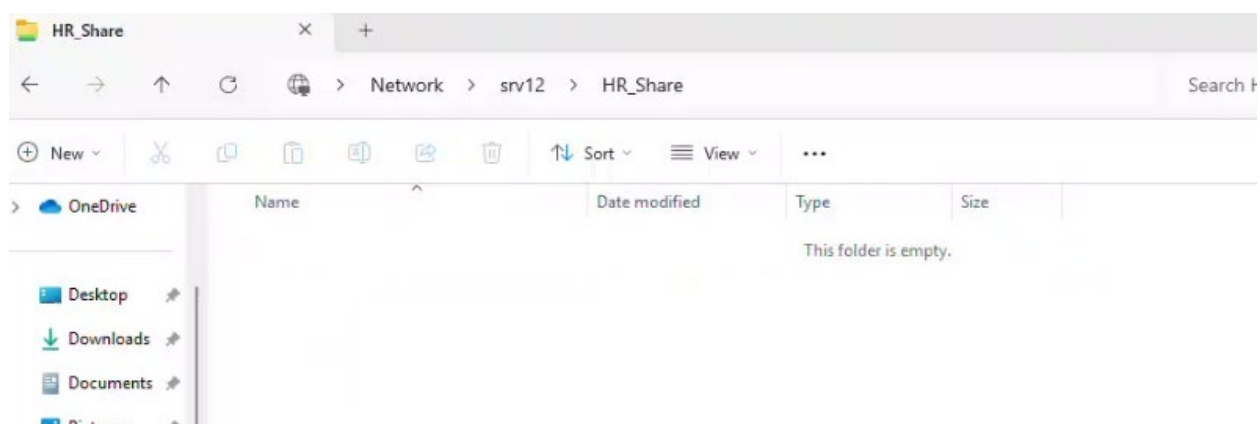
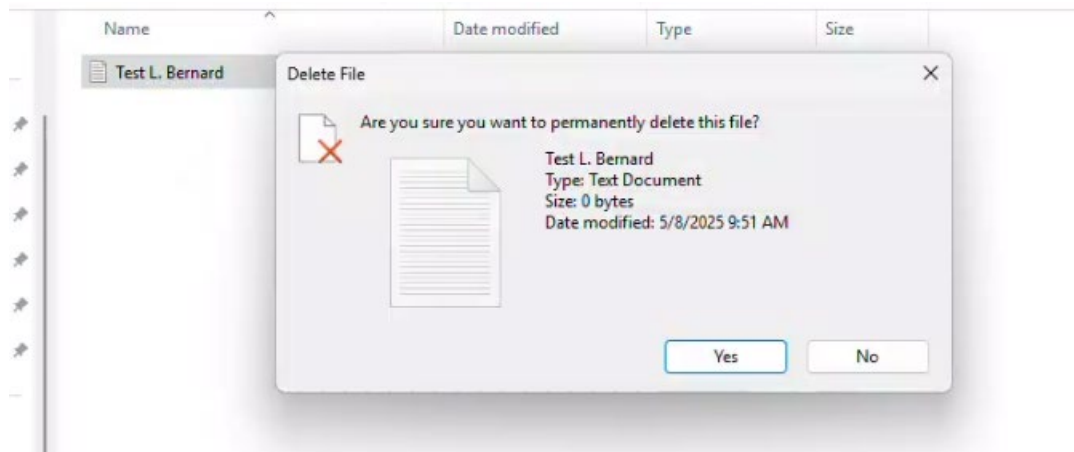
Log in as Lucas Bernard (l.bernard) on Client12 and access the HR_Share folder we just created and configured to share



Create a test file. This must work as we gave the group that Lucas is part of change permissions.



Now delete the file.



Task 7: Remove a User from a Group and Delete a User

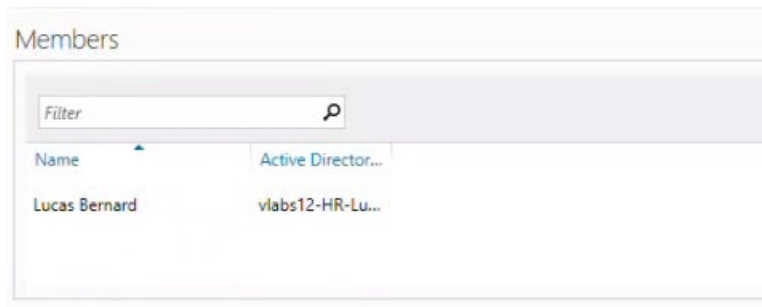
Remove Emma Morel (e.morel) from GG_HR_Admins using ADAC.

Remove Chloe Girard (c.girard) from GG_IT_Admins using PowerShell.

Remove Emma Morel from GG_HR_Admins using Active Directory Administrative Center. Scroll down to Members → select Emma Morel → Remove



Confirm only Lucas Bernard remains.



Repeat for Chloe Girard and group GG_IT_Admins on PowerShell

Remove-ADGroupMember-Identity "GG_IT_Admins" -Members "c.girard"

```
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "GG_IT_Admins"

distinguishedName : CN=Sophie Lambert,OU=IT,DC=vlabs12,DC=com
name               : Sophie Lambert
objectClass        : user
objectGUID         : 5885a491-c0db-4e89-8f9a-f841e7b00f51
SamAccountName     : s.lambert
SID                : S-1-5-21-1463046243-3978224867-743297864-1109
```

Get-ADGroupMember -Identity "GG_IT_Admins"

```
PS C:\Users\Administrator.DC112> Remove-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard"

Confirm
Are you sure you want to perform this action?
Performing the operation "Set" on target "CN=GG_IT_Admins,OU=IT,DC=vlabs12,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```

Task 8: Create IT OU and Configure Groups on DC312 and DC112

On DC312, create an OU named IT using ADAC.

Inside IT OU, create a user Fadi Tora (f.tora) using ADAC.

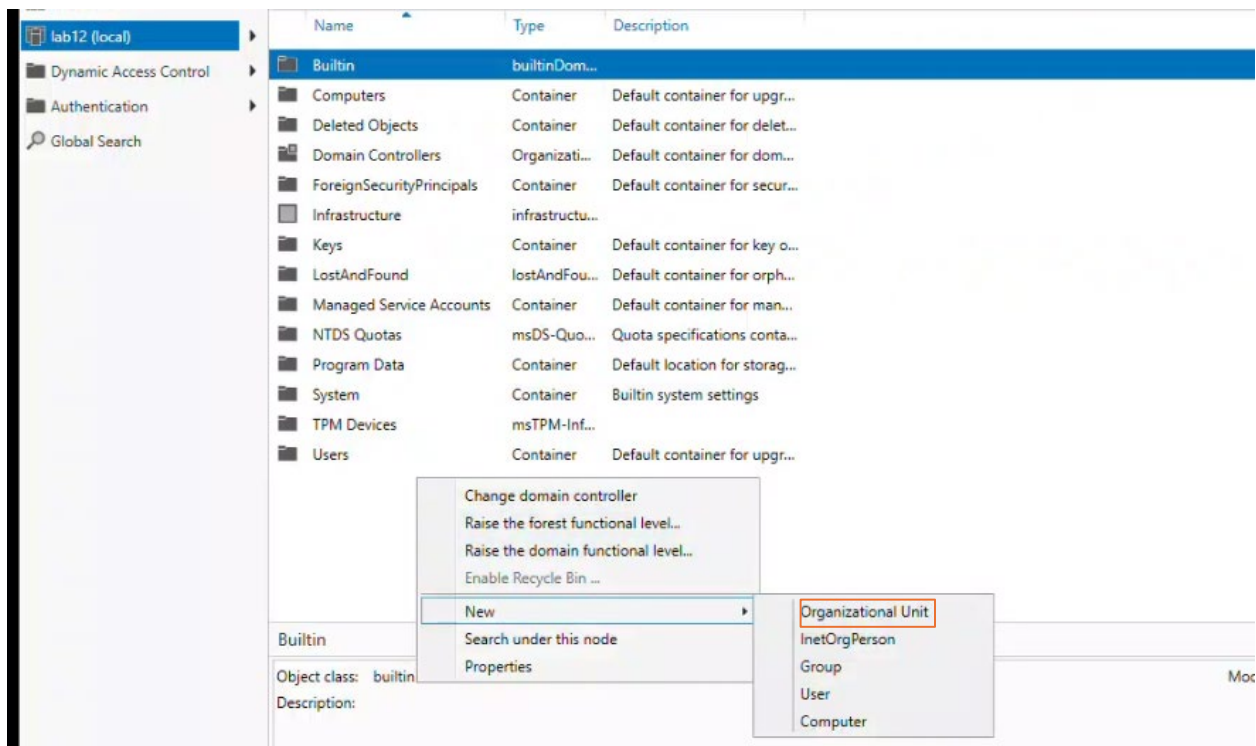
Inside IT OU, create a Global Group GG_IT_Admins and add Fadi Tora as a member using ADAC.

On DC112, create a Universal Group UG_IT_Global.

Add GG_IT_Admins from both vlabs12.com and lab12.vlabs12.com to UG_IT_Global.

Add UG_IT_Global to the Domain Local group DLG_IT_Share using PowerShell.

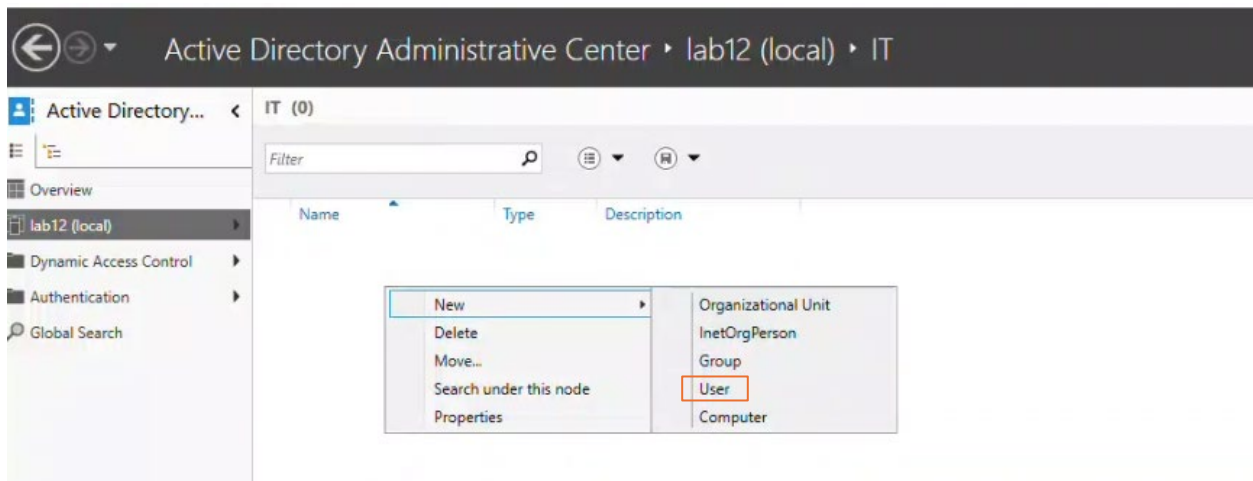
On DC312 (child domain) right click and create the OU IT



Create Organizational Unit: IT

Organizational Unit	Organizational Unit	
Managed By		
Name:	* IT	
Address:		
Street		
City	State/Province	Zip/Postal code
Country/Region:		

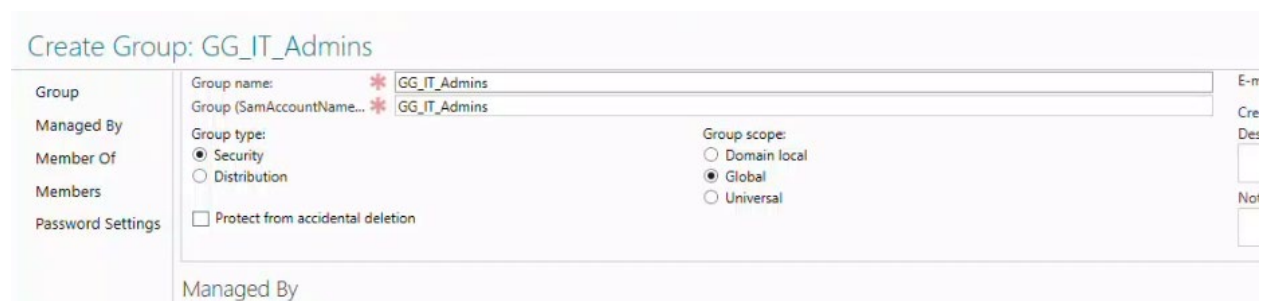
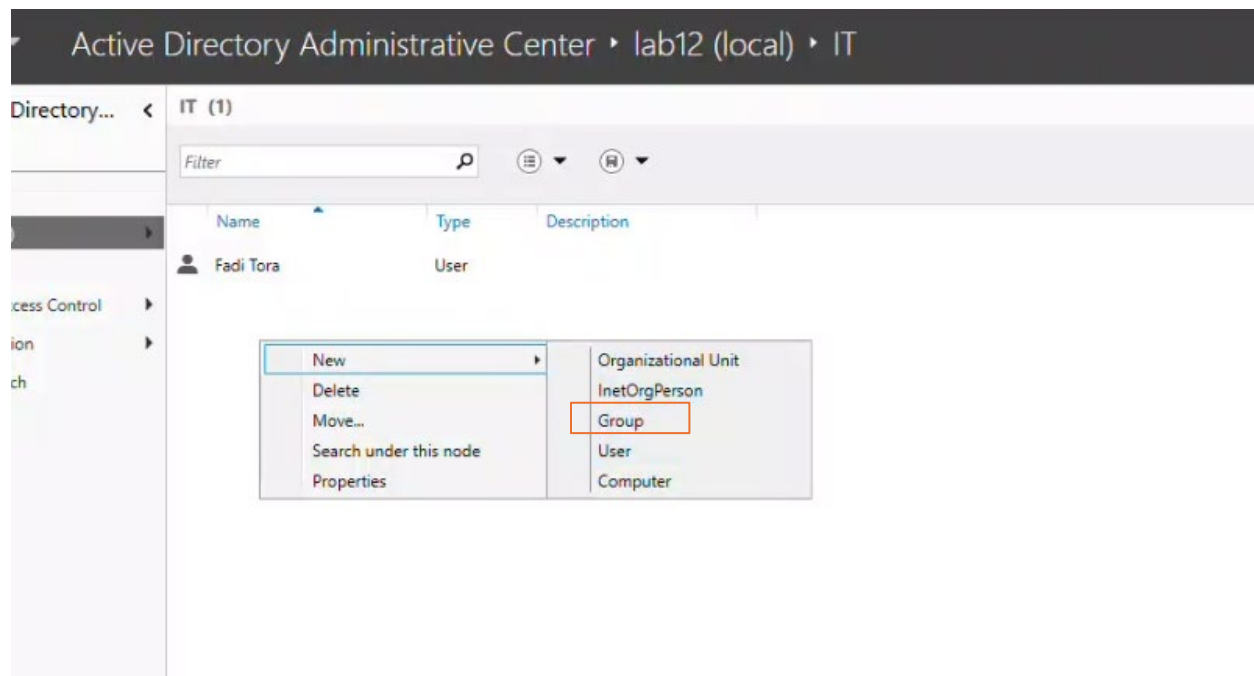
In IT, create the user Fadi Tora as usual with the UPN f.tora



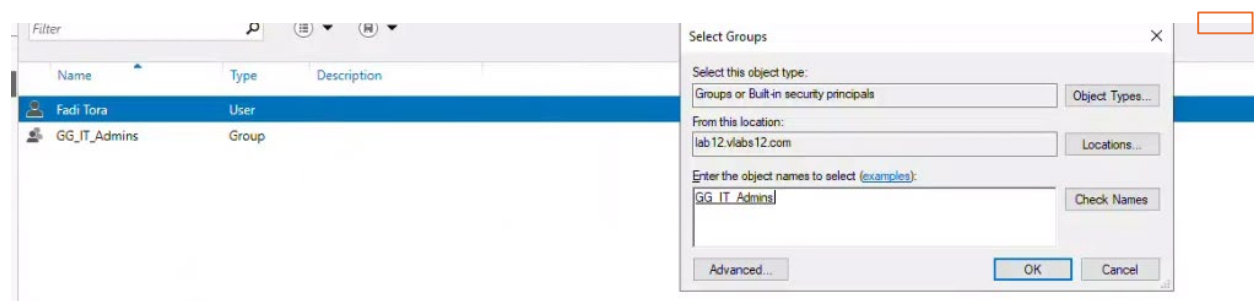
Create User: Fadi Tora

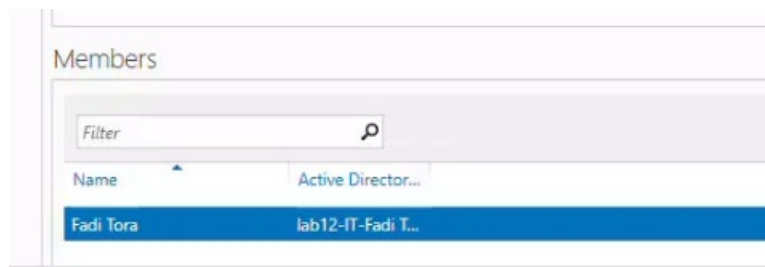
Account	Account	
Organization		
Member Of		
First name:	Fadi	Account expires:
Middle initials:		<input checked="" type="radio"/> Never
Last name:	Tora	<input type="radio"/> End of <input type="text"/>
Full name:	* Fadi Tora	Password options:
User UPN logon:	f.tora @ lab12.vlabs12.com	<input type="radio"/> User must change password at next log on
User SamAccountName lo...:	lab12 * f.tora	<input checked="" type="radio"/> Other password options
Password:	*****	<input type="checkbox"/> Microsoft Passport or smart card is required for interactive log on
Confirm password:	*****	<input checked="" type="checkbox"/> Password never expires
Create in: OU=IT,DC=lab12,DC=vlabs12,DC=com	Change...	<input type="checkbox"/> User cannot change password
<input type="checkbox"/> Protect from accidental deletion		Encryption options:
Log on hours...	Log on to...	Other options:

Create the Global group GG_IT_Admins

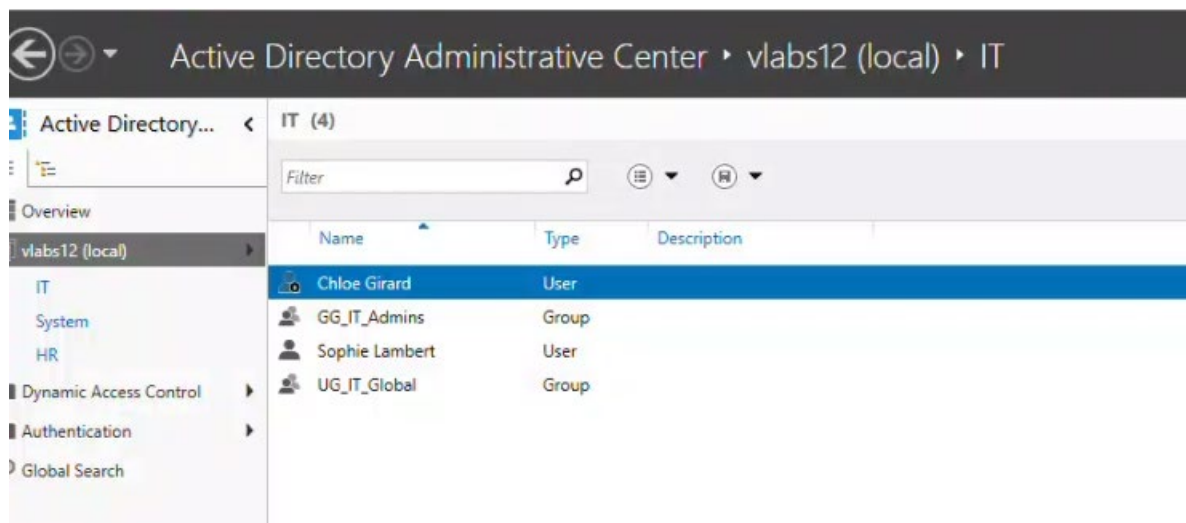
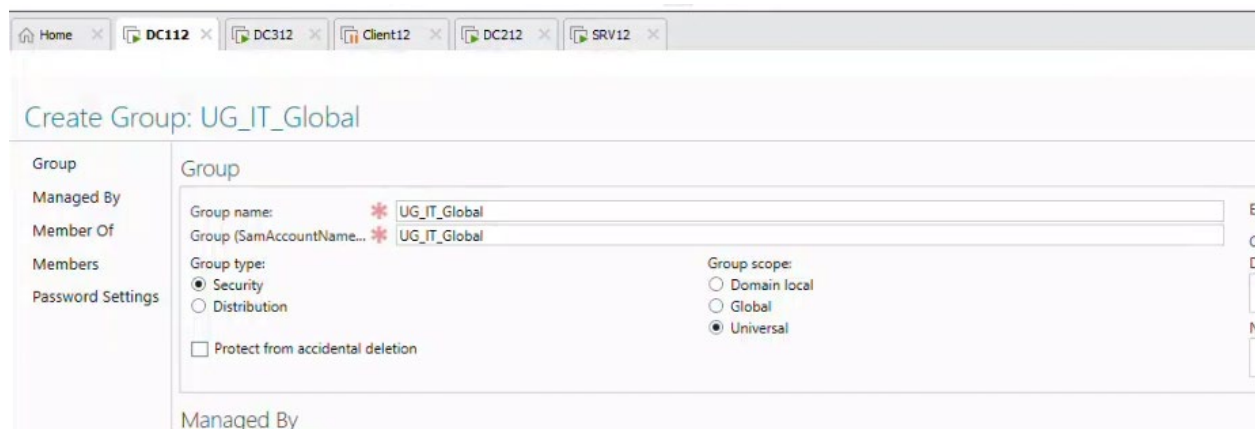


Add Fadi Tora by right clicking on his name → Add to group → GGT_IT_Admins



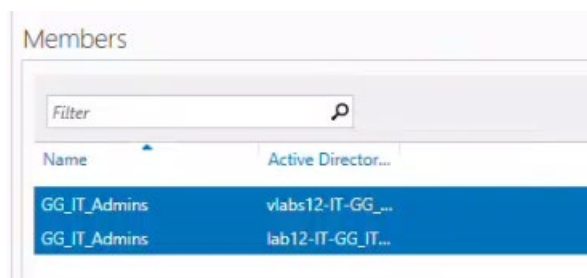
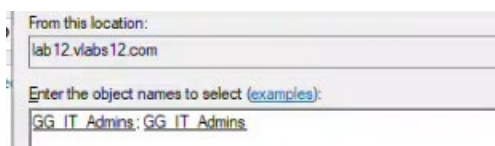
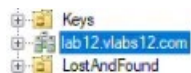
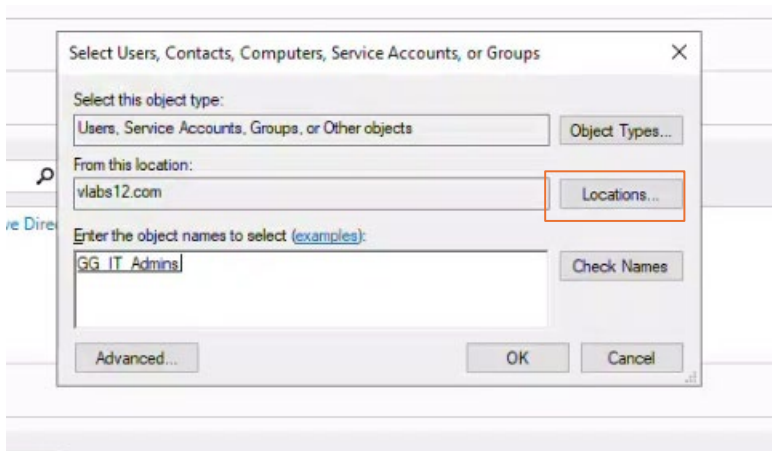


On DC112, create the Universal group UG_IT_Global



We want to add as members both Global groups GG_IT_Admins from domain vlabs12 and lab12.vlabs12.com

Click on Add in the Members section and add the first GG_IT_Admins from vlabs12, then click on Locations and switch to lab12.vlabs12. Add the GG_IT_Admins group from that domain also.



Add UG_IT_Global to the Domain Local group DLG_IT_Share using PowerShell.

```
PS C:\Users\Administrator.DC112> Add-ADGroupMember -Identity "DLG_IT_Share" -Members "UG_IT_Global"
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
```

```
PS C:\Users\Administrator.DC112> Get-ADGroupMember -Identity "DLG_IT_Share"
```

```
distinguishedName : CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com
name               : UG_IT_Global
objectClass        : group
objectGUID         : 2d35ec92-c3b6-4385-994b-9ce560080376
SamAccountName     : UG_IT_Global
SID                : S-1-5-21-1463046243-3978224867-743297864-1123

distinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs12,DC=com
name               : GG_IT_Admins
objectClass        : group
objectGUID         : f17e7bce-fdd1-4443-ba67-23a1449d6aec
SamAccountName     : GG_IT_Admins
SID                : S-1-5-21-1463046243-3978224867-743297864-1117
```

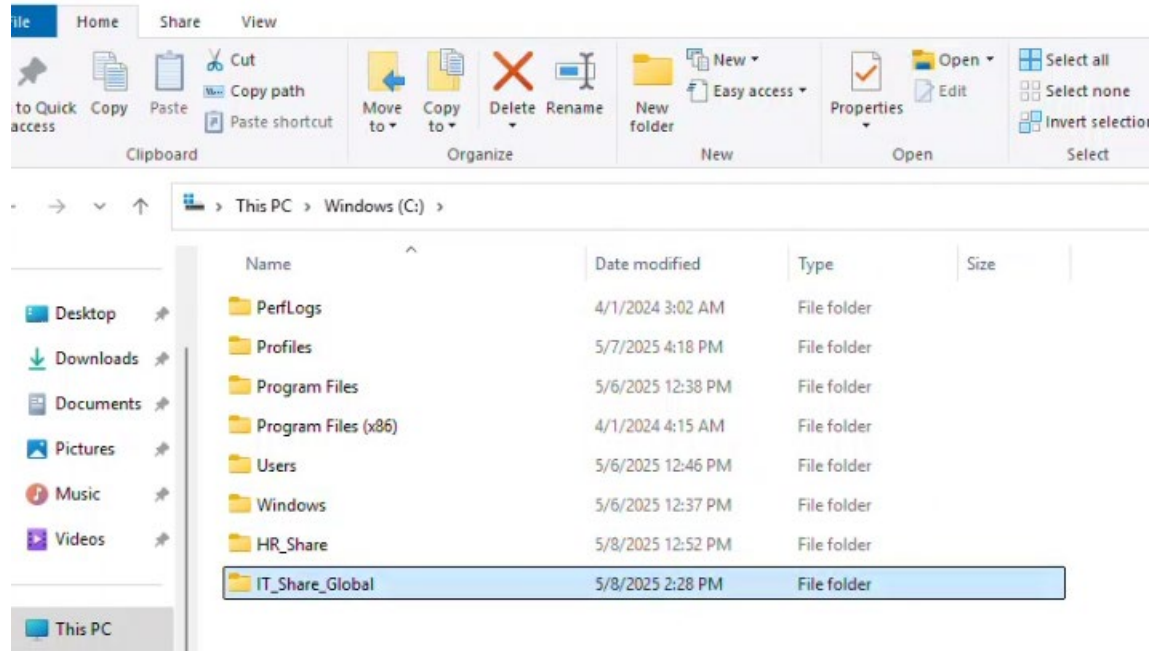
Task 9: Share and Set Permissions for IT Global Share

On SRV12, create and share **C:\IT_Share_Global** using GUI.

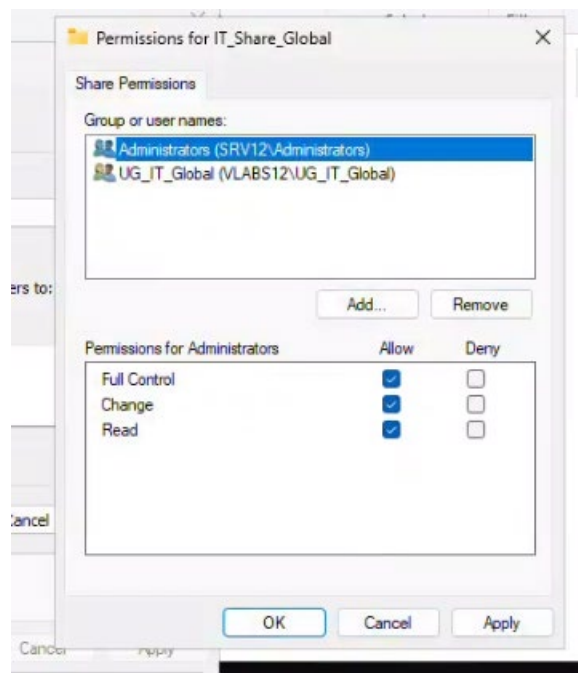
Assign Change permissions (Read/Write) to **UG_IT_Global** group, and remove the Everyone group using GUI.

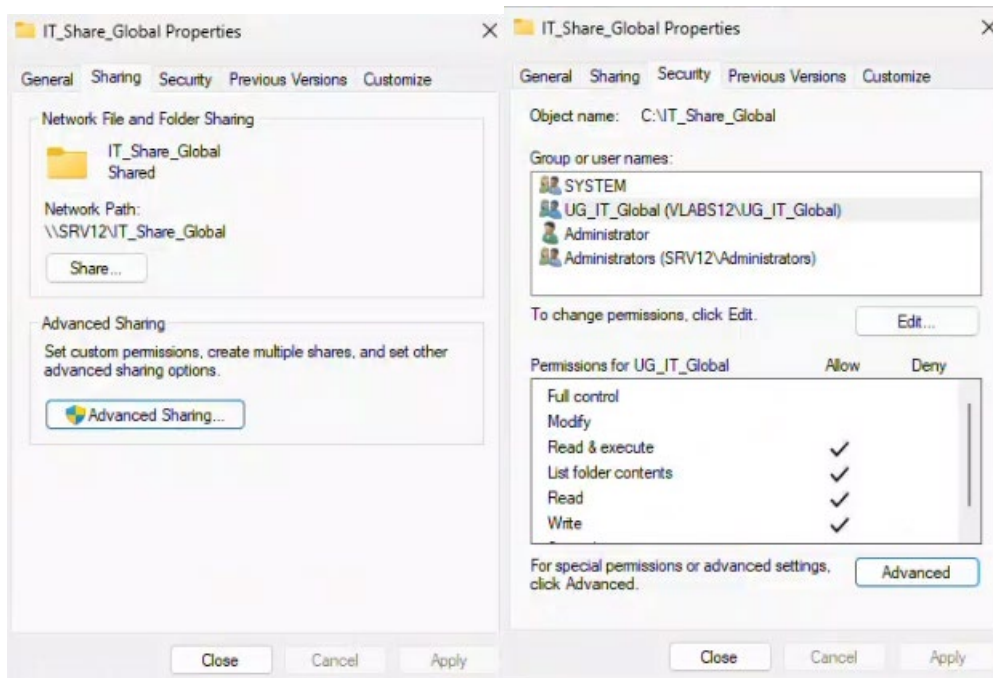
Verify the share and permissions using **PowerShell**.

Like what was done for HR_Share in the previous task, create IT_Share_Global on the SRV12 C: drive



Set the appropriate permissions, which are the same as the previous task.





Confirm the permissions using PowerShell:

```
PS C:\Users\Administrator.VLABS12> Get-SmbShareAccess -Name "IT_Share_Global"

Name          ScopeName AccountName      AccessControlType AccessRight
-----
IT_Share_Global *      BUILTIN\Administrators Allow             Full
IT_Share_Global *      VLABS12\UG_IT_Global Allow             Change

PS C:\Users\Administrator.VLABS12> |
```

Task 10: Test IT Share Access from ClientX

Log in as **Fadi Tora (f.tora)** on Windows 11 (Client12).

Check which groups Fadi Tora is a member of using Command Prompt.

Access the shared folder **\\SRVXX\IT_Share_Global\$** and verify permissions by creating and deleting files in this share.

Log in as Fadi Tora and use CMD to see which groups he's a member of. Enter “whoami /groups”

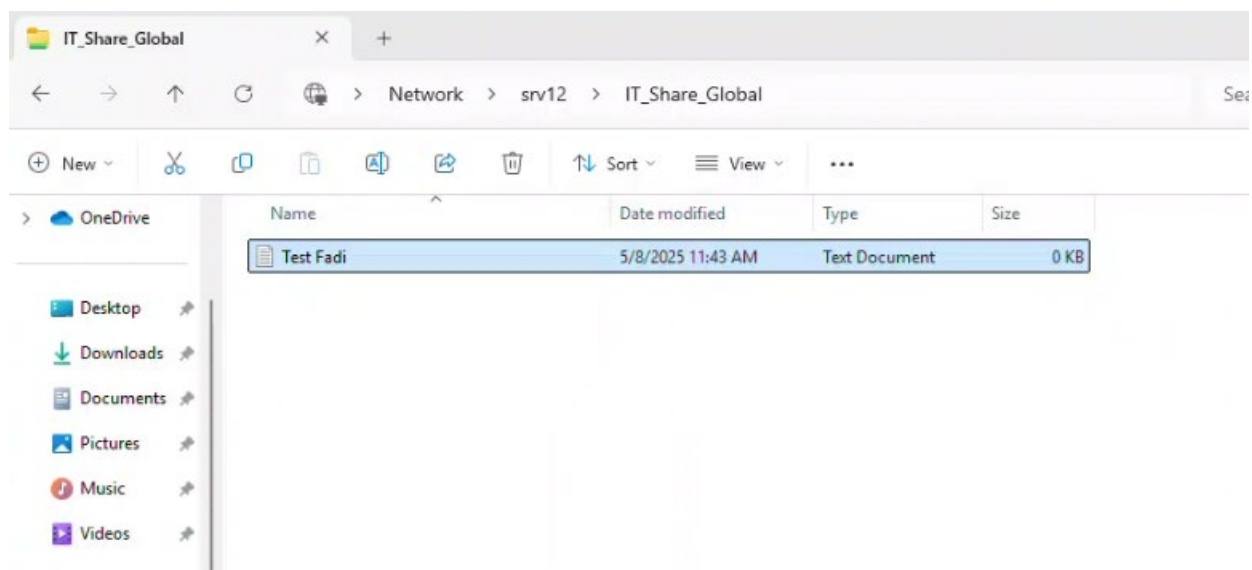
```
C:\Users\f.tora>whoami /groups

GROUP INFORMATION

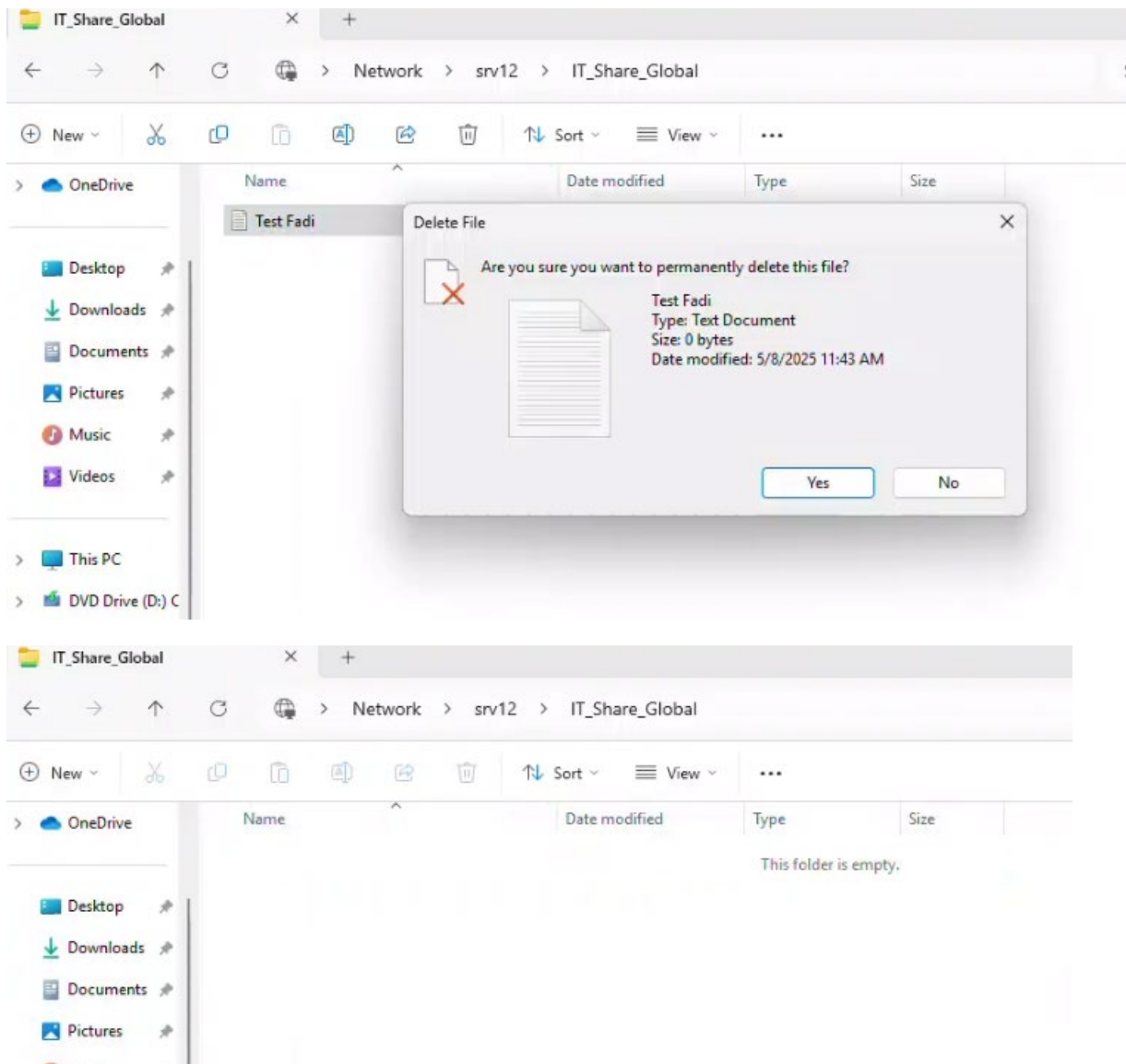
=====
Group Name                                     Type                SID                                     Attributes
=====
Everyone                                     Well-known group    S-1-1-0                               Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias               S-1-5-32-545                          Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                    Well-known group    S-1-5-4                                Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group    S-1-2-1                                Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group    S-1-5-11                               Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group    S-1-5-15                               Mandatory group, Enabled by default, Enabled group
LOCAL                                       Well-known group    S-1-2-0                                Mandatory group, Enabled by default, Enabled group
LAB12\GG_IT_Admins                         Group               S-1-5-21-634356128-4104644875-2871570820-1105 Mandatory group, Enabled by default, Enabled group
VLABS12\UG_IT_Global                       Group               S-1-5-21-1463046243-3978224867-743297864-1123 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group    S-1-18-1                               Mandatory group, Enabled by default, Enabled group
VLABS12\DLG_IT_Share                       Alias               S-1-5-21-1463046243-3978224867-743297864-1128 Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level     Label               S-1-16-8192                           Mandatory group, Enabled by default, Enabled group, Local Group

C:\Users\f.tora\
```

Go to the [\\SRV12\IT_Share_Global](#) folder and create a test file.



Delete the test file



Task 11: Change Group Scope

1. On DC1XX, convert UG_IT_Global from Universal to Global using PowerShell.
2. Verify that the group scope has changed correctly using GUI.

Since Global groups cannot have cross-domain users, we have to remove membership from lab12.vlabs12.com before converting

The screenshot shows the 'Member Of' and 'Members' sections of the Active Directory group properties for 'UG_IT_Global'. The 'Member Of' section lists 'vlab12-Share' and the 'Members' section lists 'vlab12-IT-GS...'. Below these sections, a PowerShell command is executed in a terminal window:

```
PS C:\Users\Administrator.DC112> Set-ADGroup -GroupScope:"Global" -Identity:"CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com"
Set-ADGroup : A global group cannot have a cross-domain member
At line:1 char:1
+ Set-ADGroup -GroupScope:"Global" -Identity:"CN=UG_IT_Global,OU=IT,DC= ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com:ADGroup) [Set-ADGroup], ADException
+ FullyQualifiedErrorId : ActiveDirectoryServer:8519,Microsoft.ActiveDirectory.Management.Commands.SetADGroup

PS C:\Users\Administrator.DC112> Set-ADGroup -GroupScope:"Global" -Identity:"CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com"
PS C:\Users\Administrator.DC112>
PS C:\Users\Administrator.DC112>
```

Conversion from Universal to Global successful.

The screenshot shows the 'UG_IT_Global' group properties in Active Directory. The 'Group' tab is selected, and the 'Group scope' is set to 'Global' (indicated by a red box around the 'Global' radio button). The 'Group name' is 'UG_IT_Global' and the 'Group (SamAccountName)' is 'UG_IT_Global'. The 'Group type' is 'Security'. The 'Managed By' section shows the manager's name and contact information. The 'E-mail' field is empty. The 'Description' field is empty. The 'Notes' field is empty.

```
PS C:\Users\Administrator.DC112> Get-ADGroup -Identity:"CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com"
```

```
DistinguishedName : CN=UG_IT_Global,OU=IT,DC=vlabs12,DC=com
GroupCategory      : Security
GroupScope         : Global
Name               : UG_IT_Global
ObjectClass        : group
ObjectGUID         : 2d35ec92-c3b6-4385-994b-9ce560080376
SamAccountName     : UG_IT_Global
SID                : S-1-5-21-1463046243-3978224867-743297864-1123
```

```
PS C:\Users\Administrator.DC112>
```