This lab will help you practice managing Active Directory groups using Active Directory Administrative Center (ADAC) and PowerShell

Lab 5 - Managing Group Accounts in Active Directory

420-636-AB-Network Installation and Administration II

Teacher: Antoine Tohme
Student: Monica Perez Mata
Student id : 2498056

Table of Contents

Lab 5 - Managing Group Accounts in Active Directory

1 Introduction

1.1 Objective

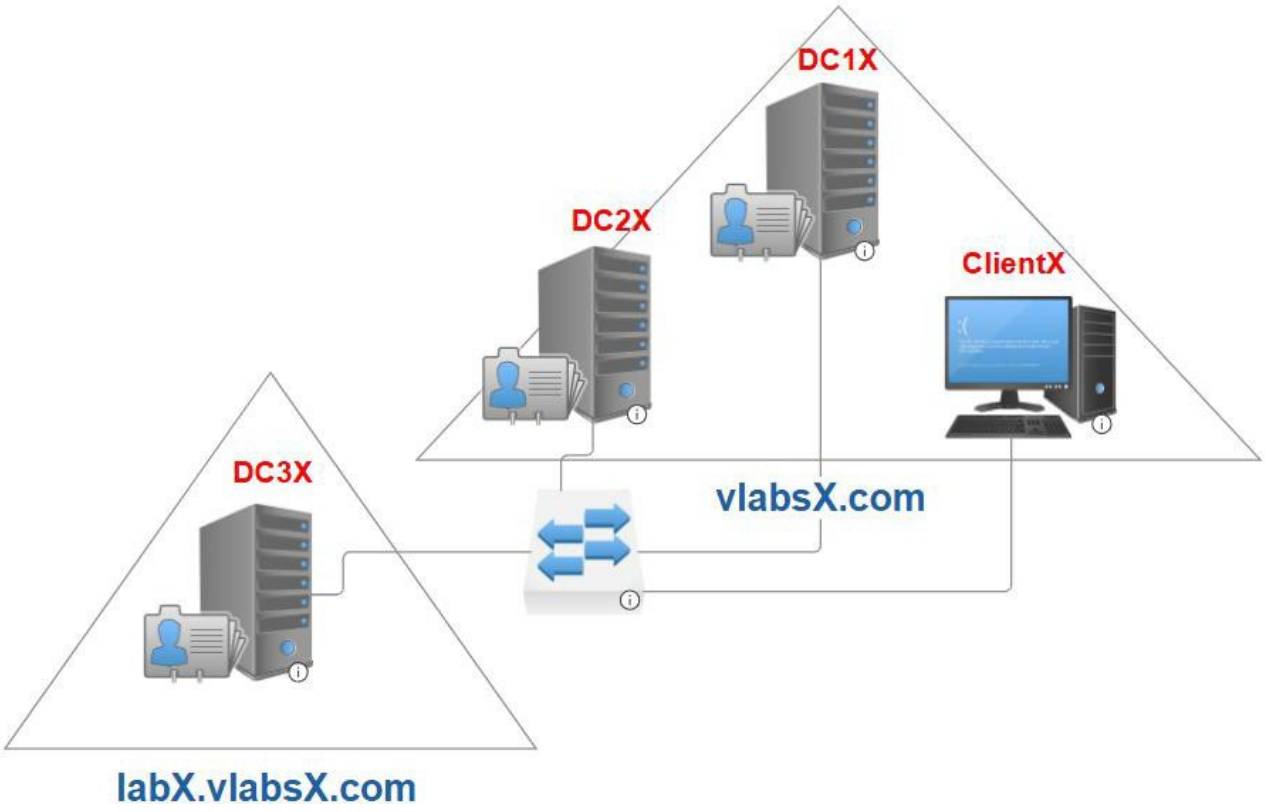
This lab will help you practice managing Active Directory groups using Active Directory Administrative Center (ADAC) and PowerShell.

You will perform tasks related to group creation, membership management, delegation, and permission assignments.

1.2 Lab Requirements

- Domain Name: vlabs1.com
- Servers:
    - DC101 (Windows Server 2022, Primary DC for vlabs1.com)
    - DC301 (Windows Server 2022, Child DC for lab1.vlabs1.com)
    - SRV01 (Windows Server 2025, File Server for shared resources)
- Client Machine: Windows 11 (Client1, domain-joined)

2 Topology



3 Task 1: Create and Manage Security Groups

3.1 Requirements

1. Create a **Global Security Group (GG_HR_Admins)** in the **HR** OU using **ADAC.**
2. Create a **Global Security Group (GG_IT_Admins)** in the **IT** OU using **PowerShell**.

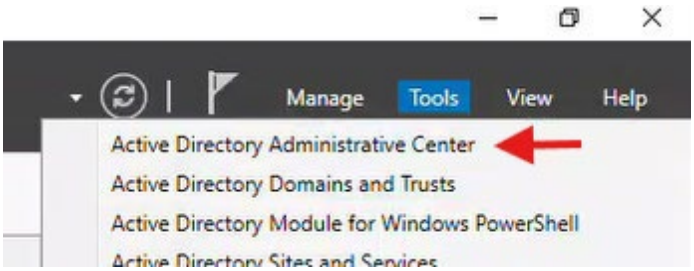
Actions (Commands and GUI) executed in DC101

3.2 Create a Global Security Group using ADAC

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

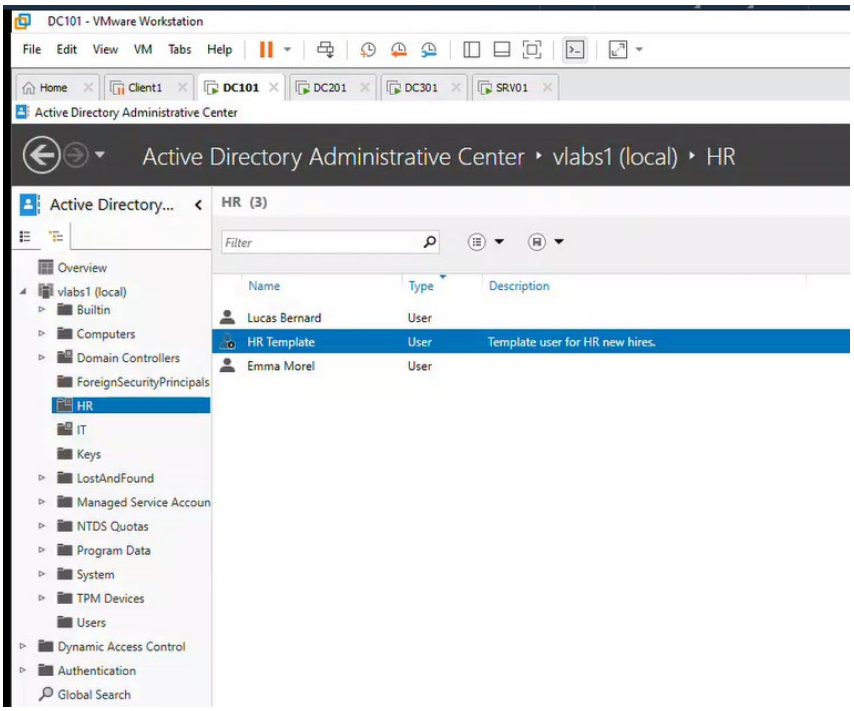
3.2.1 Verify OU and Group Existence

1. Open ADAC on DC101.



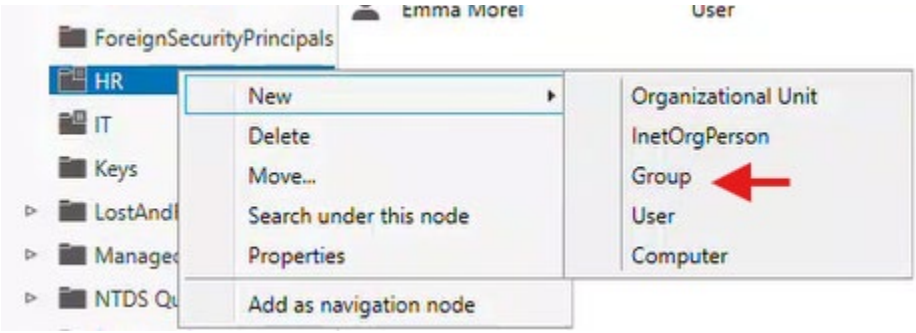
2. Navigate to HR OU under vlabs1.com.

3. Confirm the HR OU exists, and that GG_HR_Admins is not already present.



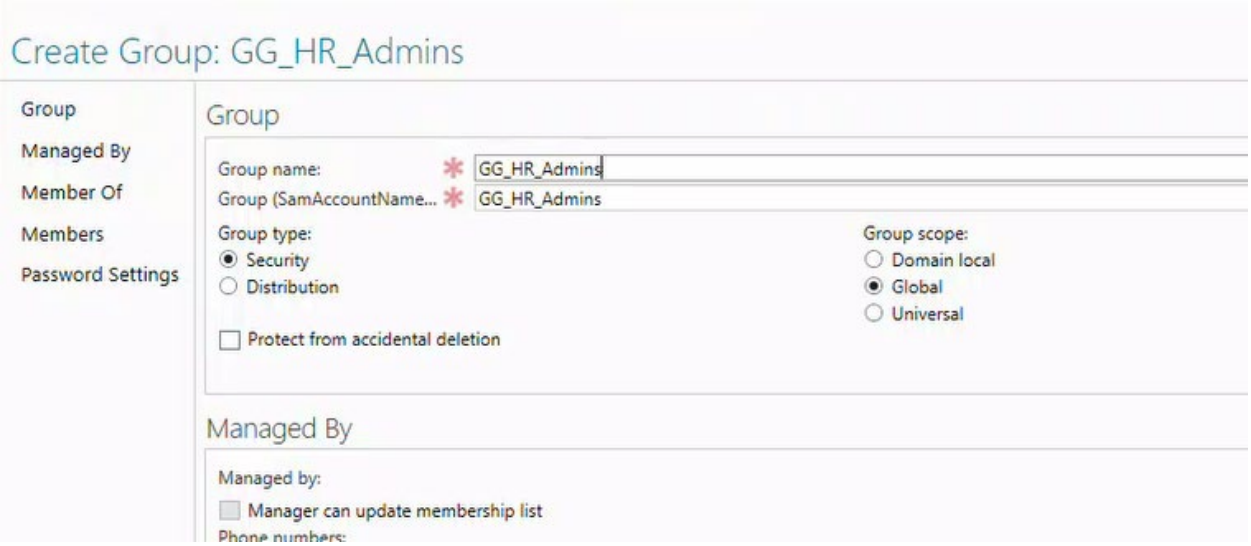
3.2.2 Create the Group:

1. In ADAC, right-click the HR OU > New > Group.



2. Configure:

- Group name: GG_HR_Admins
- Group scope: Global
- Group type: Security

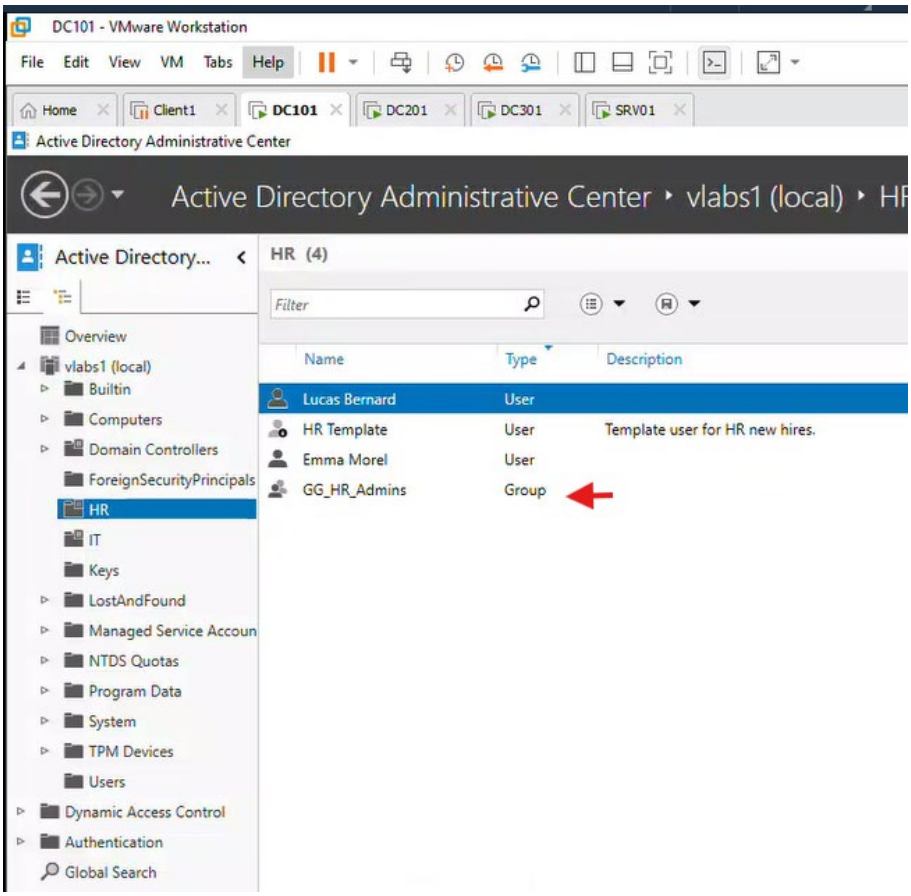


3. Click OK.

3.2.3 Verify Group Creation

Refresh the HR OU in ADAC.

Confirm GG_HR_Admins appears in the list of groups.



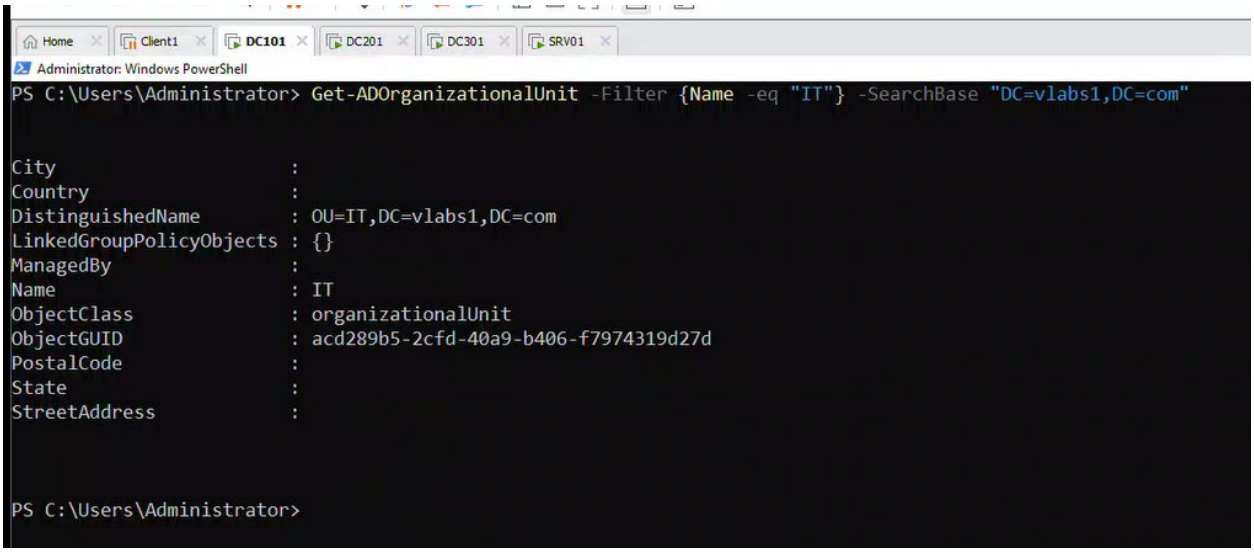
3.3 Create a Global Security Group using PowerShell

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

3.3.1 Verify OU and Group Existence

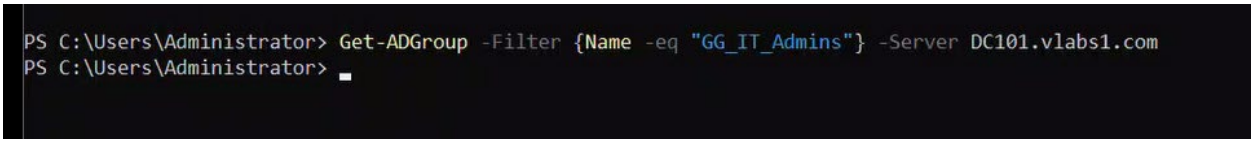
1. Check if the IT OU exists (ensure the correct path):

```
Get-ADOrganizationalUnit -Filter {Name -eq "IT"} -SearchBase "DC=vlabs1,DC=com"
```



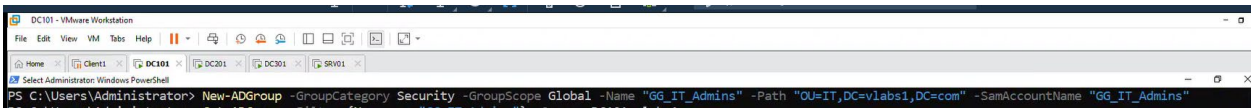
2. Check if group exists

Get-ADGroup -Filter {Name -eq "GG_IT_Admins"} -Server DC101.vlabs1.com



3.3.2 Create the Group

New-ADGroup -GroupCategory Security -GroupScope Global -Name "GG_IT_Admins" -Path "OU=IT,DC=vlabs1,DC=com" -SamAccountName "GG_IT_Admins"



3.3.3 Verify Group Creation

Get-ADGroup -Identity "GG_IT_Admins" -Properties * |
Select-Object Name, SamAccountName, GroupScope, GroupCategory, DistinguishedName

```
PS C:\Users\Administrator> Get-ADGroup -Identity "GG_IT_Admins" -Properties * |
>>   Select-Object Name, SamAccountName, GroupScope, GroupCategory, DistinguishedName


Name              : GG_IT_Admins
SamAccountName    : GG_IT_Admins
GroupScope        : Global
GroupCategory     : Security
DistinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs1,DC=com



PS C:\Users\Administrator>
```

Get-ADGroup -Filter {Name -eq "GG_IT_Admins"} -Server DC101.vlabs1.com

```
PS C:\Users\Administrator> Get-ADGroup -Filter {Name -eq "GG_IT_Admins"} -Server DC101.vlabs1.com


DistinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : GG_IT_Admins
ObjectClass       : group
ObjectGUID        : 99c47997-bc7c-46f0-95f2-330e7d0066ac
SamAccountName    : GG_IT_Admins
SID               : S-1-5-21-1268601764-4050707287-4025116504-1117
```

4 Task 2: Add Members to Groups

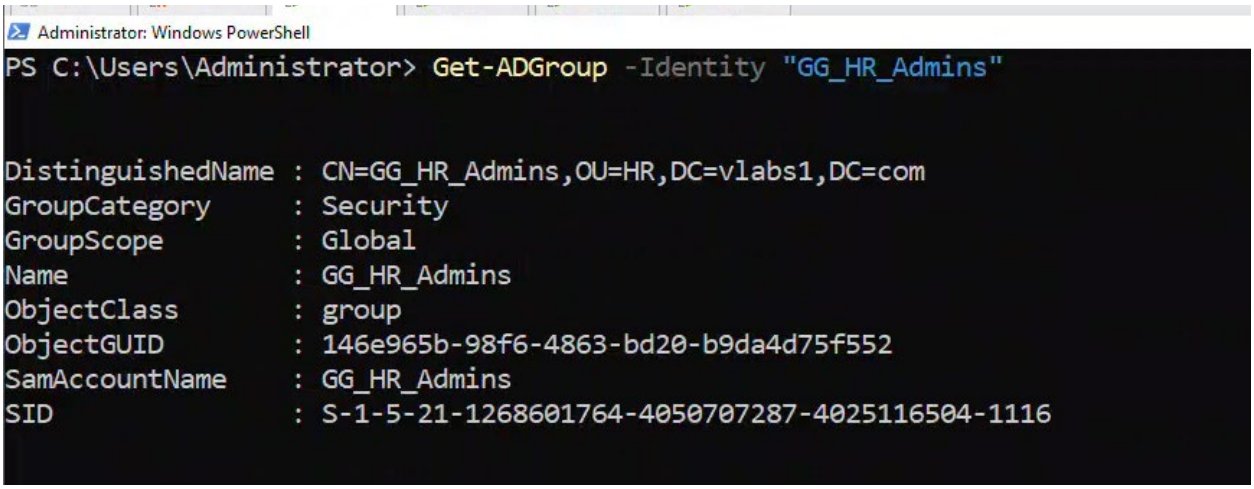
4.1 Requirements

1. Add Emma Morel (e.morel) and Lucas Bernard (l.bernard) to GG_HR_Admins using PowerShell.
2. Add Chloe Girard (c.girard) and Sophie Lambert (s.lambert) to GG_IT_Admins using PowerShell.

4.1.1 Add members to GG_HR_Admins

1. Verify the group exists:

Get-ADGroup -Identity "GG_HR_Admins"



2. Verify the users exists:
   # Check Emma Morel (e.morel)
   Get-ADUser -Identity "e.morel" -Properties SamAccountName, DistinguishedName

   # Check Lucas Bernard (l.bernard)
   Get-ADUser -Identity "l.bernard" -Properties SamAccountName, DistinguishedName

```
PS C:\Users\Administrator> # Check Emma Morel (e.morel)
PS C:\Users\Administrator> Get-ADUser -Identity "e.morel" -Properties SamAccountName, DistinguishedName


DistinguishedName : CN=Emma Morel,OU=HR,DC=vlabs1,DC=com
Enabled           : True
GivenName         : Emma
Name              : Emma Morel
ObjectClass       : user
ObjectGUID        : aa24e520-c241-450c-be23-81f23faa4280
SamAccountName    : e.morel
SID               : S-1-5-21-1268601764-4050707287-4025116504-1110
Surname           : Morel
UserPrincipalName : e.morel@vlabs1.com



PS C:\Users\Administrator> # Check Lucas Bernard (l.bernard)
PS C:\Users\Administrator> Get-ADUser -Identity "l.bernard" -Properties SamAccountName, DistinguishedName


DistinguishedName : CN=Lucas Bernard,OU=HR,DC=vlabs1,DC=com
Enabled           : True
GivenName         : Lucas
Name              : Lucas Bernard
ObjectClass       : user
ObjectGUID        : 462e363e-a981-48ce-a06b-b65ed393a058
SamAccountName    : l.bernard
SID               : S-1-5-21-1268601764-4050707287-4025116504-1111
Surname           : Bernard
UserPrincipalName : l.bernard@vlabs1.com
```

3. Add Members via PowerShell:

   Add-ADGroupMember -Identity "GG_HR_Admins" -Members "e.morel", "l.bernard"

4. Confirm e.morel and l.bernard appear in the list

   Get-ADGroupMember -Identity "GG_HR_Admins" | Select-Object Name, SamAccountName

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-ADGroupMember -Identity "GG_HR_Admins" -Members "e.morel", "l.bernard"
PS C:\Users\Administrator> Get-ADGroupMember -Identity "GG_HR_Admins" | Select-Object Name, SamAccountName

Name          SamAccountName
----          --------------
Emma Morel    e.morel
Lucas Bernard l.bernard


PS C:\Users\Administrator>
```

   Get-ADGroupMember -Identity "GG_HR_Admins"

```
PS C:\Users\Administrator> Get-ADGroupMember -Identity "GG_HR_Admins"


distinguishedName : CN=Emma Morel,OU=HR,DC=vlabs1,DC=com
name              : Emma Morel
objectClass       : user
objectGUID        : aa24e520-c241-450c-be23-81f23faa4280
SamAccountName    : e.morel
SID               : S-1-5-21-1268601764-4050707287-4025116504-1110

distinguishedName : CN=Lucas Bernard,OU=HR,DC=vlabs1,DC=com
name              : Lucas Bernard
objectClass       : user
objectGUID        : 462e363e-a981-48ce-a06b-b65ed393a058
SamAccountName    : l.bernard
SID               : S-1-5-21-1268601764-4050707287-4025116504-1111



PS C:\Users\Administrator>
```

4.1.2 Add members to GG_IT_Admins

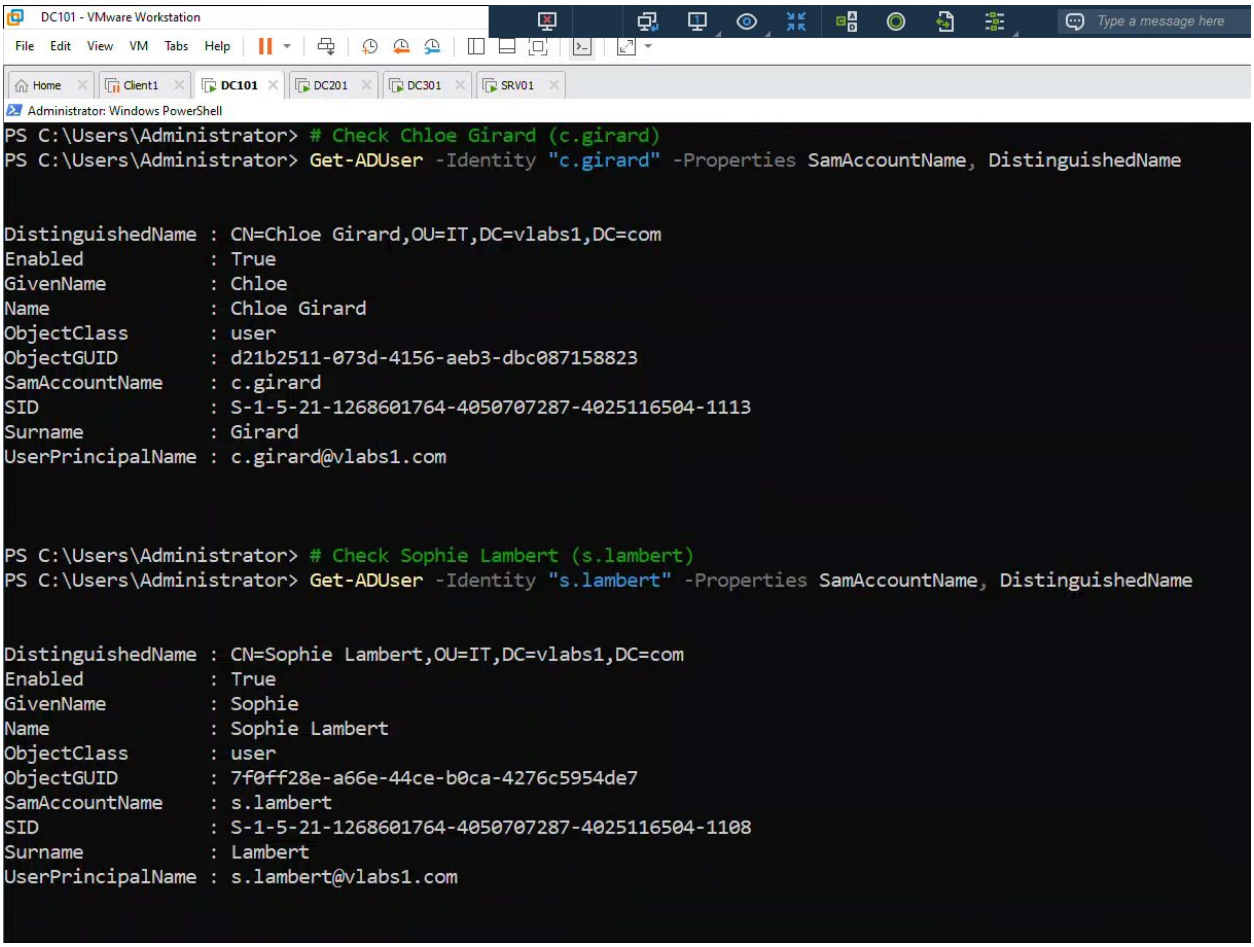
1. Verify the group exists:

   Get-ADGroup -Identity "GG_IT_Admins"

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroup -Identity "GG_IT_Admins"


DistinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : GG_IT_Admins
ObjectClass       : group
ObjectGUID        : 99c47997-bc7c-46f0-95f2-330e7d0066ac
SamAccountName    : GG_IT_Admins
SID               : S-1-5-21-1268601764-4050707287-4025116504-1117



PS C:\Users\Administrator>
```

2. Verify the users exists:

```
# Check Chloe Girard (c.girard)
Get-ADUser -Identity "c.girard" -Properties SamAccountName,
DistinguishedName

# Check Sophie Lambert (s.lambert)
Get-ADUser -Identity "s.lambert" -Properties SamAccountName,
DistinguishedName
```



3. Add Members via PowerShell:

```
Add-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard ", "
s.lambert "
```

4. Confirm e.morel and l.bernard appear in the list

   Get-ADGroupMember -Identity "GG_IT_Admins" | Select-Object Name, SamAccountName

   Get-ADGroupMember -Identity "GG_IT_Admins"

```
PS C:\Users\Administrator> Add-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard", "s.lambert"
PS C:\Users\Administrator> Get-ADGroupMember -Identity "GG_IT_Admins" | Select-Object Name, SamAccountName

Name           SamAccountName
----           --------------
Sophie Lambert s.lambert
Chloe Girard   c.girard


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


distinguishedName : CN=Sophie Lambert,OU=IT,DC=vlabs1,DC=com
name              : Sophie Lambert
objectClass       : user
objectGUID        : 7f0ff28e-a66e-44ce-b0ca-4276c5954de7
SamAccountName    : s.lambert
SID               : S-1-5-21-1268601764-4050707287-4025116504-1108

distinguishedName : CN=Chloe Girard,OU=IT,DC=vlabs1,DC=com
name              : Chloe Girard
objectClass       : user
objectGUID        : d21b2511-073d-4156-aeb3-dbc087158823
SamAccountName    : c.girard
SID               : S-1-5-21-1268601764-4050707287-4025116504-1113



PS C:\Users\Administrator>
```

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

5.1 Requirements

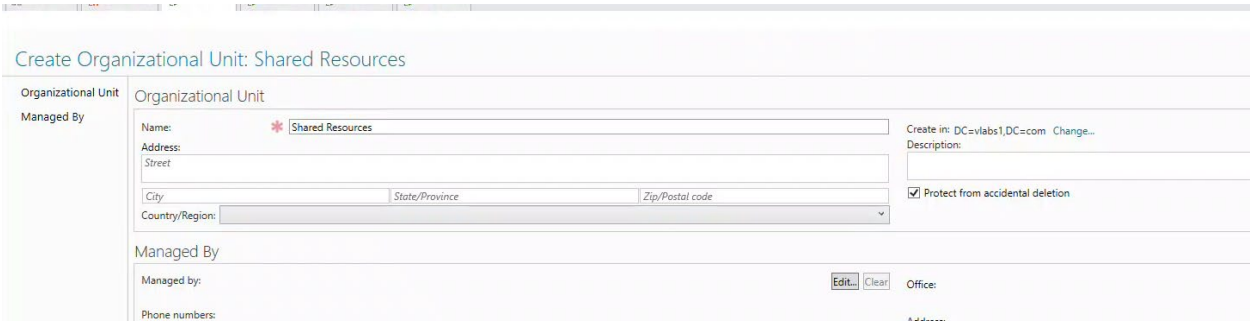
1. Create **an OU** named **Shared Resources** in **vlabs1.com** domain using **ADAC.**
2. Create a **Domain Local Group (DLG_HR_Share)** in **Shared Resources** using **ADAC.**
3. Create a **Domain Local Group (DLG_IT_Share)** in **Shared Resources** using **PowerShell**.

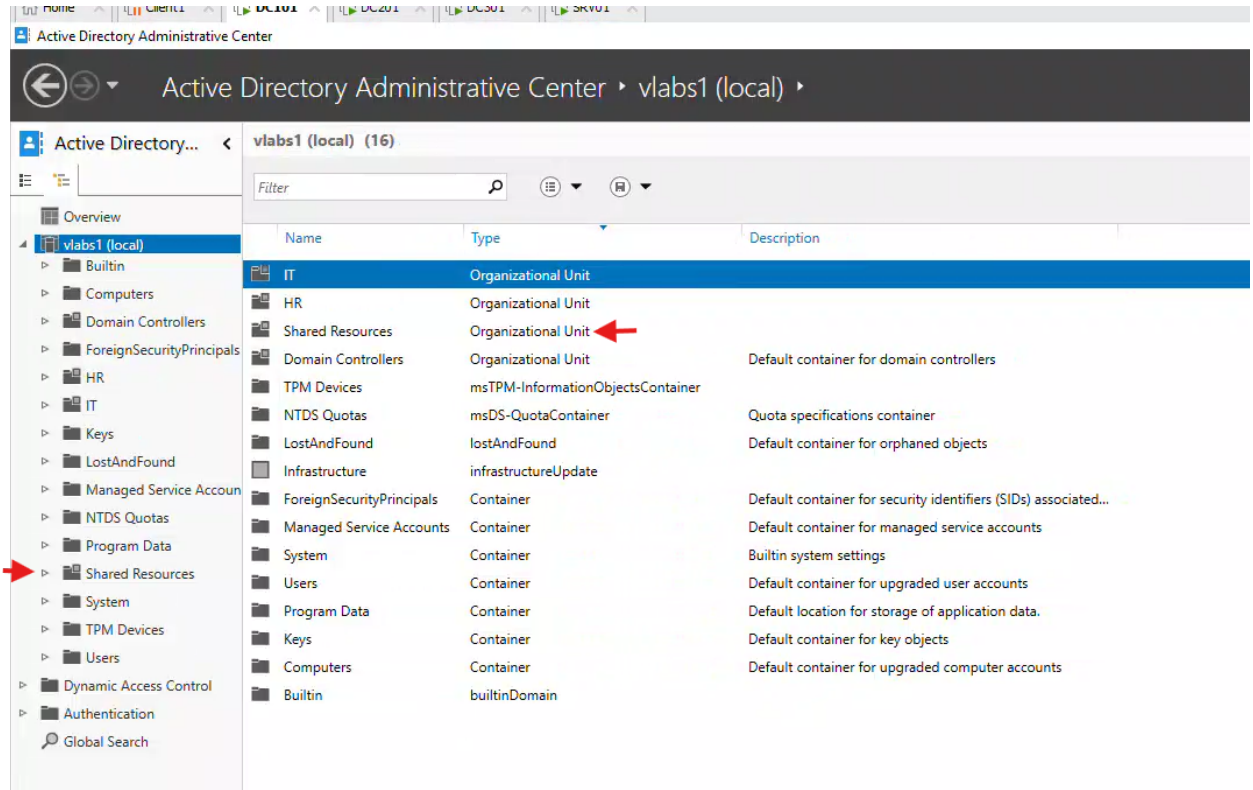
5.2 Create the Shared Resources OU using ADAC

Create the Shared Resources OU in the vlabs1.com Domain Using ADAC

Steps:

1. Open ADAC on DC101.
2. In the left pane, expand vlabs1.com.
3. Right-click the domain root (vlabs1.com) → New → Organizational Unit.
4. Name the OU Shared Resources → Click OK.



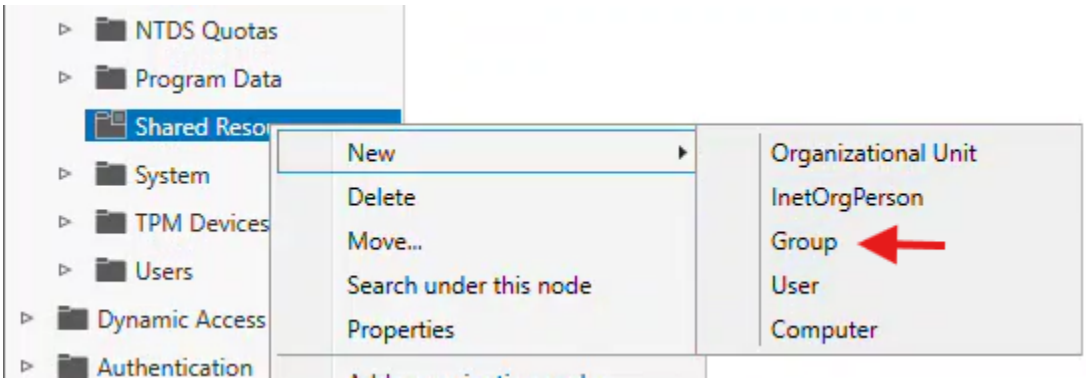


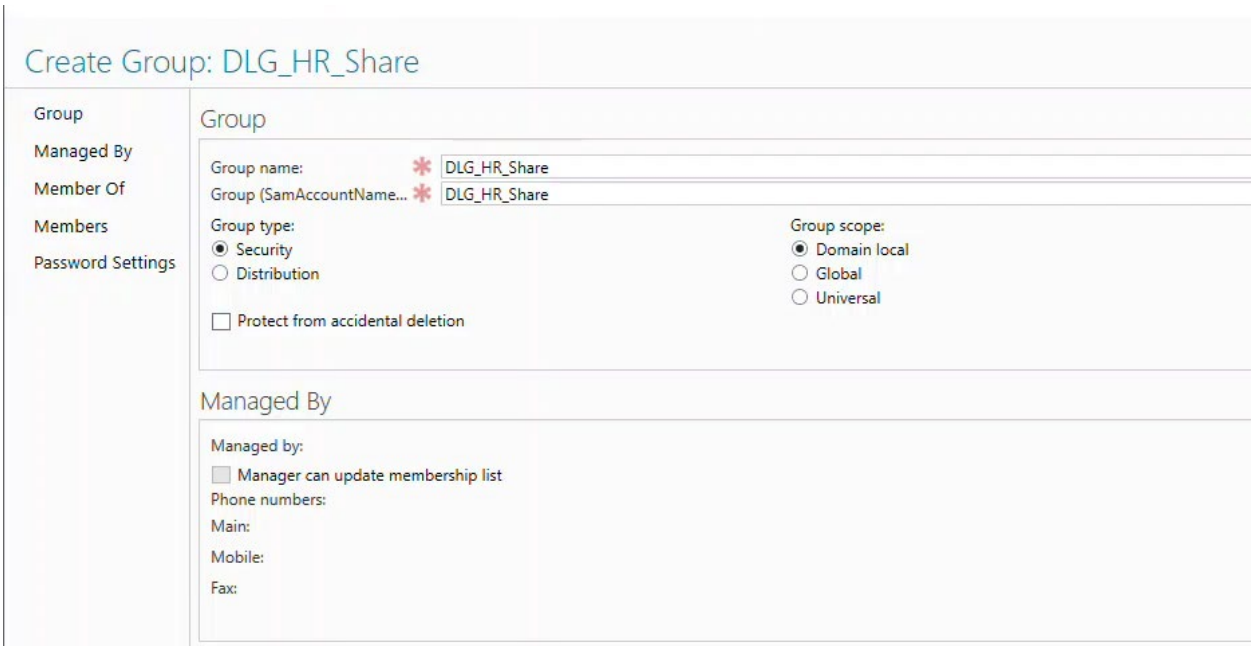
5.3 Create Domain Local Group using ADAC

Create Domain Local Group DLG_HR_Share **in the** Shared Resources **OU Using ADAC**

Steps:

1. In **ADAC**, navigate to **Shared Resources** OU.
2. Right-click the OU → **New** → **Group**.
3. Configure:
    - **Group name:** DLG_HR_Share
    - **Group scope:** Domain Local
    - **Group type:** Security
4. Click **OK**.





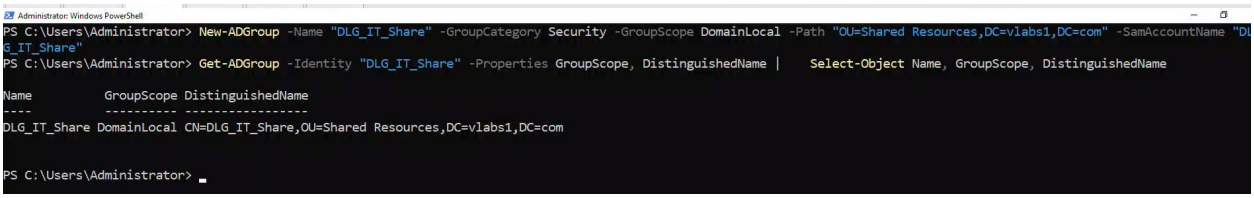
5.4 Create Domain Local Group using Powershell

Create Domain Local Group DLG_IT_Share in the Shared Resources OU Using PowerShell

New-ADGroup -Name "DLG_IT_Share" -GroupCategory Security -GroupScope DomainLocal -Path "OU=Shared Resources,DC=vlabs1,DC=com" -SamAccountName "DLG_IT_Share"

Verification:

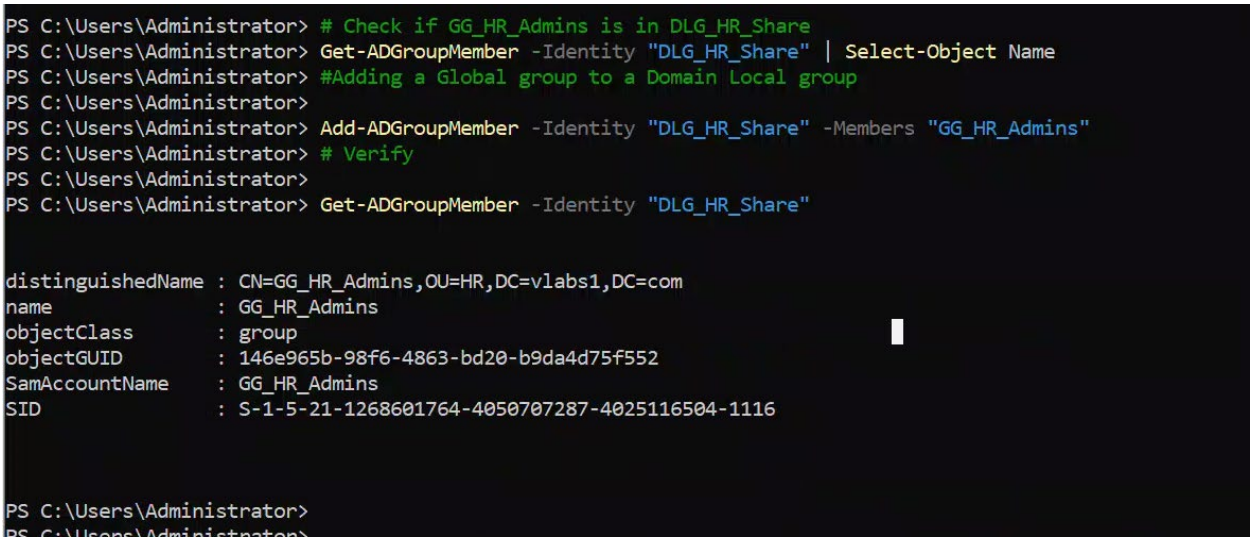
Get-ADGroup -Identity "DLG_IT_Share" -Properties GroupScope, DistinguishedName | Select-Object Name, GroupScope, DistinguishedName



5.5 GG_HR_Admins is nested into DLG_HR_Share.

ON DC101

#Adding a Global group to a Domain Local group
Add-ADGroupMember -Identity "DLG_HR_Share" -Members "GG_HR_Admins"
Get-ADGroupMember -Identity "DLG_HR_Share"



6 Task 4: Create a Local Group and Manage Membership

6.1 Requirements

1. On **SRV01,** create a **Local Group (LG_HR_Files)** using **GUI.**
2. Add **DLG_HR_Share** group **in**to **LG_HR_Files** group using **GUI.**
3. Verify the membership of **LG_HR_Files** group using **PowerShell**.

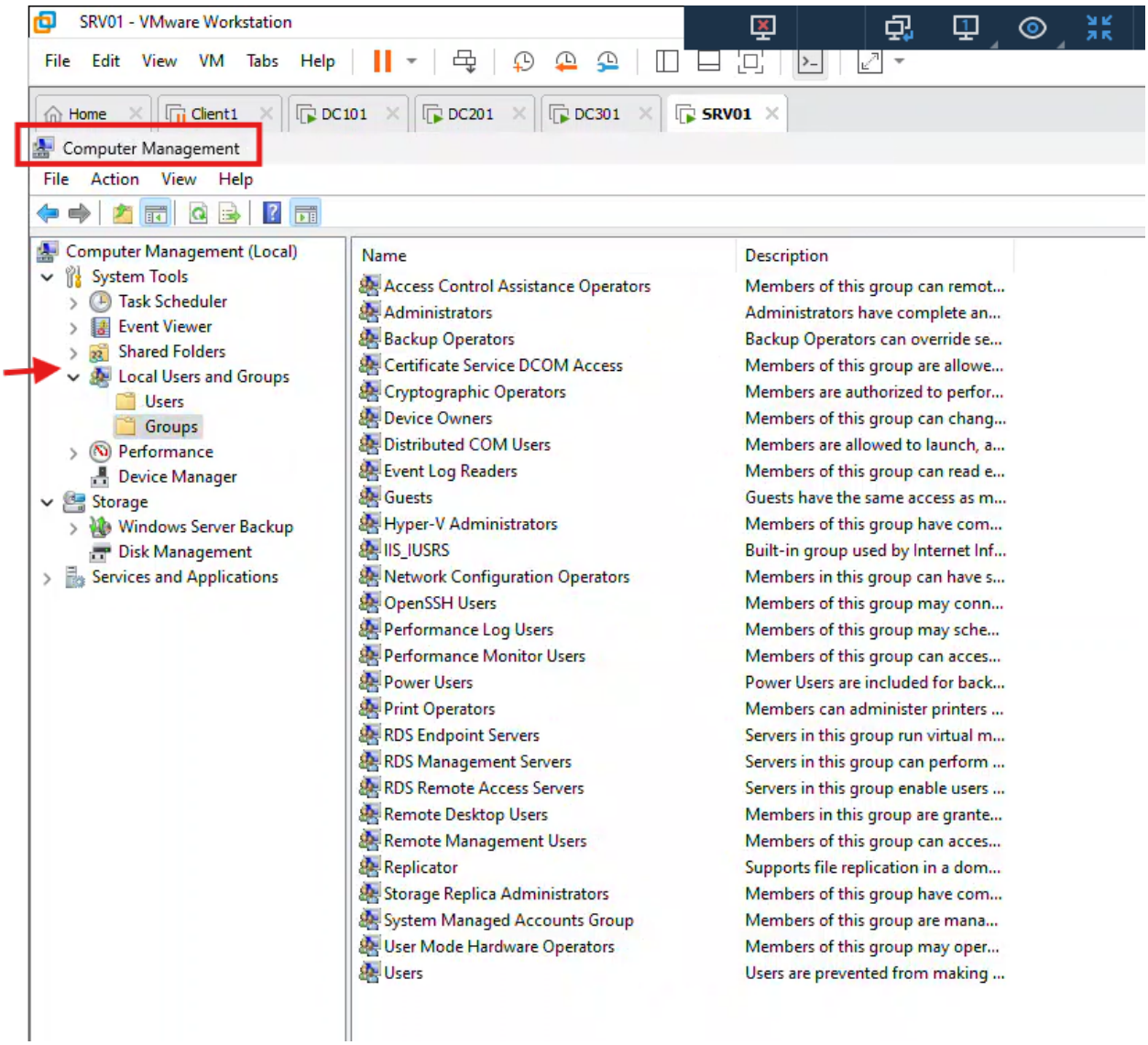
6.2 Create a Local Group on SRV01 Using GUI

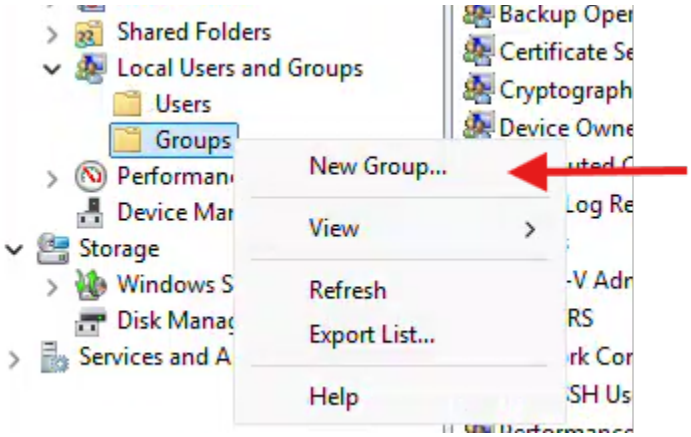
Create a Local Group LG_HR_Files on SRV01 Using GUI

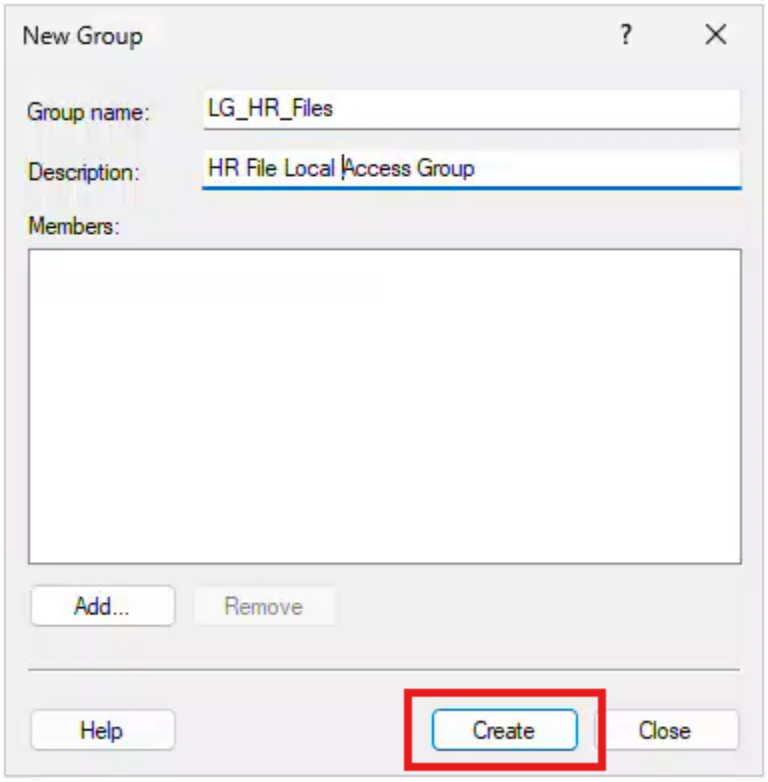
Steps:

1. **Log in to SRV01** with administrative privileges.
2. Open **Computer Management**:
    - Search for "Computer Management" in the Start menu.

3. Navigate to **Local Users and Groups** → **Groups**.
4. Right-click in the right pane → **New Group**.
5. Configure:
    - **Group name:** `LG_HR_Files`
    - Add a description.
6. Click **Create** → **Close**.







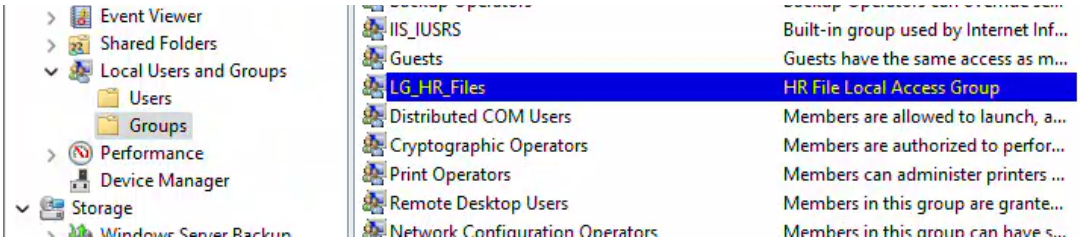
6.3 Add Domain Using GUI

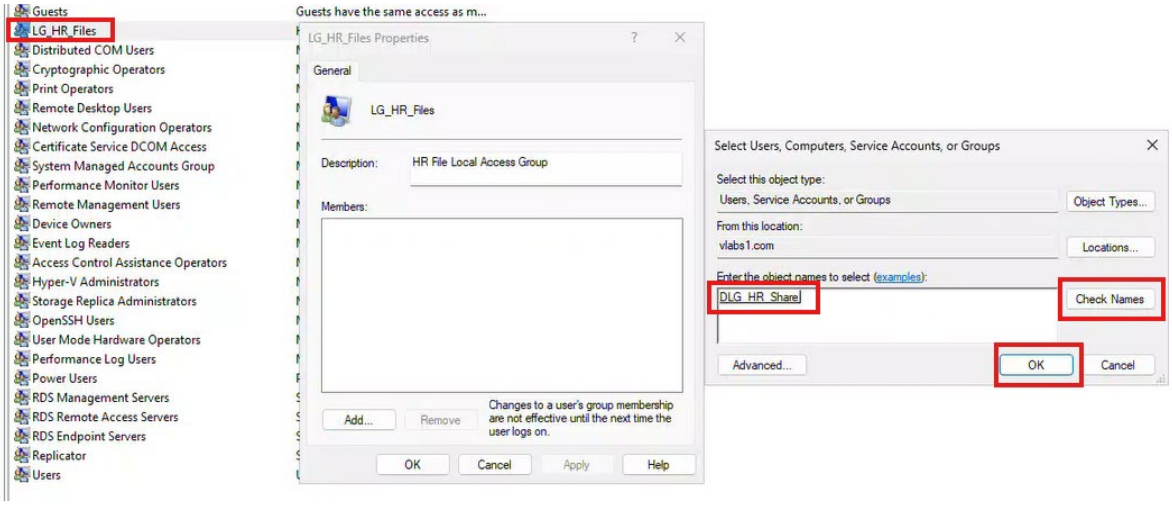
Add Domain Group DLG_HR_Share to LG_HR_Files Using GUI

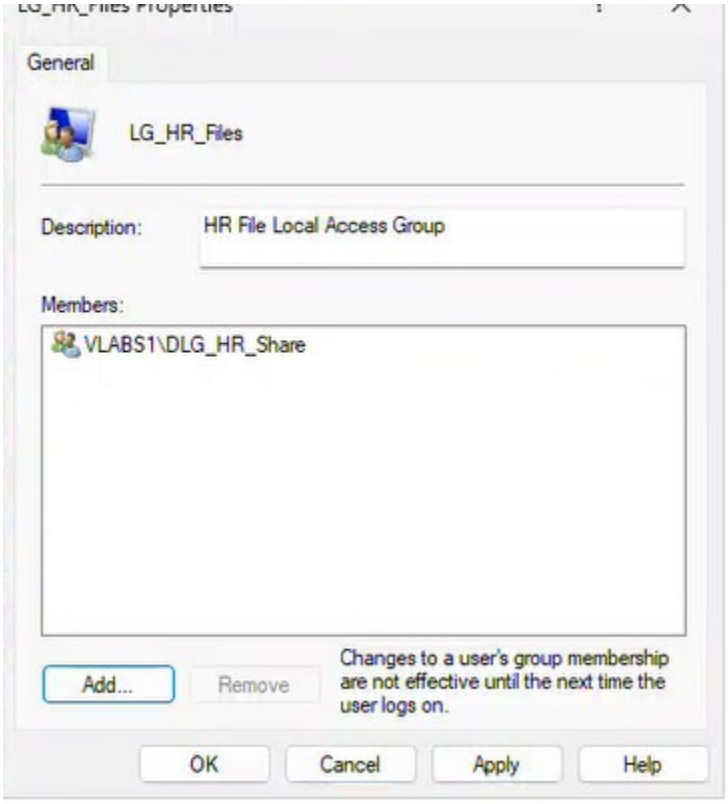
Steps:

1. In Computer Management, go to Groups → Double-click LG_HR_Files.

2. Click Add.
3. In the Select Users, Computers, or Groups window:
    - Under From this location, ensure the domain (vlabs1.com) is selected.
    - Enter DLG_HR_Share → Click Check Names to validate.
    - If resolved correctly, it will appear as DLG_HR_Share (Group from vlabs1.com).
4. Click OK → OK to save.



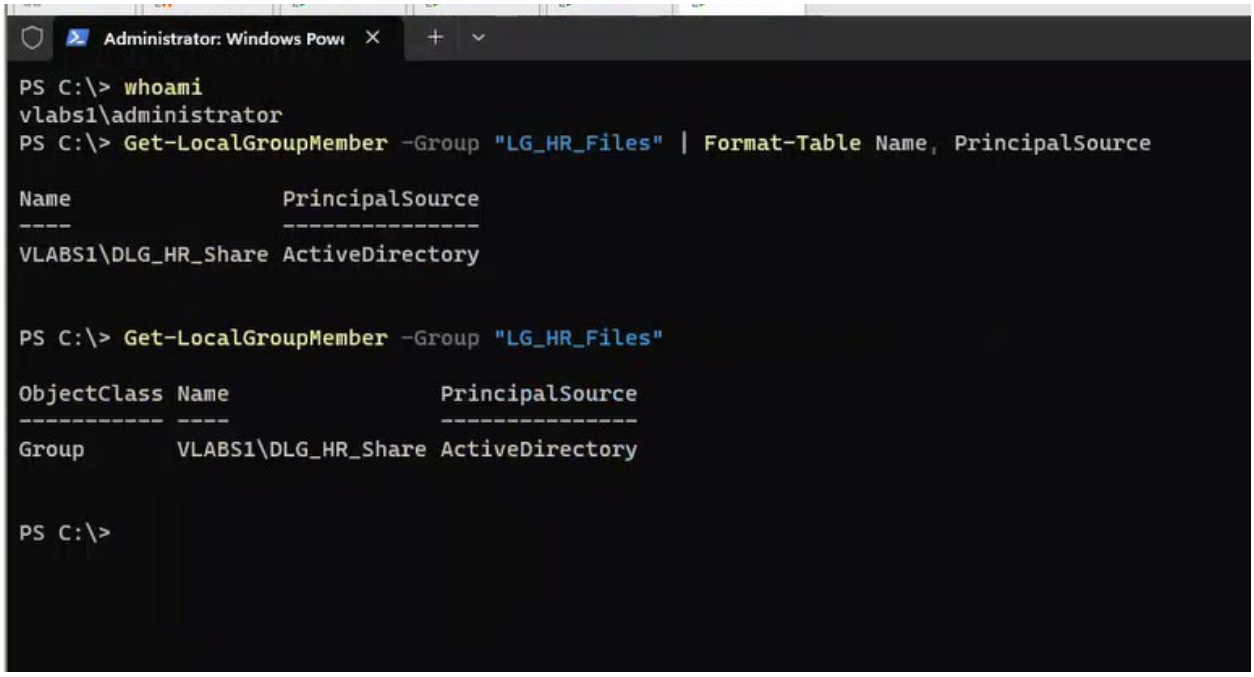




6.4 Verify Membership Using PowerShell

Verify Membership of LG_HR_Files Using PowerShell

```
Get-LocalGroupMember -Group "LG_HR_Files"
Get-LocalGroupMember -Group "LG_HR_Files" | Format-Table Name, PrincipalSource
```



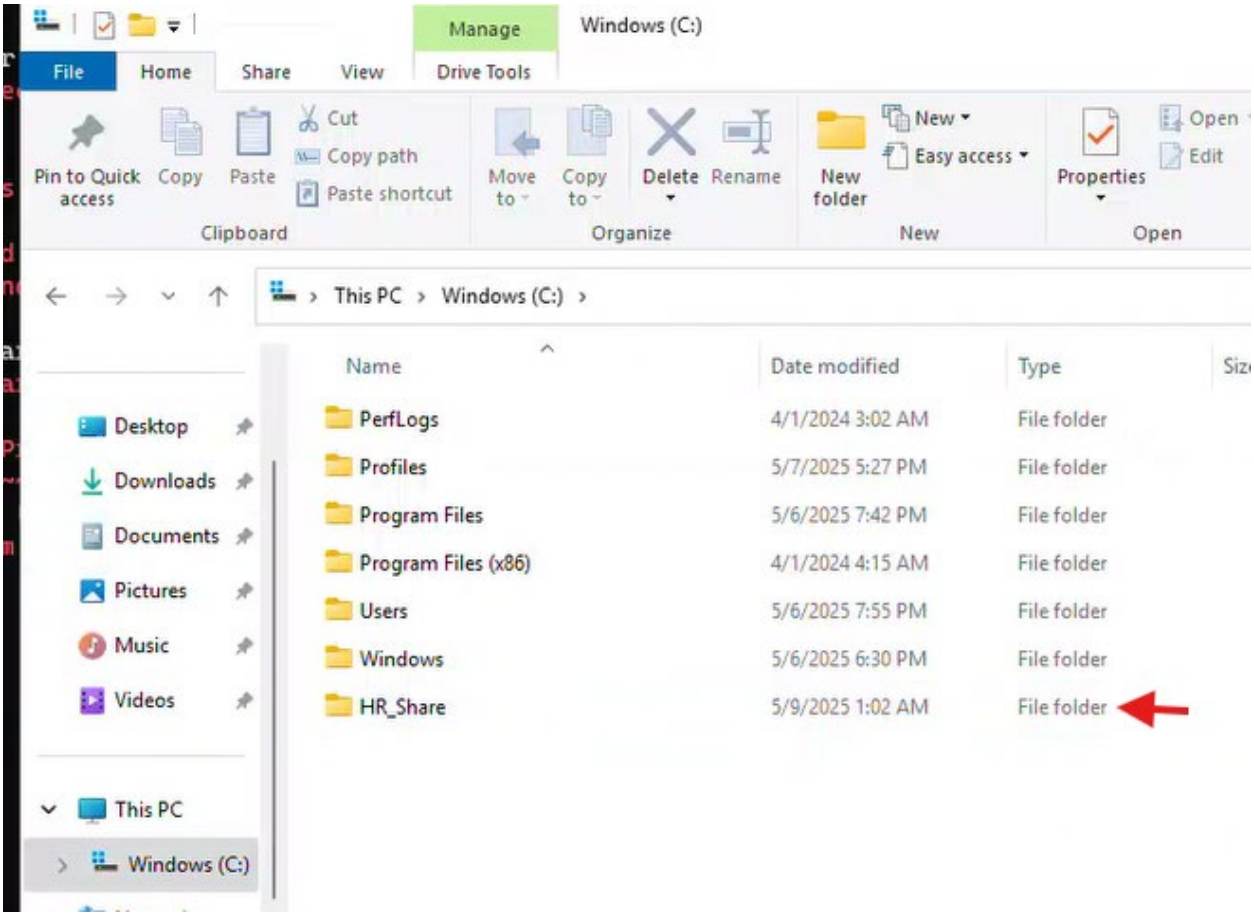
7 Task 5: Share and Set Permissions on SRV01

1. On **SRV01,** create and share a folder **C:\HR_Share** using **GUI.**
2. Assign **Change permissions (Read/Write)** to **LG_HR_Files** group, and remove the **Everyone** group using **GUI**.
3. Verify the share and permissions using **PowerShell**.

7.1 Create and Share the Folder C:\HR_Share Using GUI

1. Open File Explorer and navigate to C:\.
2. Create the Folder:

Right-click in the empty space → New → Folder → Name it HR_Share.

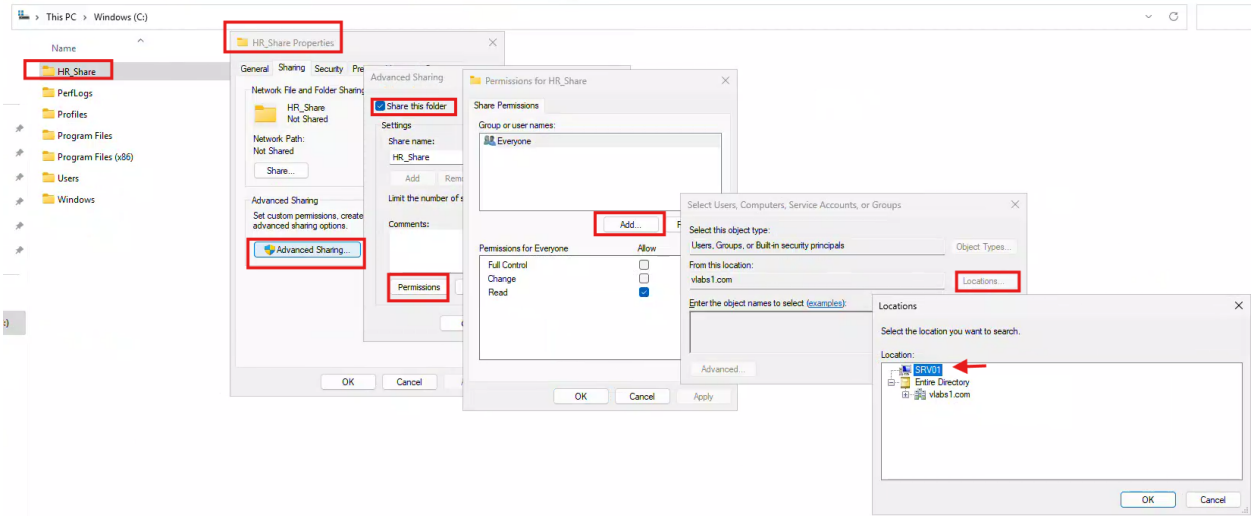


3. Share the Folder:

Right-click HR_Share → Properties → Sharing tab → Advanced Sharing.

Check Share this folder → Click Permissions.

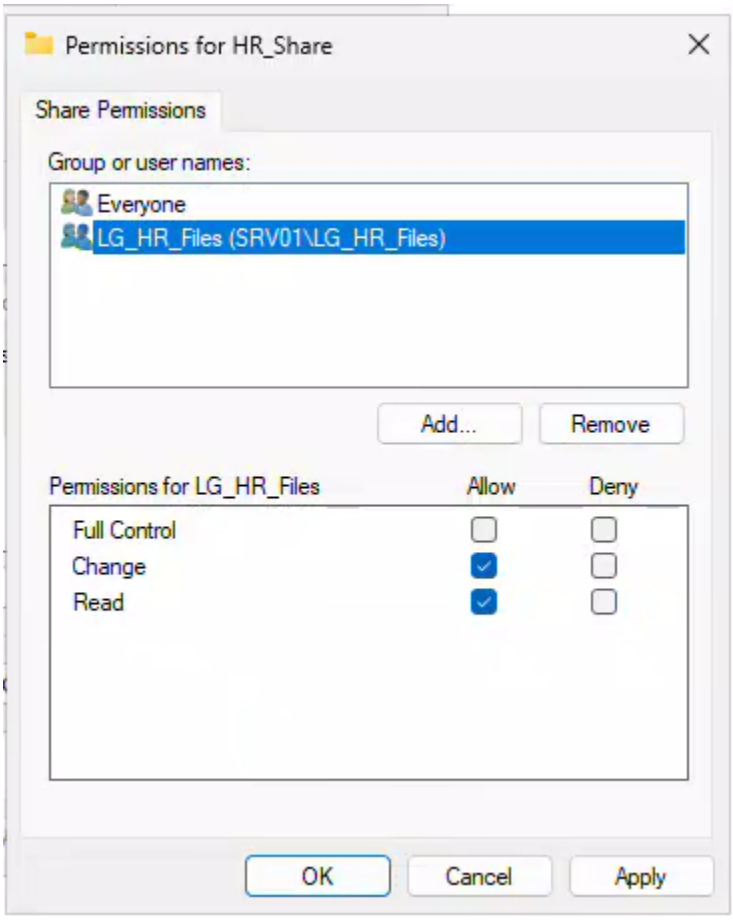
Click Add → Click Locations → Select SRV01



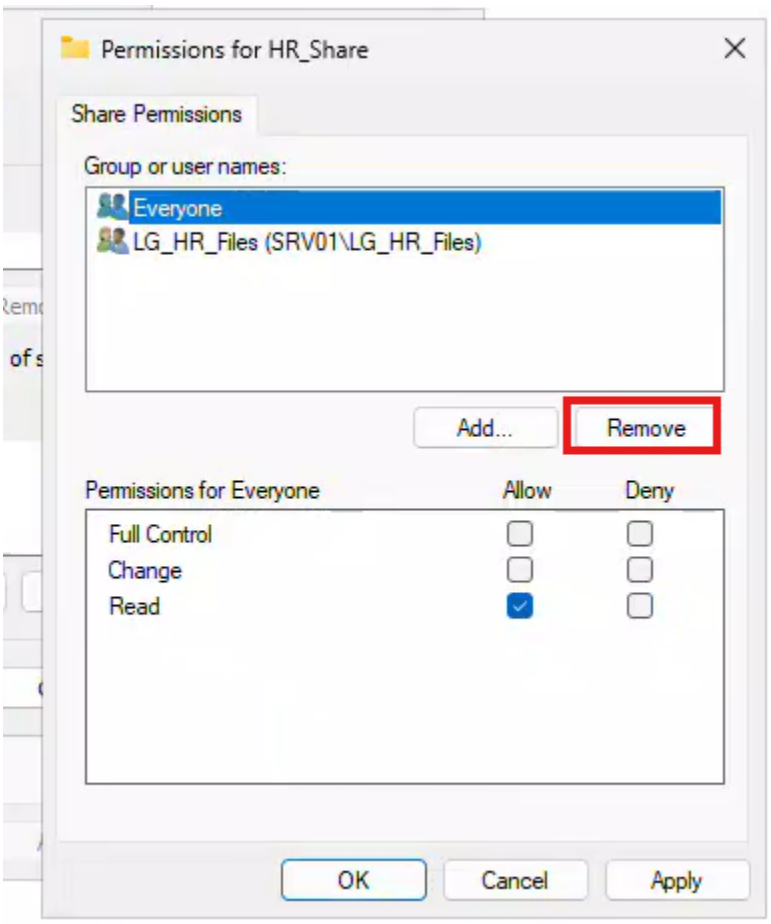
Enter LG_HR_Files → Click Check Names → OK.

See it changes to SRV01\LG_HR_Files → Click OK

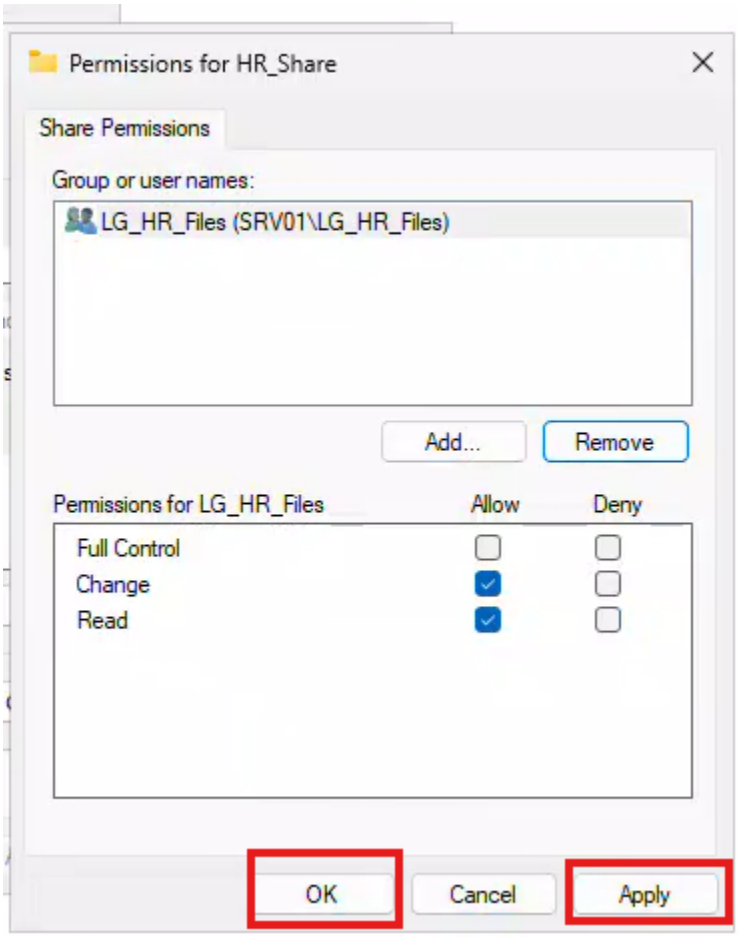
Assign Change permissions (Read/change) to LG_HR_Files → OK → OK.



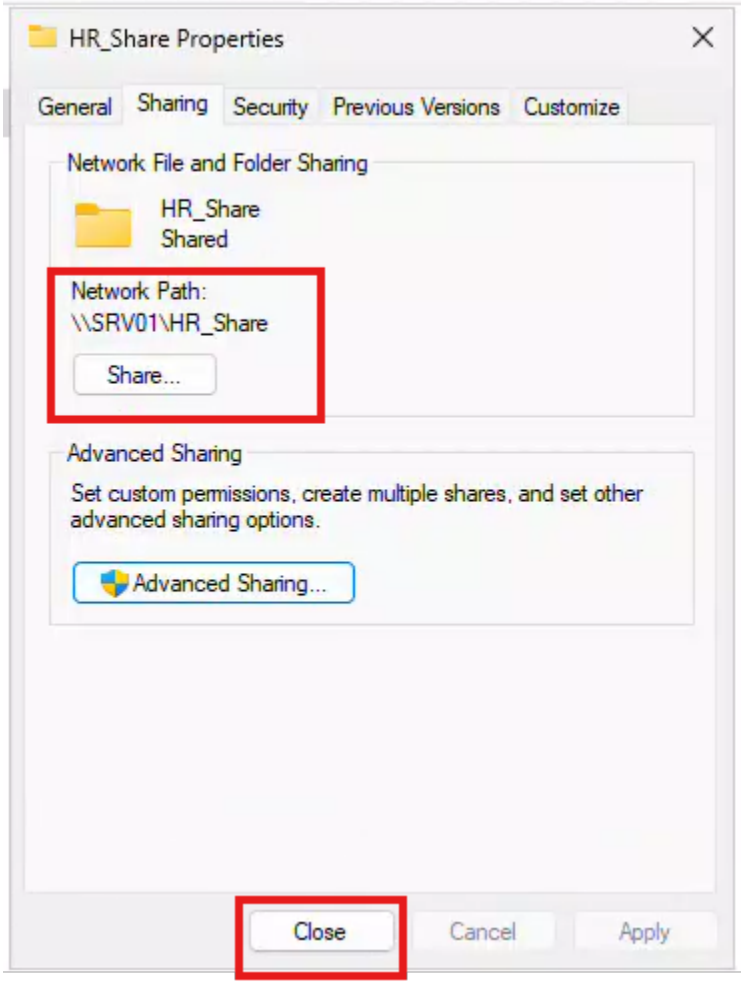
Remove the Everyone group (select it → Remove).



Click Apply → OK → Apply → OK → OK



Note Network Path changed to \\SRV01\HR_Share
Click Close



4. Verify the share and permissions using **PowerShell**
   Get-SmbShare -Name "HR_Share"

   Get-SmbShareAccess -Name "HR_Share" | Format-Table AccountName, AccessRight

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

PS C:\Users\administrator.VLABS1> Get-SmbShare -Name "HR_Share"

Name     ScopeName Path        Description
----     --------- ----        -----------
HR_Share *         C:\HR_Share


PS C:\Users\administrator.VLABS1> Get-SmbShareAccess -Name "HR_Share" | Format-Table AccountName, AccessRight

AccountName       AccessRight
-----------       -----------
SRV01\LG_HR_Files      Change
```

2. Assign NTFS Permissions and Remove Everyone
Steps:

In the HR_Share folder's Properties, go to the Security tab.

Click Edit → Add → Enter LG_HR_Files → Check Names → OK.

Select LG_HR_Files → Check Modify (includes Read/Write) under Allow.

Select the Everyone group → Click Remove → OK → OK.

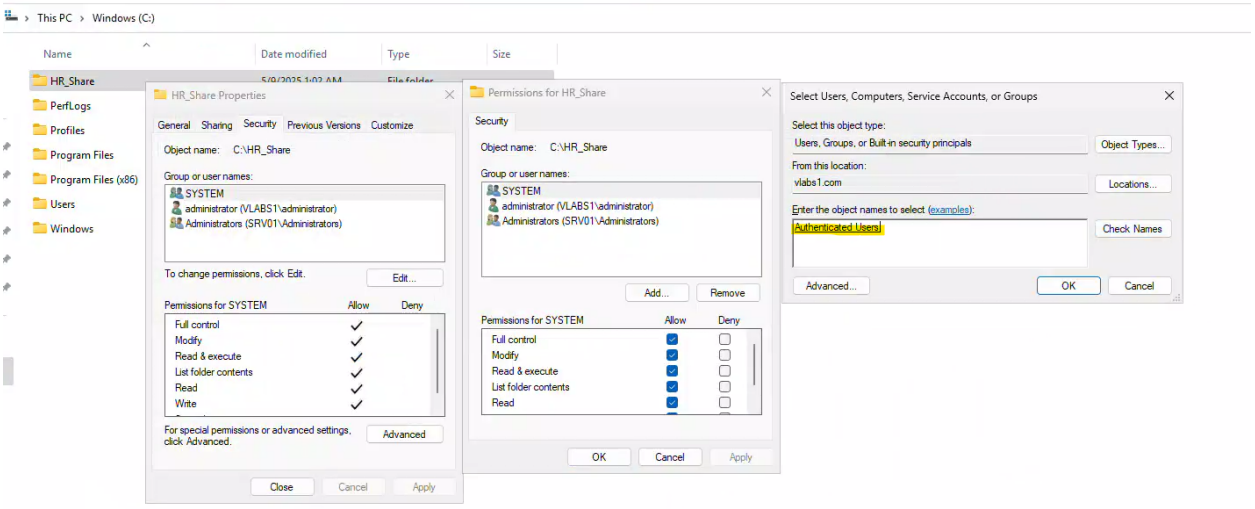
3. Verify the Share and Permissions Using PowerShell
Run these commands as Administrator on SRV01:

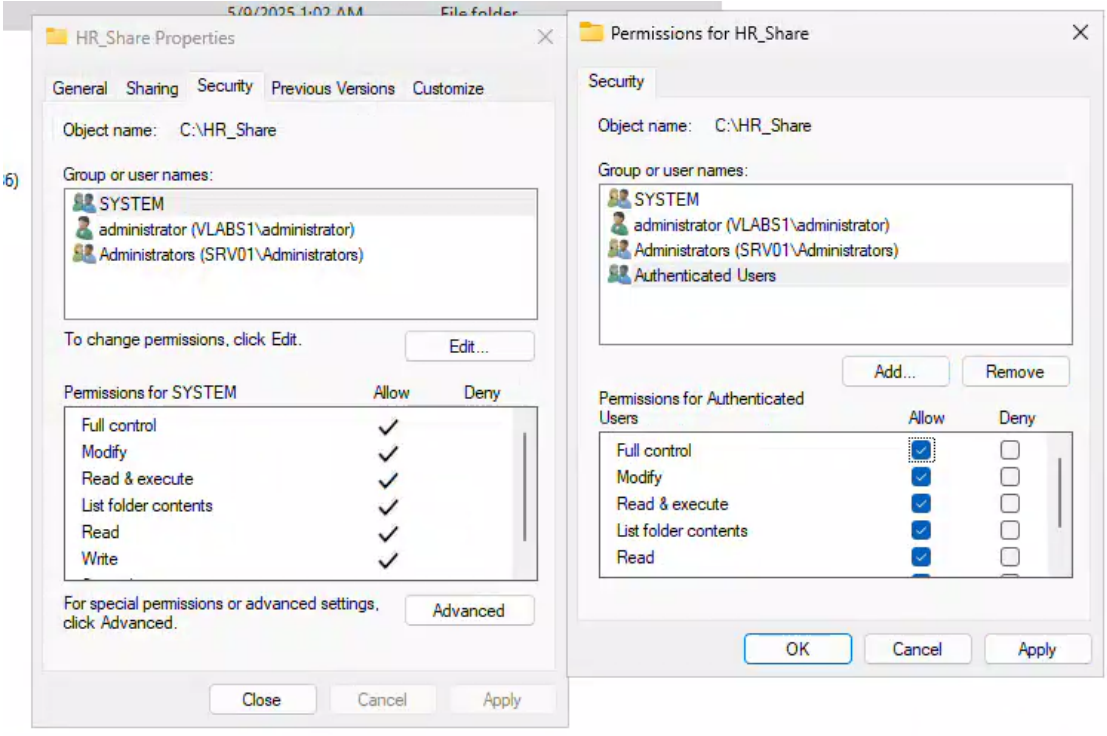
Check Shared Folder Exists:
powershell
Get-SmbShare -Name "HR_Share"
Expected Output:

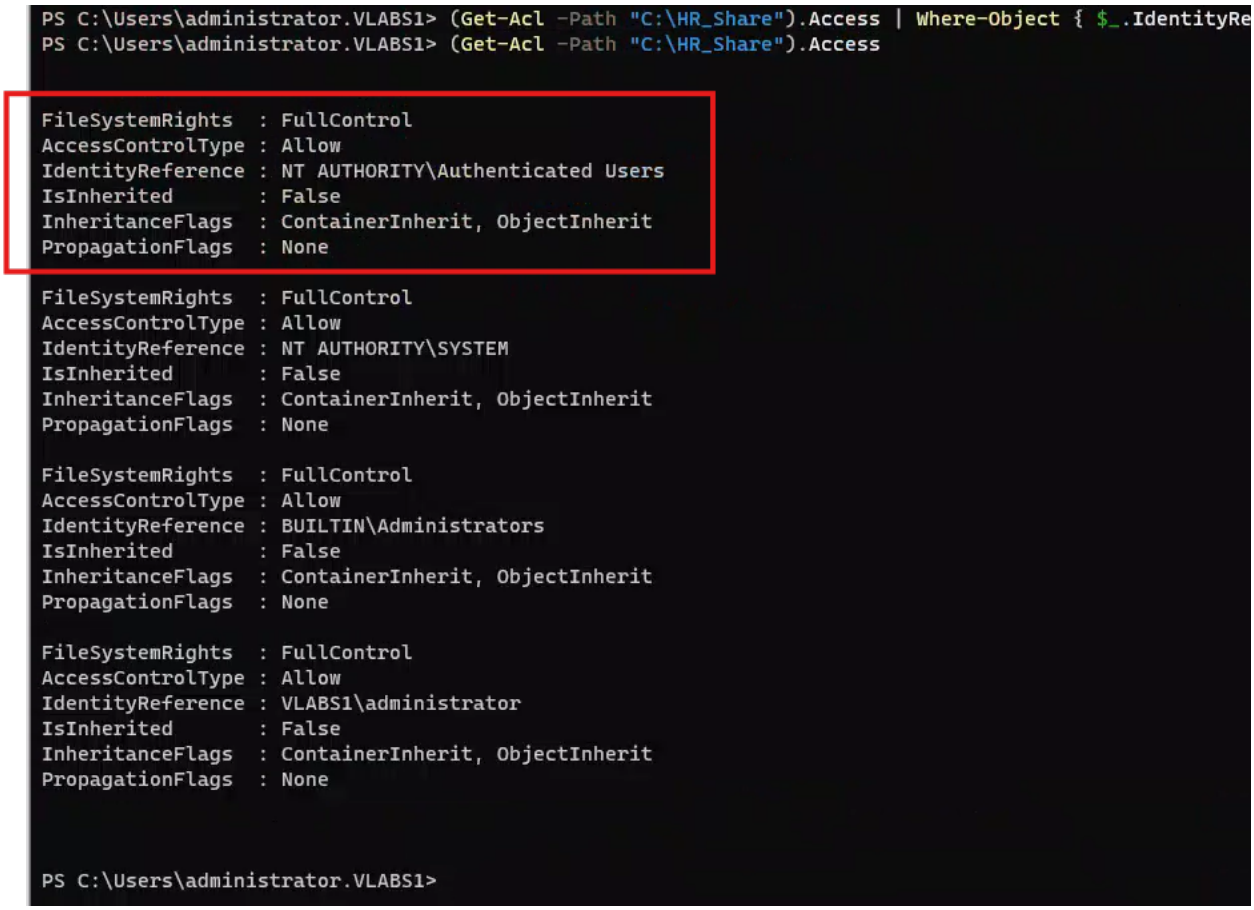
Name Path Description
---- ---- -----------
HR_Share C:\HR_Share
Verify Share Permissions:
powershell
Get-SmbShareAccess -Name "HR_Share" | Format-Table AccountName, AccessRight
Expected Output:

AccountName AccessRight
----------- -----------
LG_HR_Files Change
Verify NTFS Permissions:
powershell
```
Get-NTFSAccess -Path "C:\HR_Share" |
  Where-Object { $_.Account -eq "LG_HR_Files" } |
  Format-Table Account, AccessRights
```
Expected Output:

Account AccessRights
------- ------------
LG_HR_Files Modify, Synchronize
TASK

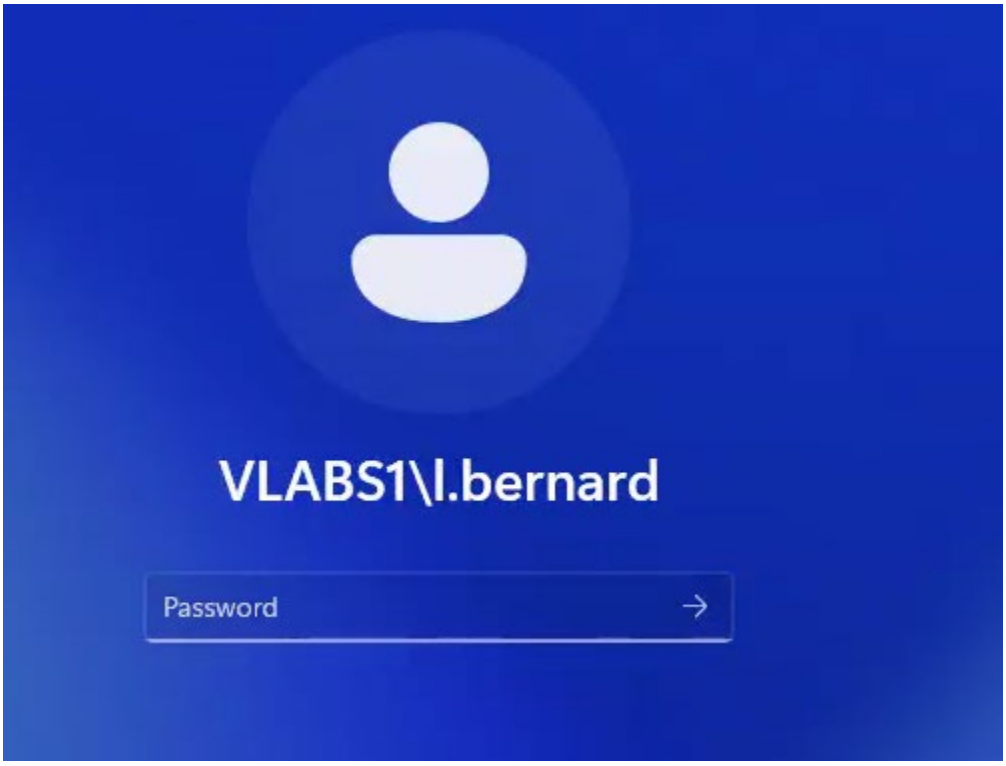

This PC › Windows (C:)
Name
Date modified
Type
Size
HR_Share
PerfLogs
Profiles
Program Files
Program Files (x86)
Users
Windows
HR_Share Properties
General Sharing Security Previous Versions Customize
Object name: C:\HR_Share
Group or user names:
SYSTEM
administrator (VLABS1\administrator)
Administrators (SRV01\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply
Permissions for HR_Share
Security
Object name: C:\HR_Share
Group or user names:
SYSTEM
administrator (VLABS1\administrator)
Administrators (SRV01\Administrators)
Add...
Remove
Permissions for SYSTEM Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply
Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
vlabs1.com
Locations...
Enter the object names to select (examples):
Authenticated Users
Check Names
Advanced...
OK
Cancel


HR_Share Properties
General Sharing Security Previous Versions Customize
Object name: C:\HR_Share
Group or user names:
SYSTEM
administrator (VLABS1\administrator)
Administrators (SRV01\Administrators)
To change permissions, click Edit.
Edit...
Permissions for SYSTEM Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply
Permissions for HR_Share
Security
Object name: C:\HR_Share
Group or user names:
SYSTEM
administrator (VLABS1\administrator)
Administrators (SRV01\Administrators)
Authenticated Users
Add...
Remove
Permissions for Authenticated Users Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply

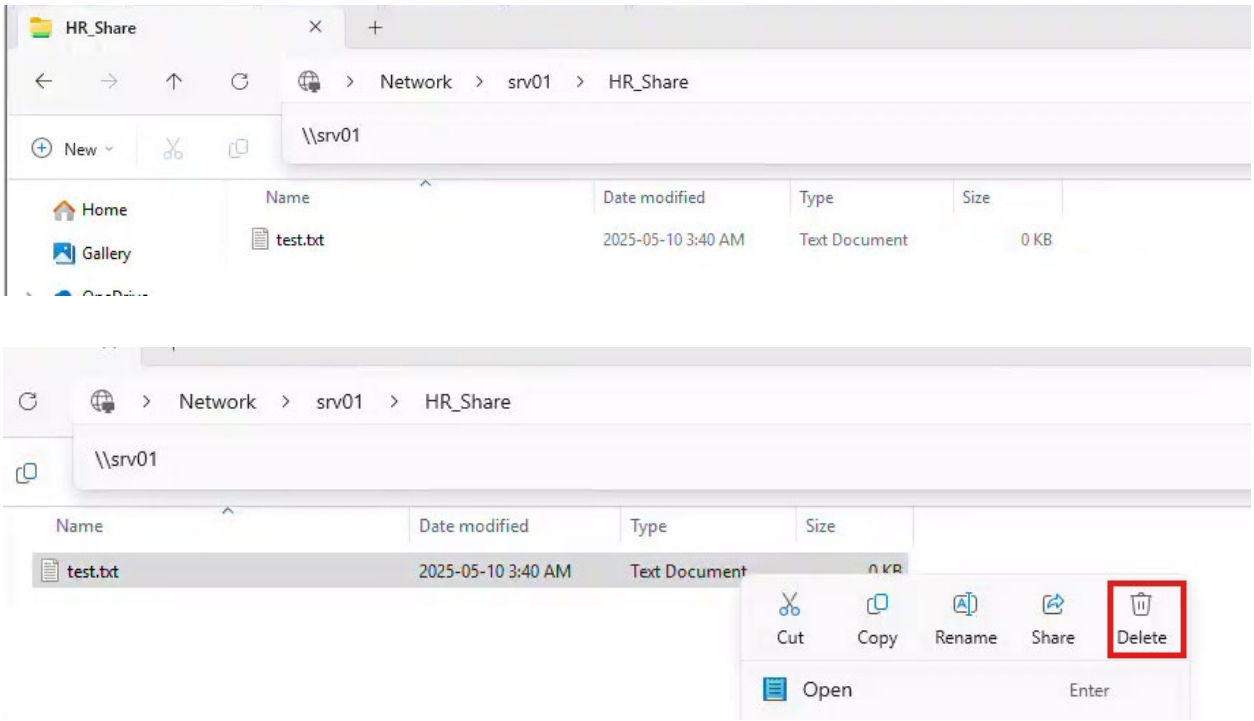


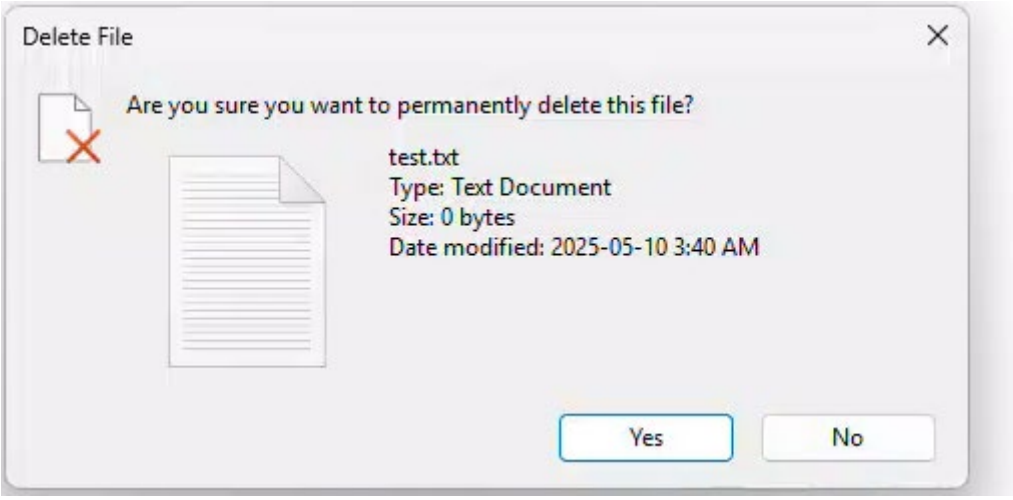
8 Task 6: Test HR Share Access from Client1

1. Log in as **Lucas Bernard (l.bernard)** on **Windows 11 (Client1).**



2. Access the shared folder **\\SRV01\HR_Share$** and verify permissions by creating and deleting files in this share.





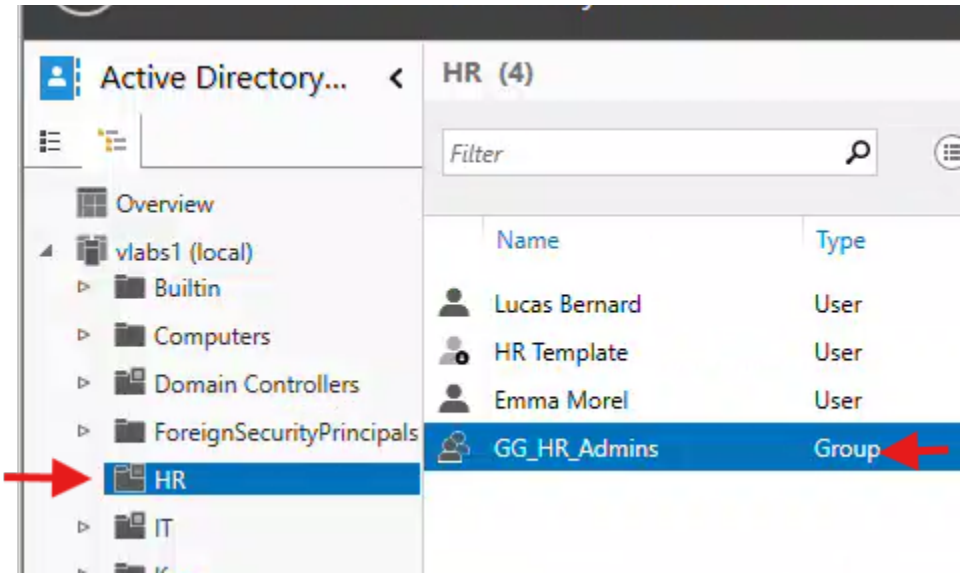
9 Task 7: Remove a User from a Group and Delete a User

9.1 Remove user using ADAC

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

Navigate to the HR OU where the group GG_HR_Admins is located.

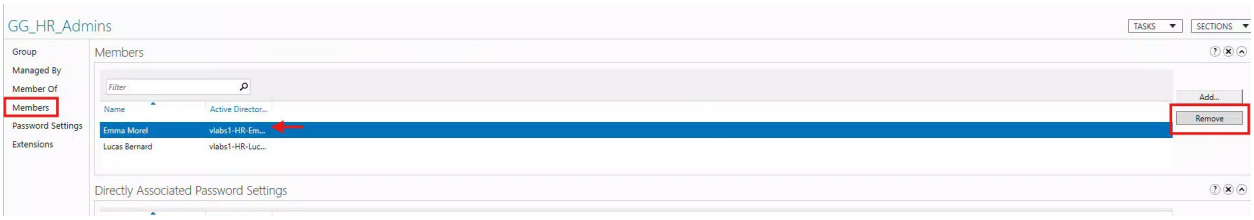
Right-click the GG_HR_Admins group and select Properties.



Go to the Members tab.

Select Emma Morel (e.morel) and click Remove.

Click OK to save changes.

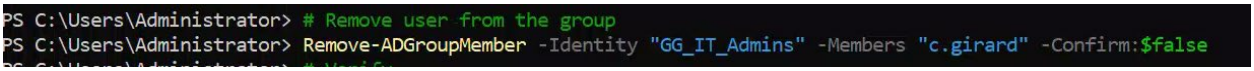


9.2 Remove user using Powershell

Remove **Chloe Girard (c.girard)** from **GG_IT_Admins** using **PowerSehll**

 # Remove user from the group

Remove-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard" -Confirm:$false



 # Verify removal

Get-ADGroupMember -Identity "GG_IT_Admins" | Select-Object Name

Expected Output (Chloe Girard should no longer appear)

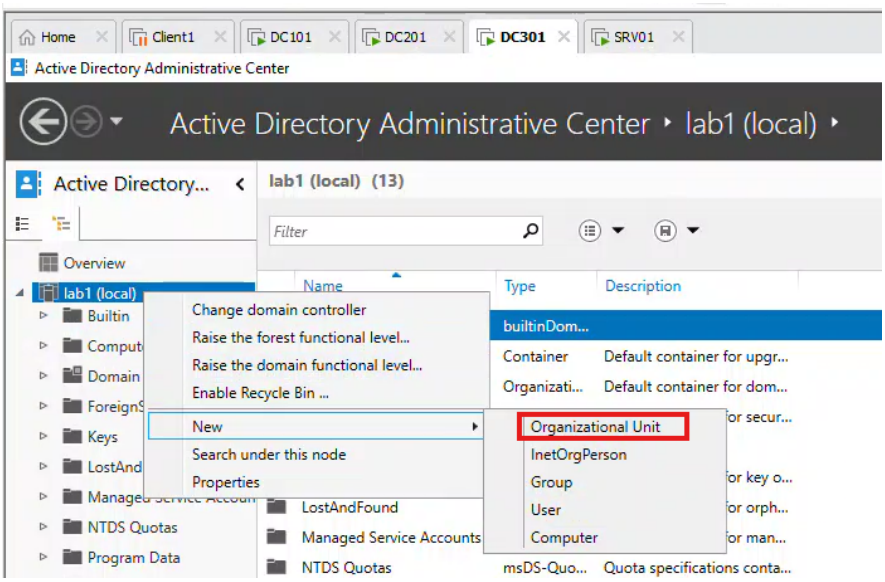
```
PS C:\Users\Administrator> # Verify removal
PS C:\Users\Administrator> Get-ADGroupMember -Identity "GG_IT_Admins" | Select-Object Name

Name
----
Sophie Lambert
```

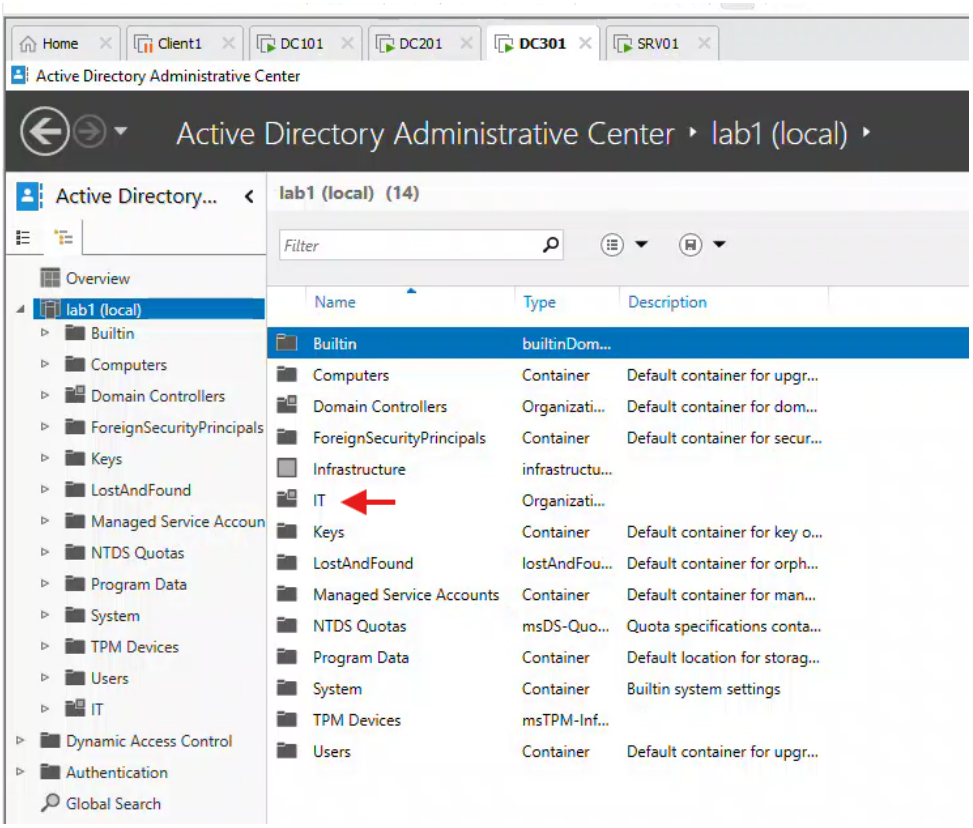
10 Task 8: Create IT OU and Configure Groups on DC301 and DC101

10.1 DC301 Child Domain (lab1.vlabs1.com)

1. On **DC301**, create an **OU** named **IT** using **ADAC.**

    a) Open ADAC on DC301.
    b) Navigate to the domain `lab1.vlabs1.com`.
    c) Right-click the domain root → New → Organizational Unit → Name: `IT`.

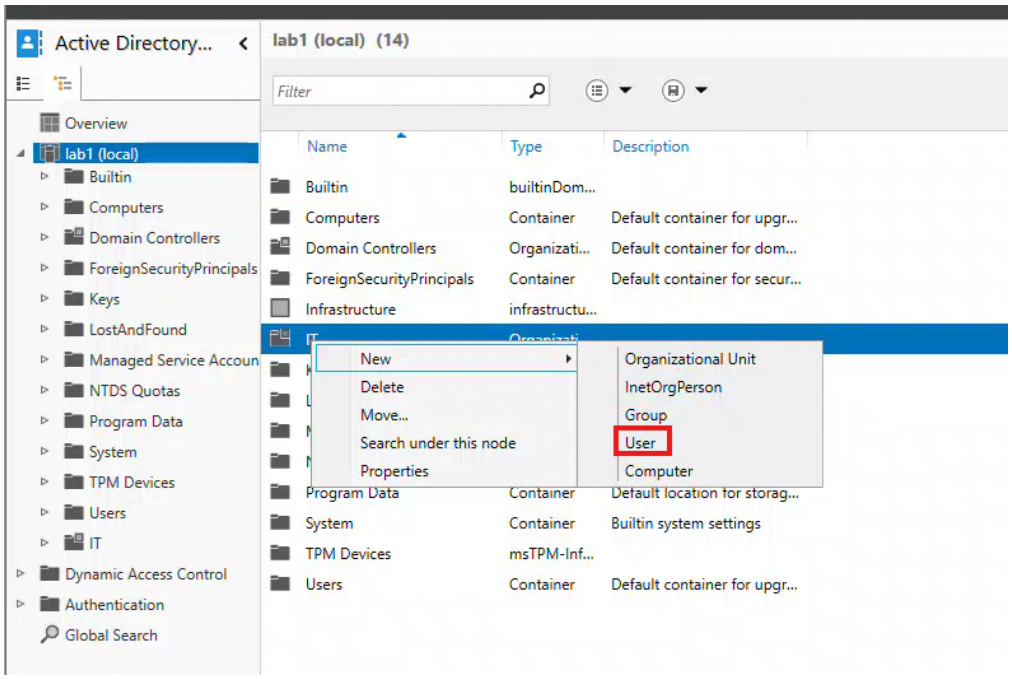


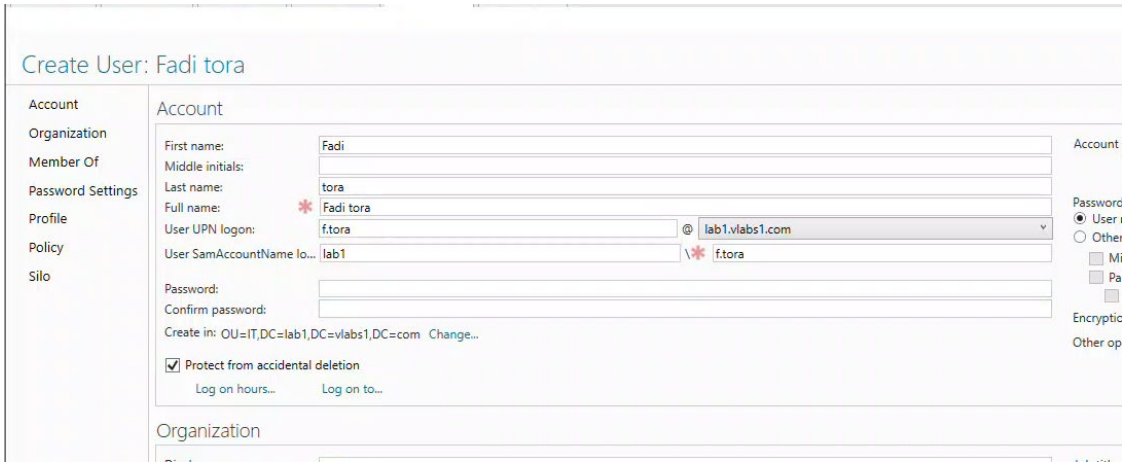


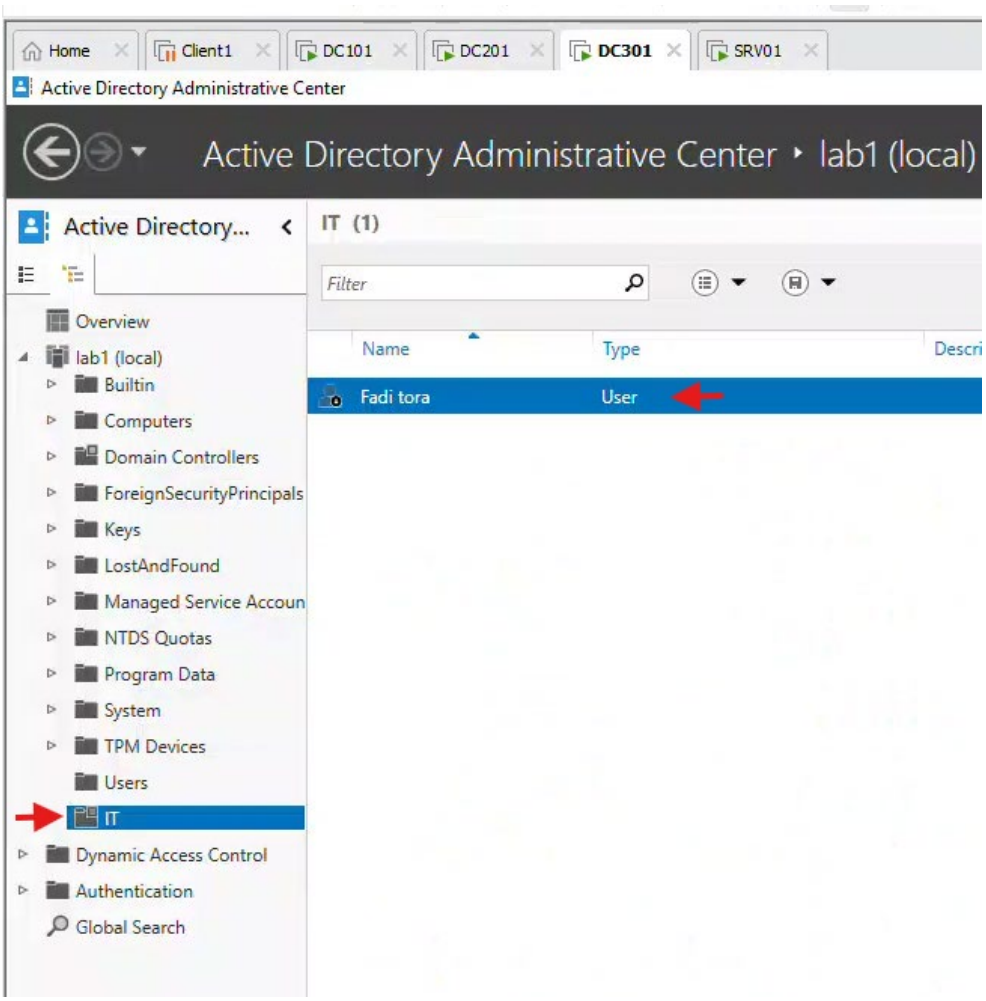
2. Inside **IT OU**, create a user **Fadi Tora (f.tora)** using **ADAC**.

a) In ADAC, navigate to the `IT` OU.
b) Right-click → New → User → Fill in details:

- First name: `Fadi`, Last name: `Tora`, User logon name: `f.tora`.

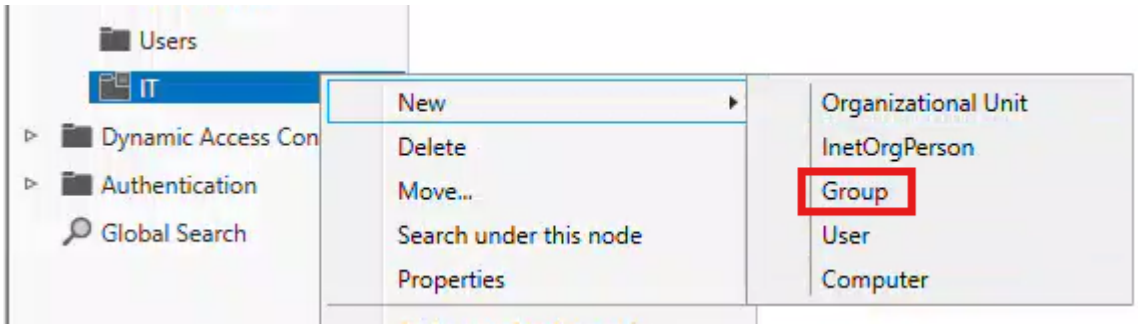

Active Directory...
lab1 (local) (14)
Filter
Overview
lab1 (local)
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accoun
NTDS Quotas
Program Data
System
TPM Devices
Users
IT
Dynamic Access Control
Authentication
Global Search
Name
Type
Description
Builtin
builtinDom...
Computers
Container
Default container for upgr...
Domain Controllers
Organizati...
Default container for dom...
ForeignSecurityPrincipals
Container
Default container for secur...
Infrastructure
infrastructu...
New
Delete
Move...
Search under this node
Properties
Organizational Unit
InetOrgPerson
Group
User
Computer
Program Data
Container
Default location for storag...
System
Container
Builtin system settings
TPM Devices
msTPM-Inf...
Users
Container
Default container for upgr...

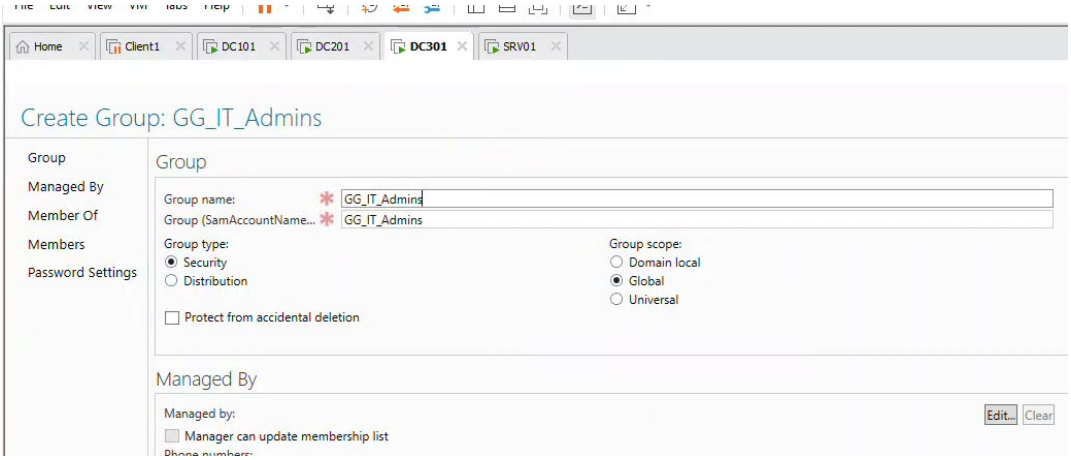

Create User: Fadi tora
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Account
First name:
Fadi
Middle initials:
Last name:
tora
Full name:
Fadi tora
User UPN logon:
f.tora
@
lab1.vlabs1.com
User SamAccountName lo...
lab1
\
f.tora
Password:
Confirm password:
Create in: OU=IT,DC=lab1,DC=vlabs1,DC=com Change...
Protect from accidental deletion
Log on hours...
Log on to...
Organization

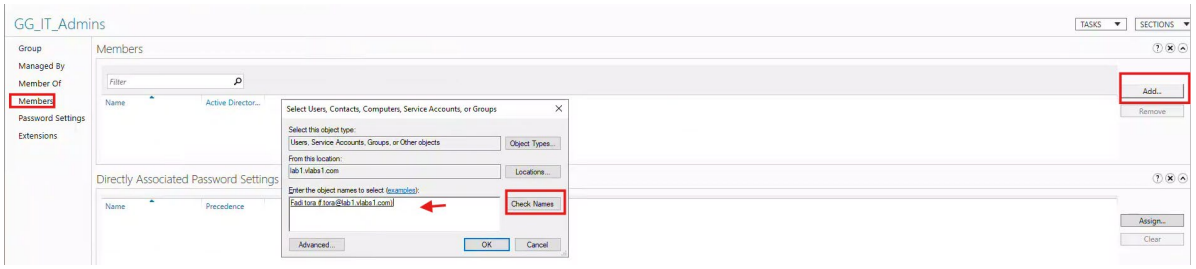


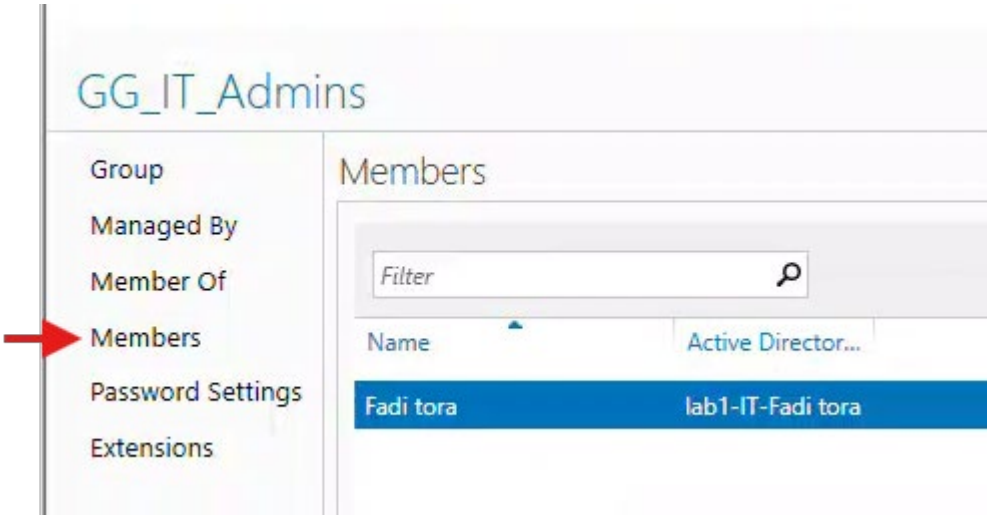
3. Inside **IT OU**, create a Global Group **GG_IT_Admins** and add **Fadi Tora** as a member using **ADAC.**

a) In ADAC, navigate to the `IT` OU.
b) Right-click → New → Group → Name: `GG_IT_Admins`, Group type: `Security`, Scope: `Global`.
c) Open `GG_IT_Admins` properties → Members → Add `f.tora`.



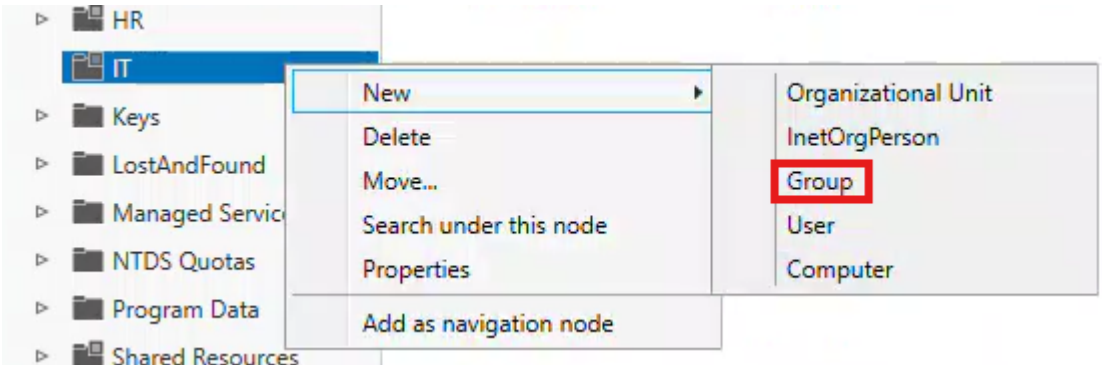


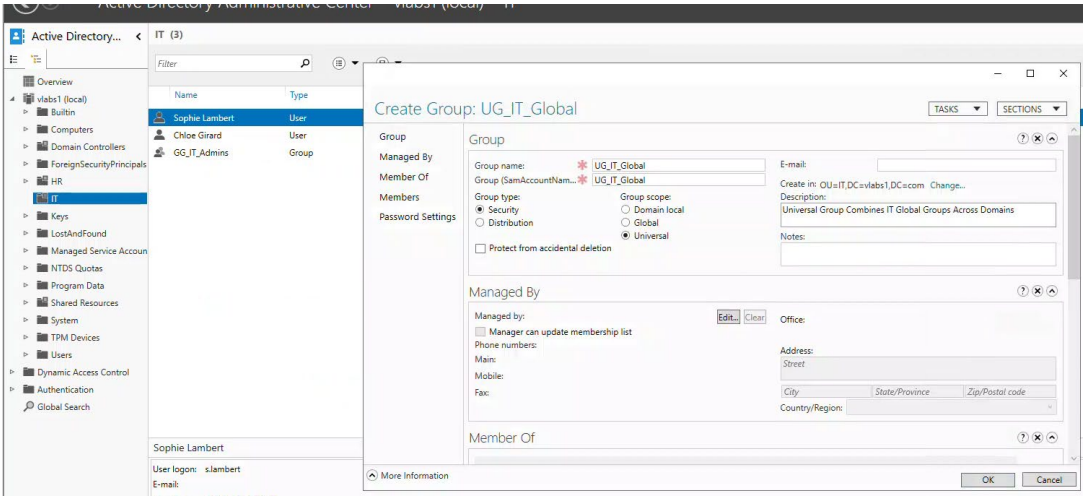


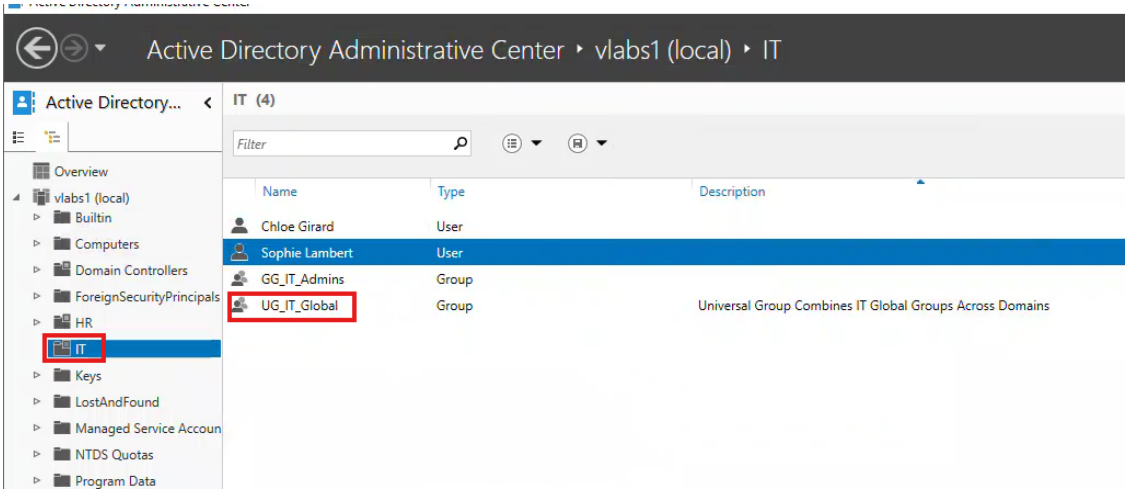


10.2 DC101 (Primary Domain Controller)

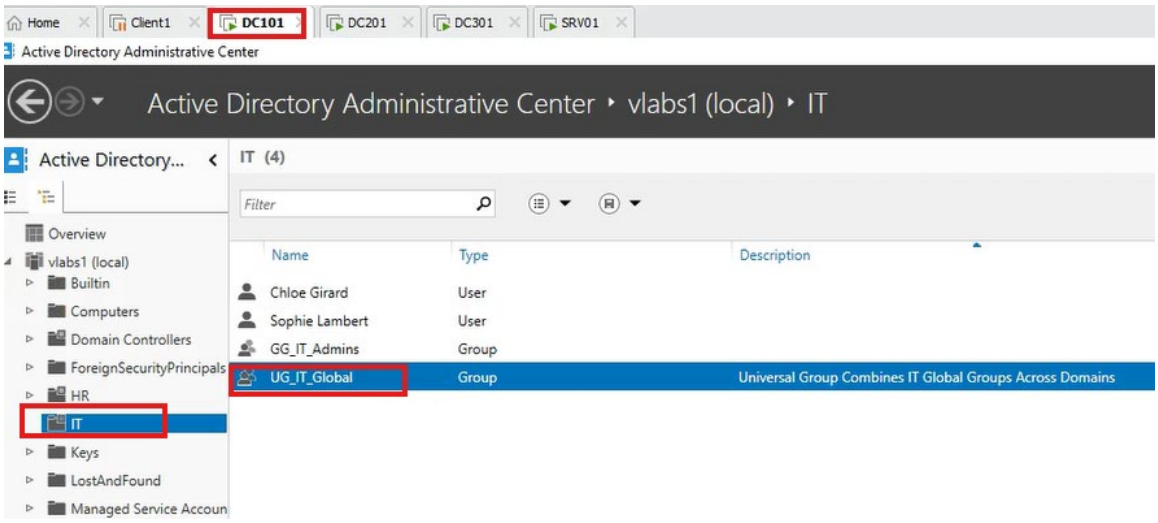
1. On **DC101**, create a Universal Group **UG_IT_Global.**



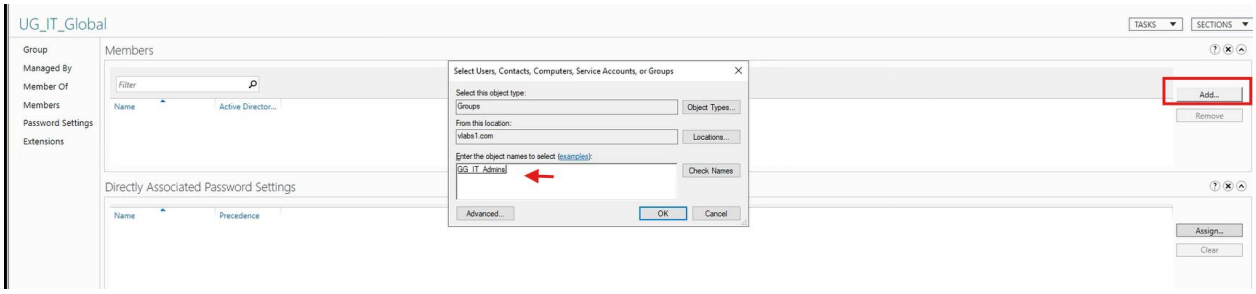




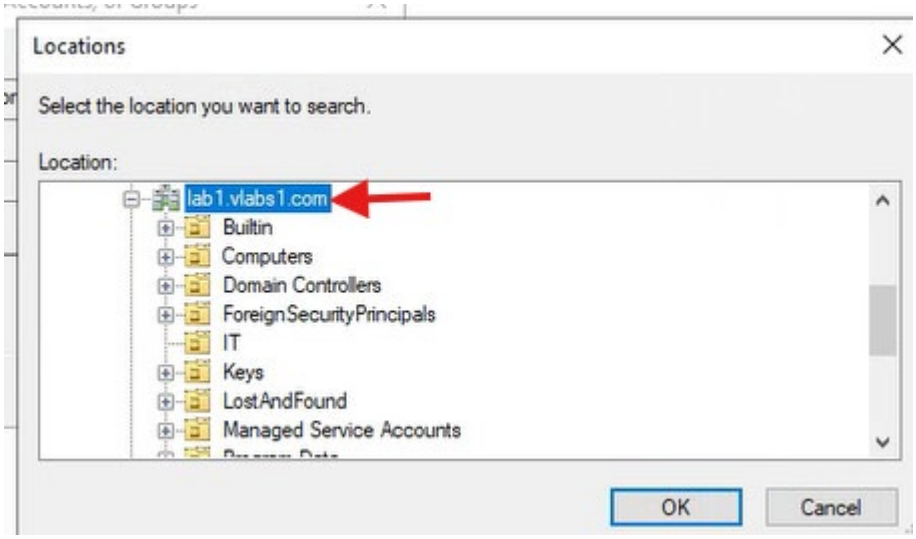
2. Add **GG_IT_Admins** from both **vlabs1.com** and **lab1.vlabs1.com** to **UG_IT_Global.**
   From DC101

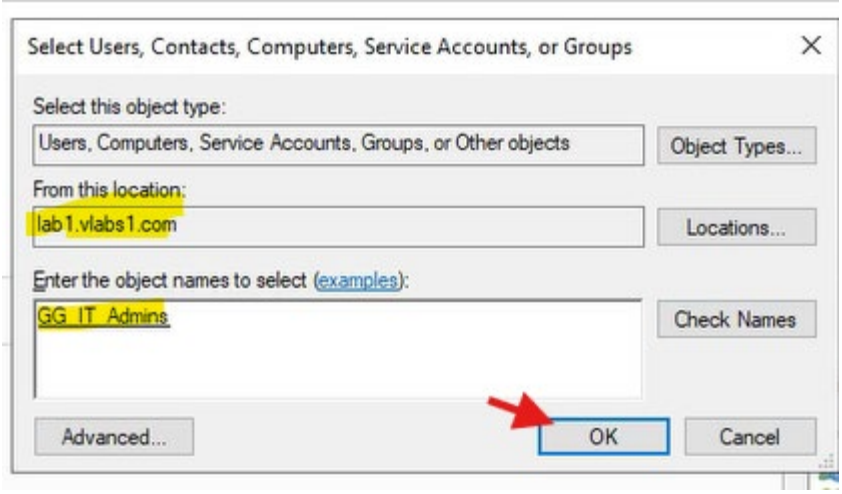


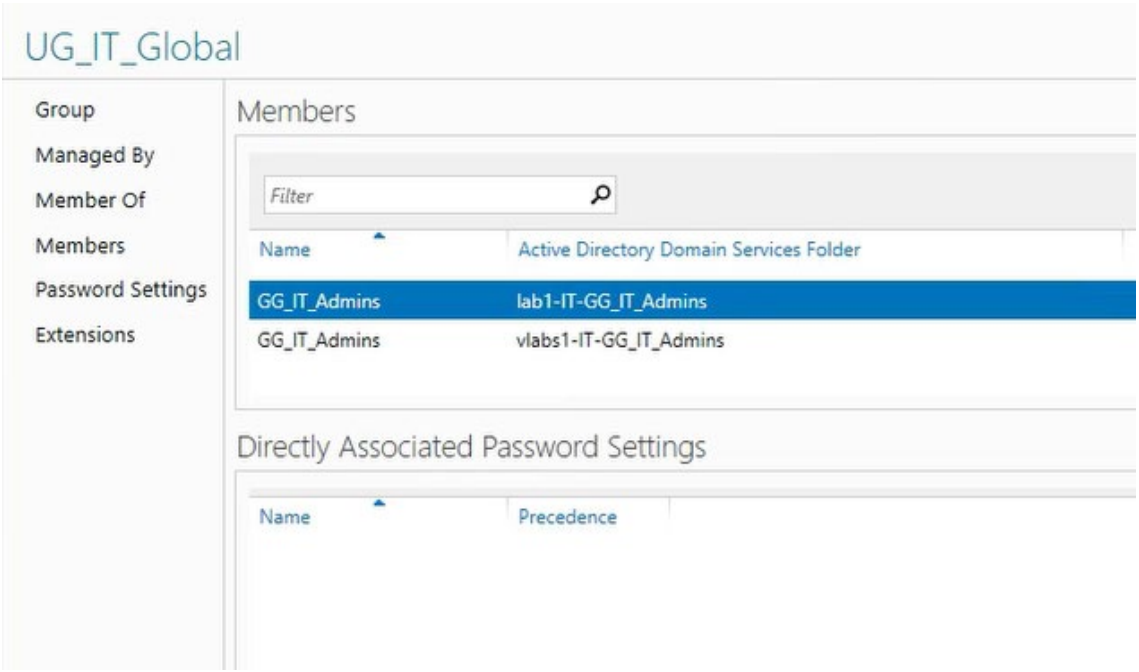
Location vlabs1



Location lab1

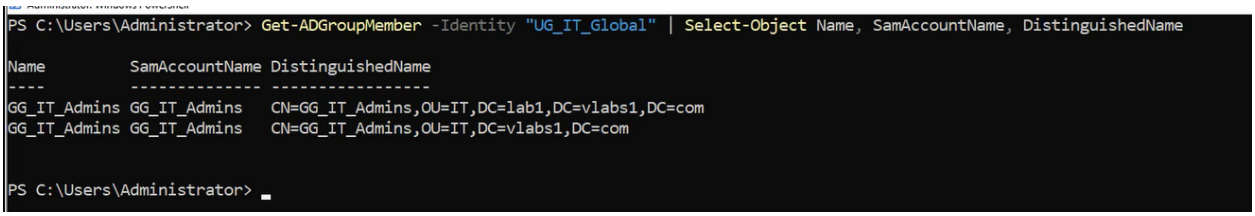






Verify

Get-ADGroupMember -Identity "UG_IT_Global" | Select-Object Name, SamAccountName, DistinguishedName



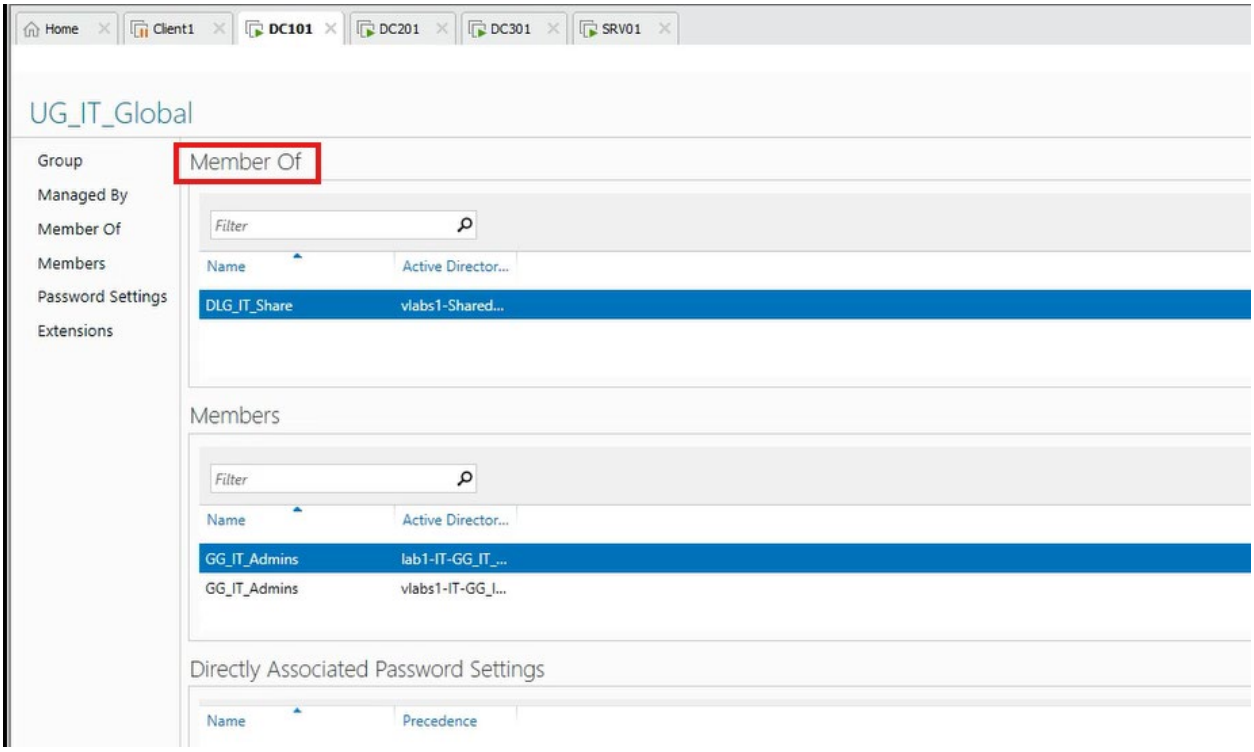
3. Add **UG_IT_Global** to the Domain Local group **DLG_IT_Share u**sing **PowerShell.**

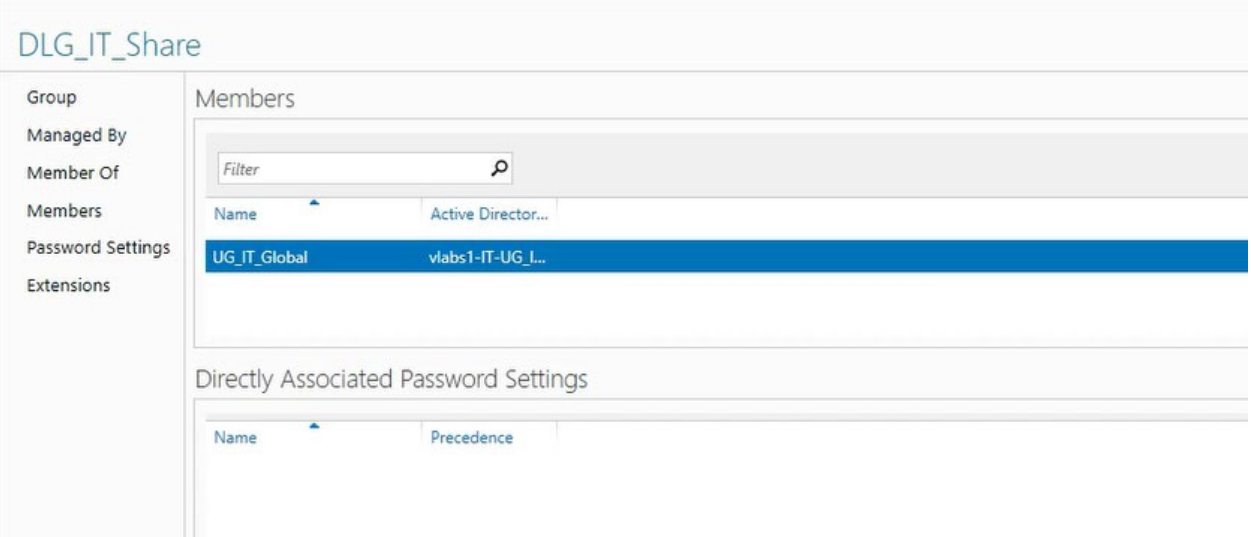
Add-ADGroupMember -Identity "DLG_IT_Share" -Members "UG_IT_Global"

Get-ADGroupMember -Identity "DLG_IT_Share" | Where-Object { $_.Name -eq "UG_IT_Global" }

```
PS C:\Users\Administrator> Add-ADGroupMember -Identity "DLG_IT_Share" -Members "UG_IT_Global"
PS C:\Users\Administrator> Get-ADGroupMember -Identity "DLG_IT_Share" | Where-Object { $_.Name -eq "UG_IT_Global" }


distinguishedName : CN=UG_IT_Global,OU=IT,DC=vlabs1,DC=com
name              : UG_IT_Global
objectClass       : group
objectGUID        : d37aa135-3879-4257-baff-c75d7180dc66
SamAccountName    : UG_IT_Global
SID               : S-1-5-21-1268601764-4050707287-4025116504-1121


PS C:\Users\Administrator>
```

Verify



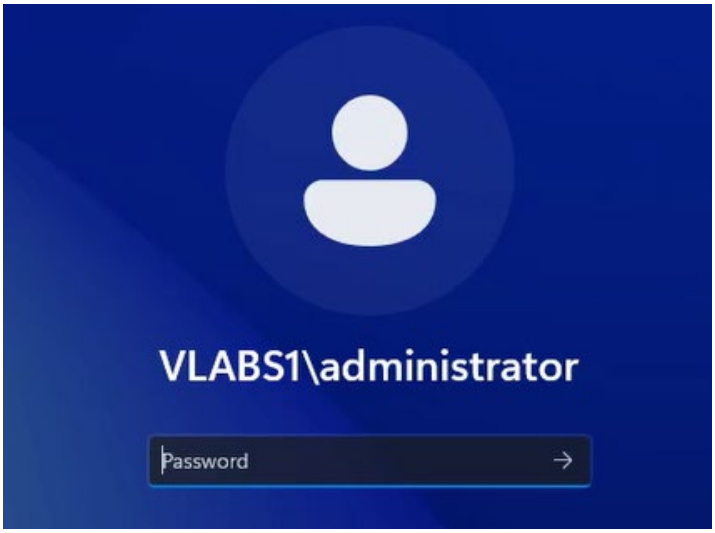


11 Task 9: Share and Set Permissions for IT Global Share

1. On **SRV01**, create and share **C:\IT_Share_Global** using **GUI**.

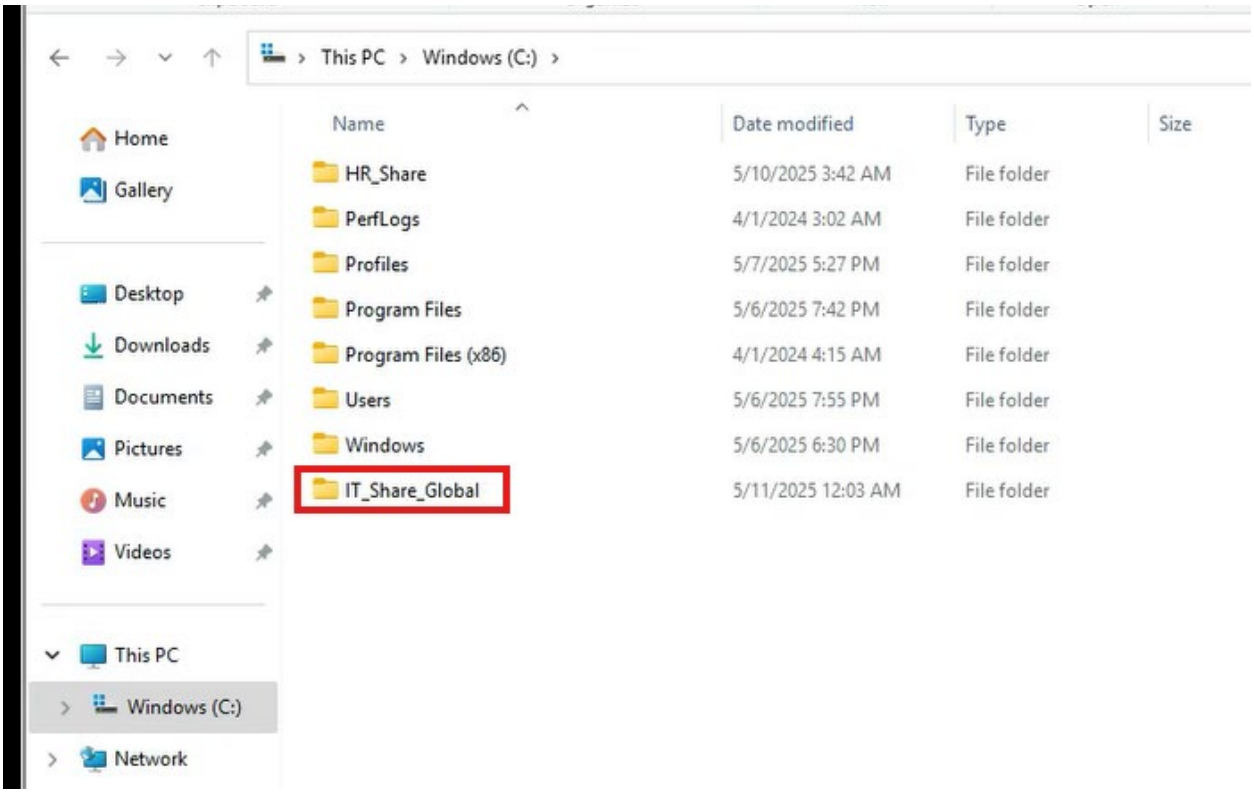
Create the Folder:

a) Log in to SRV01 as an administrator.



b) Open File Explorer → Navigate to C:\.

c) Right-click → New → Folder → Name it IT_Share_Global.



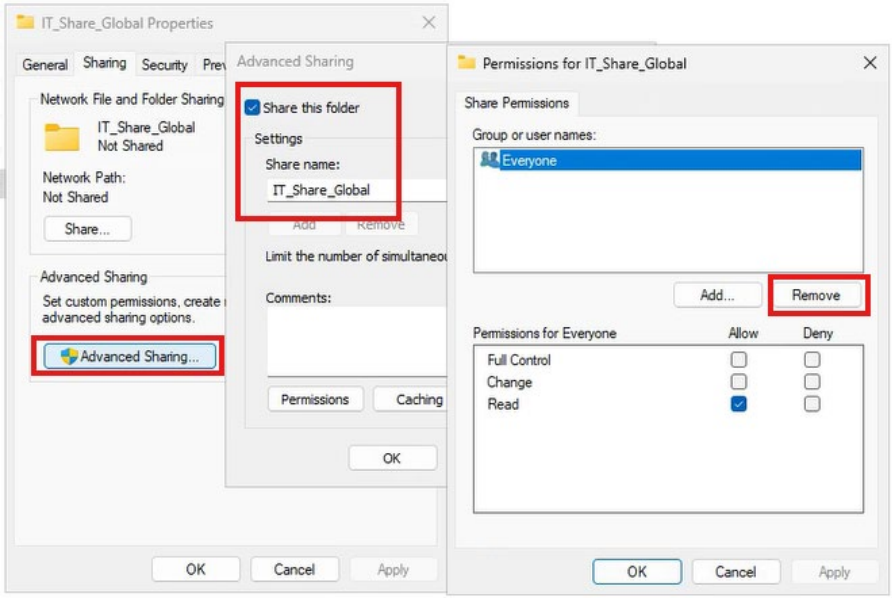
Permissions

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

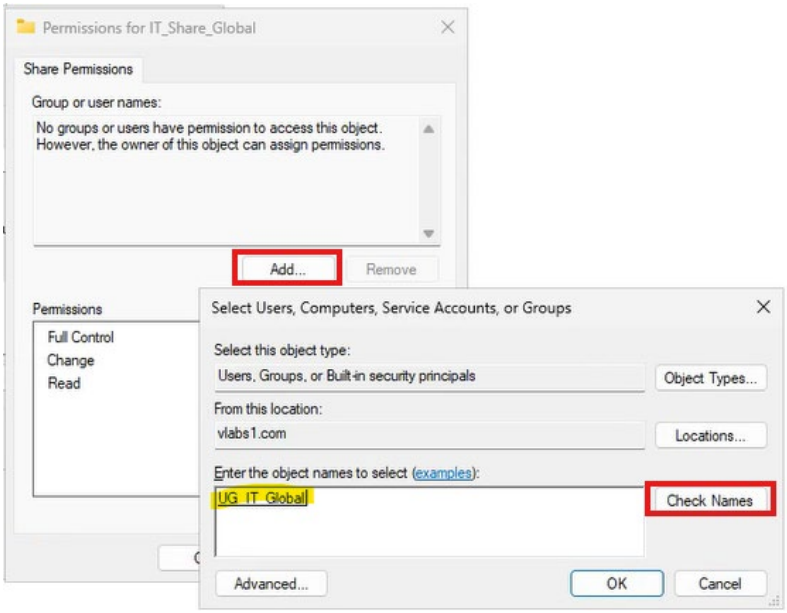
a) Share the Folder:
Right-click the folder → Properties → Sharing tab → Advanced Sharing.

b) Check Share this folder → Set Share name to IT_Share_Global.

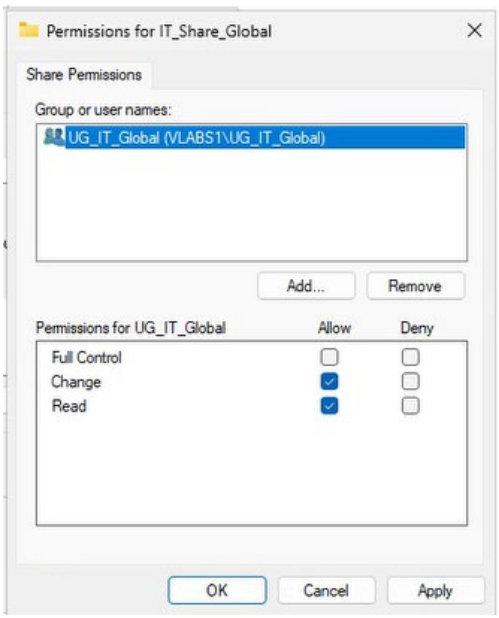
c) Click Permissions → Remove Everyone (select it → Remove).



d) Click Add → Type UG_IT_Global → Check Names → OK.

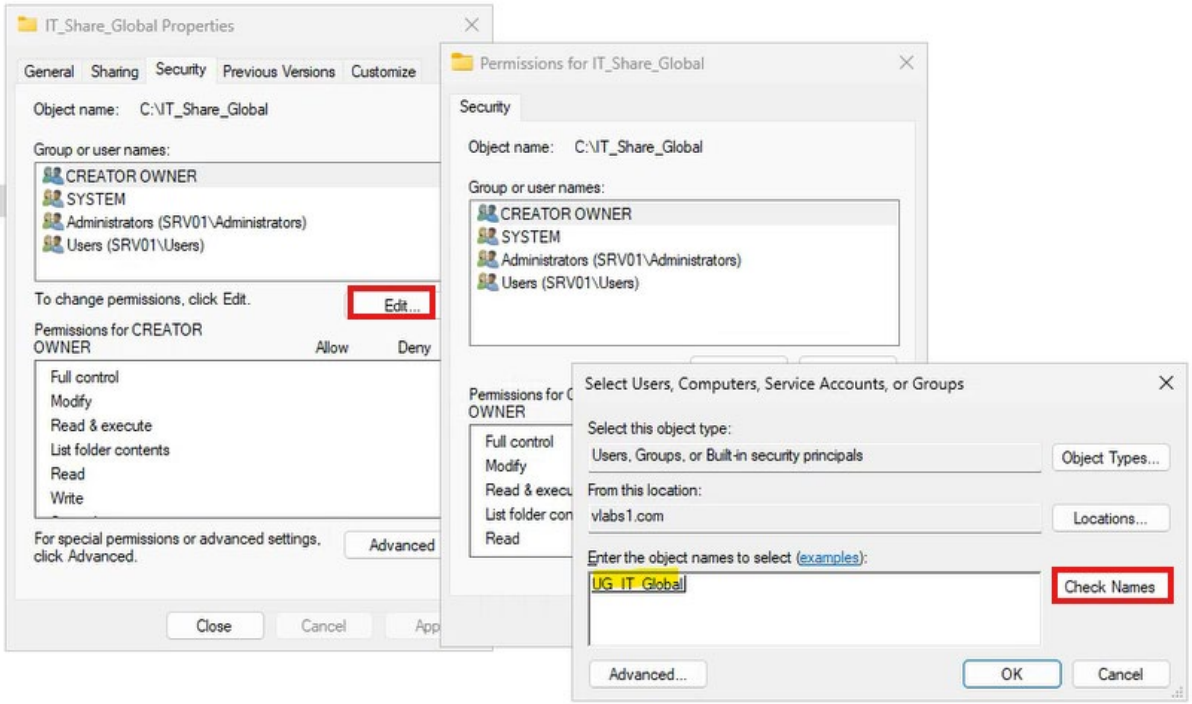


e) Select UG_IT_Global → Check Change (Read/Write) permissions → OK → OK.



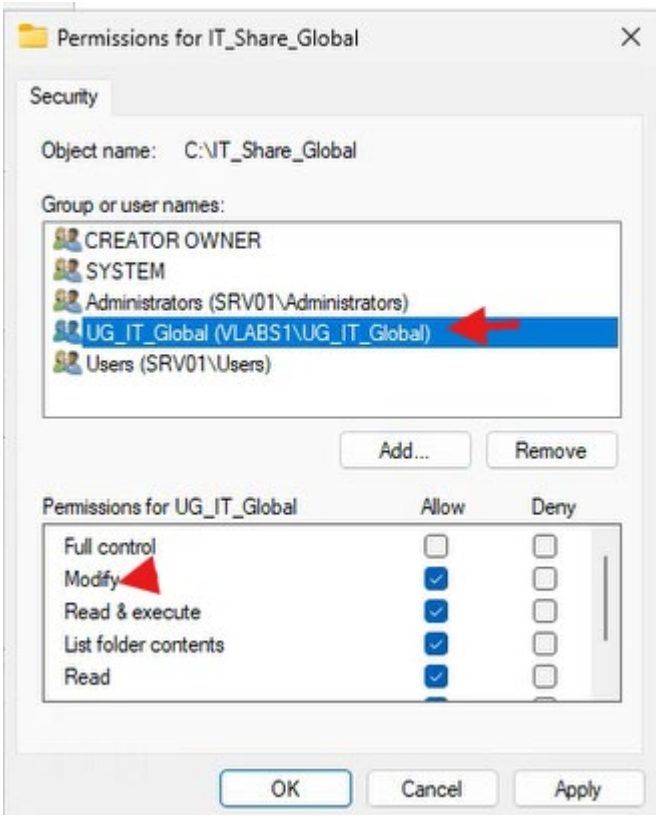
Set NTFS Permissions (GUI)

1. **Open Security Tab:**
    - Go to the folder's **Properties** → **Security** tab.
    - Click **Edit** → **Add** → Type UG_IT_Global → **Check Names** → **OK**.



2.

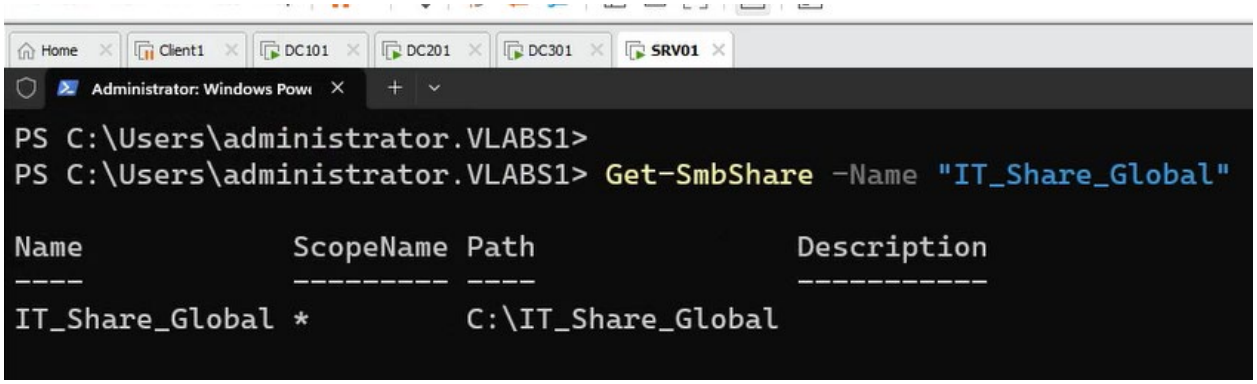
3. **Assign Permissions:**
    - Select UG_IT_Global → Check **Modify** (includes Read/Write) → **OK**.
    - Remove **Everyone** (if present) → Select it → **Remove** → **OK**.



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

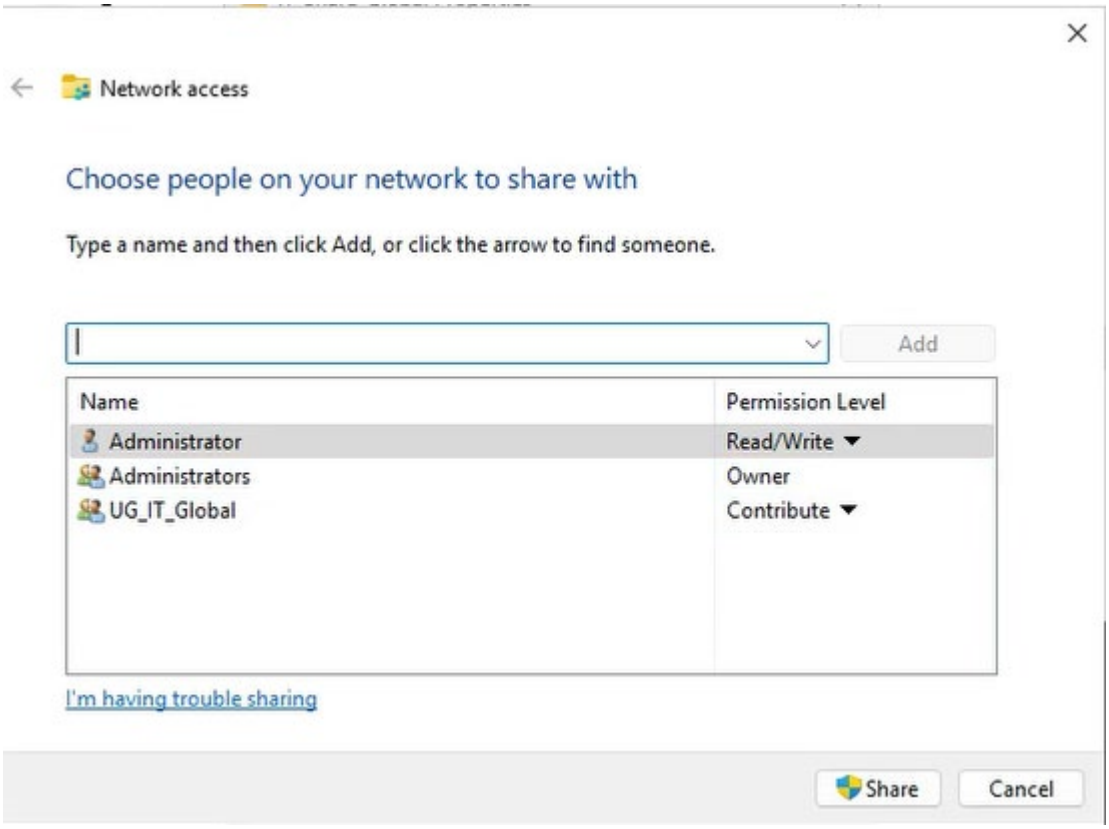
 # Check the Share:

Get-SmbShare -Name "IT_Share_Global"



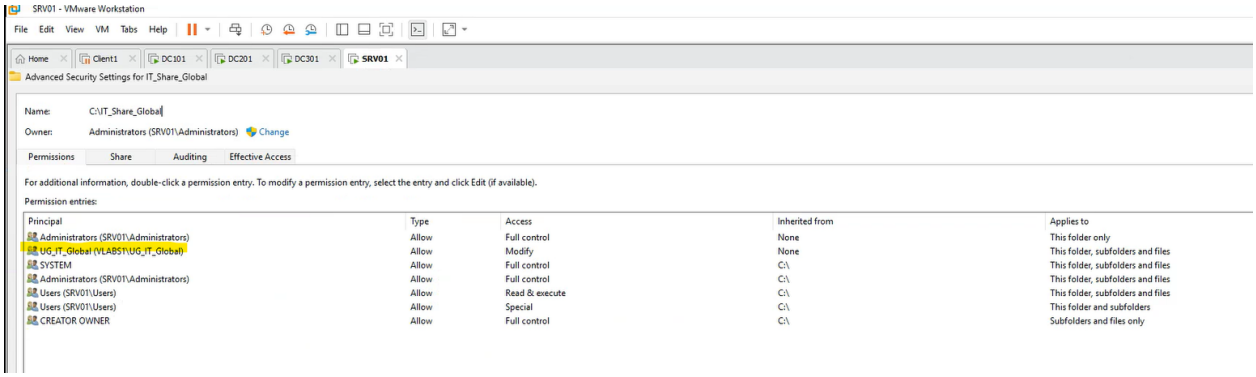
 # Verify Share Permissions:
Get-SmbShareAccess -Name "IT_Share_Global"

```
PS C:\Users\administrator.VLABS1> # Verify Share Permissions:
PS C:\Users\administrator.VLABS1> Get-SmbShareAccess -Name "IT_Share_Global"

Name            ScopeName AccountName         AccessControlType AccessRight
----            --------- -----------         ----------------- -----------
IT_Share_Global *         VLABS1\UG_IT_Global Allow             Change
```



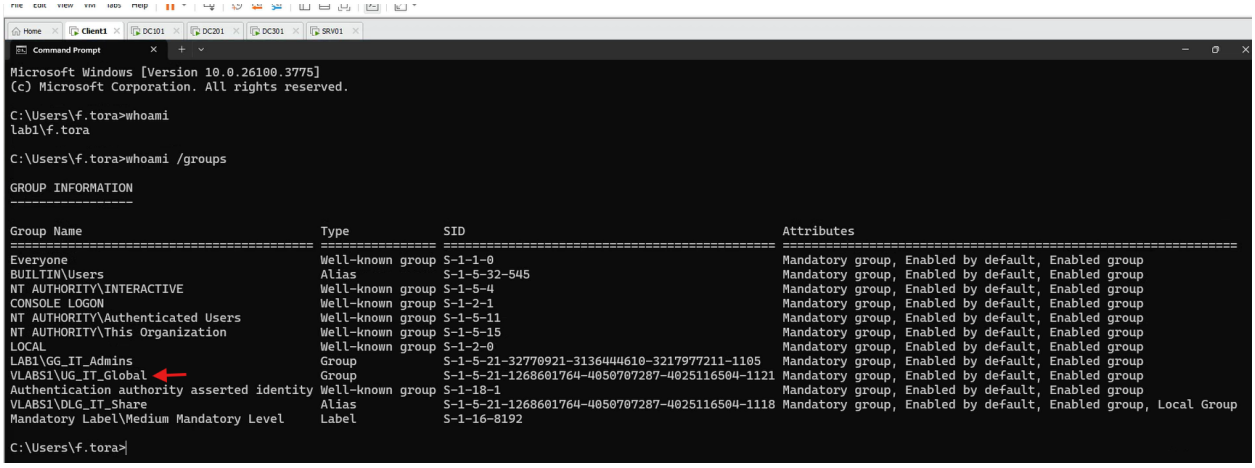
 # Verify NTFS Permissions:
(Get-Acl -Path "C:\IT_Share_Global").Access | Where-Object { $_.IdentityReference -like "*UG_IT_Global*" }

```
PS C:\Users\administrator.VLABS1> # Verify NTFS Permissions:
PS C:\Users\administrator.VLABS1> (Get-Acl -Path "C:\IT_Share_Global").Access | Where-Object { $_.IdentityReference -like "*UG_IT_Global*" }


FileSystemRights  : Modify, Synchronize
AccessControlType : Allow
IdentityReference : VLABS1\UG_IT_Global
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None
```



12 Task 10: Test IT Share Access from Client1

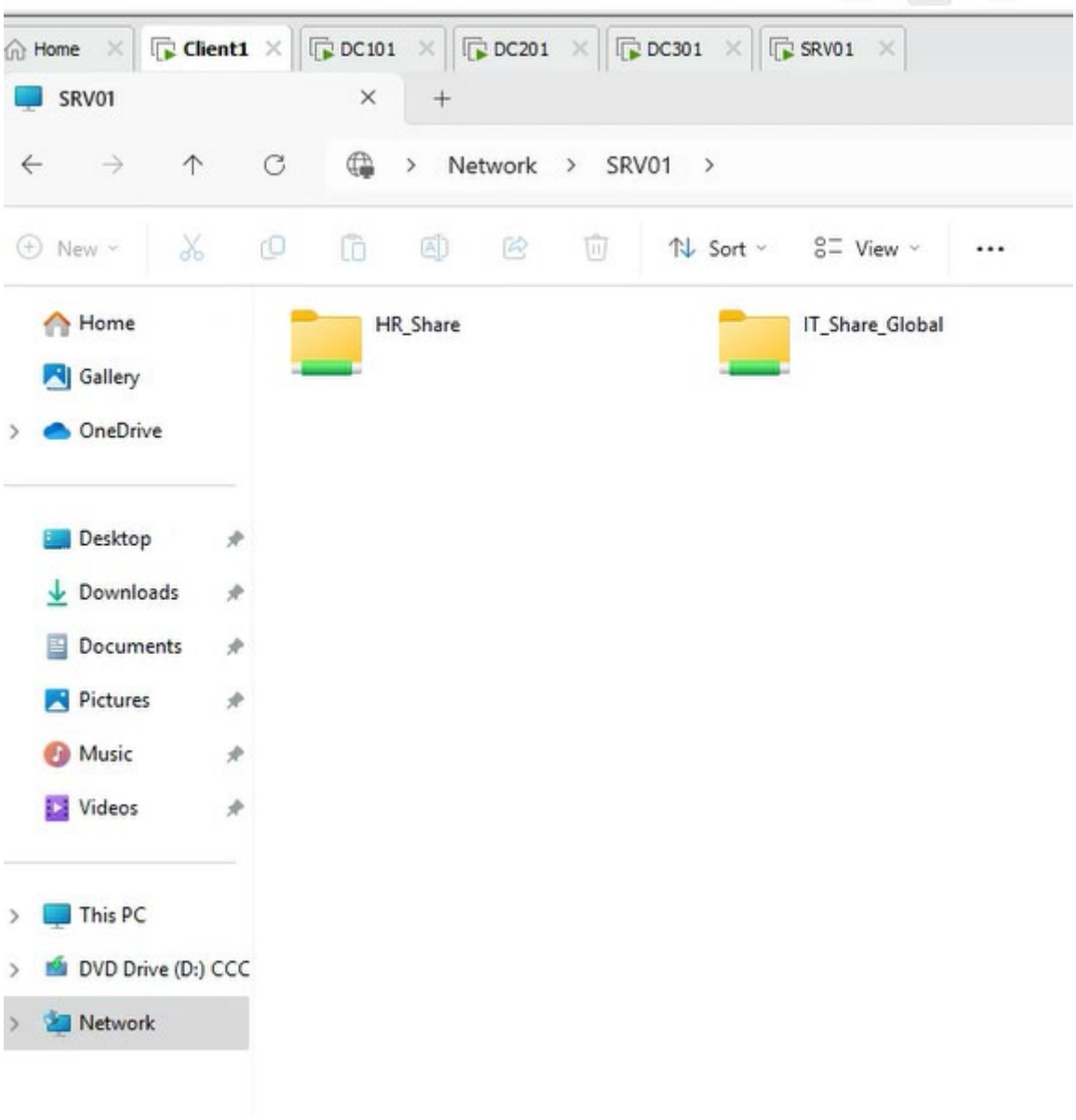
1. Log in as **Fadi Tora (f.tora)** on **Windows 11 (Client1).**
2. Check which groups **Fadi Tora** is a member of using **Command Prompt.**

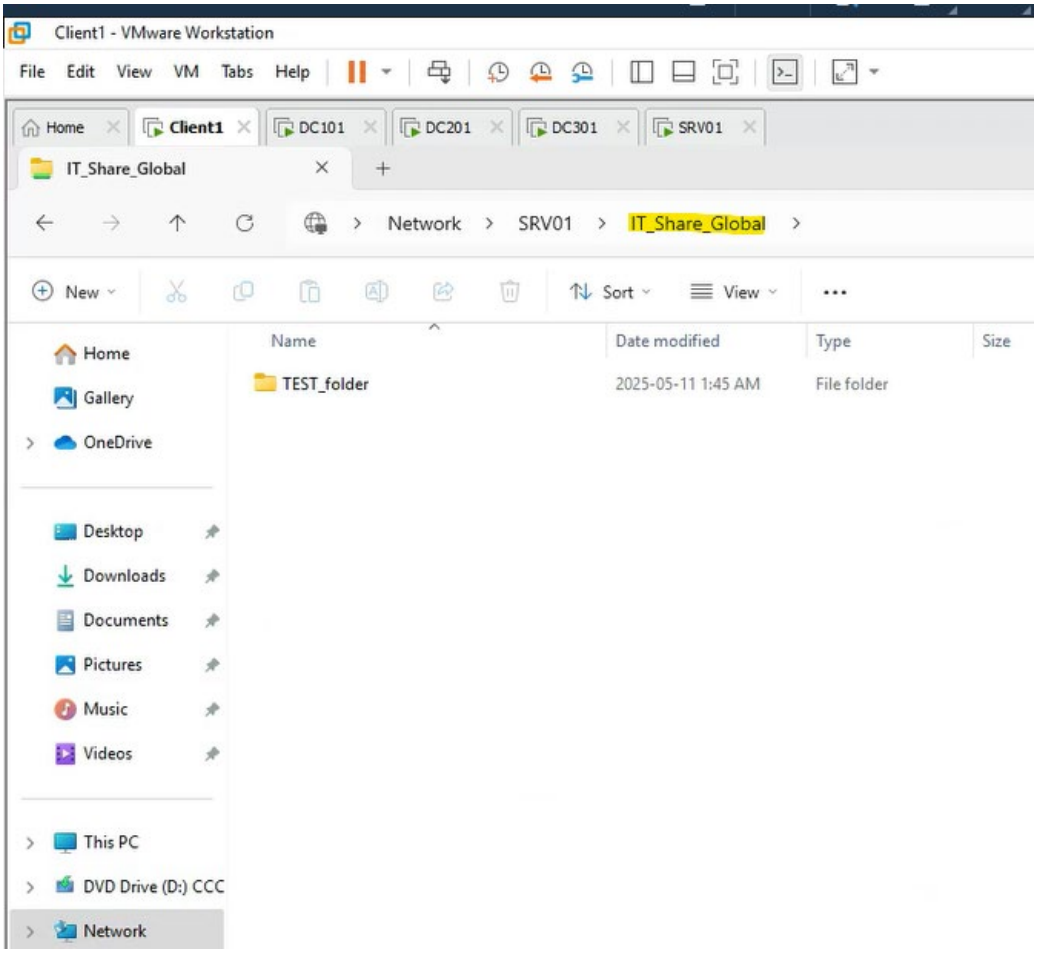


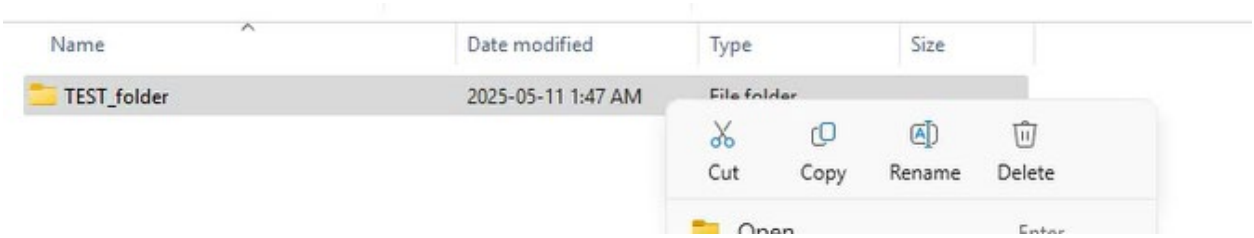
Look for membership in:

- GG_IT_Admins (Global Group, child domain)
- UG_IT_Global (Universal Group, parent domain)
- DLG_IT_Share (Domain Local Group, parent domain)

3. Access the shared folder **\\SRV01\IT_Share_Global$** and verify permissions by creating and deleting files in this share.



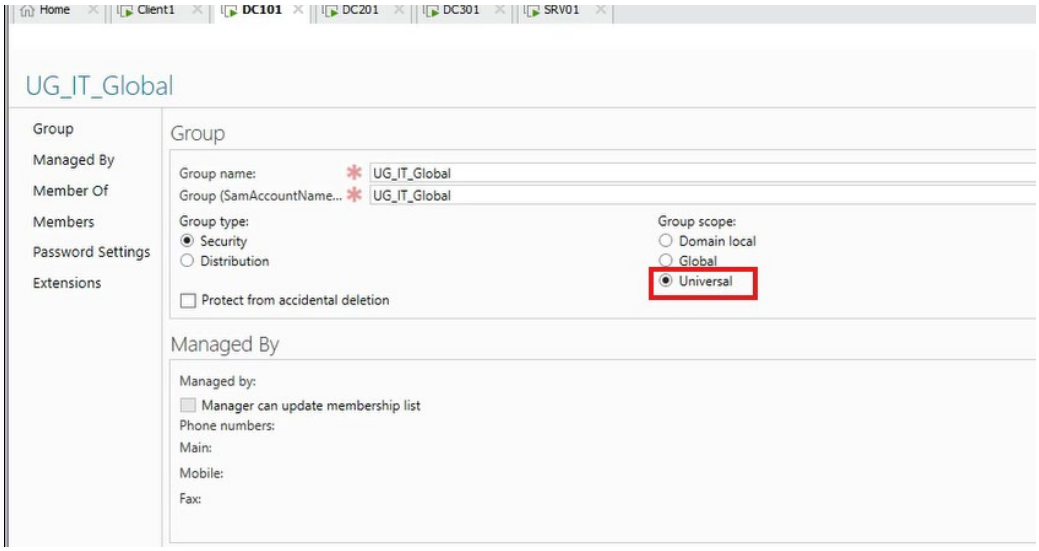




13 Task 11: Change Group Scope

1. On **DC101,** convert **UG_IT_Global** from **Universal** to **Global** using PowerShell.

   Verify current setup




```
PS C:\Users\Administrator> Set-ADGroup -GroupScope Global -Identity "CN=UG_IT_Global,OU=IT,DC=vlabs1,DC=com" -whatif
What if: Performing the operation "Set" on target "CN=UG_IT_Global,OU=IT,DC=vlabs1,DC=com".
PS C:\Users\Administrator> Set-ADGroup -GroupScope Global -Identity "CN=UG_IT_Global,OU=IT,DC=vlabs1,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=vl ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (CN=UG_IT_Global,OU=IT,DC=vlabs1,DC=com:ADGroup) [Set-ADGroup], ADException
    + FullyQualifiedErrorId : ActiveDirectoryServer:8519,Microsoft.ActiveDirectory.Management.Commands.SetADGroup

PS C:\Users\Administrator>
```

The error "A global group cannot have a cross-domain member" occurs because UG_IT_Global contains members from multiple domains (e.g., GG_IT_Admins from both vlabs1.com and lab1.vlabs1.com). Global groups can only include members from their own domain.

2. Verify that the group scope has changed correctly using **GUI.**
   Can not change the group