**Al-Najah National University**
**Network Administration Lab**

# File Server

**Instructor:Dr. Ahmed Awad**

**Mohammed Adnan**
**Dima Bshara**
**Sineen Bazyan**

# 1 Abstract

The experiment aims to build a clear idea about the file server through the way of managing it and dealing with the file server rules then accessing the shares. Also clarifies the file server sharing activity by dealing with users and groups. Also, it helps in managing the group's permission and policy.

# 2 Introduction

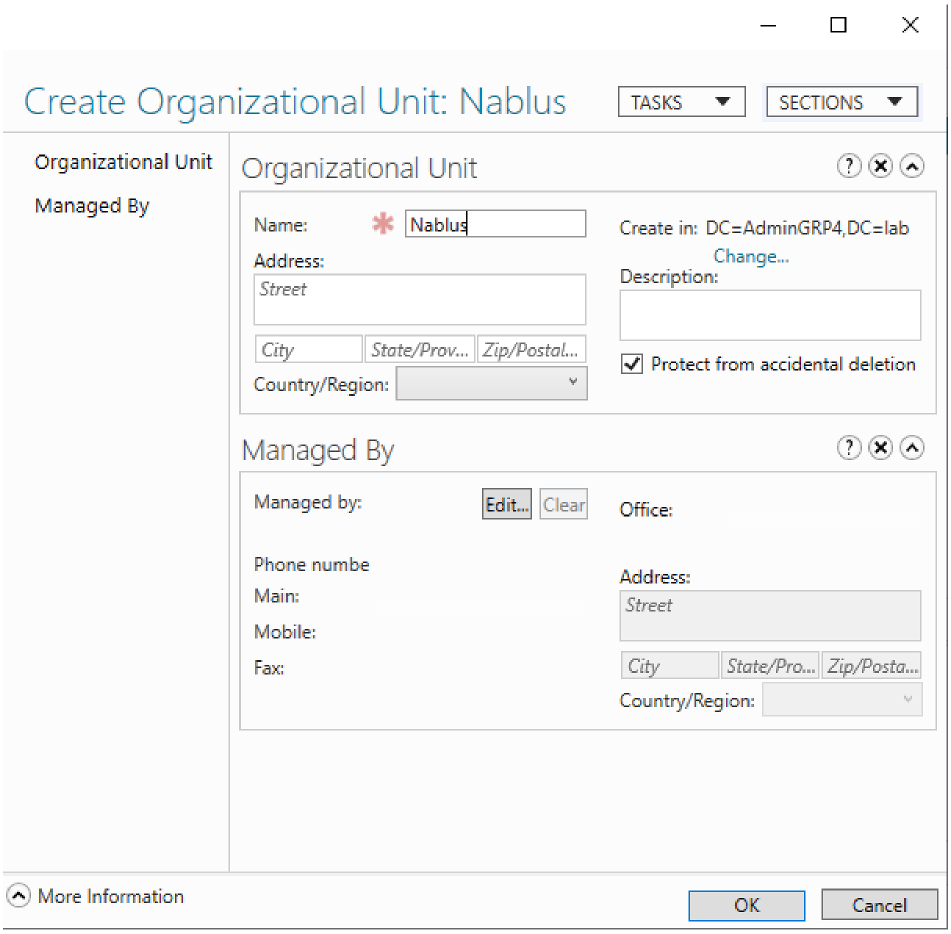
Most seasoned administrators are familiar with the fact that New Technology File System (NTFS) permissions are available on every file, folder, registry key, printer, and Active Directory object. NTFS is a type of file system used by the Windows NT operating system which is intended specifically to be highly portable. In the client or server model, a file server is a computer responsible for the central storage and management of data files to allow other computers on the same network to access the files. Information can be shared over a network without having to physically transfer files by floppy diskette or some other external storage device. Also using the Server Message Block (SMB) protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server. SMB can also communicate with any server program that is set up to receive an SMB client request, in other words, it is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba. The last thing to be mentioned, an Organizational Unit (OU) that provides a way of classifying objects located in directories, typically used either to differentiate between objects with the same name or to parcel out authority to create and manage objects.

The Active Directory groups are a collection of Active Directory objects. The group can include users, computers, other groups, and other AD objects. The administrator manages the group as a single object. Active Directory groups can be used to simplify the administration by assigning share (resource) permissions to a group rather than individual users (when you assign permissions to a group, all of its members have the same access to the resource). Also, to delegate the control by assigning user rights to a group using group policies. In the future, you can add new members to the group who need the permissions granted by this group. On the other hand, for years, IT administrators have been relying on logon scripts for mapping users' network drives in a Windows domain environment. But, more recently, administrators have found an effective alternative in group policy preferences and are increasingly making the switch. Mapping network drives using group policy preferences is flexible, provides easy control over who receives the drive mappings, and has easy-to-use user interfaces, all of which are in stark contrast with the complexities associated with scripts. To make it clear, group policy preferences are a set of extensions that increase the functionality of Group Policy Objects (GPOs). The drive maps policy in group policy preferences allows an administrator to map network drives via Group Policy. But, to map a network drive, users must be granted permission by their department or supervisor to access the material.

# 3 Procedure

## 3.1 Setting up the File server rule

1. On our domain controller in active directory users and computers, we Create a new OU named Nablus and create another one called Servers inside the Nablus OU. As shown in figures 1 and 2.



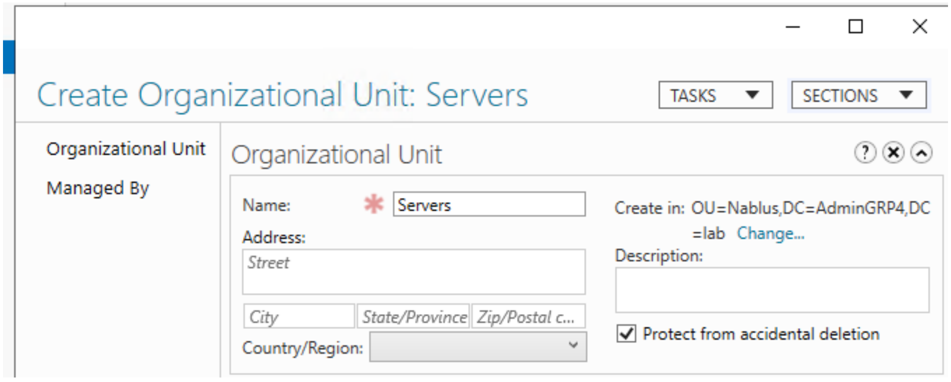
Create Organizational Unit: Nablus

Name: * Nablus

Create in: DC=AdminGRP4,DC=lab

☑ Protect from accidental deletion

Figure 1: "create OU"



Create Organizational Unit: Servers

Name: * Servers

Create in: OU=Nablus,DC=AdminGRP4,DC=lab

☑ Protect from accidental deletion

Figure 2: "create servers OU"

2. Then,we Find our file server object in the Computers OU and move it to Nablus/Servers, As figure 3 show.

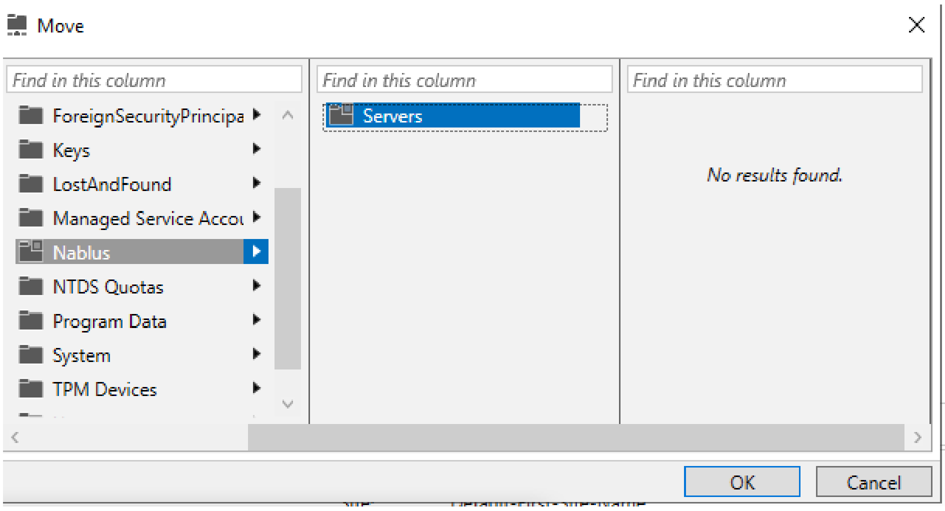
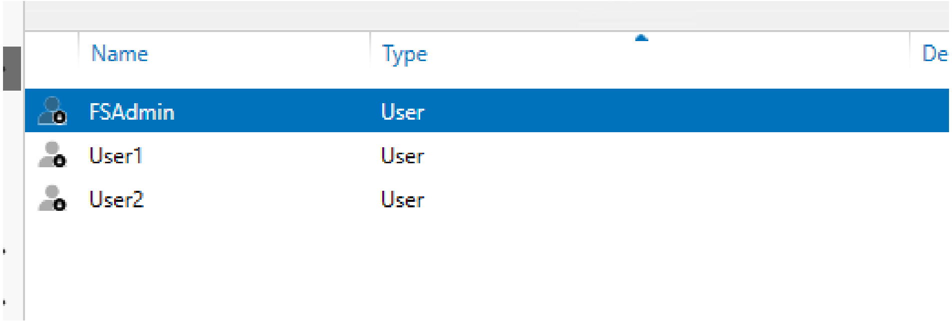


Figure 3: "Move servers Object"

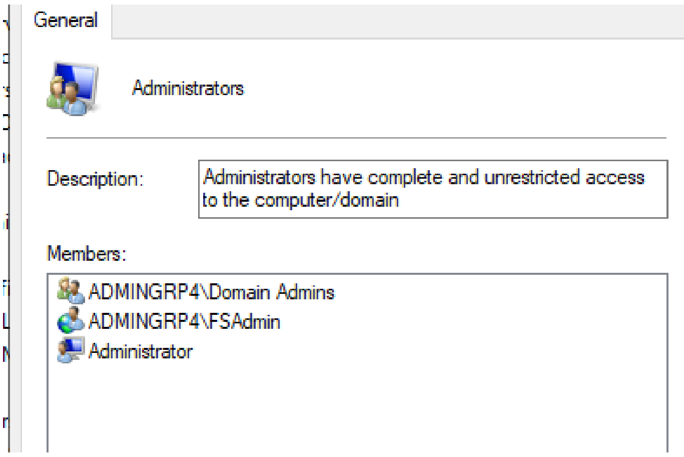
3. After that, we Create a nablus/Users OU and inside it we Create three users [ FSAdmin, User1, User2], as shown in figure 4.



| Name | Type | De |
|---|---|---|
| FSAdmin | User | |
| User1 | User | |
| User2 | User | |

Figure 4: "create users"

4. Then, we log in to the File server using the FSAdmin account, and we give FSAdmin administrative to have complete access to a computer, as figure 5 shows that we add it to the administrator group. Then we log out and log in to see that the access change and the FSadmin have now full access as shown in figure 6. After that we install file server into FSAdmin as shown in figure 7.



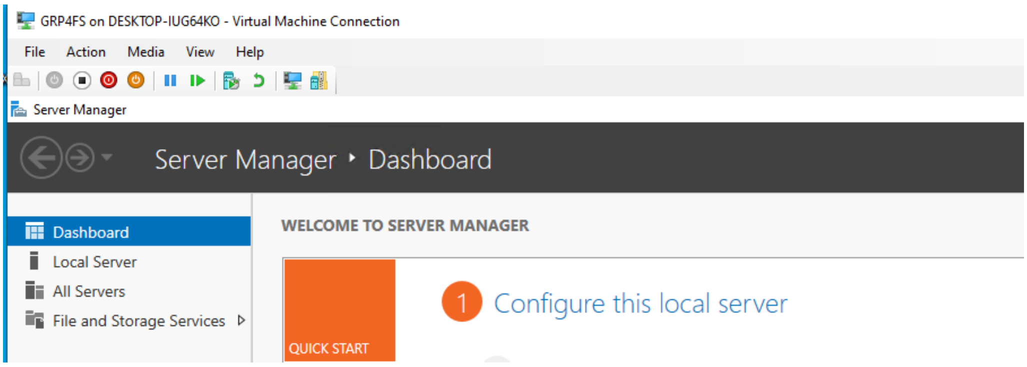
Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

ADMINGRP4\Domain Admins
ADMINGRP4\FSAdmin
Administrator

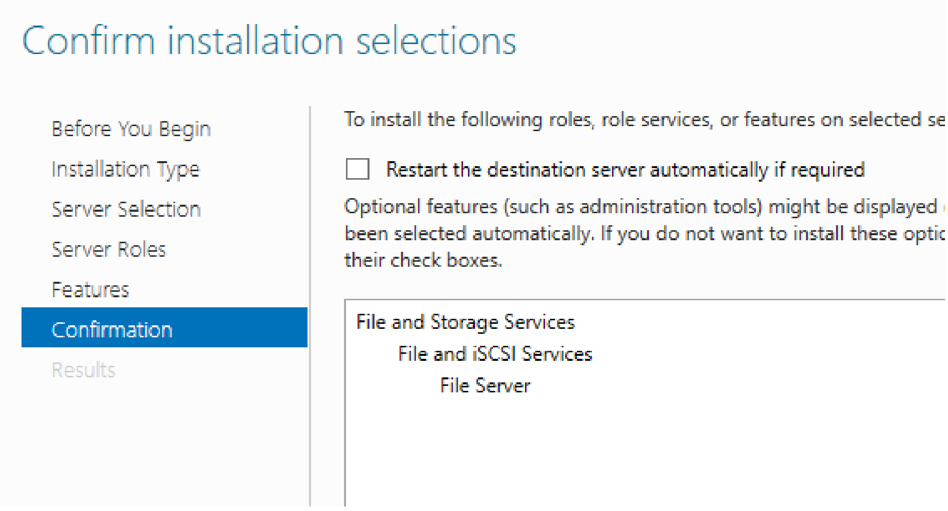
Figure 5: ”give FSAdmin administrative”


GRP4FS on DESKTOP-IUG64KO - Virtual Machine Connection

WELCOME TO SERVER MANAGER

1 Configure this local server

Figure 6: ”logout/login”


Confirm installation selections

To install the following roles, role services, or features on selected se

□ Restart the destination server automatically if required

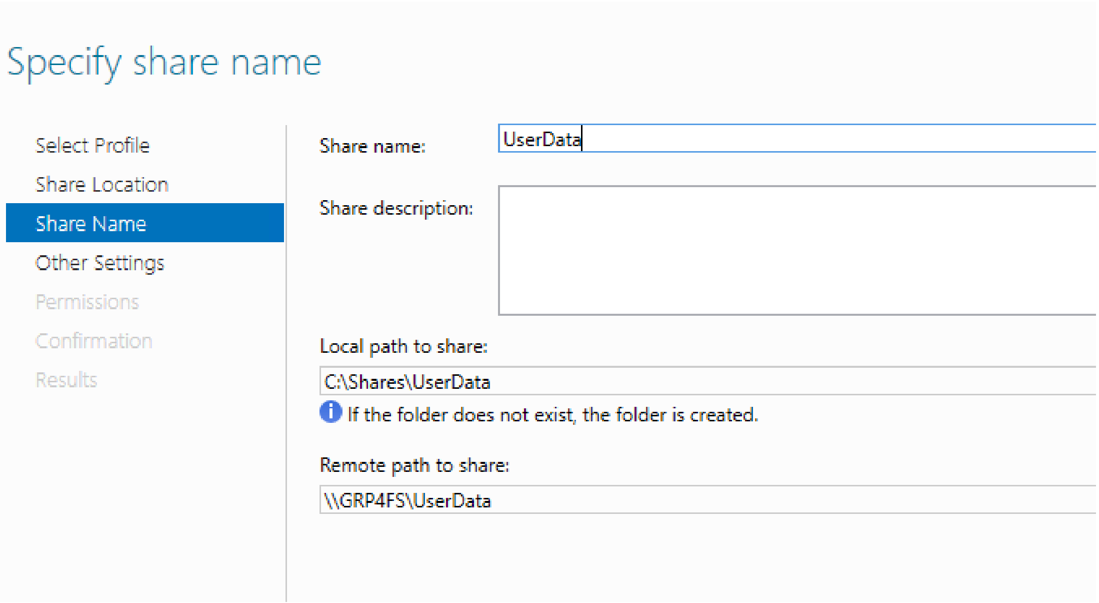
Optional features (such as administration tools) might be displayed
been selected automatically. If you do not want to install these optic
their check boxes.

File and Storage Services
File and iSCSI Services
File Server

Figure 7: ”install File server”

## 3.2 Managing the File Server

1. At first, we create file sharing (SMB-share) as shown in figure 8. After that, we made Enable access-based enumeration as figure 9 shows.



Specify share name

Share name: UserData

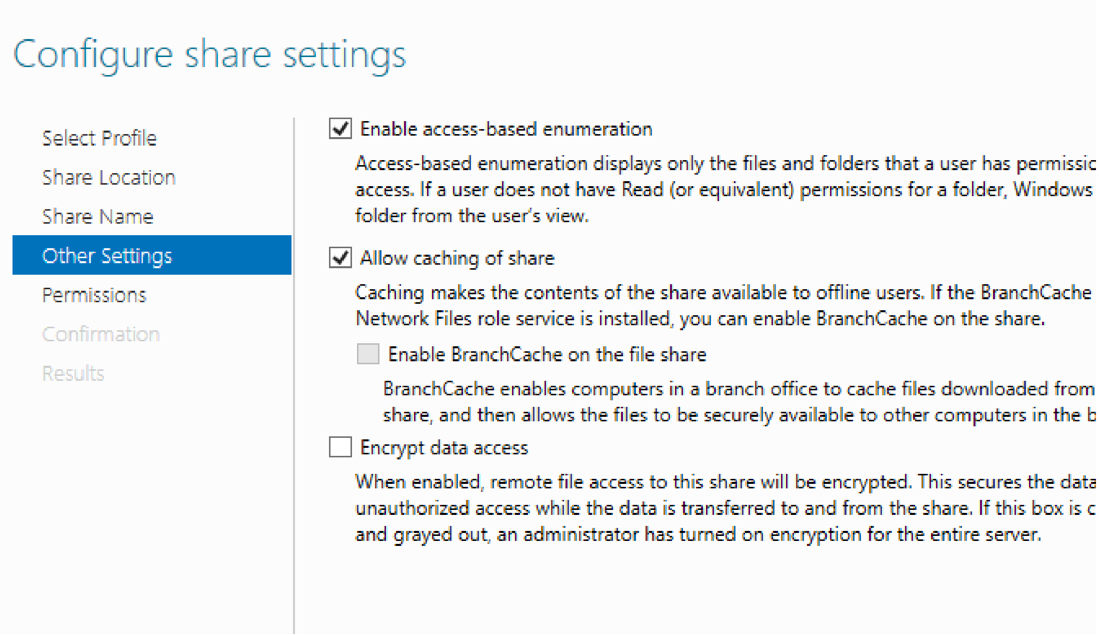
Share description:

Local path to share:
C:\Shares\UserData

If the folder does not exist, the folder is created.

Remote path to share:
\\GRP4FS\UserData

Figure 8: ”Create file sharing”



Configure share settings

☑ Enable access-based enumeration

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

☑ Allow caching of share

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

□ Enable BranchCache on the file share

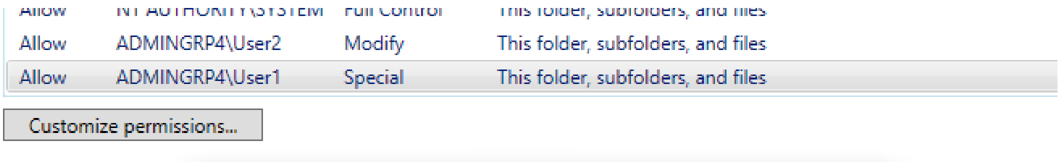
BranchCache enables computers in a branch office to cache files downloaded from
share, and then allows the files to be securely available to other computers in the b

□ Encrypt data access

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

Figure 9: ”Enable access-based enumeration”

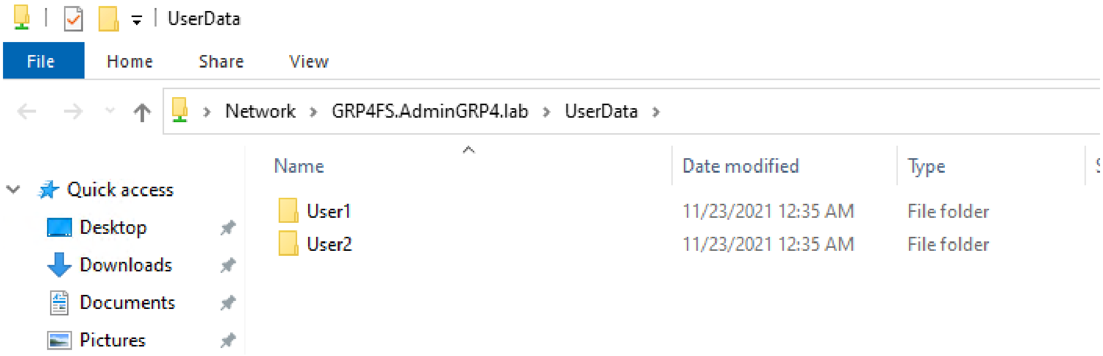
2. After that, we change permission for both users, so User1 will have special permission which read, write & execute. User2 will have Modify that will allow him to remove files, unlike User1. Figure 10 show those permissions.



| | | | |
|---|---|---|---|
| Allow | NT AUTHORITY\SYSTEM | Full Control | This folder, subfolders, and files |
| Allow | ADMINGRP4\User2 | Modify | This folder, subfolders, and files |
| Allow | ADMINGRP4\User1 | Special | This folder, subfolders, and files |

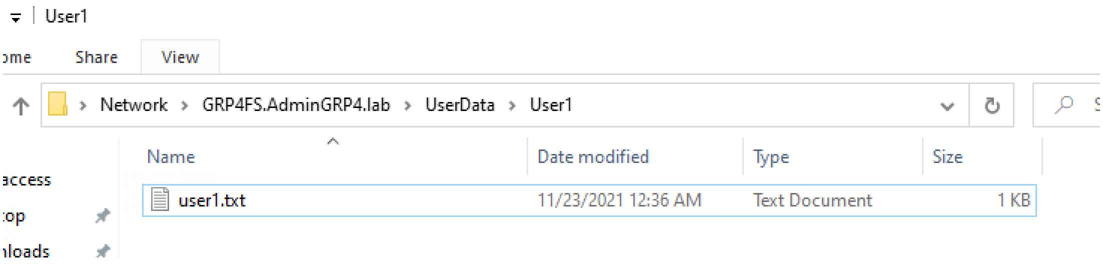
Figure 10: ”Users permissions”

3. Then, In folder UserData we create two new folders on named User1 and the other User2. And we using notepad to create a text file with text string “user1” inside and save it in User1 folder with the name user1.txt. As shown in figures 11 and 12.



| Name | Date modified | Type |
|---|---|---|
| User1 | 11/23/2021 12:35 AM | File folder |
| User2 | 11/23/2021 12:35 AM | File folder |

Figure 11: ”Create folders in UserData shared folder”

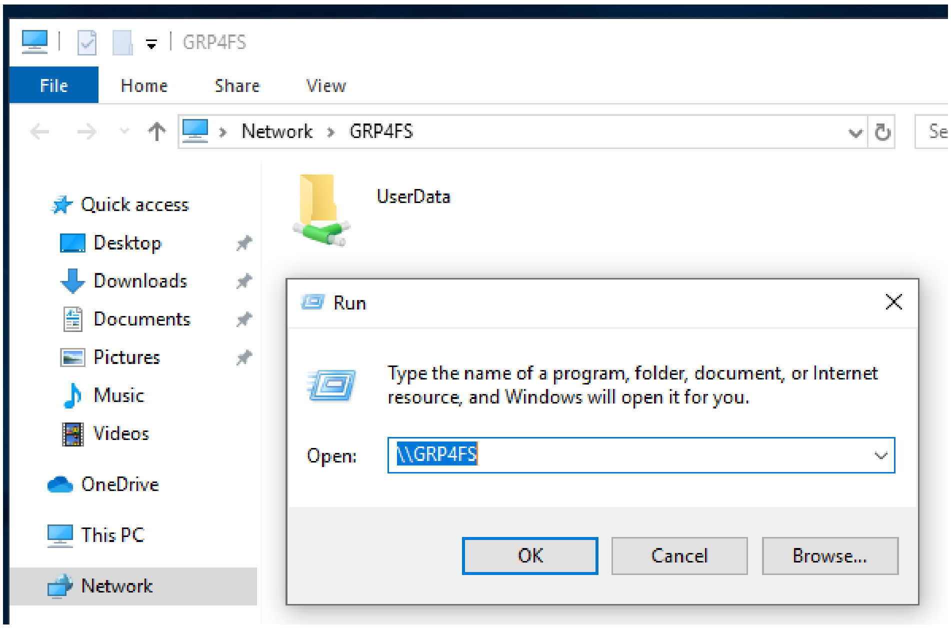


| Name | Date modified | Type | Size |
|---|---|---|---|
| user1.txt | 11/23/2021 12:36 AM | Text Document | 1 KB |

Figure 12: ”Create text inside both folders”

### 3.3 Accessing the Shares

1. In Client1 with user User1, the run was opened so we typed GRPxFS then we hit enter, as shown in Figure 13

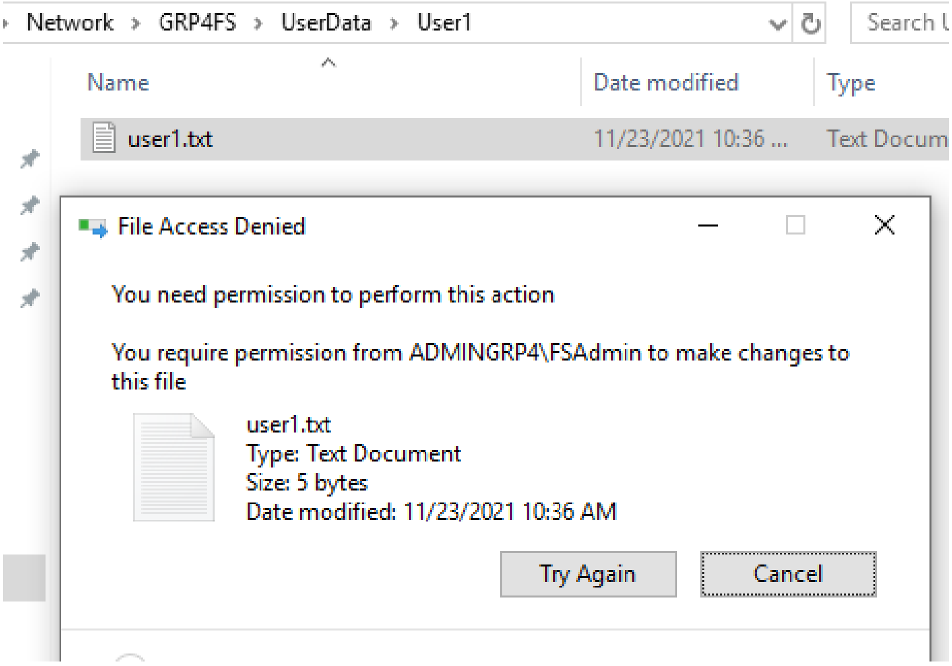


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\GRP4FS

Figure 13: Open ”GRP4FS”

2. The UserData/User1 folder was opened and then we tried to delete User1.txt, we weren’t able to do so, as shown in Figure 14



| Name | Date modified | Type |
|---|---|---|
| user1.txt | 11/23/2021 10:36 ... | Text Docum |

File Access Denied

You need permission to perform this action

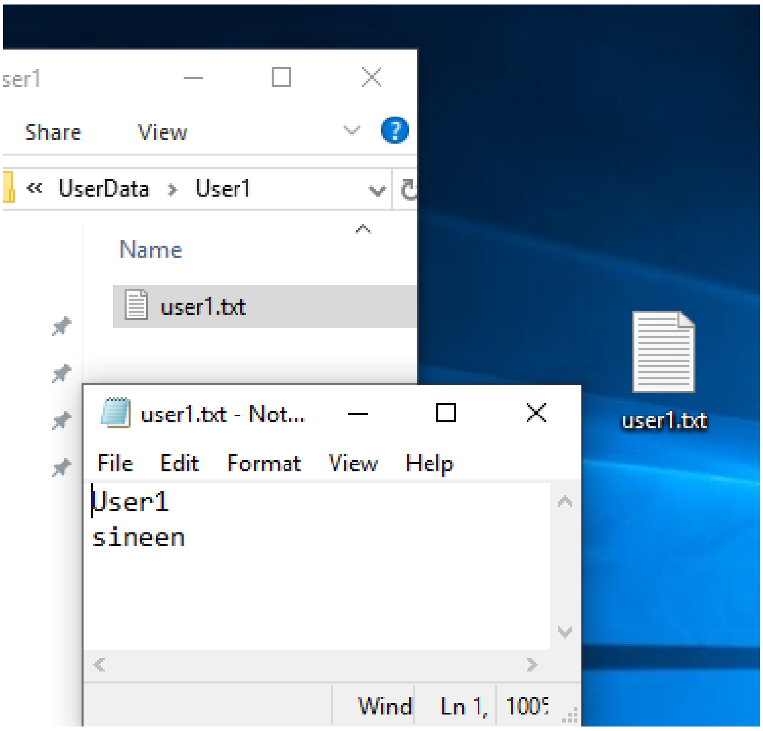
You require permission from ADMINGRP4\FSAdmin to make changes to this file

user1.txt
Type: Text Document
Size: 5 bytes
Date modified: 11/23/2021 10:36 AM

Figure 14: Failed to remove the user1.txt

3. A new text file was created and wrote something then saved. We have deleted the file we created and we successfully did it because we are the owner.

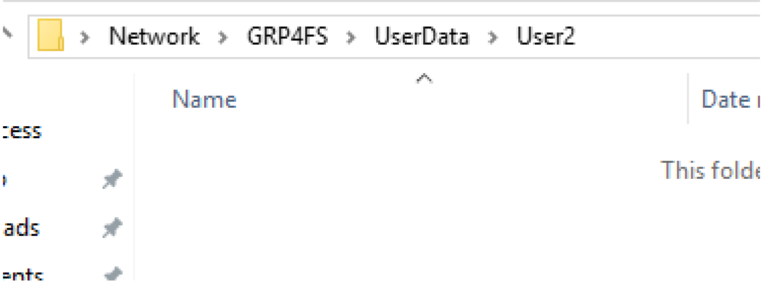
4. user1.txt was opened and modified the contents and saved. This would prompt us to create a copy of the file, as shown in Figure 15.



```
User1
sineen
```

Figure 15: Modify the user1.txt

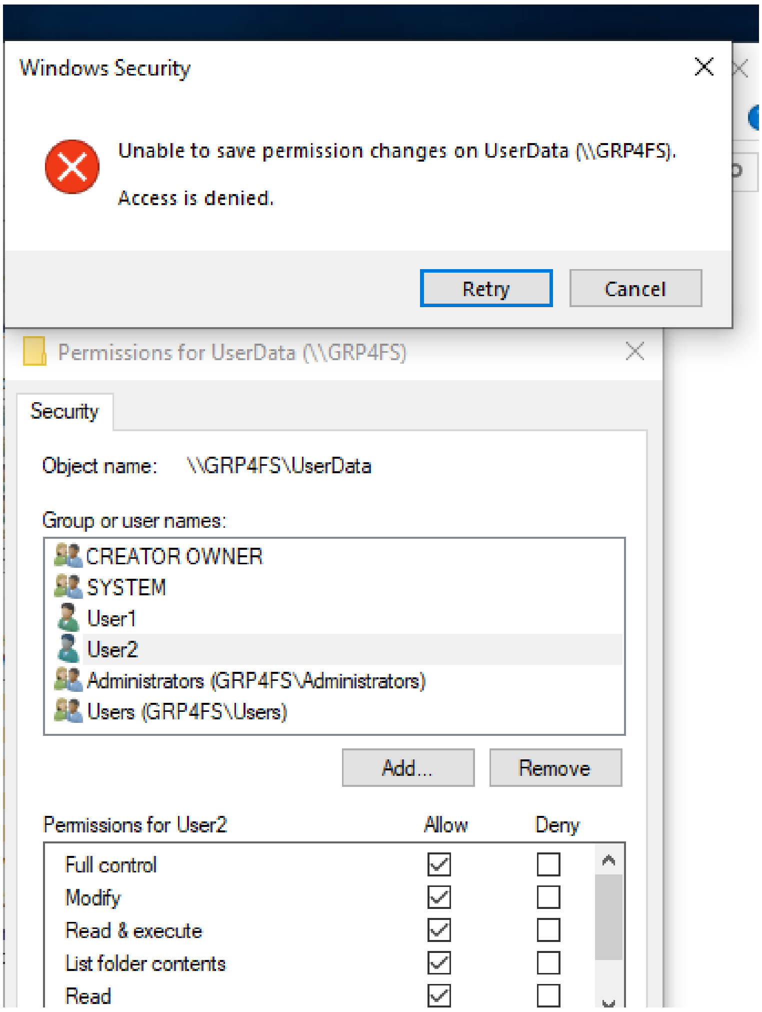
5. In Client2 with user User2 logged in the run was opened and we typed //GRPxFS and hit enter.
6. We opened the User2 folder and we deleted user2.txt, we were able to do so because we have Modify permission, as shown in Figure 16.



This folde

Figure 16: Empty folder after removing the file

7. . We tried to change user2s' permission by right-clicking anywhere then properties –¿ security –¿ edit, but we were not able to do so, as shown in Figure 17.



Windows Security

Unable to save permission changes on UserData (\\GRP4FS).

Access is denied.

Permissions for UserData (\\GRP4FS)

Object name: \\GRP4FS\UserData

Group or user names:

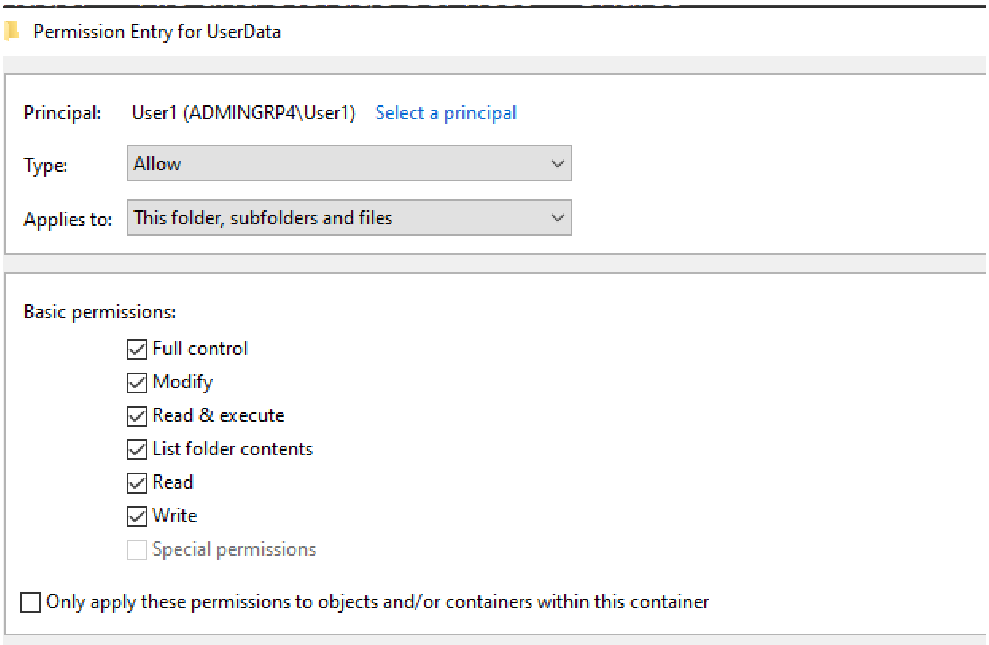
- CREATOR OWNER
- SYSTEM
- User1
- User2
- Administrators (GRP4FS\Administrators)
- Users (GRP4FS\Users)

| Permissions for User2 | Allow | Deny |
|---|---|---|
| Full control | ☑ | □ |
| Modify | ☑ | □ |
| Read & execute | ☑ | □ |
| List folder contents | ☑ | □ |
| Read | ☑ | □ |

Figure 17: Error message

8. In the permissions for user2 dialog box we clicked on user1 and tried to give him modify permission, this also failed.

9. On GRPxFS we went to C://shares and we opened the permissions of the UserData folder and gave User1 full control, as shown in figure 18.



Permission Entry for UserData

Principal: User1 (ADMINGRP4\User1) Select a principal

Type: Allow

Applies to: This folder, subfolders and files

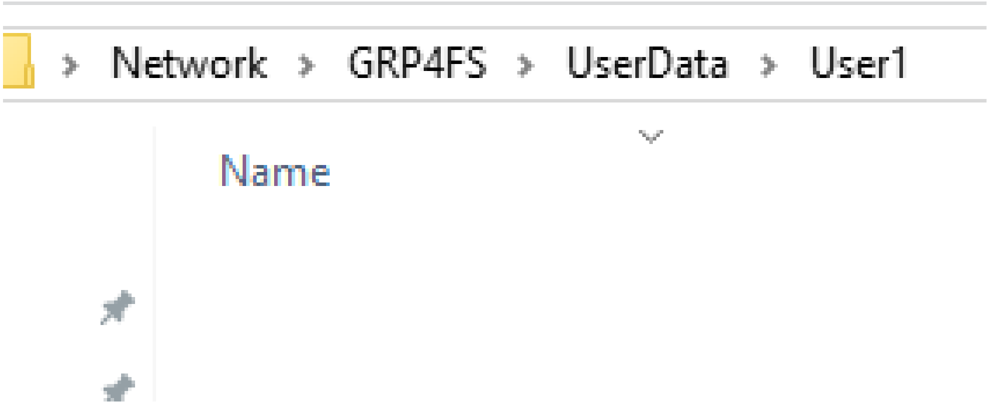
Basic permissions:

☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

□ Only apply these permissions to objects and/or containers within this container

Figure 18: change permissions

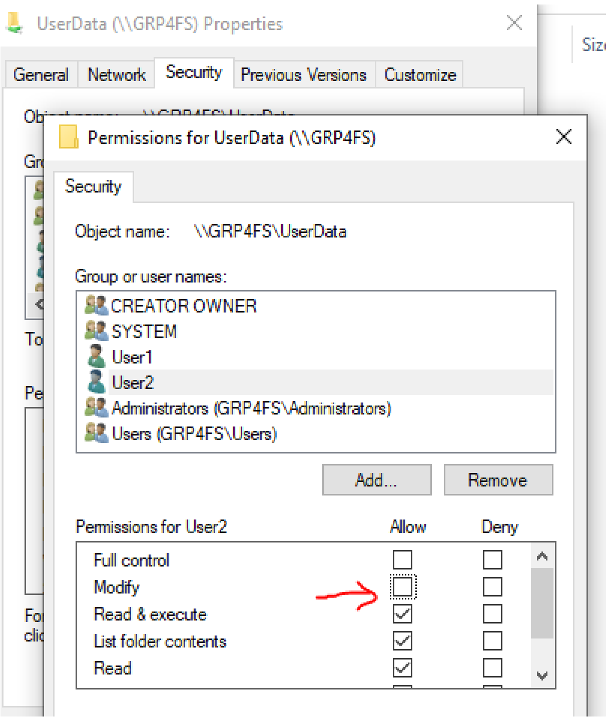
10. On Client1 with user1 logged in we opened //GRPxFS/UserData and we opened the permissions.
11. user1.txt file was deleted. Because we are permitted, as shown in Figure 19.



Network › GRP4FS › UserData › User1

Figure 19: Empty folder after removing the file

12. By right-clicking anywhere, we opened permissions and we changed user2s' permissions by removing his modify permissions, as shown in Figure 20.



Permissions for UserData (\\GRP4FS)

Security

Object name: \\GRP4FS\UserData

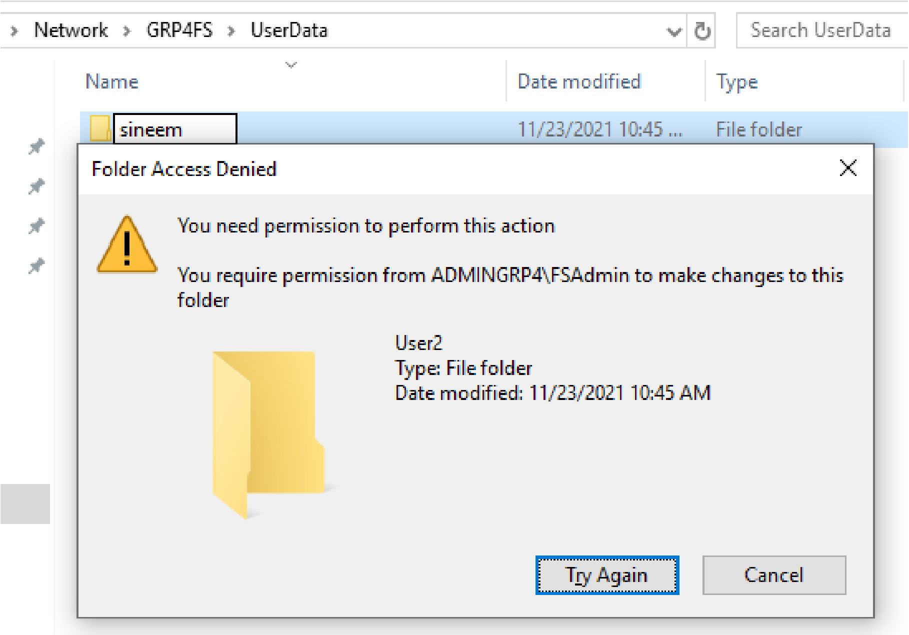
Group or user names:

- CREATOR OWNER
- SYSTEM
- User1
- User2
- Administrators (GRP4FS\Administrators)
- Users (GRP4FS\Users)

| Permissions for User2 | Allow | Deny |
|---|---|---|
| Full control | □ | □ |
| Modify | □ | □ |
| Read & execute | ☑ | □ |
| List folder contents | ☑ | □ |
| Read | ☑ | □ |

Figure 20: Remove the modify permission

13. On Client2 with user2 logged in we opened UserData and we checked our permissions then we tried to rename the User2 folder and it failed, as shown in Figure 21.



Folder Access Denied

You need permission to perform this action

You require permission from ADMINGRP4\FSAdmin to make changes to this folder

User2
Type: File folder
Date modified: 11/23/2021 10:45 AM

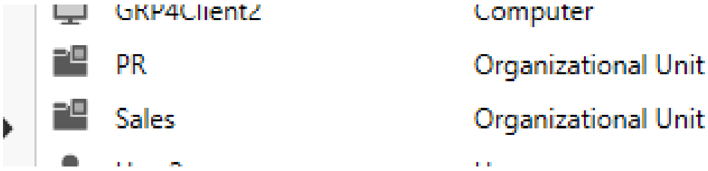
Figure 21: Access denied

# 4 Users And Groups

## 4.1 User setup

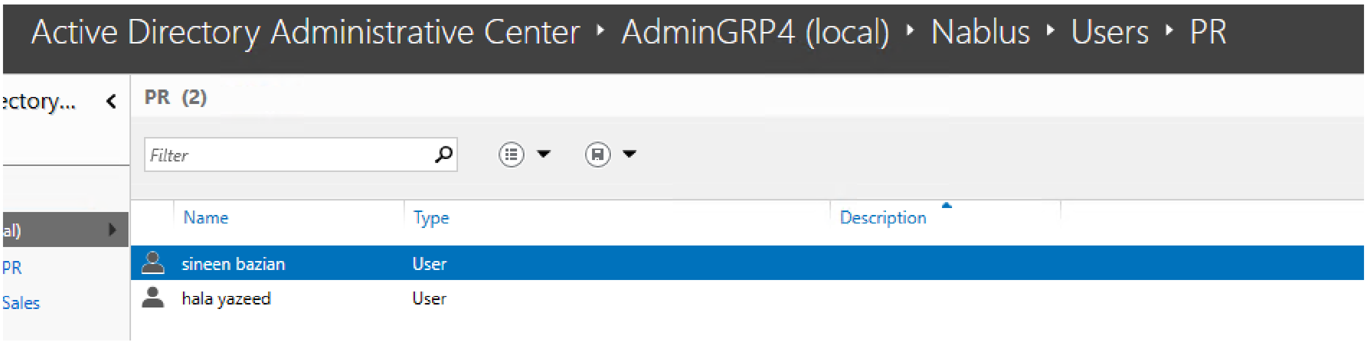
For this lab, we create a few users. All users are domain users in the Nablus branch with an initial password of **P$$w0rd** . All users with a password that doesn't expire and cannot change their passwords. To make our job as a domain admin easier we create two OUs one for each of the departments.

Inside NablusOU we create two OUs, Sales and PR as figure 22 shows. Then create 4 user inside each of the OUs as shown in figures 23 and 24.



| | |
|---|---|
| GRP4Client2 | Computer |
| PR | Organizational Unit |
| Sales | Organizational Unit |

Figure 22: Create OUs

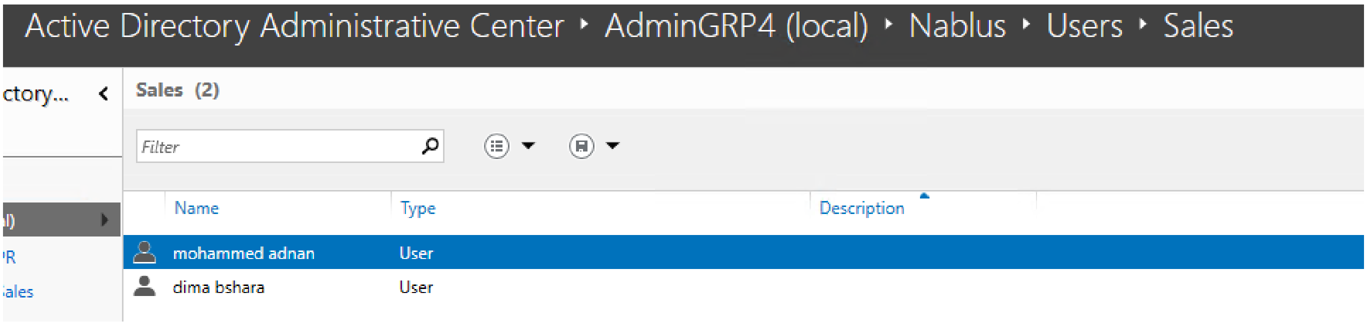


Active Directory Administrative Center ‣ AdminGRP4 (local) ‣ Nablus ‣ Users ‣ PR

PR (2)

| Name | Type | Description |
|---|---|---|
| sineen bazian | User | |
| hala yazeed | User | |

Figure 23: Create users inside PR



Active Directory Administrative Center ‣ AdminGRP4 (local) ‣ Nablus ‣ Users ‣ Sales

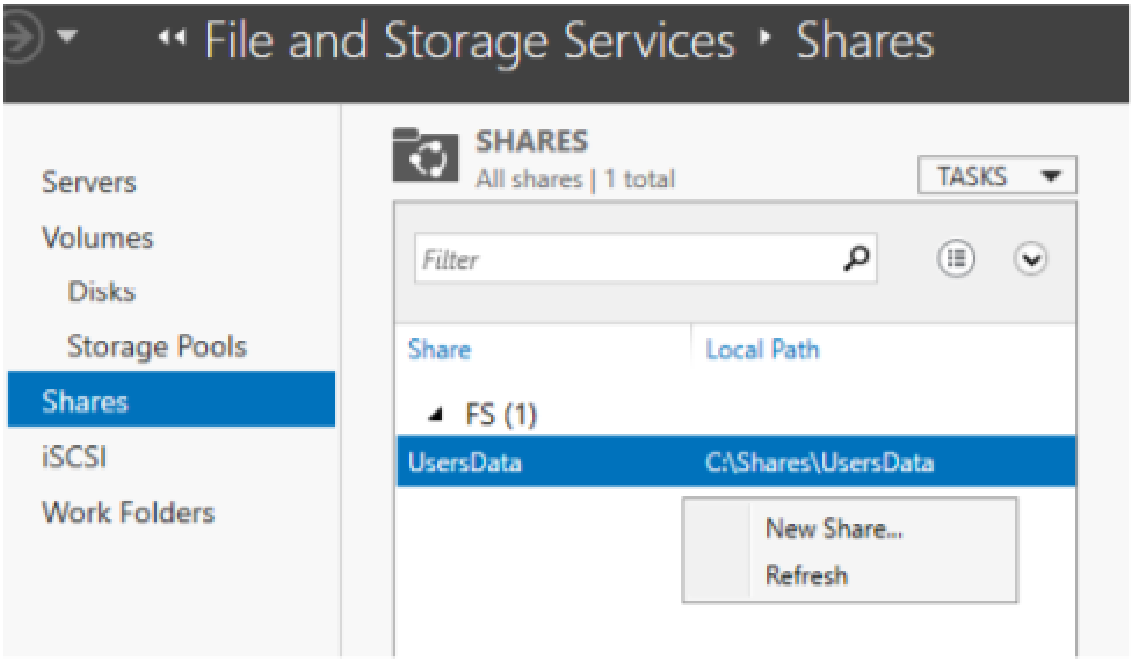
Sales (2)

| Name | Type | Description |
|---|---|---|
| mohammed adnan | User | |
| dima bshara | User | |

Figure 24: Create users inside sales

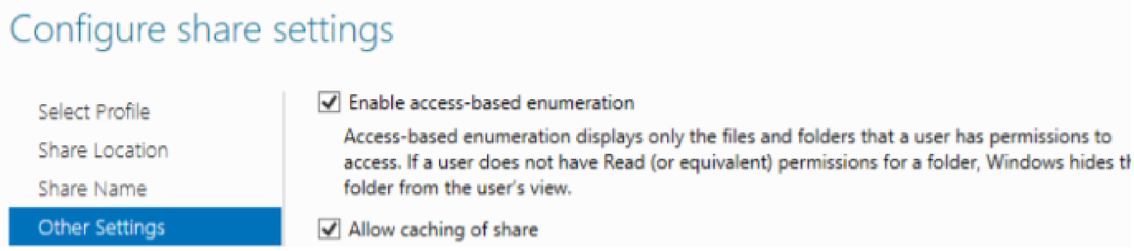
## 4.2 File Server shares

The organization has a specific workflow that dictates having a central Directory where every department has a shared folder where all employees have full access to their departments' directory on the file server. We create the user shares on the files server named Sales and another one called PR,following these steps, first, we create a new shared directory as figure 25 show and enable access-based enumeration option as figure 26 show. The resulting shares are as follows 27



| Share | Local Path |
|---|---|
| FS (1) | |
| UsersData | C:\Shares\UsersData |

Figure 25: Create a new shared folder

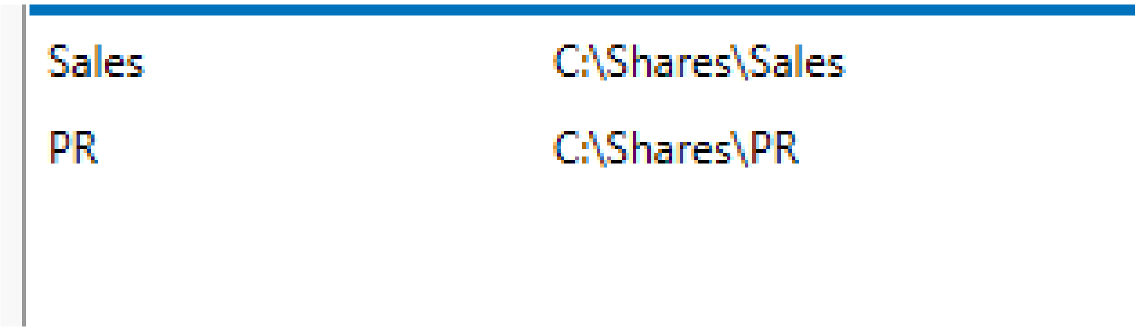


☑ Enable access-based enumeration

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 tl folder from the user's view.

☑ Allow caching of share

Figure 26: Enable access-based enumeration



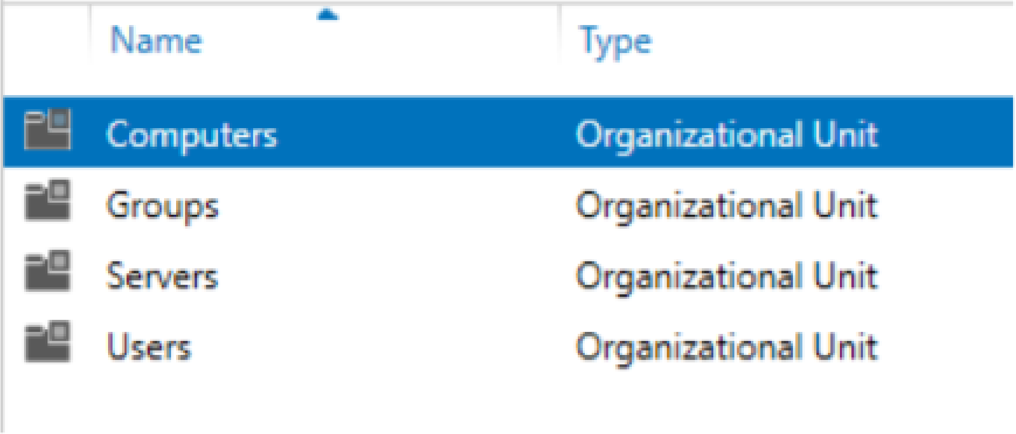
| | |
|---|---|
| Sales | C:\Shares\Sales |
| PR | C:\Shares\PR |

Figure 27: Files server named Sales & PR

## 4.3 Groups and permissions

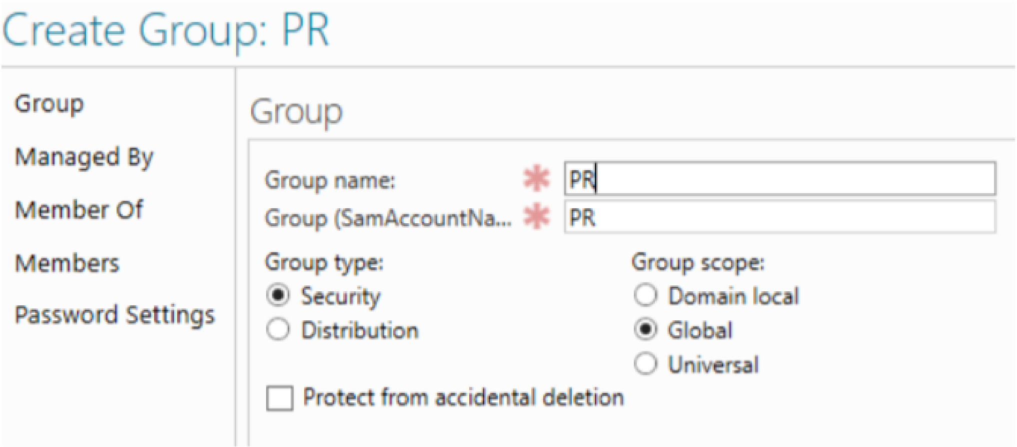
To scale with the permissions we create user groups that will make assigning access permissions to our shares easier and more efficient. On our DC server:

1. We create a new OU inside Nablus OU and call it Groups as figure 28 show, then inside this Groups OU we create a group called Sales and another one called PR as figure 29 shows. The figure30 shown final result.



| Name | Type |
|---|---|
| Computers | Organizational Unit |
| Groups | Organizational Unit |
| Servers | Organizational Unit |
| Users | Organizational Unit |

Figure 28: Create a new OU



Create Group: PR

Group

Group name: * PR

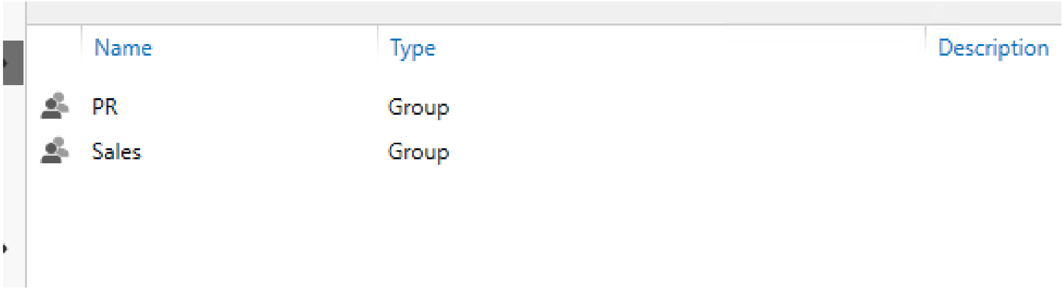
Group (SamAccountNa... * PR

Group type:
● Security
○ Distribution

Group scope:
○ Domain local
● Global
○ Universal

□ Protect from accidental deletion

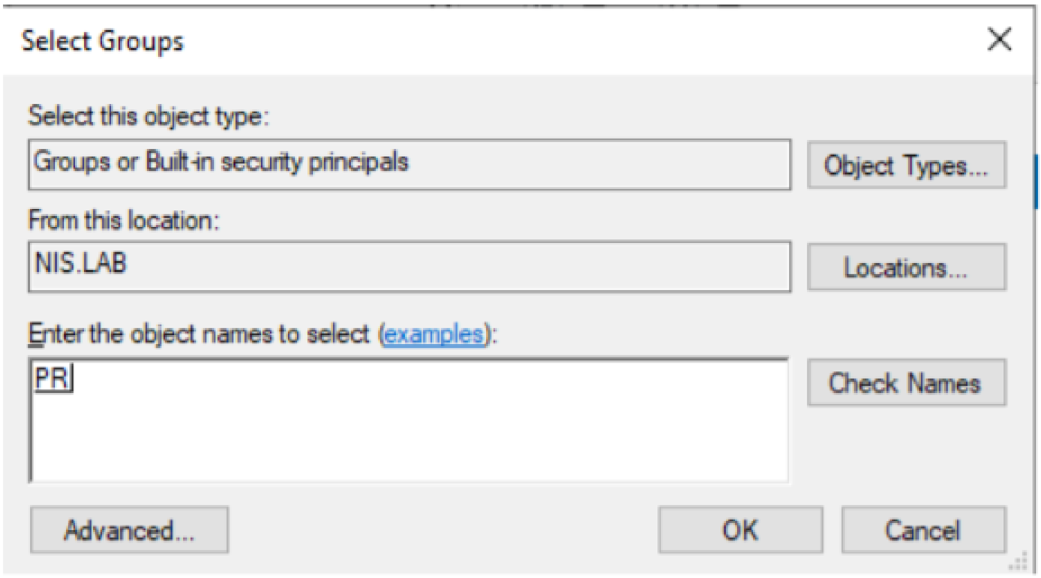
Figure 29: Create A new group



| Name | Type | Description |
|---|---|---|
| PR | Group | |
| Sales | Group | |

Figure 30: The groups

2. Then add each employee to the corresponding group. Right click a user and select add to group. Write the name of the groups and click check names select and verify as figure 31 shows.



Select Groups

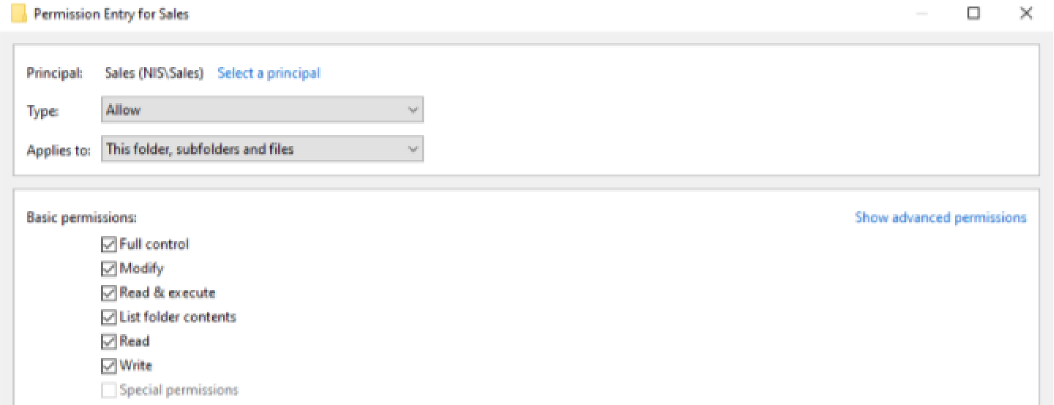
Select this object type:
Groups or Built-in security principals

From this location:
NIS.LAB

Enter the object names to select (examples):
PR

Figure 31: Add an employee to the corresponding group

3. After adding all users to their respective groups. In File and storage services (*\shares*)
   - We follow these steps to give the permissions:Right click the Sales shared folder and choose properties.
     Click Permissions then customize permissions.
     Click add then click select a principal and write sales in the box and confirm.
     In the Permission Entry for Sales, dialog box check the full control check box and click OK and confirm all open dialogs.
     The figure 32 show the final screen of permission Entry for sales.
     We did the same for PR share and PR user group.



Permission Entry for Sales

Principal: Sales (NIS\Sales) Select a principal

Type: Allow

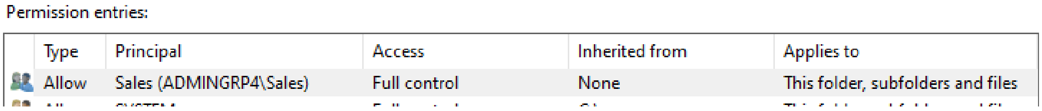
Applies to: This folder, subfolders and files

Basic permissions:

☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

Figure 32: Permission Entry for sales

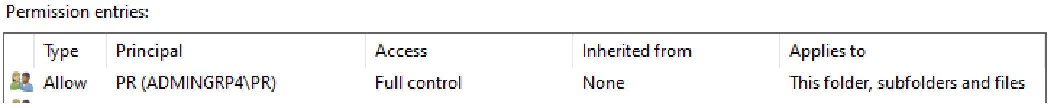
The figure 33,34 show the final result.



Permission entries:

| | Type | Principal | Access | Inherited from | Applies to |
|---|---|---|---|---|---|
| | Allow | Sales (ADMINGRP4\Sales) | Full control | None | This folder, subfolders and files |

Figure 33: Permission Entry for sales



Permission entries:

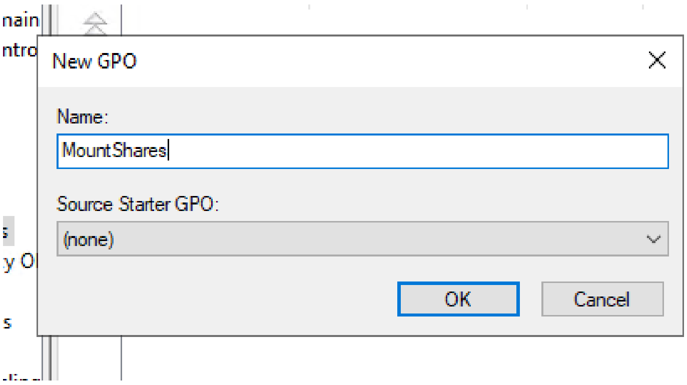
| | Type | Principal | Access | Inherited from | Applies to |
|---|---|---|---|---|---|
| | Allow | PR (ADMINGRP4\PR) | Full control | None | This folder, subfolders and files |

Figure 34: Permission Entry for PR

## 4.4 Group Policy

Group Policy is an integral feature built into Microsoft Active Directory. Its core purpose is to enable IT administrators to centrally manage users and computers across an AD domain. While mapping drives means that you're going to make a specific drive available to other users connected to a common network, mapping drives with group policy is very easy. It doesn't require any scripting experience, it's just a matter of a few clicks and select your desired settings.

1. On the Server Manager app of our domain controller, we opened group policy management from the Tools menu. Right-click the Sales OU and we chose " Create a GPO in this domain and link it here". Then, it was named MountShares, as shown in Figure 35.



Name: MountShares

Source Starter GPO: (none)

Figure 35: Create GPO

2. By Right-clicking the GPO called MountShares, we chose to edit. Navigate to User Configuration – Preferences – Windows Settings – Drive Maps, as shown in Figure 36.

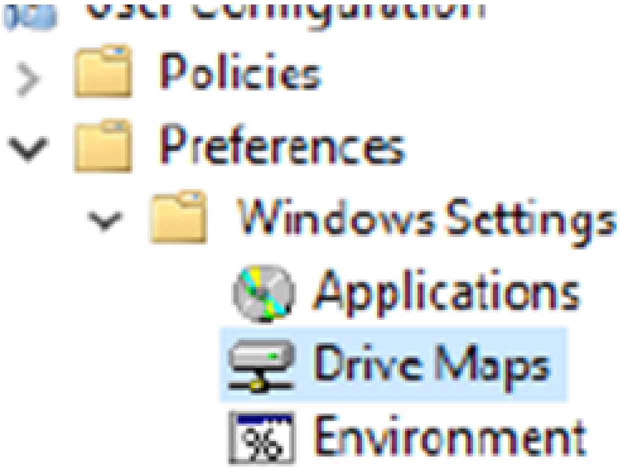
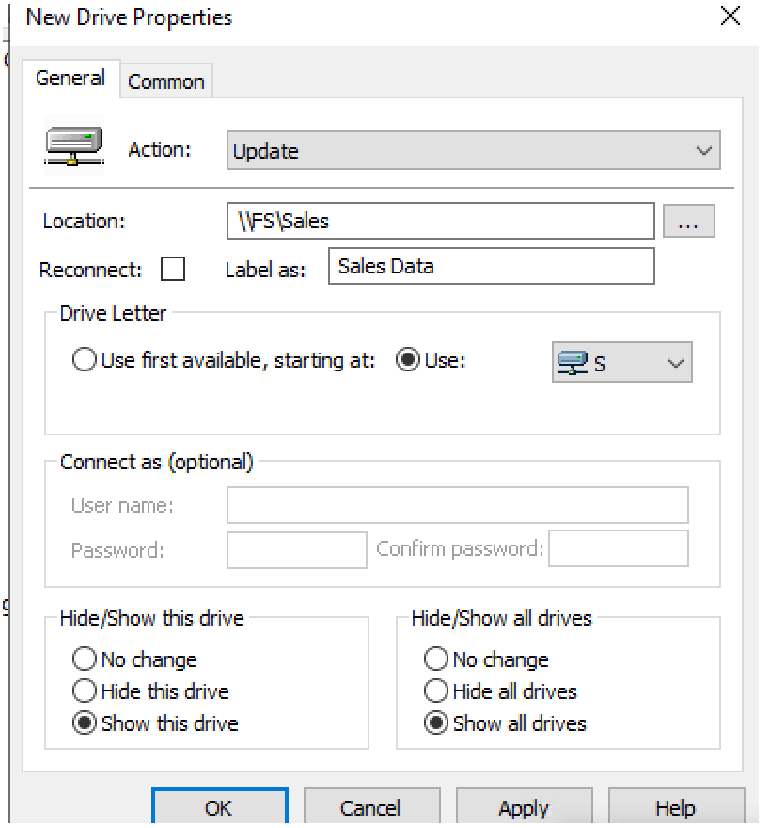


Figure 36: Drive Maps field

3. By Right-clicking Drive Maps we have created a new Mapped Drive and we Filled the fields as follows (GRP4FS is the file server name in our case), as shown in Figure 37.



New Drive Properties

General | Common

Action: Update

Location: \\FS\Sales

Reconnect: □ Label as: Sales Data

Drive Letter

○ Use first available, starting at: ● Use: S

Connect as (optional)

User name:

Password: Confirm password:

Hide/Show this drive

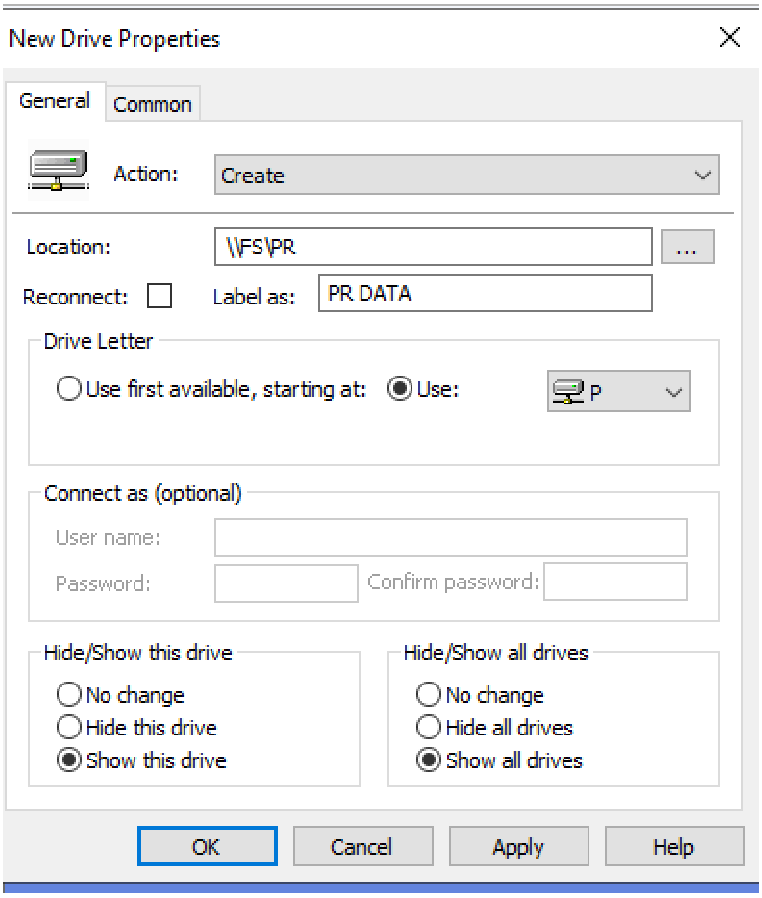
○ No change
○ Hide this drive
● Show this drive

Hide/Show all drives

○ No change
○ Hide all drives
● Show all drives

Figure 37: Set the sales drive properties

4. We did the same thing for the PR shared folder and the PR group, as shown in Figure 38



New Drive Properties

General | Common

Action: Create

Location: \\FS\PR

Reconnect: □ Label as: PR DATA

Drive Letter

○ Use first available, starting at: ● Use: P

Connect as (optional)

User name:

Password: Confirm password:

Hide/Show this drive

○ No change
○ Hide this drive
● Show this drive

Hide/Show all drives

○ No change
○ Hide all drives
● Show all drives

Figure 38: Set the PR drive properties

5. Then the new configuration was tested by logging in as a sales user to one machine and as a PR user to another machine, as shown in Figure 39 Figure 40.

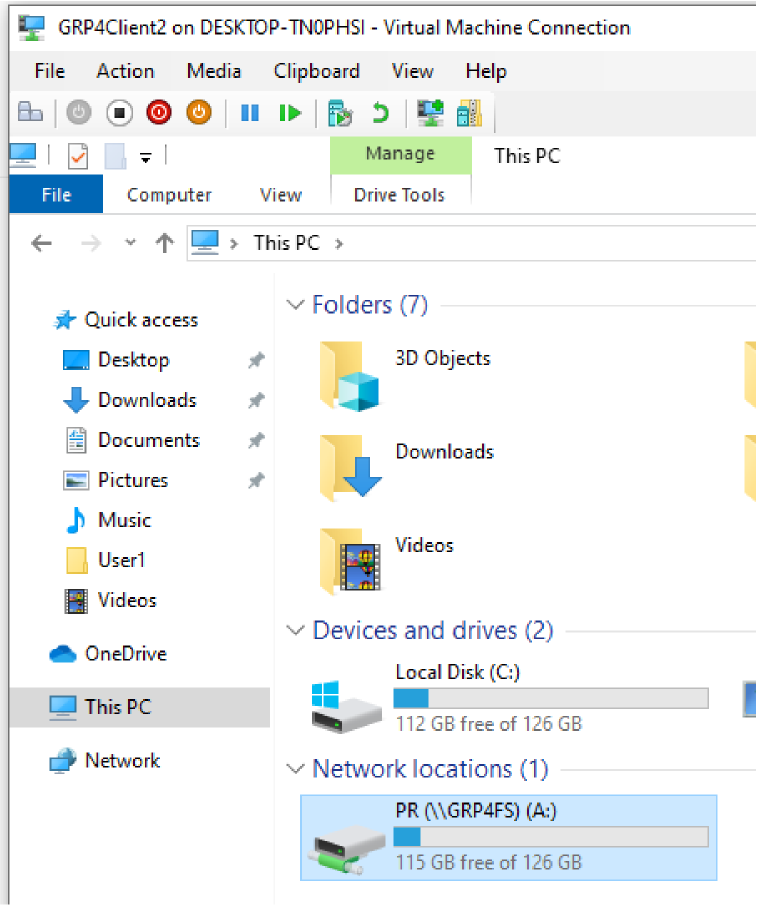


Figure 39: Login as a PR user

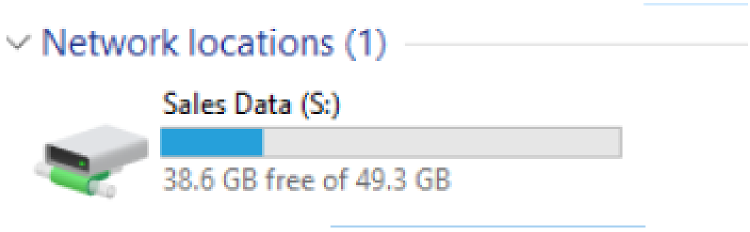


Figure 40: Login as a sales user

# 5 Conclusion

In the experiment, we went through how to create shared folders in the windows server. Using this experiment, we can specifically share one or multiple folders through the windows shared folder wizard. And we can make permission for the different users to access the files. It also, shows us the usage of users and groups and their advantages due to having strong manageable units. Plus the benefit of drive maps in storing files on network drives to provide a user more storage space, backups of their files, and secure ways of sharing files between departments.

# 6 References

https://howto.hyonix.com/article/create-shared-folders-in-windows-server/
https://www.bartleby.com/essay/File-Sharing-FKJEAC2ZVJ
https://www.osradar.com/how-to-enable-the-file-server-in-windows-server-2019/