This lab is designed to configure and test advanced Group Policy Objects (GPOs) in a domain environment.

Lab Assignment 2 (Part II) - GPO

420-636-AB-Network Installation and Administration II

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

Table of Contents

Lab Assignment 2 (Part II) - GPO

1 Lab Objective

This lab is designed to **configure and test advanced Group Policy Objects (GPOs)** in a domain environment. Students will work with Administrative Templates, security policies, folder redirection, software installation, and scripts.

The lab will focus on implementing these configurations, linking them to appropriate OUs, and verifying their impact.

2 Lab Environment Requirements

- **DC101**: Domain Controller with Active Directory, DNS, and Group Policy Management installed.
- **Client1**: Windows 11 client machine joined the domain.
- **DC301**: File Server for folder sharing.

3 Task 1: Creating a Central Store for Administrative Templates

3.1 Objective

Create a centralized ADMX/ADML repository for vlabs1.com domain to ensure consistent Group Policy administration.

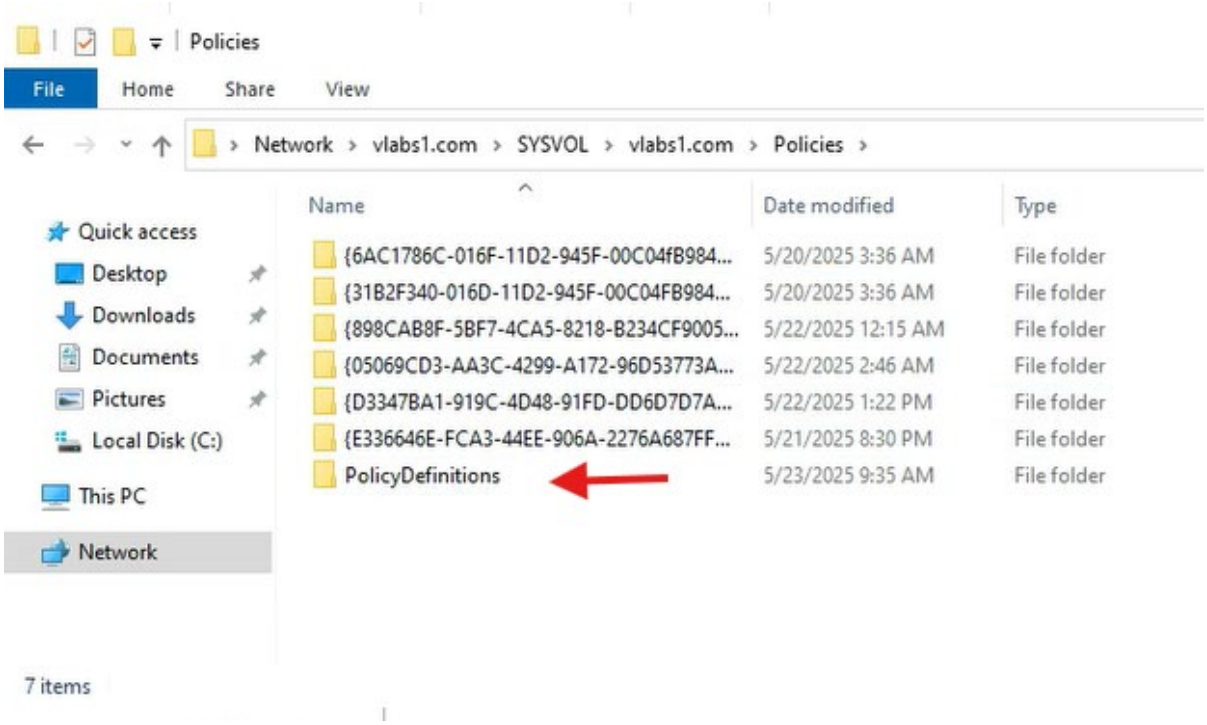
3.2 Steps

- Create a **central store** for Administrative Templates on **DC101**.
- Copy all **ADMX** and **ADML** files to this Central store.
- Verify that **Group Policy Management Console (GPMC)** loads templates from the **central store.**

3.2.1 DC101

Create the Central Store Directory

1. **On DC101 (Domain Controller):**
    - Open **File Explorer** and navigate to:\\vlabs1.com\SYSVOL\vlabs1.com\Policies
    - **Right-click → New → Folder**
      Name it: **"PolicyDefinitions"**
      (This becomes your Central Store)



2. **Copy ADMX/ADML Files**

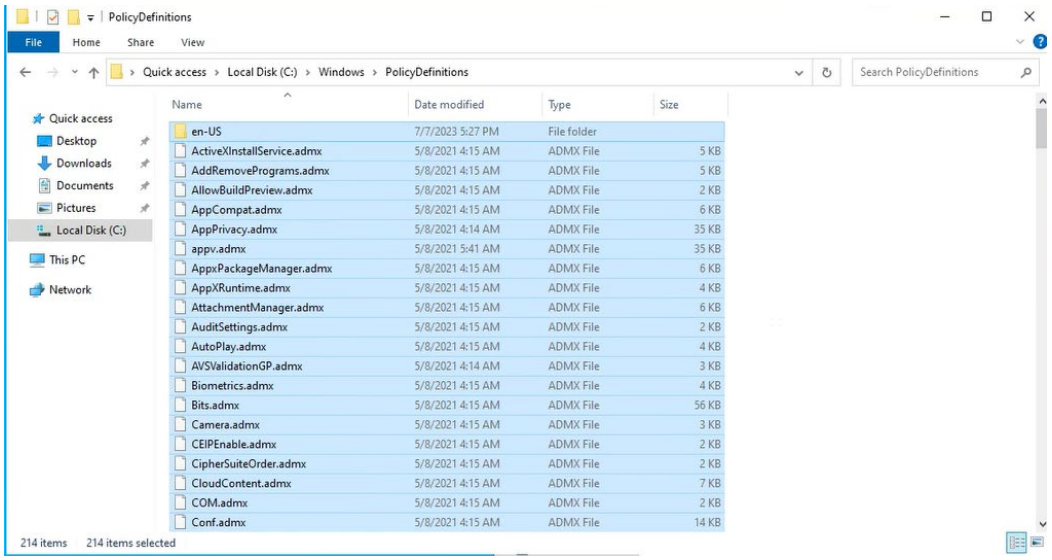
a) **On DC101, open:** C:\Windows\PolicyDefinitions

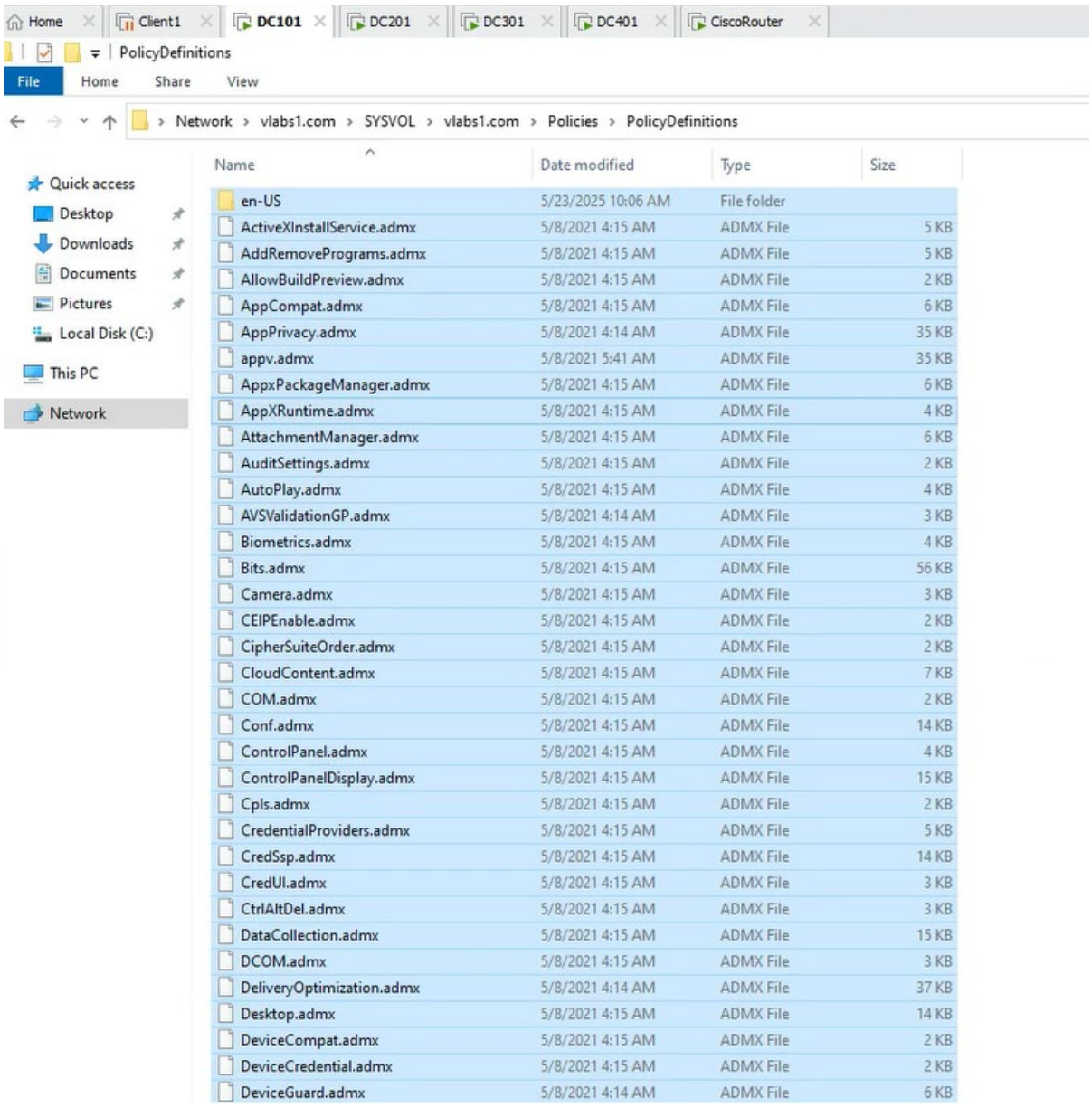
b) **Select all files:**

- **ADMX files** (e.g., WindowsDefender.admx)
- **ADML folders** (e.g., en-US for English)

c) **Copy to:** \\vlabs1.com\SYSVOL\vlabs1.com\Policies\PolicyDefinitions

(Include all language folders you need)





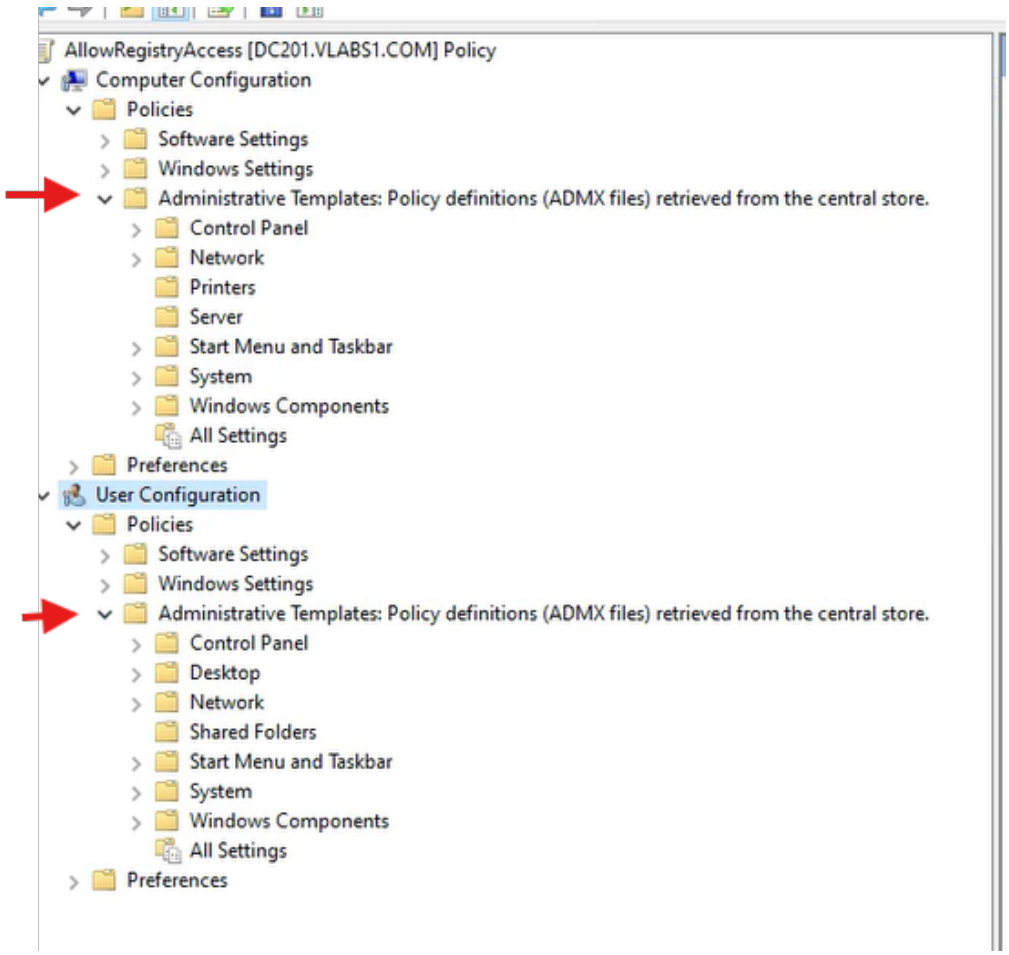
3. **Verify Central Store**

a) **On DC101:**

- Open **GPMC** (gpmc.msc)
- Edit any GPO → Navigate to:
  Computer Configuration → Policies → Administrative Templates

b) **Confirmation:**

- No warning about "local ADMX files" appears
- Right-click "Administrative Templates" → **View** → Verify:
  "PolicyDefinitions (ADMX files) retrieved from the Central Store"



Item	Path
Source ADMX Files	C:\Windows\PolicyDefinitions
Central Store	\\vlabs1.com\SYSVOL\vlabs1.com\Policies\PolicyDefinitions
Language Files	PolicyDefinitions\en-US (or other language codes)

4 Task 2: Managing and Configuring Administrative Templates

4.1 Objective

Configure Office Administrative Templates to restrict Microsoft Teams auto-start behavior for Engineering OU users.

4.2 Steps

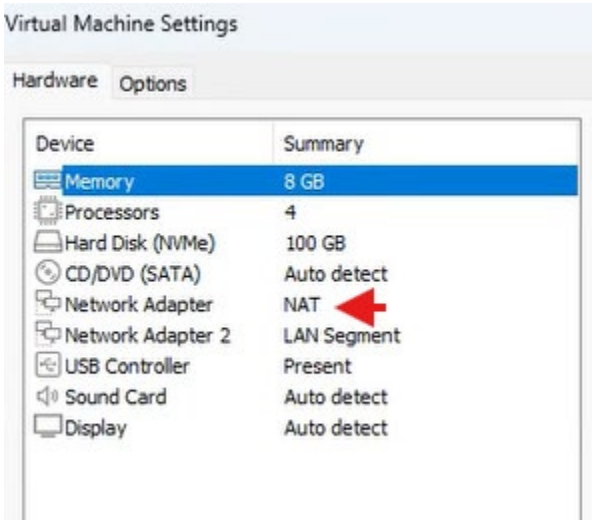
- Download and install **Microsoft Office Administrative** Templates *(You will need to **add the NAT NIC** to download this package. Remove it after completing the download).*
- Create a new GPO named **RestrictTeamsStarting.**
- Use **Filter Options** for **User Configuration** to locate **Microsoft Teams settings.**
- Enable Prevent Microsoft Teams from starting automatically after installation.
- Add a **comment** to document this setting.
- Link to **Engineering** OU *(to be tested in **Task 8 Managing Software Installation** task).*
- Run **gpupdate /force** to apply changes.

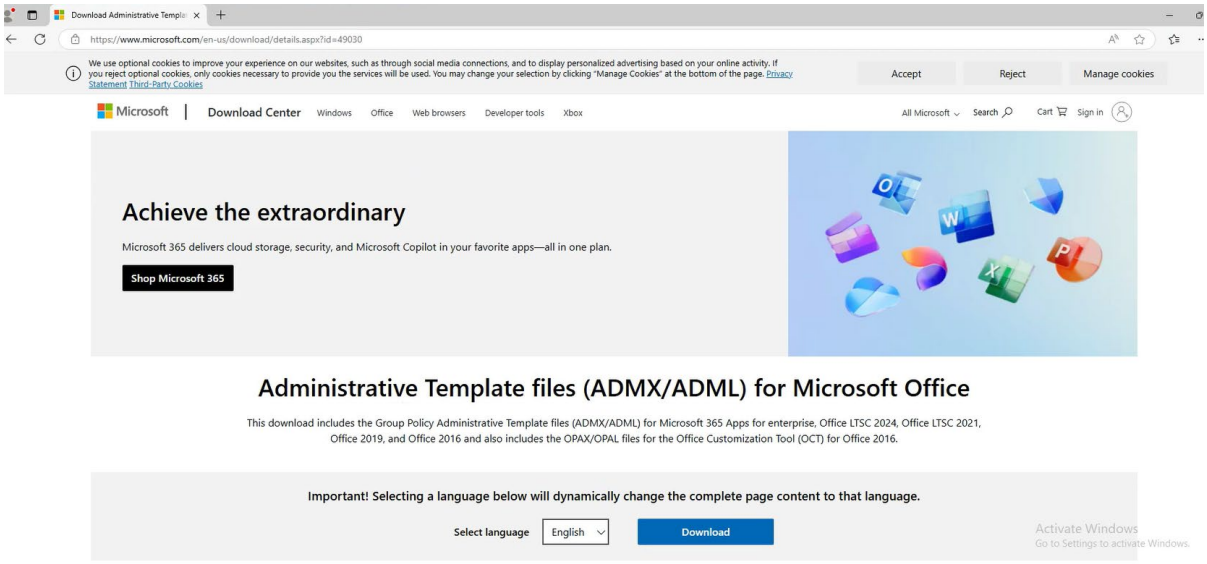
4.2.1 DC101

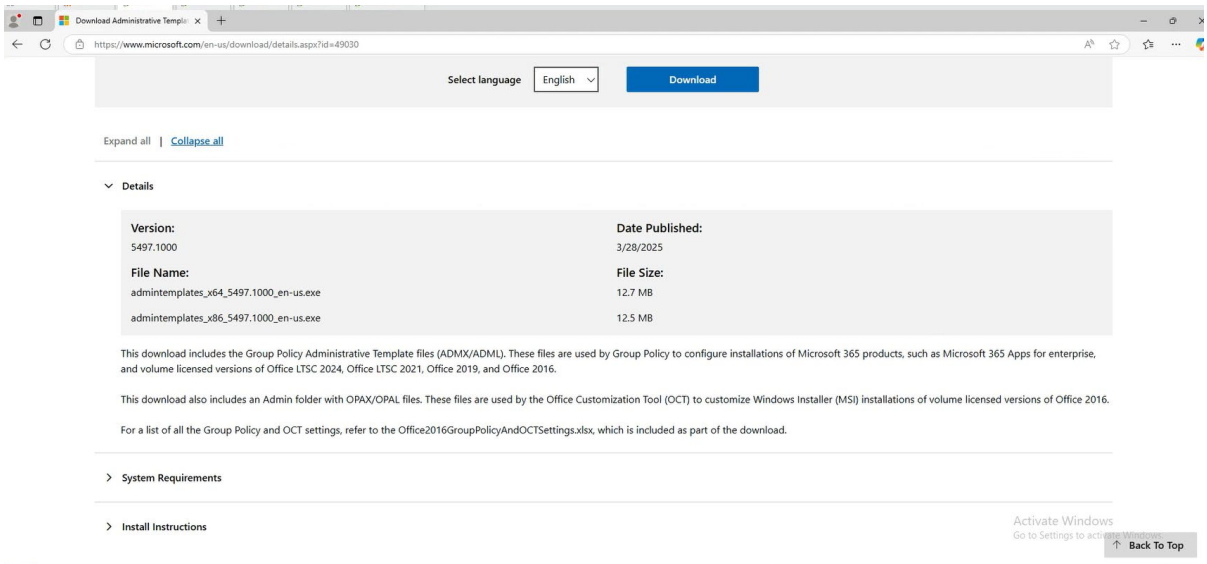
1. Download Microsoft Office Administrative Templates

a) **On DC101 (Domain Controller):**

- Temporarily **enable NAT NIC** for internet access
- Download latest Office ADMX templates from: https://www.microsoft.com/en-us/download/details.aspx?id=49030
- **Disable NAT NIC** after download completes (for security)







System Requirements

Supported Operating Systems

Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022

Note: Refer to the System requirements for Office to see the supported operating systems for specific versions of Office.

The Administrative Template files (ADMX/ADML) in this download work with the following Office programs:

- Microsoft 365 Apps for enterprise.
- Desktop versions of Project and Visio that come with subscription plans.
- Volume licensed versions of Office LTSC 2024, Project 2024, and Visio LTSC 2024. For example, Office LTSC Professional Plus 2024, Project Standard 2024, and Visio LTSC Professional 2024.
- Volume licensed versions of Office LTSC 2021, Project 2021, and Visio LTSC 2021. For example, Office LTSC Professional Plus 2021, Project Standard 2021, and Visio LTSC Professional 2021.
- Volume licensed versions of Office 2019, Project 2019, and Visio 2019. For example, Office Standard 2019 and Visio Professional 2019.
- Volume licensed versions of Office 2016, Project 2016, and Visio 2016. For example, Office Professional Plus 2016 and Project Standard 2016.

The Office Customization Tool (OPAX/OPAL) files provided in this download only work with volume licensed versions of Office 2016, Project 2016, and Visio 2016. For example, Office Professional Plus 2016 and Project Standard 2016.

Install Instructions

To download and extract the ADMX/ADML and OPAX/OPAL files:

1. Click the **Download** button (above) and choose whether you want to download the 32-bit (x86) or 64-bit (x64) files, or both. For example, if you're using the Office Customization Tool (OCT) to customize installations of the 64-bit version of Office, download the 64-bit (x64) files. If you just need the ADMX/AMDL files, you can download either the 32-bit (x86) or 64-bit (x64) files. The ADMX/ADML files are the same for both.
2. Click **Next** and choose where to save the files.
3. Go to the location where you saved the downloaded files, and double-click the admintemplates executable (.exe) file, and follow the instructions to extract the files to a location of your choosing.

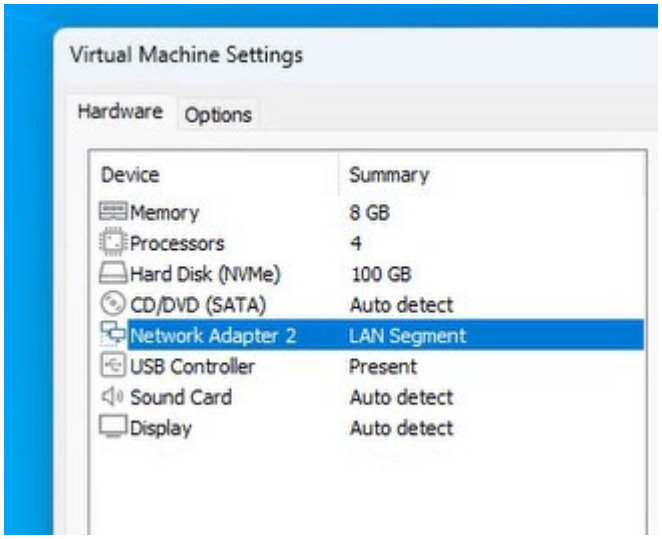
If you have Windows Server and Active Directory Domain Services (AD DS) deployed in your organization, you can configure settings for Office by using Group Policy. Copy the ADMX/ADML files to your AD DS environment and then use the Group Policy Management administrative tool to configure the Group Policy settings for Office.

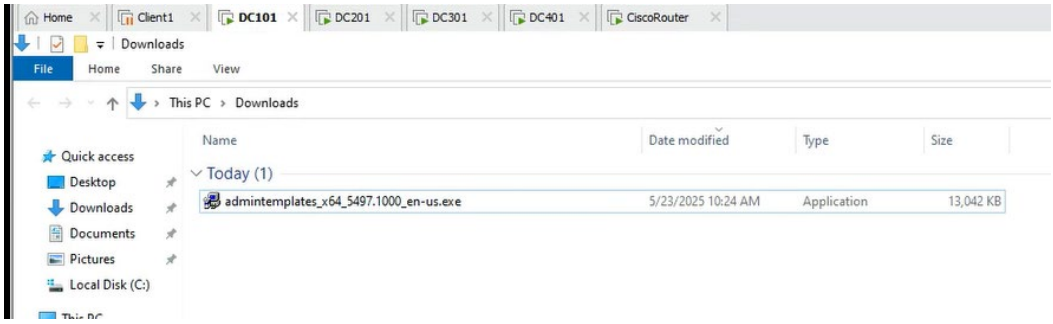
If you're using the Office Customization Tool (OCT), copy the Admin folder with the OPAX/OPAL files into the folder that contains your Office installation files. For more information about the OCT, see Office Customization Tool (OCT) 2016 Help: Overview.

Choose the download you want

File Name	Size
admintemplates_x64_5497.1000_en-us.exe	12.7 MB
admintemplates_x86_5497.1000_en-us.exe	12.5 MB

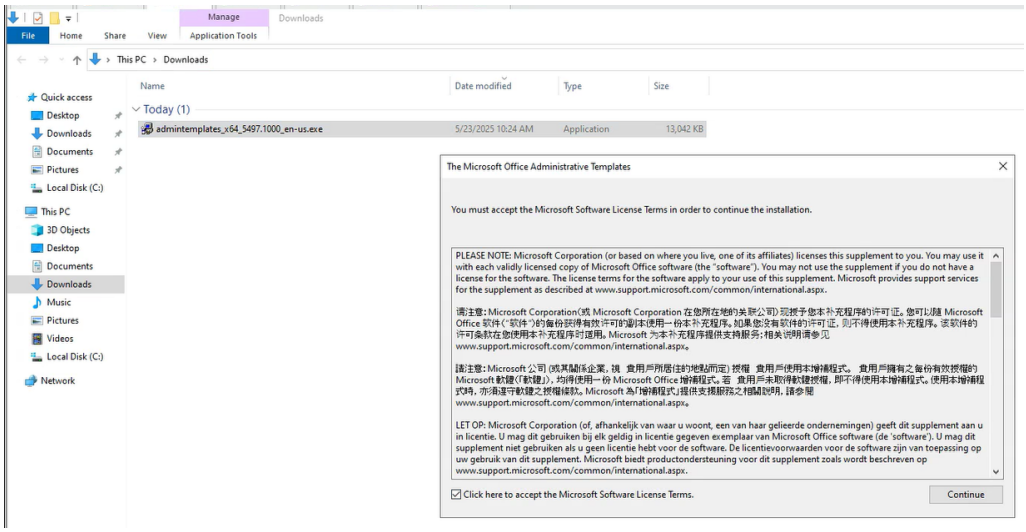
Download Total size: 12.7 MB

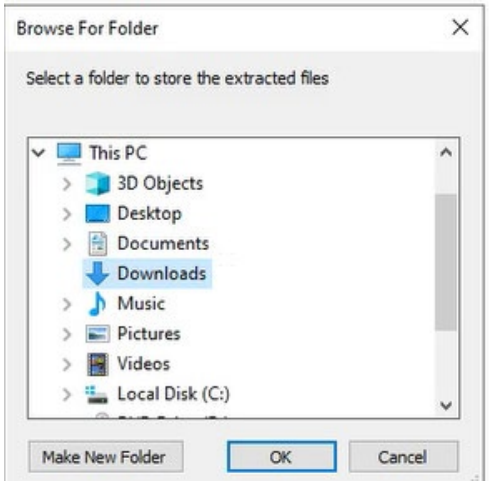


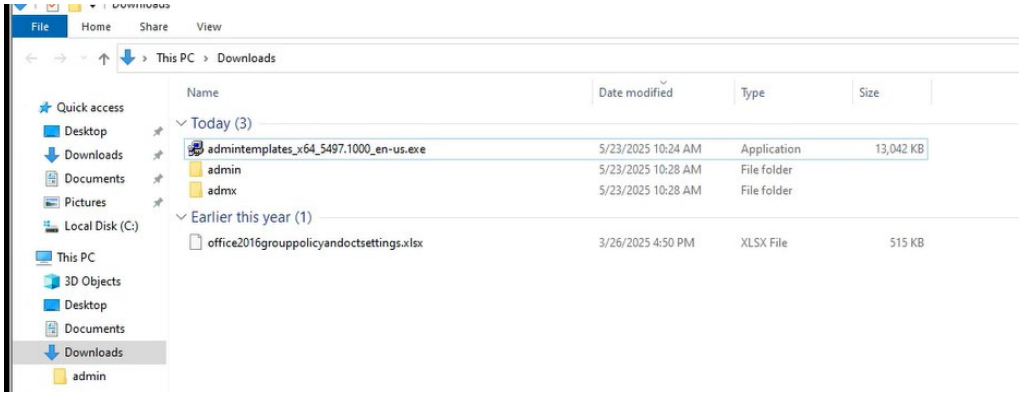


b) **Extract and Install Templates:**

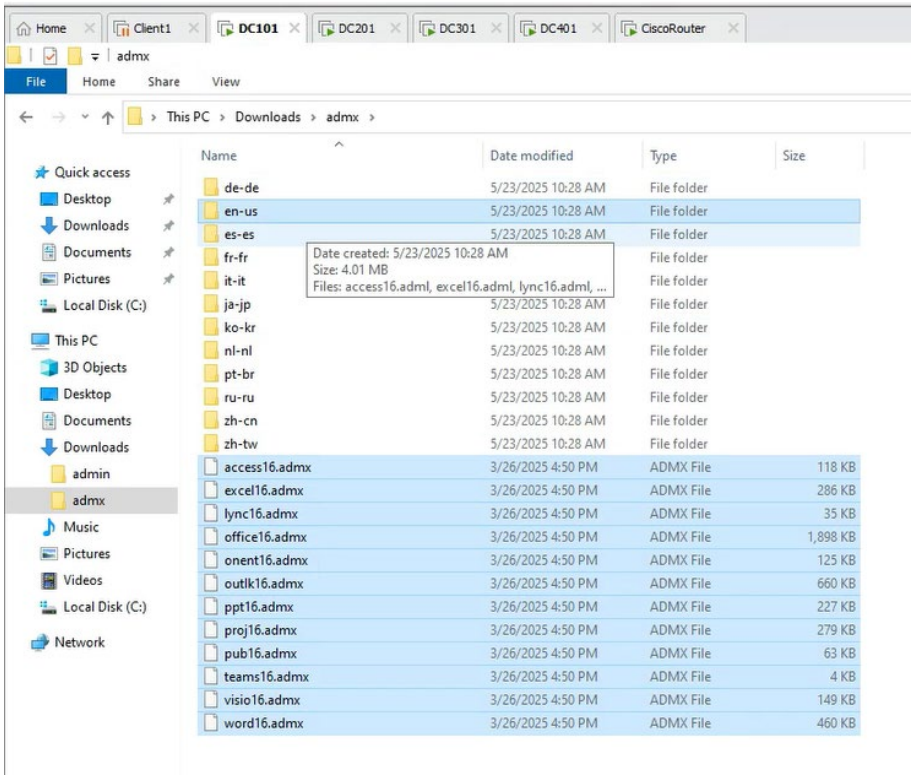
- Unzip downloaded package
- Copy contents to Central Store: \\vlabs1.com\SYSVOL\vlabs1.com\Policies\PolicyDefinitions
- Ensure all .admx files and language folders (e.g., en-US) are copied

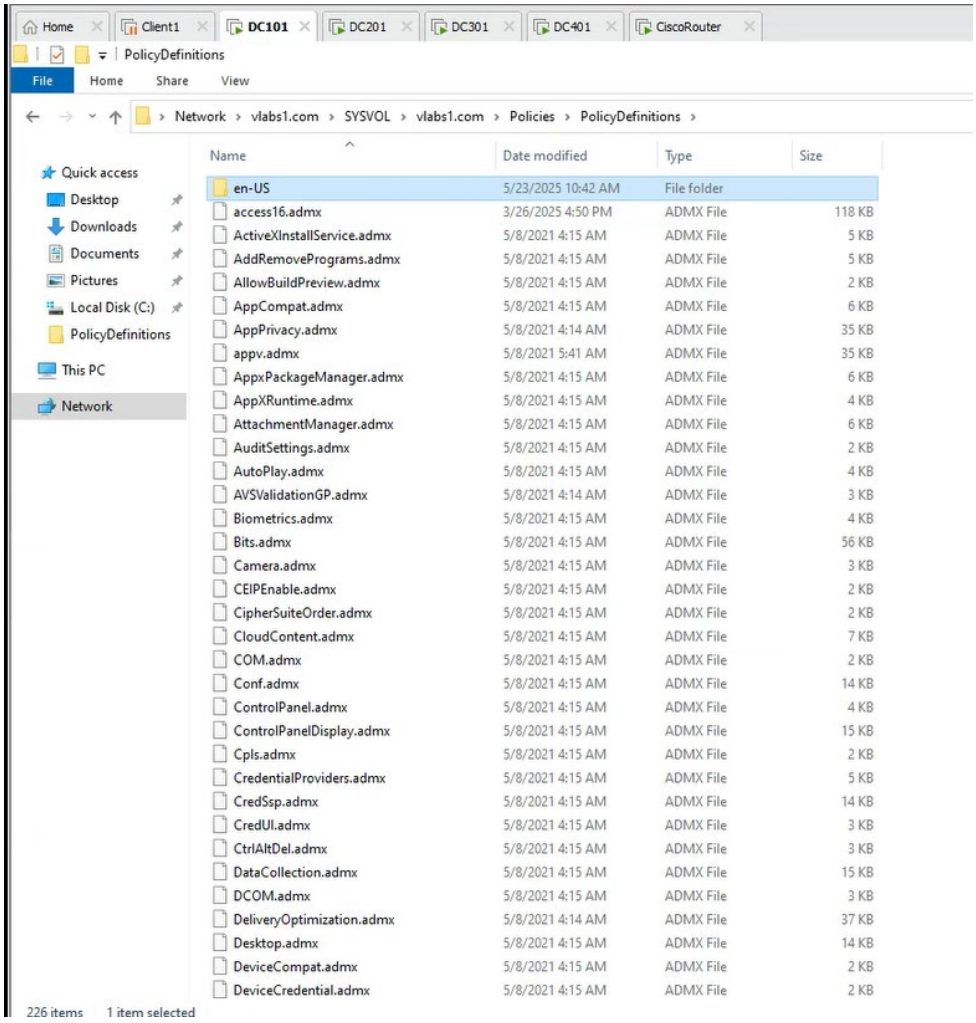




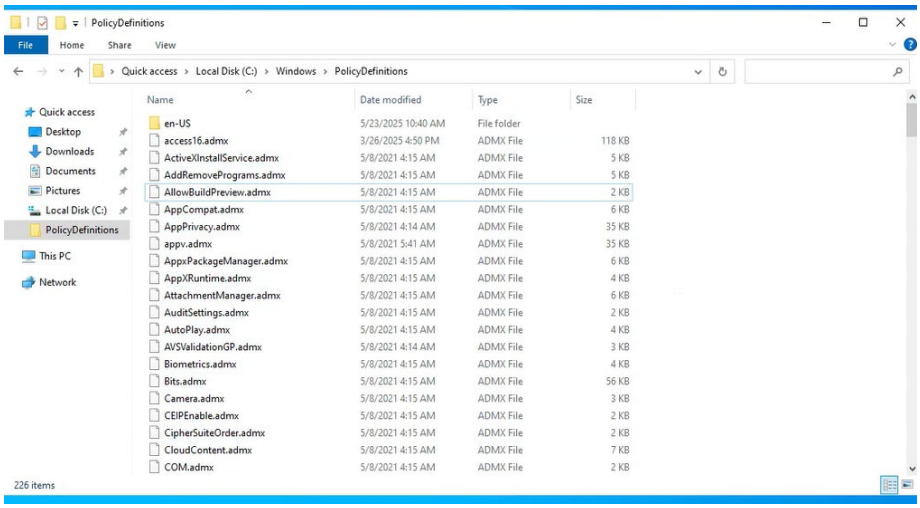


Open admx and select files and en-us folder



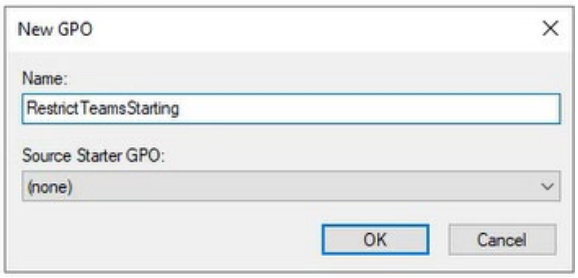


Copy in local too



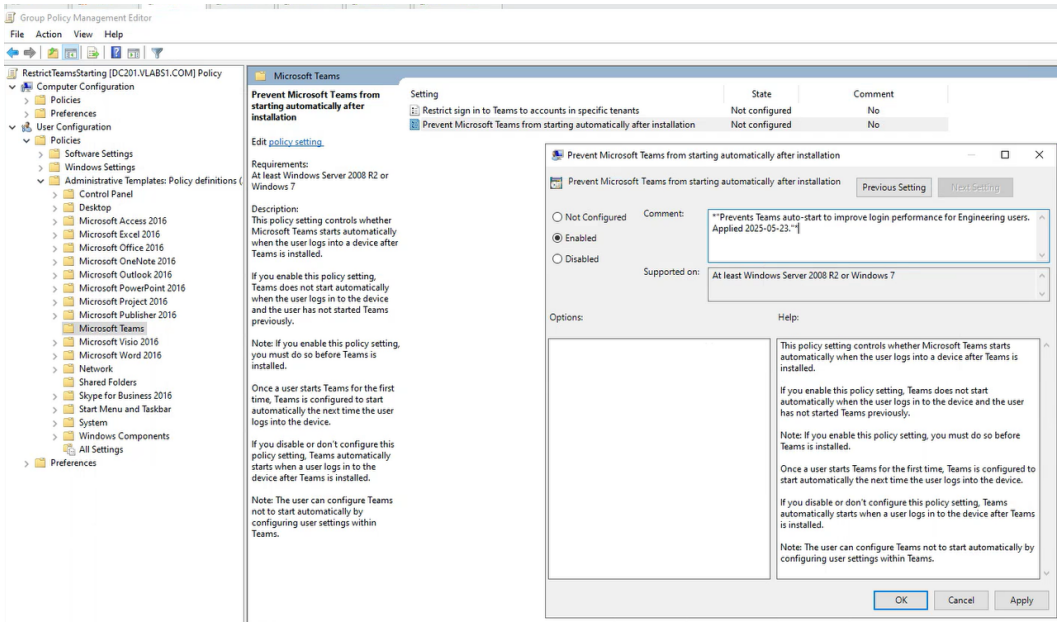
2. Create and Configure RestrictTeamsStarting GPO

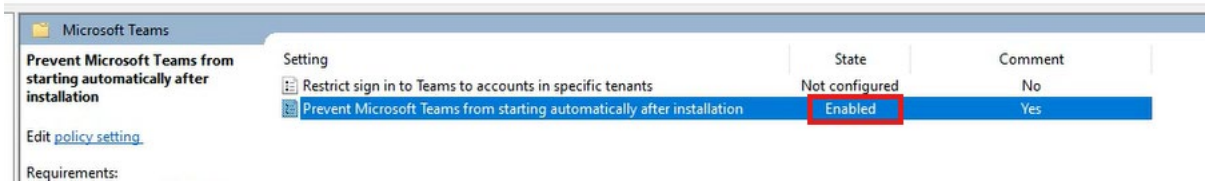
a) **In GPMC (**gpmc.msc**):**
   - Right-click **Group Policy Objects** → **New**
   - Name: RestrictTeamsStarting → Click **OK**



b) **Edit the GPO:**
   - Right-click → **Edit**
   - Navigate to: User Configuration → Policies → Administrative Templates → Microsoft Teams

c) **Configure Policy Setting:**
   - Locate: **"Prevent Microsoft Teams from starting automatically after installation"**
   - Set to: **Enabled**
   - Add **Comment**:
     "Prevents Teams auto-start to improve login performance for Engineering users. Applied 2023-11-15."

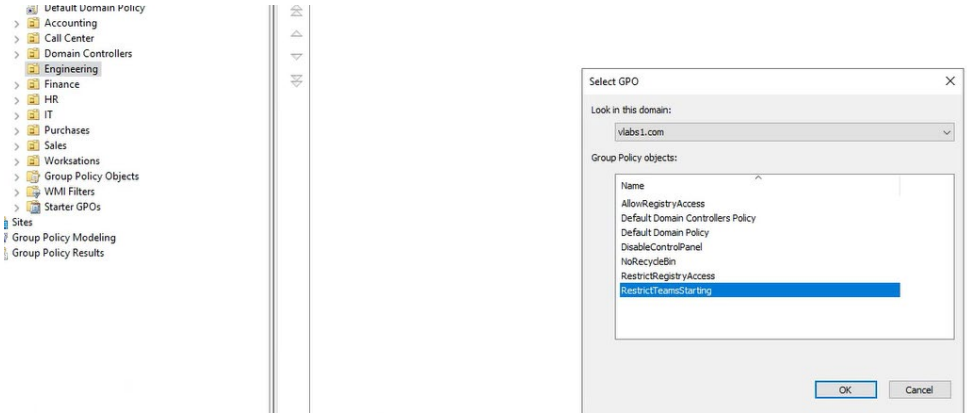




3. Link GPO to Engineering OU

a) In GPMC:

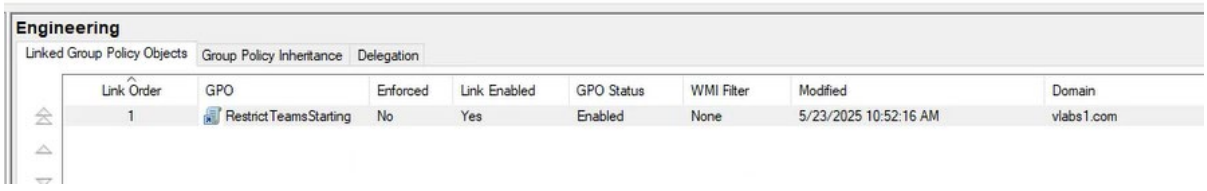
- Right-click **Engineering OU** → **Link an Existing GPO**
- Select RestrictTeamsStarting → Click **OK**



b) **Verify Link Order:**

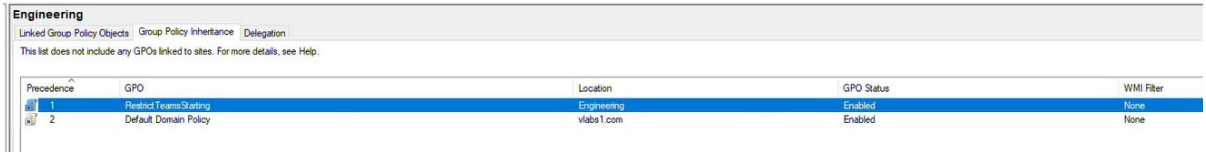
- Ensure no conflicting policies have higher precedence

1. **View Linked GPOs**
   - In the **"Linked Group Policy Objects"** tab, you'll see a list of GPOs applied to the Engineering OU.
   - **Higher precedence = Lower link number** (e.g., GPO with **Link Order 1** applies first and can override GPOs below it).



2. **Ensure** RestrictTeamsStarting **is Not Overridden**

2. Check GPO Inheritance & Enforcement



*To be tested in **Task 8 Managing Software Installation** task*

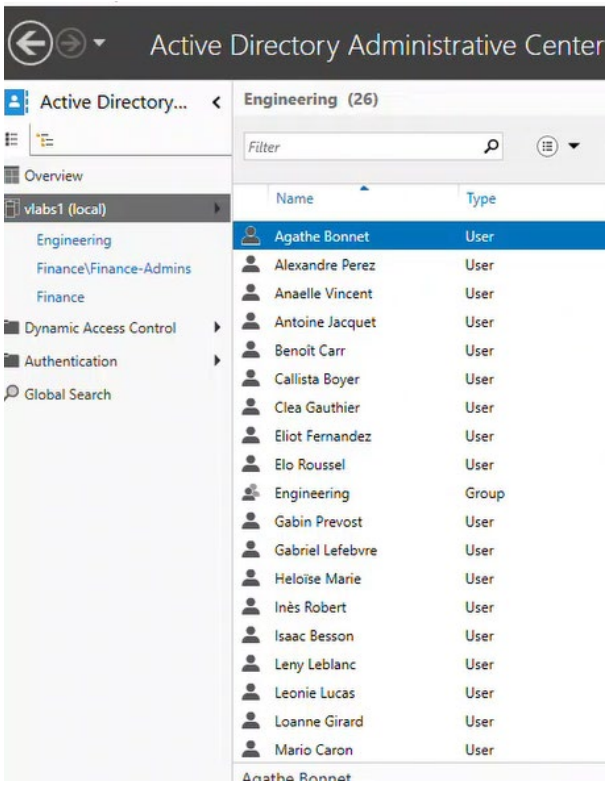
4.2.2 Client1

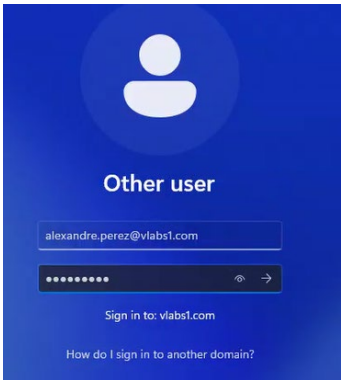
1. **Force Policy Application**

a) **On Client1 (Windows 11 test machine):**

1. Log in as Engineering OU user
2. Open Command Prompt as Administrator:
   gpupdate /force
3. Wait for confirmation: *"User Policy update has completed successfully"*

Verify users in engineering






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

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

PS C:\Users\alexandre.perez> gpupdate /force
Updating policy...

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

PS C:\Users\alexandre.perez>
```

b) **Policy Result Verification:**

1. Run:
   gpresult /r
2. Confirm RestrictTeamsStarting GPO appears under *"Applied Group Policy Objects"*

```
PS C:\Users\alexandre.perez> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  2025- 05- 23 at 12:34:21 PM


RSOP data for VLABS1\alexandre.perez on CLIENT1 : Logging Mode
-----------------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\alexandre.perez
Connected over a slow link?: No


USER SETTINGS
--------------
    CN=Alexandre Perez,OU=Engineering,DC=vlabs1,DC=com
    Last time Group Policy was applied: 2025-05-23 at 12:33:05 PM
    Group Policy was applied from:      DC201.vlabs1.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS1
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        RestrictTeamsStarting

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Engineering
        Authentication authority asserted identity
        Medium Mandatory Level

PS C:\Users\alexandre.perez>
```

Key Configuration Summary

Setting	Value	Purpose
GPO Name	RestrictTeamsStarting	Controls Teams auto-start
Policy Path	User Config → Admin Templates → Microsoft Teams	Targets user-level behavior
Linked OU	Engineering	Applies to specific department
Enforcement	gpupdate /force	Immediate policy application

5 Task 3: Managing Account Policies

5.1 Objective

Configure domain-wide password and account lockout policies in the Default Domain Policy, then verify enforcement.

5.2 Steps

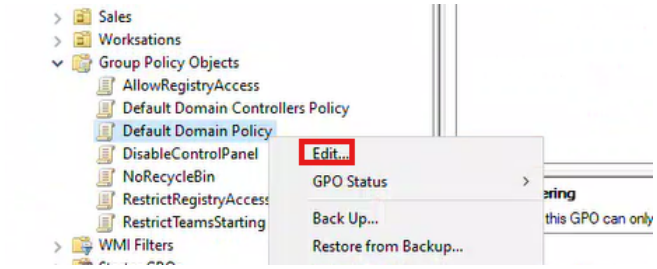
- Modify **password policies** in the **Default Domain Policy** GPO:
  - Minimum password length: **12 characters**.
  - Password complexity: **Enabled**.
  - Password expiration: **60 days**.
- Apply **Account Lockout Policy**:
  - Lock account after **2 failed login attempts**.
  - Lockout duration: **2 minutes**.
- Run **gpupdate /force** to apply changes.
- From **Client1**, test with **Emma Petit** by attempting password modification and simulating an account lockout.

5.2.1 DC101

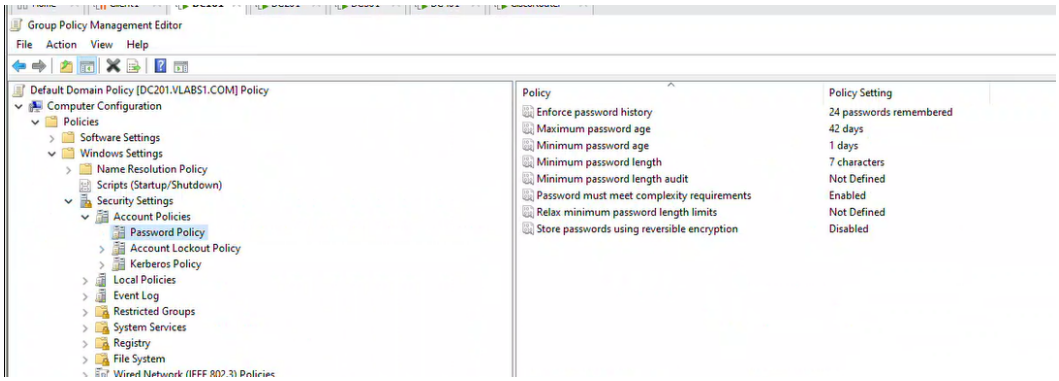
1. **Configure Password Policies**

a) **On DC101 (Domain Controller):**

- Open **GPMC** (gpmc.msc)
- Navigate to: Group Policy Objects → Default Domain Policy → Right-click → Edit

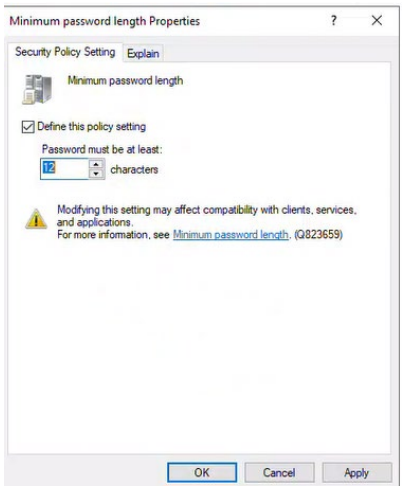


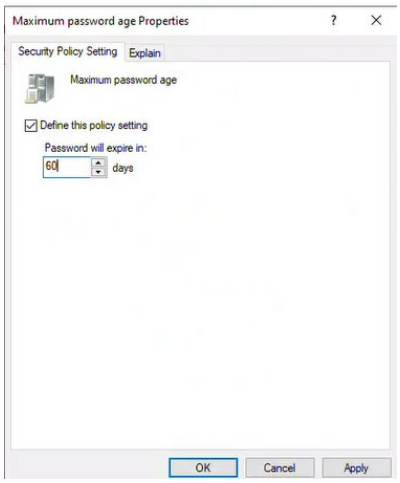
- Go to: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy

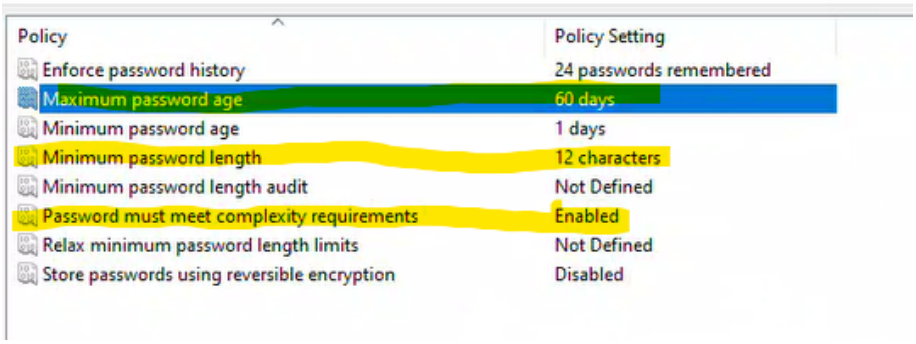


b) **Modify Settings:**

- **Minimum password length**: 12 characters *(Double-click → Set to 12 → OK)*
- **Password must meet complexity requirements**: Enabled
- **Maximum password age**: 60 days



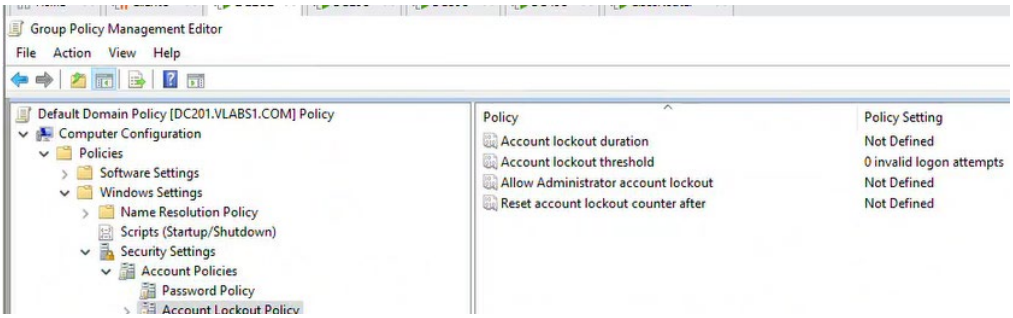




2. Configure Account Lockout Policy

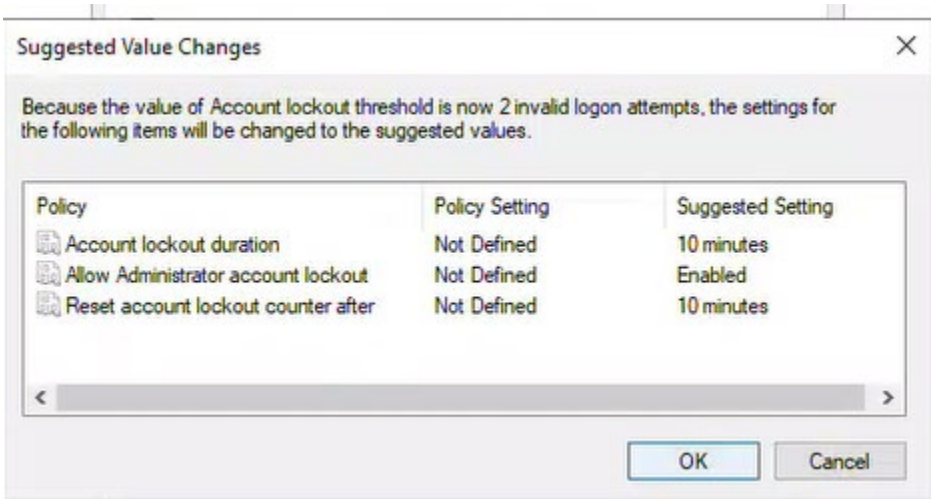
a) In the same GPO editor:

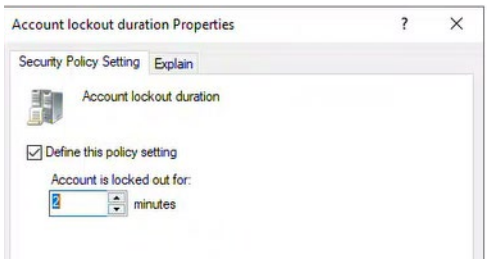
- Navigate to: Account Policies → Account Lockout Policy

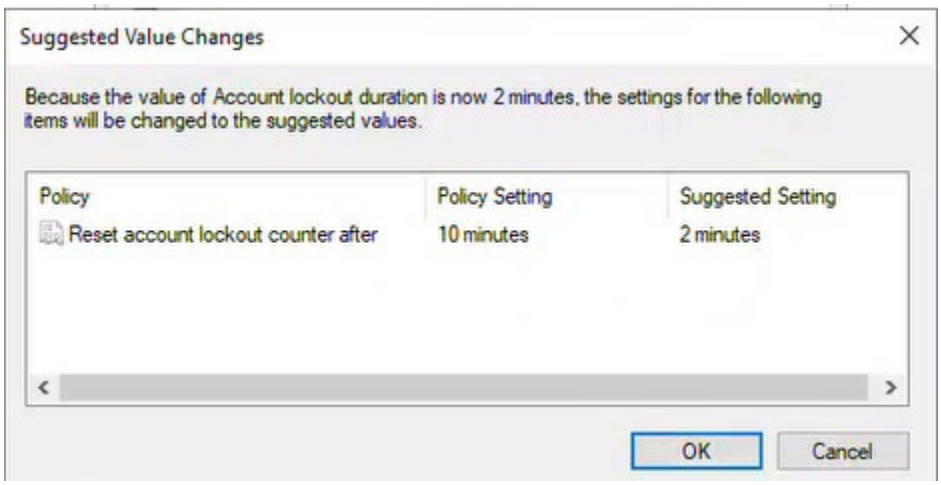


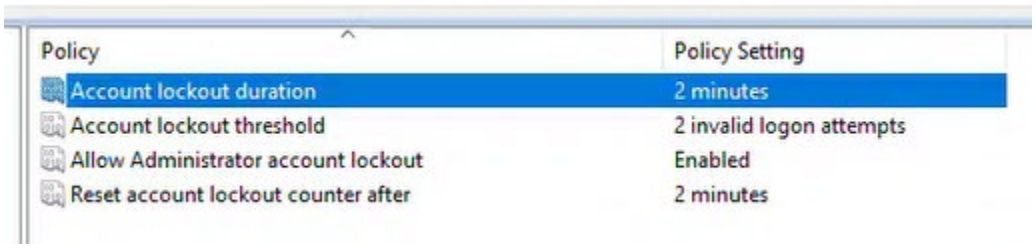
b) **Modify Settings:**

- **Account lockout threshold**: 2 invalid attempts
  (Setting this will auto-populate other values)
- **Account lockout duration**: 2 minutes
- **Reset account lockout counter after**: 2 minutes



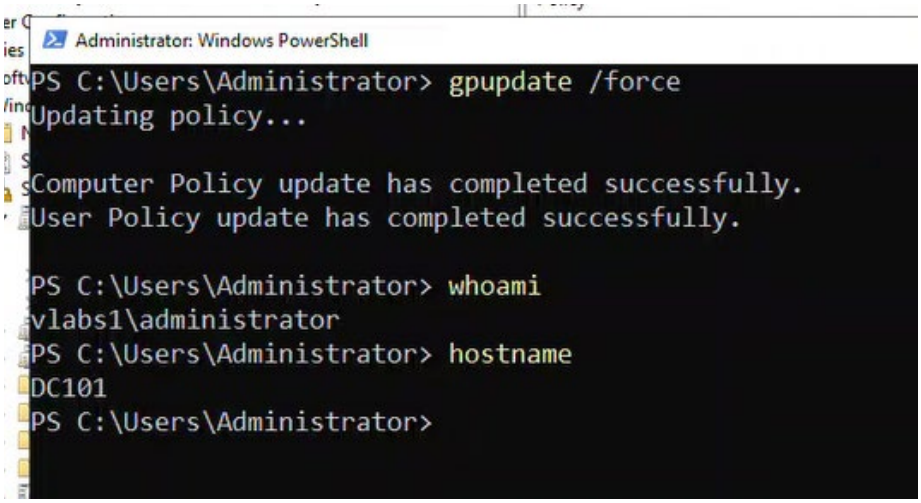






3. Apply Policies

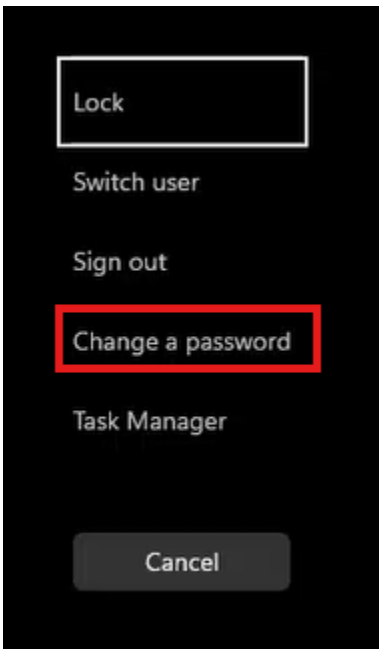
a) **Force Policy Update:**
   - On DC101, run Command Prompt as Administrator:
     gpupdate /force
   - Wait for confirmation:
     "Computer Policy update has completed successfully"



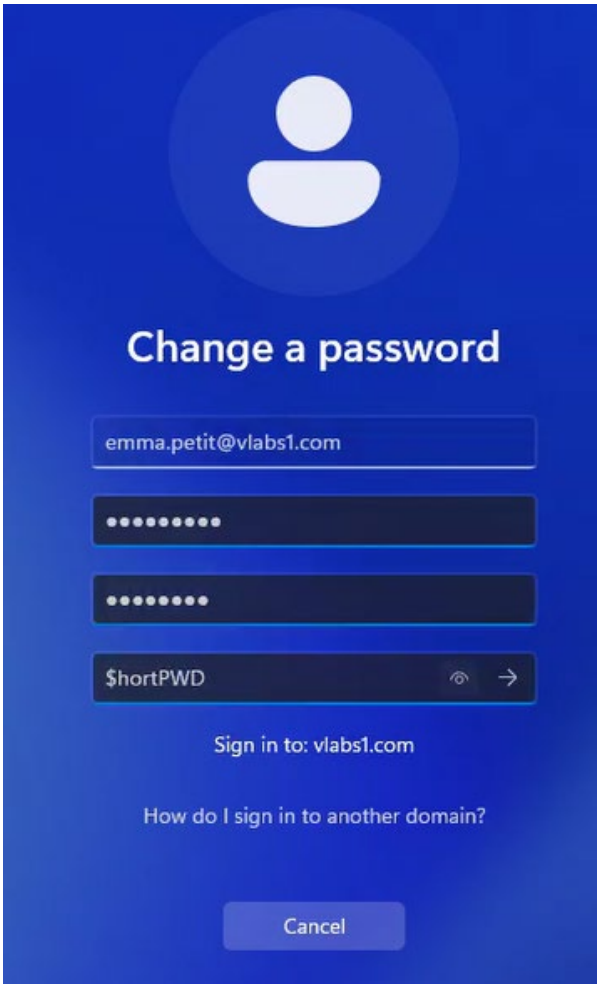
5.2.2 Client1

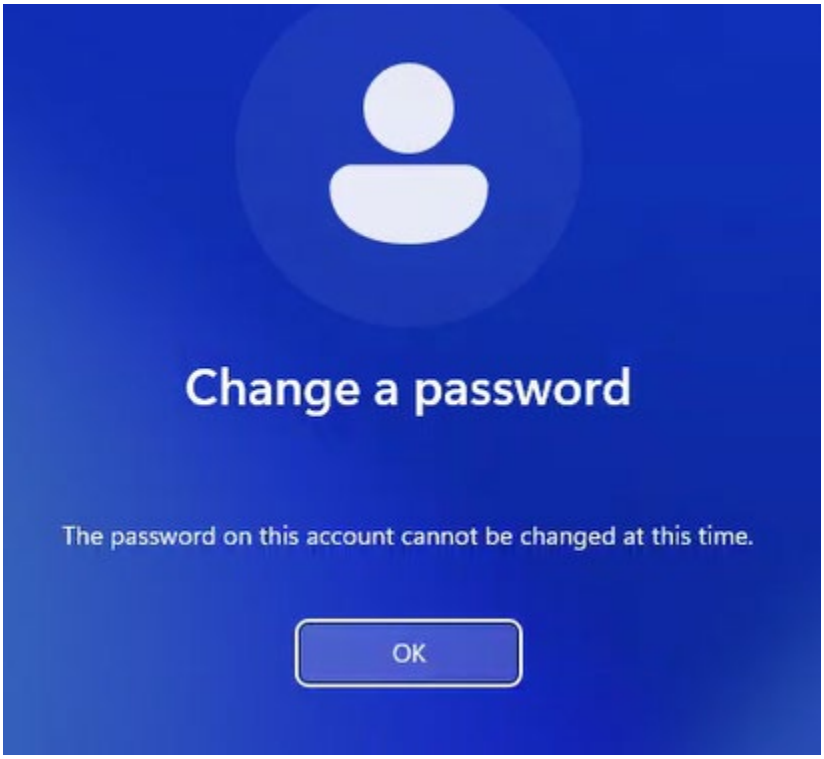
Verification Testing (From Client1)
1. Test Password Change (Emma Petit)

a) **Log in to Client1** as vlabs1.com\emma.petit
b) Attempt to change password via Ctrl+Alt+Del → Change a password:

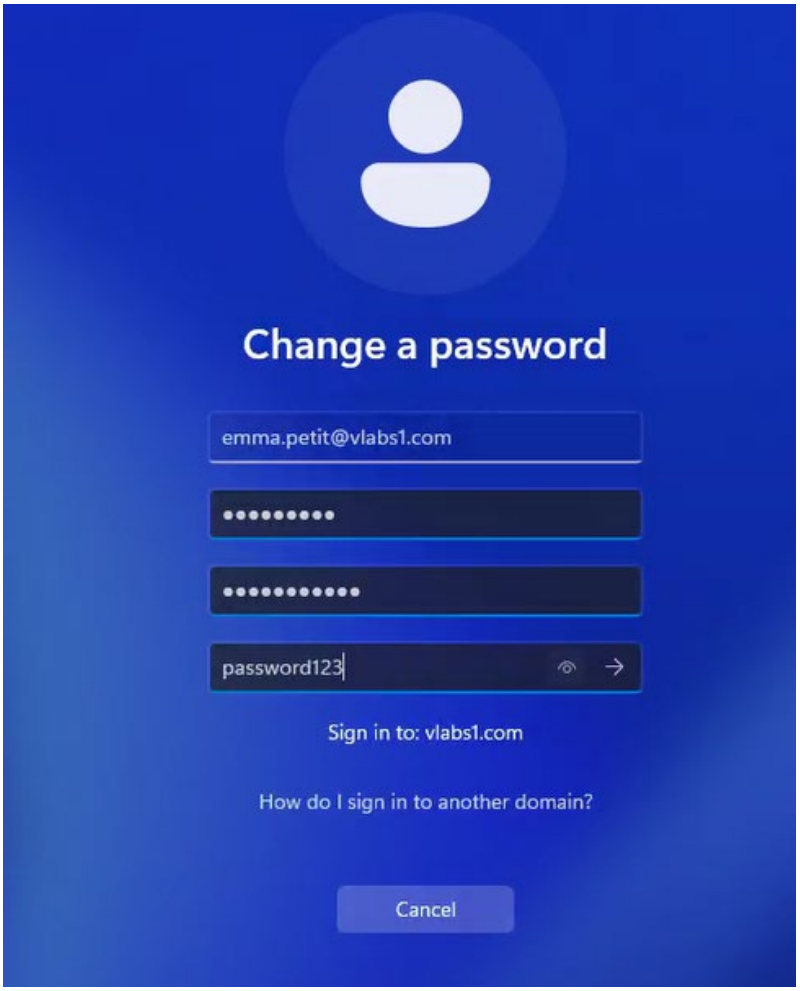


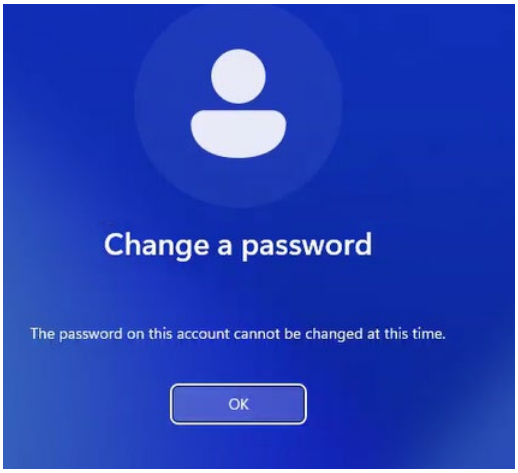
- **Test Case 1**: Try password shorter than 12 chars → Should fail





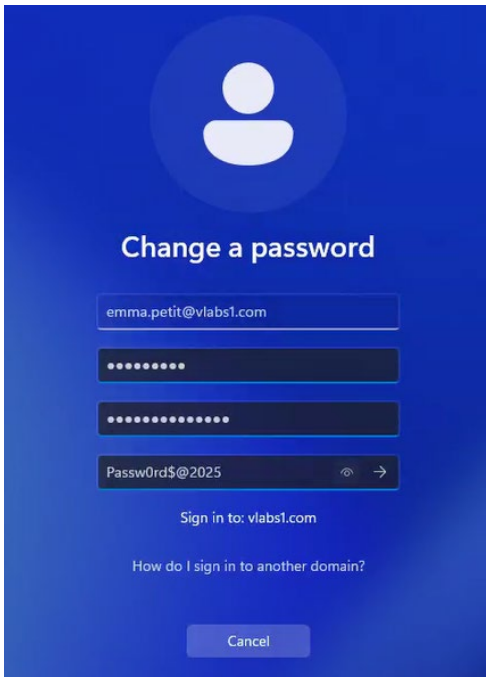
- **Test Case 2**: Try password without complexity (e.g., "password123") → Should fail

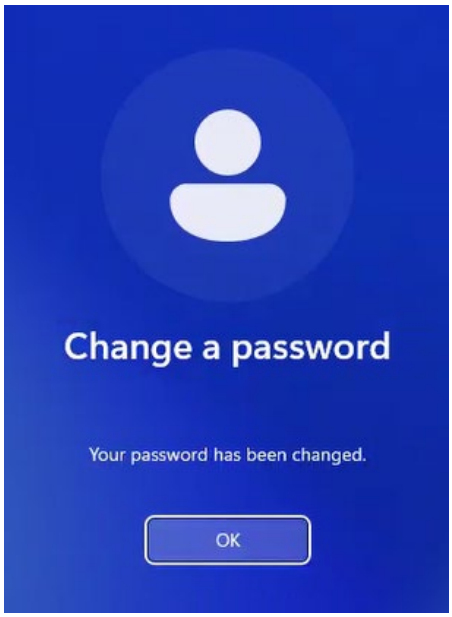




- **Test Case 3**: Valid password (e.g., "Vlabs1@2025!") → Should

succeed



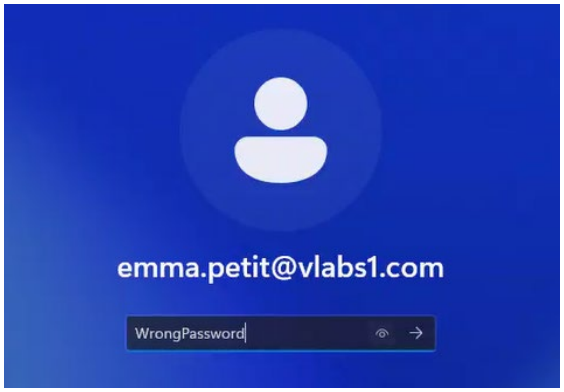


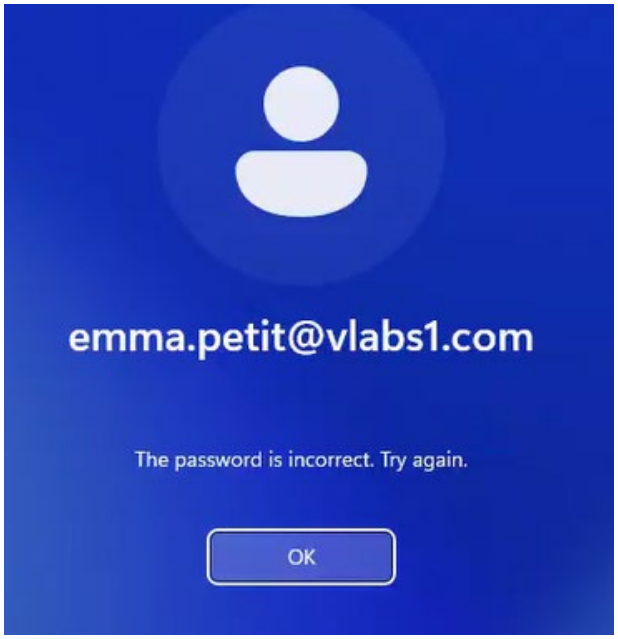
2. Test Account Lockout

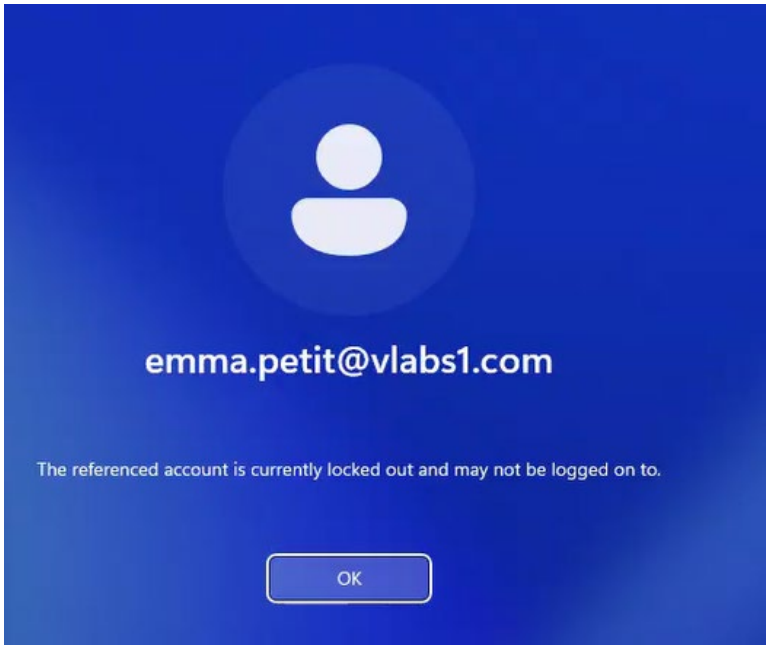
a) **Simulate Failed Logins:**

- Log out and intentionally enter **wrong password twice**

b) **Expected Result:**
   - After 2nd attempt:
     "Your account is locked out. Try again later."
   - Wait 2 minutes → Account should auto-unlock







Policy Configuration Summary

Policy Type	Setting	Value
Password Policy	Minimum length	12 characters
	Complexity requirements	Enabled
	Maximum password age	60 days
Lockout Policy	Lockout threshold	2 attempts
	Lockout duration	2 minutes
	Reset counter after	2 minutes

6 Task 4: Implementing Fine-Grained Password Policies

6.1 Objective

Create and apply customized password policies for the IT group that override Default Domain Policy settings.

6.2 Steps

- Create a new **Fine-Grained Password** Policy named **IT_FGPPolicy.**
- Modify password settings:

- Minimum password length: **10 characters**.
- Password complexity: **Disabled**.
- Password expiration: **Never**.

- Directly apply it to the **IT Group.**
- Run **gpupdate /force** to apply changes.
- From **Client1**, test with a **user from the IT group** by attempting password modification.

6.3 DC101

1. Create Fine-Grained Password Policy

Open **Active Directory Administrative Center**

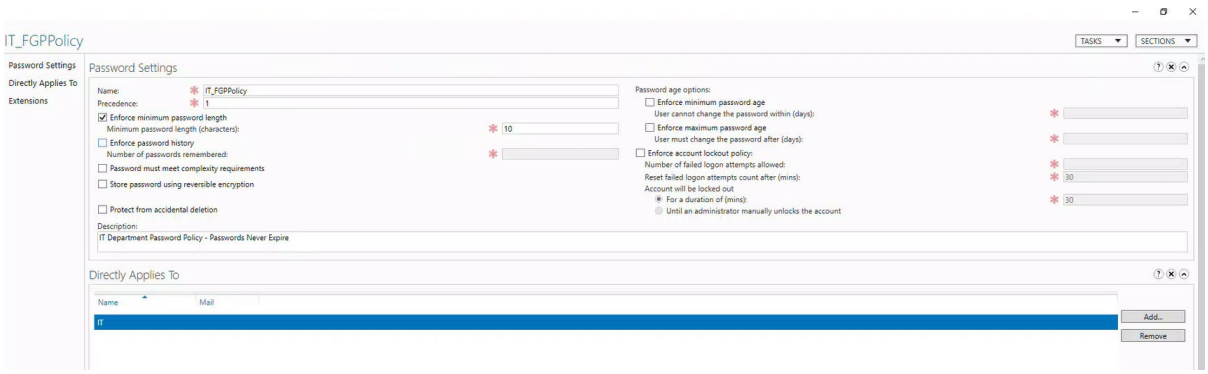
1. Navigate to Fine-Grained Password Policies:
   - In the left pane, select your domain
   - In the middle pane, double-click on "System"
   - Select "Password Settings Container"
2. Create new policy:
   - In the right pane, click "New" → "Password Settings"
   - In the dialog box that appears:
     - Name: IT_FGPPolicy
     - Precedence: 1

3. Modify Password Settings
   - **Minimum password length**: 10
   - **Password must meet complexity requirements**: **Uncheck**
   - **Enforce minimum password age**: *Leave blank*
   - **Enforce maximum password age**: *Leave blank*
   - *Leave all other fields empty or default.*

4. Apply to IT Group

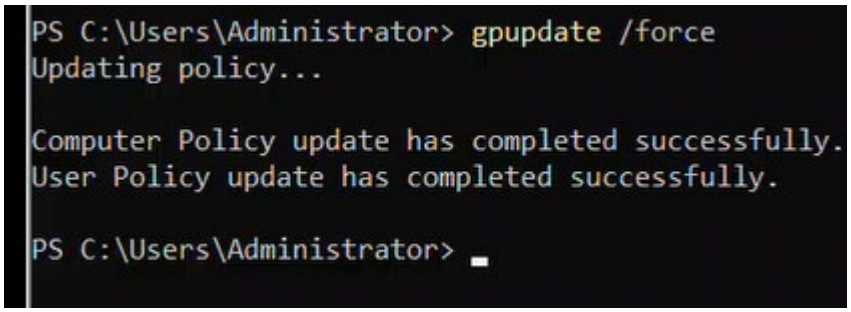
   In the same "Password Settings" dialog box:

a) Under "Directly Applies To", click "Add"
b) Browse to and select your IT group (e.g., "IT_Group")
c) Click "OK" to save the policy

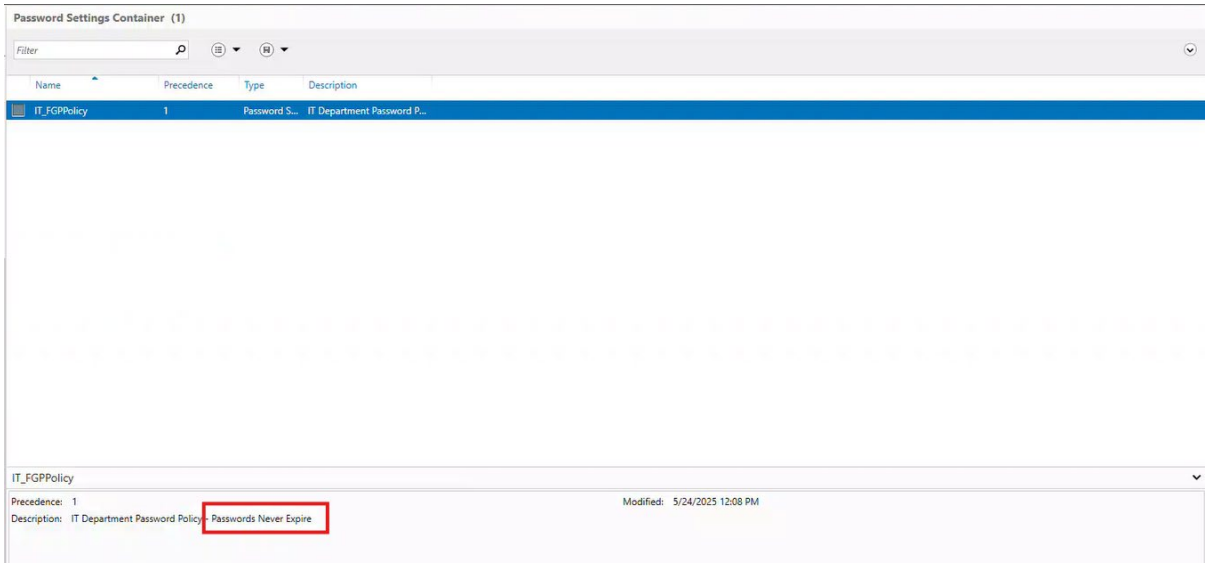


5. **Force Policy Update**

```
gpupdate /force
```



Note – It says Password never expires



2. **Verify Policy Application**

   On DC101, check effective policy:

   Get-ADUserResultantPasswordPolicy -Identity "CN=Aloyse Dupont,OU=IT,DC=vlabs1,DC=com"

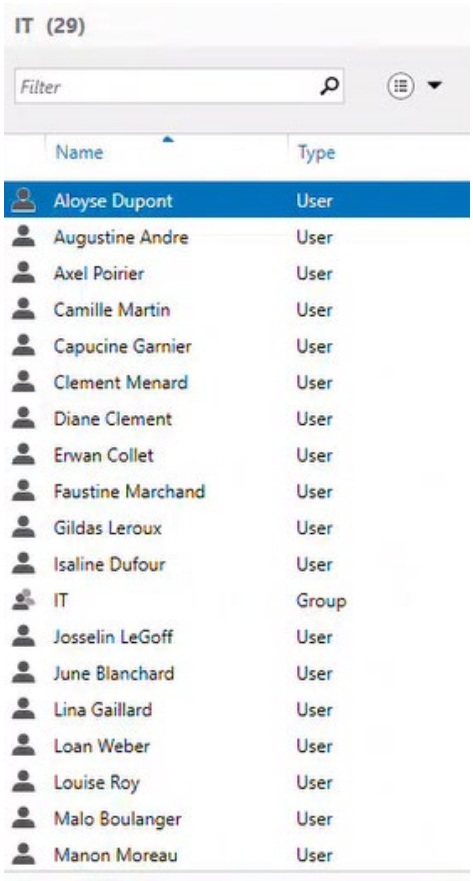
```
PS C:\Users\Administrator> Get-ADUserResultantPasswordPolicy -Identity "CN=Aloyse Dupont,OU=IT,DC=vlabs1,DC=com"


AppliesTo                   : {CN=IT,OU=IT,DC=vlabs1,DC=com}
ComplexityEnabled           : False
DistinguishedName           : CN=IT_FGPPolicy,CN=Password Settings Container,CN=System,DC=vlabs1,DC=com
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 00:00:00
MinPasswordAge              : 00:00:00
MinPasswordLength           : 10
Name                        : IT_FGPPolicy
ObjectClass                 : msDS-PasswordSettings
ObjectGUID                  : db729f94-3564-47f4-81fd-fe9e3b50e1a1
PasswordHistoryCount        : 0
Precedence                  : 1
ReversibleEncryptionEnabled : False


PS C:\Users\Administrator>
```

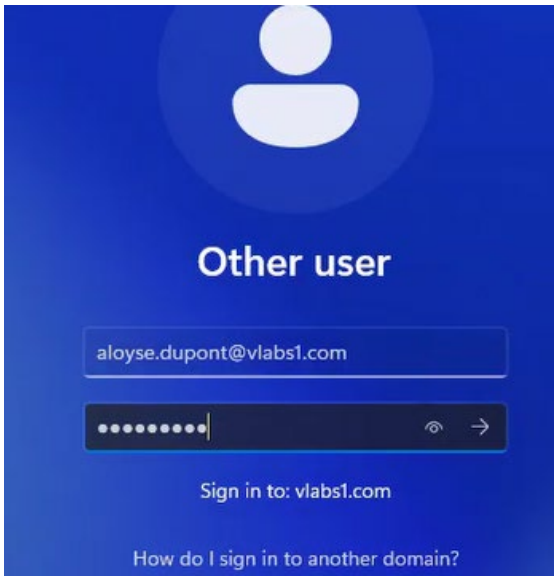
6.4 Client1

Verification Testing (From Client1)

1. Test Password Change (IT User)

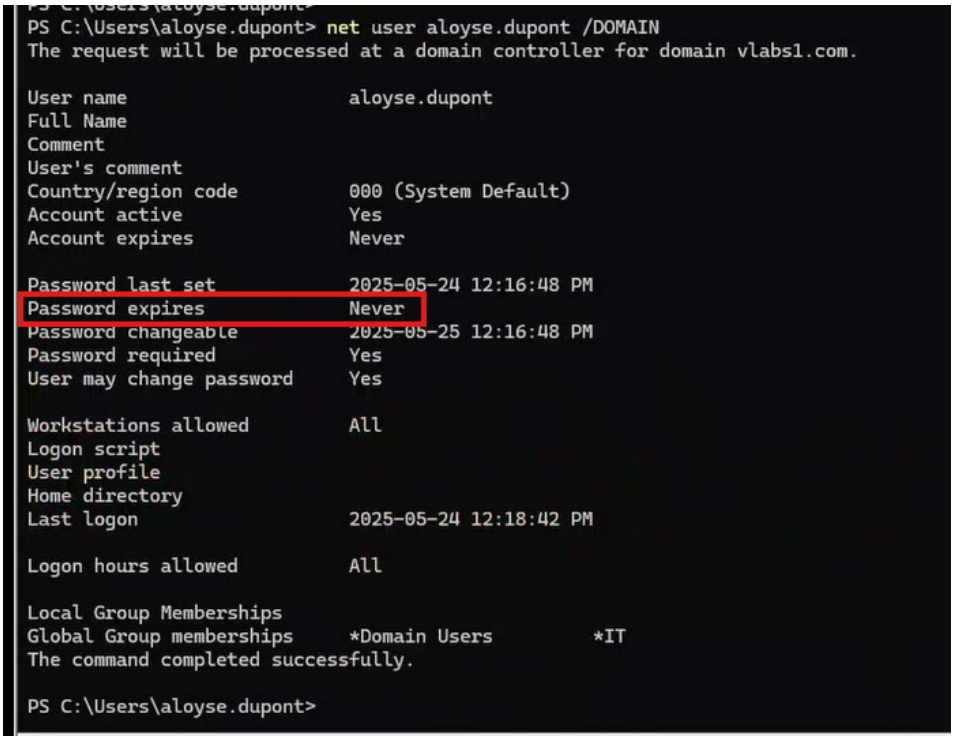
a) **Log in to Client1** as an IT group member (e.g., vlabs1.com\it.user)



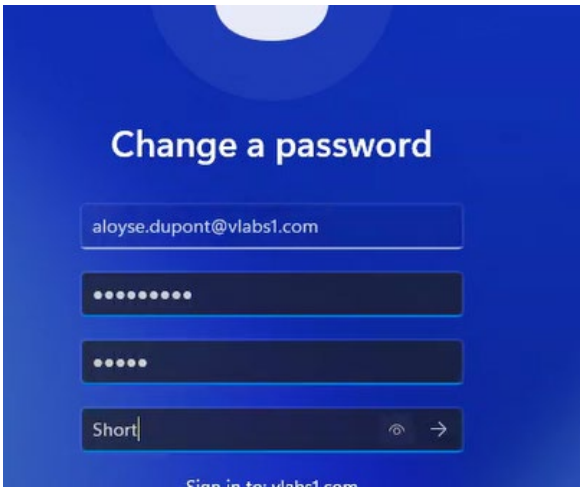


b) Attempt password change via Ctrl+Alt+Del → Change a password:

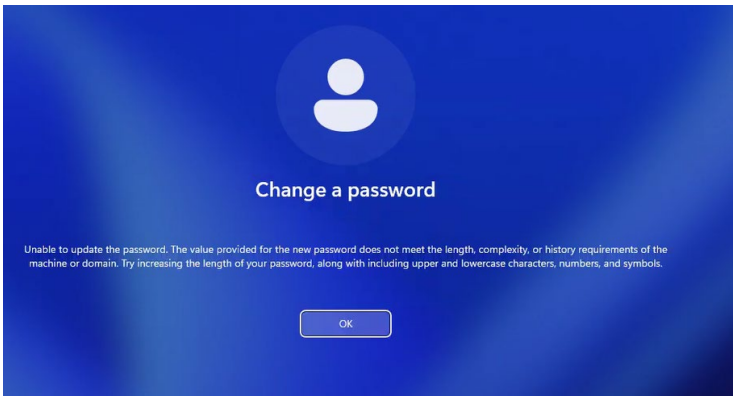
- **Test Case 1:** Password never expires → Verify via: net user aloyse.dupont /DOMAIN



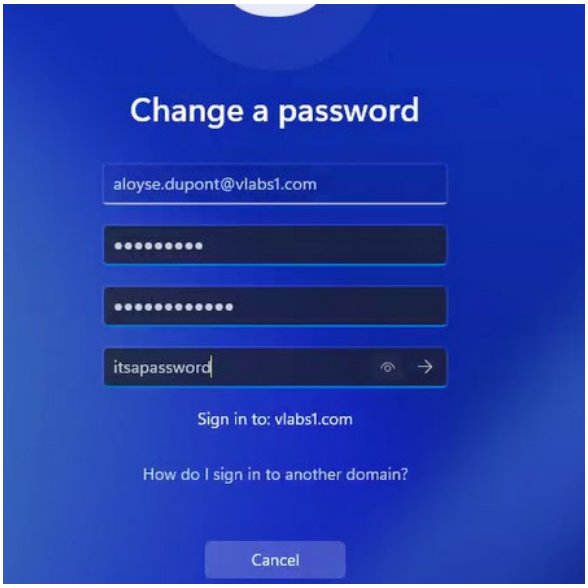
- **Test Case 2:** Try password shorter than 10 chars → Should fail

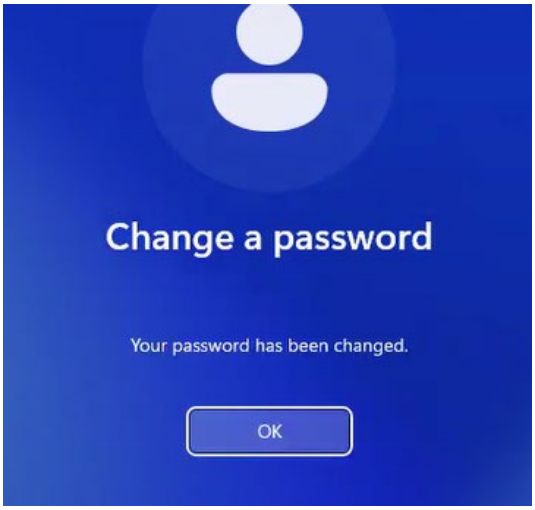


Password can not be changed



- **Test Case 2:** Try simple password (e.g., "itpassword") → Should succeed (complexity disabled)





7 Task 5: Managing Audit Authentication

- Modify **Default Domain Policy GPO** to enable **Audit Logon Events (Success and Failure)**.
- Restart the **Client1**
- Test by failing and successfully logging in with any user on **Client1.**
- Open **Event Viewer** on **DC101** and verify **Security Logs.**

7.1 Objective

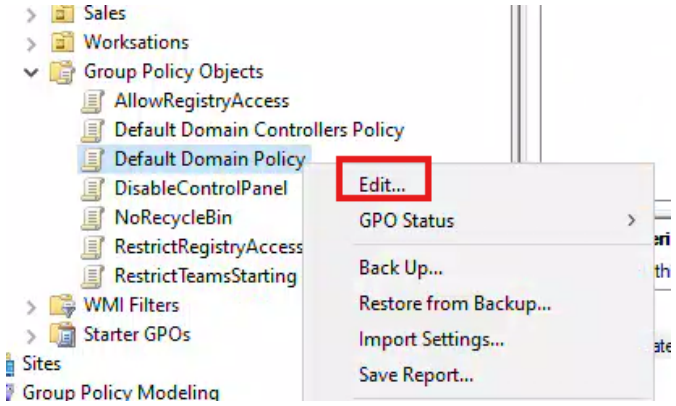
Configure domain-wide audit policies to track both successful and failed logon attempts, then verify logging functionality.

7.2 Steps

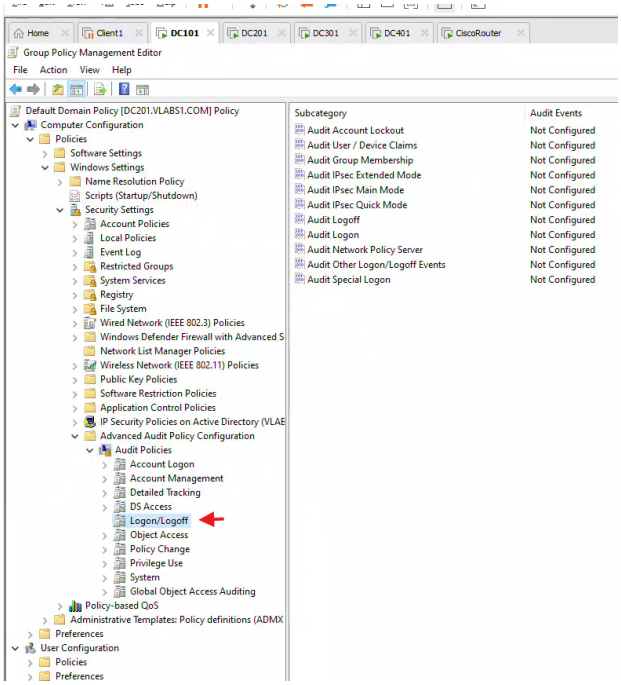
7.2.1 DC101

Configure Audit Policy in Default Domain Policy

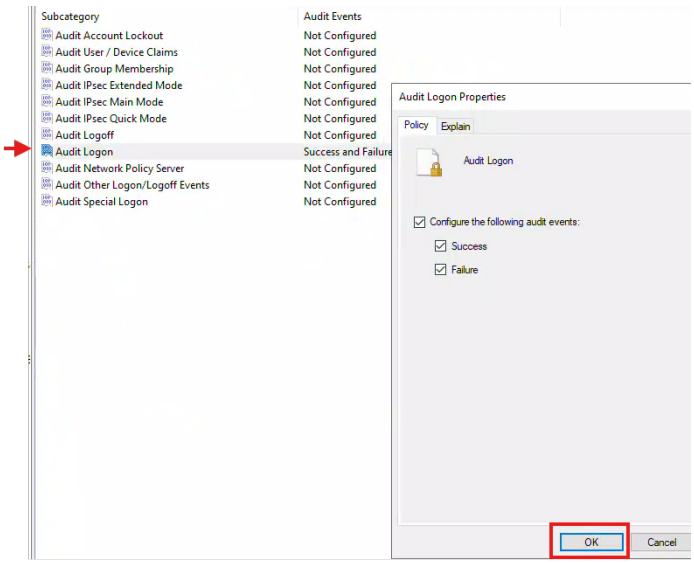
1. **On DC101 (Domain Controller):**
    - Open **Group Policy Management Console** (gpmc.msc)
    - Navigate to: Group Policy Objects → Default Domain Policy → Right-click → Edit



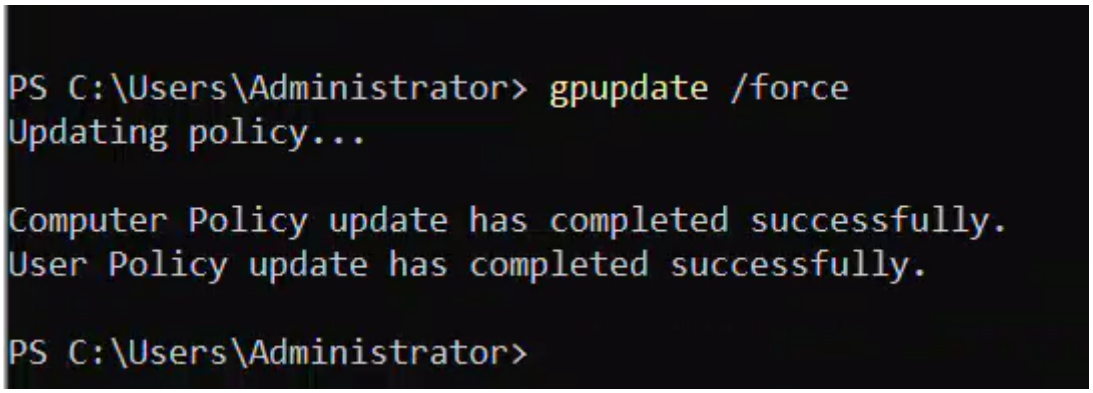
    - Go to: Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Logon/Logoff



2. **Enable Auditing:**
    - Double-click **"Audit Logon Events"**
    - Check both:
        - **"Configure the following audit events"**
        - **"Success"** and **"Failure"**
    - Click **OK**



3. **Force Policy Update:**
    - On DC101, run Command Prompt as Administrator:
    gpupdate /force



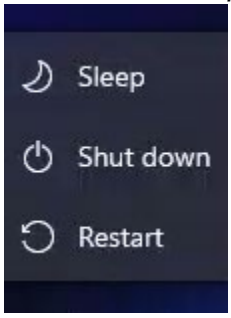
NOTE
Why You Might Not See Client1's Events on DC101:

- **Default Behavior:** By default, client computers do not forward their individual logon/logoff security events to a Domain Controller. The Domain Controller only logs events related to the authentication requests it *handles* for those clients.
- **Client-Side Logging:** Failed logon attempts *to Client1 itself* would primarily be logged on **Client1's own Security event log**. (e.g., someone trying to log directly into Client1 with local credentials or domain credentials that fail)

7.2.2 Client1

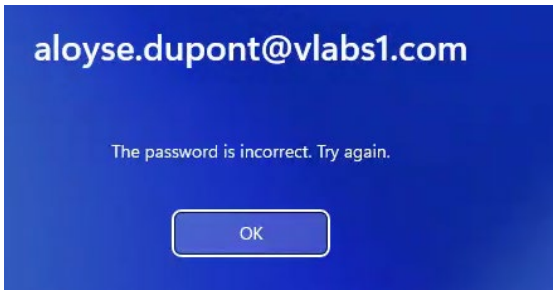
7.2.2.1 Local event in client1

1. **Restart Client1:**
    - *Wait for complete reboot*

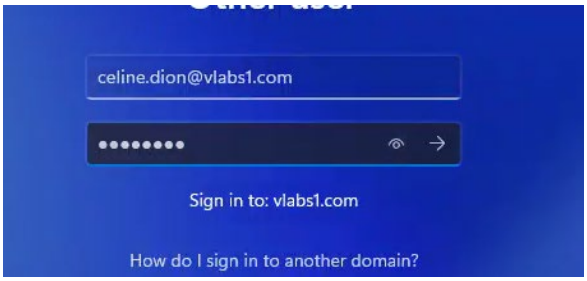


2. **Generate Test Events (On Client1)**

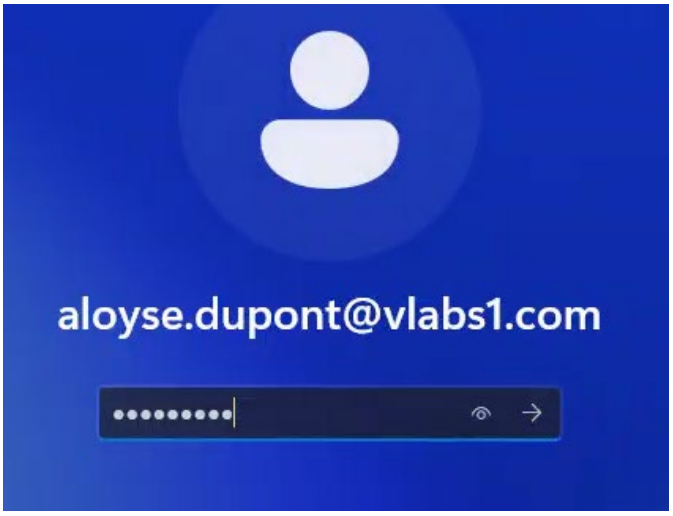
a) **Simulate Failed Logon:**
   - Attempt login with:
     - Wrong password (generates Failure event)



     - Non-existent username (generates Failure event)
   -

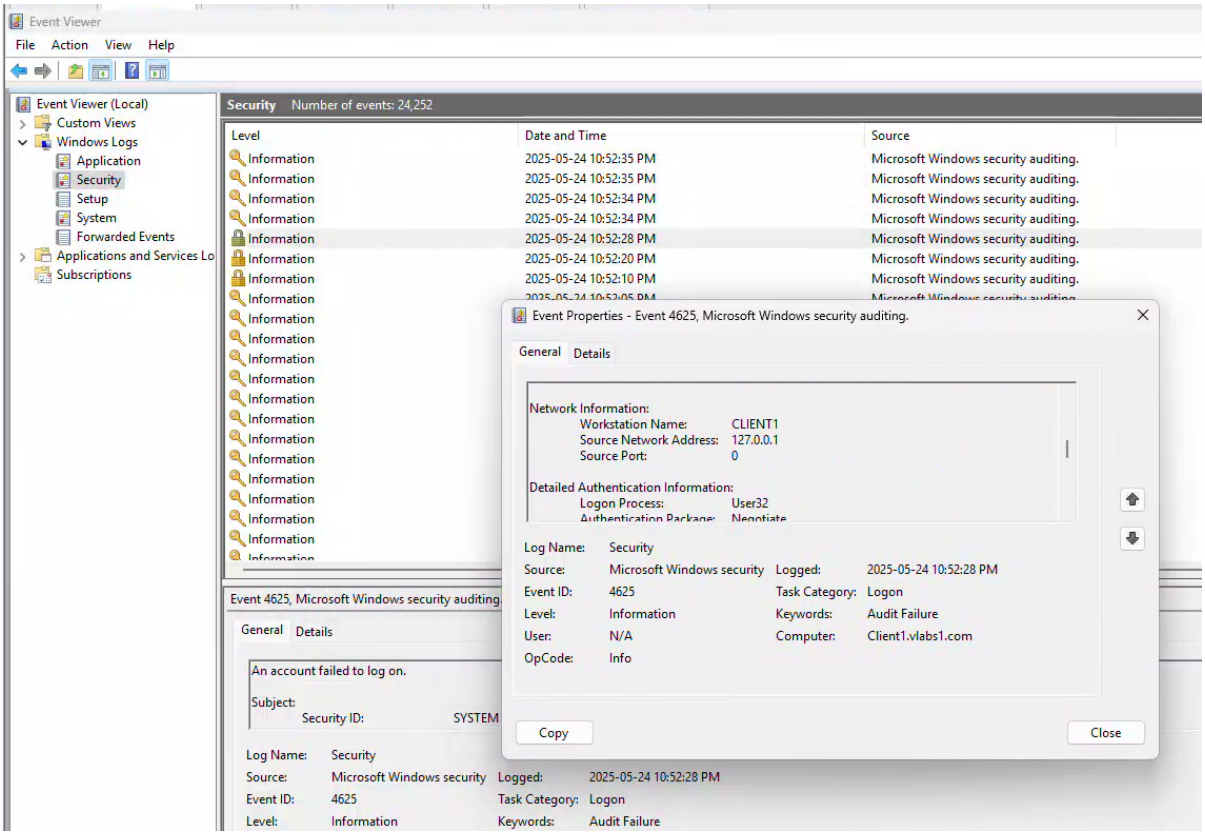


b) **Perform Successful Logon:**
   - Correct credentials for any domain user



3. Check local event log in client1

Connect event viewer as administrator. View 4265 events



+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4625

Version 0

Level 0

Task 12544

Opcode 0

Keywords 0x8010000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:52:28.7743802Z

EventRecordID 44435

- Correlation

[ActivityID] {bb6a734c-cd00-0001-ad74-6abb00cddb01}

- Execution

[ProcessID] 804
[ThreadID] 4104

Channel Security

Computer Client1.vlabs1.com

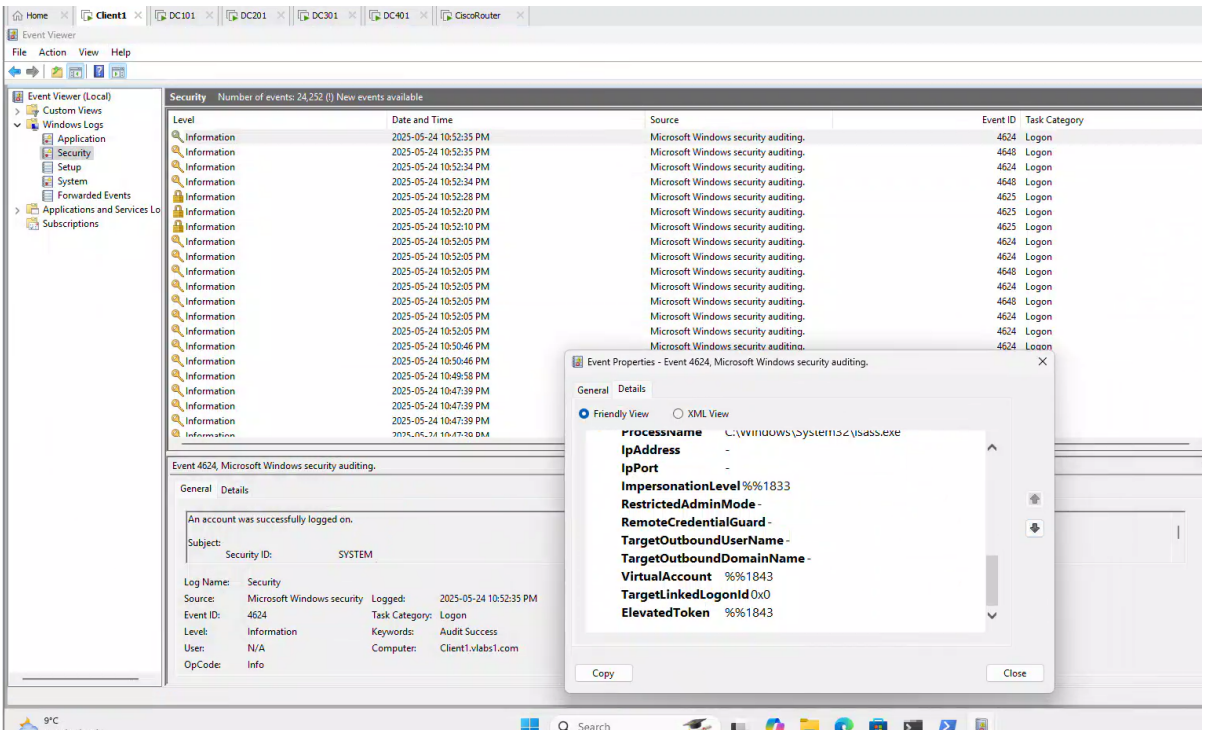
Security

- EventData

SubjectUserSid S-1-5-18
SubjectUserName CLIENT1$
SubjectDomainName VLABS1

SubjectLogonId 0x3e7
TargetUserSid S-1-0-0
TargetUserName aloyse.dupont@vlabs1.com
TargetDomainName -
Status 0xc000006d
FailureReason %%2313
SubStatus 0xc000006a
LogonType 2
LogonProcessName User32
AuthenticationPackageName Negotiate
WorkstationName CLIENT1
TransmittedServices -
LmPackageName -
KeyLength 0
ProcessId 0x66c
ProcessName C:\Windows\System32\svchost.exe
IpAddress 127.0.0.1
IpPort 0

Successful connection 4264



+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4624

Version 3

Level 0

Task 12544

Opcode 0

Keywords 0x8020000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:52:35.2079530Z

EventRecordID 44439

Correlation

- Execution

[ProcessID] 804
[ThreadID] 4136

Channel Security

Computer Client1.vlabs1.com

Security

- EventData

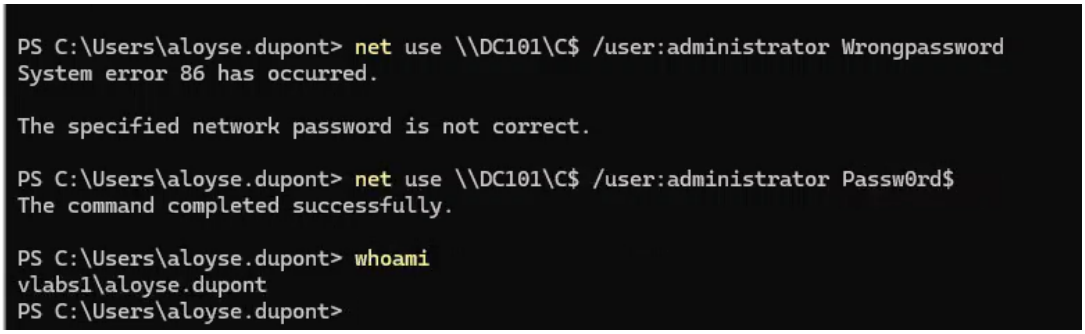
SubjectUserSid S-1-5-18
SubjectUserName CLIENT1$
SubjectDomainName VLABS1
SubjectLogonId 0x3e7
TargetUserSid S-1-5-21-1268601764-4050707287-4025116504-1760

TargetUserName aloyse.dupont
TargetDomainName VLABS1
TargetLogonId 0x8ec487
LogonType 7
LogonProcessName Negotiat
AuthenticationPackageName Negotiate
WorkstationName CLIENT1
LogonGuid {473595ac-f969-67fb-4ae8-c3de87a9fcb1}
TransmittedServices -
LmPackageName -
KeyLength 0
ProcessId 0x324
ProcessName C:\Windows\System32\lsass.exe
IpAddress -
IpPort -
ImpersonationLevel %%1833
RestrictedAdminMode -
RemoteCredentialGuard -
TargetOutboundUserName -
TargetOutboundDomainName -
VirtualAccount %%1843
TargetLinkedLogonId 0x0
ElevatedToken %%1843

7.2.2.2 Event generated in client 1 towards DC101

1. **Try to connect with bad password in client1**

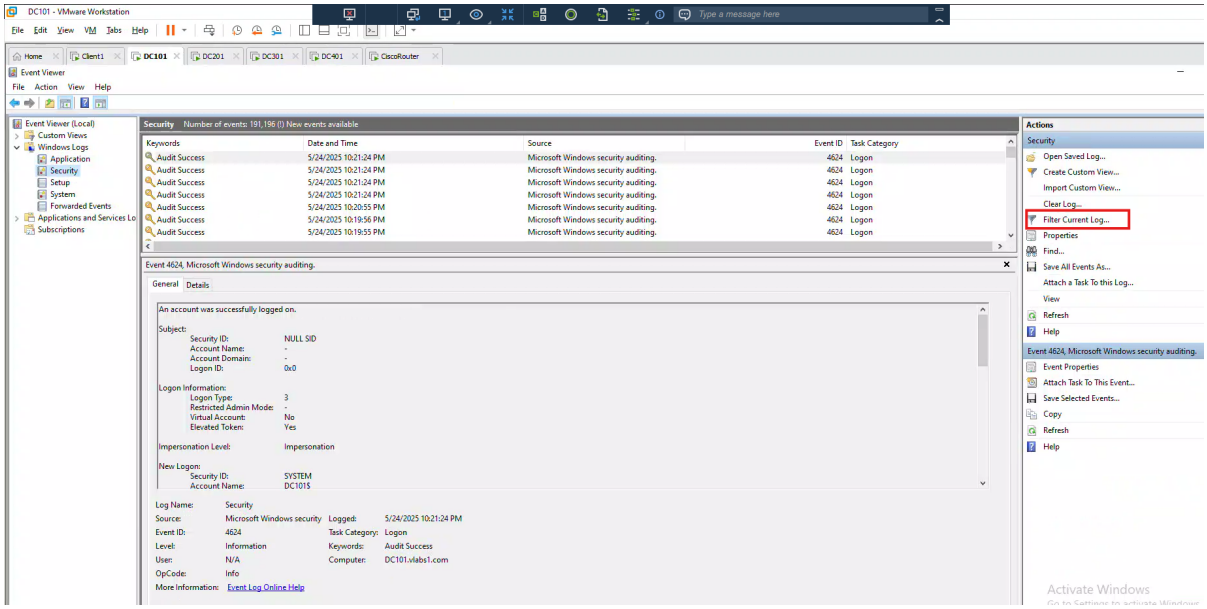
   Followed by a successful login towards DC101



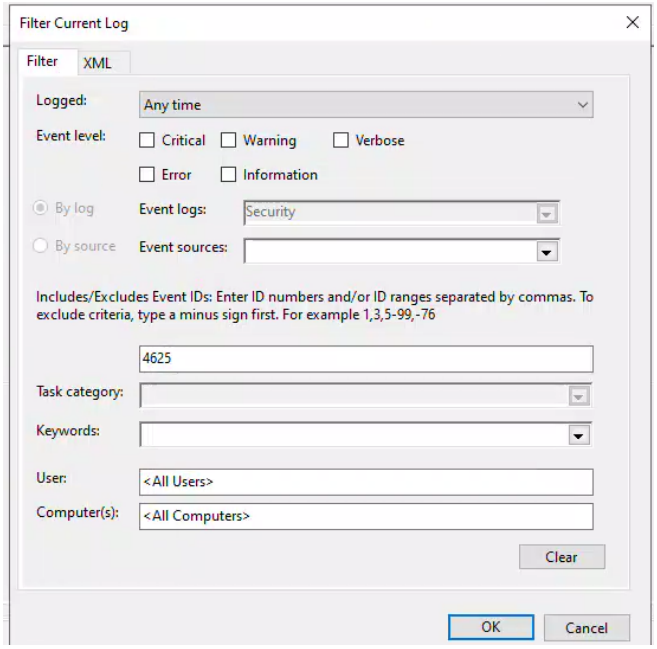
2. Check Security Logs (On DC101)

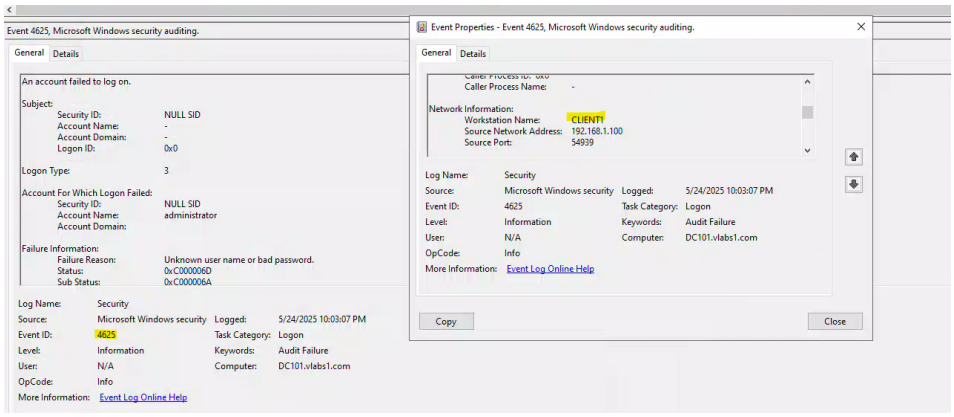
a) **Open Event Viewer:**

- Run eventvwr.msc
- Navigate to: Windows Logs → Security



b) **Filter for Relevant Events:**
   - Click **"Filter Current Log"**
   - Enter Event IDs:
     - **4624** (Successful logon)
     - **4625** (Failed logon)
   - Click **OK**



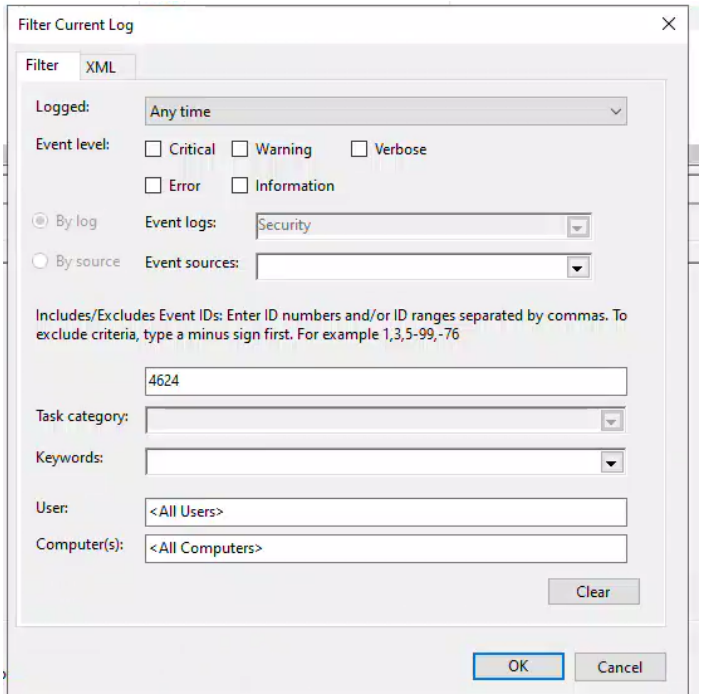


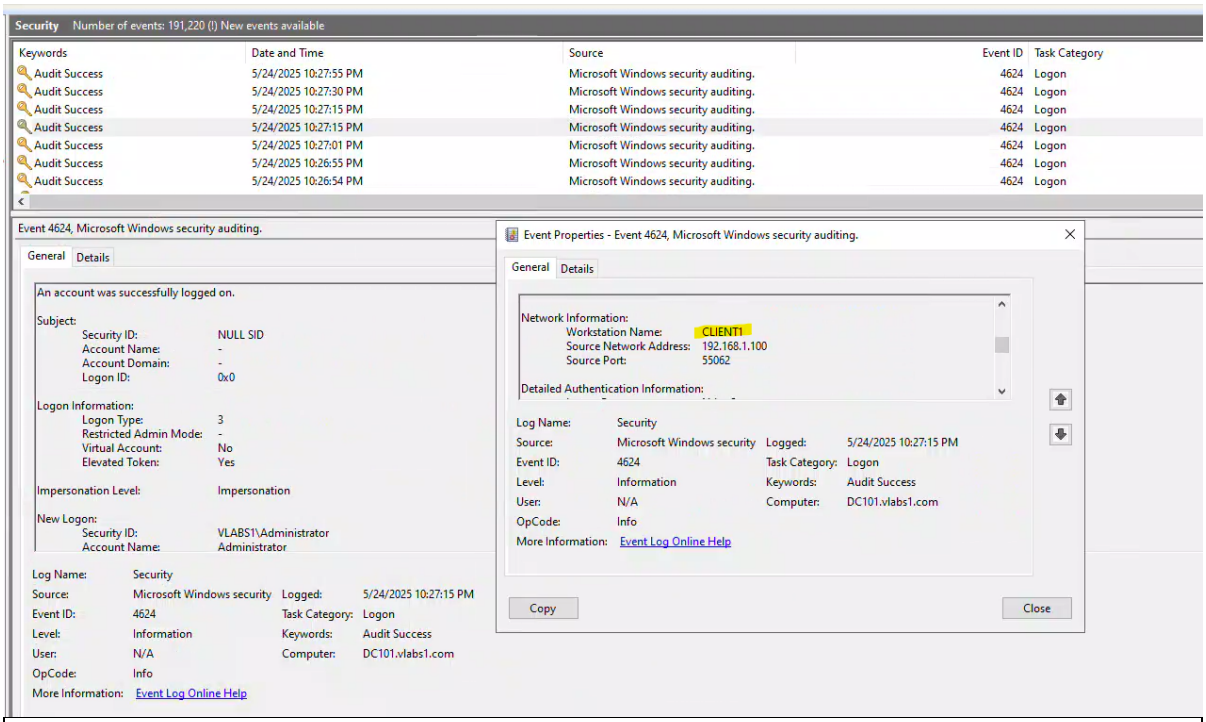
c) **Verify Events:**
   - For **failed attempts** (4625):
     - Check "Account Name" matches test user
     - Verify "Failure Reason" appears

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-
4994-a5ba-3e3b0328c30d}" />
 <EventID>4625</EventID>
 <Version>0</Version>
```

```
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8010000000000000</Keywords>
  <TimeCreated SystemTime="2025-05-25T02:03:07.7343499Z" />
  <EventRecordID>258393</EventRecordID>
  <Correlation />
  <Execution ProcessID="744" ThreadID="864" />
  <Channel>Security</Channel>
  <Computer>DC101.vlabs1.com</Computer>
  <Security />
  </System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-0-0</Data>
  <Data Name="SubjectUserName">-</Data>
  <Data Name="SubjectDomainName">-</Data>
  <Data Name="SubjectLogonId">0x0</Data>
  <Data Name="TargetUserSid">S-1-0-0</Data>
  <Data Name="TargetUserName">administrator</Data>
  <Data Name="TargetDomainName" />
  <Data Name="Status">0xc000006d</Data>
  <Data Name="FailureReason">%%2313</Data>
  <Data Name="SubStatus">0xc000006a</Data>
  <Data Name="LogonType">3</Data>
  <Data Name="LogonProcessName">NtLmSsp</Data>
  <Data Name="AuthenticationPackageName">NTLM</Data>
  <Data Name="WorkstationName">CLIENT1</Data>
  <Data Name="TransmittedServices">-</Data>
  <Data Name="LmPackageName">-</Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x0</Data>
  <Data Name="ProcessName">-</Data>
  <Data Name="IpAddress">192.168.1.100</Data>
  <Data Name="IpPort">54939</Data>
  </EventData>
  </Event>
```

- For **successful logons** (4624):
  - Confirm "Logon Type" (2=Interactive, 3=Network)
  - Verify workstation name is Client1





+ System

- Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-a5ba-3e3b0328c30d}

EventID 4624

Version 2

Level 0

Task 12544

Opcode 0

Keywords 0x8020000000000000

- TimeCreated

[SystemTime] 2025-05-25T02:27:15.6924035Z

EventRecordID 258475

Correlation

- Execution

[ProcessID] 744
[ThreadID] 864

Channel Security

Computer DC101.vlabs1.com

Security

- EventData

SubjectUserSid S-1-0-0
SubjectUserName -
SubjectDomainName -
SubjectLogonId 0x0
TargetUserSid S-1-5-21-1268601764-4050707287-4025116504-500
TargetUserName Administrator
TargetDomainName VLABS1
TargetLogonId 0x54277a0
LogonType 3
LogonProcessName NtLmSsp
AuthenticationPackageName NTLM

WorkstationName CLIENT1
LogonGuid {00000000-0000-0000-0000-000000000000}
TransmittedServices -
LmPackageName NTLM V2
KeyLength 128
ProcessId 0x0
ProcessName -
IpAddress 192.168.1.100
IpPort 55062
ImpersonationLevel %%1833
RestrictedAdminMode -
TargetOutboundUserName -
TargetOutboundDomainName -
VirtualAccount %%1843
TargetLinkedLogonId 0x0
ElevatedToken %%1842

Key Event Details

Event ID	Description	Important Fields
4624	Successful logon	- TargetUserName - WorkstationName - LogonType
4625	Failed logon	- TargetUserName - FailureReason - SourceNetworkAddress

8 Task 6: Managing Security Templates

- Create a security template named **OpenSSH_Auth.**
- In this template, modify **OpenSSH Authentication Agent** under **System Services** to start **automatically.**
- Import this **new template** into a new GPO named **OpenSSHAuth.**
- Link the GPO to **DomainControllers OU**.
- Run **gpupdate /force** on **DC101** to apply changes.

- Restart **DC101** and verify in **Services** that **OpenSSH Authentication Agent** has started.

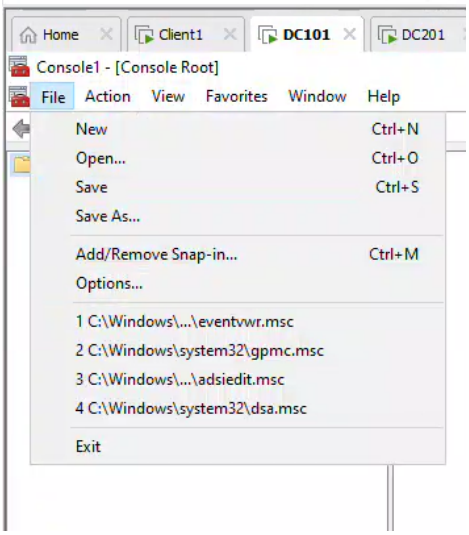
8.1 Objective:

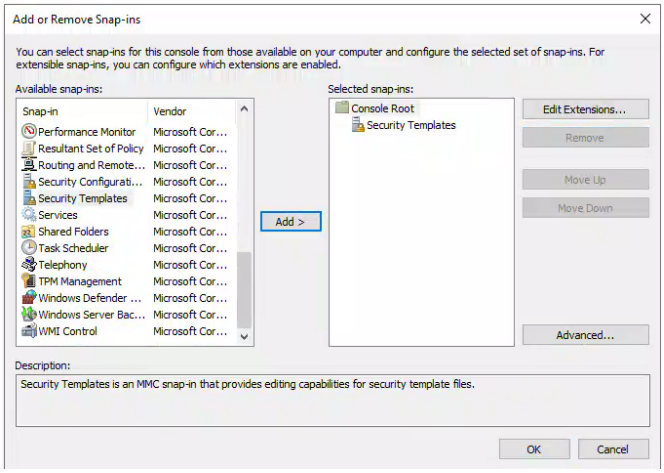
Create and deploy a security template to configure OpenSSH Authentication Agent service startup via Group Policy.

8.2 Steps

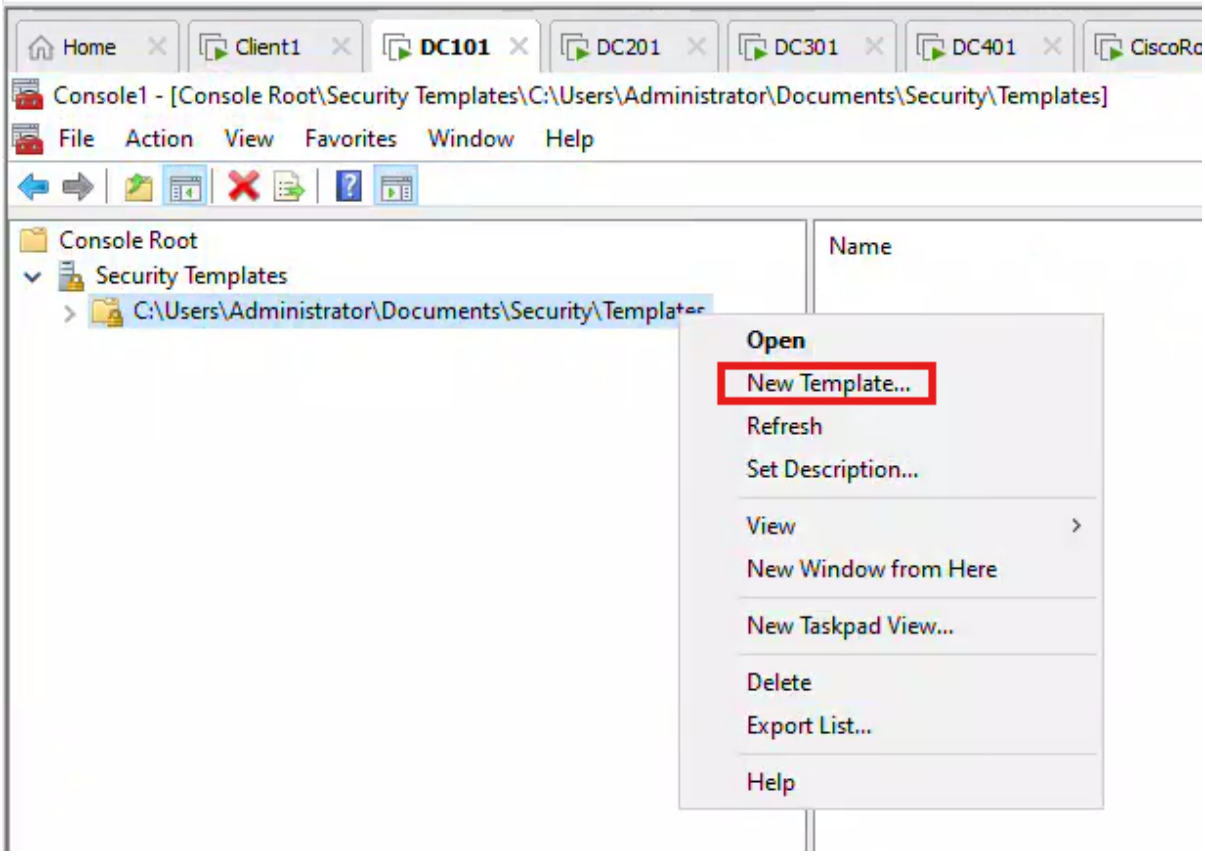
1. Create Security Template

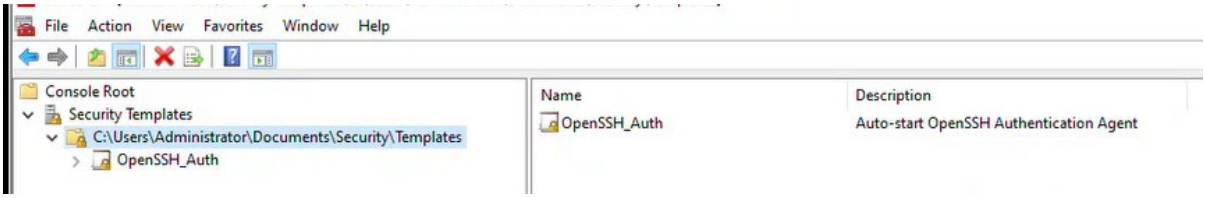
1. **On DC101 (Domain Controller):**
    - Open **Microsoft Management Console** (mmc.exe)
    - Go to **File → Add/Remove Snap-in**
    - Add **Security Templates** → Click **OK**





2. **Create New Template:**
    - In the left pane, expand: Security Templates → C:\Users\Administrator\Documents\Security\Templates
    - Right-click → **New Template**
    - Name: OpenSSH_Auth
    - Description: "Auto-start OpenSSH Authentication Agent"

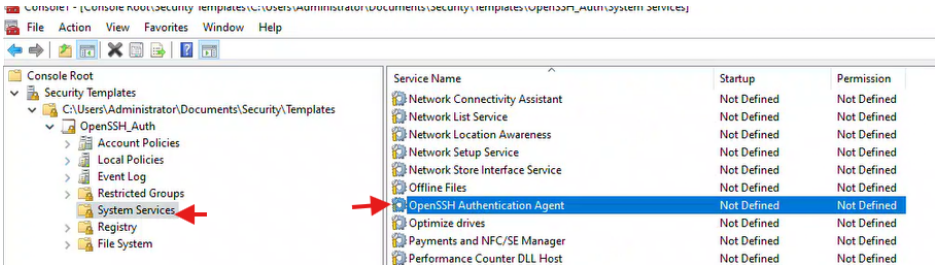


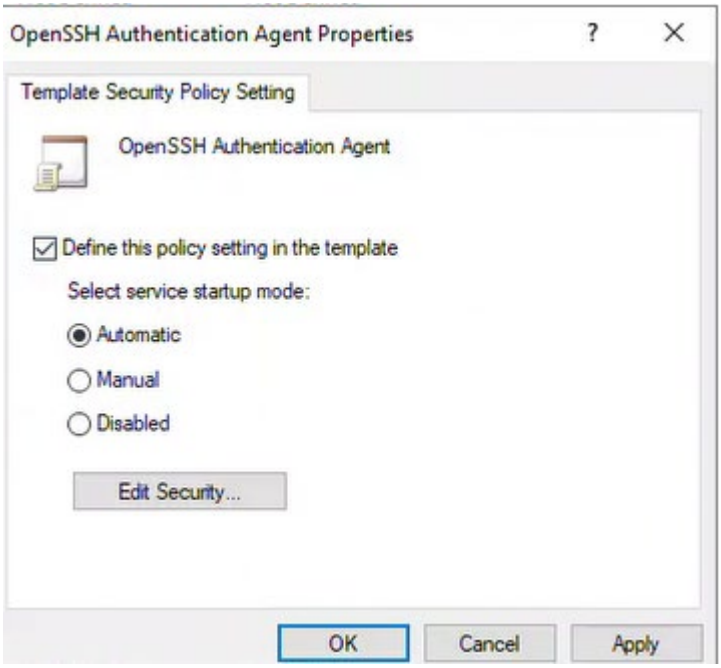


2. Configure OpenSSH Service

1. In the Security Template:

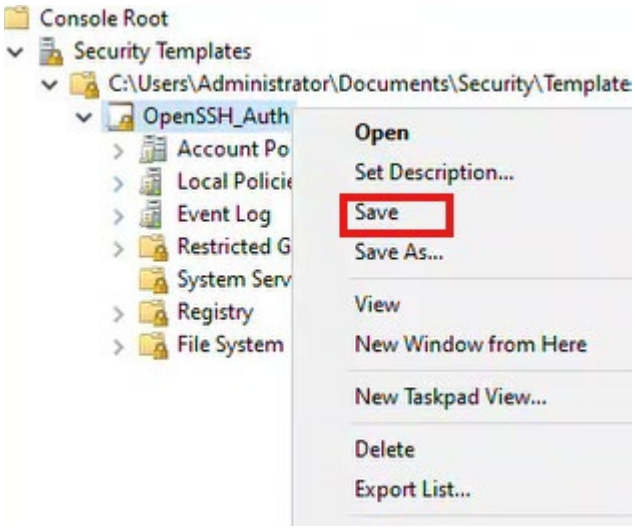
- Navigate to: OpenSSH_Auth → System Services
    - Find **"OpenSSH Authentication Agent"**
    - Double-click → Select **"Define this policy setting"**
    - Set to: **Automatic**
    - Click **OK**





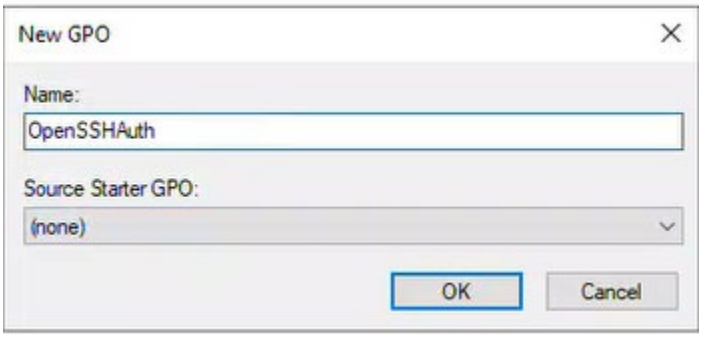
3. Save Template

- Right-click OpenSSH_Auth → **Save**

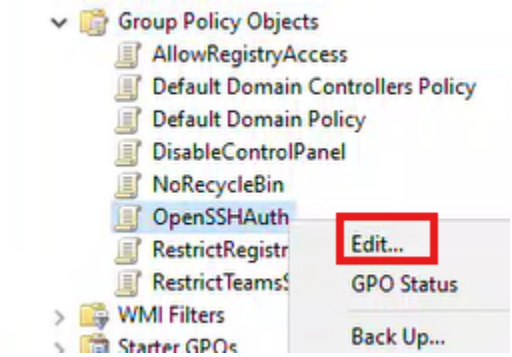


4. Create and Configure GPO

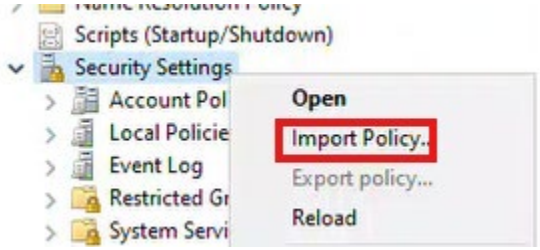
1. **In GPMC (**gpmc.msc**):**
    - Right-click **Group Policy Objects** → **New**
    - Name: OpenSSHAuth → Click **OK**



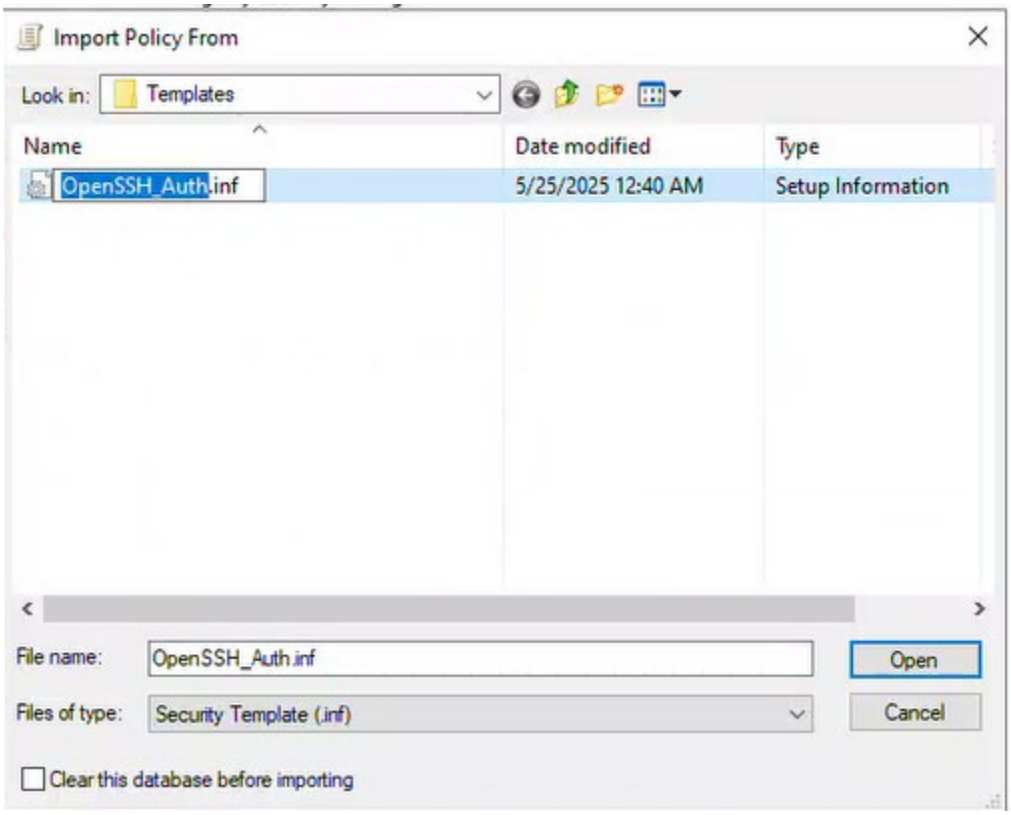
2. **Import Template:**
    - Right-click → **Edit**



    - Navigate to: Computer Configuration → Policies → Windows Settings → Security Settings
    - Right-click → **Import Policy**

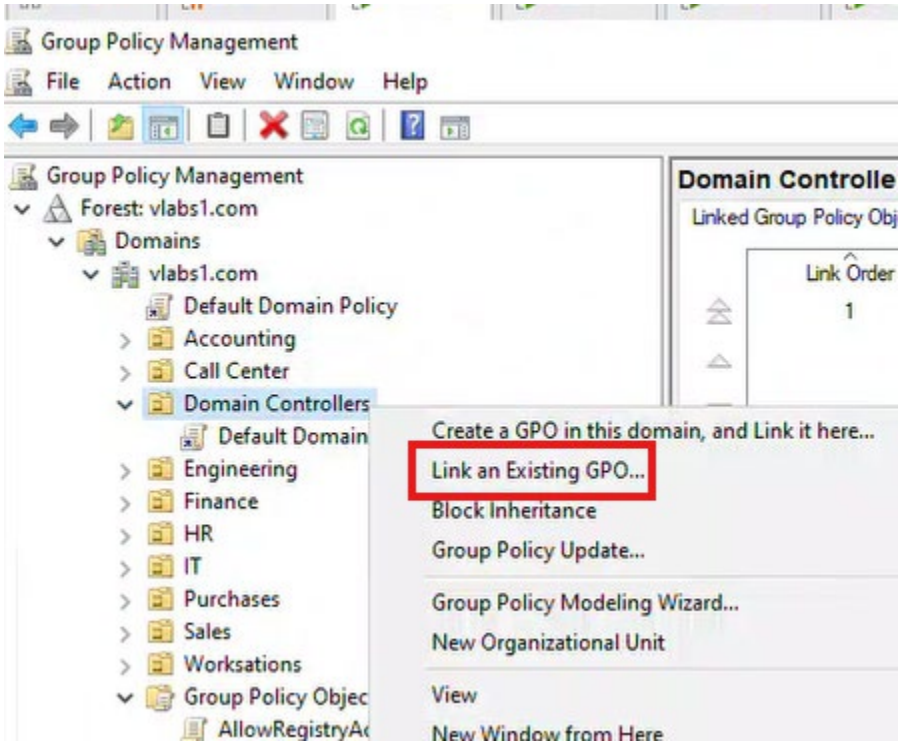


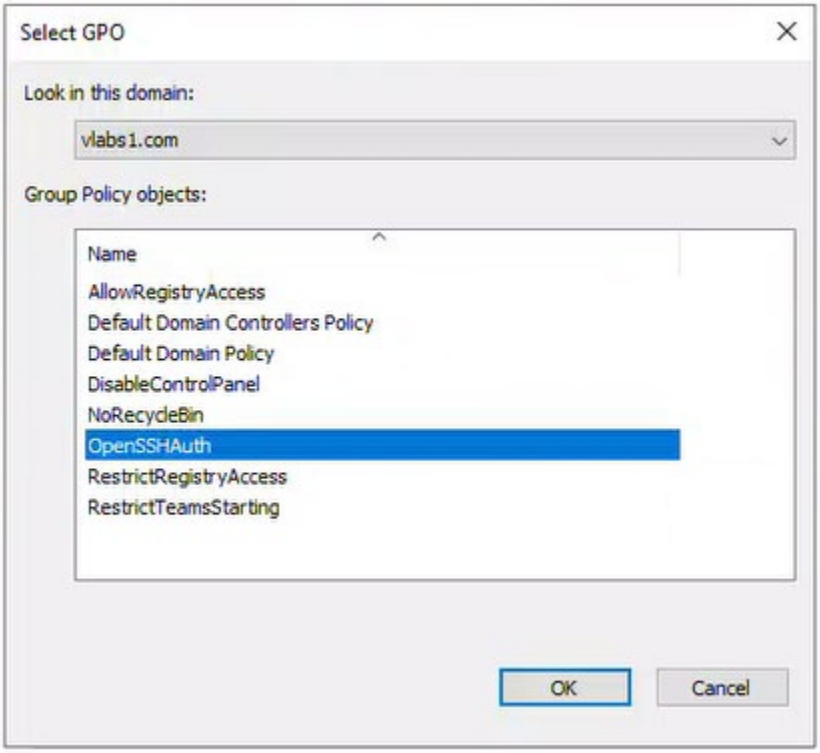
    - Browse to saved template (OpenSSH_Auth.inf)
    - Click **Open**



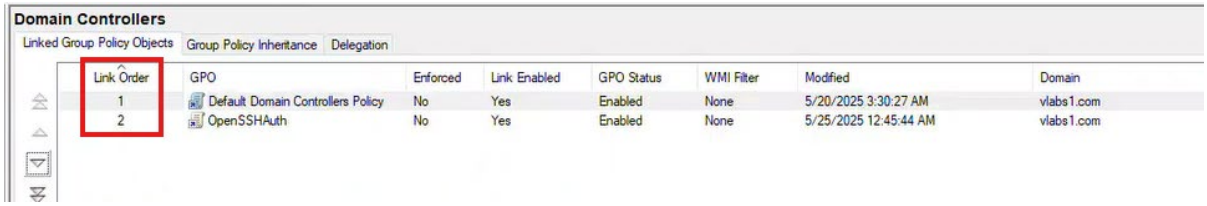
5. Link GPO to Domain Controllers

1. In GPMC:
    - Navigate to: Domain Controllers OU
    - Right-click → **Link an Existing GPO**
    - Select OpenSSHAuth → Click **OK**





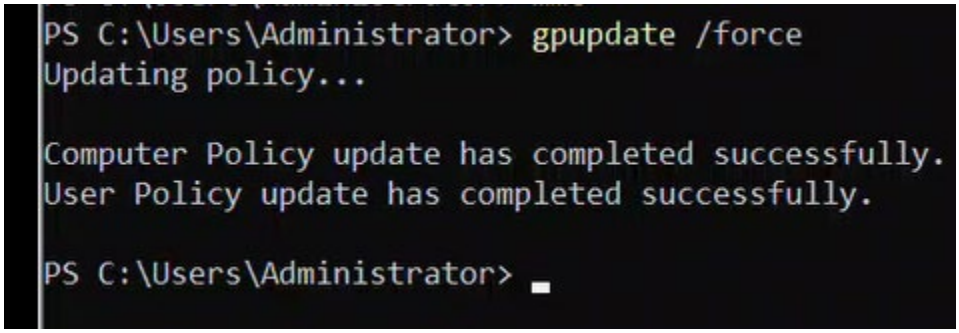
2. **Verify Link Order:**
    - Ensure no conflicting policies have higher precedence



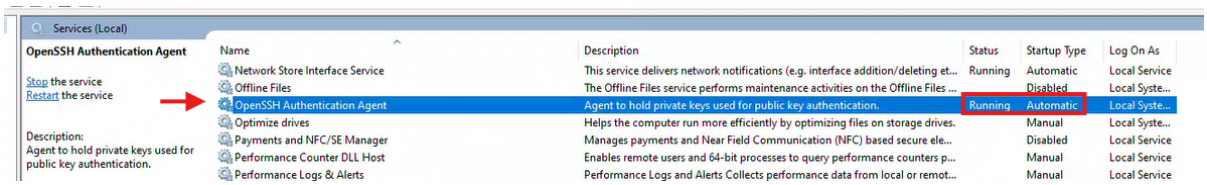
6. Apply Policy and Verify

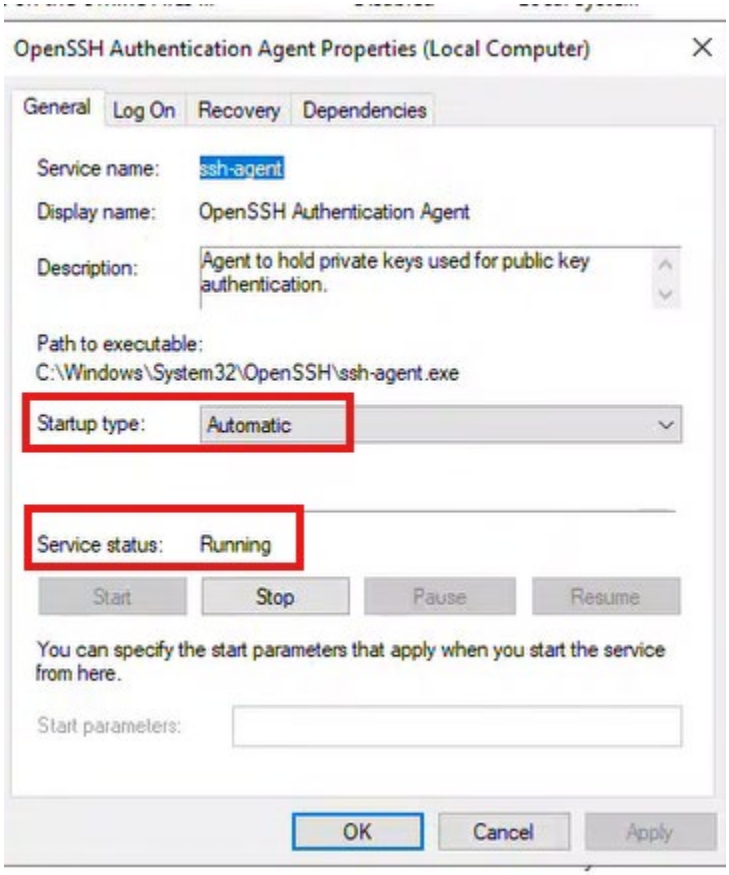
1. **Force Policy Update:**
    - On DC101, run Command Prompt as Administrator:

      gupdate /force
    - Wait for confirmation: Computer Policy update has completed successfully



2. **Restart DC101:**
3. **Verify Service Status:**
    - After reboot:
        - Open **Services** (services.msc)
        - Locate **"OpenSSH Authentication Agent"**
        - Verify:
            - **Startup Type:** Automatic
            - **Status:** Running





9 Task 7: Configuring Folder Redirection

- Use **DC301** as the file server.
- Create a shared folder: **\\DC301\UserData** to the **HR** Group (r & w).
- Create a new **GPO** named **SharedUserData**
- Use Basic redirection to Create a Folder for Each User Under the Root Path.
- Redirect **Documents** and **Desktop** to the user's respective folder under **\\DC301\UserData.**
- Link GPO to **HR** OU,
- Run **gpupdate /force** to apply changes.
- Test with **a user** from the **HR** OU.

9.1 Objective

Redirect HR users' Documents and Desktop folders to a centralized file server location with user-specific subfolders.

9.2 Steps

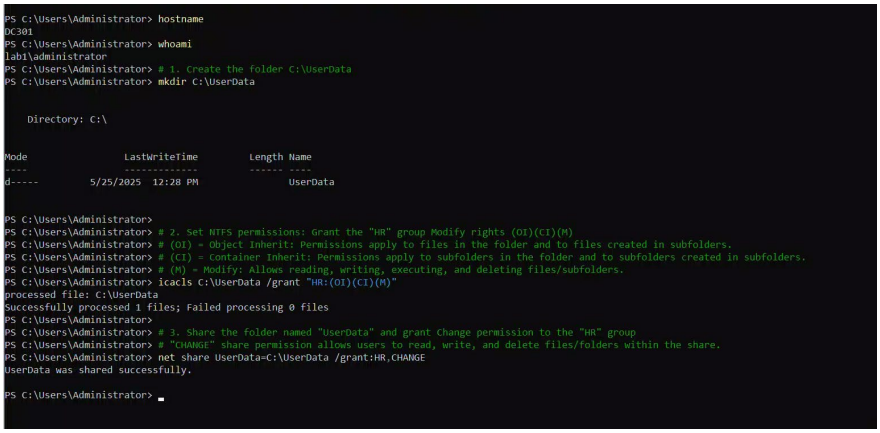
9.2.1 Prepare File Server (DC301)

Objective: Create the C:\UserData folder on DC301, set appropriate NTFS permissions, and then create a network share for it, ensuring only the HR group has the necessary access.

a) **Create Shared Folder:**

Open PowerShell or Command Prompt as an administrator. (This is crucial for creating folders under the root, modifying NTFS permissions, and creating network shares.)

```
# 1. Create the folder C:\UserData
mkdir C:\UserData

# 2. Set NTFS permissions: Grant the "HR" group Modify rights (OI)(CI)(M)
# (OI) = Object Inherit: Permissions apply to files in the folder and to files created in subfolders.
# (CI) = Container Inherit: Permissions apply to subfolders in the folder and to subfolders created in subfolders.
# (M) = Modify: Allows reading, writing, executing, and deleting files/subfolders.
icacls C:\UserData /grant "HR:(OI)(CI)(M)"

# 3. Share the folder named "UserData" and grant Change permission to the "HR" group
# "CHANGE" share permission allows users to read, write, and delete files/folders within the share.
net share UserData=C:\UserData /grant:HR,CHANGE
```

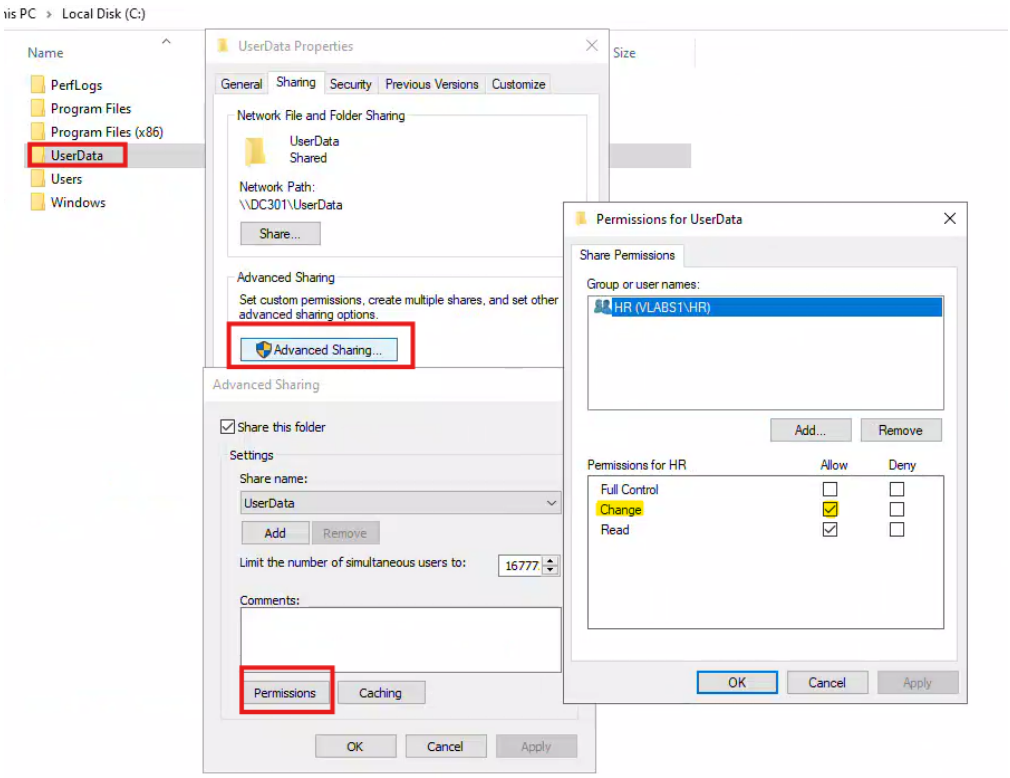


b) **Verify Permissions:**

After running the commands, you can manually verify the permissions by right-clicking on the C:\UserData folder on DC301.

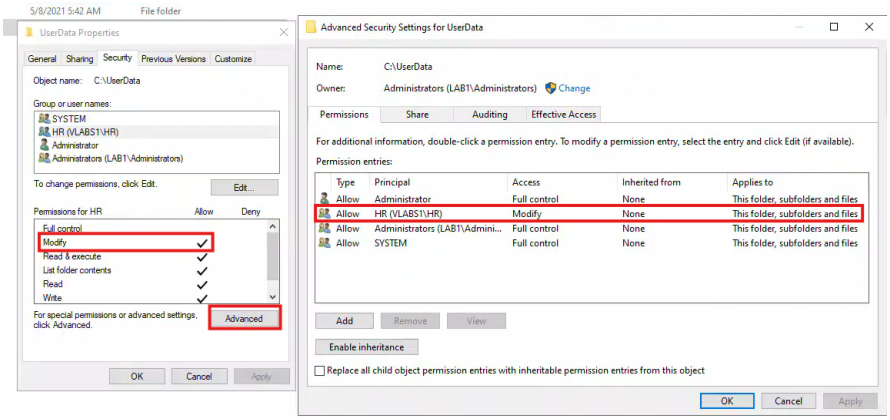
- Right-click folder → Properties → Sharing → Advance Sharing → Permissions:

- Ensure the HR group has "**Change**" selected.



- Security tab → NTFS permissions:

  Go to **Properties** -> **Security** tab -> Advance. Ensure the HR group has **"Modify"** permissions, and that it applies to "This folder, subfolders and files".



9.2.2 Create Folder Redirection GPO (DC101)

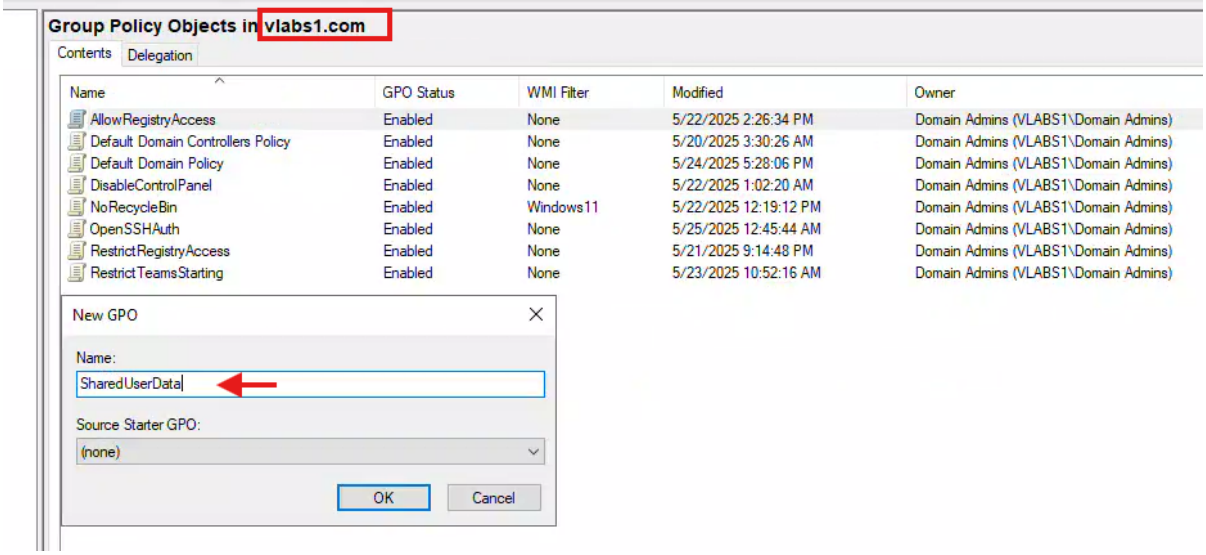
Objective: Create a new GPO named SharedUserData and configure it to redirect users' Documents and Desktop folders to their respective subfolders under **\\DC301\UserData**.

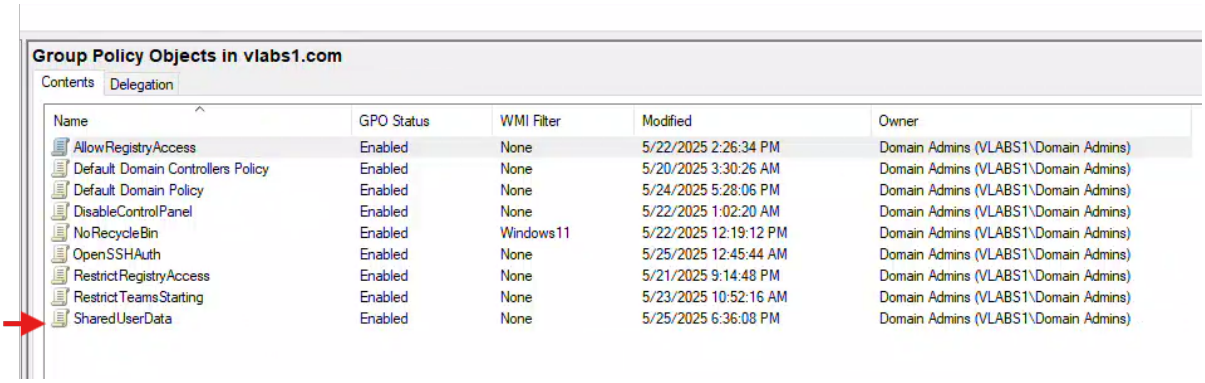
a) **Open Group Policy Management Console (GPMC):**

On a Domain Controller **DC101**, search for "Group Policy Management" in the Start Menu and open it.

b) **Create the New GPO (SharedUserData):**

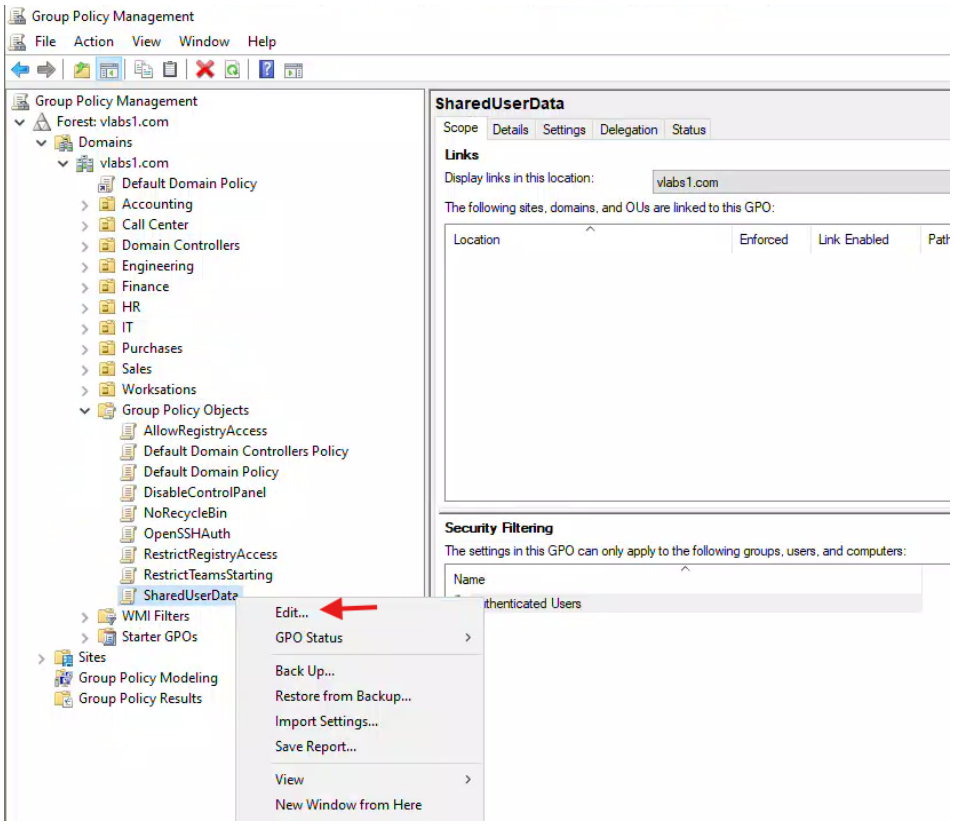
1. In the left-hand pane of GPMC, expand your forest (e.g., vlabs1.com).
2. Expand **Domains**.
3. Expand your domain (vlabs1.com).
4. Right-click on **"Group Policy Objects"** (below your domain name).
5. Select **"New"**.
6. In the "New GPO" dialog, type SharedUserData as the GPO name.
7. Click **OK**.





c) **Edit the New GPO and Navigate to Folder Redirection:**

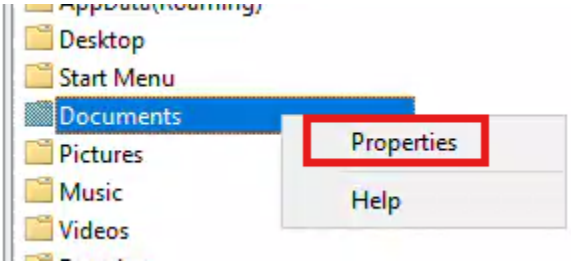
- In the GPMC, under "Group Policy Objects", find your newly created SharedUserData GPO.
- Right-click on SharedUserData and select **"Edit..."**. This will open the Group Policy Management Editor.
- In the editor, navigate through the tree: User Configuration -> Policies -> Windows Settings -> Folder Redirection



9.2.3 Configure Documents Redirection (DC101)

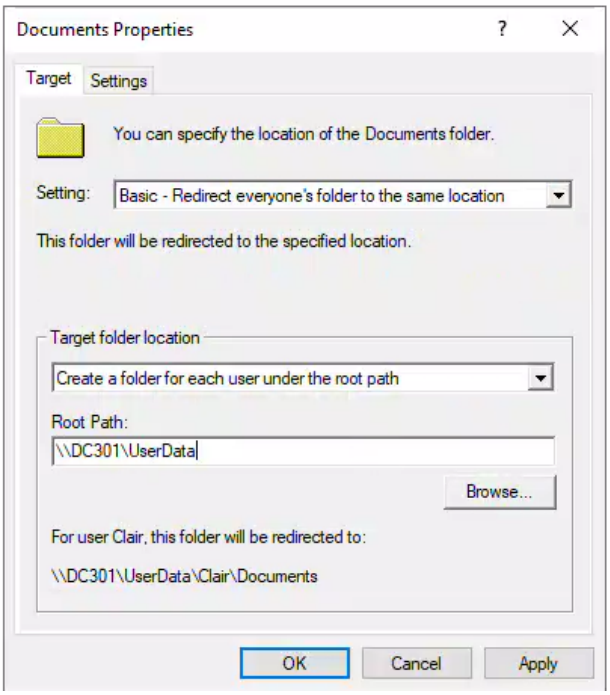
9.2.3.1 Documents

a) Under Folder Redirection, right-click on **"Documents"** and select **"Properties"**.



b) On the "Target" tab:

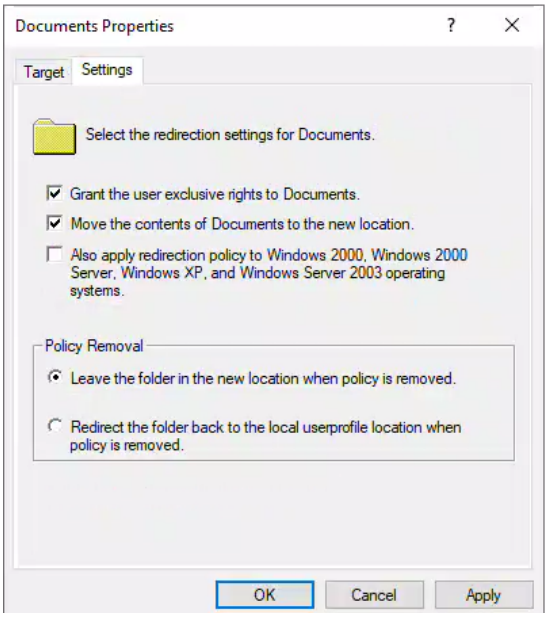
- From the "Setting:" drop-down menu, choose: **"Basic - Redirect everyone's folder to the same location"**.
- In the "Root Path:" field, enter the UNC path to your shared folder: \\DC301\UserData
- Ensure the checkbox **"Create a folder for each user under the root path"** is selected. (This is crucial for creating \\DC301\UserData\username\Documents)

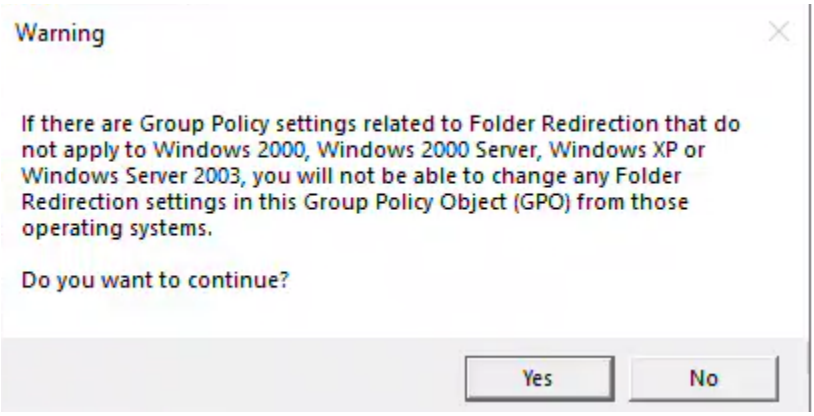


c) Click on the **"Settings"** tab:

- Make sure **"Move the contents of Documents to the new location"** is selected (this is usually the default).
- Check the box for **"Grant the user exclusive rights to Documents"**.
- Uncheck (if checked) **"Redirect the folder back to the local userprofile location when policy is removed"**.

d) Click **"Apply"**, then **"OK"**. You might get a warning about exclusive rights; click **"Yes"** to confirm.

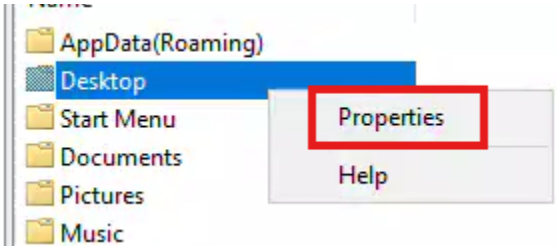




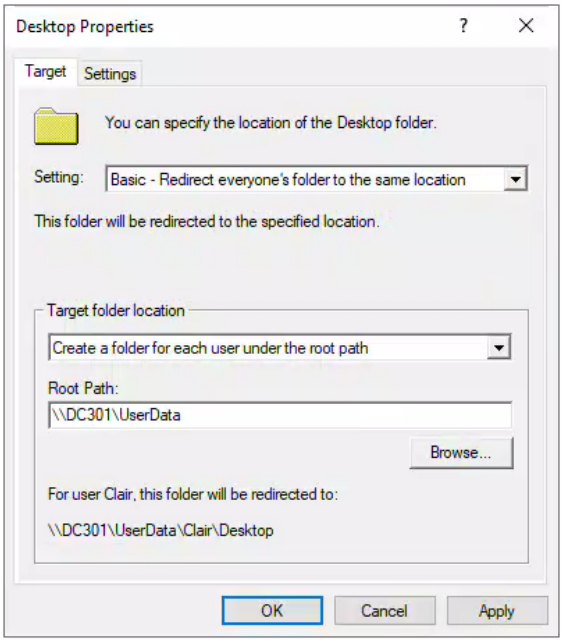
9.2.3.2 Desktop

a) **Ensure you are still in the Group Policy Management Editor** for the SharedUserData GPO.
   - You should be navigated to: User Configuration -> Policies -> Windows Settings -> Folder Redirection.

b) **Right-click on "Desktop"** (under Folder Redirection in the left pane).
   - From the context menu, select **"Properties"**.

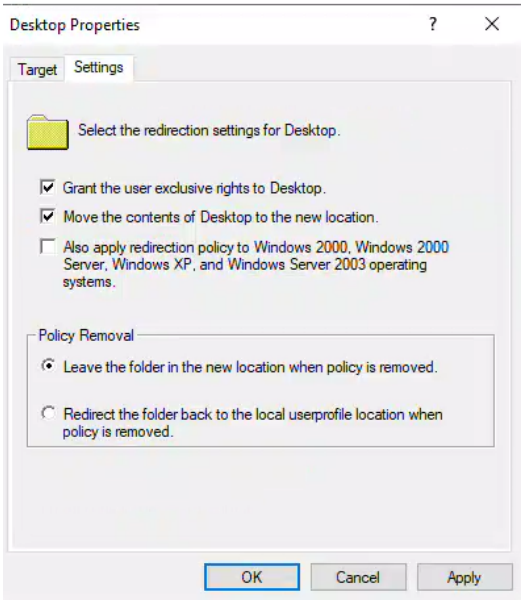


c) **Configure the "Target" Tab:**
   - In the "Desktop Properties" window, go to the **"Target"** tab.
   - From the "Setting:" drop-down menu, select: **"Basic - Redirect everyone's folder to the same location"**.
   - In the "Root Path:" text field, type the UNC path to your shared folder: \\DC301\UserData
   - **Verify** that the checkbox directly below "Root Path:" which says **"Create a folder for each user under the root path"** is **checked**. (This will ensure that a structure like \\DC301\UserData\<username>\Desktop is created).

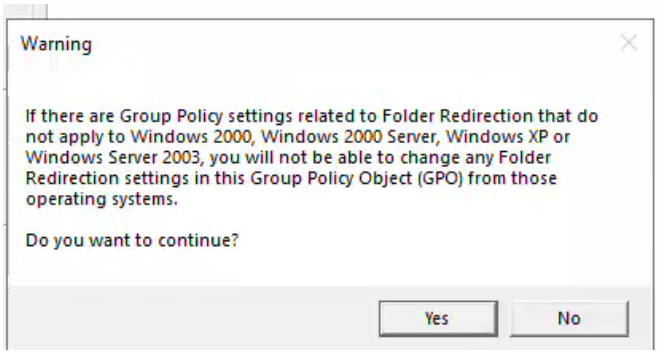


d) **Configure the "Settings" Tab:**
   - Click on the **"Settings"** tab.

- Under "Policy Removal", ensure that:
  - **"Move the contents of Desktop to the new location"** is selected (this is typically the default and moves existing files).
  - The checkbox for **"Grant the user exclusive rights to Desktop"** is **checked**. (This enhances security by ensuring only the user has full control over their redirected folder).
  - The checkbox for **"Redirect the folder back to the local userprofile location when policy is removed"** is **unchecked**. (This means if the GPO is ever removed, the Desktop contents will remain on the network share, preventing data loss).



e) **Apply and Confirm:**
   - Click **"Apply"**.
   - If a warning message appears (often about granting exclusive rights), click **"Yes"** to proceed.
   - Click **"OK"** to close the Desktop Properties window.



You have now configured both Documents and Desktop folder redirection for the SharedUserData GPO. You can now **close** the Group Policy Management Editor.

9.3 Link GPO to HR OU (DC101)

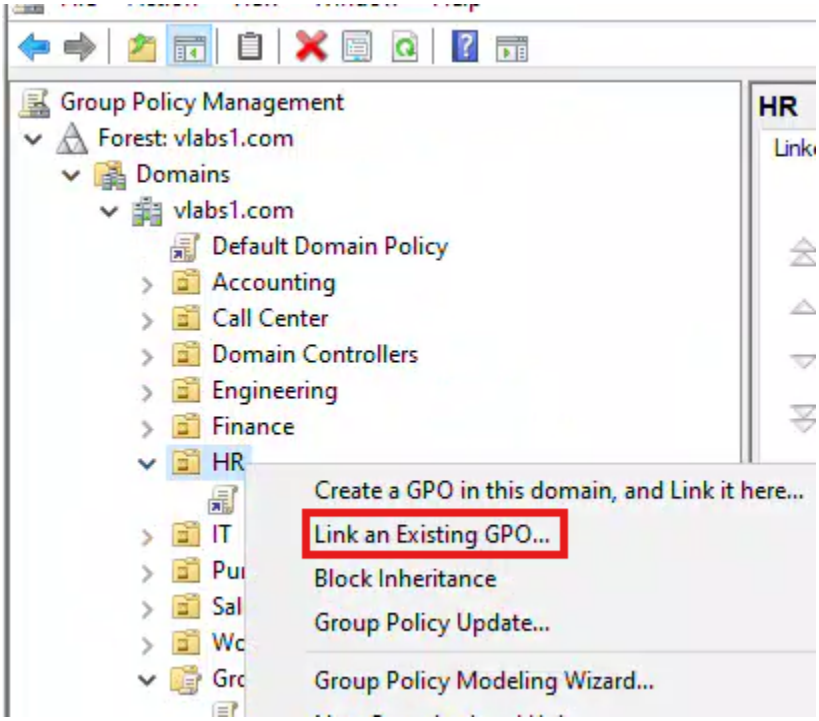
Perform these steps on DC101 or any machine with GPMC installed and administrative access to the domain

Objective: Link the SharedUserData GPO to the HR Organizational Unit (OU) so that its settings apply to users within that OU.

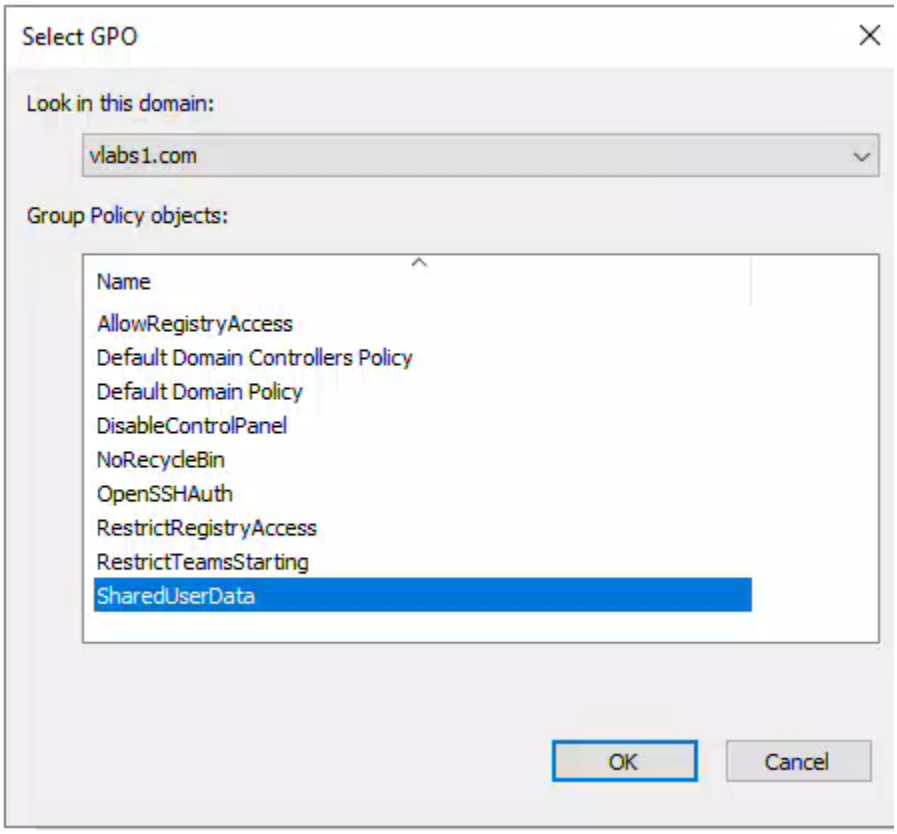
Perform these steps on **DC101**

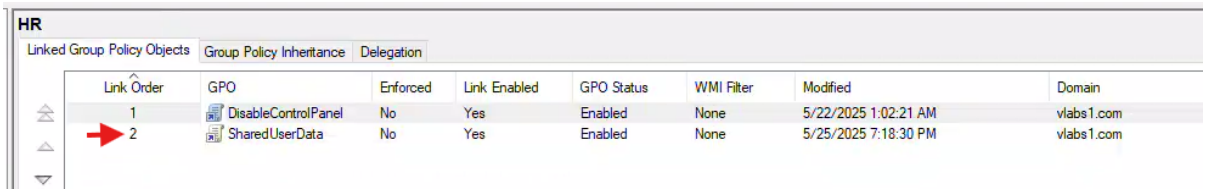
A. **In Group Policy Management Console (GPMC):**

a) In the left-hand pane, navigate to your domain (`vlabs1.com`).
b) Expand your domain and locate the **HR OU**.
c) Right-click on the **HR OU**.
d) Select **"Link an Existing GPO..."**.



e) In the "Select GPO" dialog, choose **"SharedUserData"** from the list.
f) Click **"OK"**.





B. **Verify Link Order:**

- With the **HR OU** still selected in the left-hand pane of GPMC, click on the **"Linked Group Policy Objects"** tab in the right-hand pane.
- Observe the **"Link Order"** column.

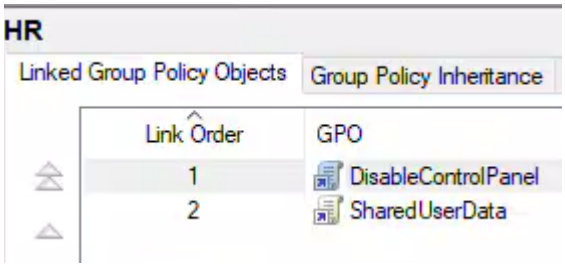
Is this the right order?

For **Folder Redirection**, the link order with `DisableControlPanel` usually doesn't create a direct conflict. Folder redirection settings are in a different area of Group Policy than Control Panel restrictions.

- `DisableControlPanel` typically configures user interface restrictions (User Configuration -> Policies -> Administrative Templates -> Control Panel).
- `SharedUserData` configures folder redirection (User Configuration -> Policies -> Windows Settings -> Folder Redirection).

These are separate policy areas, so it's **highly unlikely** that `DisableControlPanel` would override or interfere with your folder redirection settings.

Therefore, in this specific scenario, leaving the order as `DisableControlPanel` at 1 and `SharedUserData` at 2 is likely perfectly fine. Your folder redirection should still apply as intended.

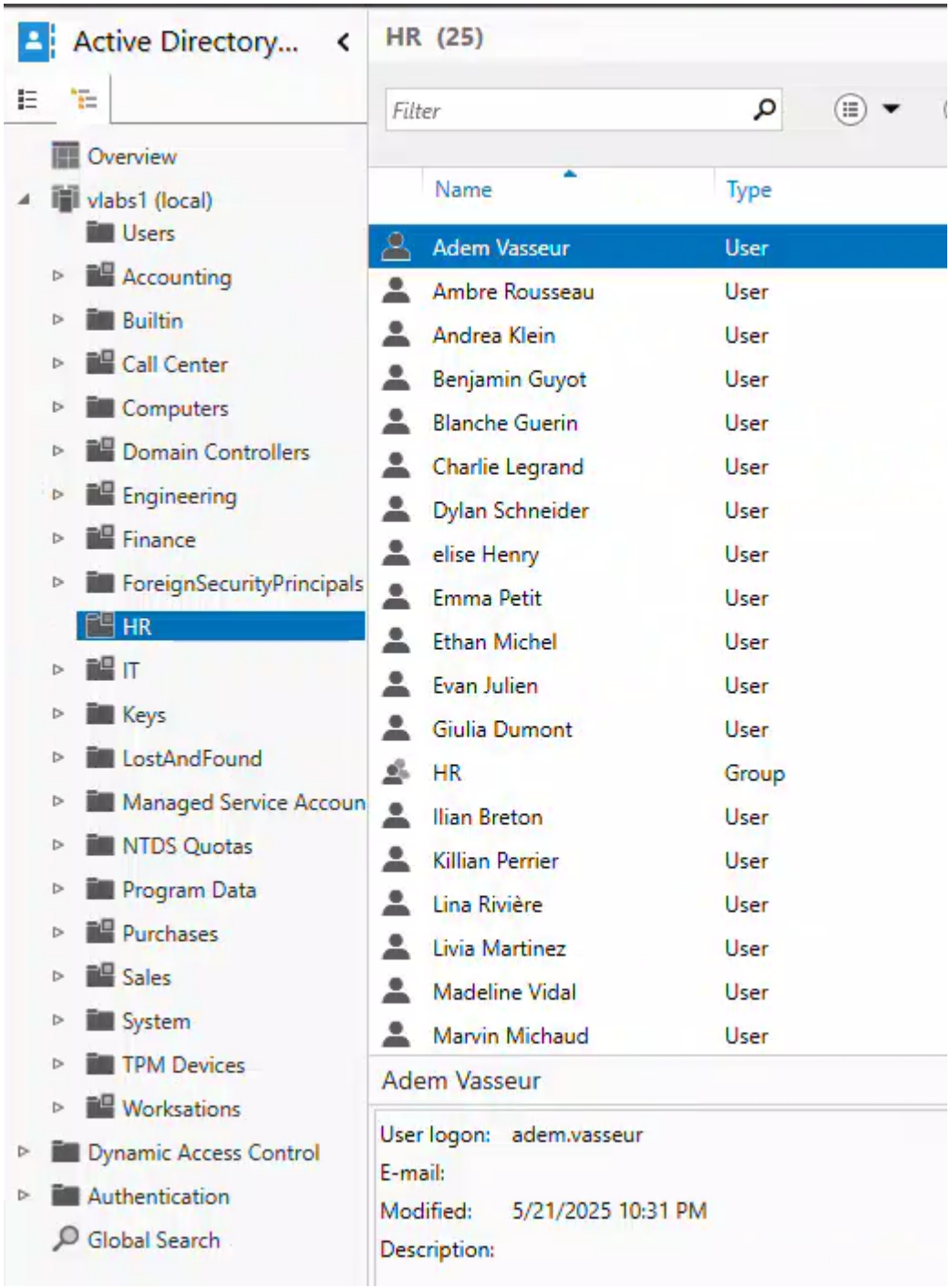


9.4 Apply and Test

Objective: Force the policy update on Client1, verify the folder redirection, and test file operations.

9.4.1 Verify HR users (DC101)

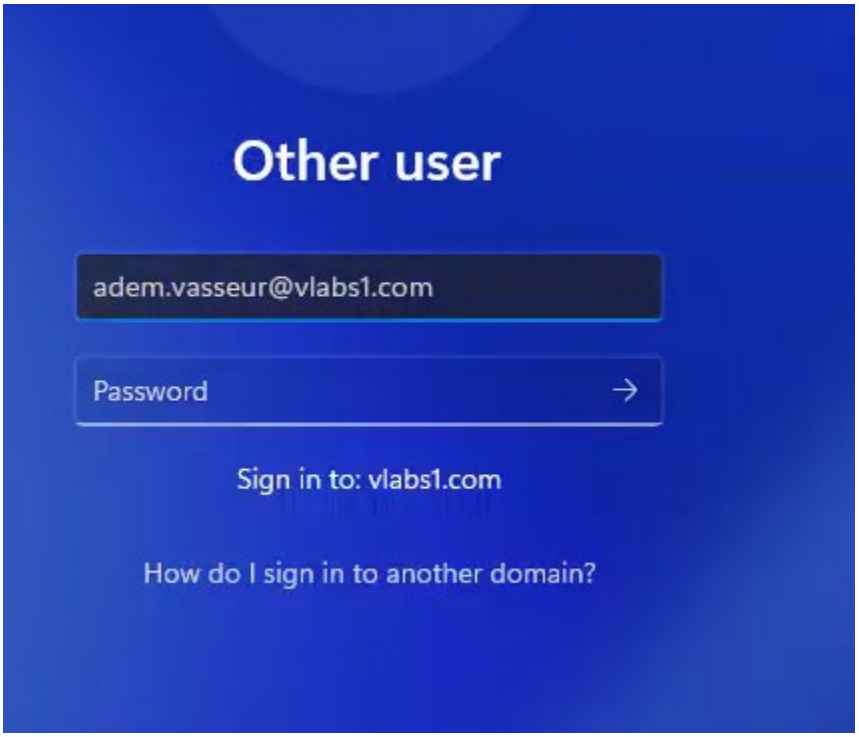
On DC101 open Active Directory Administrative Center



9.4.2 Client1

Action (Perform these steps on Client1, logged in as an HR user):

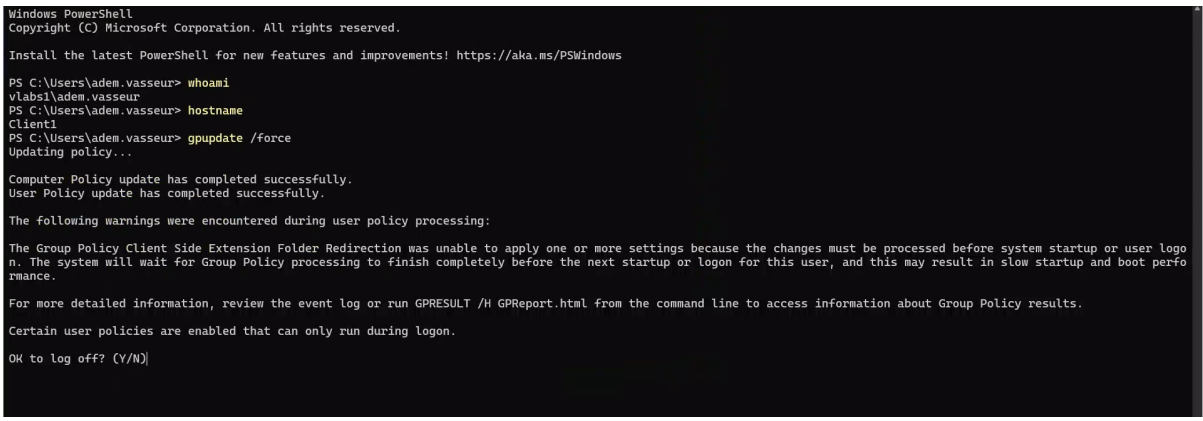
1. **Force Policy Update (On Client1):**
    - Log in to **Client1** using an account that is a member of the **HR Group**.



- Open **Command Prompt** or **PowerShell** (you don't necessarily need admin privileges for gpupdate /force as a regular user).
- Run the command:

  gpupdate /force

  This command forces the computer and user policies to refresh immediately.



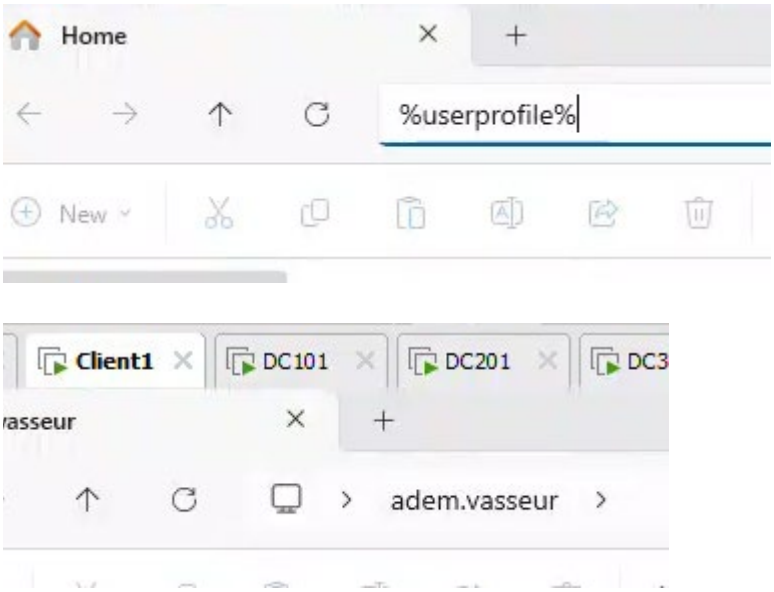
- After gpupdate /force completes (or not complete), you will need to **log off from Client1 and then log back on**. Folder redirection settings for users are applied during logon.

Check with:

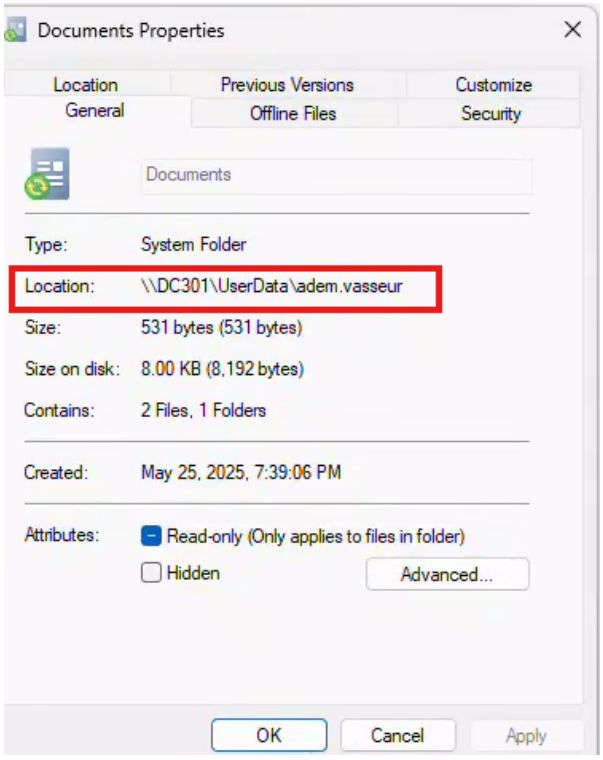
gpresult /r

```
PS C:\Users\adem.vasseur> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  2025- 05- 25 at 7:49:47 PM


RSOP data for VLABS1\adem.vasseur on CLIENT1 : Logging Mode
-----------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.26100
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\adem.vasseur
Connected over a slow link?: No


USER SETTINGS
--------------
    CN=Adem Vasseur,OU=HR,DC=vlabs1,DC=com
    Last time Group Policy was applied: 2025-05-25 at 7:49:04 PM
    Group Policy was applied from:      DC101.vlabs1.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        VLABS1
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        DisableControlPanel
        SharedUserData

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        HR
        Authentication authority asserted identity
        Medium Mandatory Level

PS C:\Users\adem.vasseur>
```

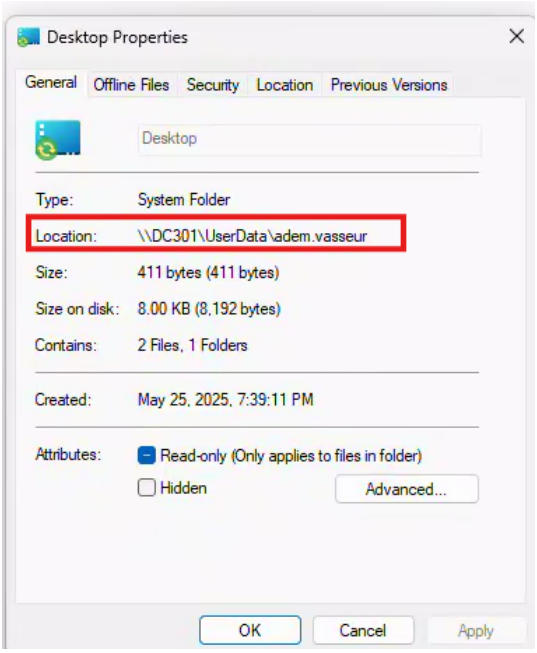
2. **Verify Redirection (On Client1, after logging back on as an HR user):**
    - Open **File Explorer**.
    - In the address bar, type %userprofile% and press Enter.



- Look for your **"Documents"** and **"Desktop"** folders.
- **Check the path:**
  - For "Documents": Right-click on the "Documents" folder, select **Properties**, then go to the **Location** tab. The path should now show \\DC301\UserData\<your_username>\Documents.

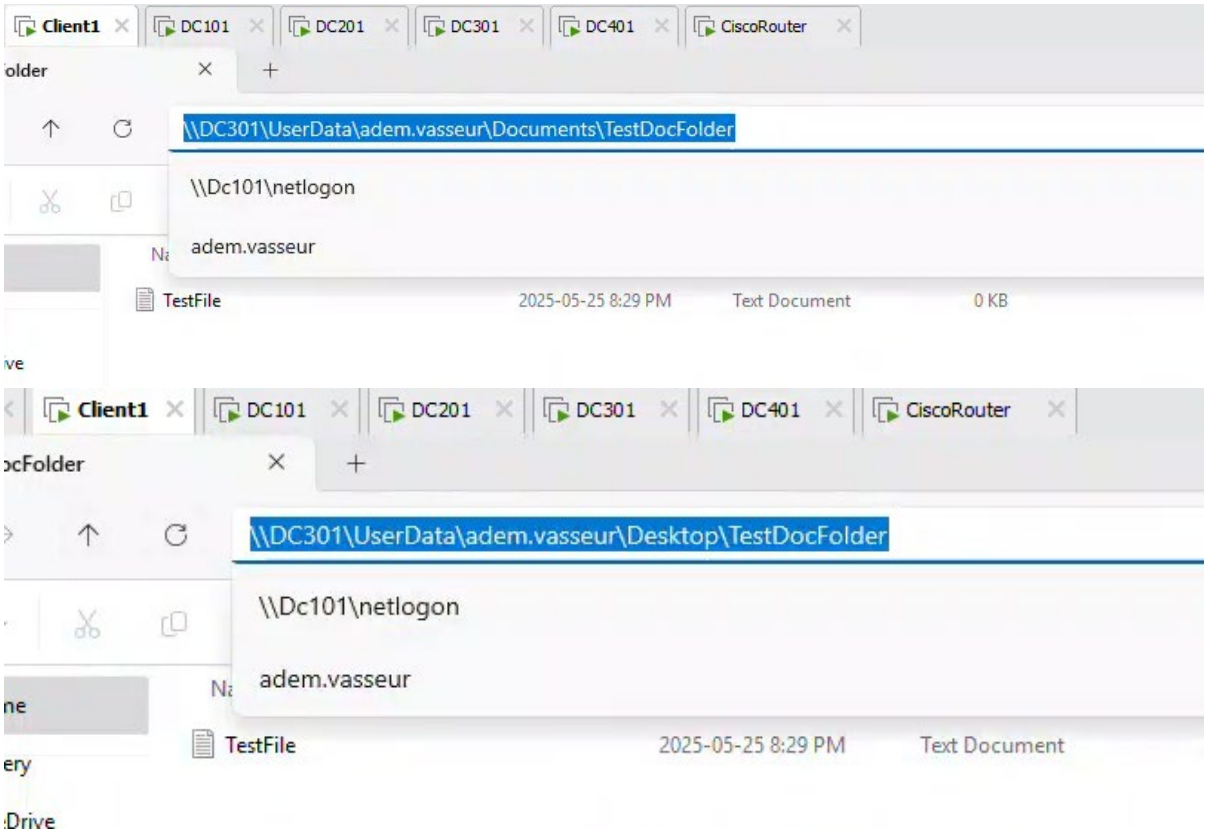


- For "Desktop": Similarly, right-click on the "Desktop" folder, select **Properties**, then go to the **Location** tab. The path should show \\DC301\UserData\<your_username>\Desktop.



- Alternatively, from a **Command Prompt** on Client1, you can type echo %userprofile%\Desktop and echo %userprofile%\Documents to see what local paths they point to. If redirection is successful, File Explorer's properties are the most definitive visual check.

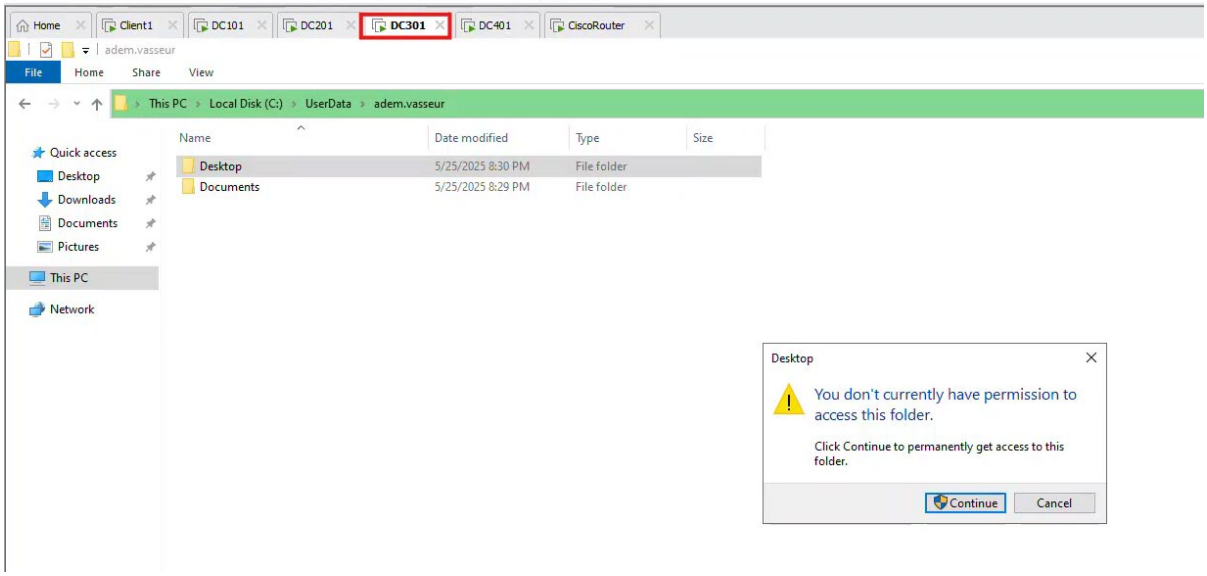
3. **Test File Operations (On Client1 and DC301):**
   - **On Client1 (as the HR user):**
     - Go to your Documents folder (which is now redirected).
     - Create a new folder (e.g., TestDocFolder).
     - Create a new text file inside it (e.g., TestDocFile.txt).
     - Repeat the same process for your Desktop (create a new folder and a new text file on the desktop).

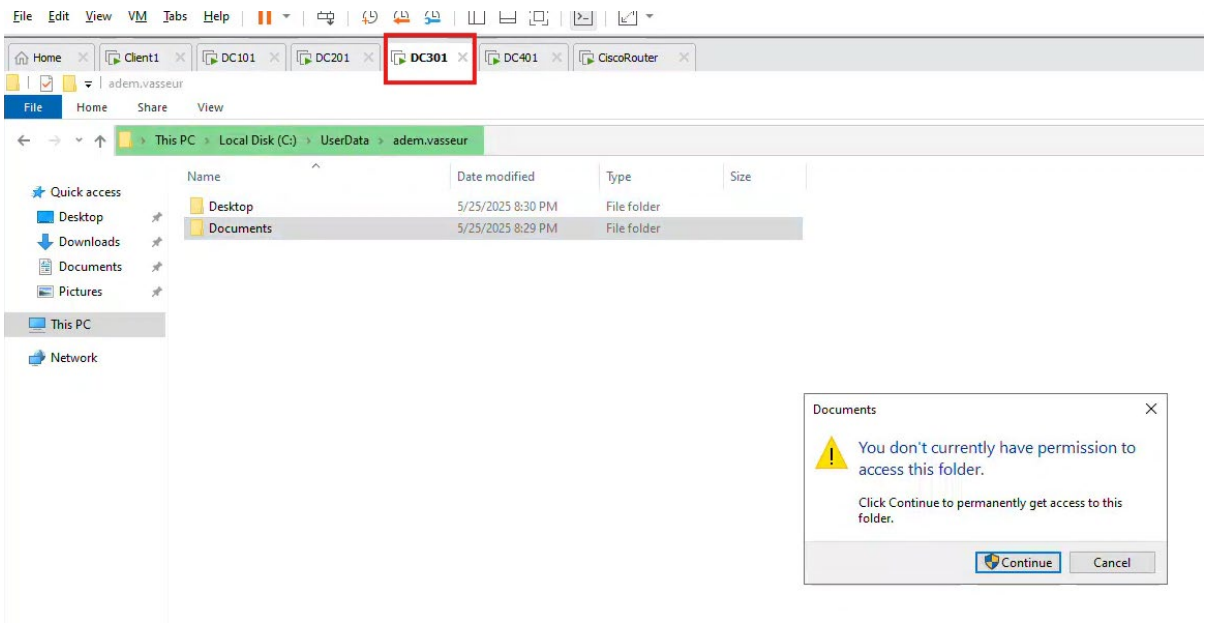


- **On DC301 (File Server):**
  - Open File Explorer and navigate to C:\UserData.
  - You should now see a new folder named after the HR user you logged in as (e.g., C:\UserData\HRUser1).
  - Open that user's folder, then navigate into the Documents and Desktop subfolders.

  - Verify that TestDocFolder and TestDocFile.txt (and any other files/folders you created) appear in their respective locations on DC301. This part is not working yet I can not access the contents of the folders. I can only see the folders

- But on the other hand maybe is not necessary to access the contents of the folders just the folders....





Verification Table

Check	Expected Result
Documents path	\\DC301\UserData\<user>\Documents
Desktop path	\\DC301\UserData\<user>\Desktop

Check	Expected Result
File creation	Files appear on server
Permissions	Only user+admin can access their folder

10 Task 8: Managing Software Installation

- Create a network share: **\\DC301\Software.**
- Download the **Microsoft Teams MSI package** *(You will need to **add the NAT NIC** to download this package. Remove it after completing the download).*
  https://learn.microsoft.com/en-us/microsoftteams/msi- deployment#msi-files
- Create a new GPO named **DC301_Teams_Installation.**
- Assign the **Teams MSI package** installation to the **Engineering OU**.
- Run **gpupdate /force to** apply changes.
- Restart **Client1**, log in with a user from **Engineering OU**, and verify that Microsoft Teams is installed.
- Confirm that Teams do **not** start automatically after installation (to test GPO **RestrictTeamsStarting**, created in Task 2).

10.1 Objective:

Deploy Microsoft Teams silently to Engineering OU users and verify installation while testing the auto-start restriction policy.

10.2 Steps

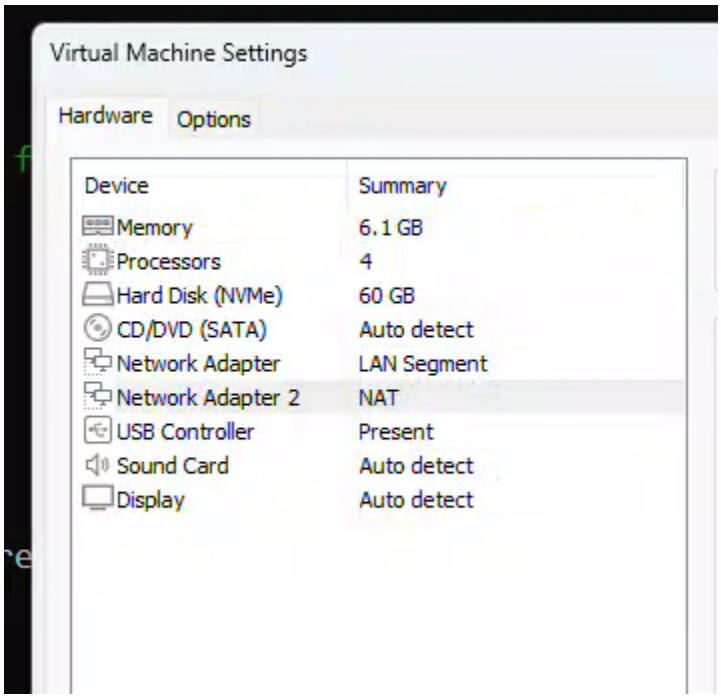
10.2.1 Prepare Software Distribution Point

a) **On DC301 (File Server)**

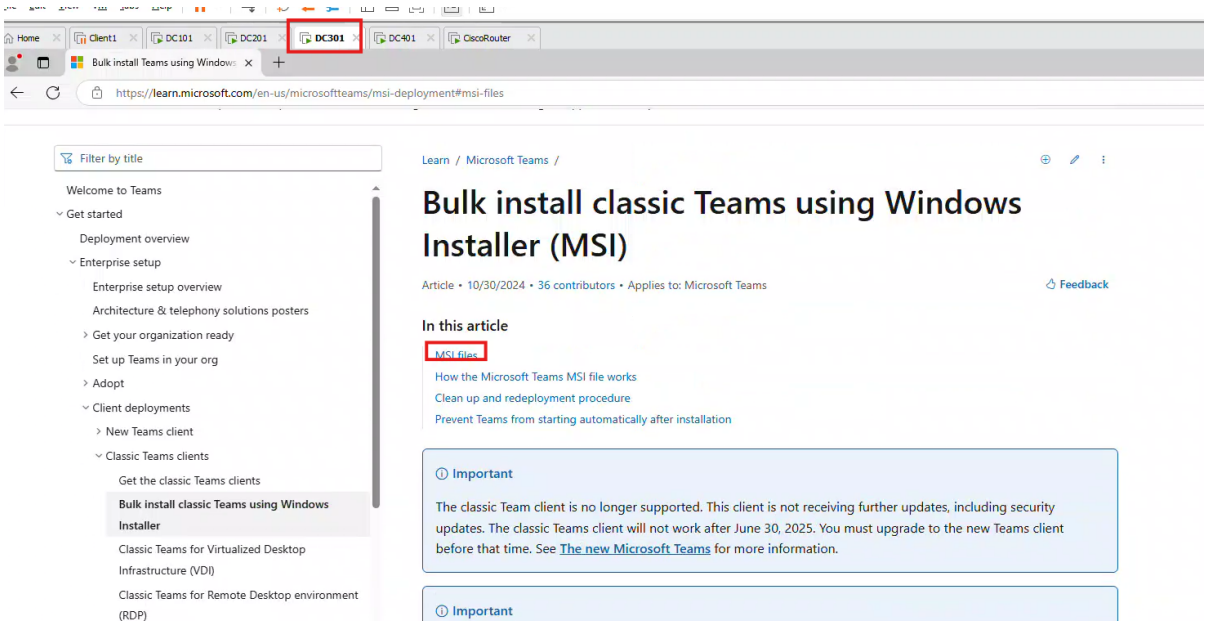
```
# Create Software folder
mkdir C:\Software

# Create network share with read access for Everyone
net share Software=C:\Software /grant:Everyone,READ

# Verify share creation
Get-SmbShare -Name Software
```

```
PS C:\UserData\adem.vasseur\Documents> hostname
DC301
PS C:\UserData\adem.vasseur\Documents> whoami
lab1\administrator
PS C:\UserData\adem.vasseur\Documents> # Create Software folder
PS C:\UserData\adem.vasseur\Documents> mkdir C:\Software


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2025   1:43 AM                Software


PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Create network share with read access for Everyone
PS C:\UserData\adem.vasseur\Documents> net share Software=C:\Software /grant:Everyone,READ
Software was shared successfully.

PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Verify share creation
PS C:\UserData\adem.vasseur\Documents> Get-SmbShare -Name Software

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


PS C:\UserData\adem.vasseur\Documents>
```

b) Temporarily enable NAT NIC (manually via Hyper-V or network settings)
DC101



c) Download Teams MSI (check latest version at https://learn.microsoft.com/en-us/microsoftteams/msi-deployment#msi-files)



MSI files

The table below provides links to 32-bit, 64-bit, and ARM64 MSI files for Teams. Download the MSI that you want to install on computers in your organization. The x86 architecture (32-bit or 64-bit) Teams supports is independent of other Office apps installed on a computer.

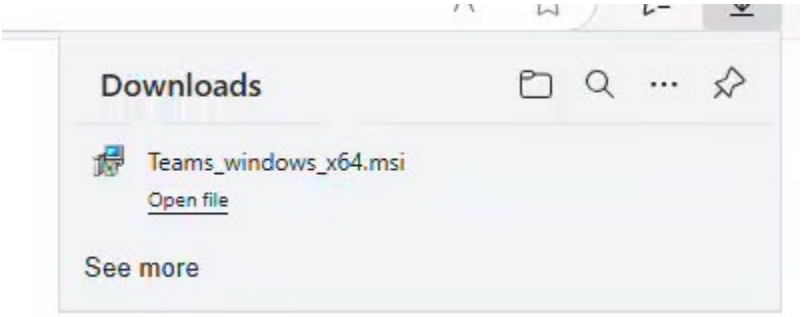
> **Note**
>
> New builds are released regularly. If you have previously downloaded the MSI, confirm if you have the most current version. Learn more: Version update history for the Microsoft Teams app

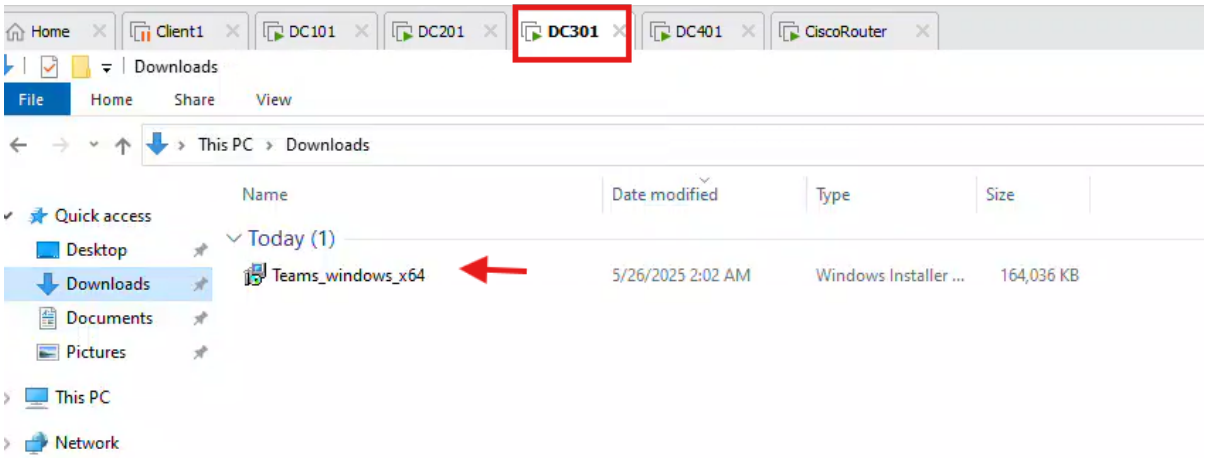
If you have 64-bit computers, we recommend installing the 64-bit Teams MSI even if the computer is running a 32-bit version of Office. The ARM64 MSI can only be installed on computers that use the ARM architecture, such as the Surface Pro X.

> **Important**
>
> Install the 64-bit version of Teams only on 64-bit operating systems. If you try to install the 64-bit version of Teams on a 32-bit operating system, the installation won't be successful and you won't receive an error message.

Expand table

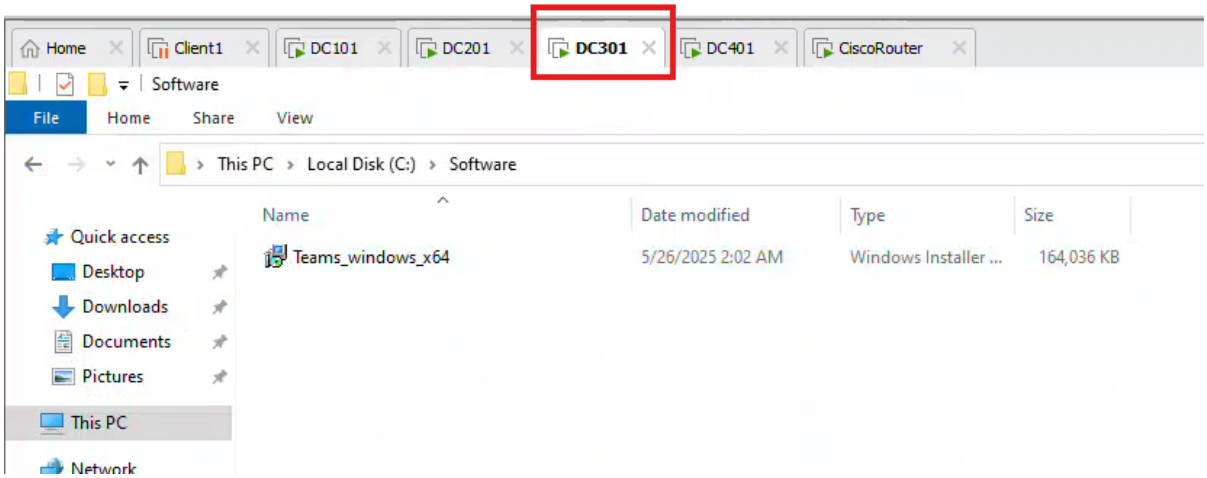
Entity	32-bit	64-bit	ARM64
Commercial	32-bit	64-bit	ARM64
U.S. Government - GCC	32-bit	64-bit	ARM64
U.S. Government - GCC High	32-bit	64-bit	ARM64



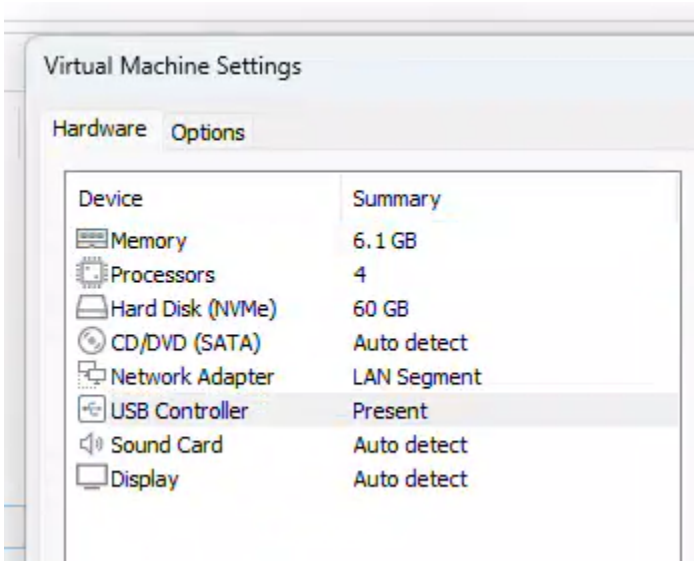


d) Verify download

Move to C:\Software\Teams_windows_x64.msi

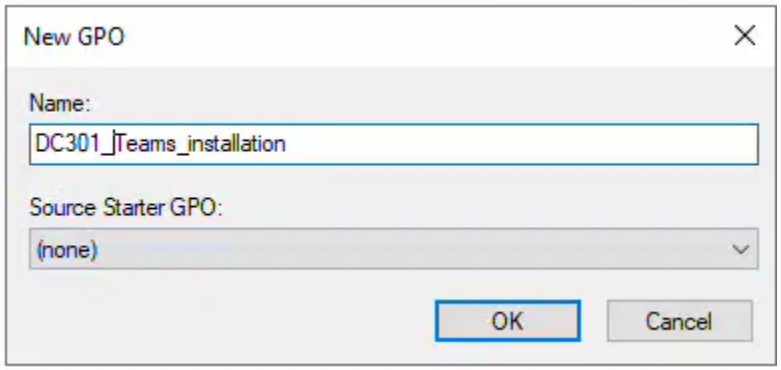


e) Disable NAT NIC (manually via Hyper-V or network settings)

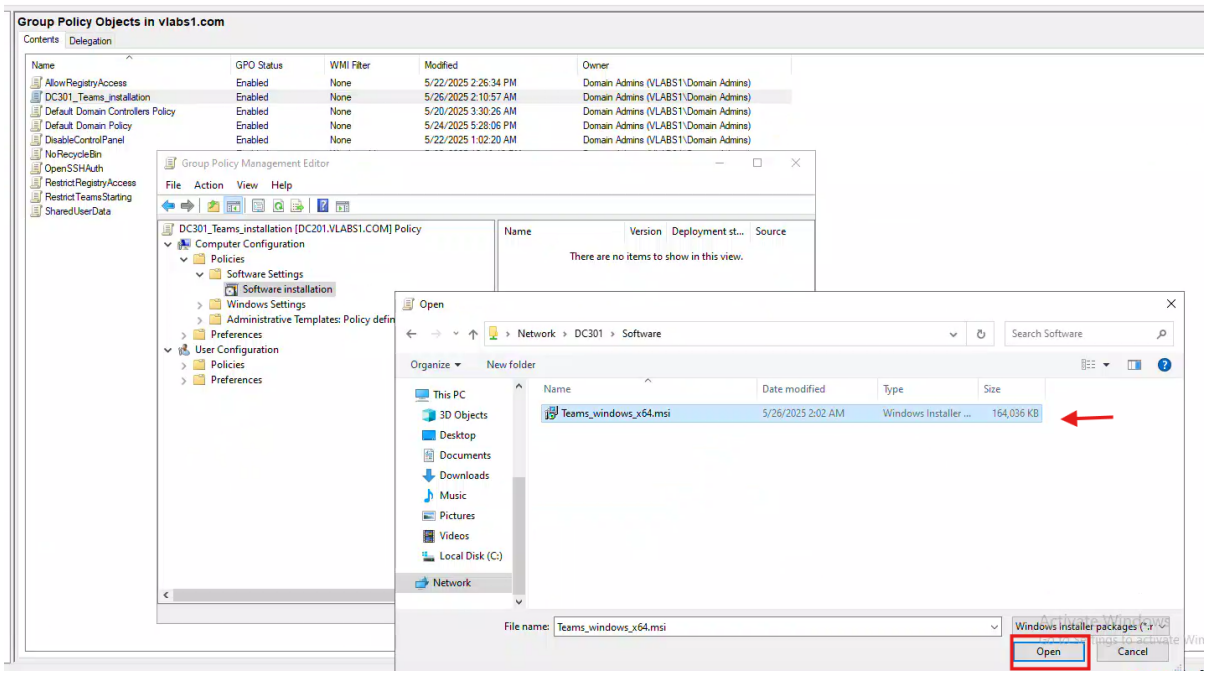


10.2.2 Create Software Installation GPO in DC101

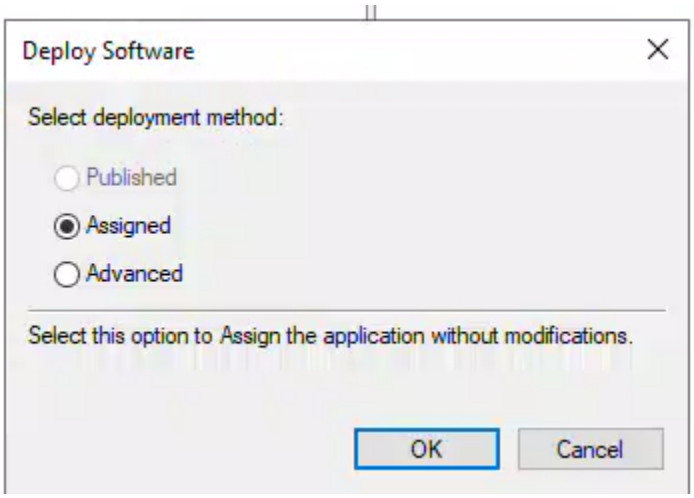
a) Open Group Policy Management (gpmc.msc).
b) Right-click Group Policy Objects → New.
c) Name: DC301_Teams_Installation → OK.

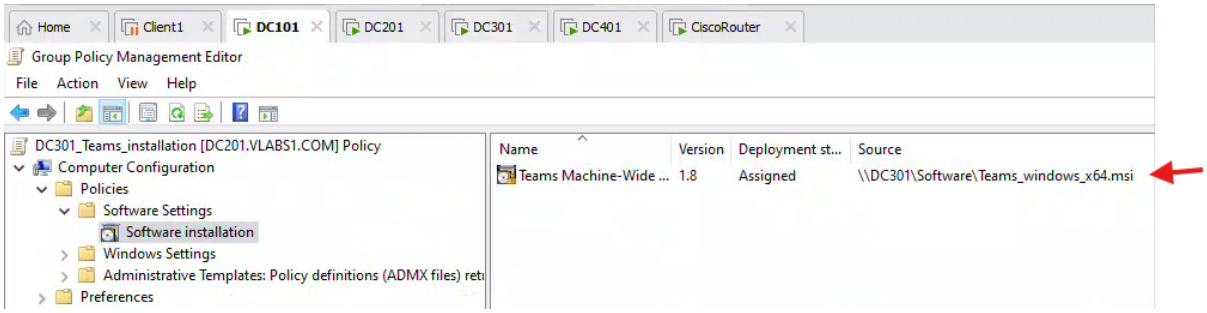


d) Right-click the new GPO → Edit.
e) Navigate to:
Computer Configuration → Policies → Software Settings → Software Installation.
f) Right-click → New → Package.
g) Browse to \\DC301\Software\Teams_windows_x64.msi.



h) Select Assigned (mandatory installation).

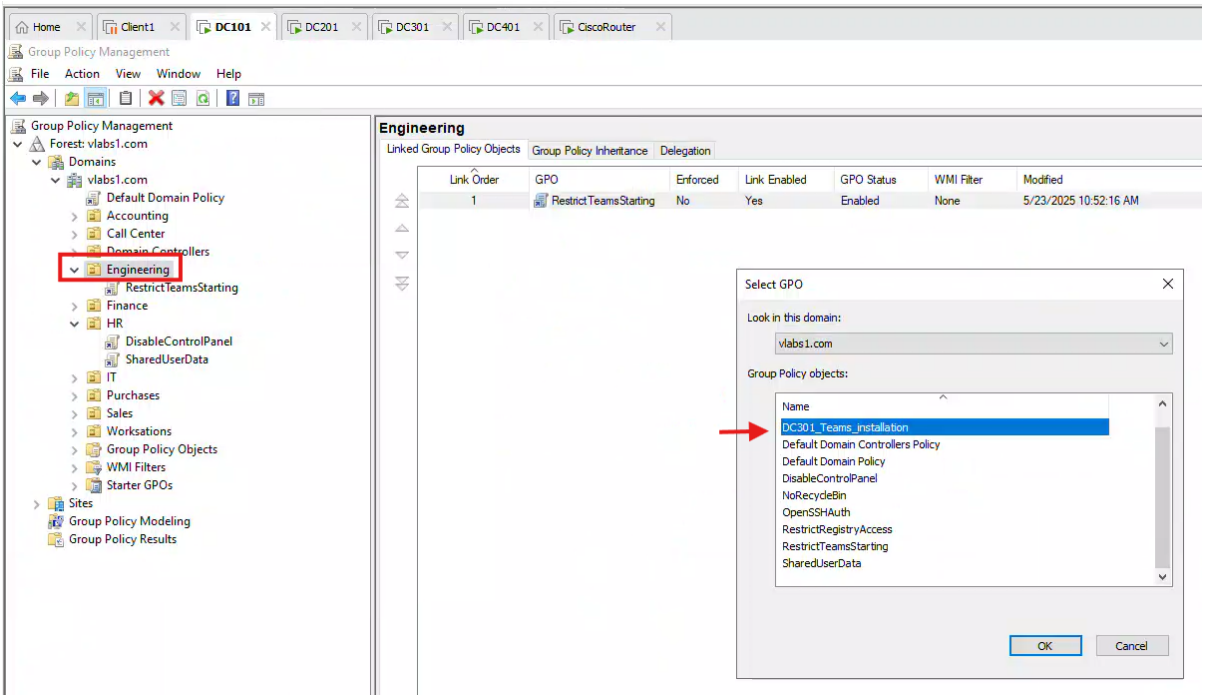




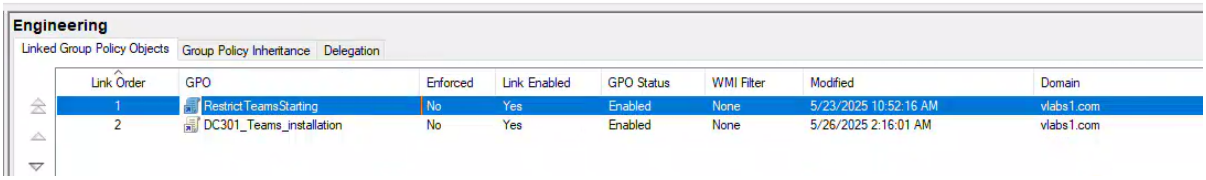
i) Close the GPO Editor.

10.2.3 Link GPO to Engineering OU (DC101)

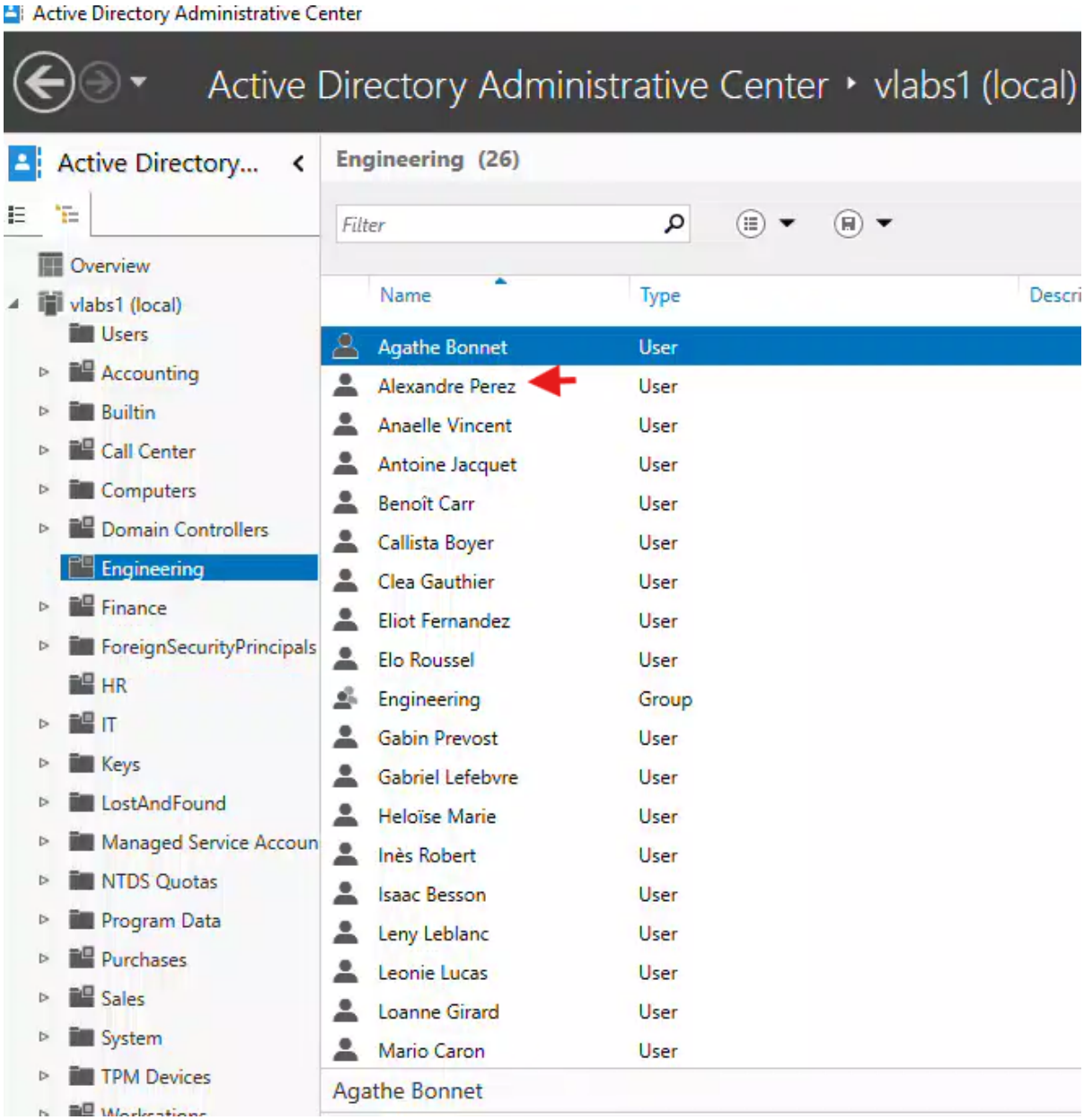
a) In GPMC:
   - Right-click **Engineering OU → Link an Existing GPO**
   - Select DC301_Teams_Installation → Click **OK**



b) **Verify Precedence:**
   - Ensure RestrictTeamsStarting GPO (from Task 2) is still applied



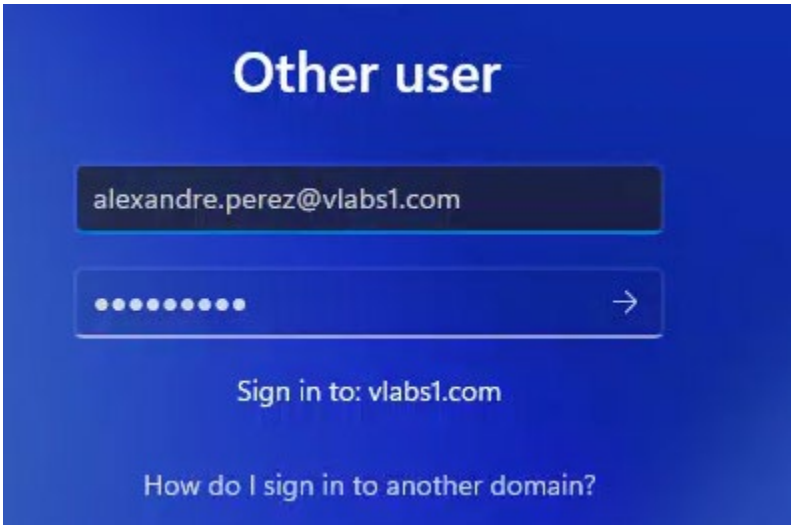
c) Verify engineering users



10.2.4 Apply– Client1

a) **Force Policy Update:**

1. Log in to `Client1`. With engineering user

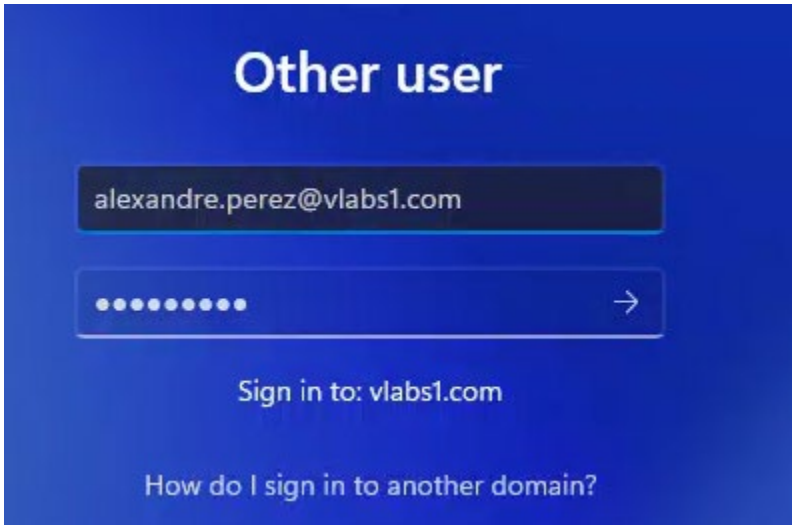


2. Open **Command Prompt** as an administrator.
3. Type `gpupdate /force` and press Enter.
4. Wait for the policy update to complete successfully.

```
PS C:\WINDOWS\system32> whoami
vlabs1\administrator
PS C:\WINDOWS\system32> hostname
Client1
PS C:\WINDOWS\system32> gpupdate /force
Updating policy...

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

PS C:\WINDOWS\system32>
```

10.2.5 Verify Teams installation:

- **Restart Client1.** This is important for the assigned software installation policy to take effect.
- Log in to `Client1` with a user account that is a member of the **Engineering OU**.

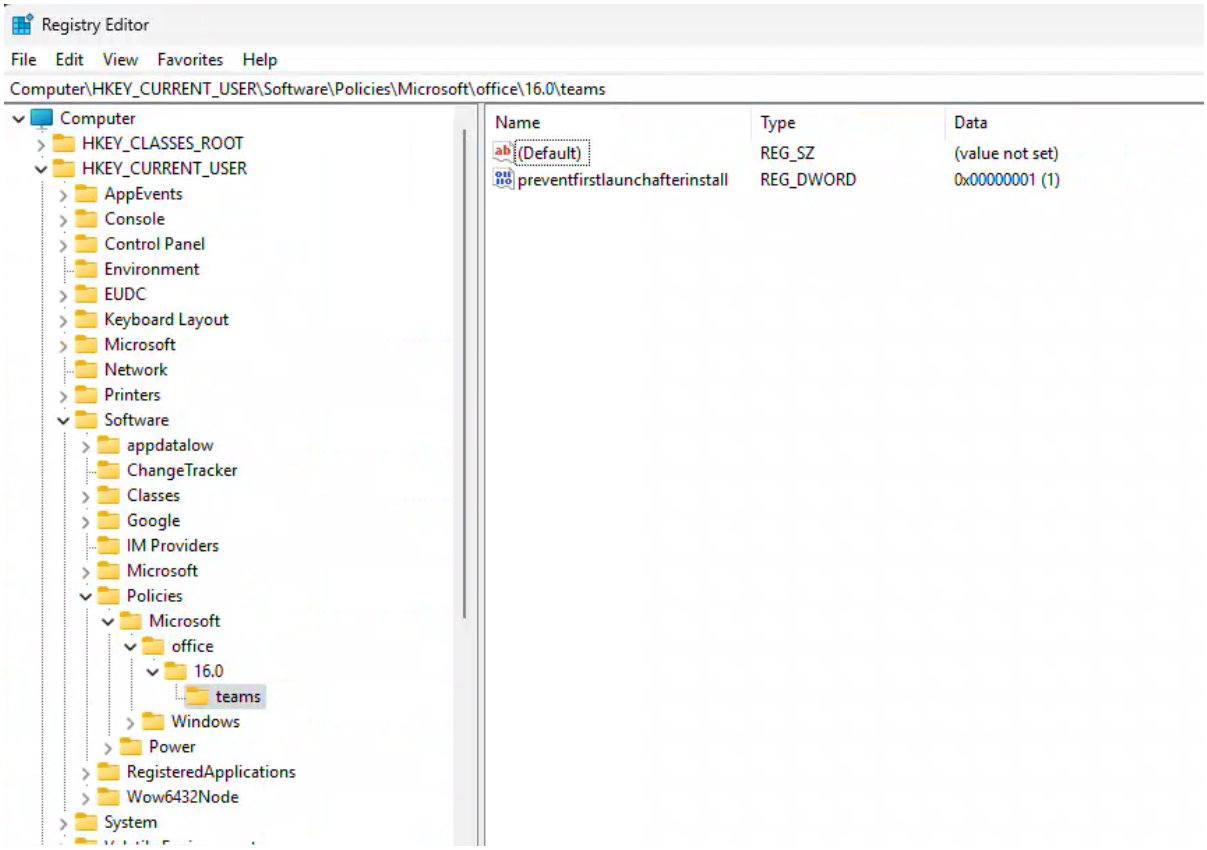


- **Verify Teams Installation:**
    - You can also verify by going to `Control Panel` > `Programs` > `Programs and Features` and looking for Microsoft Teams in the list of installed programs.

```
PS C:\Users\alexandre.perez> Get-Package -NAme "*Microsoft Teams*"

Name                           Version          Source                           ProviderName
----                           -------          ------                           ------------
Microsoft Teams Meeting Add... 1.25.8601                                         msi

PS C:\Users\alexandre.perez>
```

- **Confirm Teams Auto-start Behavior:**

Registry Verification: The corresponding registry value, PreventFirstLaunch (or PreventFirstLaunchAfterInstalled), located at HKEY_CURRENT_USER\Software\Policies\Microsoft\Teams, is correctly set to 1 on Client1 for the user. This 1 value signifies that the policy is active and instructing Teams not to auto-start.
Winning GPO: The RestrictTeamsStarting GPO is confirmed as the "Winning GPO" for this particular setting, meaning no other GPO is overriding it.



Verification Table

Check	Expected Result
MSI in network share	Accessible at \\DC301\Software
Software installation	Teams appears in Programs
Auto-start behavior	Teams doesn't launch at login
GPO precedence	RestrictTeamsStarting overrides default behavior

11 Task 9: Managing Scripts with GPO

- Create a shared folder on **DC301\Public** and share it with **Everyone**

(read and write).

- Create a **logon script** (**MapDrive.bat**) to map this shared network drive. Add this text in this file: **net use Z: \\DC301\Public**
- Store the script in **\\DC101\NETLOGON.**
- Create a new GPO named **Public_Share.**
- Add this new logon script to **User Configuration Scripts Logon.**
- Link GPO to the **Domain.**
- Run **gpupdate /force** to apply changes.
- Test with any by logging into **Client1** and verifying the drive mapping.
- Try to create files and folders in this drive.

11.1 Objective

Create and deploy a logon script via Group Policy to automatically map a network drive for all domain users, then verify functionality.

11.2 Steps

11.2.1 1. Prepare Shared Folder on DC301

1. **On DC301 (File Server):**
    - Create folder and set permissions (use powershell as administrator)

      # Create the folder

      mkdir C:\Public

      # Set NTFS permissions (Everyone: Modify, which includes Read, Write, Execute)

      icacls C:\Public /grant "Everyone:(OI)(CI)(M)"

      # Create the network share

      net share Public=C:\Public /grant:Everyone,FULL

```
PS C:\UserData\adem.vasseur\Documents> # Create the folder
PS C:\UserData\adem.vasseur\Documents> mkdir C:\Public


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2025   3:51 AM                Public


PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Set NTFS permissions (Everyone: Modify, which includes Read, Write, Execute)
PS C:\UserData\adem.vasseur\Documents> icacls C:\Public /grant "Everyone:(OI)(CI)(M)"
processed file: C:\Public
Successfully processed 1 files; Failed processing 0 files
PS C:\UserData\adem.vasseur\Documents>
PS C:\UserData\adem.vasseur\Documents> # Create the network share
PS C:\UserData\adem.vasseur\Documents> net share Public=C:\Public /grant:Everyone,FULL
Public was shared successfully.

PS C:\UserData\adem.vasseur\Documents>
```

2. **Verify Share:**

   - From Client1, test access:

     dir \\DC301\Public

```
PS C:\Users\alexandre.perez> dir \\DC301\Public
PS C:\Users\alexandre.perez>
```

11.2.2 Create Logon Script

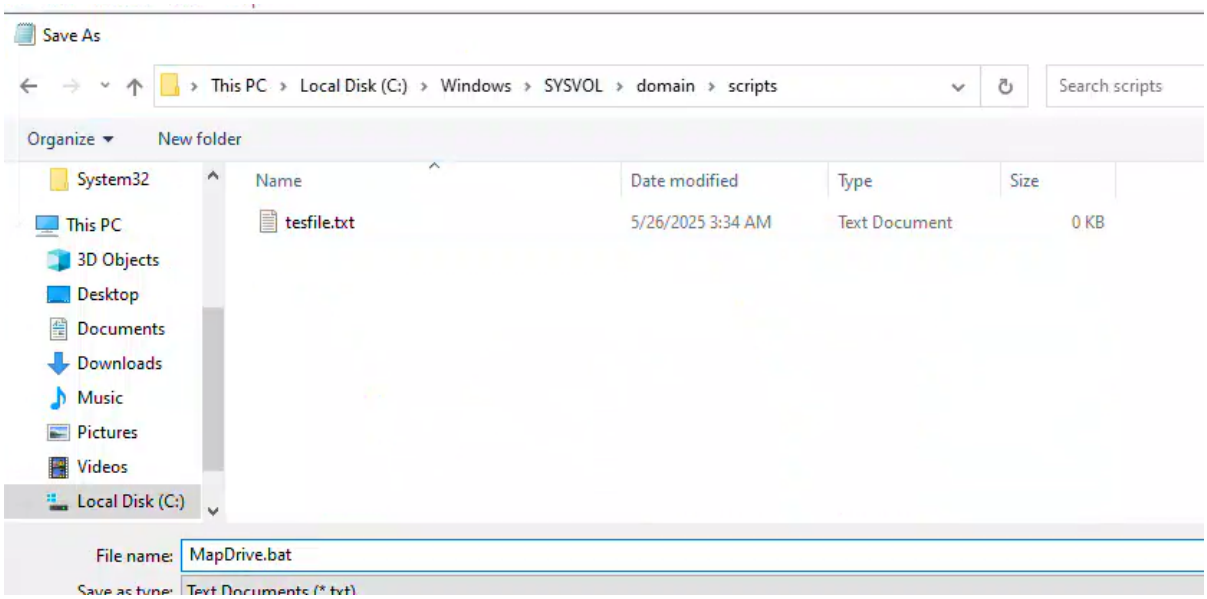
1. **On DC101 (Domain Controller):**

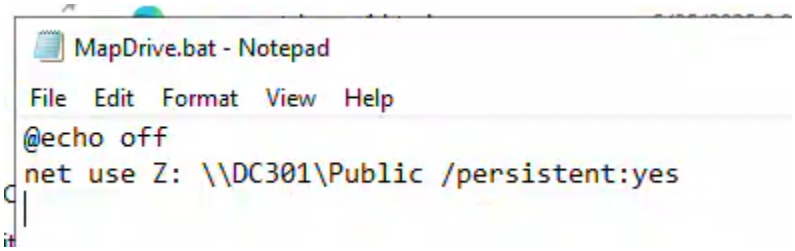
   - Open Notepad and create MapDrive.bat with:

     @echo off

     net use Z: \\DC301\Public /persistent:yes

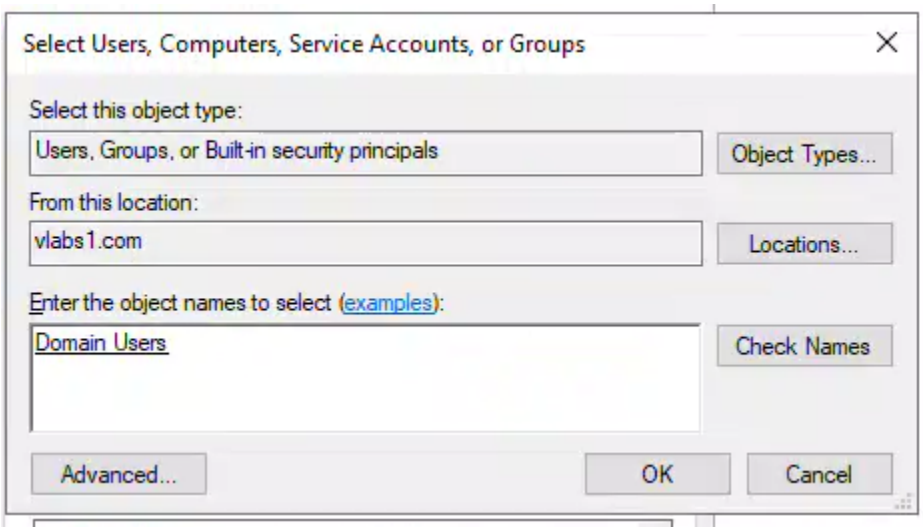
   - Save to: C:\Windows\SYSVOL\domain\scripts\MapDrive.bat

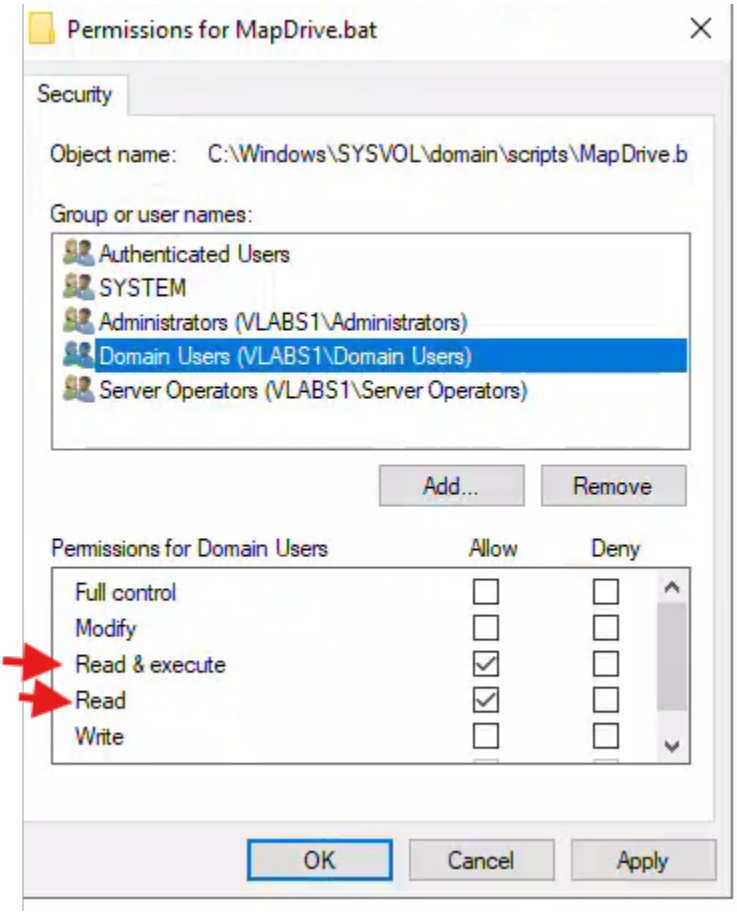


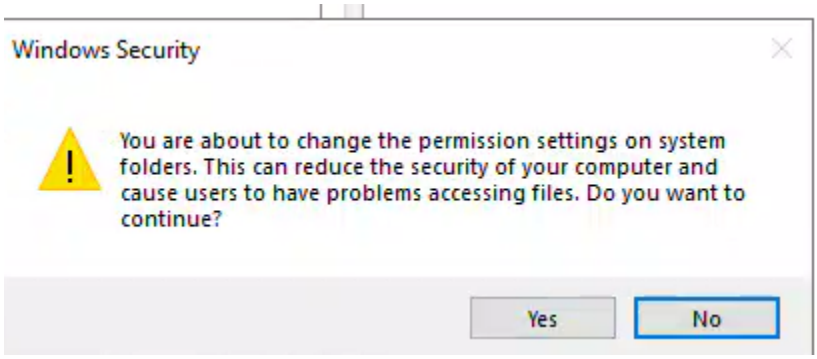


2. **Set Permissions:**

- Right-click on `MapDrive.bat` and select **Properties**.
- Go to the **Security** tab.
- Click **Edit...**
- Click **Add...**
- Type `Domain Users` in the object name field, click **Check Names**, then **OK**.
- Select `Domain Users` from the list.
- Ensure `Read & execute` is checked under "Allow." Also ensure `Read` is checked.
- Click **OK** twice to apply the permissions.

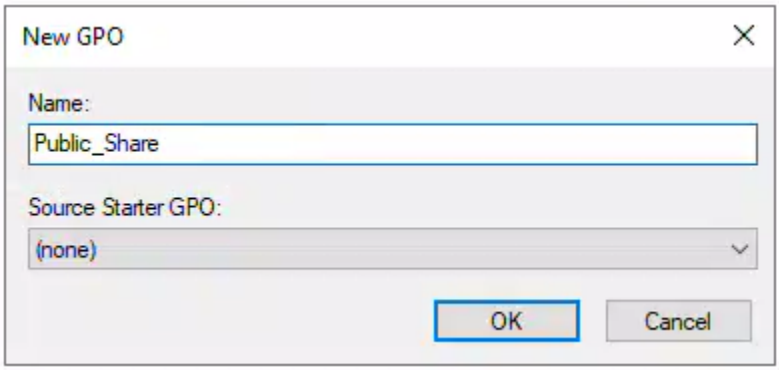

Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
vlabs1.com
Locations...
Enter the object names to select (examples):
Domain Users
Check Names
Advanced...
OK
Cancel


Permissions for MapDrive.bat
Security
Object name: C:\Windows\SYSVOL\domain\scripts\MapDrive.b
Group or user names:
Authenticated Users
SYSTEM
Administrators (VLABS1\Administrators)
Domain Users (VLABS1\Domain Users)
Server Operators (VLABS1\Server Operators)
Add...
Remove
Permissions for Domain Users
Allow
Deny
Full control
Modify
Read & execute
Read
Write
OK
Cancel
Apply

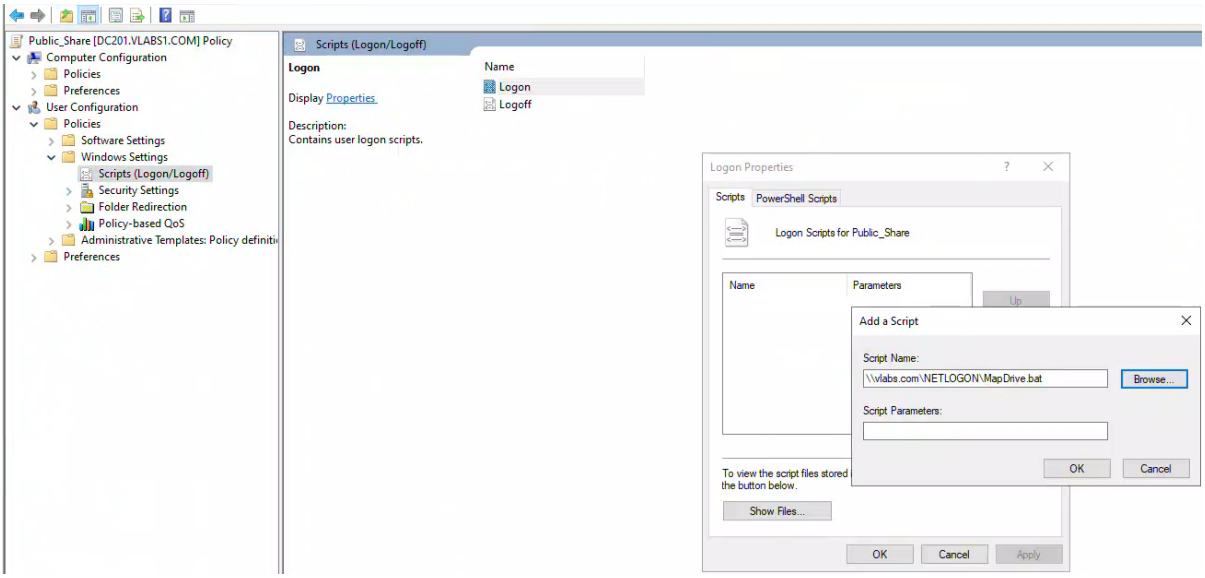


11.2.3 Configure GPO for Script Deployment (DC101)

1. **In GPMC (**gpmc.msc**):**
    - Right-click **Group Policy Objects** → **New**
    - Name: Public_Share → Click **OK**



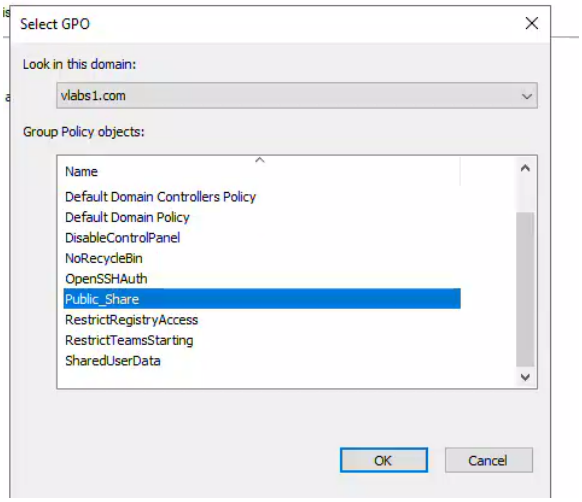
2. **Add Logon Script:**
    - Right-click → **Edit**
    - Navigate to: User Configuration → Policies → Windows Settings → Scripts (Logon/Logoff)
    - Double-click **Logon** → Click **Add**
    - Browse to: \\vlabs1.com\NETLOGON\MapDrive.bat
    - Click **OK** twice



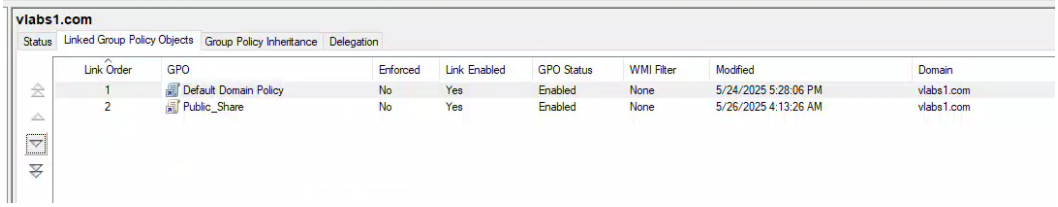
11.2.4 Link GPO to Domain Level

1. In GPMC:

- In the left pane, right-click on your **Domain** (`vlabs1.com`).
- Select **Link an Existing GPO...**.
- From the "Select GPO" dialog, choose `Public_Share`.
- Click **OK**.



\

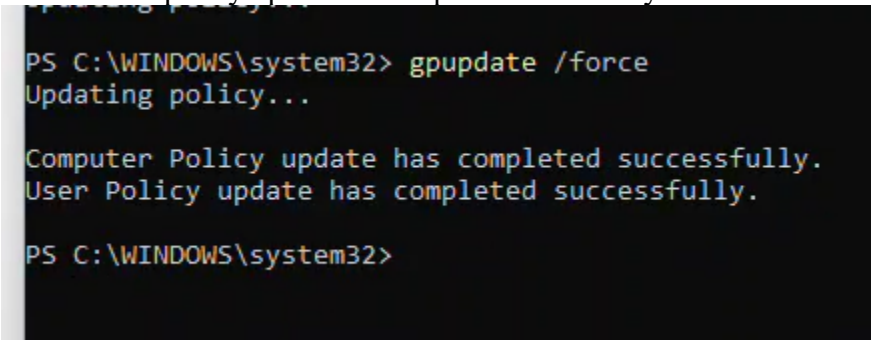


11.2.5 Force Policy Update:

Open **Command Prompt as an Administrator**.
Run the following command to force a Group Policy update:

```
gpupdate /force
```

Wait for the policy update to complete successfully.

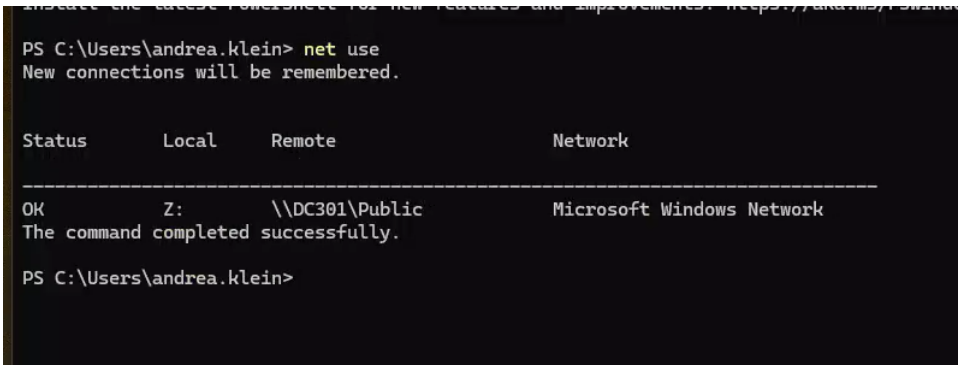


11.2.6 Verification Testing

1. Test Drive Mapping

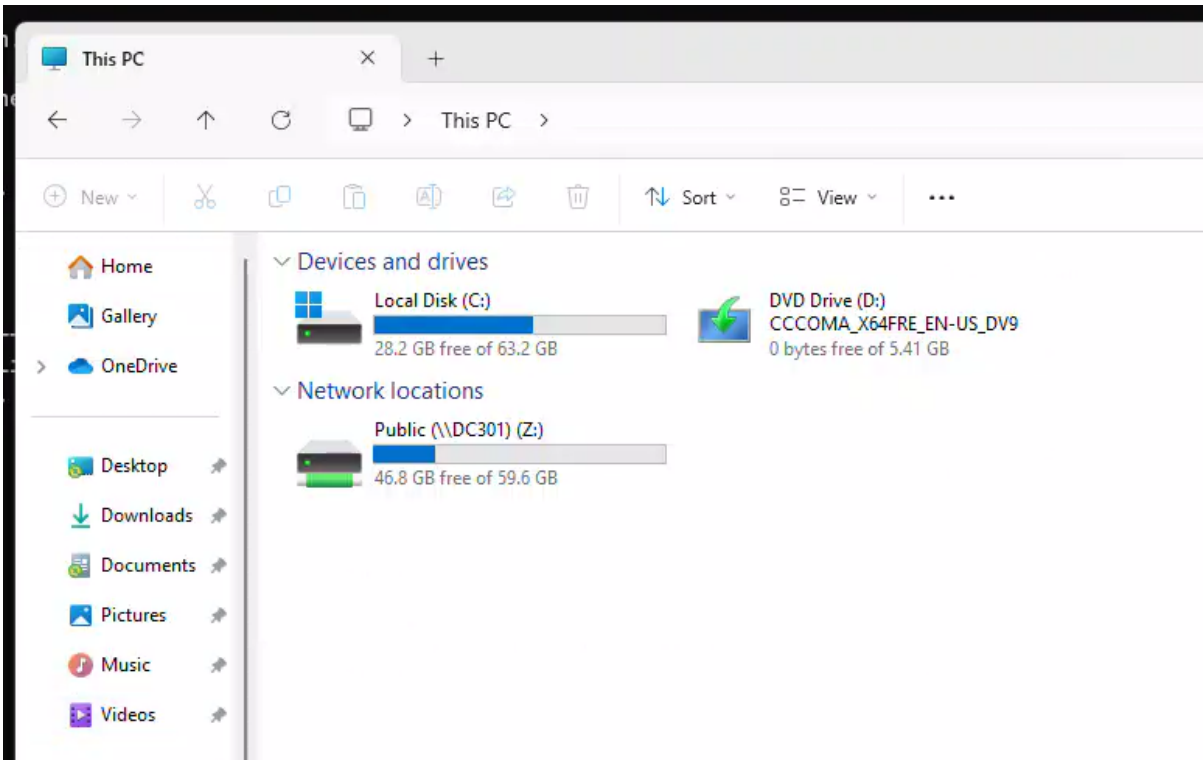
1. **Log in to Client1** as any domain user
2. Verify:
    - **Z:** drive appears in File Explorer
    - Command prompt shows mapping:

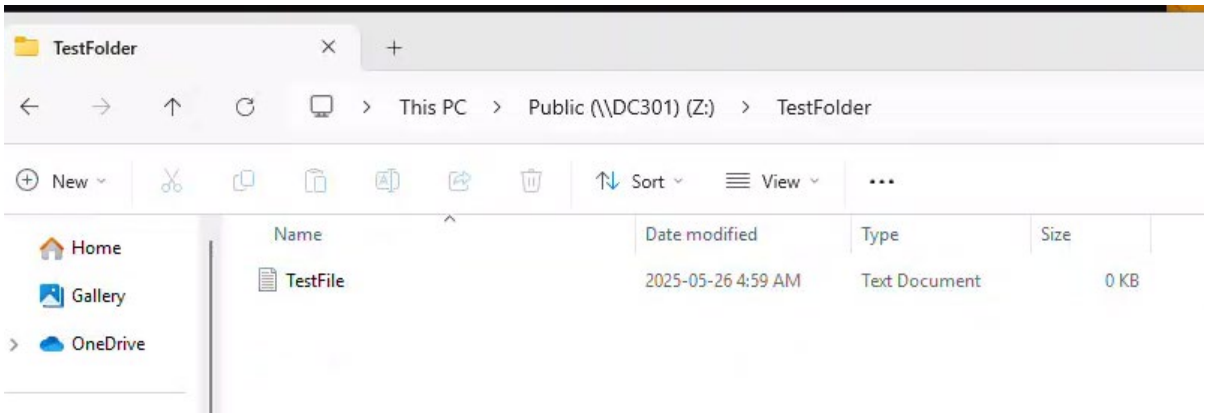
      net use
      Should list "Z: \DC301\Public"



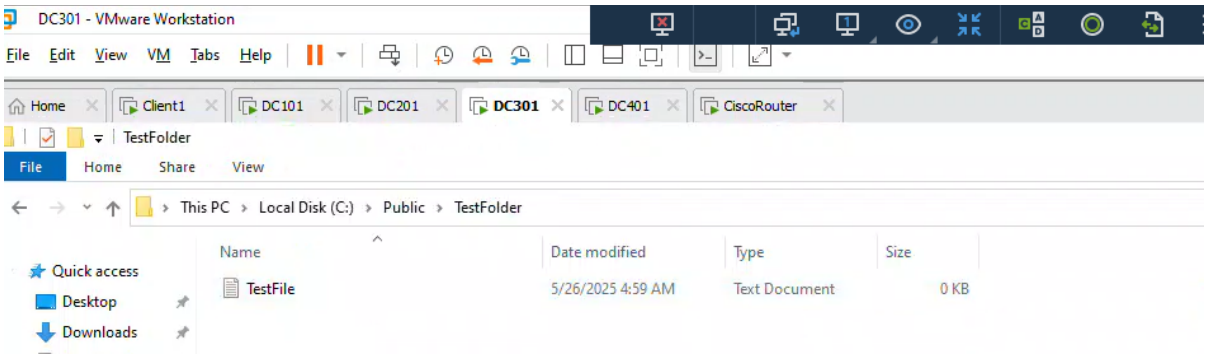
3. **Test File Operations**

1. **Create Test Files:**
    - In Z: drive:
        - New folder: Right-click → New → Folder
        - New file: Right-click → New → Text Document
    -





2. **Verify on DC301:**
    - Check files appear in: C:\Public




```
PS C:\Users\Administrator> cd C:
PS C:\Users\Administrator> dir  C:\Public


    Directory: C:\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2025   4:59 AM                TestFolder


PS C:\Users\Administrator> cd C:\Public\
PS C:\Public> dir


    Directory: C:\Public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/26/2025   4:59 AM                TestFolder
```