



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

1	Introduction	3
1.1	Objective	3
1.2	Lab Requirements.....	3
2	Topology.....	4
3	Task 1: Create and Manage Security Groups.....	4
3.1	Requirements	4
3.2	Create a Global Security Group using ADAC	4
3.2.1	Verify OU and Group Existence.....	4
3.2.2	Create the Group:	5
3.2.3	Verify Group Creation.....	6
3.3	Create a Global Security Group using PowerShell	7
3.3.1	Verify OU and Group Existence.....	7
3.3.2	Create the Group	8
3.3.3	Verify Group Creation.....	8
4	Task 2: Add Members to Groups.....	9
4.1	Requirements	9
4.1.1	Add members to GG_HR_Admins	9
4.1.2	Add members to GG_IT_Admins.....	12
5	Task 3: Create Organizational Units (OUs) and Domain Local Groups	14
5.1	Requirements	14
5.2	Create the Shared Resources OU using ADAC.....	15
5.3	Create Domain Local Group using ADAC	16
5.4	Create Domain Local Group using Powershell	17
5.5	GG_HR_Admins is nested into DLG_HR_Share.....	17
6	Task 4: Create a Local Group and Manage Membership	18
6.1	Requirements	18

6.2	Create a Local Group on SRV01 Using GUI	18
6.3	Add Domain Using GUI.....	20
6.4	Verify Membership Using PowerShell.....	22
7	Task 5: Share and Set Permissions on SRV01.....	23
7.1	Create and Share the Folder C:\HR_Share Using GUI	23
8	Task 6: Test HR Share Access from Client1	32
9	Task 7: Remove a User from a Group and Delete a User	34
9.1	Remove user using ADAC	34
9.2	Remove user using Powershell	35
10	Task 8: Create IT OU and Configure Groups on DC301 and DC101	36
10.1	DC301 Child Domain (lab1.vlabs1.com)	36
10.2	DC101 (Primary Domain Controller)	40
11	Task 9: Share and Set Permissions for IT Global Share.....	45
12	Task 10: Test IT Share Access from Client1	51
13	Task 11: Change Group Scope.....	53

Lab 5 - Managing Group Accounts in Active Directory

1 Introduction

1.1 Objective

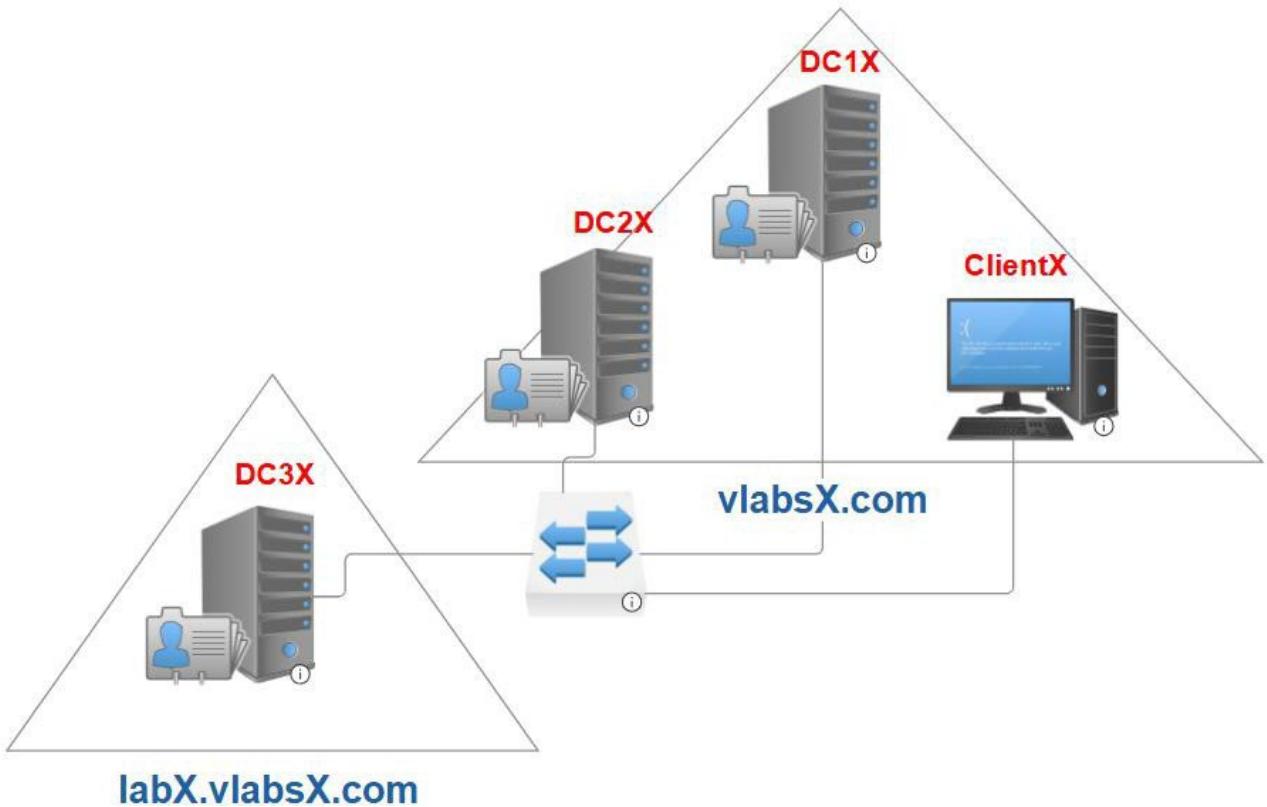
This lab will help you practice managing Active Directory groups using Active Directory Administrative Center (ADAC) and PowerShell.

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**.

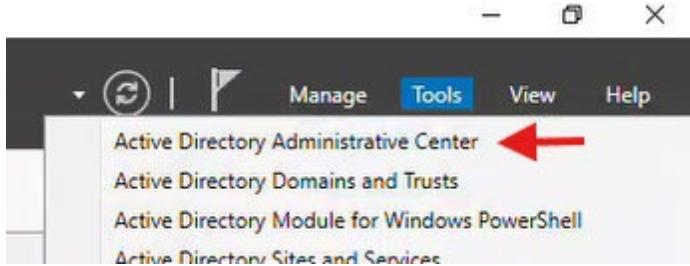
Actions (Commands and GUI) executed in DC101

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.



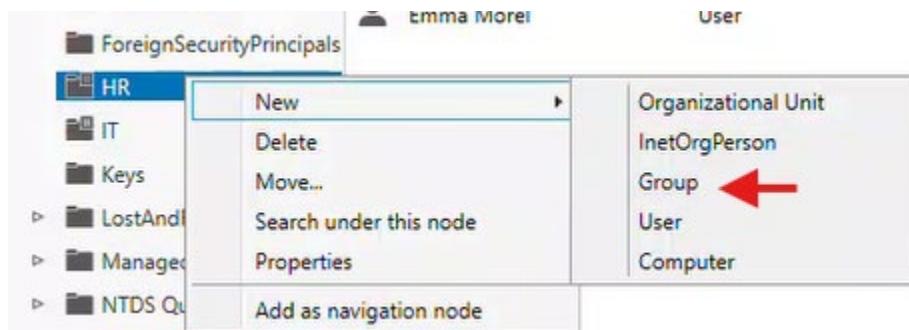
2. Navigate to HR OU under vlabs1.com.
3. Confirm the HR OU exists, and that GG_HR_Admins is not already present.

A screenshot of the Active Directory Administrative Center interface. The left navigation pane shows the structure: Active Directory... > vlabs1 (local) > HR. The 'HR' node is selected. The main pane displays a table titled 'HR (3)' showing three users: Lucas Bernard, HR Template, and Emma Morel. The 'HR Template' row is highlighted with a blue background. A red arrow points to the 'HR Template' user entry.

Name	Type	Description
Lucas Bernard	User	
HR Template	User	Template user for HR new hires.
Emma Morel	User	

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

Create Group: GG_HR_Admins

Group	Group Group name: <input type="text" value="GG_HR_Admins"/> * Group (SamAccountName...): <input type="text" value="GG_HR_Admins"/> *
Managed By	
Member Of	
Members	Group type: <input checked="" type="radio"/> Security <input type="radio"/> Distribution
Password Settings	Group scope: <input type="radio"/> Domain local <input checked="" type="radio"/> Global <input type="radio"/> Universal
<input type="checkbox"/> Protect from accidental deletion	
Managed By	
Managed by: <input type="checkbox"/> Manager can update membership list Phone numbers:	

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.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane lists various OUs and administrative sections. The 'HR' OU is selected and highlighted in blue. The right pane displays a list of objects within the HR OU, including four entries: 'Lucas Bernard' (User), 'HR Template' (User), 'Emma Morel' (User), and 'GG_HR_Admins' (Group). A red arrow points to the 'GG_HR_Admins' entry.

Name	Type	Description
Lucas Bernard	User	
HR Template	User	Template user for HR new hires.
Emma Morel	User	
GG_HR_Admins	Group	

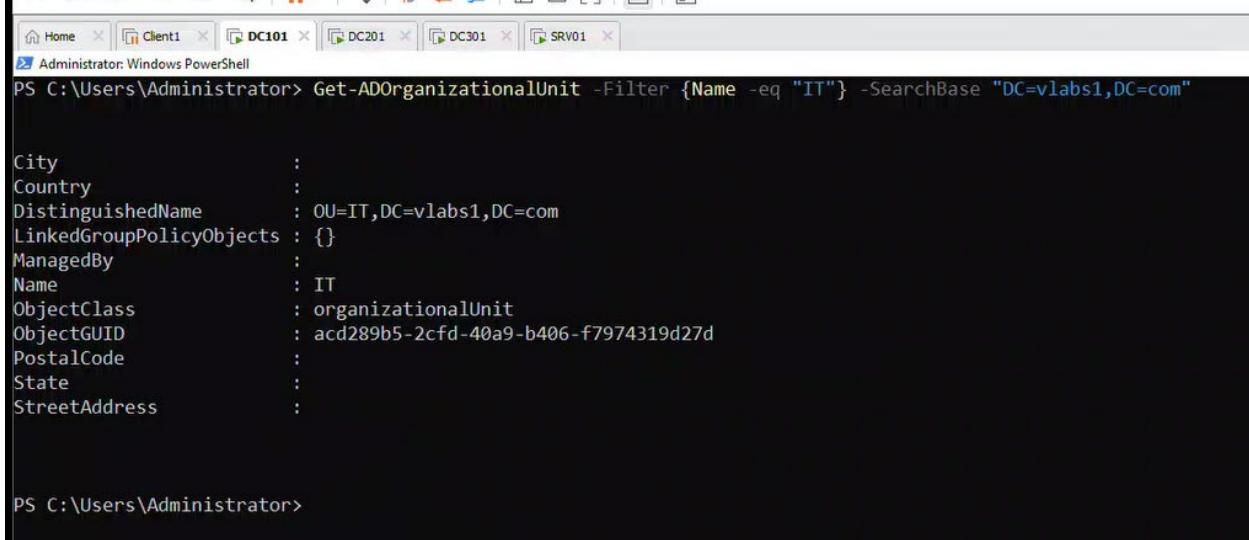
3.3 Create a Global Security Group using PowerShell

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"
```



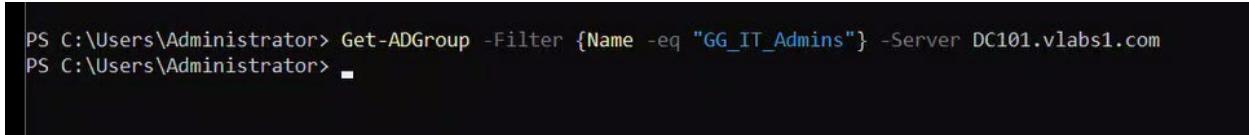
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter {Name -eq "IT"} -SearchBase "DC=vlabs1,DC=com"

City          :
Country       :
DistinguishedName : OU=IT,DC=vlabs1,DC=com
LinkdGroupPolicyObjects : {}
ManagedBy      :
Name          : IT
ObjectClass    : organizationalUnit
ObjectGUID     : acd289b5-2cf8-40a9-b406-f7974319d27d
PostalCode     :
State         :
StreetAddress  :


PS C:\Users\Administrator>
```

2. Check if group exists

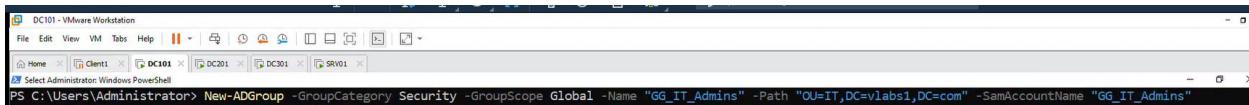
Get-ADGroup -Filter {Name -eq "GG_IT_Admins"} -Server DC101.vlabs1.com



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

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"



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> 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

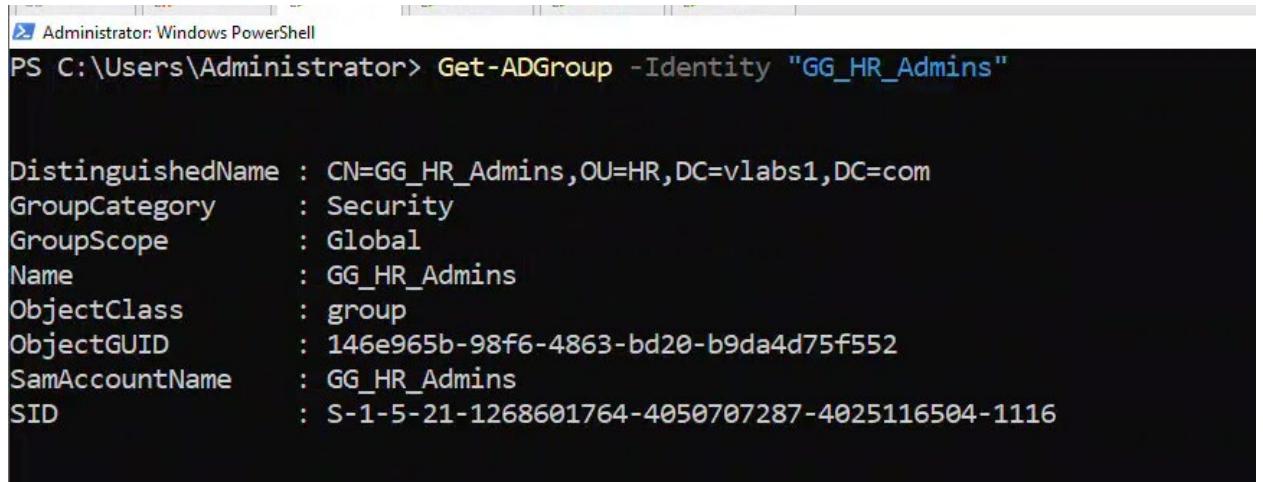
4.1 Requirements

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"



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

DistinguishedName : CN=GG_HR_Admins,OU=HR,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : GG_HR_Admins
ObjectClass       : group
ObjectGUID        : 146e965b-98f6-4863-bd20-b9da4d75f552
SamAccountName   : GG_HR_Admins
SID               : S-1-5-21-1268601764-4050707287-4025116504-1116
```

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"

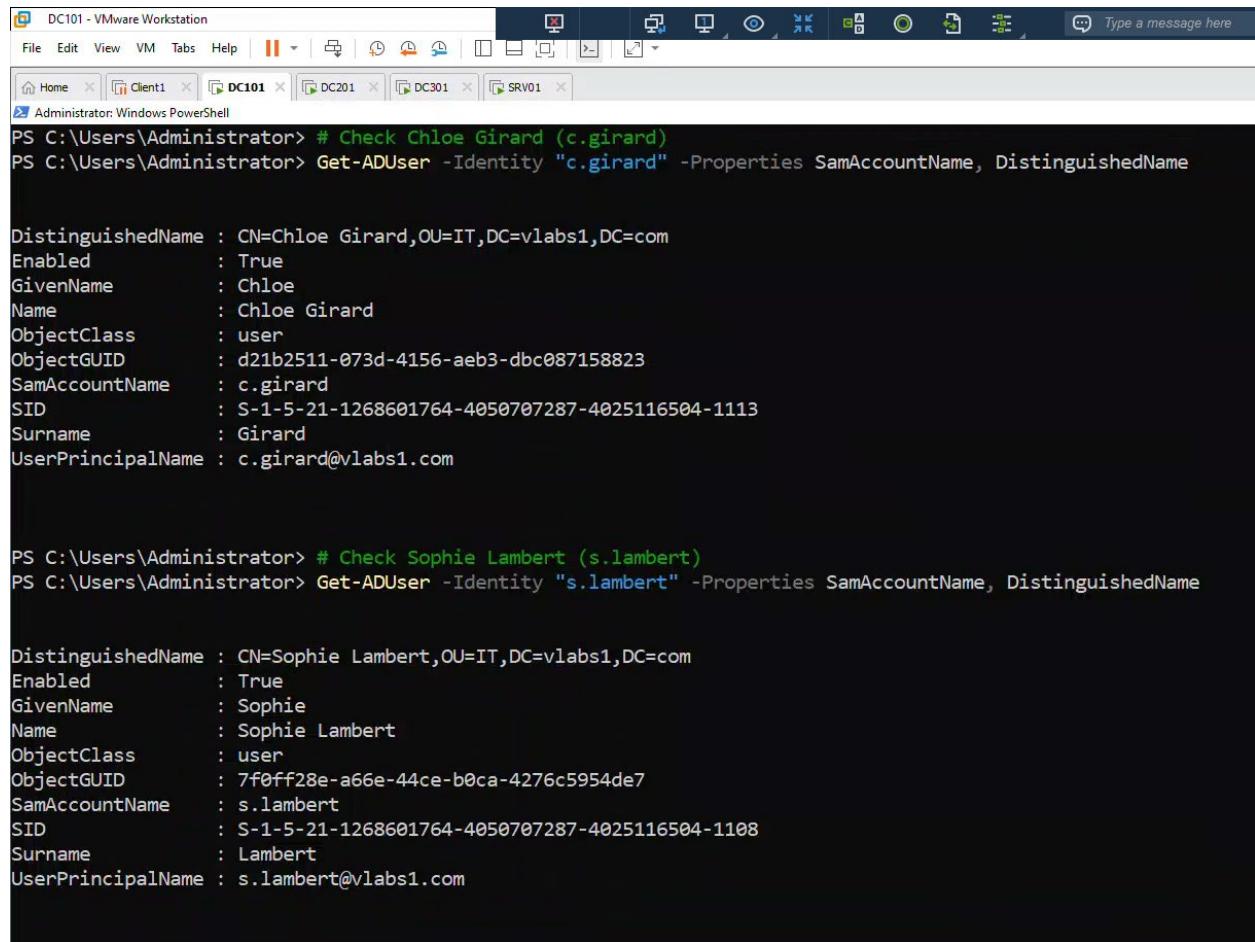
DistinguishedName : CN=GG_IT_Admins,OU=IT,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : GG_IT_Admins
ObjectClass       : group
ObjectGUID        : 99c47997-bc7c-46f0-95f2-330e7d0066ac
SamAccountName   : GG_IT_Admins
SID               : S-1-5-21-1268601764-4050707287-4025116504-1117

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
```



```
PS C:\Users\Administrator> # Check Chloe Girard (c.girard)
PS C:\Users\Administrator> Get-ADUser -Identity "c.girard" -Properties SamAccountName, DistinguishedName

DistinguishedName : CN=Chloe Girard,OU=IT,DC=vlabs1,DC=com
Enabled          : True
GivenName        : Chloe
Name             : Chloe Girard
ObjectClass      : user
ObjectGUID       : d21b2511-073d-4156-aeb3-dbc087158823
SamAccountName   : c.girard
SID              : S-1-5-21-1268601764-4050707287-4025116504-1113
Surname          : Girard
UserPrincipalName : c.girard@vlabs1.com

PS C:\Users\Administrator> # Check Sophie Lambert (s.lambert)
PS C:\Users\Administrator> Get-ADUser -Identity "s.lambert" -Properties SamAccountName, DistinguishedName

DistinguishedName : CN=Sophie Lambert,OU=IT,DC=vlabs1,DC=com
Enabled          : True
GivenName        : Sophie
Name             : Sophie Lambert
ObjectClass      : user
ObjectGUID       : 7f0ff28e-a66e-44ce-b0ca-4276c5954de7
SamAccountName   : s.lambert
SID              : S-1-5-21-1268601764-4050707287-4025116504-1108
Surname          : Lambert
UserPrincipalName : s.lambert@vlabs1.com
```

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

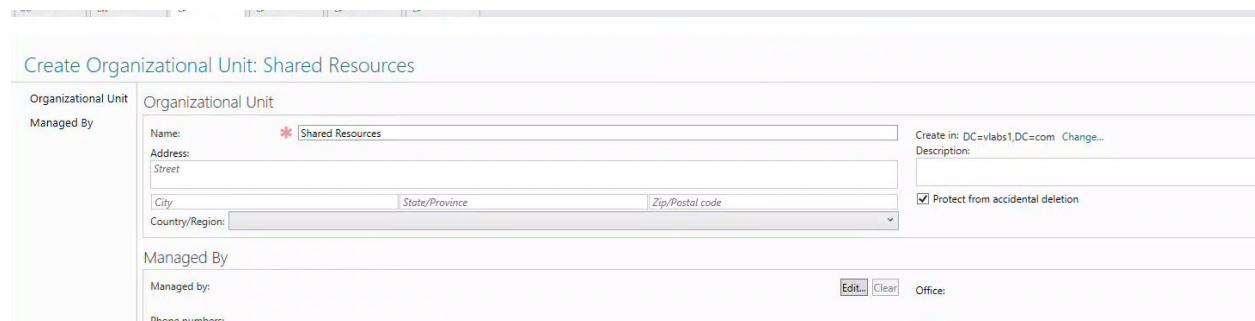
1. Create an OU named **Shared Resources** in **v labs1.com** domain using **ADAC**.
2. Create a **Domain Local Group (DLG_HR_Share)** in **Shared Resources** using **ADAC**.
3. Create a **Domain Local Group (DLG_IT_Share)** in **Shared Resources** using **PowerShell**.

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.



The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is expanded to show the 'vlabs1 (local)' container, which includes 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'HR', 'IT', 'Keys', 'LostAndFound', 'Managed Service Accounts', 'NTDS Quotas', 'Program Data', 'Shared Resources', 'System', 'TPM Devices', 'Users', 'Dynamic Access Control', 'Authentication', and 'Global Search'. The main pane displays a table of objects under 'vlabs1 (local) (16)'. The table has columns for 'Name', 'Type', and 'Description'. One row for 'Shared Resources' is highlighted with a red arrow pointing to it. Other rows include 'IT' (Organizational Unit), 'HR' (Organizational Unit), 'Domain Controllers' (Organizational Unit), 'TPM Devices' (msTPM-InformationObjectsContainer), 'NTDS Quotas' (msDS-QuotaContainer), 'LostAndFound' (lostAndFound), 'Infrastructure' (infrastructureUpdate), 'ForeignSecurityPrincipals' (Container), 'Managed Service Accounts' (Container), 'System' (Container), 'Users' (Container), 'Program Data' (Container), 'Keys' (Container), 'Computers' (Container), and 'Builtin' (builtinDomain). Descriptions for some objects mention they are default containers for specific types of objects.

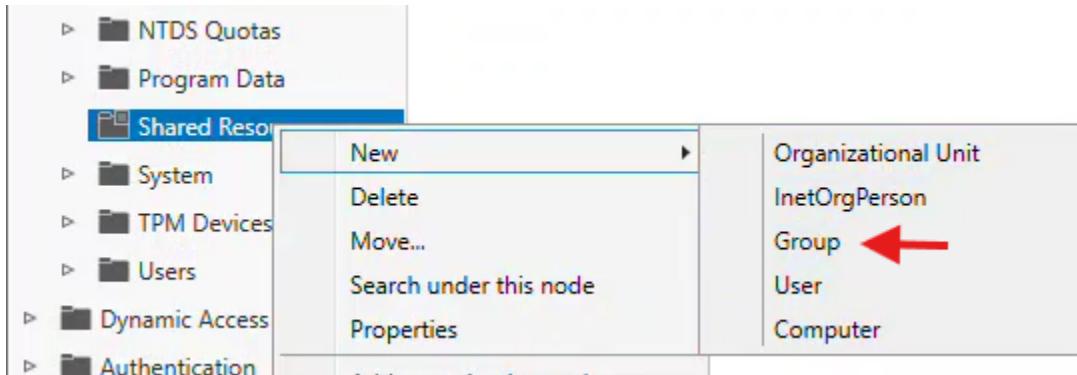
Name	Type	Description
IT	Organizational Unit	
HR	Organizational Unit	
Shared Resources	Organizational Unit	Default container for domain controllers
Domain Controllers	Organizational Unit	
TPM Devices	msTPM-InformationObjectsContainer	
NTDS Quotas	msDS-QuotaContainer	Quota specifications container
LostAndFound	lostAndFound	Default container for orphaned objects
Infrastructure	infrastructureUpdate	
ForeignSecurityPrincipals	Container	Default container for security identifiers (SIDs) associated...
Managed Service Accounts	Container	Default container for managed service accounts
System	Container	Builtin system settings
Users	Container	Default container for upgraded user accounts
Program Data	Container	Default location for storage of application data.
Keys	Container	Default container for key objects
Computers	Container	Default container for upgraded computer accounts
Builtin	builtinDomain	

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:
 - o **Group name:** DLG_HR_Share
 - o **Group scope:** Domain Local
 - o **Group type:** Security
4. Click **OK**.



Create Group: DLG_HR_Share

Group	Group Group name: <input type="text" value="DLG_HR_Share"/> * Group (SamAccountName...): <input type="text" value="DLG_HR_Share"/> * Group type: <input checked="" type="radio"/> Security <input type="radio"/> Distribution <input type="checkbox"/> Protect from accidental deletion	Group scope:	<input checked="" type="radio"/> Domain local <input type="radio"/> Global <input type="radio"/> Universal
Managed By	Managed By Managed by: <input type="checkbox"/> Manager can update membership list Phone numbers: Main: Mobile: Fax:		
Member Of			
Members			
Password Settings			

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
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-ADGroup -Name "DLG_IT_Share" -GroupCategory Security -GroupScope DomainLocal -Path "OU=Shared Resources,DC=vlabs1,DC=com" -SamAccountName "DLG_IT_Share"
PS C:\Users\Administrator> Get-ADGroup -Identity "DLG_IT_Share" -Properties GroupScope, DistinguishedName | Select-Object Name, GroupScope, DistinguishedName
Name      GroupScope DistinguishedName
----      -----
DLG_IT_Share DomainLocal CN=DLG_IT_Share,OU=Shared Resources,DC=vlabs1,DC=com

PS C:\Users\Administrator>
```

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"
```

```
PS C:\Users\Administrator> # Check if GG_HR_Admins is in DLG_HR_Share  
PS C:\Users\Administrator> Get-ADGroupMember -Identity "DLG_HR_Share" | Select-Object Name  
PS C:\Users\Administrator> #Adding a Global group to a Domain Local group  
PS C:\Users\Administrator>  
PS C:\Users\Administrator> Add-ADGroupMember -Identity "DLG_HR_Share" -Members "GG_HR_Admins"  
PS C:\Users\Administrator> # Verify  
PS C:\Users\Administrator>  
PS C:\Users\Administrator> Get-ADGroupMember -Identity "DLG_HR_Share"  
  
distinguishedName : CN=GG_HR_Admins,OU=HR,DC=vlabs1,DC=com  
name : GG_HR_Admins  
objectClass : group  
objectGUID : 146e965b-98f6-4863-bd20-b9da4d75f552  
SamAccountName : GG_HR_Admins  
SID : S-1-5-21-1268601764-4050707287-4025116504-1116  
  
PS C:\Users\Administrator>  
PS C:\Users\Administrator>
```

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 into **LG_HR_Files** group using **GUI**.
3. Verify the membership of **LG_HR_Files** group using **PowerShell**.

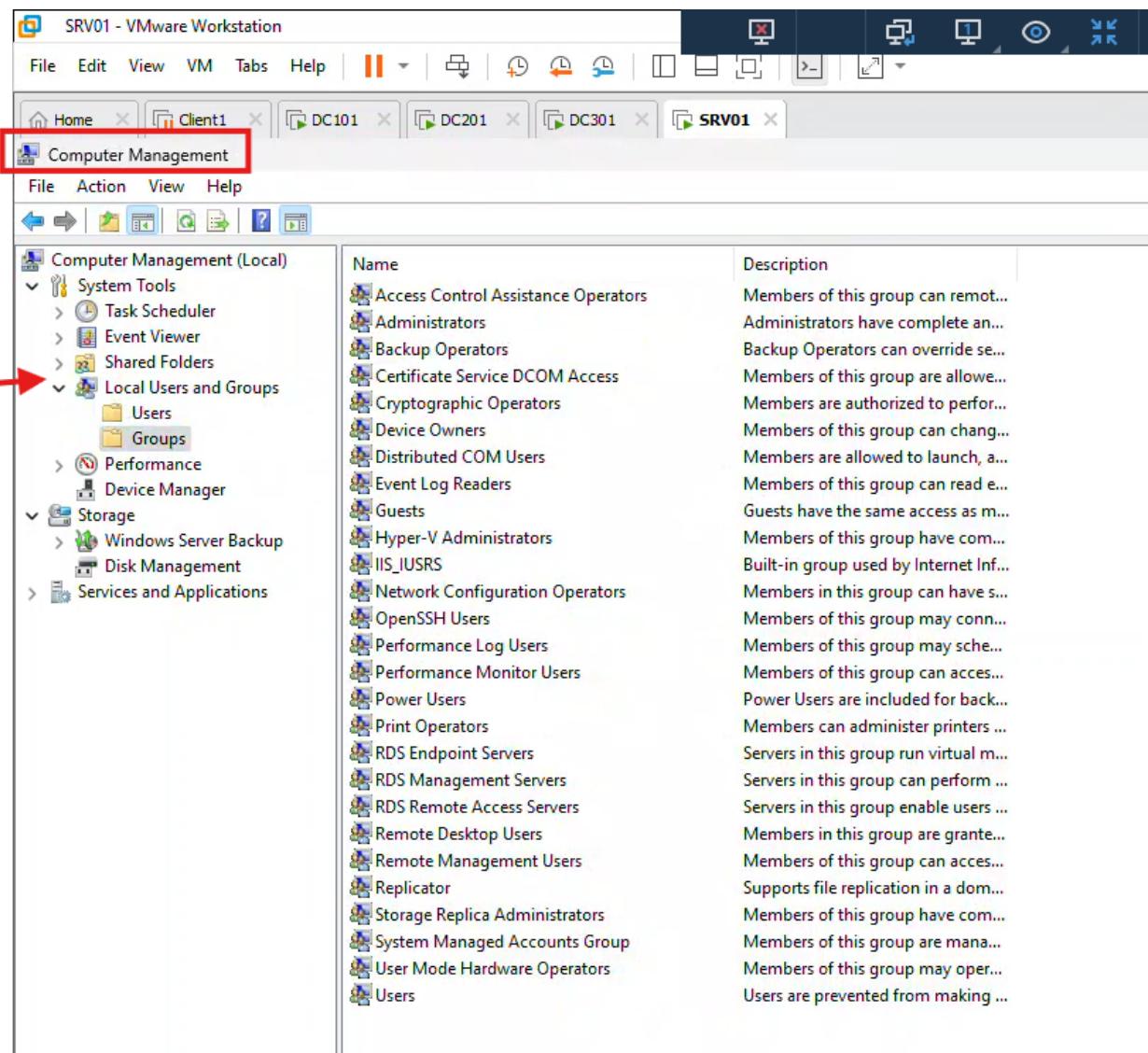
6.2 Create a Local Group on SRV01 Using GUI

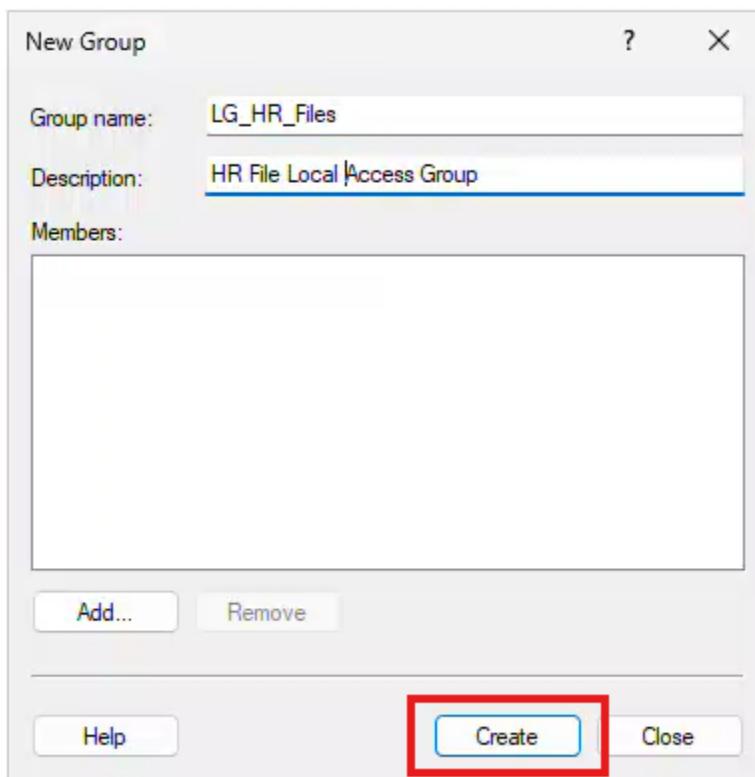
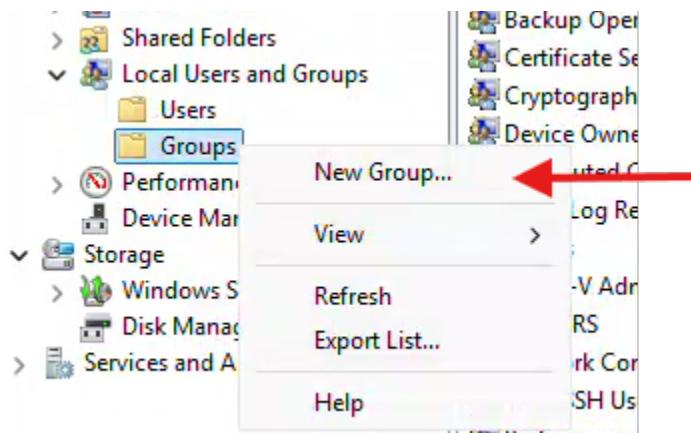
Create a Local Group **LG_HR_Files** on SRV01 Using GUI

Steps:

1. **Log in to SRV01** with administrative privileges.
2. Open **Computer Management**:
 - o 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**.





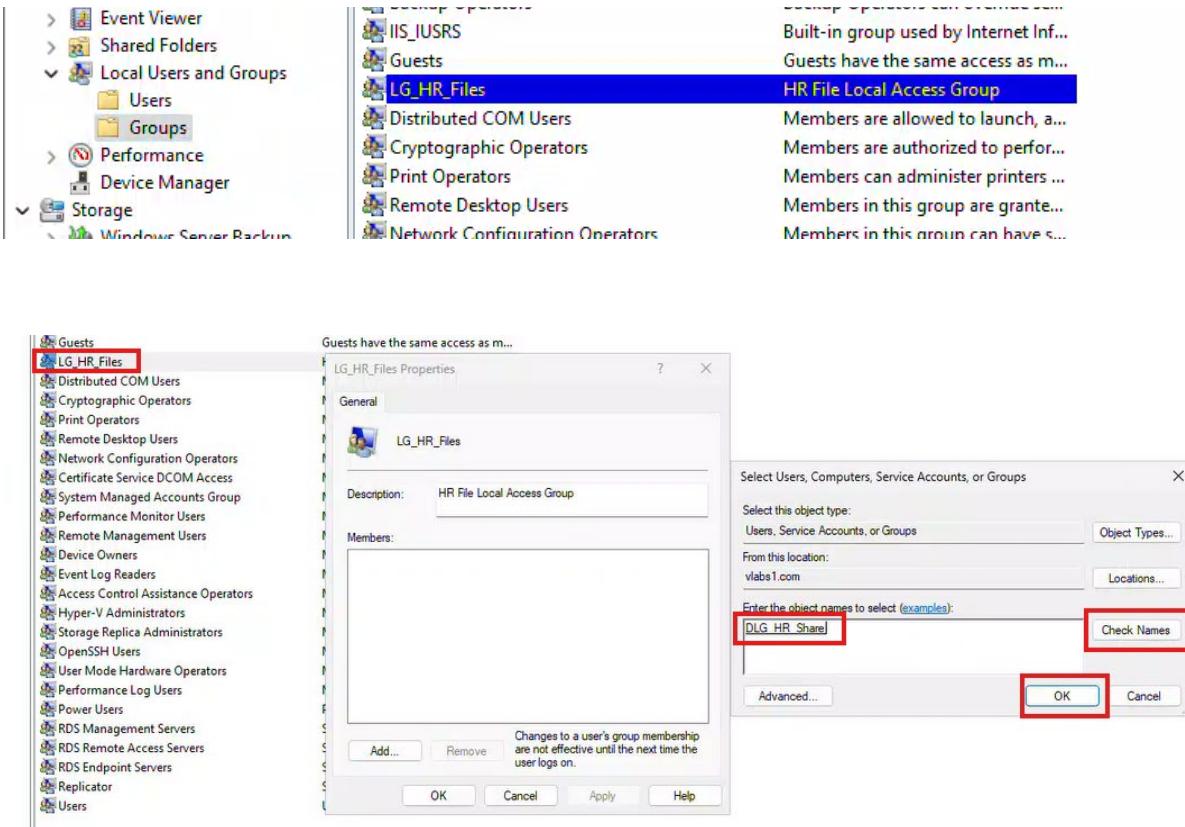
6.3 Add Domain Using GUI

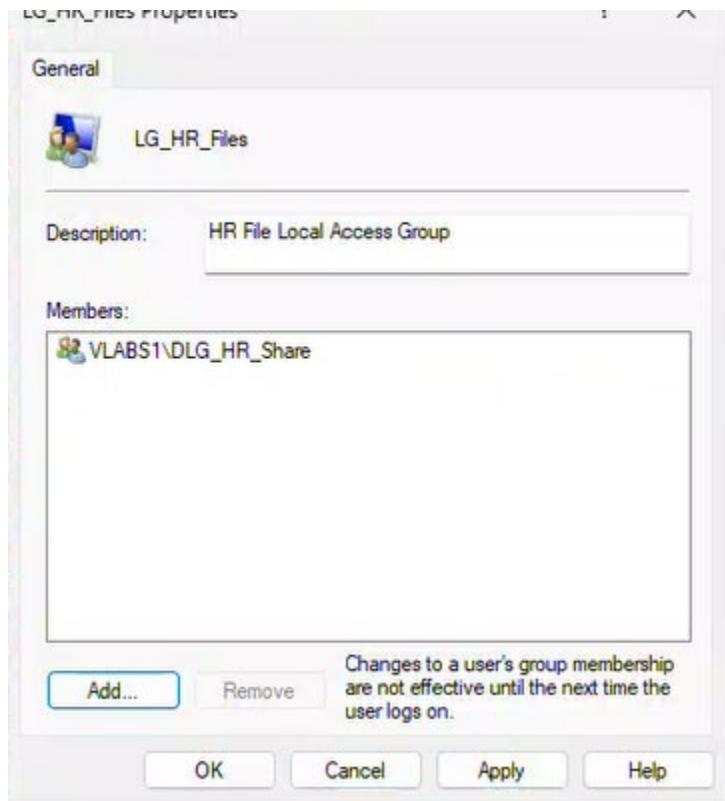
Add Domain Group DLG_HR_Share to LG_HR_Files Using GUI

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:
 - o Under From this location, ensure the domain (vlabs1.com) is selected.
 - o Enter DLG_HR_Share → Click Check Names to validate.
 - o If resolved correctly, it will appear as DLG_HR_Share (Group from vlabs1.com).
4. Click OK → OK to save.



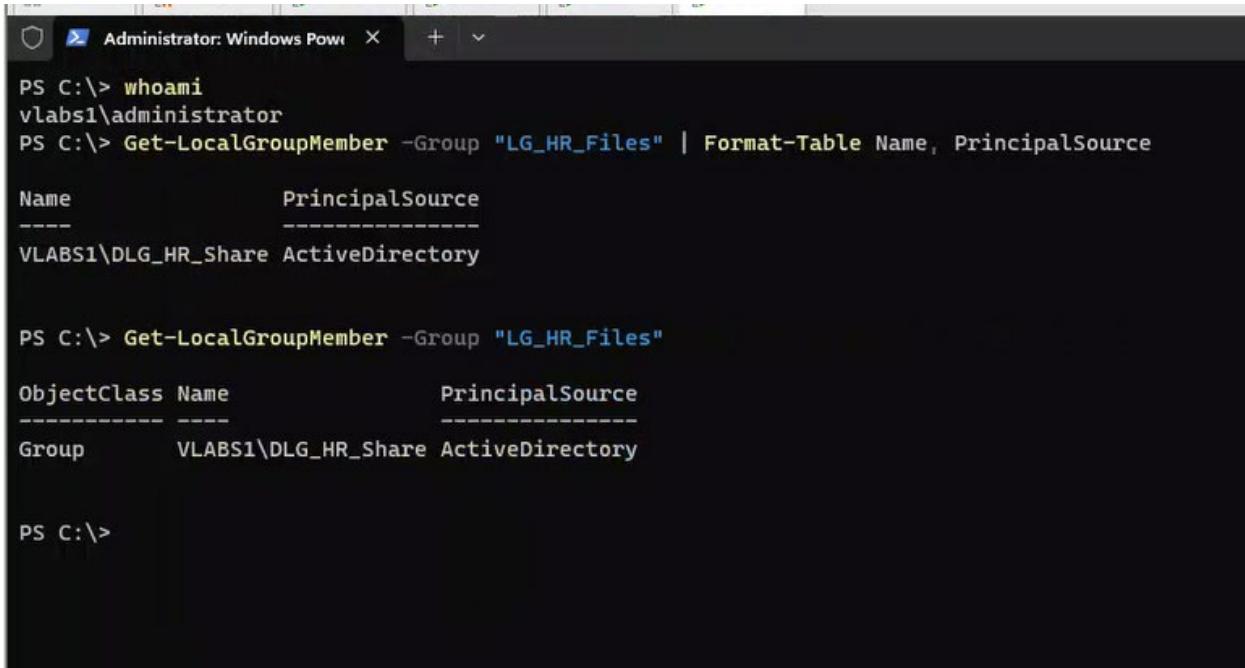


6.4 Verify Membership Using PowerShell

Verify Membership of LG_HR_Files Using PowerShell

Get-LocalGroupMember -Group "LG_HR_Files"

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



The screenshot shows a Windows PowerShell window titled "Administrator: Windows Pow" with the path "PS C:\>". The user has run several commands to check group membership:

```
PS C:\> whoami
vlabs1\administrator
PS C:\> Get-LocalGroupMember -Group "LG_HR_Files" | Format-Table Name, PrincipalSource
Name          PrincipalSource
----          -----
VLABS1\DLG_HR_Share ActiveDirectory

PS C:\> Get-LocalGroupMember -Group "LG_HR_Files"

ObjectClass Name          PrincipalSource
-----  ----          -----
Group      VLABS1\DLG_HR_Share ActiveDirectory

PS C:\>
```

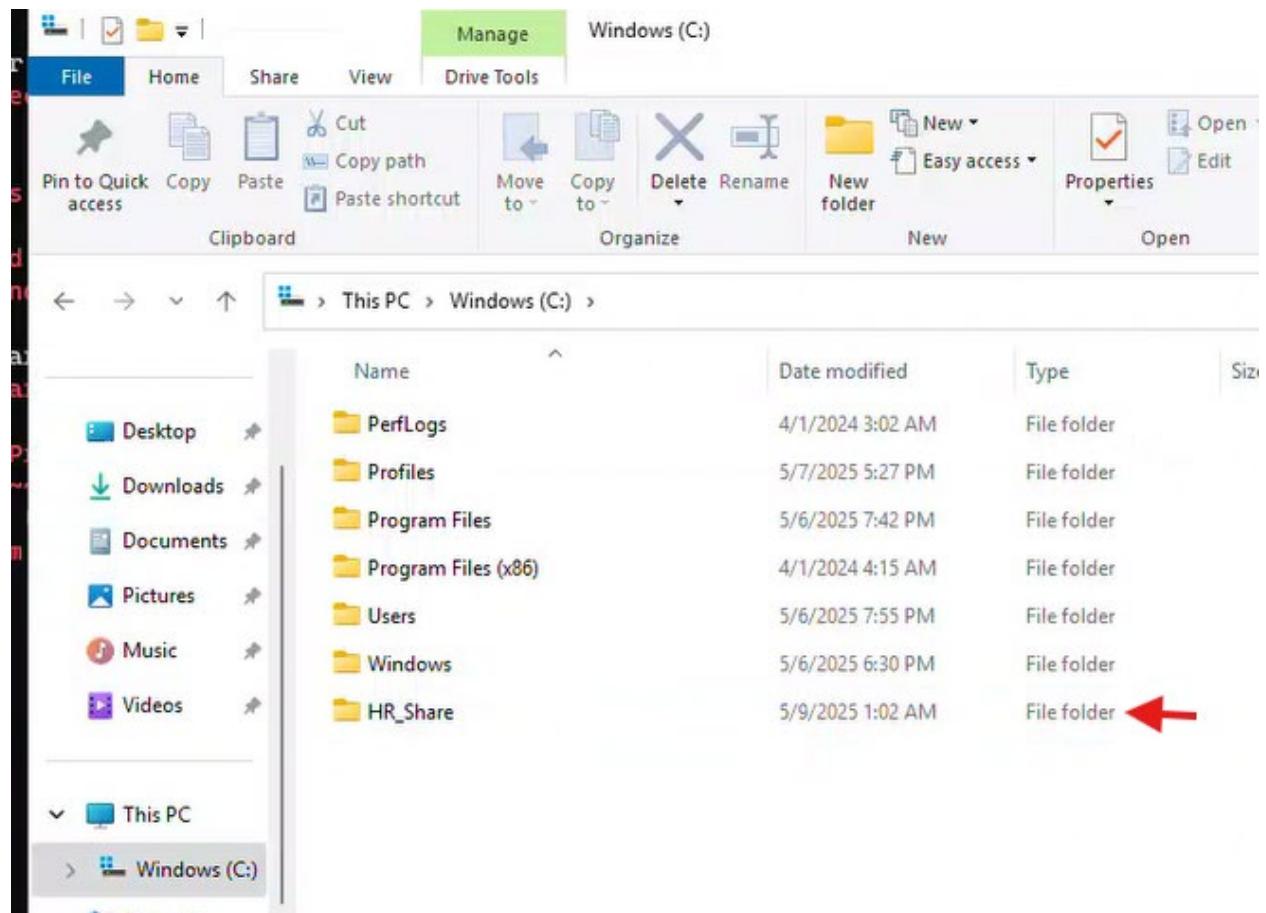
7 Task 5: Share and Set Permissions on SRV01

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.

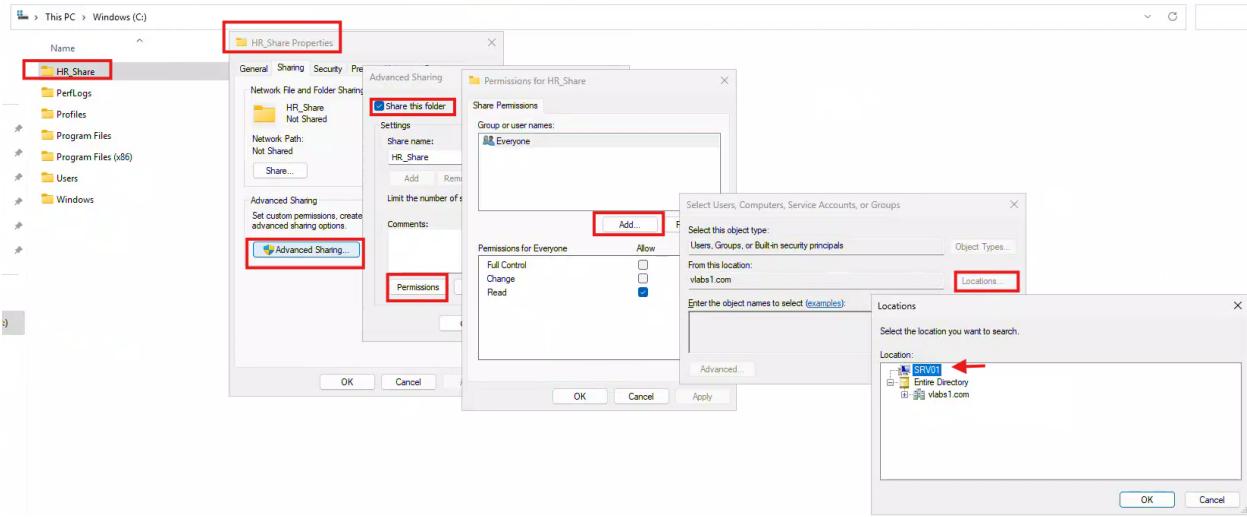


3. Share the Folder:

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

Check Share this folder → Click Permissions.

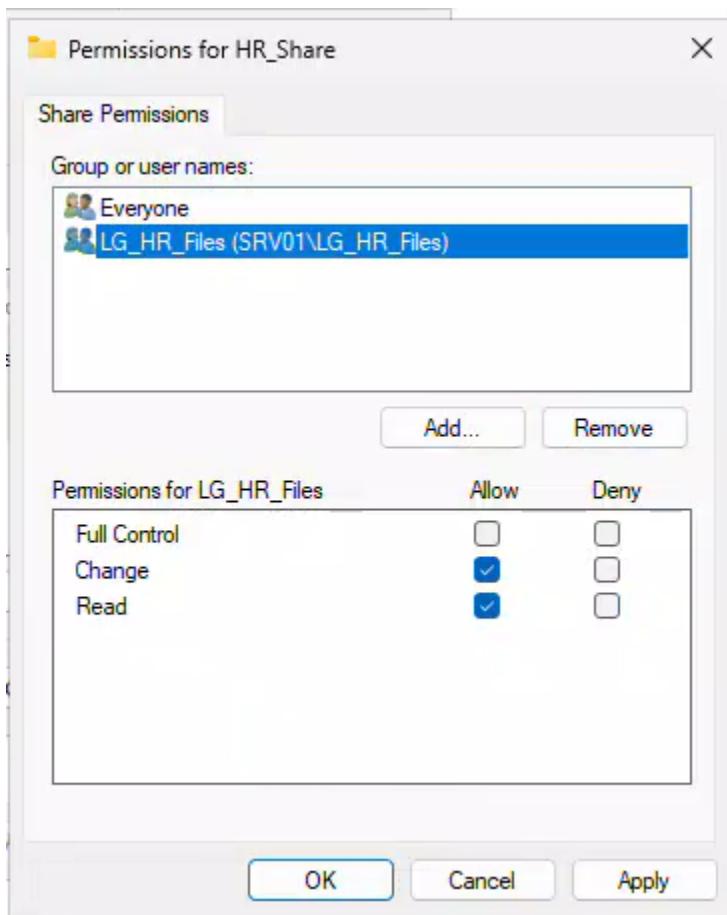
Click Add → Click Locations → Select SRV01



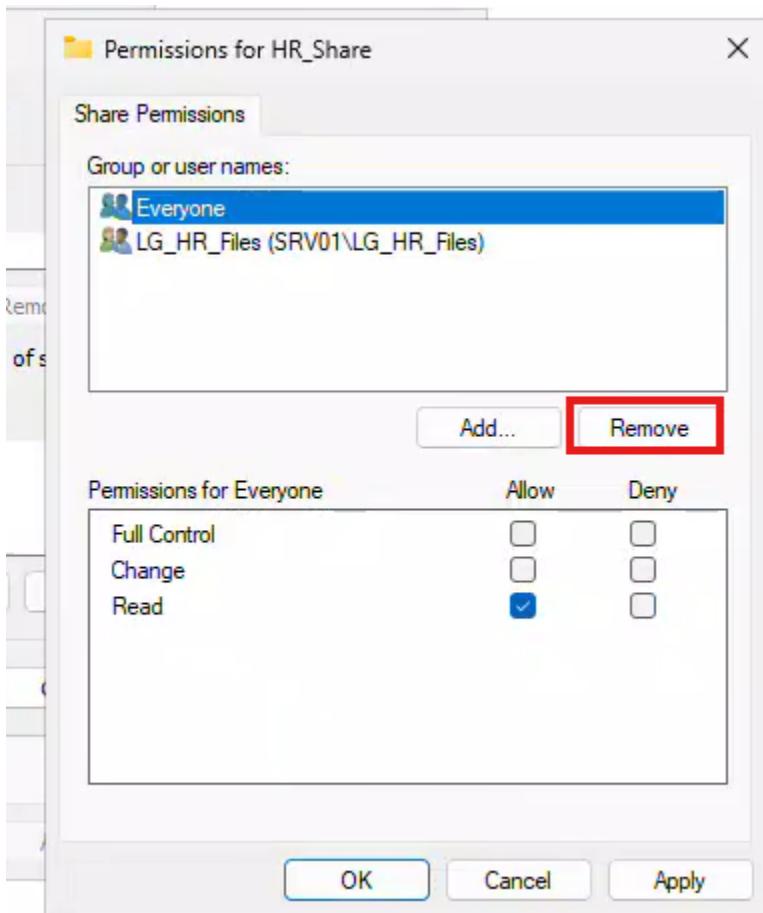
Enter LG_HR_Files → Click Check Names → OK.

See it changes to SRV01\LG_HR_Files → Click OK

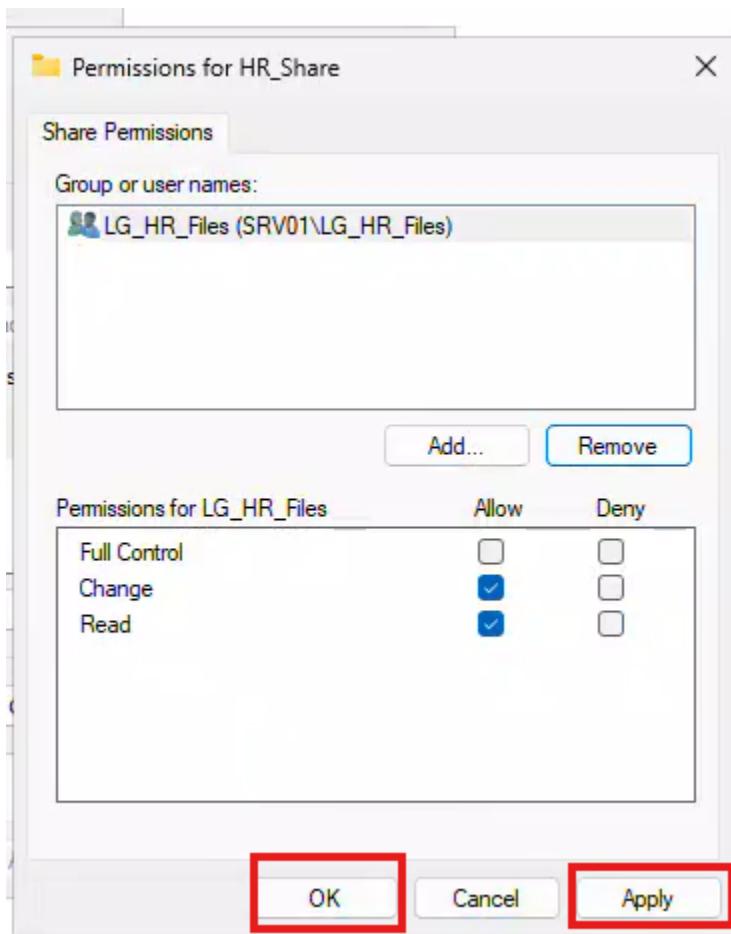
Assign Change permissions (Read/change) to LG_HR_Files → OK → OK.



Remove the Everyone group (select it → Remove).

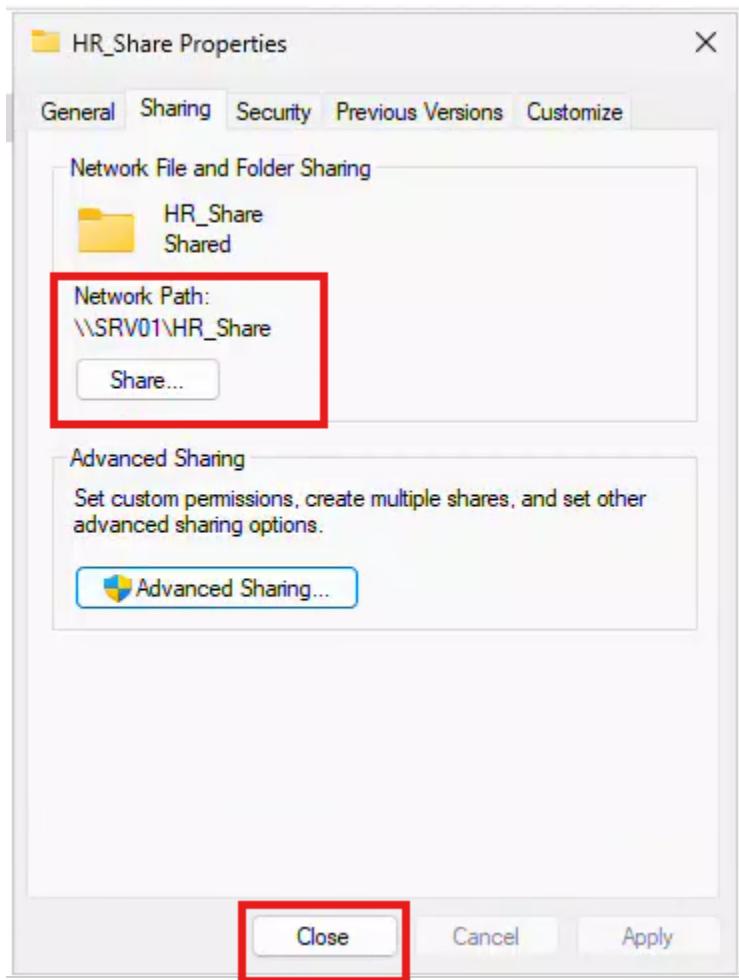


Click Apply → OK → Apply → OK → OK



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
```

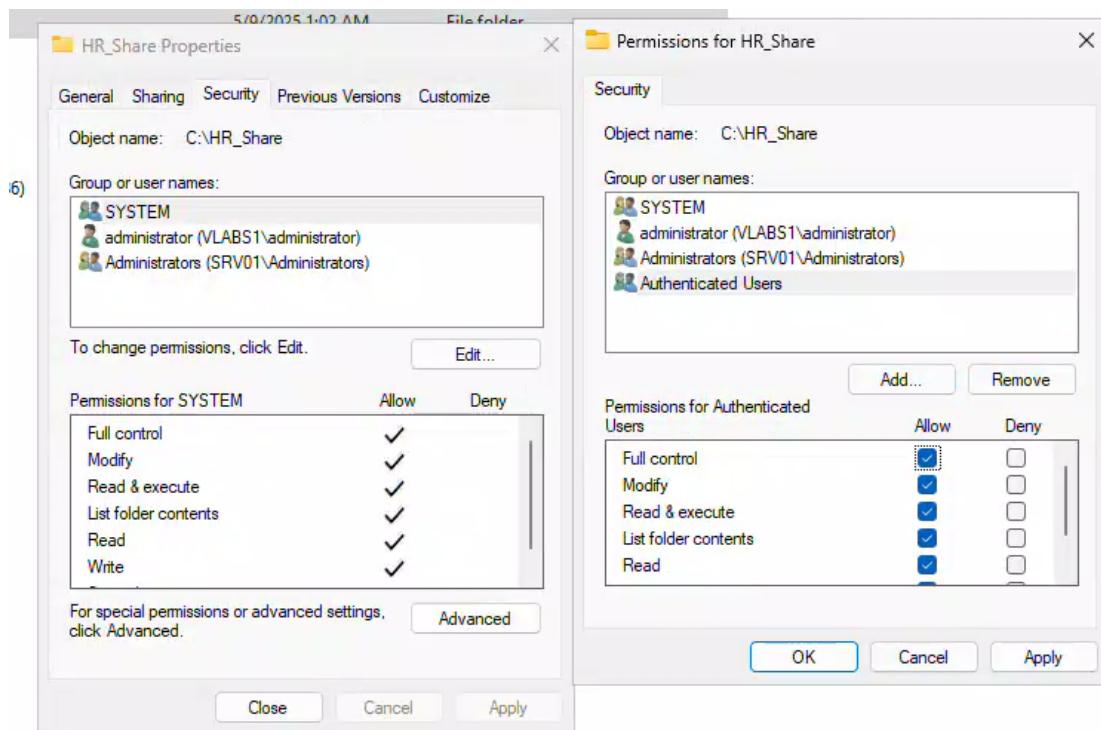
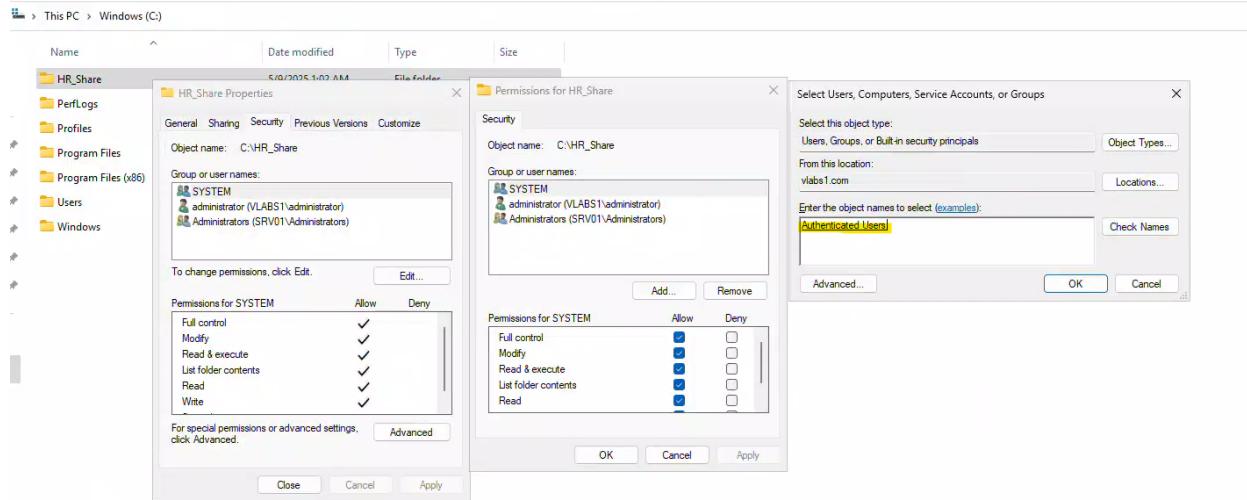
Expected Output:

Account	AccessRights
---------	--------------

-----	-----
-------	-------

LG_HR_Files	Modify, Synchronize
-------------	---------------------

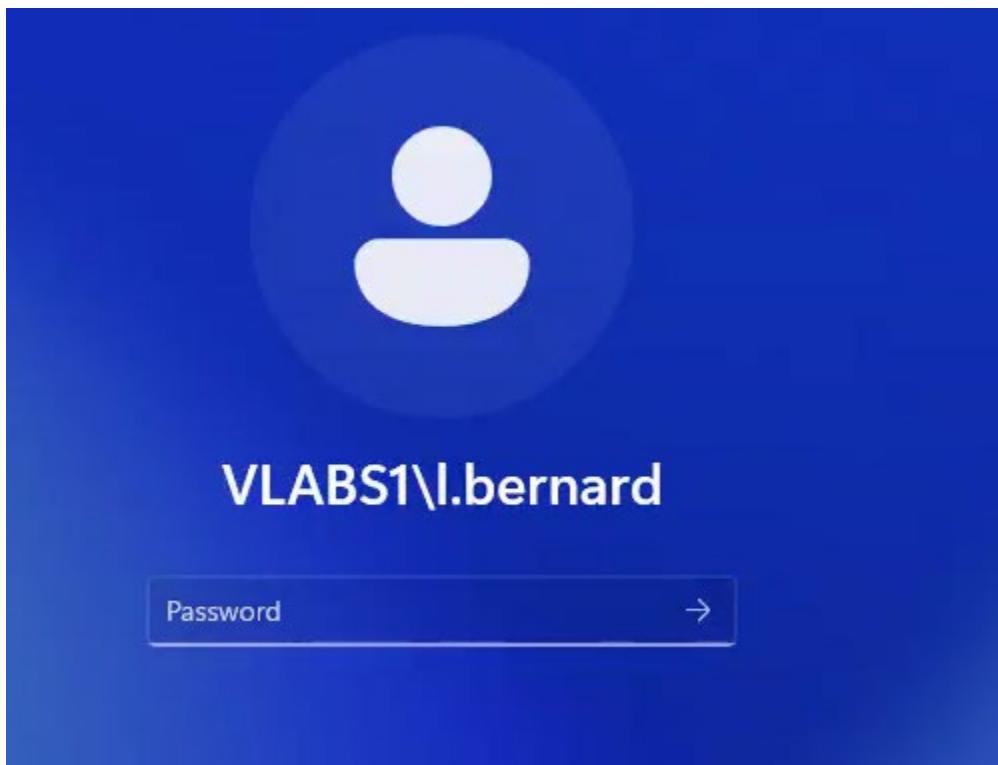
TASK



```
PS C:\Users\administrator.VLABS1> (Get-Acl -Path "C:\HR_Share").Access | Where-Object { $_.IdentityReference -eq "I.L.Bernard" } | Format-List  
PS C:\Users\administrator.VLABS1> (Get-Acl -Path "C:\HR_Share").Access | Where-Object { $_.IdentityReference -eq "I.L.Bernard" } | Format-List  
  
FileSystemRights : FullControl  
AccessControlType : Allow  
IdentityReference : NT AUTHORITY\Authenticated Users  
IsInherited : False  
InheritanceFlags : ContainerInherit, ObjectInherit  
PropagationFlags : None  
  
FileSystemRights : FullControl  
AccessControlType : Allow  
IdentityReference : NT AUTHORITY\SYSTEM  
IsInherited : False  
InheritanceFlags : ContainerInherit, ObjectInherit  
PropagationFlags : None  
  
FileSystemRights : FullControl  
AccessControlType : Allow  
IdentityReference : BUILTIN\Administrators  
IsInherited : False  
InheritanceFlags : ContainerInherit, ObjectInherit  
PropagationFlags : None  
  
FileSystemRights : FullControl  
AccessControlType : Allow  
IdentityReference : VLABS1\administrator  
IsInherited : False  
InheritanceFlags : ContainerInherit, ObjectInherit  
PropagationFlags : None  
  
PS C:\Users\administrator.VLABS1>
```

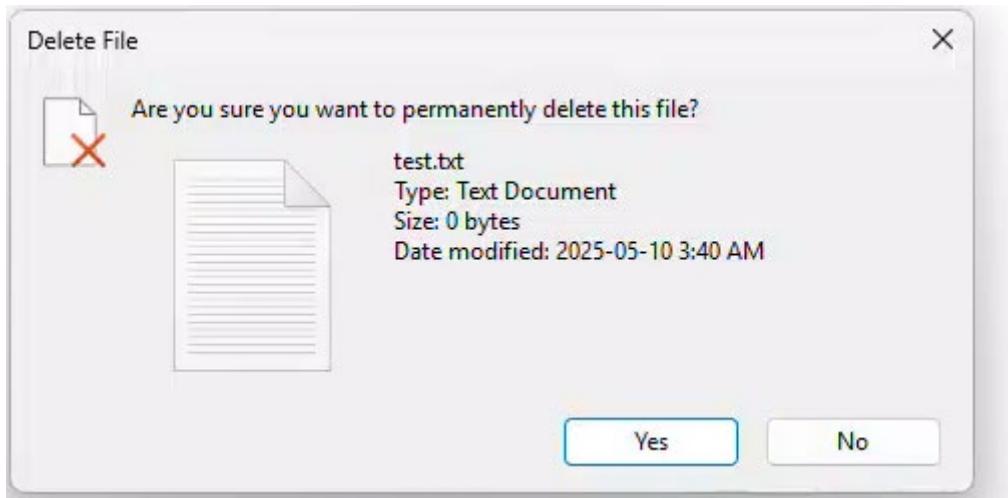
8 Task 6: Test HR Share Access from Client1

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.

Two screenshots of a Windows File Explorer window. The top screenshot shows the contents of the "HR_Share" folder, which contains a single file named "test.txt". The bottom screenshot shows a context menu for the same file "test.txt". The "Delete" option in the menu is highlighted with a red box. The status bar at the bottom of the window indicates "0 KB".



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.

Name	Type
Lucas Bernard	User
HR Template	User
Emma Morel	User
GG_HR_Admins	Group

Go to the Members tab.

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

Click OK to save changes.

Name	Active Directory...
Emma Morel	vlab1-HR-Em...
Lucas Bernard	vlab1-HR-Luc...

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

```
PS C:\Users\Administrator> # Remove user from the group
PS C:\Users\Administrator> Remove-ADGroupMember -Identity "GG_IT_Admins" -Members "c.girard" -Confirm:$false
```

```
# Verify removal
```

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

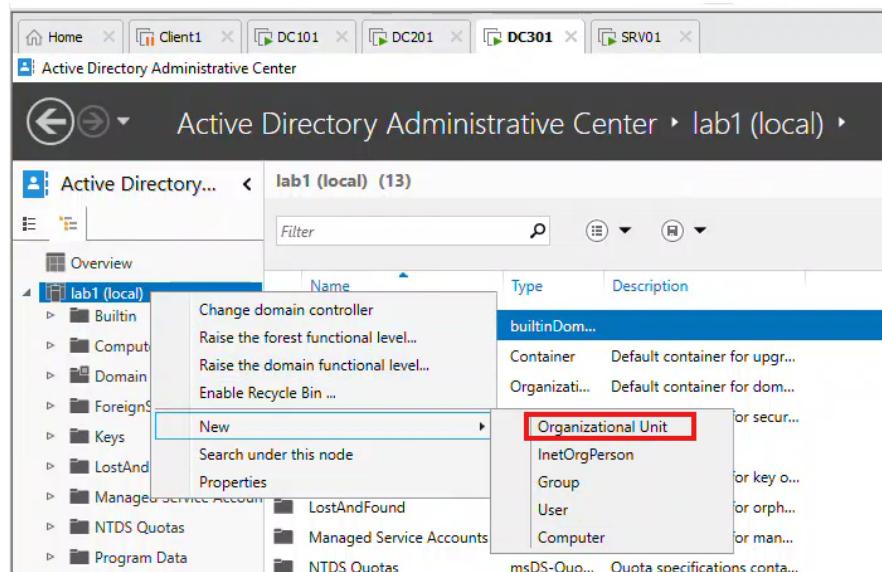
Expected Output (Chloe Girard should no longer appear)

```
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`.



Create Organizational Unit: IT

Organizational Unit	
Managed By	
Name:	<input type="text" value="IT"/>
Address:	<input type="text"/>
Street	<input type="text"/>
City	<input type="text"/>
State/Province	<input type="text"/>
Zip/Postal code	<input type="text"/>
Country/Region:	<input type="text"/>

Active Directory Administrative Center › lab1 (local) ›

Active Directory... lab1 (local) (14)

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...	
IT →	Organizati...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

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

- In ADAC, navigate to the `IT` OU.
- Right-click → New → User → Fill in details:
 - First name: `Fadi`, Last name: `Tora`, User logon name: `f.tora`.

Active Directory... < lab1 (local) (14)

Overview

lab1 (local)

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Keys
- LostAndFound
- Managed Service Account
- NTDS Quotas
- Program Data
- System
- TPM Devices
- Users
- IT

New

- Organizational Unit
- InetOrgPerson
- Group
- User **Red Box**
- Computer

Name Type Description

Name	Type	Description
Builtin	Container	Default container for upgr...
Computers	Container	Default container for dom...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

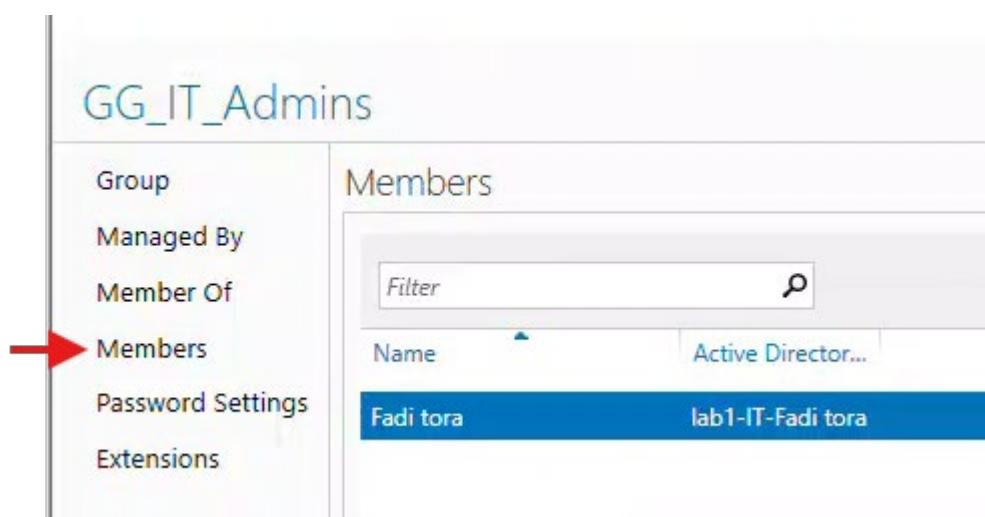
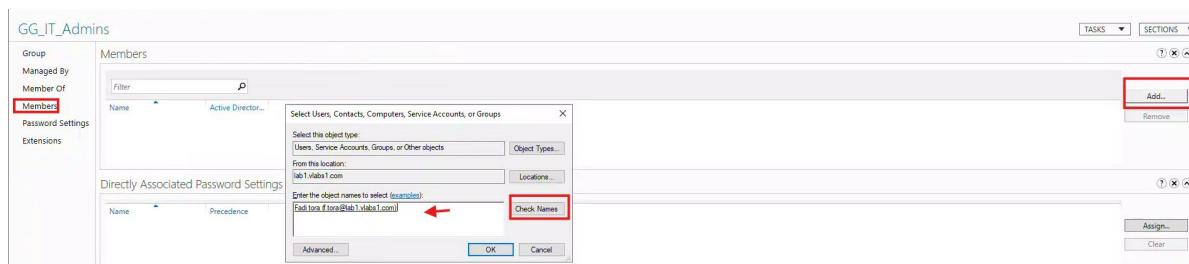
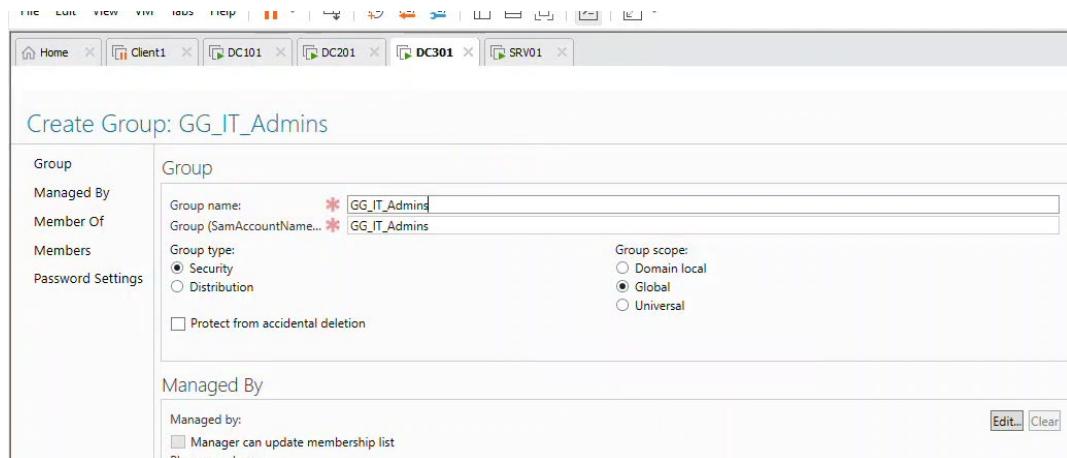
Create User: Fadi tora

Account	<p>First name: Fadi</p> <p>Middle initials:</p> <p>Last name: tora</p> <p>Full name: Fadi tora</p> <p>User UPN logon: f.tora @ lab1.vlabs1.com</p> <p>User SamAccountName logon: lab1 \ f.tora</p> <p>Password:</p> <p>Confirm password:</p> <p>Create in: OU=IT,DC=lab1,DC=vlabs1,DC=com Change...</p> <p><input checked="" type="checkbox"/> Protect from accidental deletion</p> <p>Log on hours... Log on to...</p>	Account
Organization		Password <input checked="" type="radio"/> User i <input type="radio"/> Other Mi Pa Other op Encryptic

The screenshot shows the Active Directory Administrative Center (ADAC) interface. In the left navigation pane, under the 'lab1 (local)' container, the 'IT' organizational unit is selected, indicated by a red arrow. The main pane displays a list of objects in the 'IT' OU, with a single entry for 'Fadi Tora' highlighted in blue, also indicated by a red arrow. The list includes columns for Name, Type, and Description.

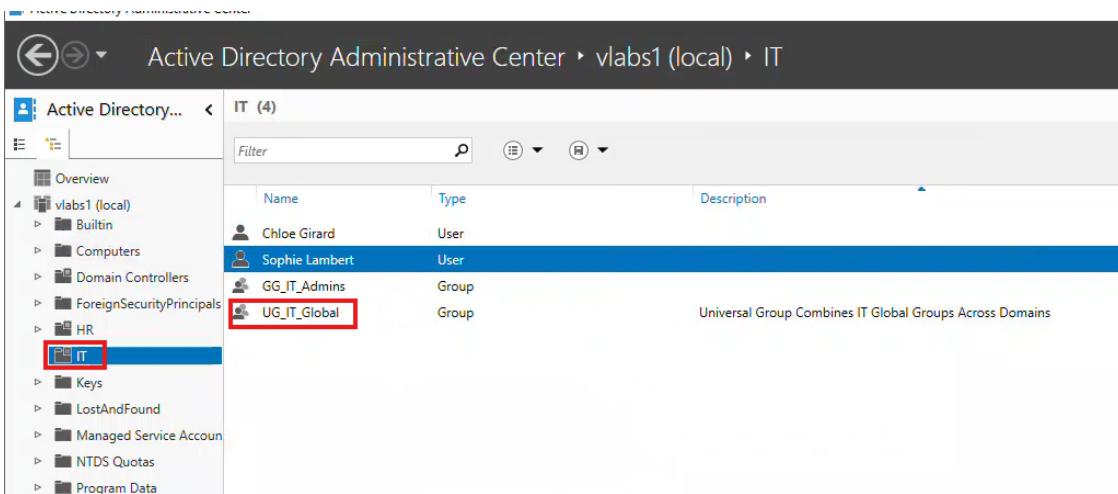
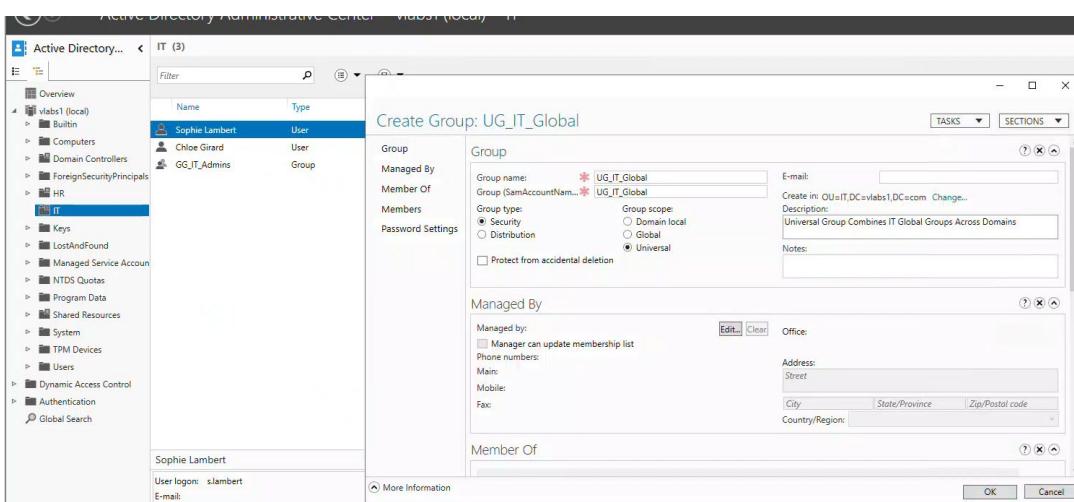
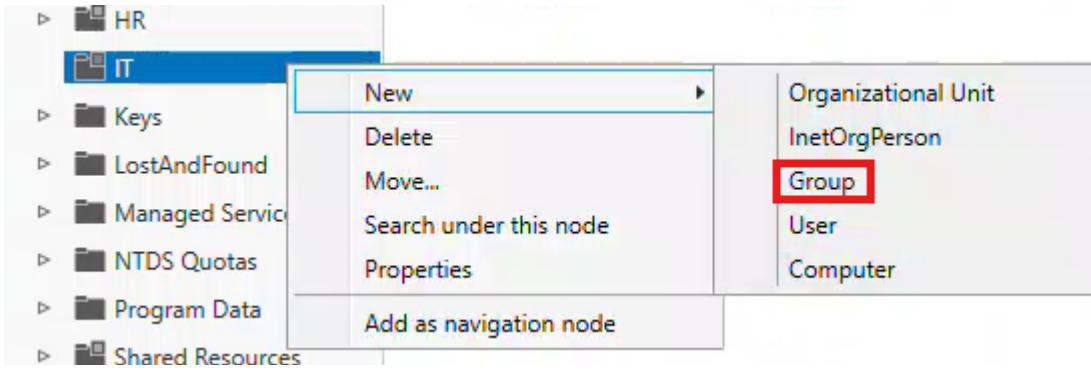
3. Inside **IT OU**, create a Global Group **GG_IT_Admins** and add **Fadi Tora** as a member using **ADAC**.
 - a) In ADAC, navigate to the 'IT' OU.
 - b) Right-click → New → Group → Name: 'GG_IT_Admins', Group type: 'Security', Scope: 'Global'.
 - c) Open 'GG_IT_Admins' properties → Members → Add 'f.tora'.

The screenshot shows a context menu for the 'IT' organizational unit in the ADAC navigation pane. The 'Group' option is highlighted with a red box. Other options visible in the menu include New, Delete, Move..., Search under this node, and Properties.



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

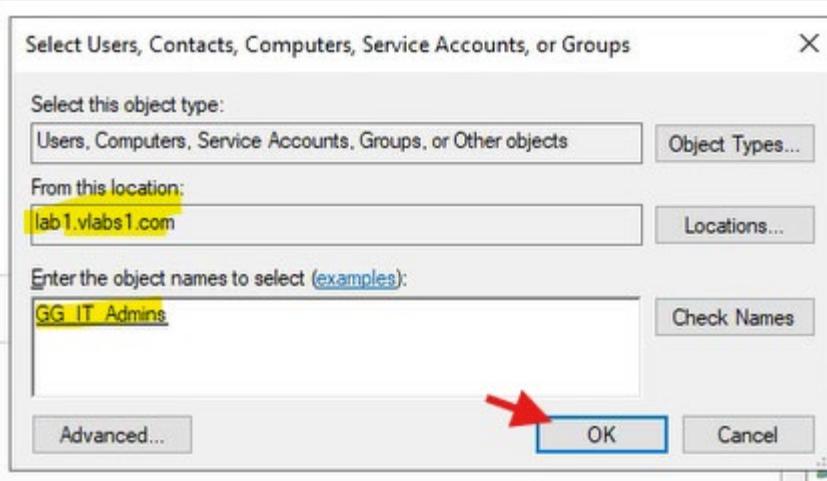
The screenshot shows the Active Directory Administrative Center interface. The top navigation bar includes tabs for Home, Client1, DC101 (which is highlighted in red), DC201, DC301, and SRV01. The main title is "Active Directory Administrative Center • vlabs1 (local) • IT". On the left, a navigation pane shows the structure: Overview, vlabs1 (local) (with Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, HR, and IT), and Keys, LostAndFound, Managed Service Account. The "IT" node is selected and highlighted with a red box. The right pane displays a table titled "IT (4)" with columns for Name, Type, and Description. It lists four entries: Chloe Girard (User), Sophie Lambert (User), GG_IT_Admins (Group), and UG_IT_Global (Group). A tooltip for UG_IT_Global states "Universal Group Combines IT Global Groups Across Domains".

Location vlabs1

This screenshot shows the "UG_IT_Global" group properties dialog. The "Members" tab is selected. In the main pane, there's a table for "Directly Associated Password Settings". On the right, a "Select Users, Contacts, Computers, Service Accounts, or Groups" dialog is open. The "From this location:" dropdown is set to "vlabs1.com". The "Enter the object names to select (examples):" input field contains "GG_IT_Admins" and has a red arrow pointing to it. The "OK" button is visible at the bottom of the dialog.

Location lab1

This screenshot shows the "Locations" dialog. The instruction "Select the location you want to search." is displayed. Under "Location:", a tree view shows the hierarchy: lab1.vlabs1.com (highlighted with a red arrow), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, IT, Keys, LostAndFound, Managed Service Accounts, and Personal Data. At the bottom are "OK" and "Cancel" buttons.



UG_IT_Global

Group	Members
Managed By	
Member Of	
Members	Name Active Directory Domain Services Folder GG_IT_Admins lab1-IT-GG_IT_Admins
Password Settings	
Extensions	Name vlabs1-IT-GG_IT_Admins

Directly Associated Password Settings

Name	Precedence

Verify

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

```
PS C:\Users\Administrator> Get-ADGroupMember -Identity "UG_IT_Global" | Select-Object Name, SamAccountName, DistinguishedName
Name      SamAccountName DistinguishedName
-----  -----
GG_IT_Admins  GG_IT_Admins  CN=GG_IT_Admins,OU=IT,DC=lab1,DC=vlabs1,DC=com
GG_IT_Admins  GG_IT_Admins  CN=GG_IT_Admins,OU=IT,DC=vlabs1,DC=com

PS C:\Users\Administrator>
```

3. Add **UG_IT_Global** to the Domain Local group **DLG_IT_Share** using **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

The screenshot shows the Active Directory Users and Computers (ADUC) interface. A group named "UG_IT_Global" is selected. The "Member Of" tab is active, showing that the group is a member of the "DLG_IT_Share" group. The "Members" tab lists two users: "GG_IT_Admins" and "UG_IT_Global". The "Directly Associated Password Settings" tab is also present.

DLG_IT_Share

Group	Members
Managed By	
Member Of	
Members	
Password Settings	
Extensions	

Members

Name	Active Director...
UG_IT_Global	vlabs1-IT-UG_I...

Directly Associated Password Settings

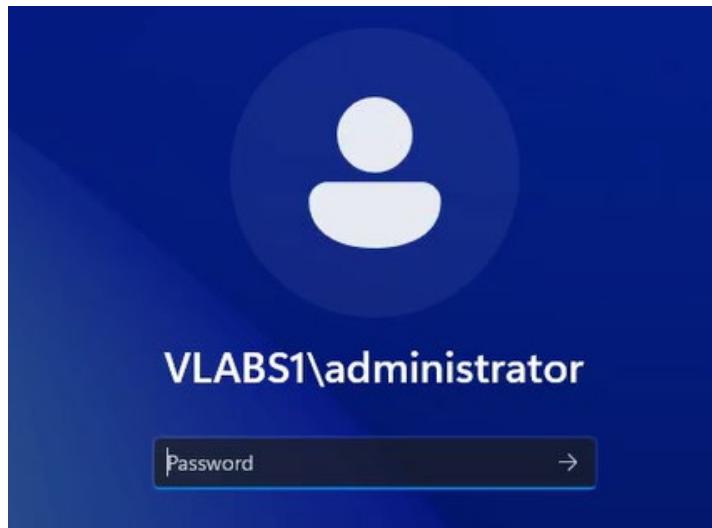
Name	Precedence

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

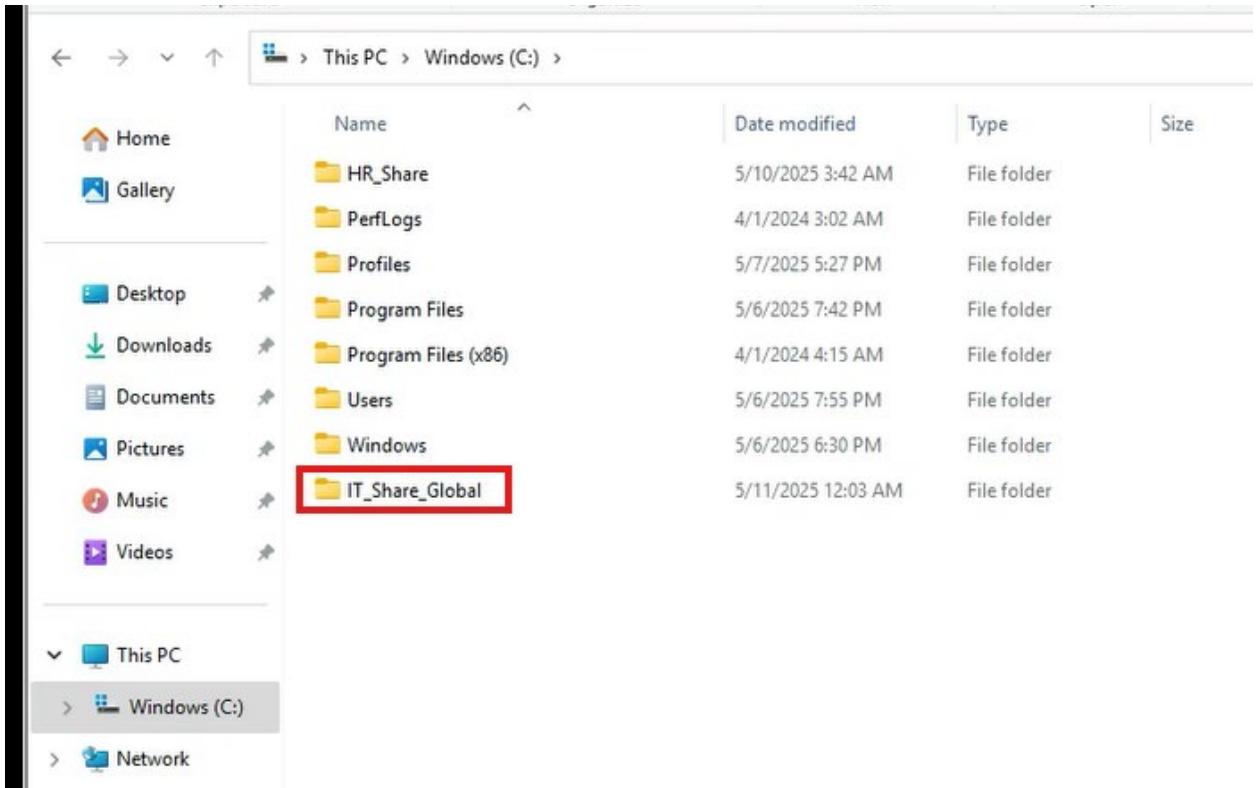
1. On **SRV01**, create and share **C:\IT_Share_Global** using **GUI**.

Create the Folder:

- a) Log in to SRV01 as an administrator.

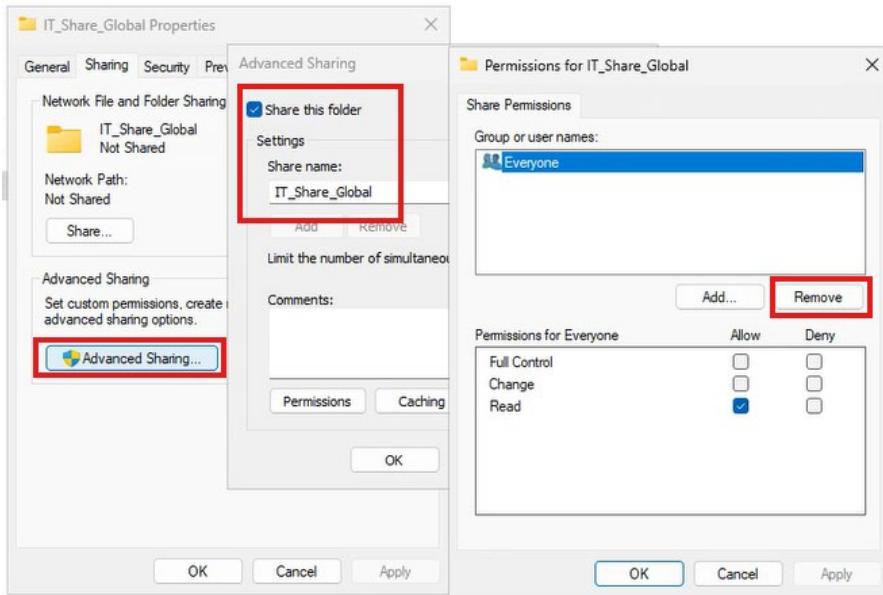


- b) Open File Explorer → Navigate to C:\.
- c) Right-click → New → Folder → Name it **IT_Share_Global**.

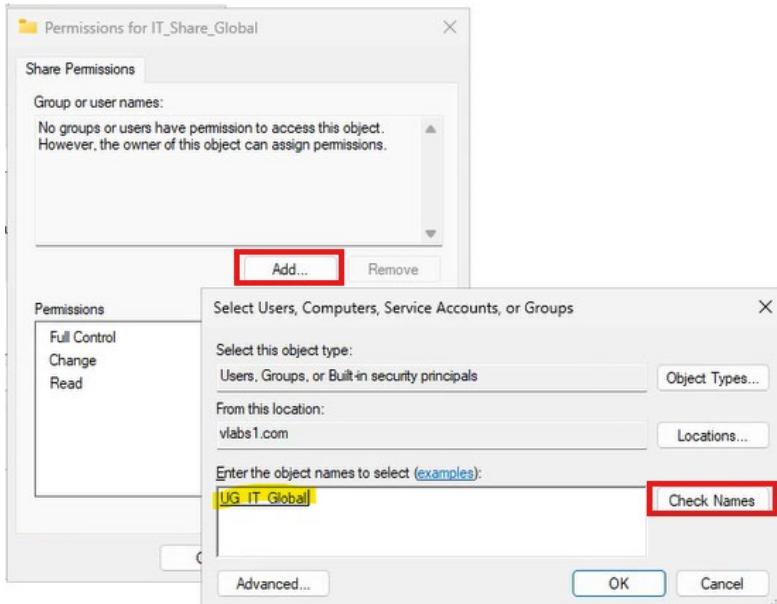


Permissions

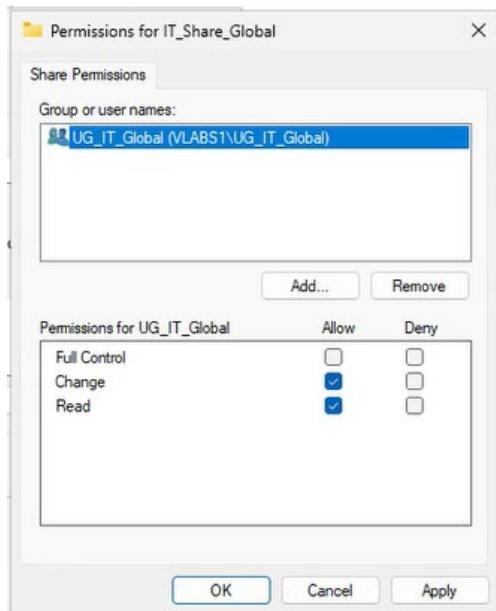
2. Assign Change permissions (Read/Write) to UG_IT_Global group, and remove the Everyone group using GUI.
 - a) Share the Folder:
Right-click the folder → Properties → Sharing tab → Advanced Sharing.
 - b) Check Share this folder → Set Share name to IT_Share_Global.
 - c) Click Permissions → Remove Everyone (select it → Remove).



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



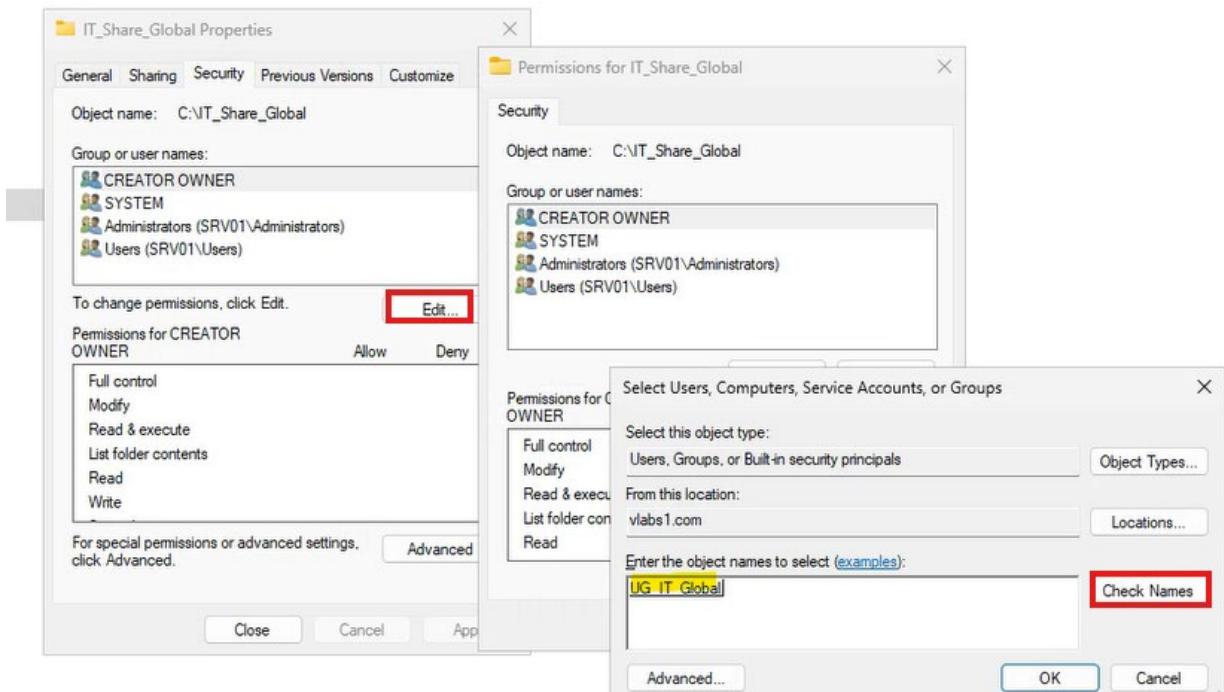
e) Select UG_IT_Global → Check Change (Read/Write) permissions → OK → OK.



Set NTFS Permissions (GUI)

1. Open Security Tab:

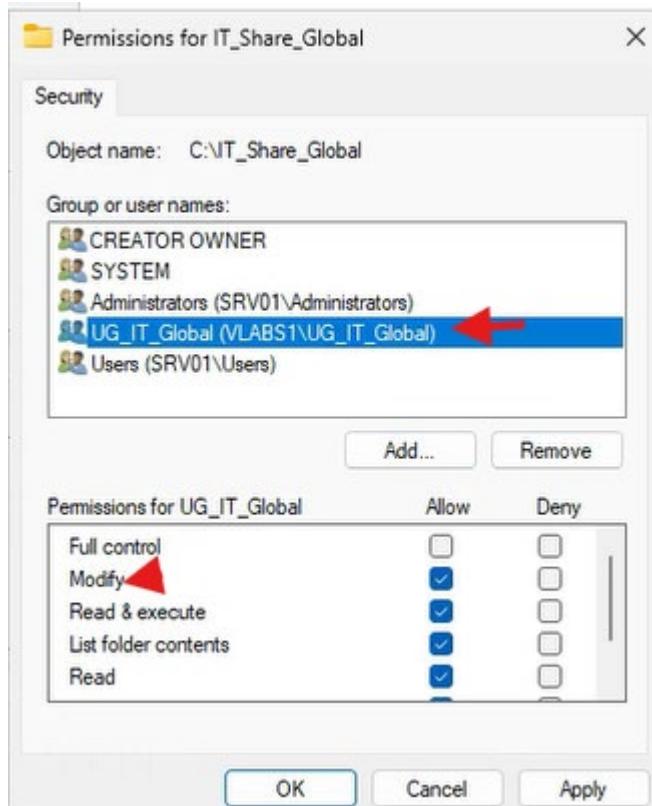
- Go to the folder's **Properties** → **Security** tab.
- Click **Edit** → **Add** → Type **UG_IT_Global** → **Check Names** → **OK**.



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**.

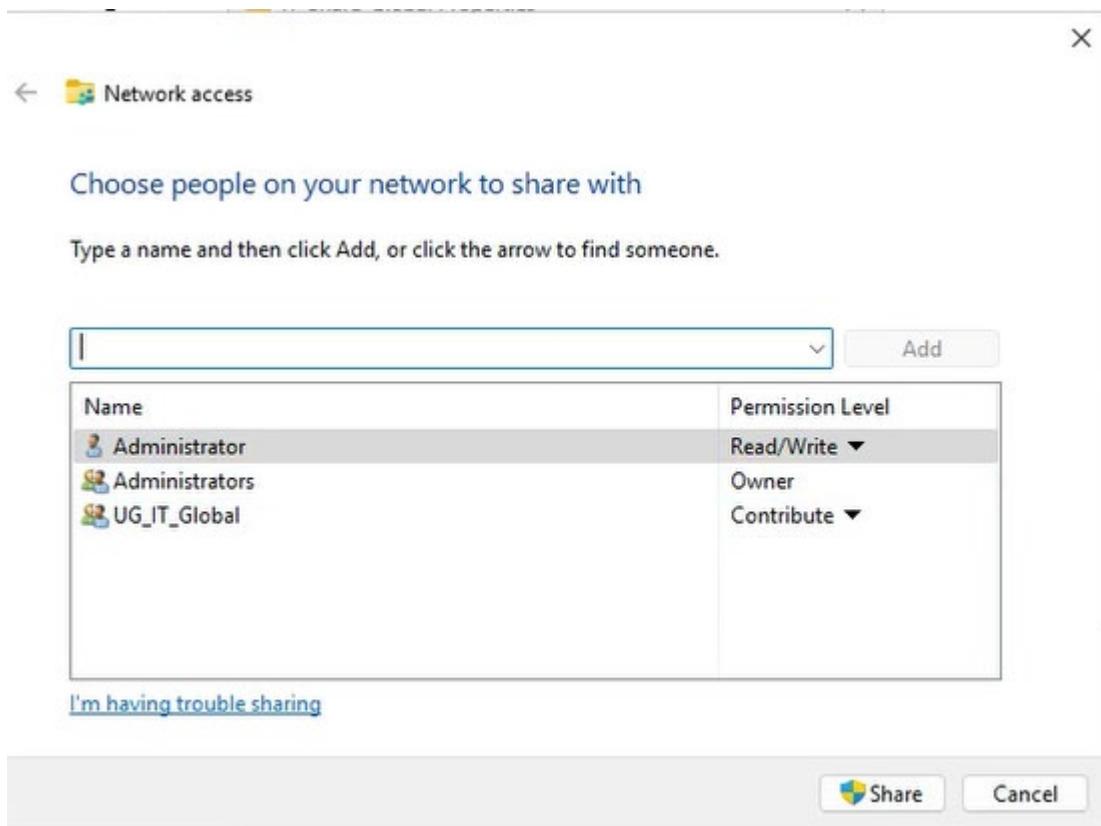
Check the Share:

```
Get-SmbShare -Name "IT_Share_Global"
```

Name	ScopeName	Path	Description
IT_Share_Global	*	C:\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

```

Principal	Type	Access	Inherited from	Applies to
Administrators (SRV01\Administrators)	Allow	Full control	None	This folder only
UG_IT_Global (VLABS1\UG_IT_Global)	Allow	Modify	None	This folder, subfolders and files
SYSTEM	Allow	Full control	C:\	This folder, subfolders and files
Administrators (SRV01\Administrators)	Allow	Full control	C:\	This folder, subfolders and files
Users (SRV01\Users)	Allow	Read & execute	C:\	This folder, subfolders and files
Users (SRV01\Users)	Allow	Special	C:\	This folder and subfolders
CREATOR OWNER	Allow	Full control	C:\	Subfolders and files only

12 Task 10: Test IT Share Access from Client1

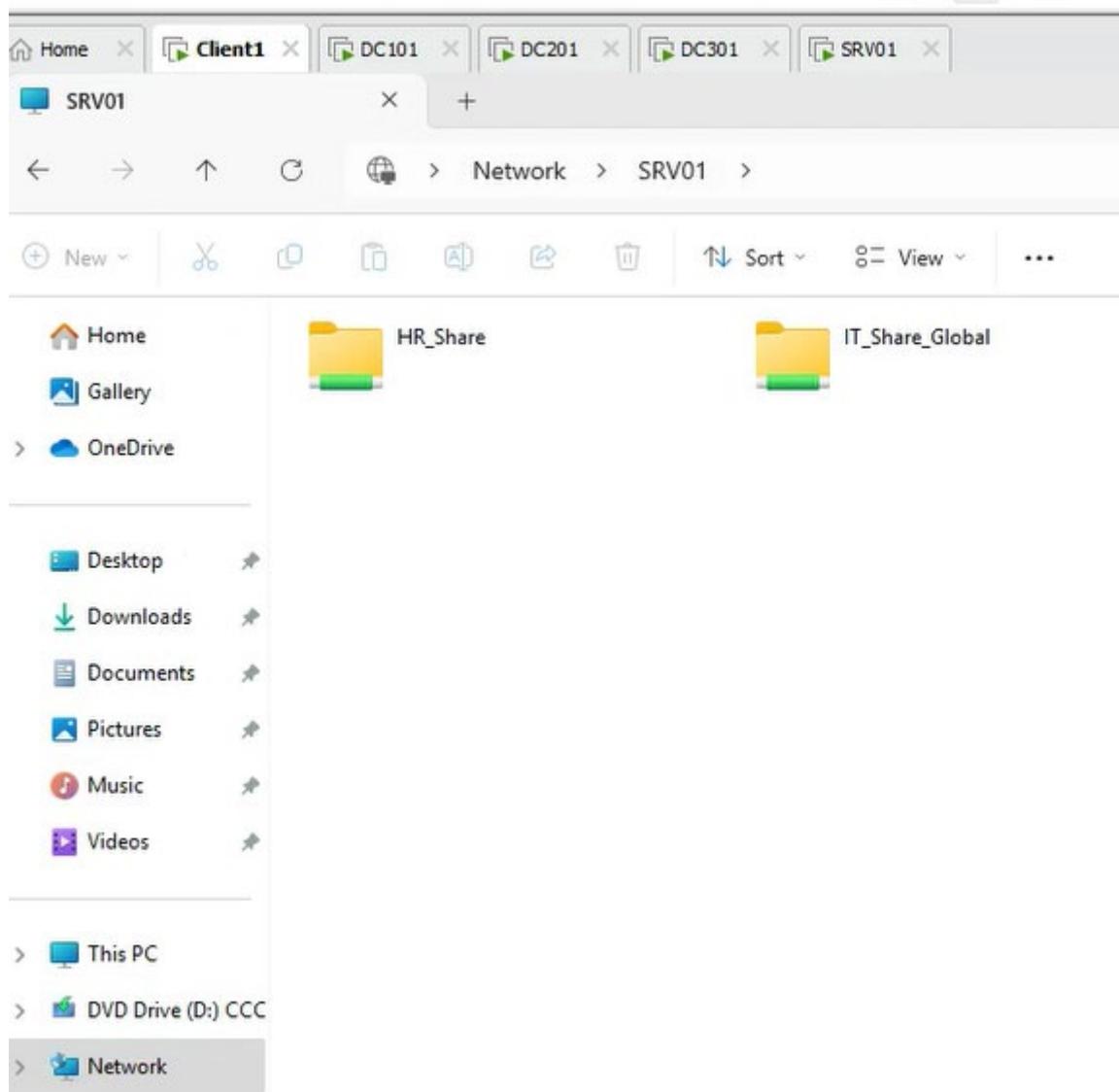
1. Log in as **Fadi Tora (f.tora)** on **Windows 11 (Client1)**.
2. Check which groups **Fadi Tora** is a member of using **Command Prompt**.

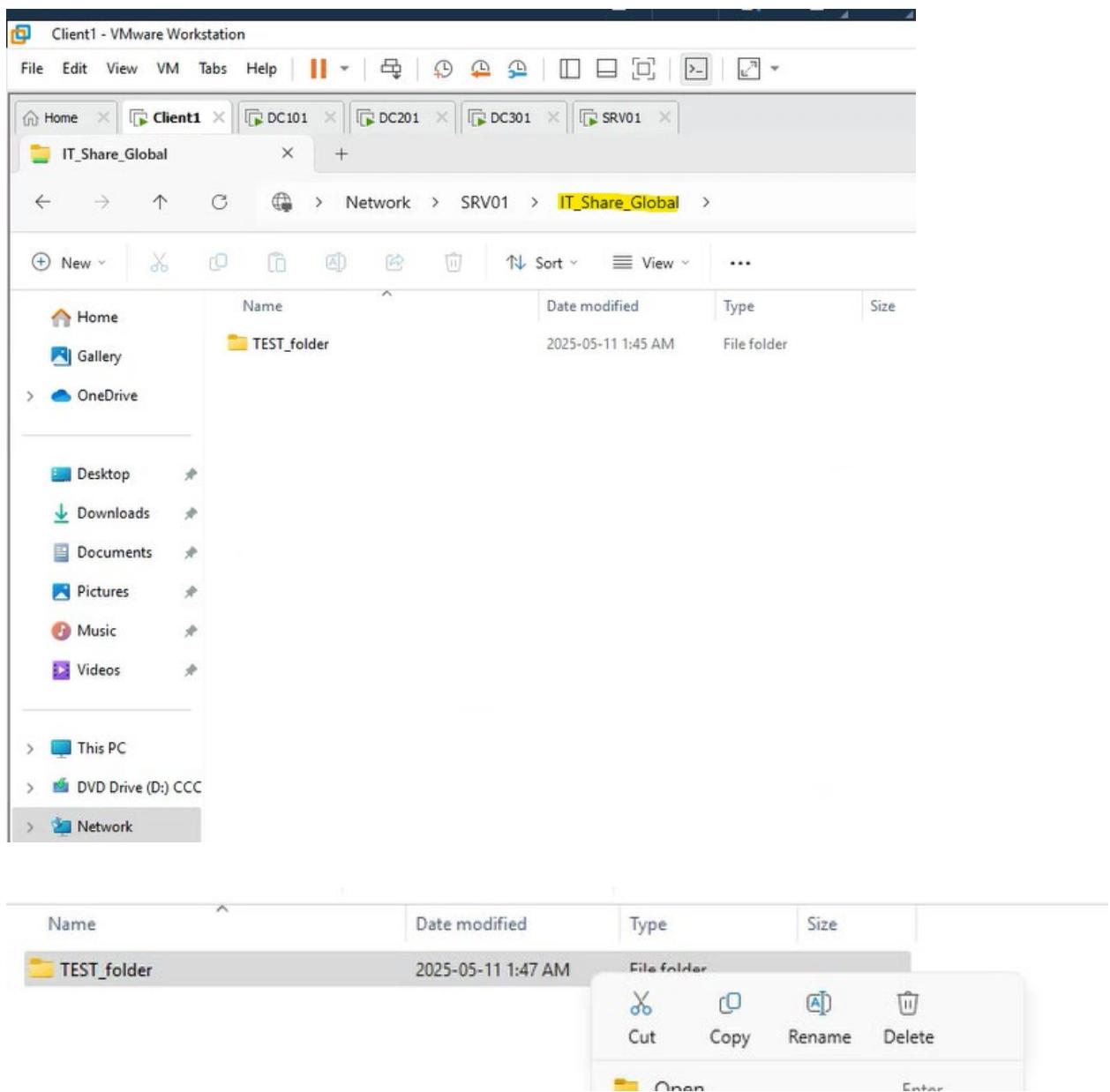
Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group, Enabled by default, Enabled group
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
LAB1\GG_IT_Admins	Group	S-1-5-21-32770921-3136444610-3217977211-1105	Mandatory group, Enabled by default, Enabled group
VLABS1\UG_IT_Global	Group	S-1-5-21-1268601764-4050707287-4025116564-1121	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
VLABS1\DLG_IT_Share	Alias	S-1-5-21-1268601764-4050707287-4025116564-1118	Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192	

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.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