Lab 5 – Managing Group Accounts

Task 1: Create and Manage Security Groups

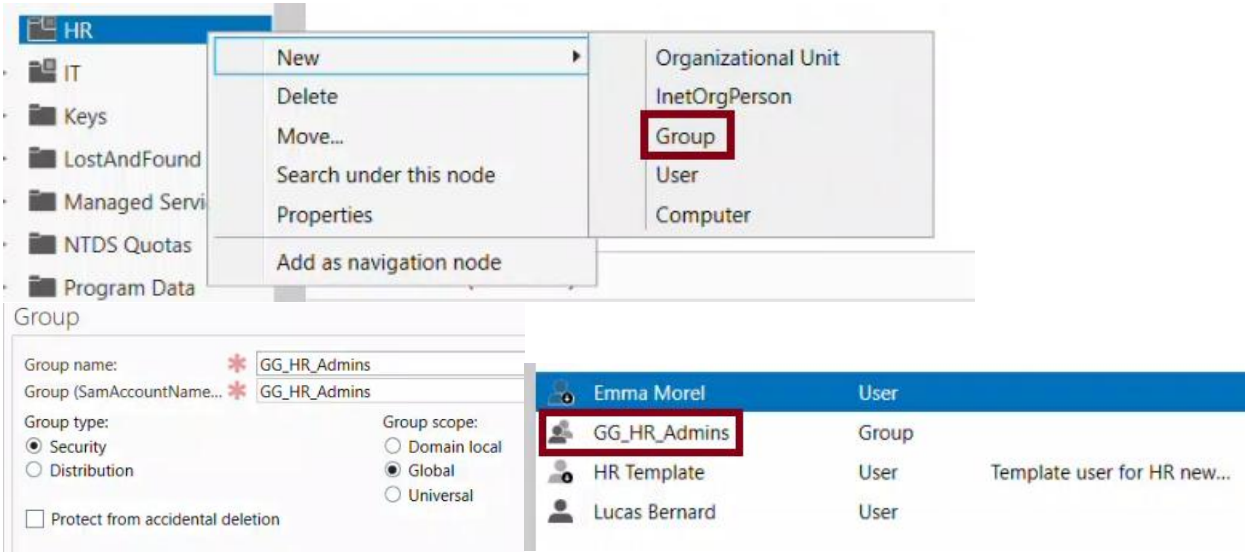
▨ Step 1: Create GG_HR_Admins using ADAC
System: DC107 (Primary Domain Controller for vlabs07.com)

Explanation:
We used Active Directory Administrative Center (ADAC) on DC107 to create a new Global Security Group called GG_HR_Admins inside the HR Organizational Unit.

This group will be used to assign permissions to HR administrators in the domain.

Steps:
- Log in to DC107
- Open Active Directory Administrative Center
- Navigate to the vlabs07.com domain
- Go to the HR OU
- Click "New > Group"
- Enter the following:
  Name: GG_HR_Admins
  Group scope: Global
  Group type: Security
- Click OK to create the group

Screenshot:



▨ Step 2: Create GG_IT_Admins using PowerShell
System: DC107 (Continue using the same server)

Command:

```
New-ADGroup `
  -Name "GG_IT_Admins" `
  -GroupScope Global `
  -GroupCategory Security `
  -Path "OU=IT,DC=vlabs07,DC=com" `
  -SamAccountName "GG_IT_Admins"
```

Explanation:

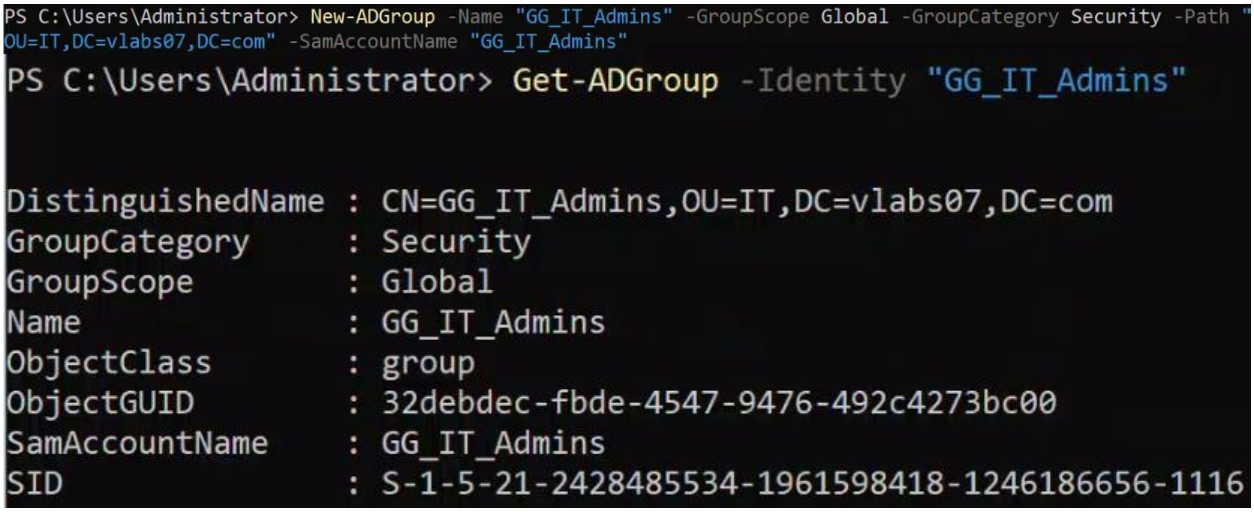
This command creates a Global Security Group named GG_IT_Admins in the IT Organizational Unit of the vlabs07.com domain.

- -Name defines the groups display name
- -GroupScope Global allows the group to be used for permissions across domains (members must be from this domain)
- -GroupCategory Security marks it as usable for ACLs (access control)
- -Path tells AD to place the group inside the IT OU
- -SamAccountName is the legacy-compatible login name

To confirm the group was created successfully, run:

```
Get-ADGroup -Identity "GG_IT_Admins"
```

Screenshot:



▨ Step 3: Verify Group Creation (GG_HR_Admins and GG_IT_Admins)
System: DC107

Command:

```
Get-ADGroup -Filter * | Where-Object { $_.Name -in @("GG_HR_Admins",
"GG_IT_Admins") } | Select-Object Name, GroupScope, DistinguishedName
```

Explanation:

This command checks that both security groups exist in Active Directory and confirms their scope and location.

Keyword breakdown:

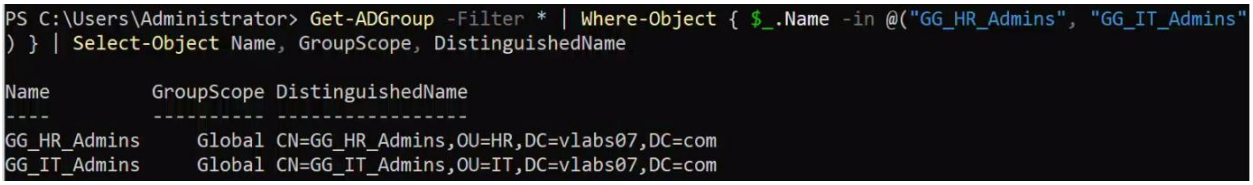
- Get-ADGroup -Filter *
  → Retrieves all groups in Active Directory.

- Where-Object { $_.Name -in @("GG_HR_Admins", "GG_IT_Admins") }
  → Filters the list to only include groups whose Name matches either "GG_HR_Admins" or "GG_IT_Admins".
  → `$_` refers to the current object in the pipeline.
  → `-in` is used to check if the group name is in the list provided with `@(...)`.

- Select-Object Name, GroupScope, DistinguishedName
  → Selects and displays only these specific fields:
    - Name: shows the group's display name.
    - GroupScope: confirms if it is Global, Universal, or DomainLocal.
    - DistinguishedName: shows the full path to where the group is stored in Active Directory.

This is a good way to double-check that the groups were created in the right OU and with the correct scope.

Screenshot:



Task 2: Add Members to Groups

▨ Step 1: Add Emma Morel and Lucas Bernard to GG_HR_Admins
System: DC107 (Primary Domain Controller for vlabs07.com)

Command:

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

Explanation:

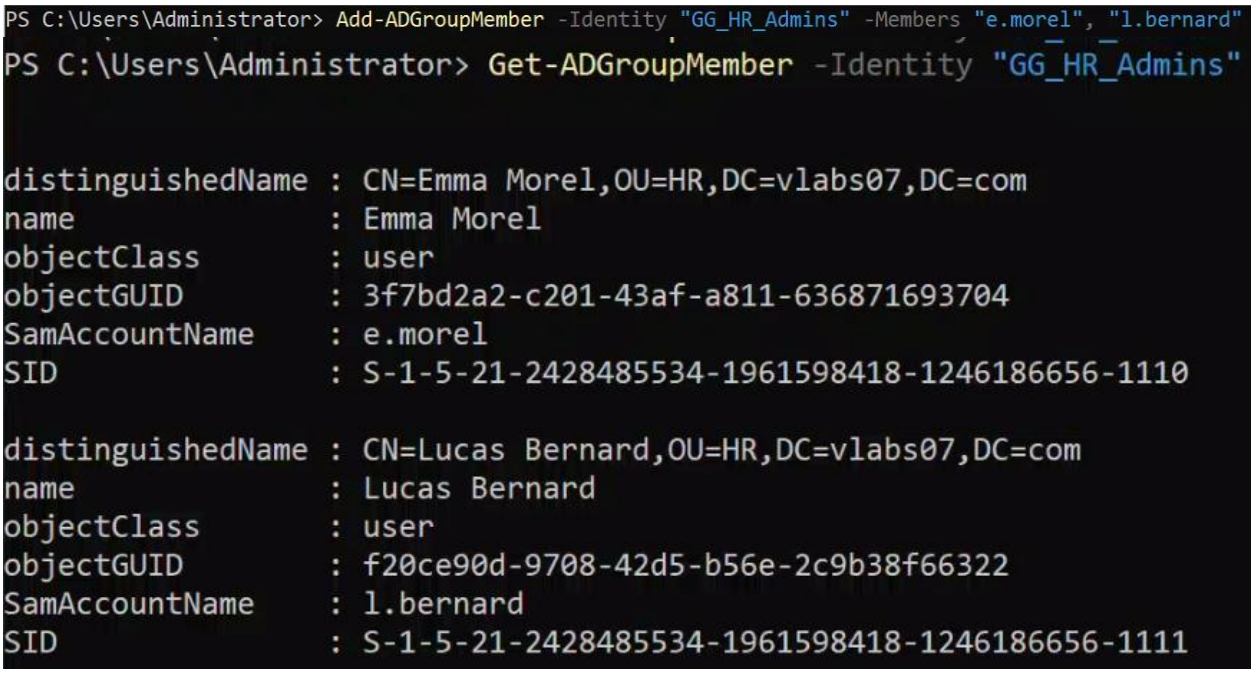
This command adds two users (Emma Morel and Lucas Bernard) to the GG_HR_Admins group using PowerShell.

- Add-ADGroupMember → Cmdlet used to add members to an AD group.
- -Identity "GG_HR_Admins" → Specifies the group were modifying.
- -Members → Lists the usernames (SamAccountName) to be added to the group.

Both users must already exist in Active Directory for this command to succeed.

To confirm the results, you can run:
```
Get-ADGroupMember -Identity "GG_HR_Admins"
```

Screenshot:



▨ Step 2: Add Chloe Girard and Sophie Lambert to GG_IT_Admins
System: DC107 **(Continue using** the same server**)**

Command:

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

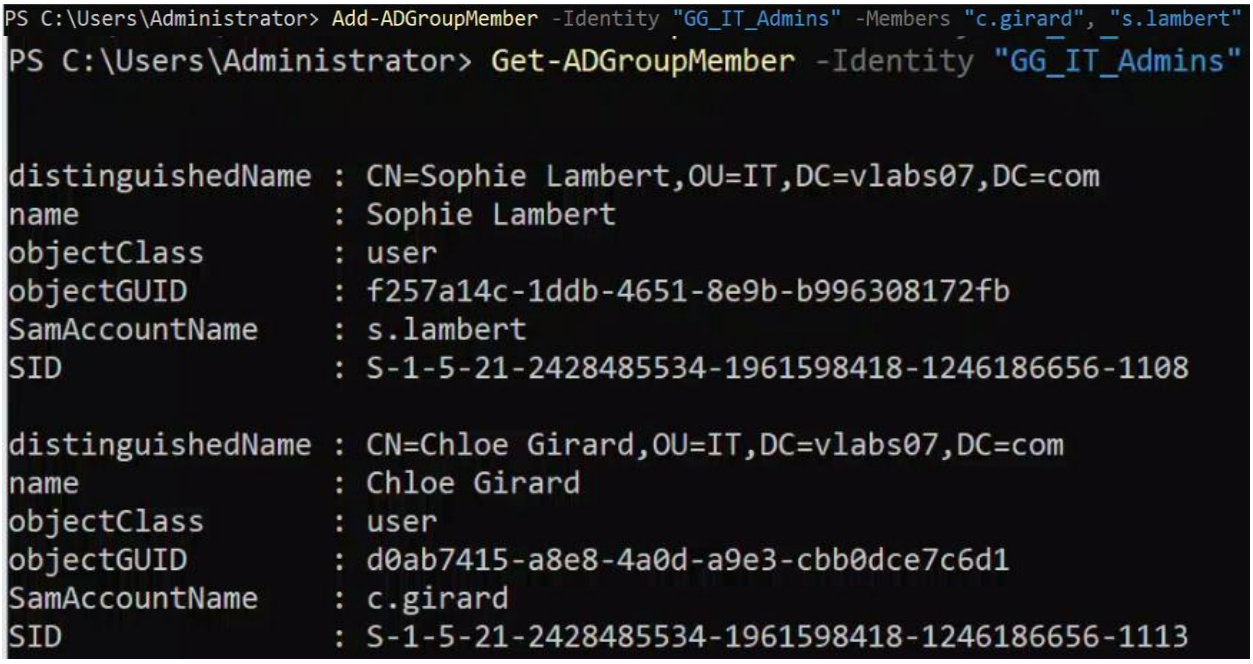
Explanation:

This command adds two users **(**Chloe Girard and Sophie Lambert**)** to the GG_IT_Admins group.

- **-**Identity "GG_IT_Admins" → The target group **for** adding members.
- **-**Members → Specifies the users by their SamAccountNames.

To verify the update, run:
```
Get-ADGroupMember -Identity "GG_IT_Admins"
```

Screenshot:



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

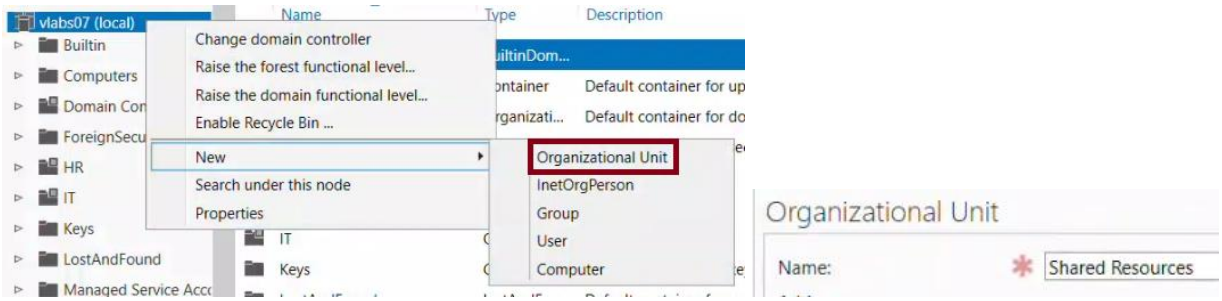
▨ Step 1: Create an OU named "Shared Resources"
System: DC107 (Primary Domain Controller for vlabs07.com)

Explanation:

I used Active Directory Administrative Center (ADAC) to create a new Organizational Unit (OU) named "Shared Resources" at the root of the vlabs07.com domain.
I will place domain local groups inside this OU to manage shared folder access later.

Steps:
- Logged in to DC107
- Opened Active Directory Administrative Center
- Navigated to vlabs07.com
- Clicked "New > Organizational Unit"
- Named the OU: Shared Resources
- Clicked OK to create it

Screenshot:



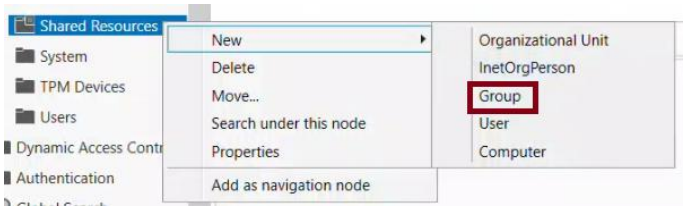
▨ Step 2: Create DLG_HR_Share using ADAC
System: DC107

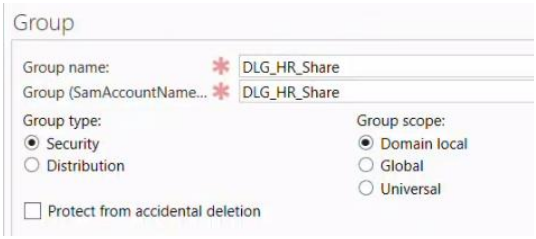
Explanation:

I created a Domain Local Security Group called DLG_HR_Share in the "Shared Resources" OU.
I will use this group to assign folder permissions for the HR department.

Steps:
- In ADAC, I navigated to the "Shared Resources" OU
- Clicked "New > Group"
- Entered:
  Name: DLG_HR_Share
  Group scope: Domain Local
  Group type: Security
- Clicked OK to finish

Screenshot:





▨ Step 3: Create DLG_IT_Share **using** PowerShell

System: DC107

Command:

```
New-ADGroup `
  -Name "DLG_IT_Share" `
  -GroupScope DomainLocal `
  -GroupCategory Security `
  -Path "OU=Shared Resources,DC=vlabs07,DC=com" `
  -SamAccountName "DLG_IT_Share"
```

Explanation:

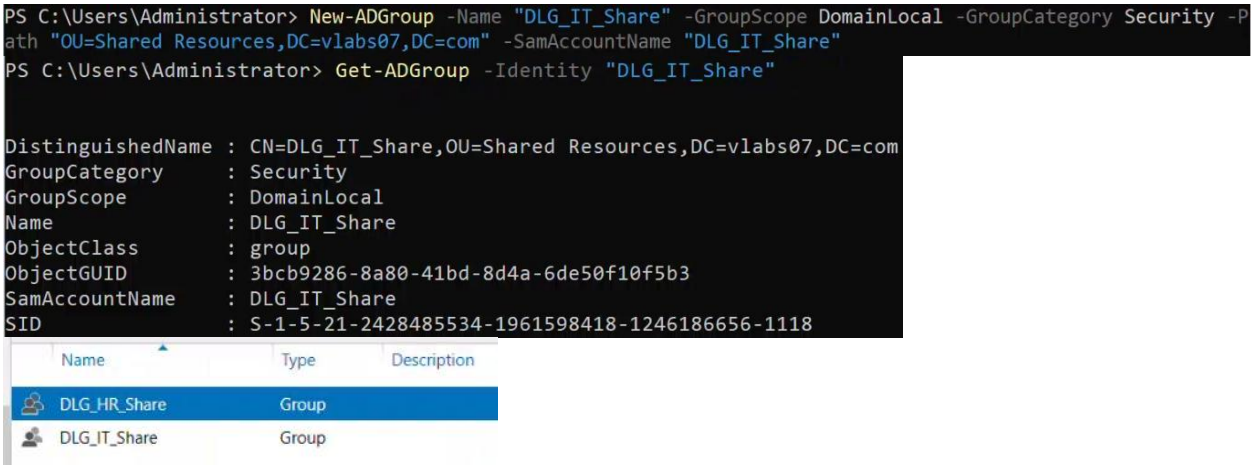
I used this command to create a Domain Local group called DLG_IT_Share inside the "Shared Resources" OU.

- -Name sets the group name
- -GroupScope DomainLocal makes it usable **for** permission assignments within the domain
- -GroupCategory Security allows it to be added to ACLs
- -Path sets the destination OU
- -SamAccountName defines the legacy logon name

To verify that the group was created, I ran:

```
Get-ADGroup -Identity "DLG_IT_Share"
```

Screenshot:



Task 4: Create a Local Group and Manage Membership

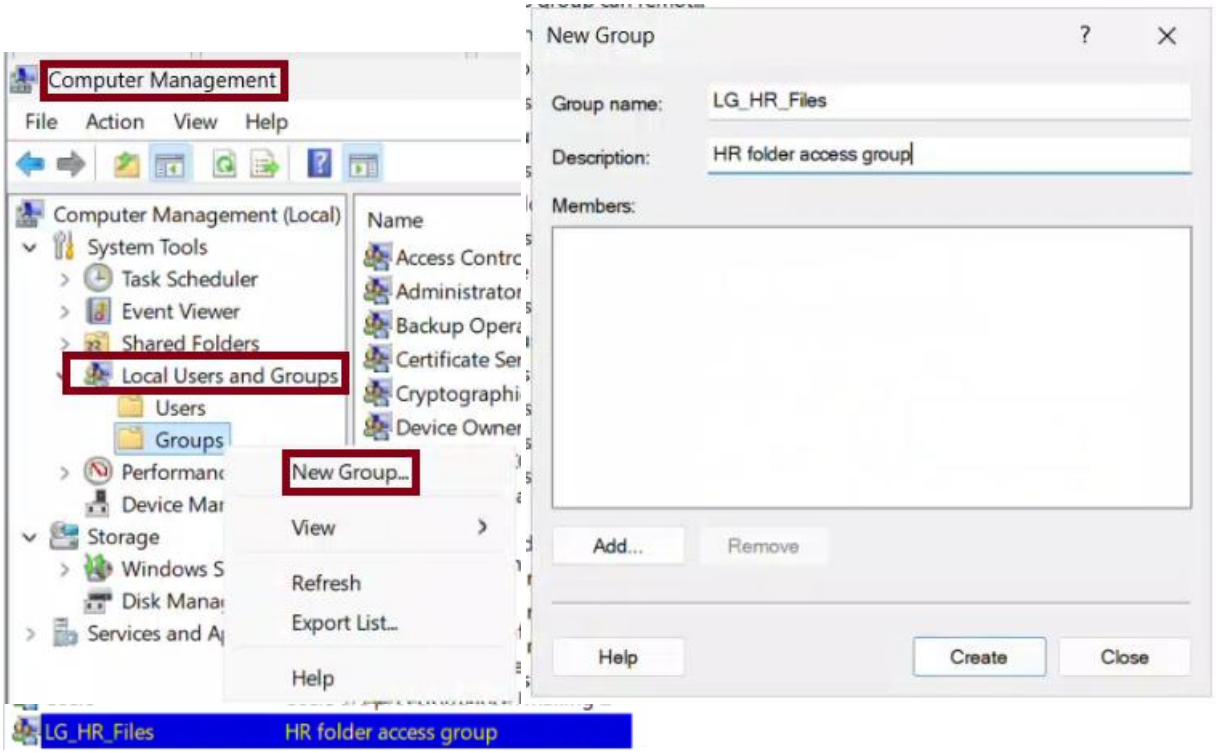
▨ Step 1: Create a local group called LG_HR_Files
System: SRV07 (Windows Server 2025 File Server)

Explanation:

I created a local group named LG_HR_Files **using** the GUI **in** Computer Management.
This group will later be used to assign NTFS permissions to an HR folder on SRV07.

Steps:
- Logged **in** to SRV07
- Opened **Computer Management**
- Navigated to **Local Users and Groups > Groups**
- Right-clicked **Groups**, selected **New Group**
- Entered:
  Group name: LG_HR_Files
  Description: HR folder access group
- Clicked **Create**, then **Close**

Screenshot:



▨ Step 2: Add DLG_HR_Share to LG_HR_Files
System: SRV07

Explanation:

I added the Domain Local Group **DLG_HR_Share** from Active Directory to the local group **LG_HR_Files** on SRV07.
This follows the IGDLA model, where a Domain Local Group is added to a Local Group to manage local access.

Steps:
- Still in **Computer Management > Local Users and Groups > Groups**
- Double-clicked **LG_HR_Files**
- Clicked **Add...**
- Typed: `DLG_HR_Share`
- Clicked **Check Names** (confirmed it resolved from Active Directory)
- Clicked **OK** to add the group

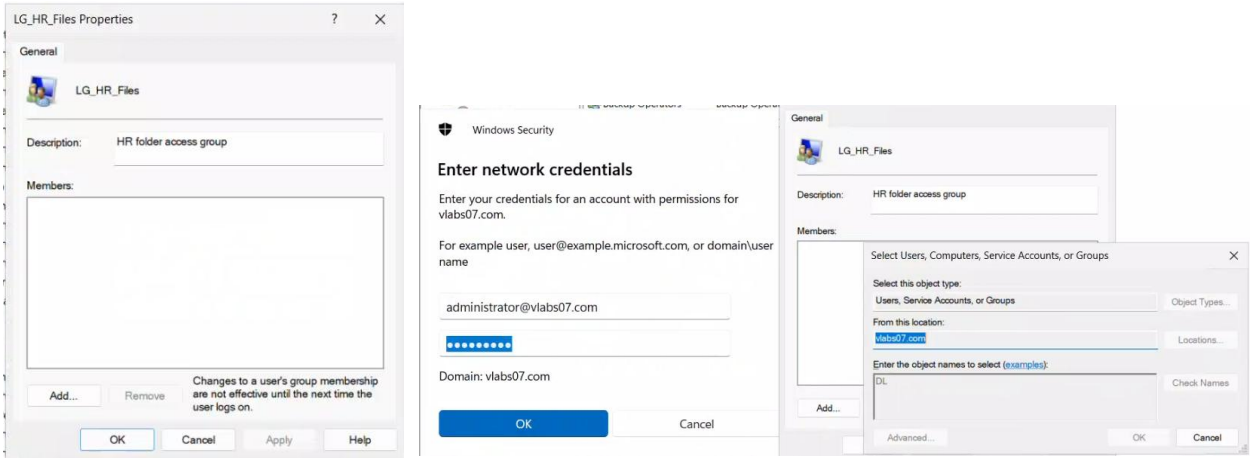
💡 At this point, Windows prompted me for **domain credentials** to search Active Directory. This is expected when the current login is not a domain account.

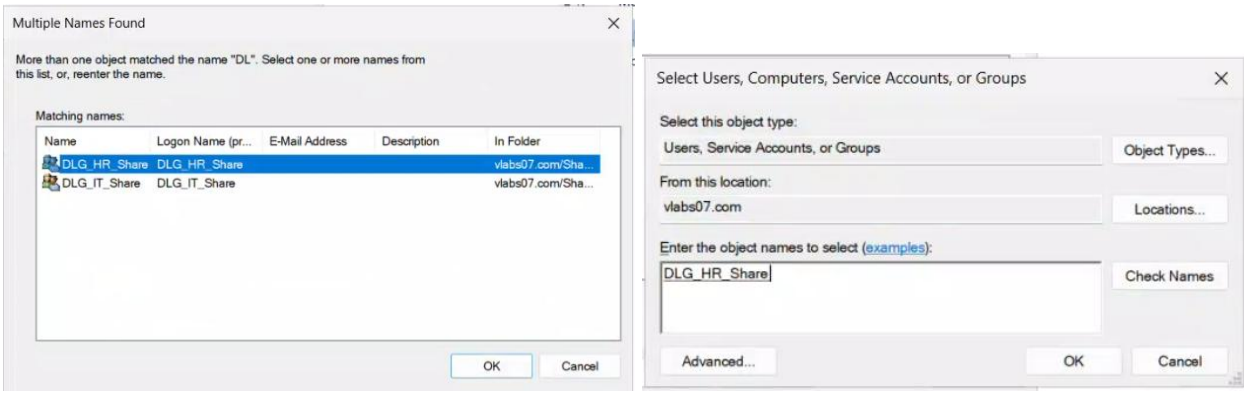
I used one of the following formats to authenticate:

    vlabs07\administrator
    administrator@vlabs07.com

After authentication, the name resolved correctly and I clicked **OK** to add the group.

Screenshot:





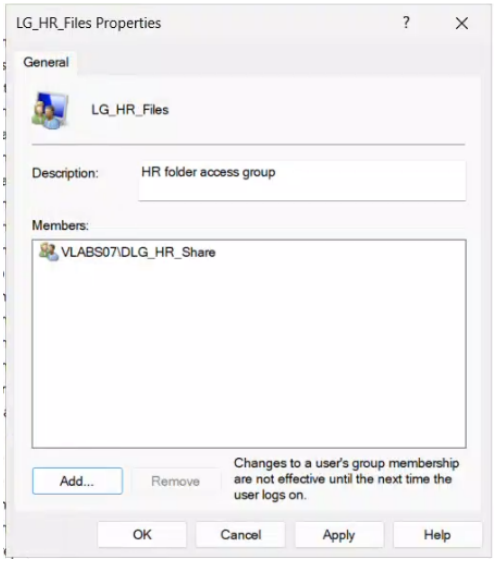
GUI Verification:

After closing the **Select Users, Computers, Service Accounts, or Groups** window, I was returned to the **LG_HR_Files Properties** dialog.

I confirmed that **DLG_HR_Share** appeared in the **Members** list of the group.

Then I clicked **Apply > OK** to finalize the change.

Screenshot:



▨ Step 3: Verify membership of LG_HR_Files
System: SRV07

Command:

```
Get-LocalGroupMember -Group "LG_HR_Files"
```

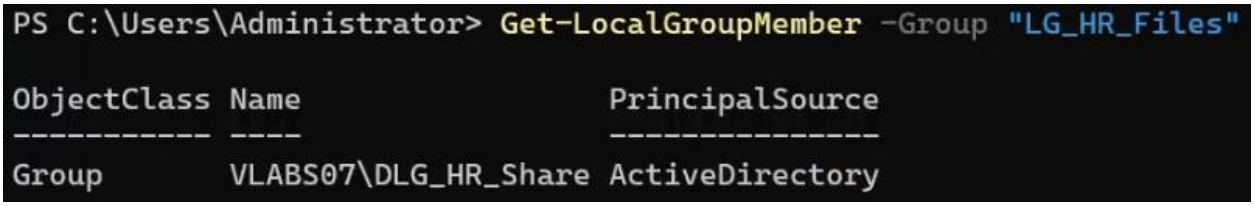
Explanation:

I ran this PowerShell command to confirm that **DLG_HR_Share** was successfully added to **LG_HR_Files**.

- Get-LocalGroupMember lists the current members of a local group
- -Group specifies the name of the local group to check

The output shows that DLG_HR_Share is a domain-based member of the local group.

Screenshot:



Task 5: Share and Set Permissions on SRV07

Step 1: Create and share the folder C:\HR_Share

System: SRV07 (Windows Server 2025 File Server)

Explanation:

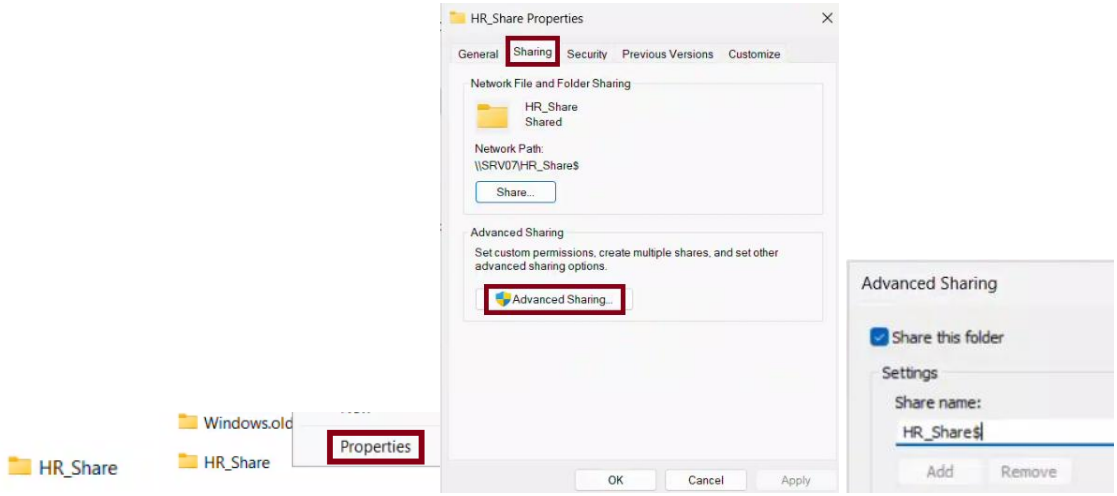
I created a new folder called `HR_Share` on the C: drive of SRV07 and shared it using the GUI.
Then I configured the share permissions to grant access only to the **local group LG_HR_Files**, which controls who can access the share.

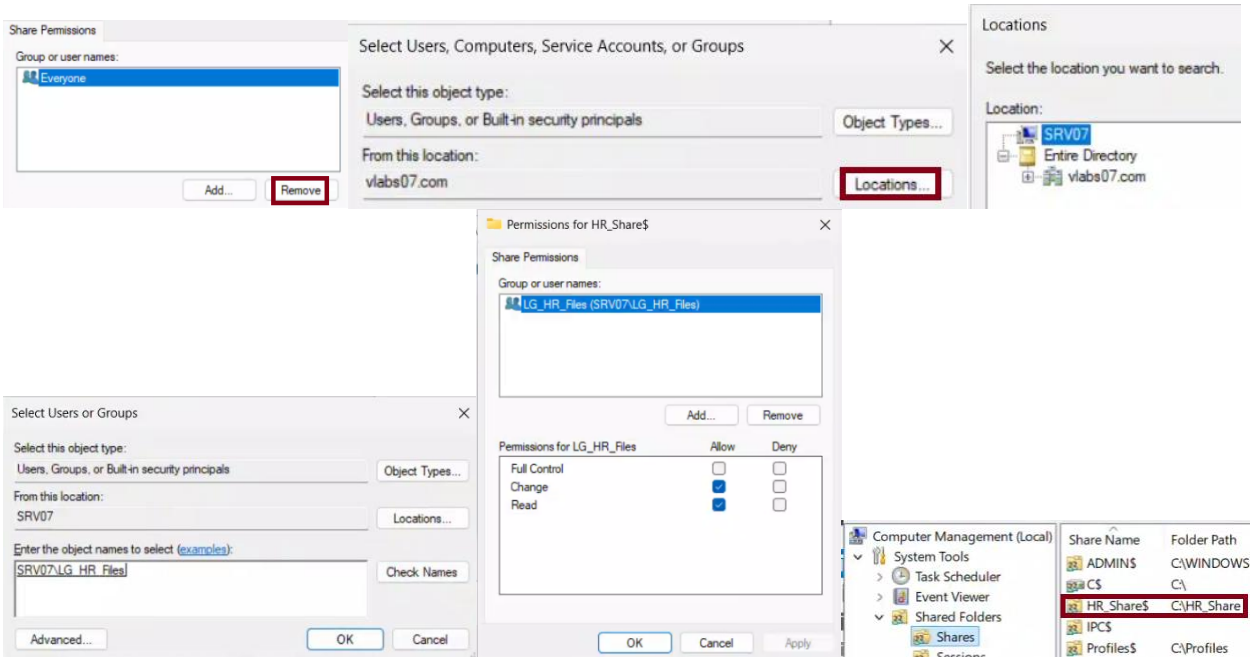
Steps:

- Opened **File Explorer** on SRV07
- Created a new folder: `C:\HR_Share`
- Right-clicked the folder → **Properties**
- Went to the **Sharing** tab → clicked **Advanced Sharing**
- Checked **"Share this folder"**
- Set the **Share name** as: `HR_Share$` *(dollar sign hides it from browsing)*
- Clicked **Permissions...**
- Removed the default **Everyone** group
- Clicked **Add...**
- In the object picker dialog:
  - Clicked **Locations**
  - Selected **SRV07** *(very important: LG_HR_Files is a local group)*
  - Clicked **OK**
  - Entered: `LG_HR_Files` → clicked **Check Names** to resolve it
  - Clicked **OK**
- Selected LG_HR_Files in the list and checked **Full Control**
- Clicked **OK > OK > Close**

Note:
LG_HR_Files is a **local group**, so it only exists on SRV07. If you leave the default domain (vlabs07.com) selected in the "From this location" box, the group wont be found. You must switch to SRV07 to resolve it.

Screenshot:





▨ Step 2: Set NTFS permissions for LG_HR_Files

System: SRV07 (Windows Server 2025 File Server)

Explanation:

I configured NTFS permissions on the `C:\HR_Share` folder so that only members of **LG_HR_Files** have the ability to read, write, and modify files.

I also confirmed that **Everyone** was not present, so no removal was needed.

Steps:

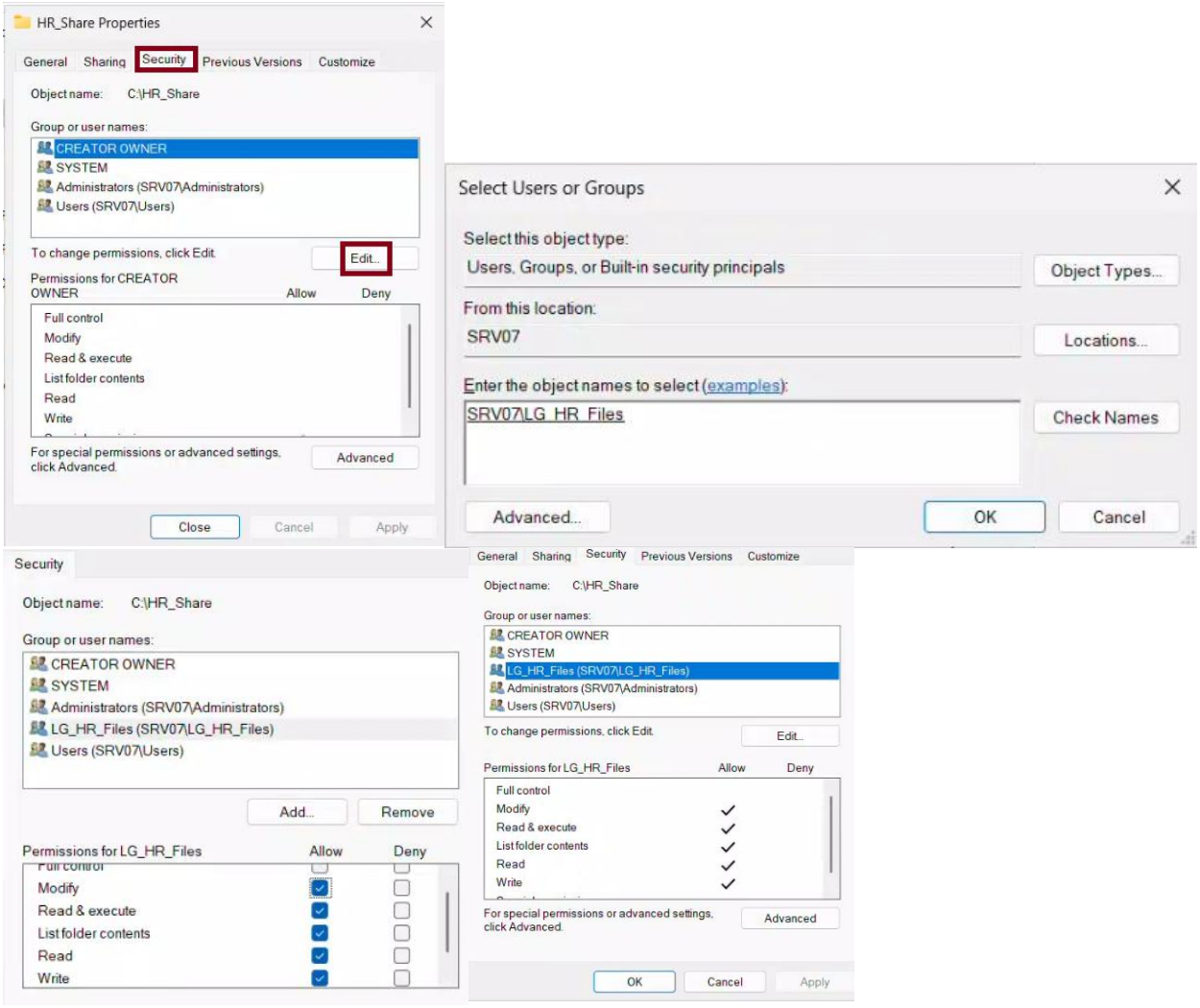
- Right-clicked `C:\HR_Share` → selected **Properties**
- Went to the **Security** tab
- Clicked **Edit...**

- In the Permissions window:
  - Verified that **Everyone** was not present
  - Clicked **Add...**
  - In the object picker:
    - Clicked **Locations...**
    - Selected **SRV07** as the search location (LG_HR_Files is a local group)
    - Clicked **OK**
    - Entered: `LG_HR_Files` and clicked **Check Names**
    - The name resolved as: `SRV07\LG_HR_Files`
    - Clicked **OK**

- With `LG_HR_Files` selected:
    - Checked **Modify**
    - Confirmed that other required permissions (Read & Execute, List Folder Contents, Read, Write) were auto-checked
    - Did not check **Full Control**

- Clicked **Apply > OK > OK** to finalize the NTFS settings

Screenshot:



▨ Step 3: Verify the share and permissions using PowerShell
System: SRV07

Command:

```
Get-SmbShare -Name "HR_Share$"
Get-SmbShareAccess -Name "HR_Share$"
```

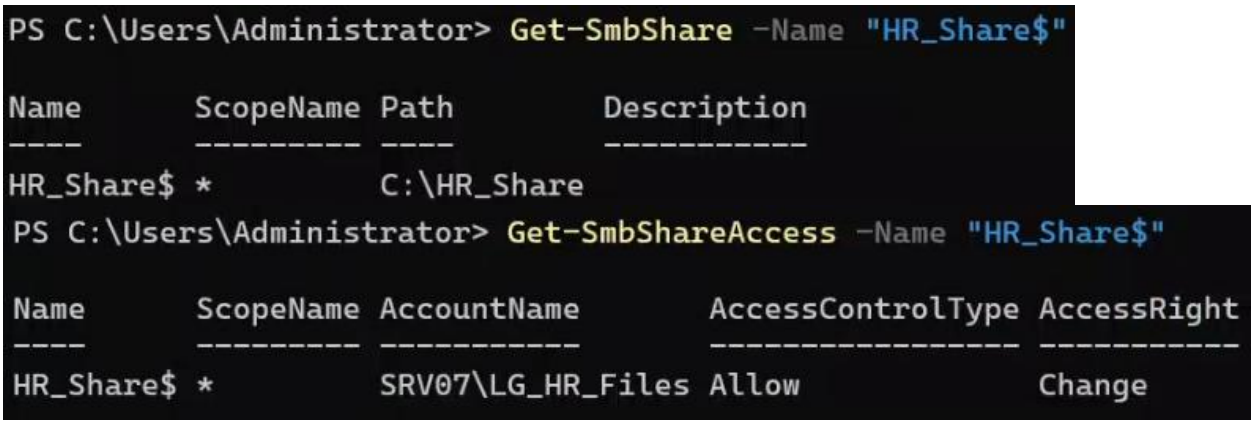
Explanation:

I used these PowerShell commands to confirm that the `HR_Share$` folder was successfully shared and that access permissions were applied correctly.

- `Get-SmbShare` shows the list of all configured shares, including their path and properties.
- `-Name "HR_Share$"` filters for the specific hidden share I created earlier.
- `Get-SmbShareAccess` displays the access control list (ACL) for the share, including what permissions each user or group has.

The output should confirm that:
- The share path is `C:\HR_Share`
- The group `LG_HR_Files` has **Full** or **Change** access, depending on what was configured in the GUI

Screenshot:



Task 6: Test HR Share Access from Client07

▨ Step 1: Log in as Lucas Bernard (l.bernard)
System: Client07 (Windows 11 Client)

Explanation:

I logged in to Client07 using the domain user **Lucas Bernard**, whose username is `l.bernard`.

Lucas is a member of `GG_HR_Admins`, which is a member of `DLG_HR_Share`, and that group was added to `LG_HR_Files` on SRV07.
This structure follows the IGDLA model and should give him access to the HR shared folder.

Steps:
- Started **Client07** (Windows 11)
- Logged in with:
  Username: `l.bernard`
  Password: *(provided by the instructor or domain default)*

Screenshot:

▨ Step 2: Access \\SRV07\HR_Share$ and test file access
System: Client07

Command:

Open File Explorer manually and enter the UNC path below:
\\SRV07\HR_Share$

Then, **in** the shared folder:
1. Right-click **>** New **>** Text Document
2. Name it: lucas_test.txt
3. Open and type: Test from Lucas
4. Save and close the file
5. Right-click the file and select Delete

Explanation:

I logged **in** as Lucas Bernard on Client07 and opened File Explorer.

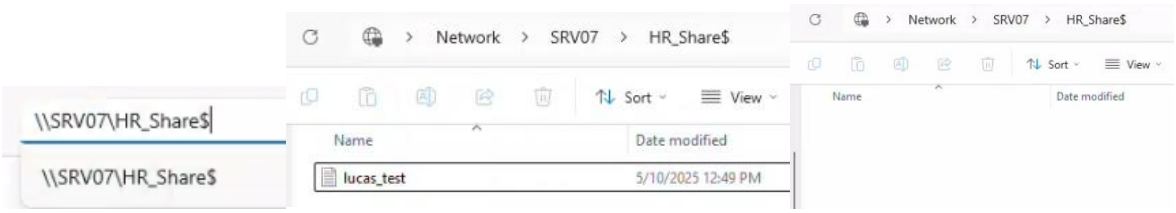
Since the share HR_Share**$** is **hidden**, I manually entered the full UNC path:
\\SRV07\HR_Share**$**

The folder opened successfully, confirming Lucas had inherited access through:
GG_HR_Admins → DLG_HR_Share → LG_HR_Files

To test Modify permission, I created a new file, saved it, then deleted it.

All operations completed without error, confirming that:
- NTFS permission = Modify
- Share permission = Change

Screenshot:



▨ Step 3: Resolve access issue by completing group inheritance
System: DC107

Command:

```
Add-ADGroupMember -Identity "DLG_HR_Share" -Members "GG_HR_Admins"
```

Explanation:

While testing access as Lucas Bernard, I received an access denied message when trying to reach the share \\SRV07\HR_Share$.

After investigation, I found that the Global Group `GG_HR_Admins` was not yet added to the Domain Local Group `DLG_HR_Share`.

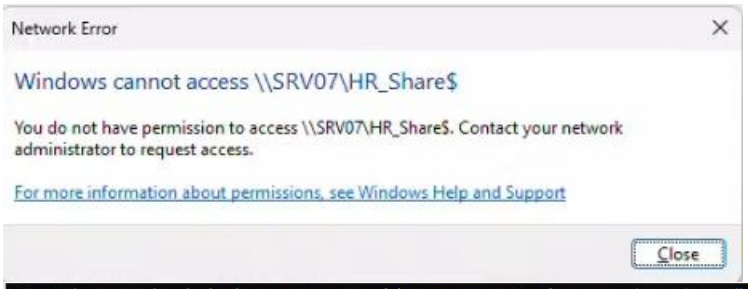
According to the IGDLA model, I must nest the Global Group inside the Domain Local Group to allow permission inheritance.

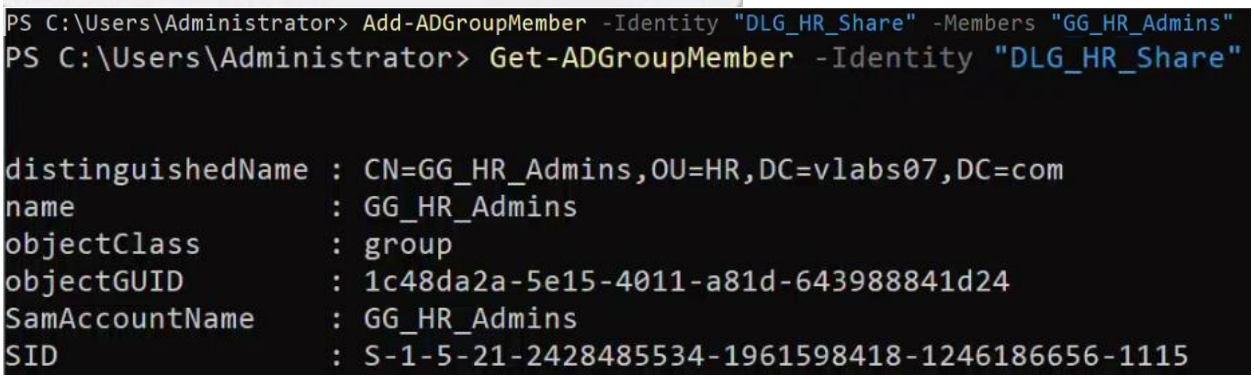
This command adds `GG_HR_Admins` to `DLG_HR_Share`, completing the group chain:
GG_HR_Admins → DLG_HR_Share → LG_HR_Files

To verify:
```
Get-ADGroupMember -Identity "DLG_HR_Share"
```

After running this, I was able to access the share from Client07 as Lucas Bernard.

Screenshot:





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

▨ Step 1: Remove Emma Morel from GG_HR_Admins **using** ADAC
System: DC107

Command:

No PowerShell command — this step is completed **using** ADAC **(**Active Directory Administrative Center**)**

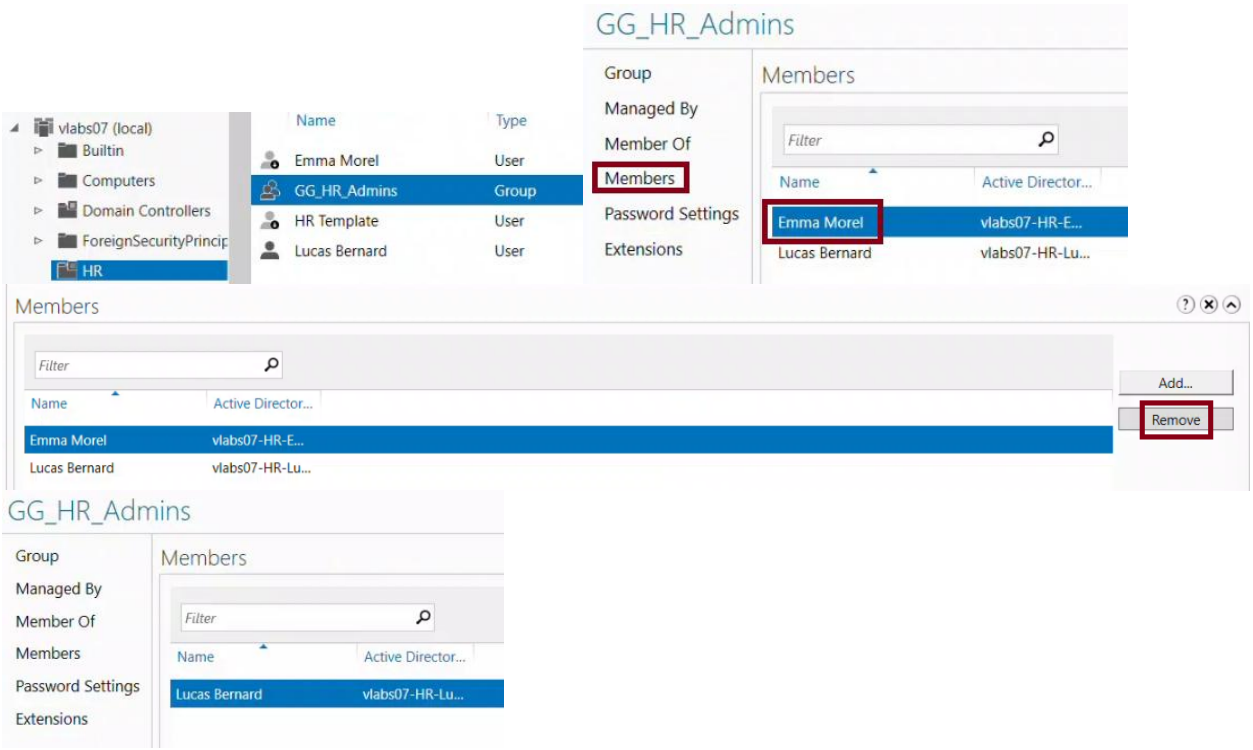
GUI Actions:
1. Open Active Directory Administrative Center **(**ADAC**)** on DC107
2. Navigate to: vlabs07.com **>** HR
3. Double-click GG_HR_Admins
4. Under Members, locate and select "Emma Morel (e.morel)"
5. Click Remove
6. Click OK to confirm and Apply to save changes

Explanation:

I used the ADAC interface to remove user **Emma Morel** from the global group `GG_HR_Admins`.
This simulates revoking share access permissions that were granted indirectly through the IGDLA structure.

After removal, Emma should no longer have access to the HR shared folder.

Screenshot:



▨ Step 2: Remove Chloe Girard from GG_IT_Admins **using** PowerShell
System: DC107

Command:

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

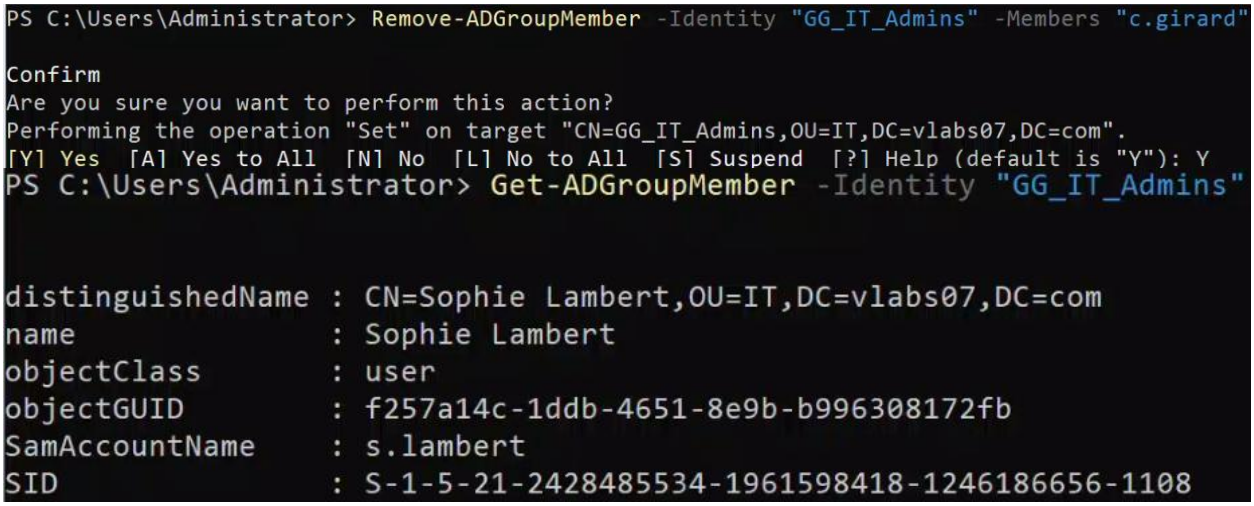
Explanation:

I removed user **Chloe Girard (c.girard)** from the global group `GG_IT_Admins` **using** the `Remove-ADGroupMember` cmdlet.

- `-Identity` specifies the group to remove the member from
- `-Members` specifies the user account to remove
- `-Confirm:$false` skips the confirmation prompt

This change removes Chloe's inherited access to any shared resources linked to `GG_IT_Admins`.

Screenshot:



Task 8: Create IT OU and Configure Groups on DC307 and DC107

▨ Step 1: Create an IT OU using ADAC
System: DC307

Command:

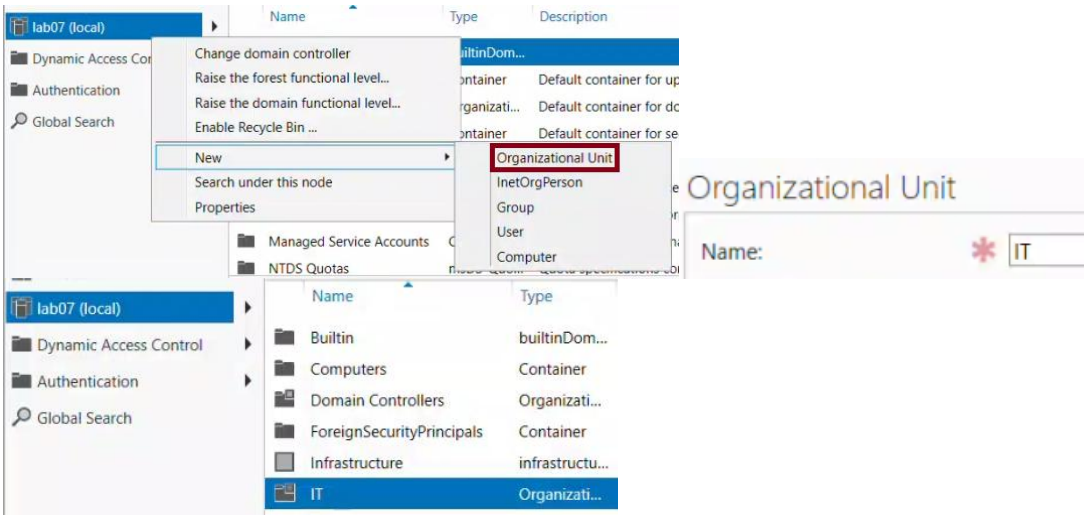
This task is completed using the GUI (ADAC)

GUI Actions:
1. Open Active Directory Administrative Center on DC307
2. Right-click the domain lab07.vlabs07.com
3. Select New > Organizational Unit
4. Name the OU: IT
5. Click OK

Explanation:

I created a new Organizational Unit named **IT** in the child domain **lab07.vlabs07.com** using ADAC.

Screenshot:



▨ Step 2: Create user Fadi Tora (f.tora) inside the IT OU using ADAC
System: DC307

Command:

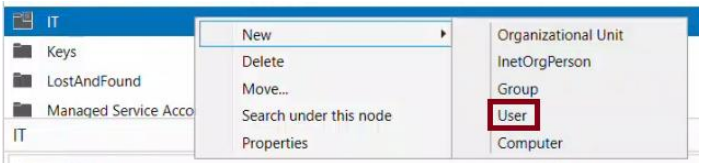
Completed using ADAC GUI

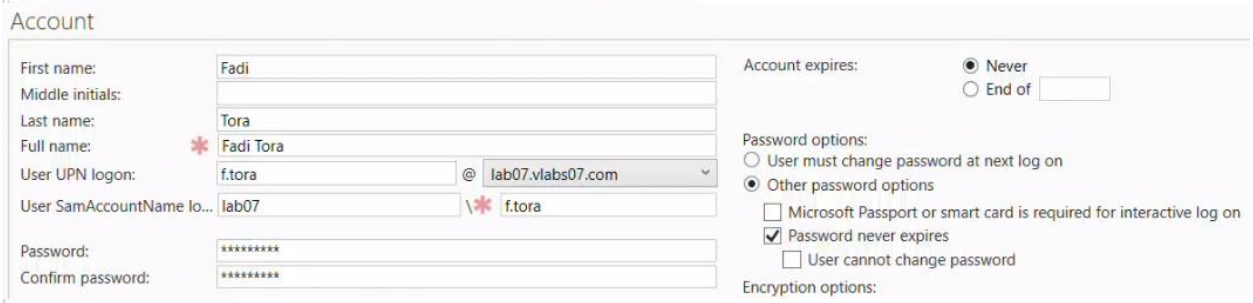
GUI Actions:
1. In the IT OU, right-click > New > User
2. First name: Fadi
3. Last name: Tora
4. Full Name: Fadi Tora
5. User logon name: f.tora
6. Set a password and uncheck "User must change password at next logon"
7. Click OK

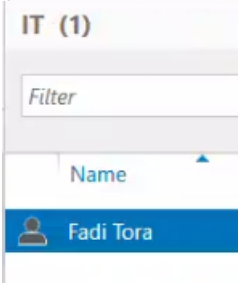
Explanation:

I created a new user **Fadi Tora (f.tora)** inside the **IT OU** under the child domain. This user will later be added to the IT group for cross-domain group nesting.

Screenshot:







▨ Step 3: Create GG_IT_Admins and add Fadi Tora to it using ADAC
System: DC307

Command:

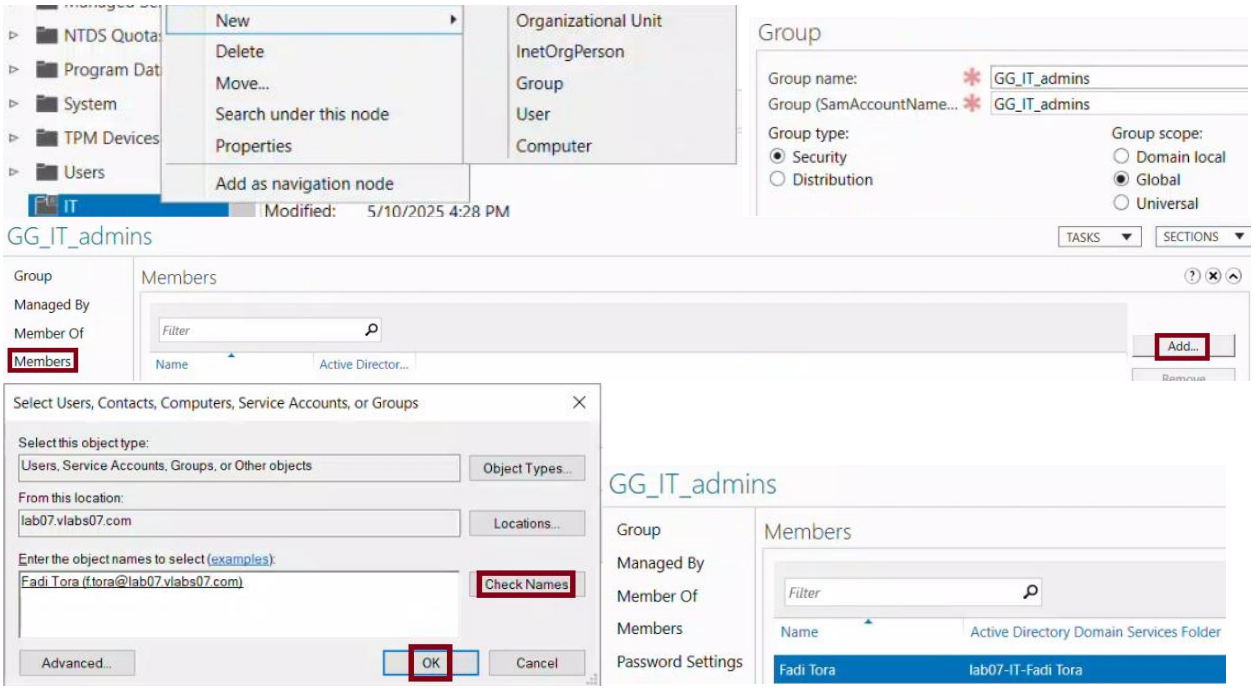
Completed using ADAC GUI

GUI Actions:
1. In the IT OU, right-click > New > Group
2. Group name: GG_IT_Admins
3. Group type: Security
4. Group scope: Global
5. Click OK
6. Open GG_IT_Admins > Members > Add
7. Add: f.tora > Check Names > OK > Apply

Explanation:

I created a Global Group called **GG_IT_Admins** inside the IT OU in lab07.vlabs07.com, and added **Fadi Tora** as a member. This group will be added to a Universal Group on DC107.

Screenshot:



▨ Step 4: Create UG_IT_Global on DC107
System: DC107

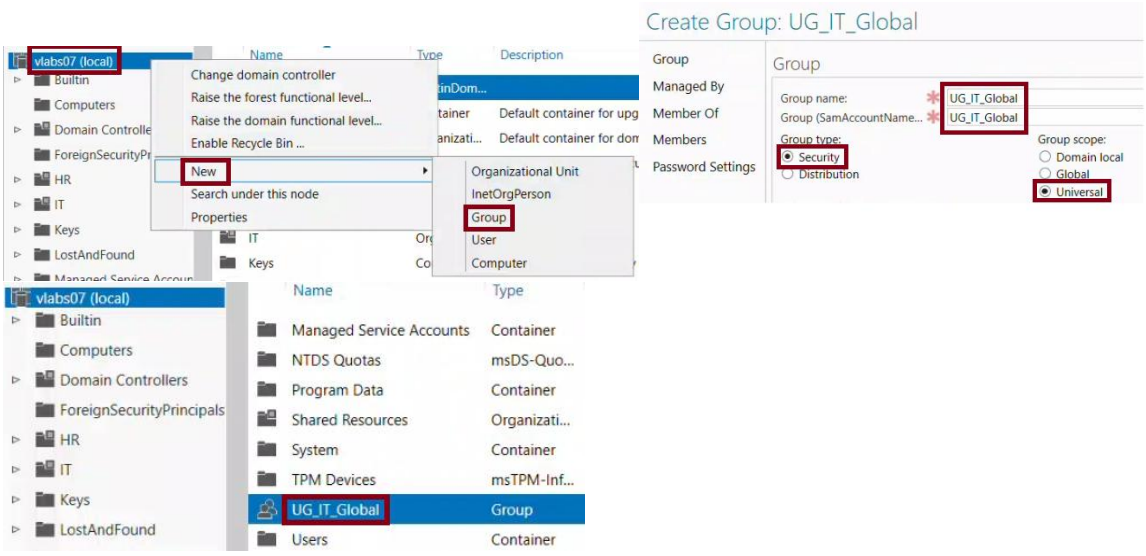
Command:

GUI Method (ADAC):
1. Open ADAC on DC107
2. Navigate to vlabs07.com domain
3. Right-click > New > Group
4. Group name: UG_IT_Global
5. Group scope: Universal
6. Group type: Security
7. Click OK

Explanation:

I created a Universal Group named **UG_IT_Global** in the parent domain (**vlabs07.com**) using ADAC. This group will unify Global Groups from both domains.

Screenshot:



▨ Step 5: Add GG_IT_Admins (from both domains) to UG_IT_Global
System: DC107

Command:

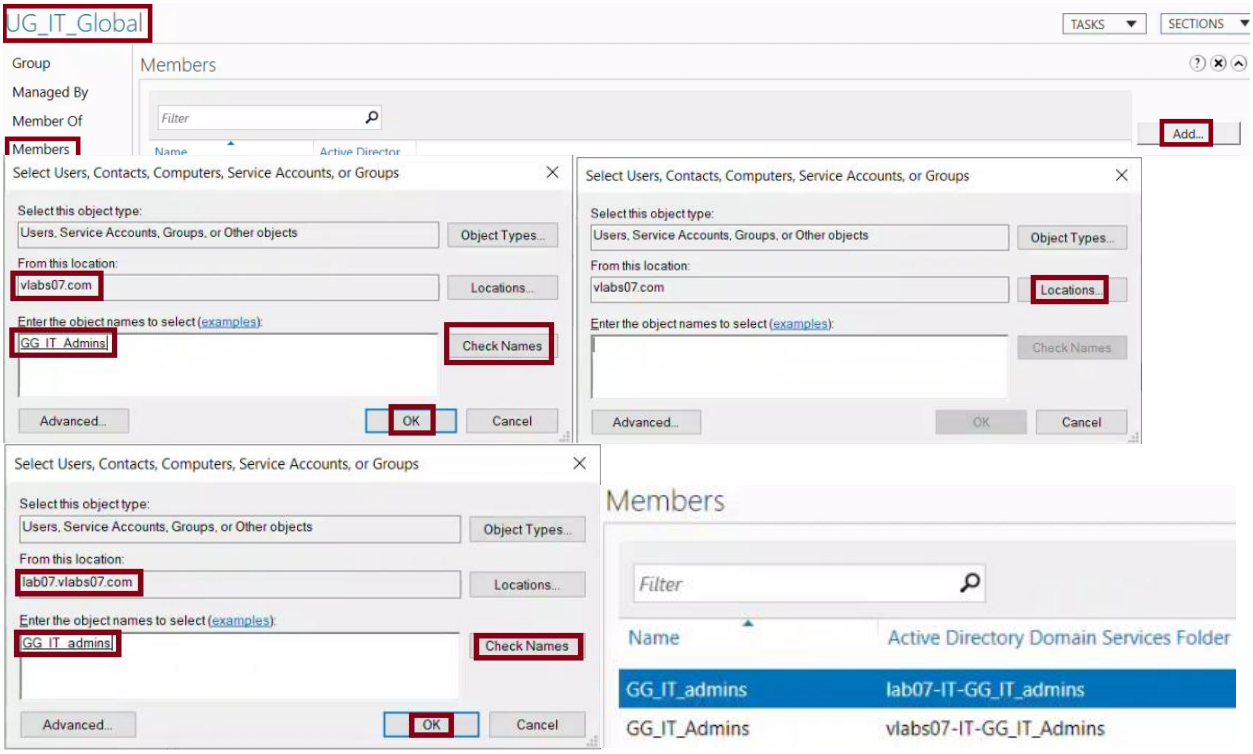
GUI Method (ADAC):
1. Open UG_IT_Global > Members > Add
2. Add:
   - GG_IT_Admins from vlabs07.com
   - GG_IT_Admins from lab07.vlabs07.com
3. Use Locations button to browse both domains if needed
4. Confirm both are listed
5. Click OK

Explanation:

I added both instances of **GG_IT_Admins** from:
- The **parent domain (vlabs07.com)**
- The **child domain (lab07.vlabs07.com)**

to the **Universal Group UG_IT_Global**. This allows cross-domain user membership to be centralized.

Screenshot:



▨ Step 6: Add UG_IT_Global to DLG_IT_Share using PowerShell
System: DC107

Command:

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

Explanation:

I used PowerShell to nest the Universal Group **UG_IT_Global** inside the Domain Local Group **DLG_IT_Share**.

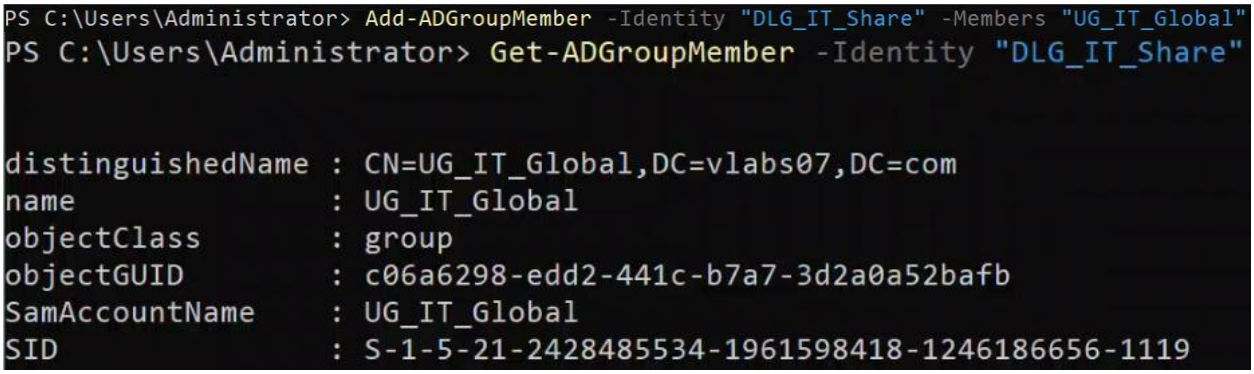
This follows the IGDLA group structure and allows users from both domains to inherit access to shared resources through `DLG_IT_Share`.

Verification:

To confirm the group nesting, I used the following command:
```
Get-ADGroupMember -Identity "DLG_IT_Share"
```

The output displayed `UG_IT_Global` as a member, confirming that the group was added successfully.

Screenshot:



Task 9: Share and Set Permissions for IT Global Share

▨ Step 1: Create and share C:\IT_Share_Global **using** GUI
System: SRV07

Command:

GUI Method:
1. On SRVXX, open File Explorer and navigate to C:\
2. Create a new folder named: IT_Share_Global
3. Right-click the folder **>** Properties **>** Sharing tab
4. Click "Advanced Sharing"
5. Check "Share this folder"
6. Share name: IT_Share_Global**$**
7. Click "Permissions" → Remove "Everyone"
8. Click "Add" → Add UG_IT_Global and grant "Change" **+** "Read" permissions
9. Click OK to close all dialogs

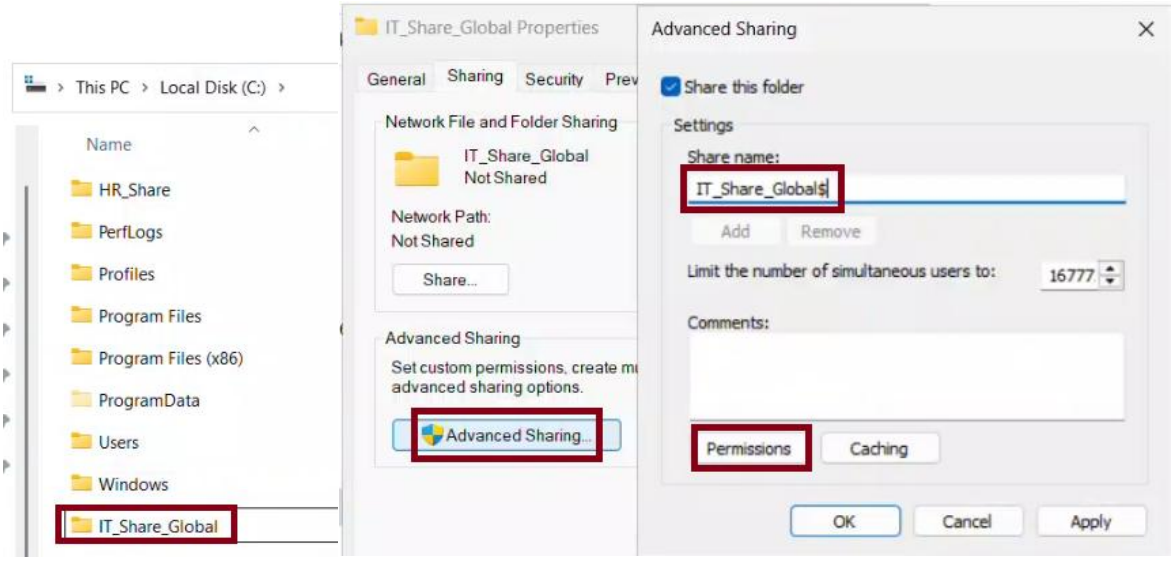
Explanation:

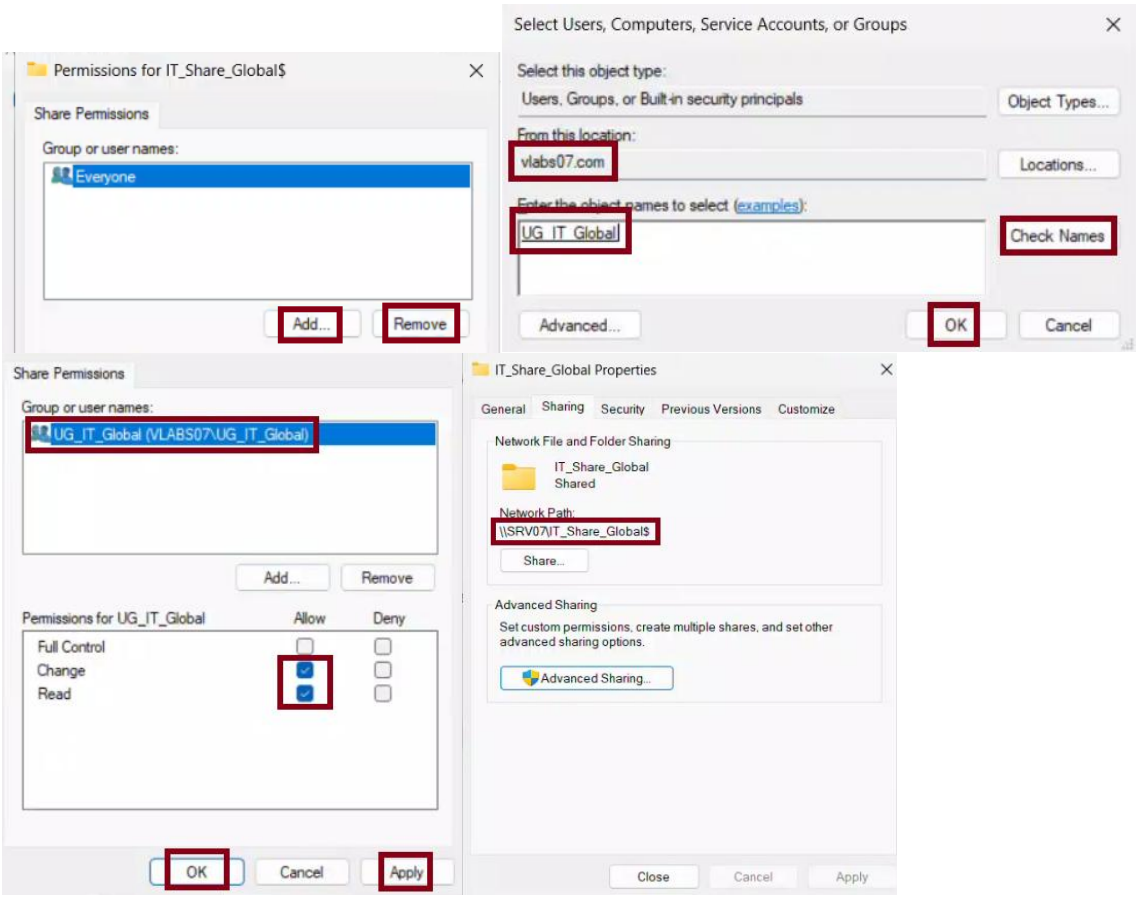
I created and shared a new folder named `C:\IT_Share_Global` on the file server **SRV07** **using** the GUI.

The share name used a `$` suffix to make it **hidden**: `IT_Share_Global**$**`.

I removed the default `Everyone` group and assigned **Change permissions** to the **UG_IT_Global** group, following the lab's access control instructions.

Screenshot:





▨ Step 2: Assign NTFS permissions (Change) to UG_IT_Global **using** GUI
System: SRV07

Command:

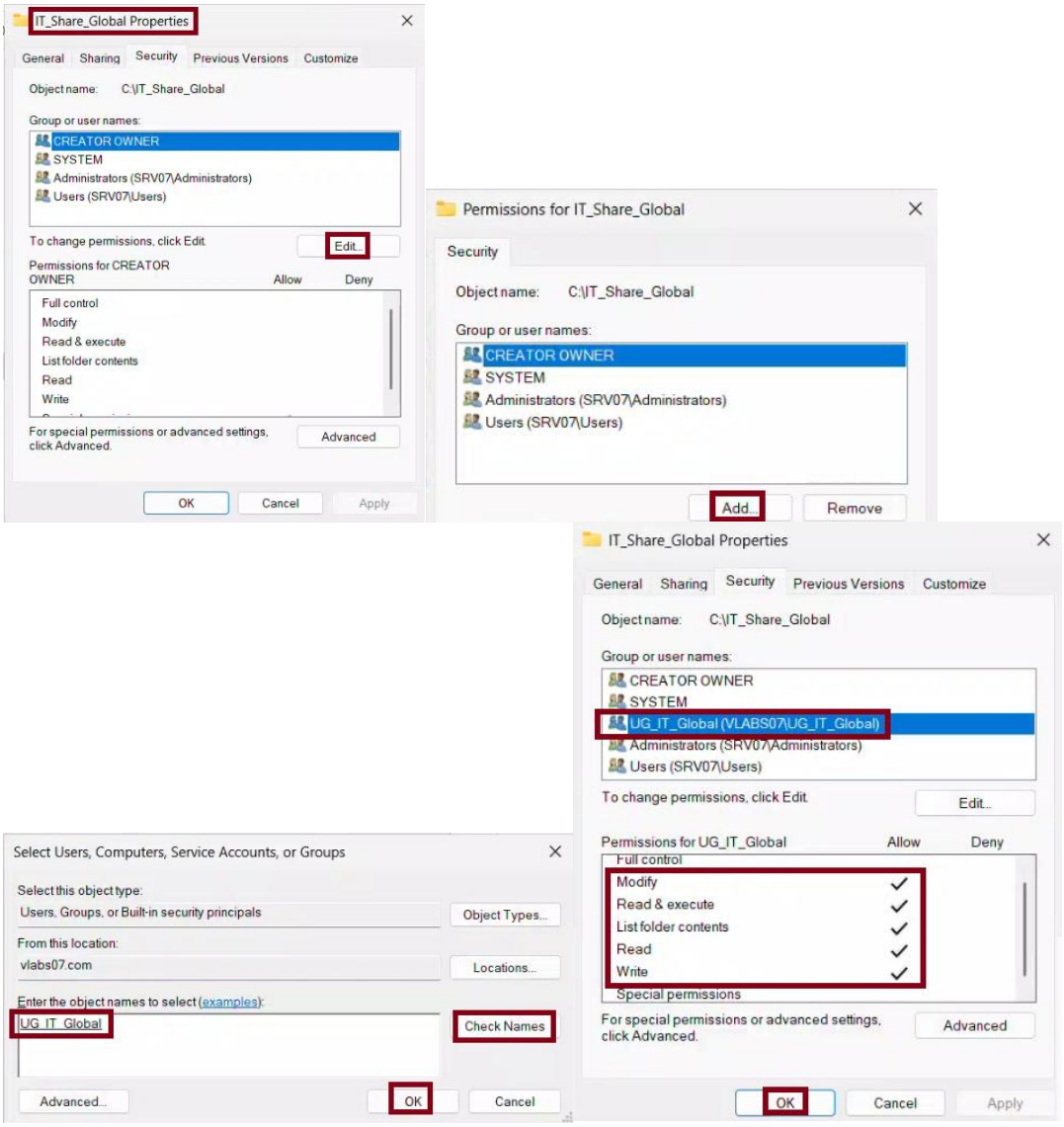
GUI Method:
1. Go to the Security tab of the IT_Share_Global folder
2. Click Edit → Add → Enter: UG_IT_Global
3. Grant the group the following NTFS permissions:
   - Modify
   - Read & execute
   - List folder contents
   - Read
   - Write
4. Click Apply and OK to close all dialogs

Explanation:

I configured NTFS permissions on `C:\IT_Share_Global` so that the group **UG_IT_Global** has full **Modify-level access**.

This complements the share-level "Change" permissions to ensure the group can fully read, write, and delete files.

Screenshot:



▨ Step 3: Verify the share and permissions **using** PowerShell
System: SRV07

Command:

```
Get-SmbShare -Name "IT_Share_Global$"
Get-SmbShareAccess -Name "IT_Share_Global$"
```

Explanation:

I used PowerShell to verify that the `IT_Share_Global**$**` share was created correctly and that **UG_IT_Global** has “Change” access.

These cmdlets confirm both the share path and the assigned access control.

Screenshot:

```
PS C:\Users\Administrator> Get-SmbShare -Name "IT_Share_Global$"

Name             ScopeName Path              Description
----             --------- ----              -----------
IT_Share_Global$ *         C:\IT_Share_Global
PS C:\Users\Administrator> Get-SmbShareAccess -Name "IT_Share_Global$"

Name             ScopeName AccountName          AccessControlType AccessRight
----             --------- -----------          ----------------- -----------
IT_Share_Global$ *         VLABS07\UG_IT_Global Allow             Change
```

Task 10: Test IT Share Access from Client07

▨ Step 1: Log in as Fadi Tora (f.tora)
System: Client07 (Windows 11)

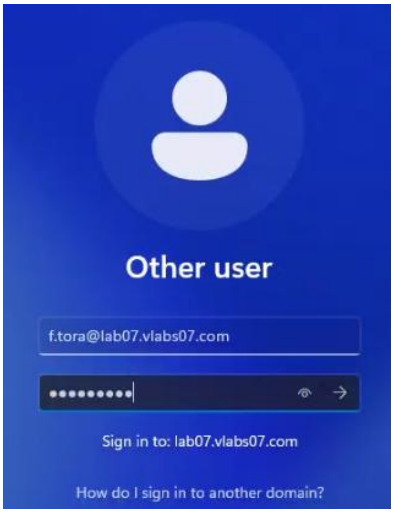
Command:

GUI Method:
1. Sign out of the current user session on Client07
2. Log in as:
    Username: f.tora
    Domain: lab07.vlabs07.com

Explanation:

I logged into the domain-joined Windows 11 client (**Client07**) using the account **Fadi Tora (f.tora)**, which was created earlier in the child domain `lab07.vlabs07.com`.

Screenshot:



▨ Step 2: Check group membership of f.tora using Command Prompt
System: Client07

Command:
---
whoami /groups

Explanation:

I opened Command Prompt and used `whoami /groups` to list all security groups that the user **f.tora** is currently a member of.

This output confirms the users indirect membership in **UG_IT_Global**, which grants access to the shared folder.

Screenshot:

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

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ==================
Everyone                                   Well-known group S-1-1-0                                       Mandatory group, En
abled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4                                       Mandatory group, En
abled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1                                       Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group, En
abled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0                                       Mandatory group, En
abled by default, Enabled group
LAB07\GG_IT_admins                         Group            S-1-5-21-987840292-880875472-4280997625-1105  Mandatory group, En
abled by default, Enabled group
VLABS07\UG_IT_Global                       Group            S-1-5-21-2428485534-1961598418-1246186656-1119 Mandatory group, En
abled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                      Mandatory group, En
abled by default, Enabled group
VLABS07\DLG_IT_Share                       Alias            S-1-5-21-2428485534-1961598418-1246186656-1118 Mandatory group, En
abled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
```

▨ Step 3: Access \\SRV07\IT_Share_Global$ and test permissions
System: Client07

Command:

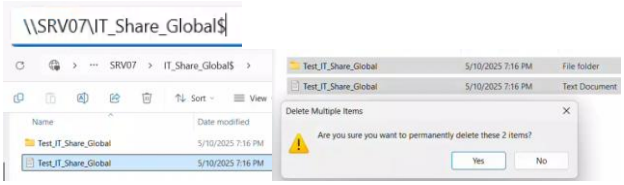
GUI Method:
1. Open File Explorer
2. In the address bar, type:
   \\SRV07\IT_Share_Global$
3. Press Enter
4. Inside the folder, right-click > New > Text Document
5. Create, rename, and delete the file to confirm full write access

Explanation:

I accessed the **hidden** network share `\\SRV07\IT_Share_Global$` from File Explorer.

I then created and deleted a file inside the folder to confirm that **f.tora**, through the group **UG_IT_Global**, has the correct **read/write (Change)** permissions set on both the share and NTFS levels.

Screenshot:



Task 11: Change Group Scope

▨ Step 1: Remove Cross-Domain Member Before Conversion

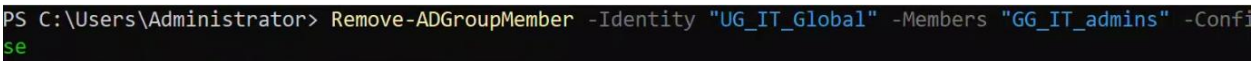
Command:

```
Remove-ADGroupMember -Identity "UG_IT_Global" -Members "GG_IT_admins" -Confirm:$false
```

Explanation:

Before converting a Universal group to a Global group, any cross-domain members must be removed.
In our case, **GG_IT_admins** from the child domain `lab07.vlabs07.com` was removed from **UG_IT_Global** to allow the group scope change.

Screenshot:



▨ Step 2: Change Group Scope to Global

Command:

```
Set-ADGroup -Identity "UG_IT_Global" -GroupScope Global
```

Explanation:

With the child domain group removed, I changed the scope of **UG_IT_Global** from **Universal** to **Global** using PowerShell.
This change is required for environments where Global scope is preferred or needed for compatibility.

Screenshot:

▨ Step 3: Confirm in GUI (ADAC)

Action:
---
1. Open Active Directory Administrative Center on DC107
2. Navigate to vlabs07.com > UG_IT_Global
3. Check the group properties

Explanation:

I confirmed that the group scope is now **Global** by viewing the properties of **UG_IT_Global** inside ADAC.

Screenshot:


UG_IT_Global
Group
Managed By
Member Of
Members
Password Settings
Extensions
Group
Group name:
UG_IT_Global
Group (SamAccountName...
UG_IT_Global
Group type:
Security
Distribution
Group scope:
Domain local
Global
Universal