

Table of Contents

Lab Assignment 2 (Part III) - GPO	2
Task 1: Understanding Domain-Based GPOs	2
Task 2: GPO Storage and Replication.....	11
Task 3: Group Policy Troubleshooting	15
Task 4: Group Policy Modeling and Results	24
Task 5: Delegating GPO Management	28

Lab Assignment 2 (Part III) - GPO

Task 1: Understanding Domain-Based GPOs

System: DC107, Client07

Step 1 - What are Domain-Based GPOs and why are we working with them?

Group Policy Objects (GPOs) are used to manage user and computer settings in a domain.

There are two main default GPOs in every domain:

- Default Domain Policy: applies security settings like password and account lockout rules.
- Default Domain Controllers Policy: applies settings specific to Domain Controllers.

In this task, we will:

- View the existing GPOs
- Delete and restore the default policies using PowerShell
- Turn off Local GPO processing to prioritize domain-based settings
- Compare domain-based GPOs to local GPOs on a client machine

This helps us understand how domain-based policies take precedence and are centrally managed.

Step 2 - View Existing Domain-Based GPOs

On DC107:

Open the Group Policy Management Console

Start → Run → type: gpmmc.msc → Enter

In the left panel:

Expand vlabs07.com

Click on "Group Policy Objects"

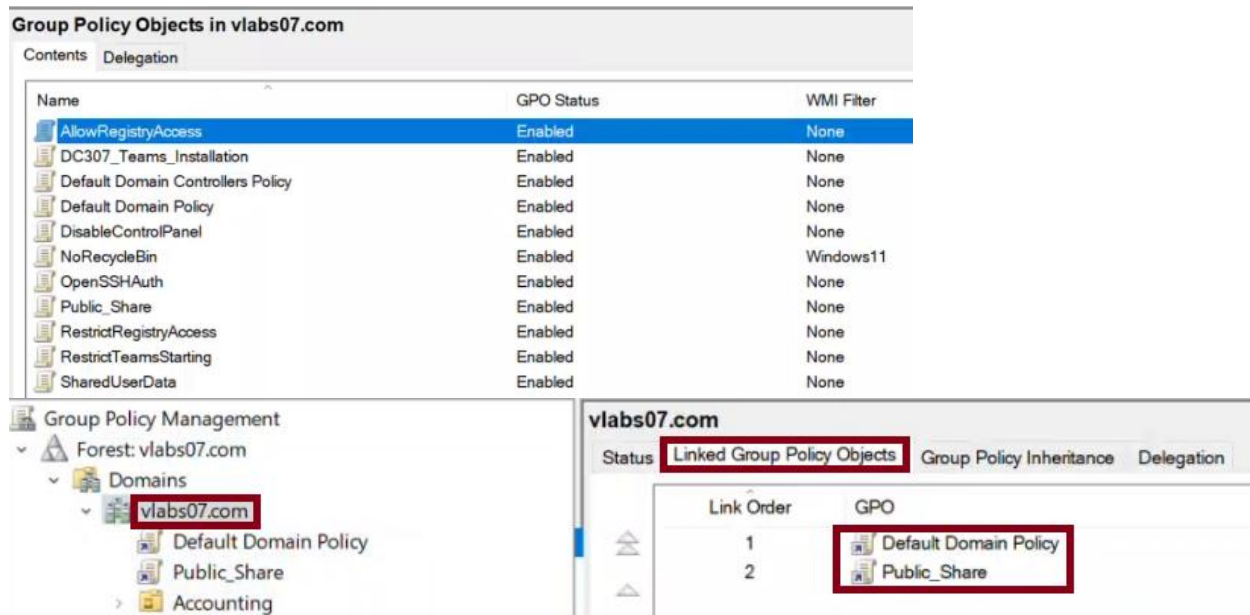
You will see a list of all GPOs defined in the domain.

This shows **which GPOs exist**, but **not where they are linked**.

To see where GPOs are linked:

Click on the domain root and each Organizational Unit (OU),

Then select the "Linked Group Policy Objects" tab on the right panel.



Optional – Use PowerShell to Display Linked GPOs by Container

This PowerShell method lists all domain containers (OUs and domain root) and shows which GPOs are linked to them.

You can run it one line at a time:

1. Get the distinguished name (DN) of the domain:

```
$domainDN = (Get-ADDomain).DistinguishedName
```

```
PS C:\Users\Administrator> $domainDN = (Get-ADDomain).DistinguishedName
```

Explanation:

This gets the unique name that identifies your domain – something like "DC=vlabs07,DC=com". We'll use this to target the root of the domain.

2. Get the distinguished names of all OUs and add the domain to the list:

```
$containers = @($domainDN) + (Get-ADOrganizationalUnit -Filter *)
.DistinguishedName
```

```
PS C:\Users\Administrator> $containers = @($domainDN) + (Get-ADOrganizationalUnit -Filter *)
.DistinguishedName
```

Explanation:

This creates a list of every Organizational Unit in your domain and adds the domain root at the beginning. Now we can loop through every container and check GPO links.

3. Loop through each container and show its linked GPOs:

Once `$containers` is ready, run the following one-liner to display linked GPOs:

```
$containers | ForEach-Object { $links = Get-GPINheritance -Target $_ -ErrorAction SilentlyContinue; if ($links.GpoLinks) { Write-Host "Container: $_"; $links.GpoLinks | ForEach-Object { Write-Host "  GPO: $($_.DisplayName) (Enforced: $($_.Enforced))" }; Write-Host "" } }
```

```
PS C:\Users\Administrator> $containers | ForEach-Object { $links = Get-GPINheritance -Target $_ -ErrorAction SilentlyContinue; if ($links.GpoLinks) { Write-Host "Container: $_"; $links.GpoLinks | ForEach-Object { Write-Host "  GPO: $($_.DisplayName) (Enforced: $($_.Enforced))" }; Write-Host "" } }
```

Command Breakdown:

```
** $containers | ForEach-Object { ... } **
```

This means: "For each container (OU or domain) in the list, run the block of code inside { }"

```
** $links = Get-GPINheritance -Target $_ -ErrorAction SilentlyContinue **
```

This checks the current container (represented by `$_`) to see what GPOs are linked to it

`SilentlyContinue` hides errors for containers that don't have any GPOs

```
** if ($links.GpoLinks) { ... } **
```

Only continues if there are GPOs linked to that container

```
** Write-Host "Container: $_" **
```

Displays the name of the container currently being processed

```
** $links.GpoLinks | ForEach-Object { ... } **
```

Goes through each GPO linked to the container

```
** Write-Host "  GPO: $($_.DisplayName) (Enforced: $($_.Enforced))" **
```

Prints the name of the GPO and whether its enforced (True or False)

```
** Write-Host "" **
```

Adds a blank line between each container for easier reading

Result:

This script will display one container at a time, followed by any GPOs linked to it.

It's useful for documentation and verification of GPO link locations.

```
Container: DC=vlabs07,DC=com
  GPO: Default Domain Policy (Enforced: False)
  GPO: Public_Share (Enforced: False)

Container: OU=Domain Controllers,DC=vlabs07,DC=com
  GPO: Default Domain Controllers Policy (Enforced: False)

Container: OU=HR,DC=vlabs07,DC=com
  GPO: DisableControlPanel (Enforced: False)
  GPO: SharedUserData (Enforced: False)

Container: OU=Call Center,DC=vlabs07,DC=com
  GPO: NoRecycleBin (Enforced: False)

Container: OU=Finance,DC=vlabs07,DC=com
  GPO: AllowRegistryAccess (Enforced: False)
```

```
Container: OU=Engineering,DC=vlabs07,DC=com
  GPO: RestrictTeamsStarting (Enforced: False)
  GPO: DC307_Teams_Installation (Enforced: False)

Container: OU=Finance-Admins,OU=Finance,DC=vlabs07,DC=com
  GPO: RestrictRegistryAccess (Enforced: False)
```

Step 3 - Attempt to Delete the Default Domain Policies

Still **in** GPMC on DC107:

Right-click "Default Domain Policy" → Delete → Yes

Right-click "Default Domain Controllers Policy" → Delete → Yes

We are doing this to simulate a recovery scenario **using** PowerShell.

In real environments, these GPOs **should** never be deleted unless you plan to restore them immediately.

In our lab environment, deletion was not possible.

Even after taking ownership **in** ADSI Edit and assigning Full Control permissions,

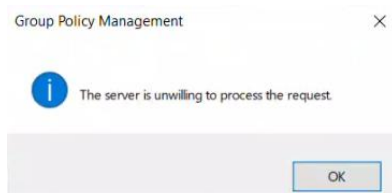
attempts to delete these policies **using** GPMC and PowerShell failed.

The error received was:

"The server is unwilling to process the request (0x80072035)"

This indicates that these GPOs are protected at a deeper system level, possibly enforced by Active Directory schema rules or internal protections.

As a result, we proceeded to Step 4 **using** the dcgpofix tool to reset the policies.



Step 4 - Restore the Default GPOs **Using** PowerShell

Open PowerShell as Administrator on DC107

Run the following two commands to restore the built-in policies:

```
dcgpofix /ignore schema /Target:Domain
```

```
PS C:\Users\Administrator> dcgpofix /ignore schema /Target:Domain

Microsoft(R) Windows(R) Operating System Default Group Policy Restore Utility v5.1
Copyright (C) Microsoft Corporation. 1981-2003

Description: Recreates the Default Group Policy Objects (GPOs) for a domain

Syntax: DcGPOFix [/ignore schema] [/Target: Domain | DC | BOTH]

This utility can restore either or both the Default Domain Policy or the
Default Domain Controllers Policy to the state that exists immediately after
domain creation. You must be a domain administrator to perform this operation.

WARNING: YOU WILL LOSE ANY CHANGES YOU HAVE MADE TO THESE GPOs. THIS UTILITY
IS INTENDED ONLY FOR DISASTER RECOVERY PURPOSES.

You are about to restore Default Domain Policy for the following domain:
vlabs07.com
Do you want to continue: <Y/N>? Y
```

```
dcpofix /ignoreschema /Target:DC
```

```
PS C:\Users\Administrator> dcpofix /ignoreschema /Target:DC

Microsoft(R) Windows(R) Operating System Default Group Policy Restore Utility v5.1

Copyright (C) Microsoft Corporation. 1981-2003

Description: Recreates the Default Group Policy Objects (GPOs) for a domain

Syntax: DcGPOFix [/ignoreschema] [/Target: Domain | DC | BOTH]

This utility can restore either or both the Default Domain Policy or the
Default Domain Controllers Policy to the state that exists immediately after
domain creation. You must be a domain administrator to perform this operation.

WARNING: YOU WILL LOSE ANY CHANGES YOU HAVE MADE TO THESE GPOS. THIS UTILITY
IS INTENDED ONLY FOR DISASTER RECOVERY PURPOSES.

You are about to restore Default Domain Controller Policy for the following domain:
vlabs07.com
Do you want to continue: <Y/N>? Y
```

Command Breakdown:

- dcpofix: Resets default Group Policy Objects
- /Target:Domain: Restores Default Domain Policy
- /Target:DC: Restores Default Domain Controllers Policy
- /ignoreschema: Ensures it runs even if schema version mismatch occurs

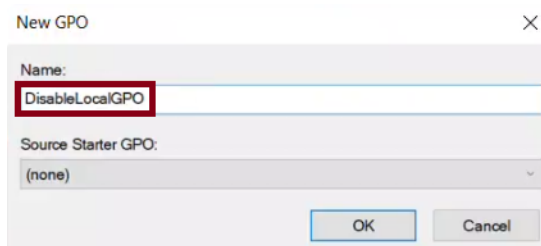
Press `Y` when prompted to confirm restoration

Step 5 - Disable Local GPO Processing

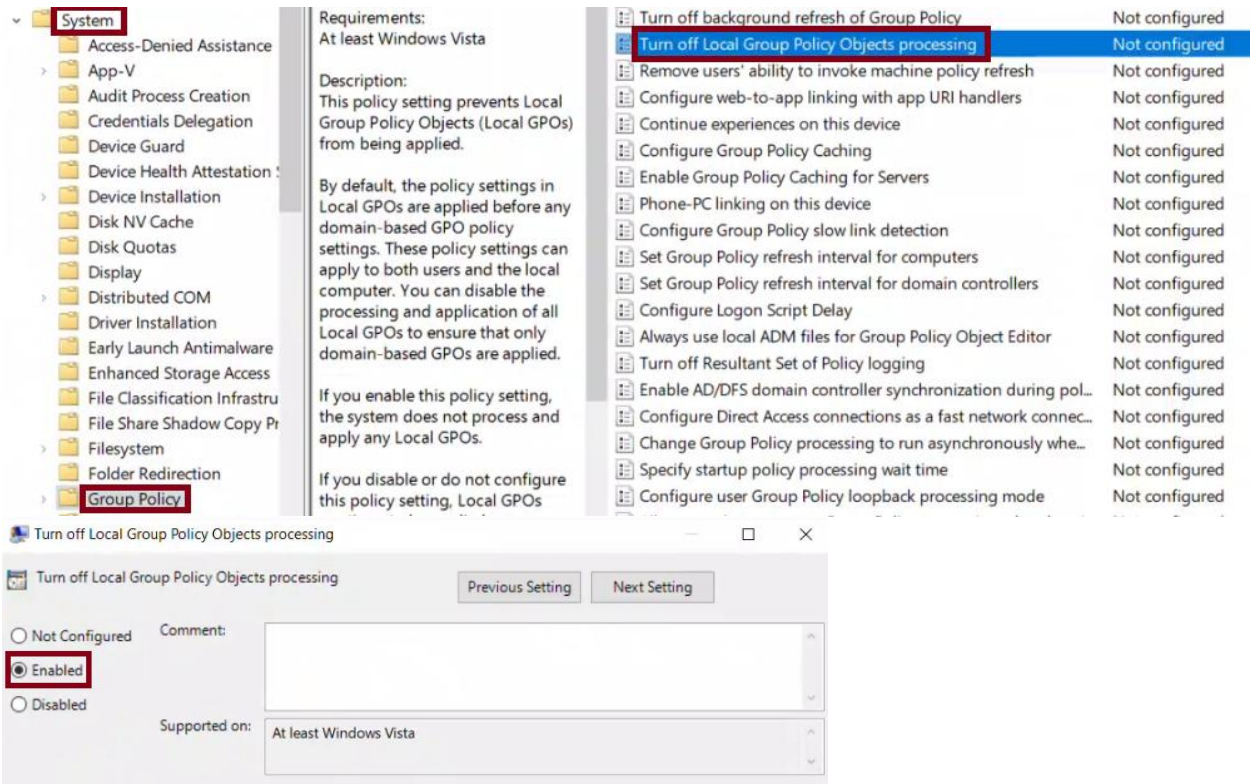
We want to enforce that only domain-based GPOs are applied.
To **do** this, we'll create and link a new GPO that disables local GPO processing.

In GPMC on DC107:

Right-click "Group Policy Objects" → New
Name the new GPO: DisableLocalGPO → Click OK

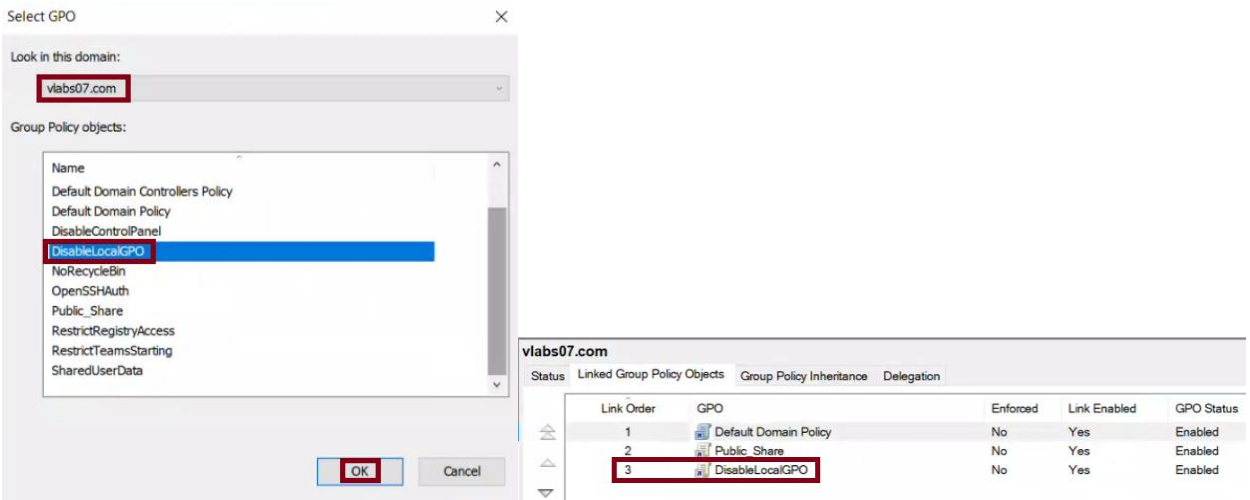


Right-click the new GPO → Edit
Navigate to:
Computer Configuration → Policies → Administrative Templates → System → Group Policy
Double-click: Turn off Local Group Policy objects processing
Set it to: Enabled → Click OK



Close the editor

Now link the new GPO:
In GPMC, right-click the domain name (vlabs07.com) → Link an Existing GPO
Select: DisableLocalGPO → Click OK



Step 6 - Open the Local Group Policy on Client07

Before starting, we need to make sure that Client07 receives the latest version of the domain policies.

To **do** this, log **in** to Client07 as Administrator and run the following command:

```
gpupdate /force
```

```
PS C:\Users\administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

This forces the client to refresh both Computer and User policies from the domain controller.

It ensures that any restored or modified GPOs are applied before we **compare** settings.

Once the update completes, proceed to check the local GPO.

Open Run → **type**: gpedit.msc → Enter

This opens the Local Group Policy Editor on the client machine.

Navigate to:

Computer **Configuration** → Windows Settings → Security Settings



This is **where** local security settings are configured when no domain-based GPOs are applied.

Step 7 - Compare Local GPO and Domain-Based GPOs

On DC107:

Open GPMC → Expand Group Policy Objects

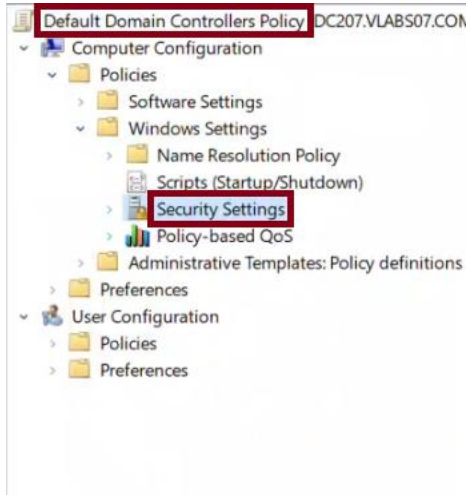
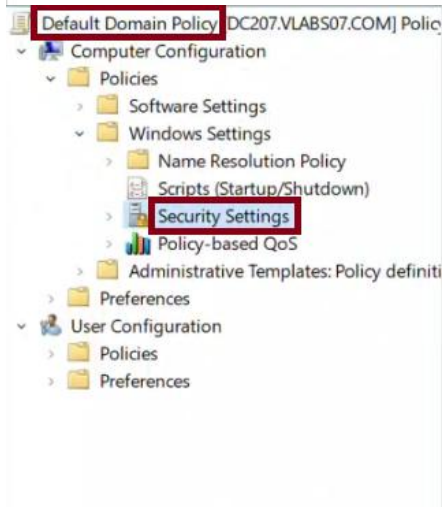
Right-click and Edit:

- Default Domain Policy
- Default Domain Controllers Policy

Go to:

Computer Configuration → Policies → Windows Settings → Security Settings

Review settings like Password Policy, Audit Policy, etc.

Default Domain Controllers Policy DC207.VLABS07.COM		Name	Description
		Account Policies	Password and account lockout policies
		Local Policies	Auditing, user rights and security options policies
		Event Log	Event Log
		Restricted Groups	Restricted Groups
		System Services	System service settings
		Registry	Registry security settings
		File System	File system security settings
		Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
		Windows Defender Firewall with Advance...	Windows Defender Firewall with Advanced Secu...
		Network List Manager Policies	Network name, icon and location group policies.
		Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Manag...
		Public Key Policies	
		Software Restriction Policies	
		Application Control Policies	Application Control Policies
		IP Security Policies on Active Directory (VL...	Internet Protocol Security (IPsec) Administration. ...
		Advanced Audit Policy Configuration	Advanced Audit Policy Configuration
		Account Policies	Password and account lockout policies
		Local Policies	Auditing, user rights and security options policies
		Event Log	Event Log
		Restricted Groups	Restricted Groups
		System Services	System service settings
		Registry	Registry security settings
		File System	File system security settings
		Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
		Windows Defender Firewall with Advance...	Windows Defender Firewall with Advanced Secu...
		Network List Manager Policies	Network name, icon and location group policies.
		Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Manag...
		Public Key Policies	
		Software Restriction Policies	
		Application Control Policies	Application Control Policies
		IP Security Policies on Active Directory (VL...	Internet Protocol Security (IPsec) Administration. ...
		Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

On Client07:
Open gpedit.msc again
Compare the same paths under Security Settings



By completing this task, we have explored how domain-based GPOs are restored and enforced over local settings.

We also learned how to simulate policy deletion and recovery using dcgpofix, and how GPMC gives us centralized control over policy application in the domain.

Task 2: GPO Storage and Replication

System: DC107 (GUI), DC207 (PowerShell)

Step 1 - What is GPO Storage and Replication?

When a Group Policy Object is created, it is stored in two places:

- In **Active Directory** (directory-based part, such as settings and links)
- In the **SYSVOL folder** (file-based part, such as scripts and templates)

This dual-storage model ensures that GPOs are both centrally managed and distributed to all domain controllers through **DFS Replication (DFSR)**.

In this task, we will:

- Verify the presence of GPOs in both SYSVOL and AD
- Use the GUI to examine storage locations
- Use PowerShell to confirm that replication between DC107 and DC207 is functioning properly

Step 2 - View Stored GPOs in SYSVOL

On DC107, we need to check the file-based storage of all Group Policy Objects.


Each GPO has a corresponding folder stored under SYSVOL in the Policies directory.

Press Win + R → type:

\\DC107\SYSVOL\vlabs07.com\Policies

Press Enter

This will show folders named by GUIDs, each representing a GPO object.



Name	Date modified	Type
(6AB24B7C-1912-40B9-A280-79D382114...	5/22/2025 2:39 PM	File folder
(6AC1786C-016F-11D2-945F-00C04FB98...	5/26/2025 6:30 PM	File folder
(31B2F340-016D-11D2-945F-00C04FB98...	5/26/2025 6:25 PM	File folder
(89BE2AFE-2475-435C-90EE-1AABAB7D...	5/25/2025 3:10 PM	File folder
(126AA8E6-B504-4C94-A308-45079D5D...	5/25/2025 11:37 PM	File folder
(499B0F2D-9282-46C2-967C-4B9A82226...	5/22/2025 12:44 PM	File folder
(B42BF684-3A72-4669-A3D1-353C089F7...	5/25/2025 10:43 PM	File folder
(CF4F0E80-AD35-49DB-AF05-03DA2E3F...	5/23/2025 8:16 PM	File folder
(E016FB9E-3833-4709-AD45-14A7E2A1F...	5/21/2025 5:02 PM	File folder
(EE83CB6F-D4F8-48FC-B0AC-02929E114...	5/26/2025 6:36 PM	File folder
(F052ABE1-472D-4151-B8C4-4EDDA7A5...	5/21/2025 9:18 PM	File folder
(FC0A3902-DDC4-4FB5-9DB8-C781C7AF...	5/25/2025 5:20 PM	File folder
PolicyDefinitions	5/23/2025 7:47 PM	File folder

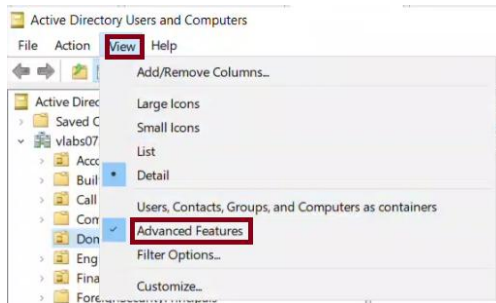
Step 3 - View the Policies Container in Active Directory

Open Active Directory Users and Computers on DC107

Start → Run → `dsa.msc` → Enter

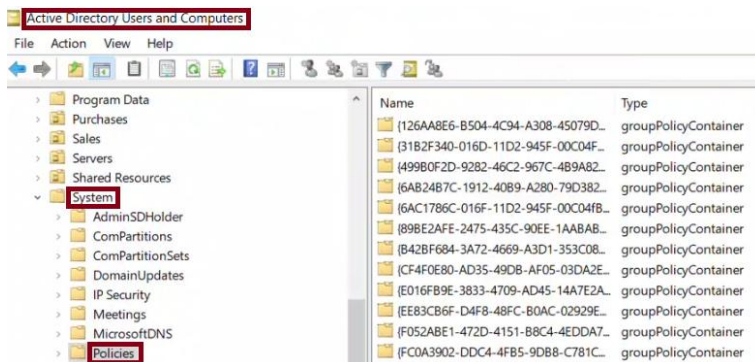
From the menu bar, click:

View → Advanced Features



In the left pane, navigate to:
vlabs07.com → System → Policies

This section shows the directory objects representing all GPOs, stored in Active Directory with attributes.



Step 4 - Verify DFSR Service is Running

On DC207 (Server Core), open PowerShell and verify that the DFS Replication service is active.

Run the following command:

Get-Service DFSR

```
PS C:\Users\Administrator.VLABS07> Get-Service DFSR
```

Status	Name	DisplayName
Running	DFSR	DFS Replication

The status should be "Running". This confirms that DFS is available to replicate GPO data.

Step 5 - Trigger DFS Replication Manually

The lab asked us to manually force DFS replication **using** PowerShell on DC207.

I first tried to use the following command:

```
dfsrdiag pollad
```

But I got the error:

```
"dfsrdiag is not recognized as the name of a cmdlet..."
```

This indicated that the tool was not installed.

I tried to install it **using**:

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

```
PS C:\Users\Administrator.VLABS07> Install-WindowsFeature RSAT-DFS-Mgmt-Con
Install-WindowsFeature : ArgumentNotValid: The role, role service, or feature name is not
valid: 'RSAT-DFS-Mgmt-Con'. The name was not found.
At line:1 char:1
+ Install-WindowsFeature RSAT-DFS-Mgmt-Con
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (RSAT-DFS-Mgmt-Con:String) [Install-WindowsFeat
ure], Exception
+ FullyQualifiedErrorId : NameDoesNotExist,Microsoft.Windows.ServerManager.Commands.AddWin
dowsFeatureCommand

Success Restart Needed Exit Code      Feature Result
-----
False    No                InvalidArgs      {}
```

That failed with:

```
"The role, role service, or feature name is not valid."
```

So I realized that Server Core does not support installing DFS Management Tools like this.

I also tried **using** the PowerShell command:

```
Update-DfsrConfigurationFromAD
```

```
PS C:\Users\Administrator.VLABS07> Update-DfsrConfigurationFromAD
Update-DfsrConfigurationFromAD : The term 'Update-DfsrConfigurationFromAD' is not recognized
as the name of a cmdlet, function, script file, or operable program. Check the spelling of the
name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Update-DfsrConfigurationFromAD
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Update-DfsrConfigurationFromAD:String) [], Comm
andNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

But that command was also not recognized on DC207.

To resolve the issue, I installed the DFS Replication feature itself **using**:

```
Install-WindowsFeature FS-DFS-Replication
```

```
PS C:\Users\Administrator.VLABS07> Install-WindowsFeature FS-DFS-Replication

Success Restart Needed Exit Code      Feature Result
-----
True     No                Success      {DFS Replication}
```


After the installation was successful, I retried the command:

```
dfsrdiag pollad
```

```
PS C:\Users\Administrator.VLABS07> dfsrdiag pollad  
Operation Succeeded
```

This time **it** worked and displayed:
"Operation Succeeded"

This confirms that DFS Replication is enabled and responding correctly on DC207, fulfilling the manual replication requirement **for** the lab.

Step 6 - Check DFS Replication Backlog

Still on DC207, I checked the DFS replication backlog to make sure everything was syncing correctly between DC107 and DC207.

I ran the following PowerShell commands:

```
Get-DfsrBacklog -SourceComputerName DC107 -DestinationComputerName DC207  
Get-DfsrBacklog -SourceComputerName DC207 -DestinationComputerName DC107
```

```
PS C:\Users\Administrator.VLABS07> Get-DfsrBacklog -SourceComputerName DC107 -DestinationComputerName DC207  
PS C:\Users\Administrator.VLABS07> Get-DfsrBacklog -SourceComputerName DC207 -DestinationComputerName DC107  
PS C:\Users\Administrator.VLABS07>
```

In both cases, the command returned no output. This is normal when replication is healthy and there are no files waiting to sync.

To test further, I created a new test GPO and added a test file to the SYSVOL scripts folder on DC107:

```
echo "trigger" > \\DC107\SYSVOL\vlabs07.com\scripts\trigger1.txt
```

Even after these changes, DFSR backlog still returned no results. This suggests that replication is happening very quickly and there is no delay, which confirms that DFSR is functioning as expected **in** this lab.

To further validate SYSVOL health, I also ran the following command on both DC107 and DC207:

```
dcdiag /test:frssysvol
```

```
PS C:\Users\Administrator.VLABS07> dcdiag /test:frssysvol
```

In both cases, the output confirmed that each domain controller passed the FrsSysVol test.

This means SYSVOL is correctly shared and functioning on both systems, reinforcing that DFS Replication is healthy and fully operational.

Task 3: Group Policy Troubleshooting

System: DC107 (GUI and PowerShell)

Step 1 - What are Common GPO Management Tasks?

Group Policy Objects (GPOs) are central to managing domain-based configurations in Active Directory. Over time, GPOs may need to be backed up, restored, duplicated, or have settings imported from others. This task demonstrates how to perform essential GPO operations using both the GUI and PowerShell.

Backing up GPOs protects existing configurations before major changes. Importing or copying GPOs helps administrators replicate tested policies or apply templates to new GPOs. These skills are critical for version control, disaster recovery, and maintaining consistency in enterprise environments.

Step 2 - Backup All Existing GPOs (GUI)

Before backing up, create a folder to store GPO backups:

Navigate to C:\
Right-click → New → Folder
Name the folder: GPO_Backups

Alternatively, open PowerShell and run:

```
New-Item -Path "C:\GPO_Backups" -ItemType Directory
```

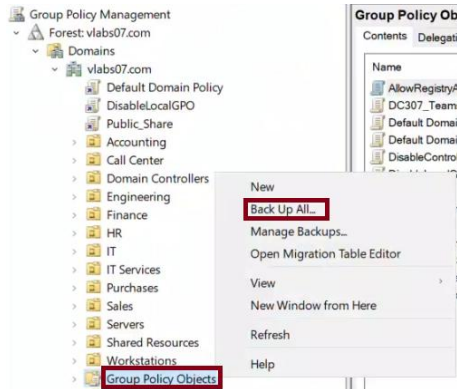
```
PS C:\Users\Administrator> New-Item -Path "C:\GPO_Backups" -ItemType Directory

Directory: C:\

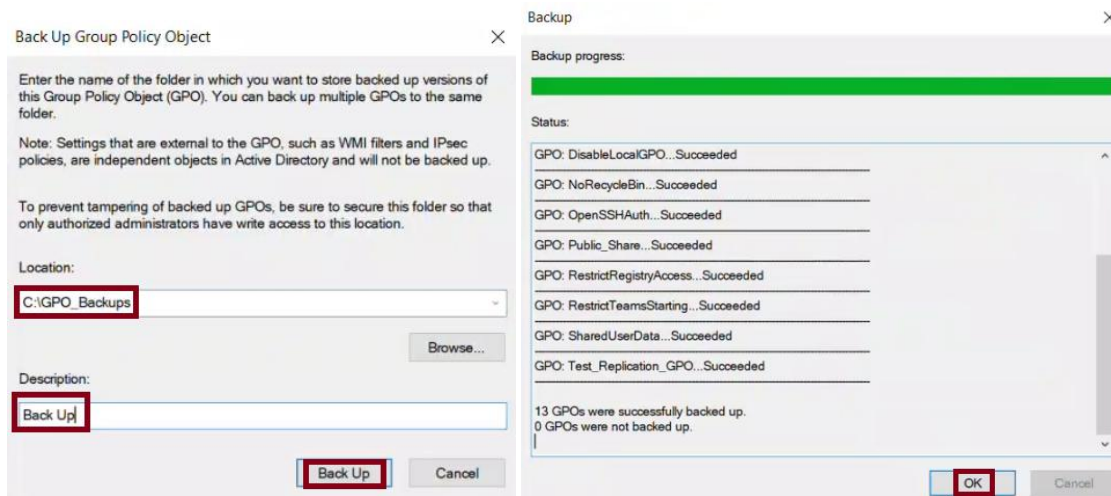
Mode                LastWriteTime         Length Name
----                -
d-----          5/26/2025  11:17 PM              GPO_Backups
```

Then Open **Group Policy Management** on DC107:
Tools → **Group Policy Management**

Right-click on the ****Group Policy Objects**** container → Click ****Back Up All...****



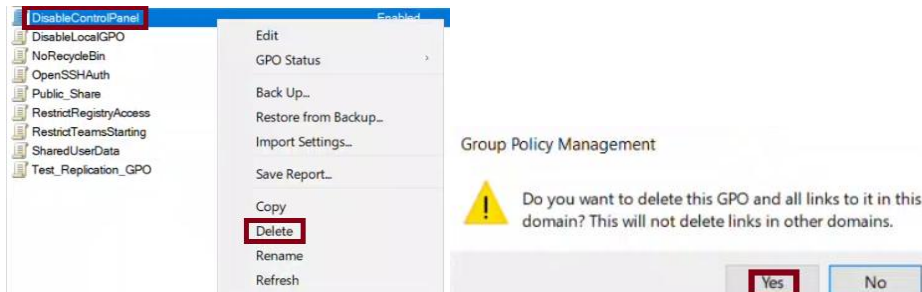
Set the backup folder path to: `C:\GPO_Backups`
Add an optional description and click ****Back Up****

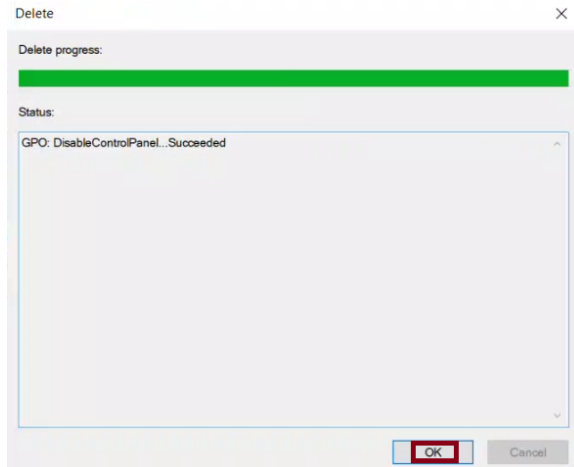


Once completed, confirm that all GPOs are backed up.

Step 3 - Delete a GPO and Restore It (GUI)

Right-click any existing GPO (e.g., `DisableControlPanel`) → Click ****Delete****
→ Confirm deletion

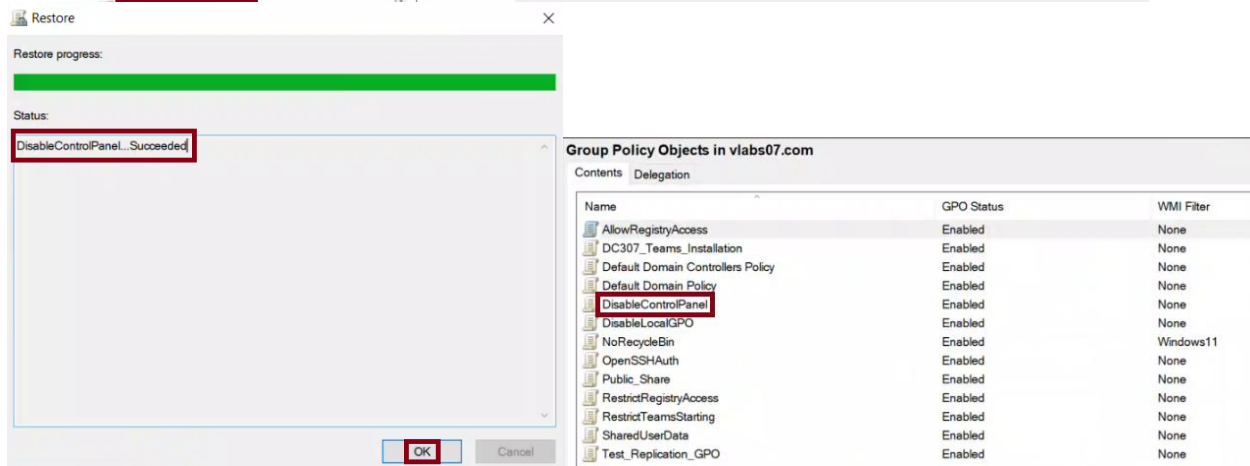
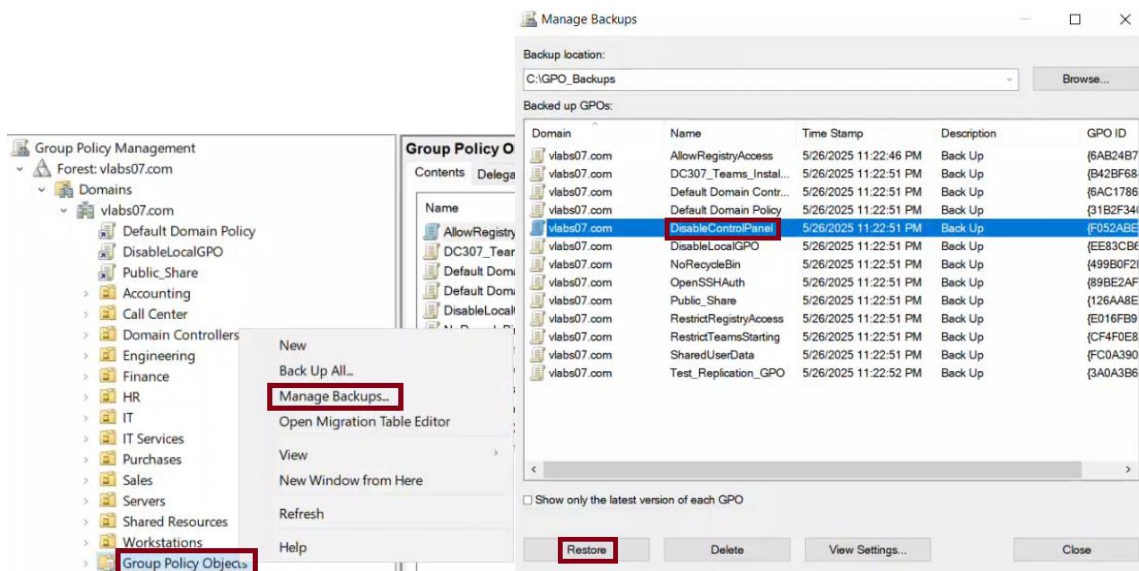




Then go to:

Group Policy Objects → Right-click → ****Manage Backups****

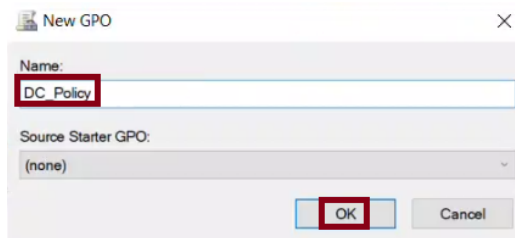
Browse to: `C:\GPO_Backups` → **Select** the deleted GPO → Click ****Restore****



Confirm the GPO is restored **in** the Group Policy Objects list.

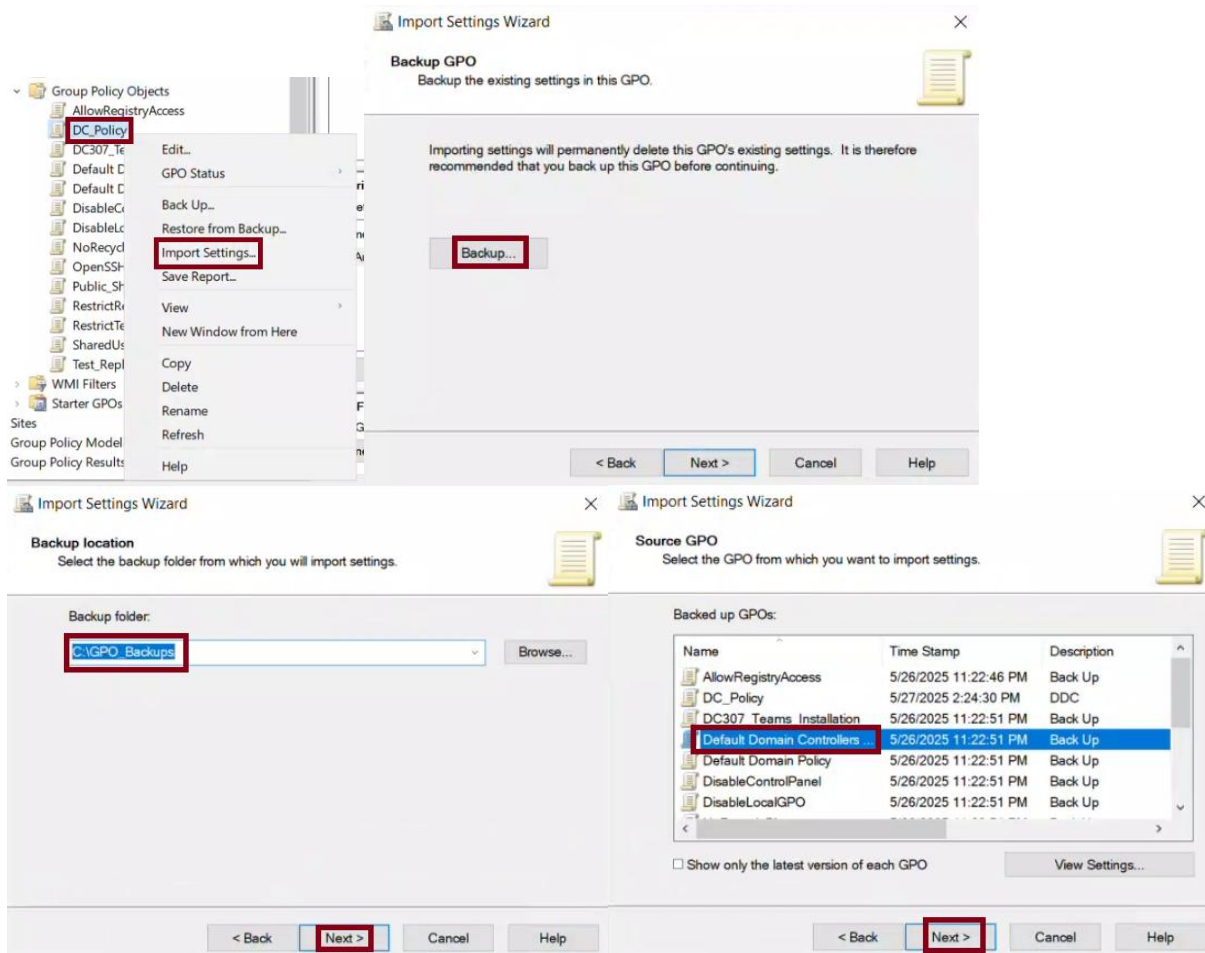
Step 4 - Create New GPO Named DC_Policy (GUI)

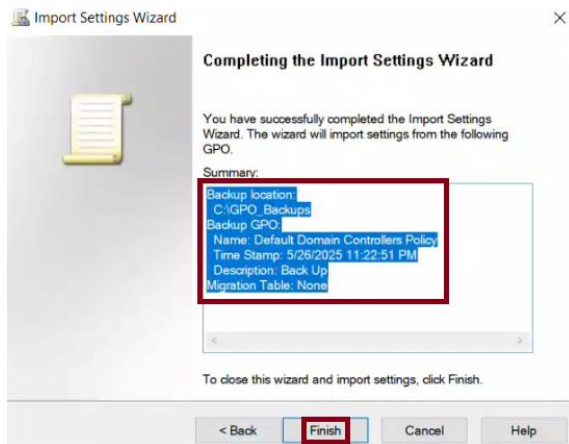
Right-click **Group Policy Objects** → Click ****New****
Name the new GPO: `DC_Policy` → Click OK



Step 5 - Import Settings from Default Domain Controllers Policy into DC_Policy (GUI)

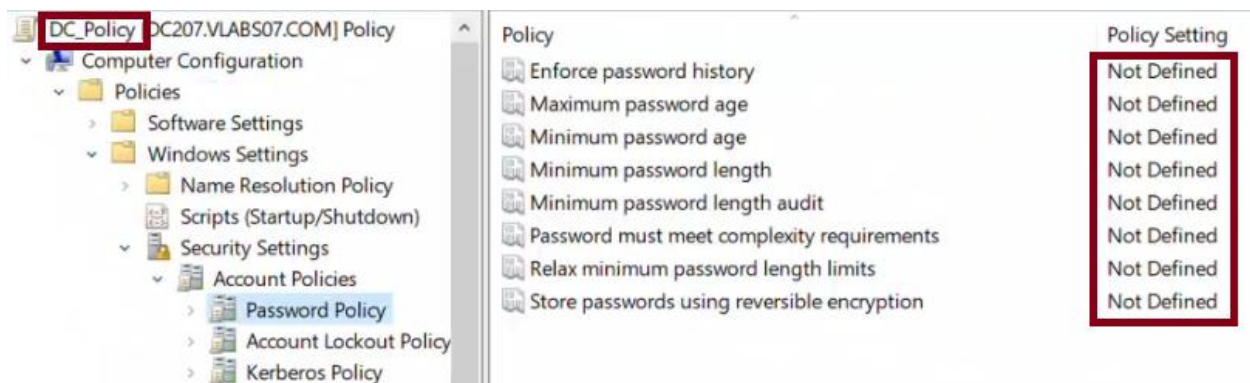
Right-click `DC_Policy` → Click ****Import Settings****
Click Next → Choose "Import from a backup"
Browse to `C:\GPO_Backups` → **Select** the backup of ****Default Domain Controllers Policy****
Follow the wizard to complete the import





Step 6 - Verify Imported Settings in DC_Policy (GUI)

1. Open Group Policy Management Console (GPMC)
2. Under 'Group Policy Objects', right-click 'DC_Policy' → Click 'Edit'
3. In Group Policy Management Editor, navigate to:
Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy
4. Review the settings.
Since the 'Default Domain Controllers Policy' was restored to its default state in Task 1,
no password policies or other configurations will be defined in DC_Policy.



Lab Report Note:

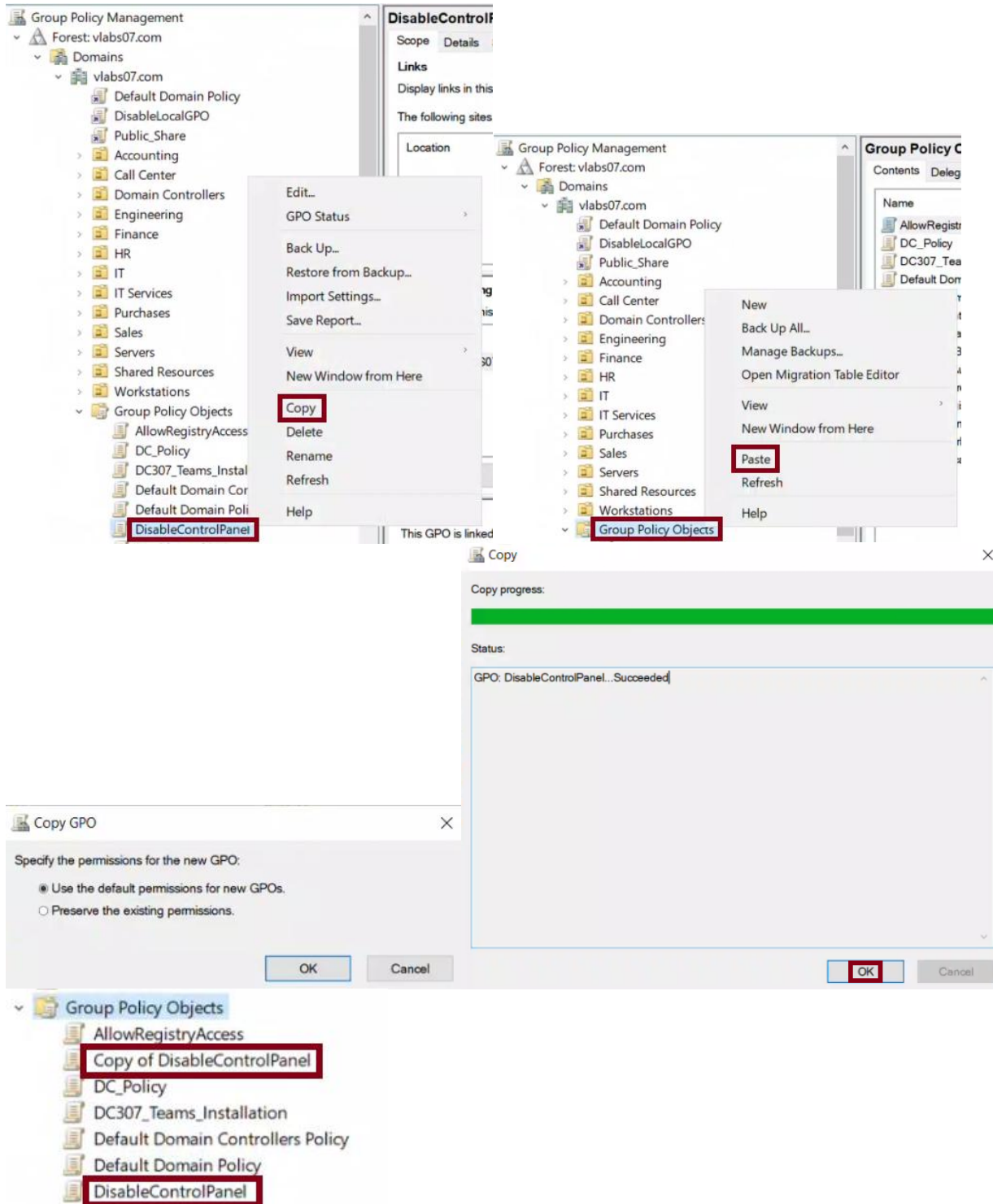
"This screenshot shows the Password Policy section of the DC_Policy GPO. As expected, the settings are undefined because the source GPO was reset in Task 1. This confirms the import succeeded, and DC_Policy now reflects the source GPO's current state."

Step 7 - Copy an Existing GPO to a New One (GUI)

Right-click a GPO such as `DisableControlPanel` → Click ****Copy****

Right-click **in** Group Policy Objects → ****Paste****

Name the new GPO something like `DisableControlPanel_Copy`

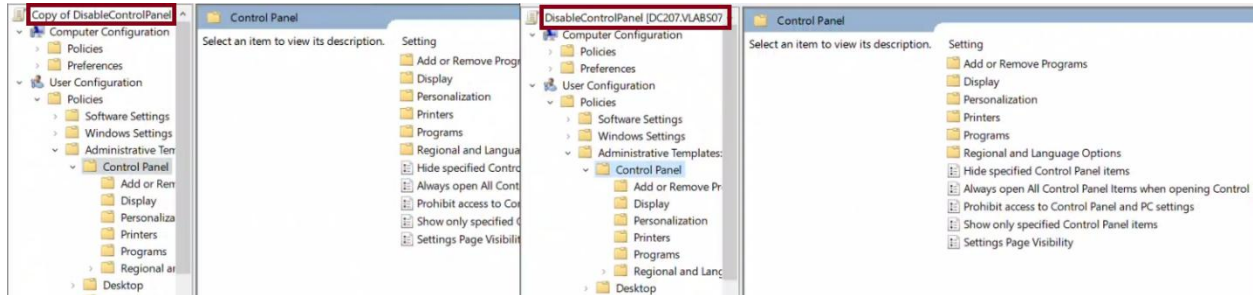


Step 8 - Verify Settings in the Copied GPO (GUI)

Right-click the copied GPO → Click ****Edit****

Open the same setting as the original (e.g., User Configuration → Policies → Admin Templates → Control Panel)

Confirm the setting is identical



Step 9 - Perform the Same Tasks Using PowerShell (DC107)

Open PowerShell as Administrator on DC107

1. Backup all GPOs:

Backup-GPO -All -Path "C:\GPO_Backups"

```
PS C:\Users\Administrator> Backup-GPO -All -Path "C:\GPO_Backups"

DisplayName : Public_Share
GpoId       : 126aa8e6-b504-4c94-a308-45079d5d9d53
Id          : 7e176c5f-bfd8-4c0d-b975-87d916506d42
BackupDirectory : C:\GPO_Backups
CreationTime  : 5/27/2025 3:39:15 PM
DomainName   : vlabs07.com
Comment      :

DisplayName : Default Domain Policy
GpoId       : 31b2f340-016d-11d2-945f-00c04fb984f9
Id          : b6a79574-97ef-49db-8bed-15c059a56513
BackupDirectory : C:\GPO_Backups
CreationTime  : 5/27/2025 3:39:15 PM
DomainName   : vlabs07.com
Comment      :

DisplayName : Test_Replication_GPO
GpoId       : 3a0a3b62-fdc8-457b-9484-7c81ab8b9411
```

2. Delete a GPO:

Remove-GPO -Name "DisableControlPanel"

```
PS C:\Users\Administrator> Remove-GPO -Name "DisableControlPanel"
```

3. Restore the deleted GPO using its BackupId:

```
Restore-GPO -BackupId "85ead705-bfb7-42b1-9132-3330ad5077ba" -Path "C:\GPO_Backups"
```

```
PS C:\Users\Administrator> Restore-GPO -BackupId "85ead705-bfb7-42b1-9132-3330ad5077ba" -Path "C:\GPO_Backups"

DisplayName      : DisableControlPanel
DomainName       : vlabs07.com
Owner            :
Id               : f052abe1-472d-4151-b8c4-4edda7a5562b
GpoStatus        : AllSettingsEnabled
Description       : GPO to restrict access to Control Panel
CreationTime     : 5/27/2025 6:58:10 PM
ModificationTime : 5/27/2025 6:58:10 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

4. Create a new GPO:

```
New-GPO -Name "DC_Policy_PS"
```

```
PS C:\Users\Administrator> New-GPO -Name "DC_Policy_PS"

DisplayName      : DC_Policy_PS
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : 84ca9dcd-2941-4cbb-a129-c33861c42d5c
GpoStatus        : AllSettingsEnabled
Description       :
CreationTime     : 5/27/2025 7:20:52 PM
ModificationTime : 5/27/2025 7:20:52 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :
```

5. Import settings from Default Domain Controllers Policy:

```
Import-GPO -BackupGpoName "Default Domain Controllers Policy" -TargetName "DC_Policy_PS" -Path "C:\GPO_Backups"
```

```
PS C:\Users\Administrator> Import-GPO -BackupGpoName "Default Domain Controllers Policy" -TargetName "DC_Policy_PS" -Path "C:\GPO_Backups"

DisplayName      : DC_Policy_PS
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : 84ca9dcd-2941-4cbb-a129-c33861c42d5c
GpoStatus        : AllSettingsEnabled
Description       :
CreationTime     : 5/27/2025 7:20:52 PM
ModificationTime : 5/27/2025 7:24:47 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

6. Copy an existing GPO:

Copy-GPO -SourceName "Public_Share" -TargetName "Public_Share_Copy"

```
PS C:\Users\Administrator> Copy-GPO -SourceName "Public_Share" -TargetName "Public_Share_Copy"
```

```
DisplayName      : Public_Share_Copy
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : 05014432-565c-494f-8ce6-d0539cad3275
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 5/27/2025 7:35:06 PM
ModificationTime : 5/27/2025 7:35:06 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

7. List all GPOs to confirm:

Get-GPO -All

```
PS C:\Users\Administrator> Get-GPO -All
```

```
DisplayName      : Public_Share_Copy
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : 05014432-565c-494f-8ce6-d0539cad3275
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 5/27/2025 7:35:06 PM
ModificationTime : 5/27/2025 7:35:06 PM
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : Public_Share
DomainName       : vlabs07.com
Owner            : VLABS07\Domain Admins
Id               : 126aa8e6-b504-4c94-a308-45079d5d9d53
GpoStatus        : AllSettingsEnabled
Description      :
```

Task 4: Group Policy Modeling and Results

System: DC107 (GUI)

Step 1 - What Are Group Policy Modeling and Results?

Group Policy Modeling and Group Policy Results are tools in the Group Policy Management Console (GPMC) used for planning and troubleshooting GPO application.

- **Group Policy Modeling** is a simulation tool. It predicts which GPOs would apply to a user or computer based on domain structure, GPO links, inheritance, security filtering, and WMI filters. It does not require real execution on the target machine.
- **Group Policy Results** is a reporting tool that shows which GPOs were actually applied during the last logon or startup. It collects live data from the target system and includes applied and denied GPOs.

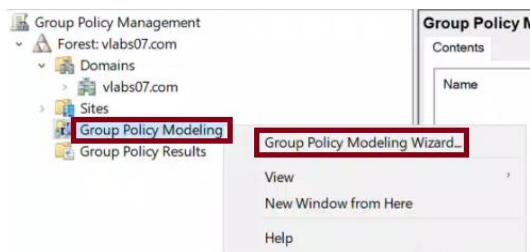
These tools are critical for validating policy design and resolving issues related to GPO application.

In this task, we will:

- Simulate the effective policies for a user in the HR OU using Group Policy Modeling
- Analyze the actual applied policies on DC107 using Group Policy Results

Step 2 - Simulate GPO Application Using Group Policy Modeling (GUI)

1. Open the Group Policy Management Console (GPMC) on DC107
2. In the left pane, right-click **Group Policy Modeling** → Click **Group Policy Modeling Wizard**



3. Choose the domain (vlabs07.com) and domain controller (DC107) → Click ****Next****

The screenshot shows the 'Domain Controller Selection' step of the Group Policy Modeling Wizard. The domain 'vlabs07.com' is selected in the 'Show domain controllers in this domain:' dropdown. Under 'Process the simulation on this domain controller:', the radio button for 'This domain controller' is selected. A table lists two domain controllers: 'DC107.vlabs07.com' and 'DC207.vlabs07.com', both located in the 'Montreal' site. The 'DC107.vlabs07.com' entry is highlighted. At the bottom, the 'Next >' button is highlighted.

Name	Site
DC107.vlabs07.com	Montreal
DC207.vlabs07.com	Montreal

4. For the ****User information****, select the ****Container**** option
→ Click ****Browse**** and choose the ****HR OU**** (e.g.,
OU=HR,DC=vlabs07,DC=com)

5. For the ****Computer information****, also select the ****Container**** option
→ Click ****Browse**** and select the ****same HR OU****

The screenshot shows the 'User and Computer Selection' step of the Group Policy Modeling Wizard. It displays example container names and user/computer names. Under 'Simulate policy settings for the following:', both 'User information' and 'Computer information' have the 'Container' radio button selected. The text 'OU=HR,DC=vlabs07,DC=com' is entered in both text boxes. To the right, a list of 'Security groups' shows 'Authenticated Users' and 'Everyone', with 'Authenticated Users' selected. At the bottom, the 'Next >' button is highlighted.

6. Proceed through the rest of the wizard, keeping default options
→ Click ****Next**** on each screen, then click ****Finish****

The wizard will simulate GPO application based on both the user and computer being located **in** the HR OU. The report will show which GPOs would be applied, their precedence, and filtering behavior.

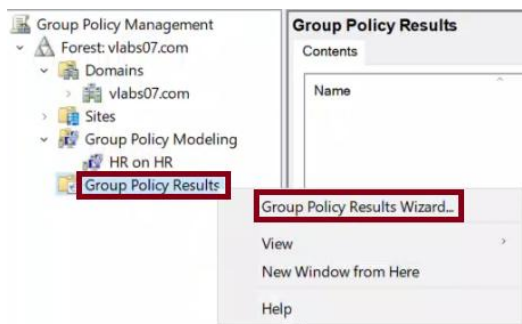
HR on HR	
Summary	Details Query
Group Policy Modeling	
vlabs07.com/HR on vlabs07.com/HR	
Data collected on: 5/27/2025 8:11:01 PM	
show all	
Summary	
hide	
During last computer policy refresh on 5/27/2025 8:10:32 PM	
A fast link was detected More information...	
During last user policy refresh on 5/27/2025 8:10:32 PM	
A fast link was detected More information...	
Computer Details	
hide	
General	
hide	
Computer container	vlabs07.com/HR
Domain	vlabs07.com
Site	(None)
Slowlink processing	No
Component Status	
hide	
Component Name	Status
Group Policy Infrastructure	Success
Activate Windows	

Lab Report Note:

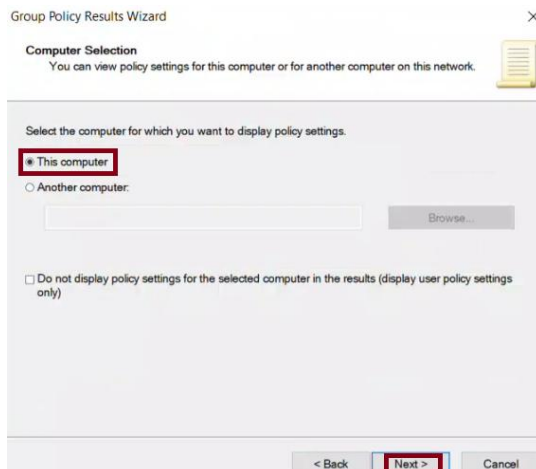
"This modeling simulation predicts which GPOs would apply when both the user and the computer are located in the HR OU. This configuration reflects the typical OU design seen in enterprise environments and helps validate the effects of OU-level GPO links and inheritance."

Step 3 - Analyze Applied GPOs Using Group Policy Results (GUI)

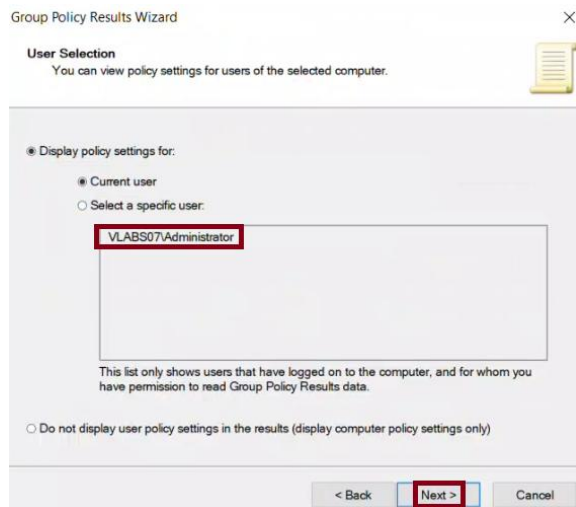
1. In GPMC, right-click **Group Policy Results** → Click **Group Policy Results Wizard**



2. Select the computer: **DC107**



3. Select the user: **Administrator**



Group Policy Results Wizard

User Selection
You can view policy settings for users of the selected computer.

Display policy settings for:

- ☒ Current user
- ☐ Select a specific user:
VLABS07\Administrator

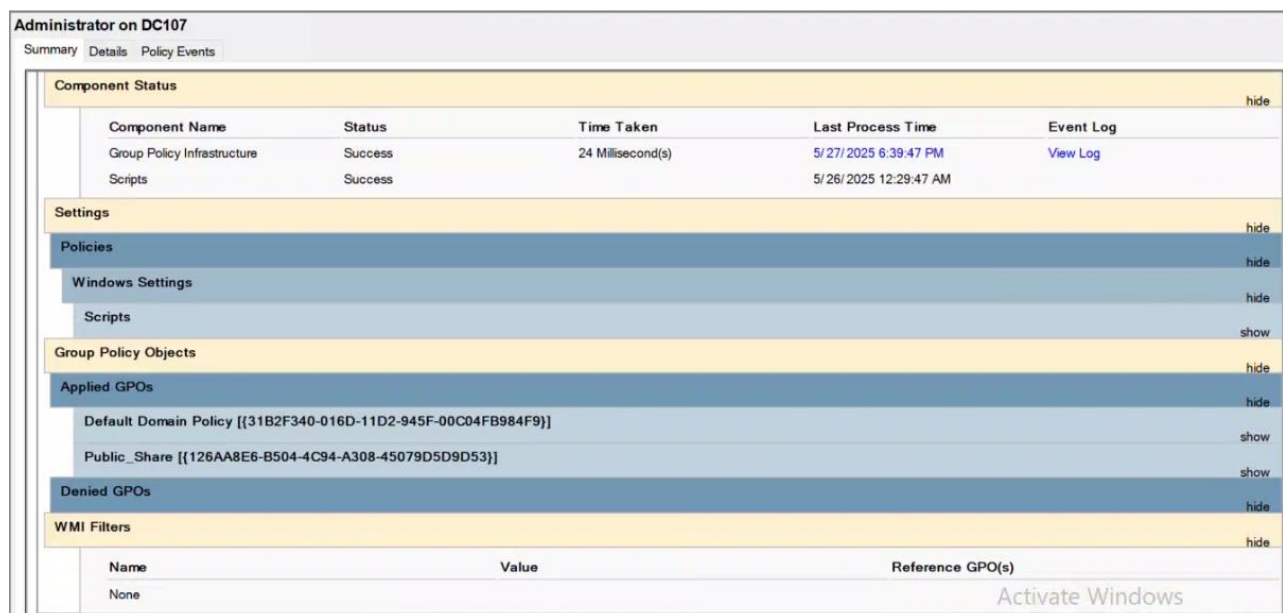
This list only shows users that have logged on to the computer, and for whom you have permission to read Group Policy Results data.

☐ Do not display user policy settings in the results (display computer policy settings only)

< Back Next > Cancel

4. Click **Next**, then **Finish**

The wizard will connect to the system and generate a Group Policy Results report.



Administrator on DC107

Summary Details Policy Events

Component Status					hide
Component Name	Status	Time Taken	Last Process Time	Event Log	
Group Policy Infrastructure	Success	24 Millisecond(s)	5/27/2025 6:39:47 PM	View Log	
Scripts	Success		5/26/2025 12:29:47 AM		
Settings					hide
Policies					hide
Windows Settings					hide
Scripts					show
Group Policy Objects					hide
Applied GPOs					hide
Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]					show
Public_Share [{126AA8E6-B504-4C94-A308-45079D5D9D53}]					show
Denied GPOs					hide
WMI Filters					hide
Name	Value	Reference GPO(s)			
None					

Activate Windows

This report shows:

- All applied GPOs (with precedence)
- GPOs that were denied and why
- User and computer policy settings

Lab Report Note:

"This report shows which GPOs actually applied to DC107 and the Administrator account during the last logon. It's valuable for confirming that domain policies were enforced and troubleshooting any that were blocked."

Task 5: Delegating GPO Management

System: DC107 (GUI)

Step 1 - What Is GPO Delegation and Why Do We Use It?

In enterprise environments, delegating GPO management allows you to assign GPO-related responsibilities to specific users or groups without granting full domain admin rights. This improves security and administrative efficiency.

In this task, we will:

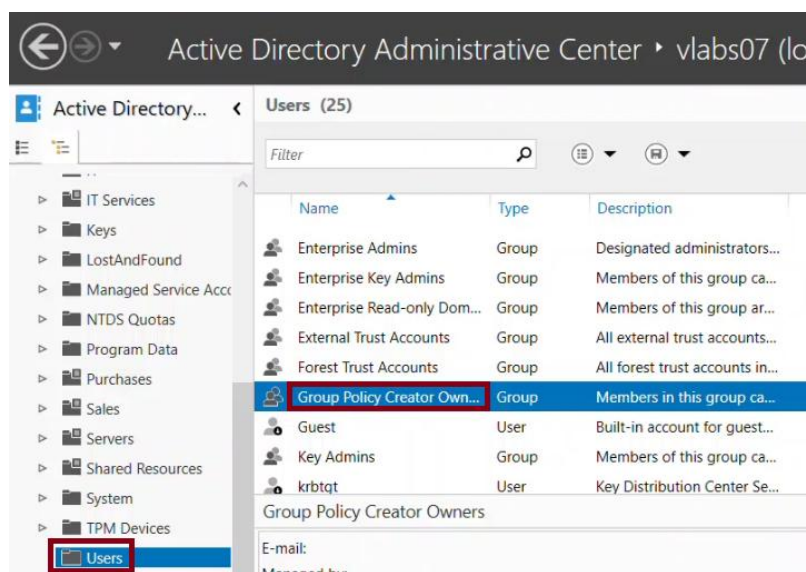
- Grant Lina Gaillard the ability to create new GPOs
- Allow her to edit existing GPOs
- Give her permission to link GPOs to the Finance OU

We will follow the exact method shown in the instructor's course slides using the **Group Policy Management Console (GPMC)**.

Step 2 - Grant Lina Gaillard the Right to Create GPOs

By default, only Domain Admins, Enterprise Admins, and members of the **Group Policy Creator Owners** group can create new GPOs. To delegate this right:

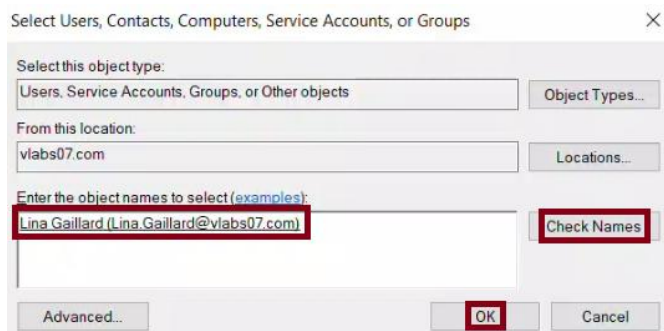
1. On DC107, open **Server Manager** → Click **Tools** → Select **Active Directory Administrative Center**
2. In the left pane, click your domain (e.g., `vlabs07.com`)
3. In the center pane, double-click the **Users** container
4. Scroll to find and double-click **Group Policy Creator Owners**



5. Click the **Members** section → Then click **Add**



6. Enter `Lina Gaillard` → Click **OK**

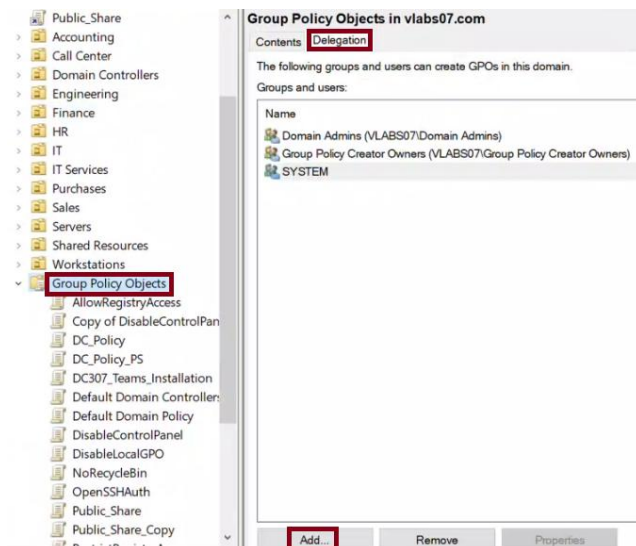


This adds Lina to the **group**, giving her permission to create GPOs **in** the domain.

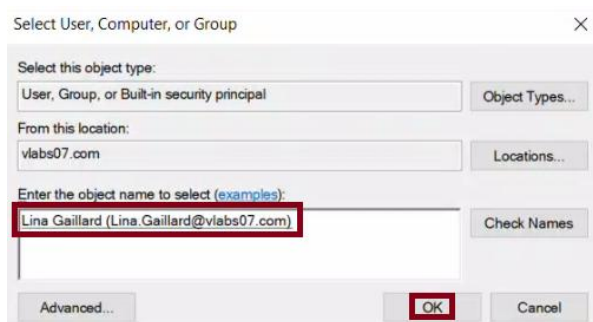
Step 3 - Explicitly Delegate GPO Management Rights

We will now give Lina explicit permissions to manage (edit and delete) any GPO **in** the domain.

1. Open **Group Policy Management Console**
2. **In** the left pane, select **Group Policy Objects**
3. **In** the right pane, go to the **Delegation** tab



4. Click ****Add**** → Enter: `Lina Gaillard` → Click ****OK****



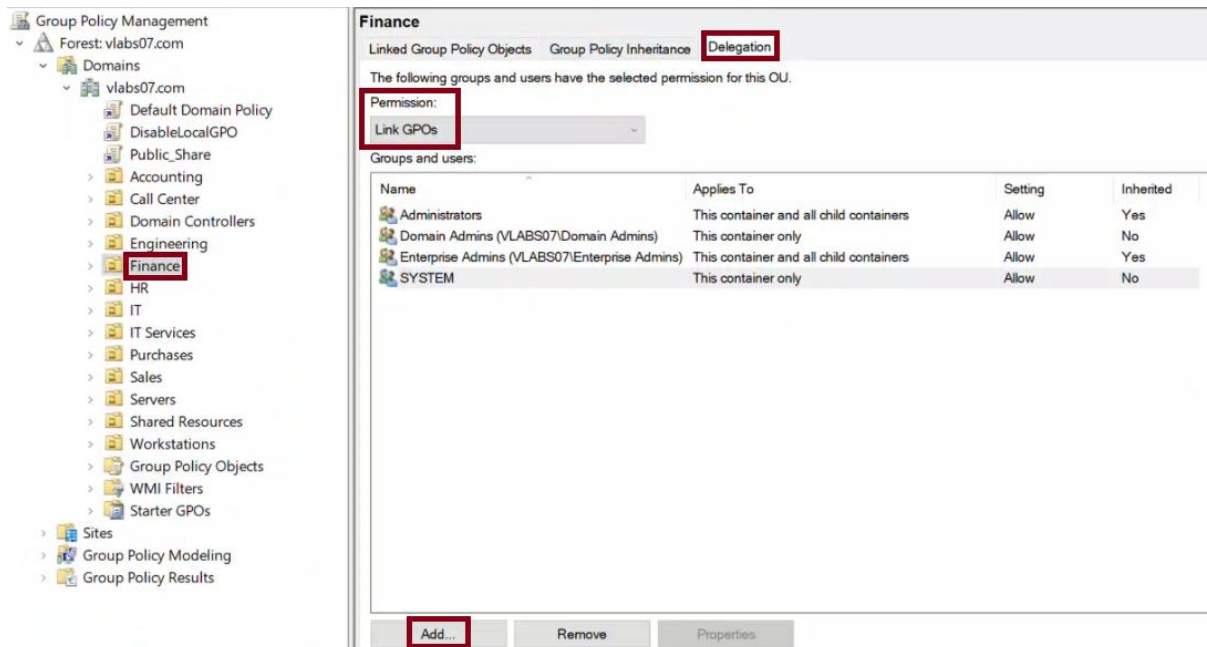
Lina will now appear **in** the list of users with permission to create and manage GPOs.



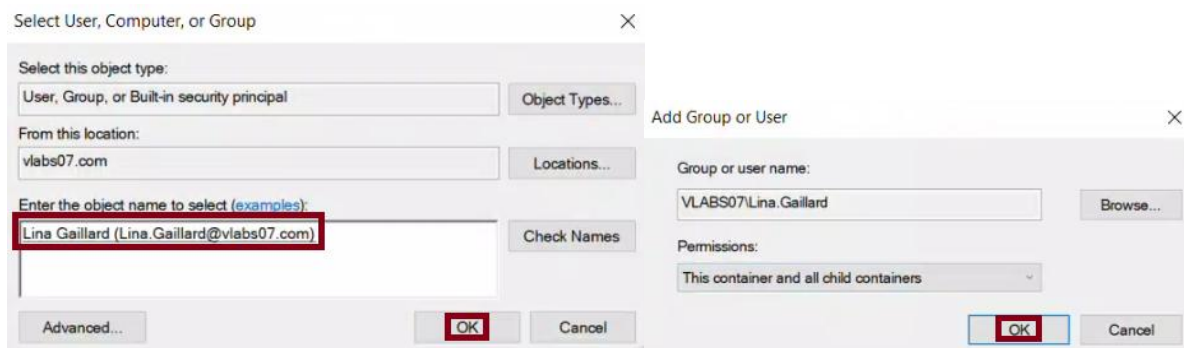
Step 4 - Delegate GPO Linking to the Finance OU

To allow Lina to link GPOs to the Finance OU:

1. In ****Group Policy Management Console****, click on the ****Finance OU****
2. In the right pane, **switch** to the ****Delegation**** tab
3. At the top, **select**Permission: Link GPOs****



4. Click ****Add**** → Type: `Lina Gaillard` → Click ****OK****



Lina Gaillard is being delegated GPO linking rights on the Finance OU. The scope "This container and all child containers" ensures her permission applies to both the Finance OU and any sub-OU's beneath it.

Lab Report Note:

"This task demonstrates how to delegate GPO creation, linking, and editing rights. Lina Gaillard was added to the Group Policy Creator Owners group, explicitly granted permission to manage all GPOs, and authorized to link GPOs to the Finance OU. These steps enable secure, delegated administration for departmental policy management."

Step 5 - PowerShell Verification of Delegated Rights

Confirm Lina Gaillard is a member of the "Group Policy Creator Owners" group. This confirms she has permission to create new GPOs in the domain.

```
PS C:\Users\Administrator> Get-ADGroupMember "Group Policy Creator Owners" | Where-Object { $_.SamAccountName -eq "Lina.Gaillard" }

distinguishedName : CN=Lina Gaillard,OU=IT,DC=vlabs07,DC=com
name               : Lina Gaillard
objectClass        : user
objectGUID         : 0d53d5ea-8b37-49a1-b2d5-0b85191ae0d6
SamAccountName     : Lina.Gaillard
SID                : S-1-5-21-2428485534-1961598418-1246186656-1238
```

Output shows:

- SamAccountName: Lina.Gaillard
- DistinguishedName: CN=Lina Gaillard,OU=IT,DC=vlabs07,DC=com
- Group: Group Policy Creator Owners

Her inclusion in this group validates the delegation of GPO creation rights, fulfilling Task 5 - Step 2 of the lab instructions.

****Bonus Step: Powershell Confirmation of OU Level-Permissions****

```
PS C:\Users\Administrator> (Get-ACL "AD:OU=Finance,DC=vlabs07,DC=com").Access | Where-Object { $_.IdentityReference -like "*Lina.Gaillard*" }
```