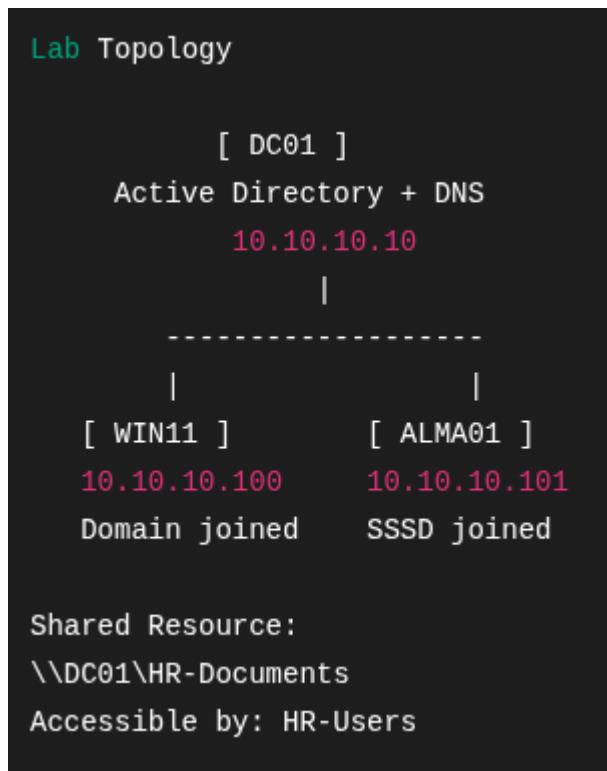


OBJECTIVES

- Create OU or Group-specific policies and deploy them
- Assign permissions and resources via Groups
- Validate Policy propagation on different OS clients

IMPLEMENTATION

BASIC TOPOLOGY



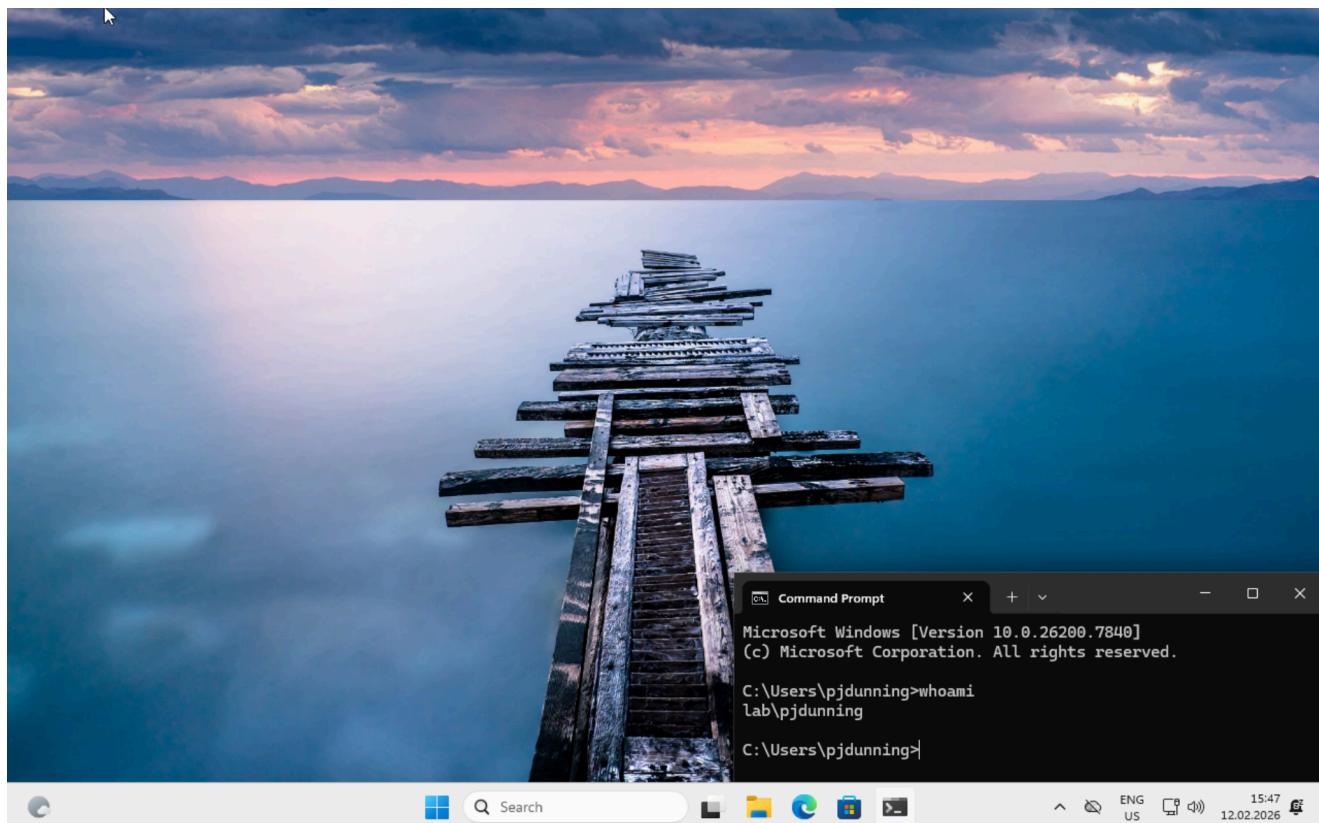
Manufacturing Group GPO

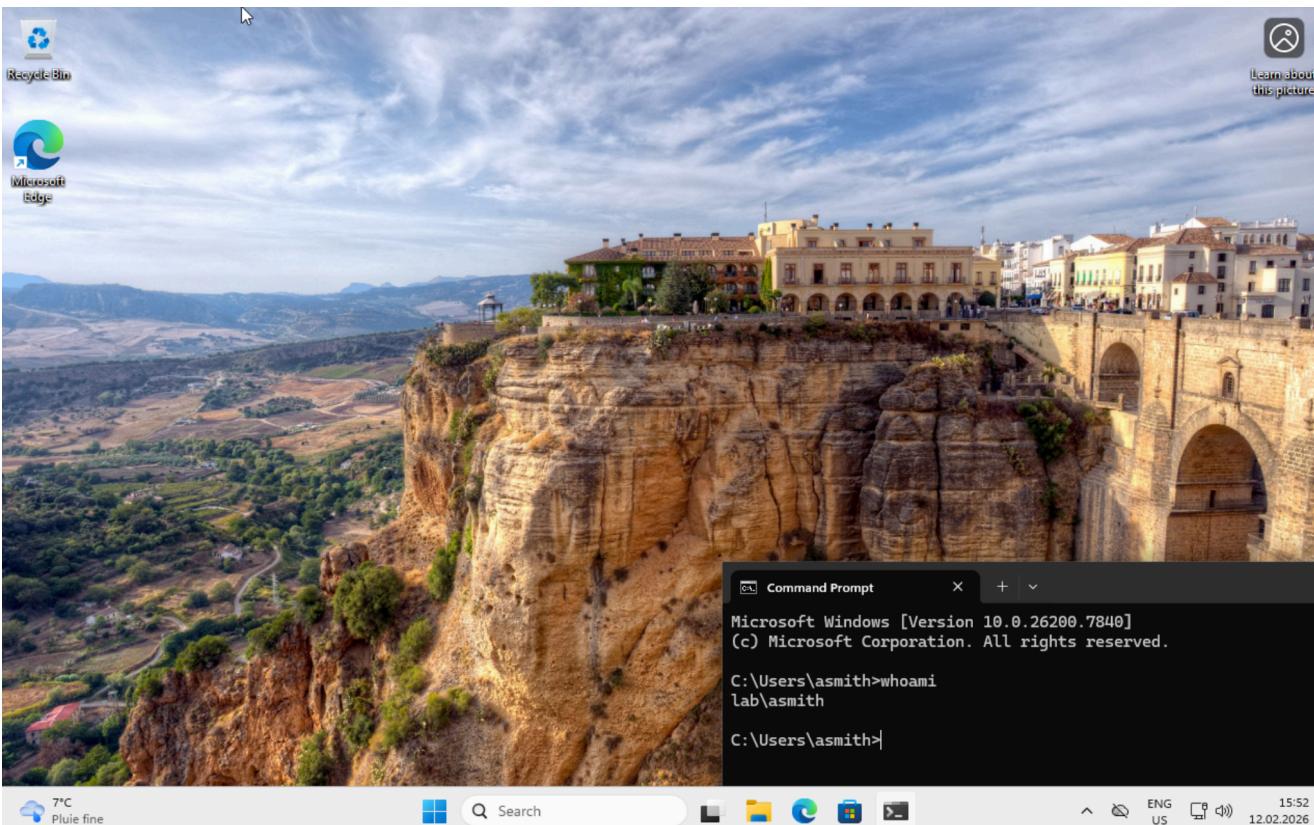
The GPO "MFG - GP" was created and linked to the "Manufacturing" OU
The object contains a simple, verifiable policy: Hide and Disable Desktop Icons

The screenshot shows the Group Policy Management console interface. On the left, the navigation pane displays the organizational unit structure under 'Forest: lab.local'. The 'Manufacturing' OU is selected. The main pane shows the 'Manufacturing' GPO object details. The 'Group Policy Inheritance' tab is selected, showing a single entry for 'MFG - GP' with 'Enforced' set to 'No' and 'Link Enabled' set to 'Yes'. The 'Delegation' tab shows delegation to the 'Manufacturing' location. The 'Group Policy Management Editor' window is open, displaying the policy settings for 'MFG - GP'. Under 'Computer Configuration', the 'Policies' node is expanded, showing 'Prohibit User from manually redirecting Profile Folders' and 'Hide and disable all items on the desktop'. The latter is highlighted. Under 'User Configuration', the 'Policies' node is expanded, showing 'Software Settings' and 'Windows Settings'. The 'Windows Settings' node is expanded, showing 'Administrative Temp'. The 'Location' tab shows the 'Manufacturing' location with 'Enforced' and 'Link Enabled' both set to 'Yes'.

VALIDATING

In order to validate the propagation, we compare below the resulting desktop environment of the accounts P. J. Dunning, assigned to Manufacturing, with that of Amber Smith, assigned to HR. We can clearly verify the change has taken effect, and only within the intended scope.





RESOURCE PERMISSIONS

A shared folder " HR-Documents" was created with the following configuration

New Share Wizard

Configure share settings

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Enable access-based enumeration
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

Access-based enumeration enforces least privilege and makes the share invisible to unauthorized user groups

Caching was deliberately **disabled** to address requirements for sensitive content

- preventing local files from remaining on laptops
- preventing sensitive personal data from being replicated outside server control

- facilitate access revocation and prevent abuse

Online access is required to read or write, and credentials and times are thus **logged**

Encryption is a standard precaution for data in transit

ACCESS PERMISSION

The following standard permissions were assigned to the shared folder resource object, via Groups

Name:	C:\Shares\HR-Documents			
Owner:	Administrators (LAB\Administrators) Change			
Permissions	Share	Auditing	Effective Access	
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).				
Permission entries:				
Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (LAB\Administrators)	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	HR-Users (LAB\HR-Users)	Modify	None	Subfolders and files only

ISSUE ENCOUNTERED

Despite correct configuration of NTFS and Share permissions, the intended test user - asmith@lab.local - HR users (Group) - was not granted the Modify permissions.

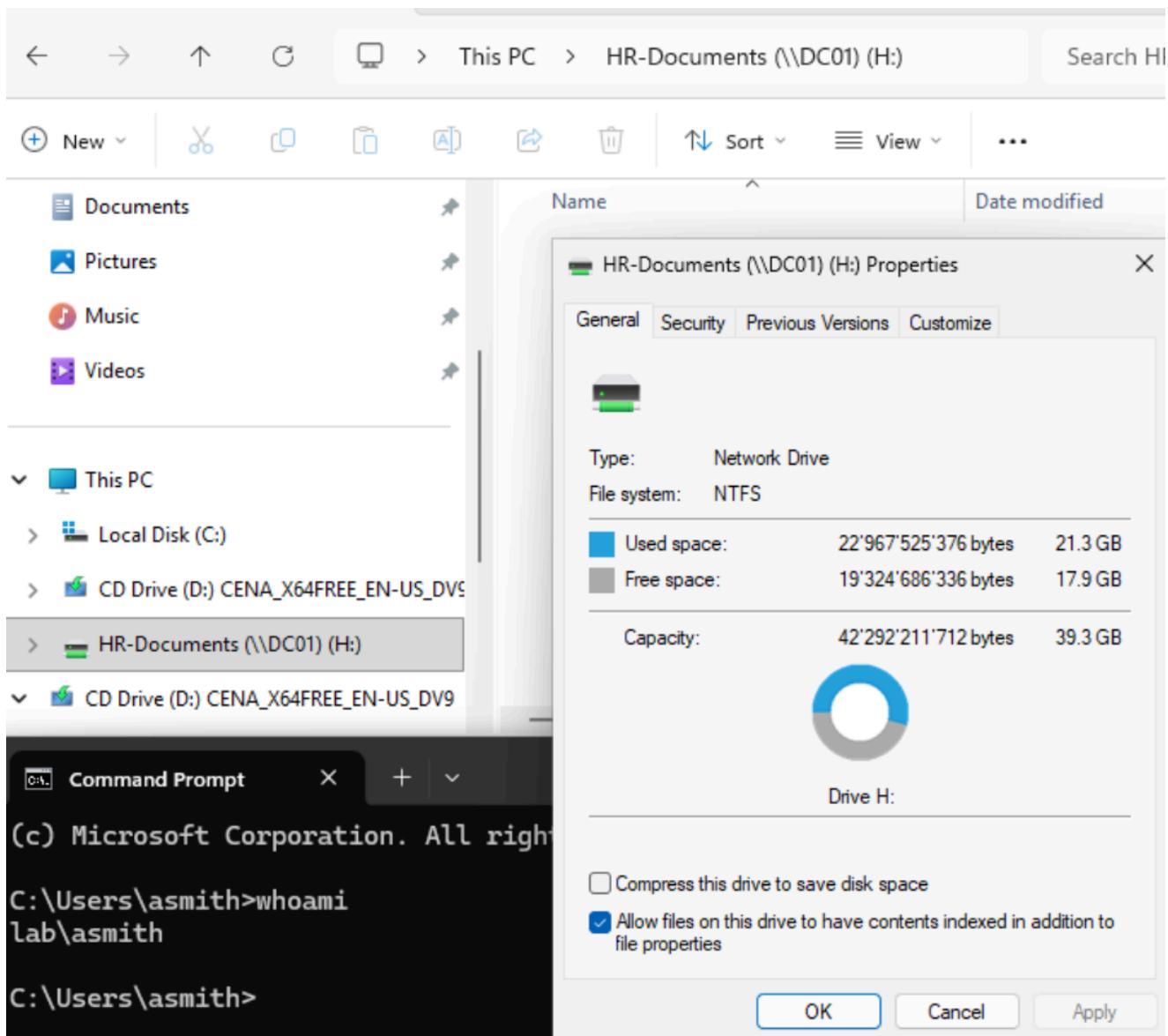
SOLUTION

The issue came from **Inheritance**. Specifically, to remove the general domain Group "Users" from the permissions table, Inheritance had to be disabled and the permissions converted to explicit on the object.

The issue was resolved by changing the "Applies to" scope to include "This folder, subfolders and files" for the HR-Users Group.

VALIDATION

Below are the tests for intended behavior validating that "**asmith**" under "HR-Users" can cleanly map and access the share, both on Windows 11 and Alma Linux:



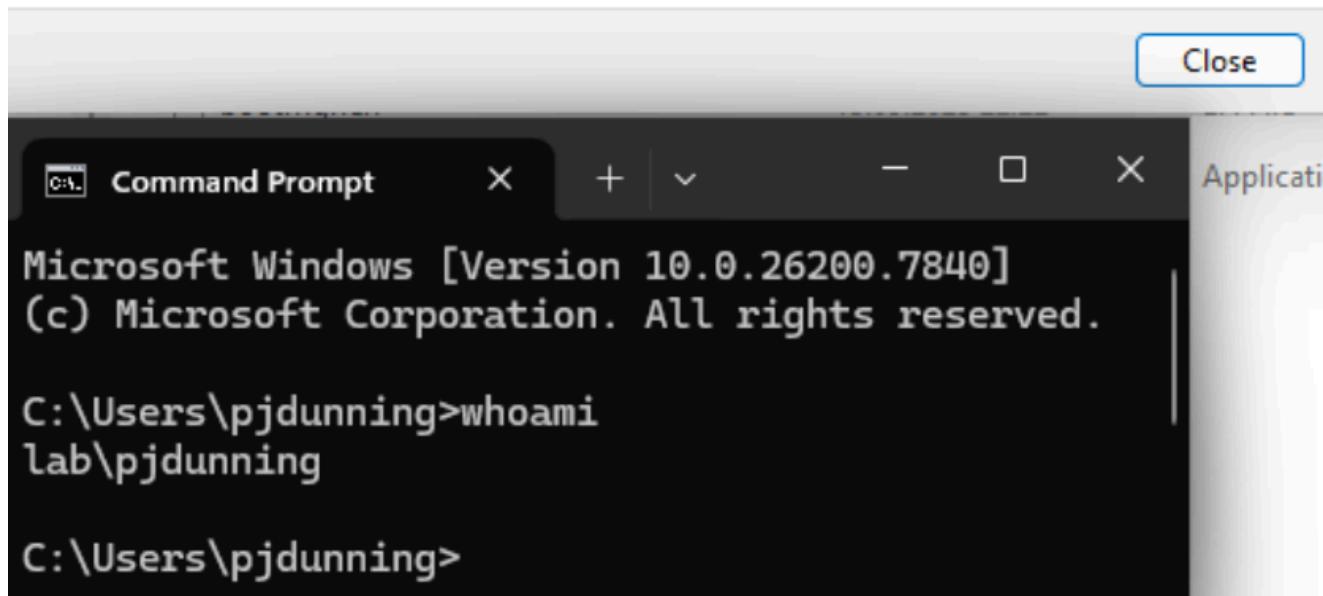
```
asmith@lab.local@alma01:~ - sudo -i
+
asmith@lab.local@alma01:~$ findmnt /mnt/hr-docs
TARGET SOURCE FSTYPE OPTIONS
/mnt/hr-docs
    //dc01/HR-Documents
        cifs    rw,relatime,vers=3.0,cache=strict,upcall_target=app,username=asmith,password=,uid=1285201112,gid=1285200513,context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
asmith@lab.local@alma01:~$ ls /mnt/hr-docs
asmith@lab.local@alma01:~$ touch /mnt/hr-docs/test.txt
asmith@lab.local@alma01:~$ ls /mnt/hr-docs
test.txt
asmith@lab.local@alma01:~$ df -h | grep hr-docs
//dc01/HR-Documents      40G   22G   19G  55% /mnt/hr-docs
asmith@lab.local@alma01:~$ id
uid=1285201112(asmith@lab.local) gid=1285200513(domain users@lab.local) groups=1285200513(domain users@lab.local),1285201108(hr-users@lab.local) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
asmith@lab.local@alma01:~$
```

While "pjdunning" under "MFG-Users" is denied as intended:

Windows cannot access \\DC01\HR-Documents\

You do not have permission to access \\DC01\HR-Documents\. Contact your network administrator to request access.

[For more information about permissions, see Windows Help and Support](#)



A screenshot of a Microsoft Windows Command Prompt window. The title bar says "Command Prompt". The window content shows the following text:

```
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pjdunning>whoami
lab\pjdunning

C:\Users\pjdunning>
```

The window has a standard Windows title bar with minimize, maximize, and close buttons. A "Close" button is also visible in the top right corner of the window frame.

NOTES

Several predictable issues were encountered during the activation of the permanent mount point on Linux:

- **CIFS** installation was required
- **/etc/fstab** has to be edited to include not only the mount point, but also specific permission for the non-root user asmith@lab.local
- initial permissions were validated server side, but Linux client-side permissions caused conflicts initially

The troubleshooting steps for the Linux integration in particular were the longest portion of the exercise, but provided invaluable insight into common cross-platform conflicts