OBJECTIVES

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

IMPLEMENTATION

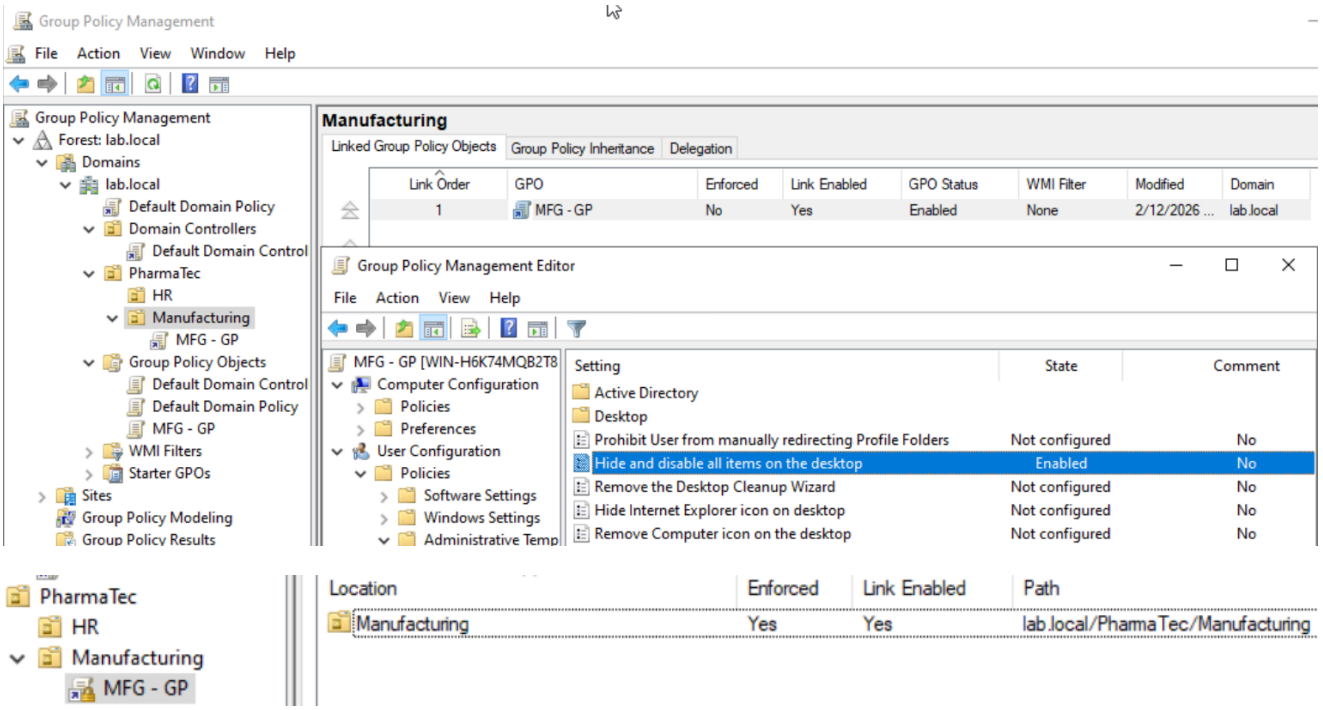
BASIC TOPOLOGY

```
Lab Topology

           [ DC01 ]
     Active Directory + DNS
           10.10.10.10
                |
        ------------------
        |                |
   [ WIN11 ]        [ ALMA01 ]
   10.10.10.100     10.10.10.101
   Domain joined    SSSD joined

Shared Resource:
\\DC01\HR-Documents
Accessible by: HR-Users
```

`

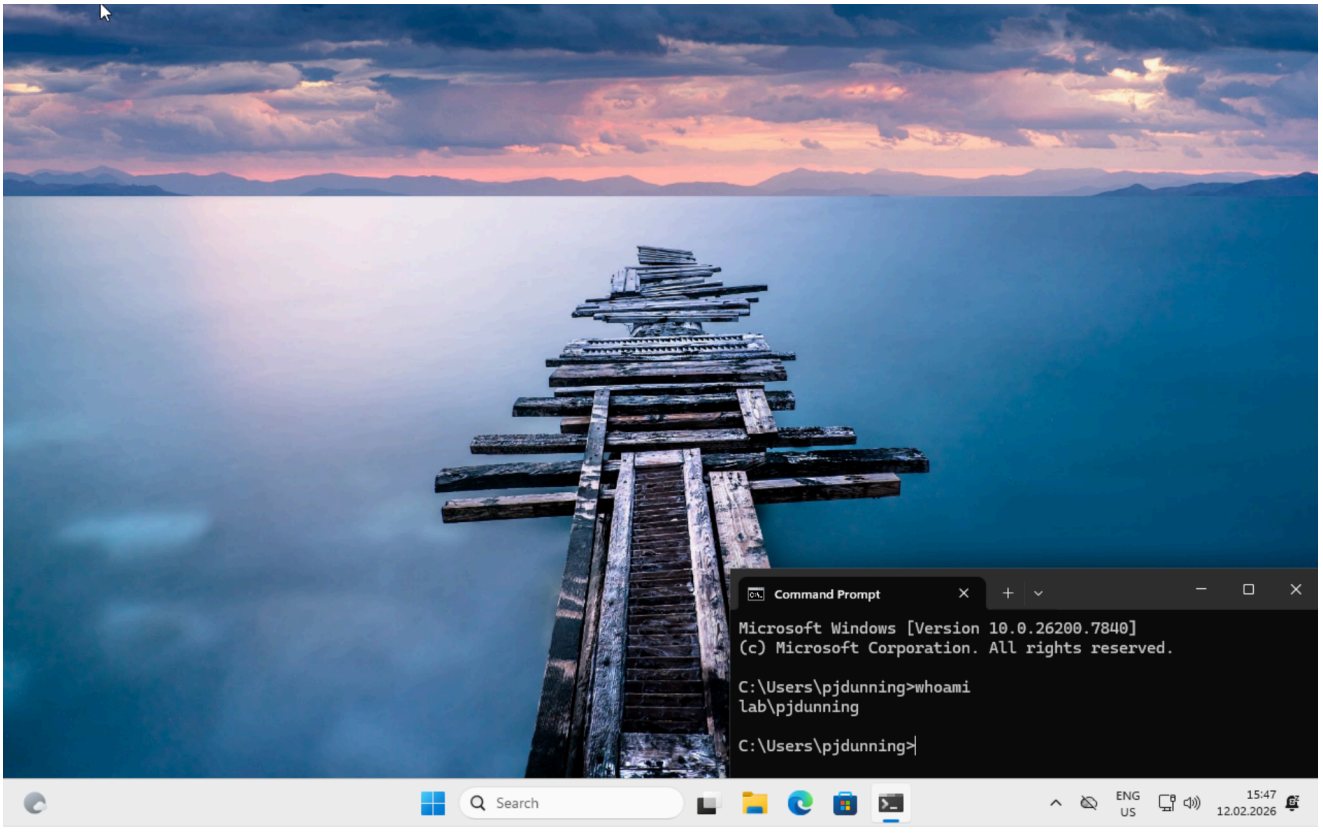
Manufacturing Group GPO

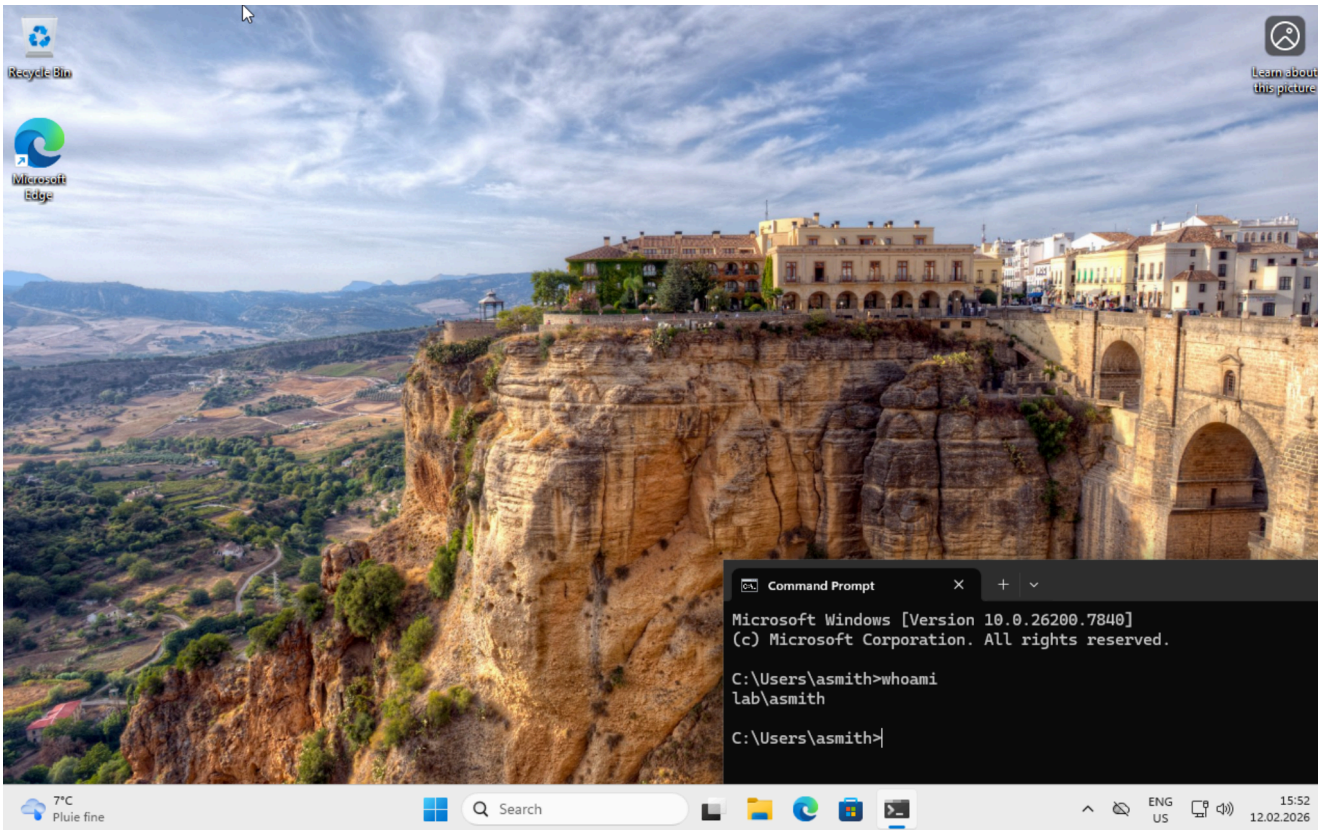
The GPO "MFG - GP" was created and linked to the "Manufacturing" OU
The object contains a simple, verifiable policy: Hide and Disable Desktop Icons



VALIDATING

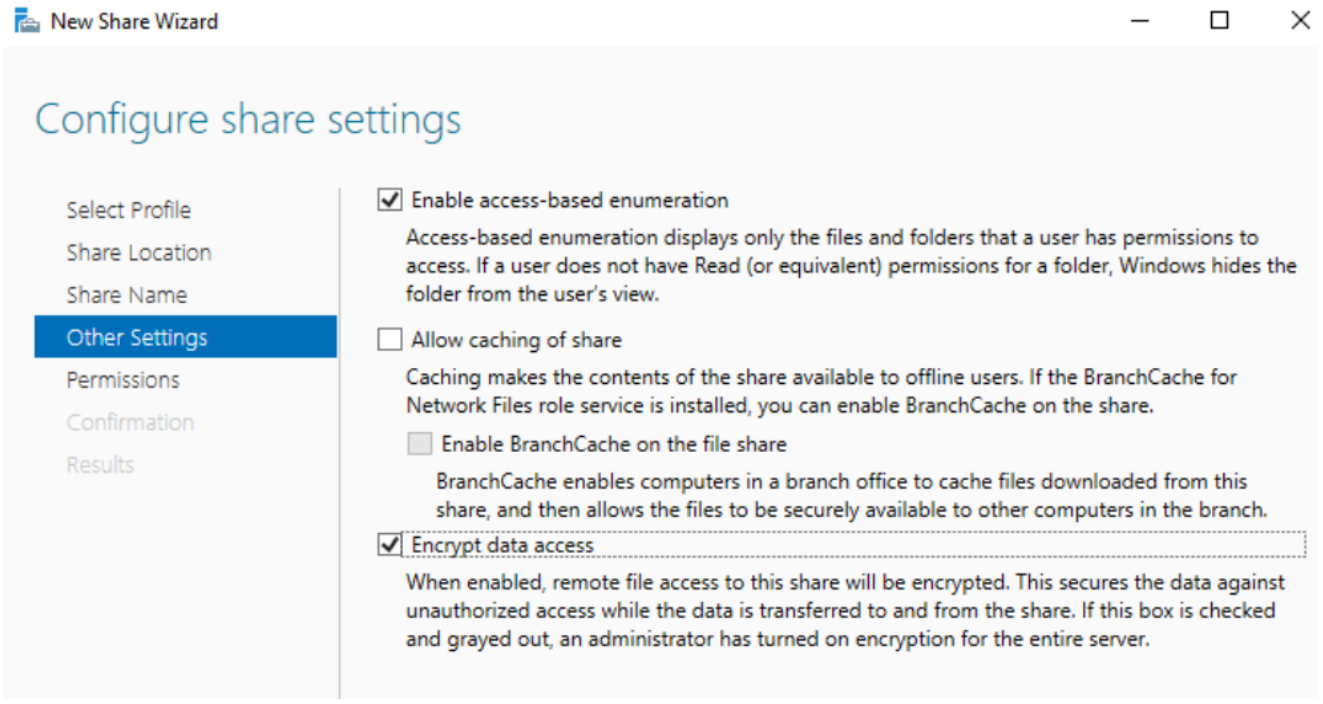
In order to validate the propagation, we compare below the resulting desktop environment of the accounts P. J. Dunning, assigned to Manufacturing, with that of Amber Smith, assigned to HR. We can clearly verify the change has taken effect, and only within the intended scope.





RESOURCE PERMISSIONS

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



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

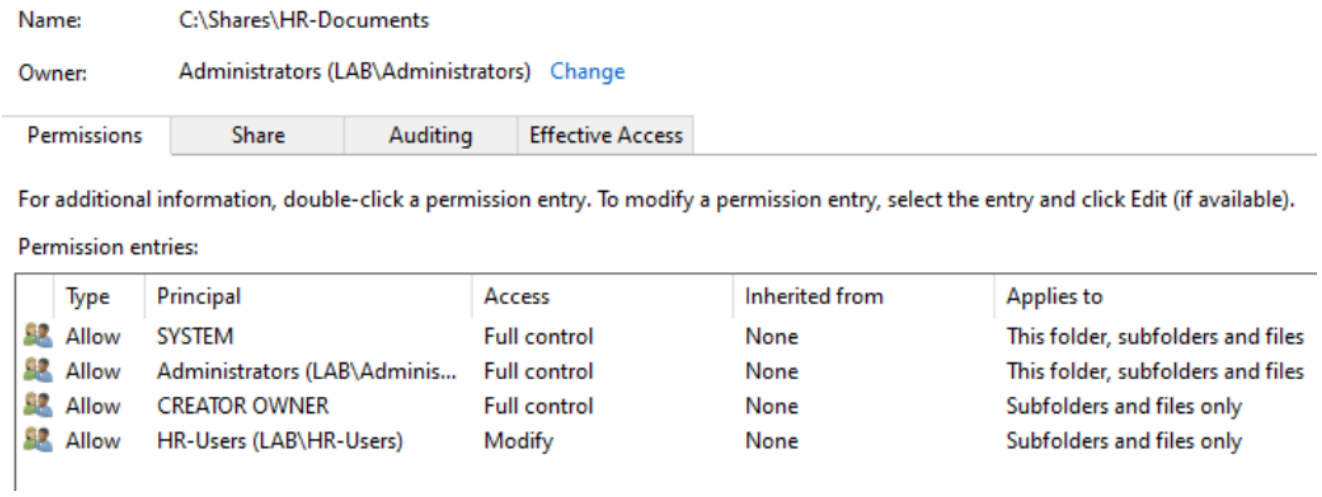
- facilitate access revocation and prevent abuse

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



ISSUE ENCOUNTERED

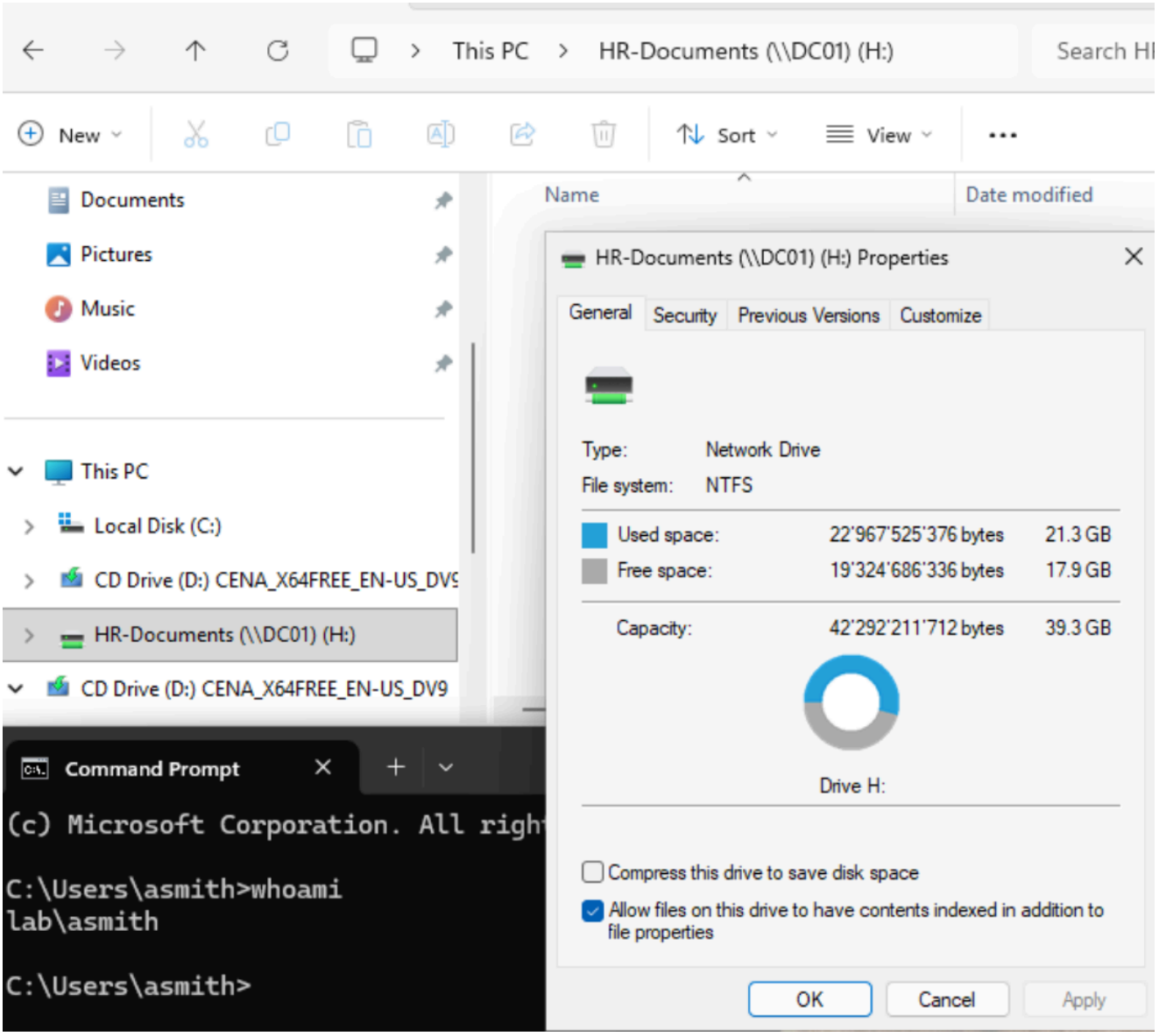
Despite correct configuration of NTFS and Share permissions, the intended test user - asmith@lab.local - HR users (Group) - was not granted the Modify permissions.

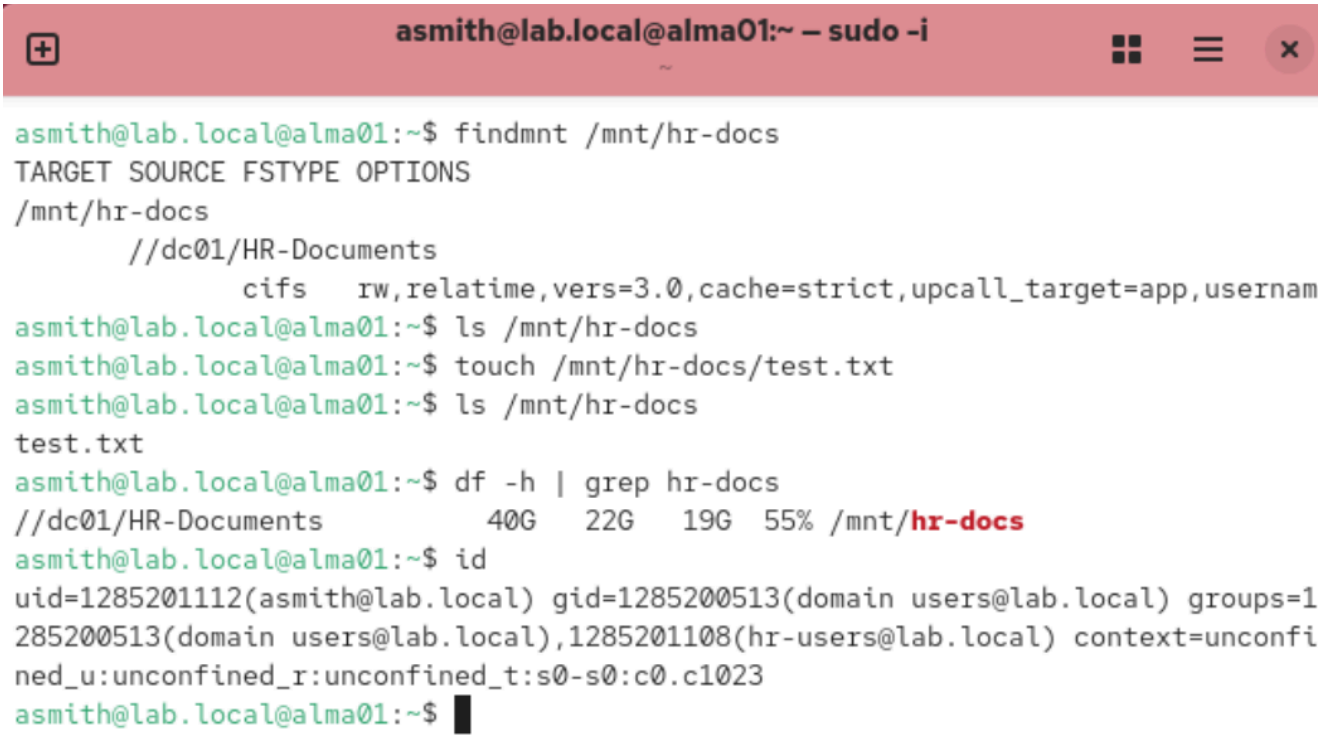
SOLUTION

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.

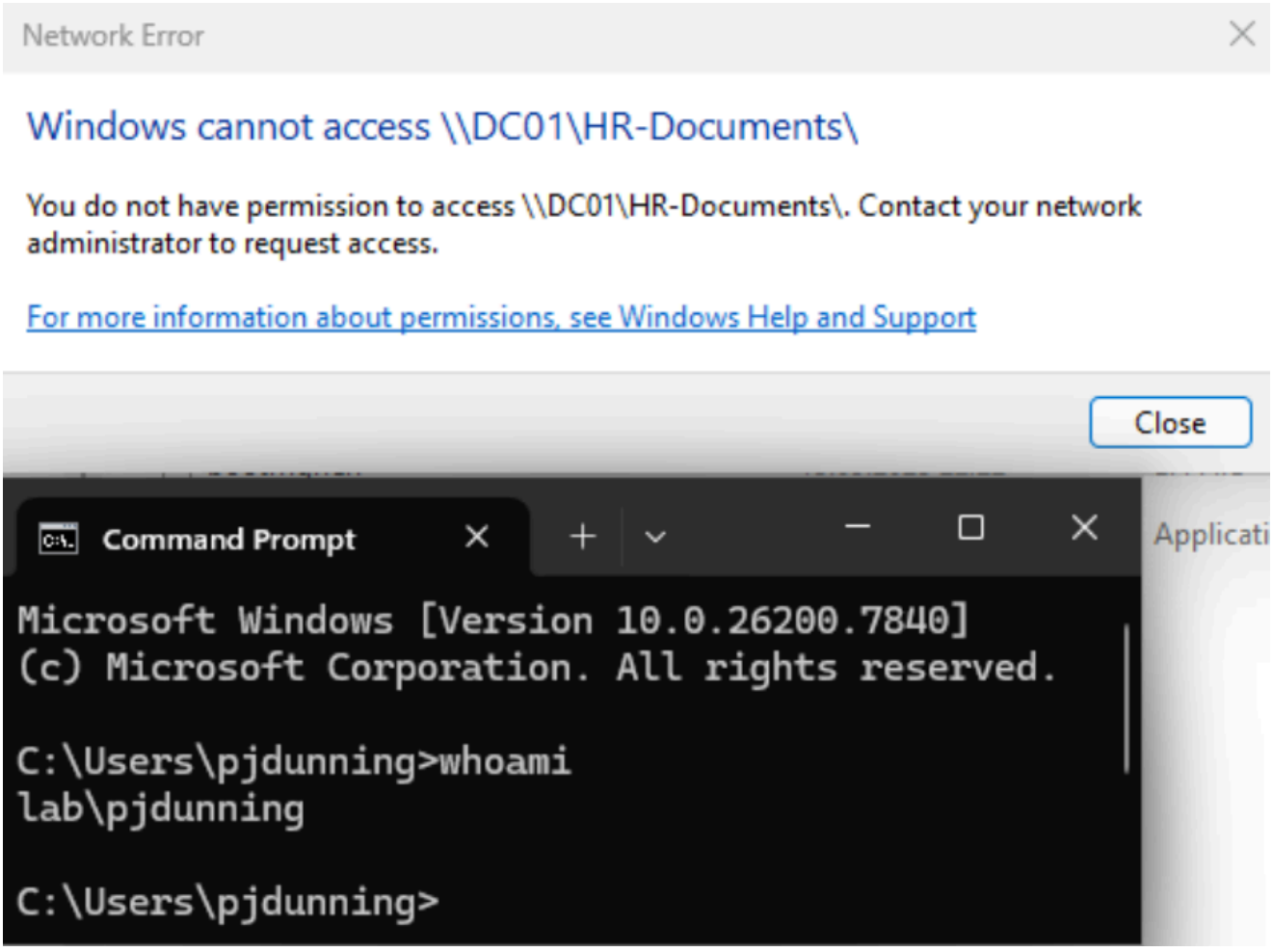
VALIDATION

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:





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



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