

Users And Groups

Lab Setup

In this Lab we will be using the previously created VMs during the Windows Server and active Directory labs.

In total you will have 4 VMs:

1. Domain Controller VM.
2. File Server VM.
3. 2 client machines.

User Setup

For this lab we need to create a few users. All users are domain users in the **Nablus** branch with an initial password of **P@\$sw0rd** . All users with a password that doesn't expire and cannot change their passwords.

To make our job as a domain admin easier we need to create two OUs one for each of the departments mentioned in the user table below.

Inside Nablus\Users OU create two OUs, Sales and PR as follows:



PR

Organizational Unit



Sales

Organizational Unit

Create the users as follows [see example user below]:

| Full Name | User Name | Department/OU |
|----------------|-----------|---------------|
| Mohammad Ahmad | m.ahmad | Sales |
| Yousif Saed | y.saeed | Sales |
| Tariq Moneer | t.moneer | PR |
| Hala Yazeed | h.yazeed | PR |

Example User:

Create User: Mohammad Ahmad

TASKS SECTIONS

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Account

First name: Mohammad

Middle initials:

Last name: Ahmad

Full name: * Mohammad Ahmad

User UPN login: @

User SamAccountName... NIS * m.ahmad

Password:

Confirm password:

Create in: OU=Users,OU=Nablus,DC=NIS,DC=LAB Change...

☐ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ☒ Never ☐ End of

Password options:

☐ User must change password at next log on

☒ Other password options

☐ Microsoft Passport or smart card is required for interactive l...

☒ Password never expires

☒ User cannot change password

Encryption options:

Other options:

Organization

Display name: Mohammad Ahmad

Office:

E-mail:

Job title:

Department: Sales

Company:

Your Final Nablus\Users OU contents should look something like this after creating the users and OUs above mentioned:

◀ NIS (local) ▶ Nablus ▶ Users ▶

ry... < Users (5)

Filter

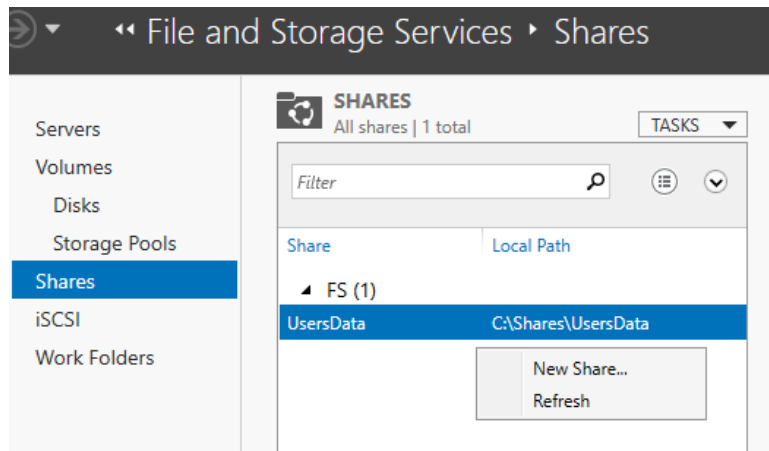
| Name | Type |
|---------|---------------------|
| FSAdmin | User |
| PR | Organizational Unit |
| Sales | Organizational Unit |
| user1 | User |
| User2 | User |

rol ▶

File Server Shares

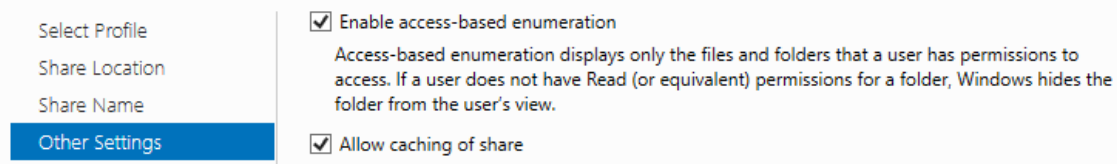
Our organization has a specific work flow that dictates having a central Directory where every department has a shared folder where all employees have full access to their departments' directory on the file server. We need to create the user shares on the files server as follows:

Create a shared directory named Sales and another one called PR:



Don't forget to set the Enable access-based enumeration option:

Configure share settings







The resulting shares are as follows:

| Share | Local Path |
|-----------|---------------------|
| FS (3) | |
| UsersData | C:\Shares\UsersData |
| Sales | C:\Shares\Sales |
| PR | C:\Shares\PR |

Groups and permissions

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

1. Create a new OU inside Nablus OU and call it Groups:

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

2. inside this Groups OU create a group called Sales and another one called PR:

Create Group: PR

| | |
|-------------------|-------|
| Group | Group |
| Managed By | |
| Member Of | |
| Members | |
| Password Settings | |

Group name: *

Group (SamAccountNa... *)

Group type:

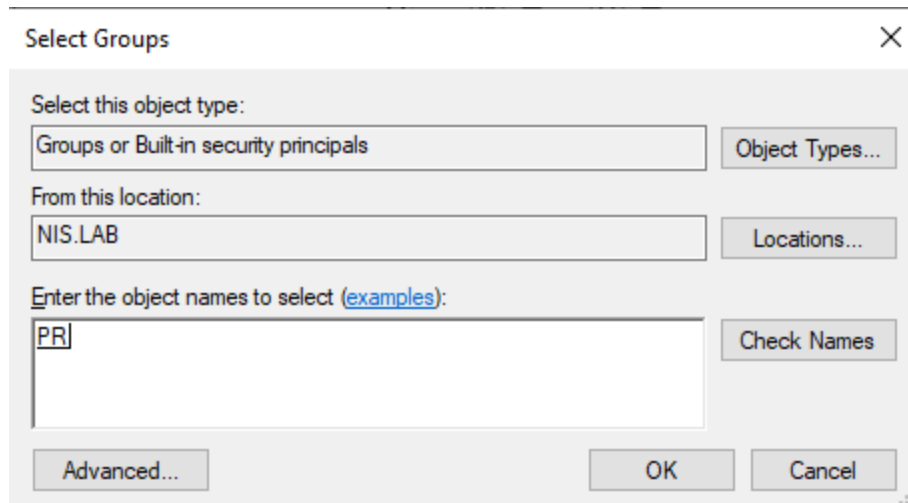
- ☒ Security
- ☐ Distribution

Group scope:

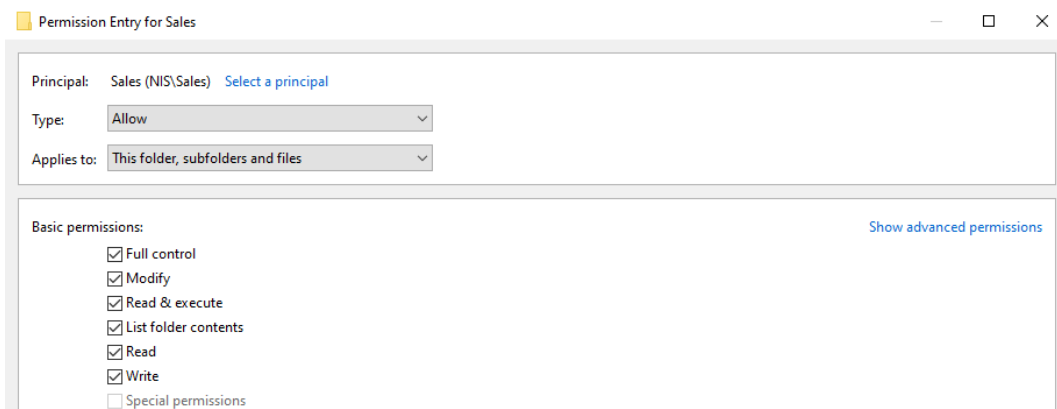
- ☐ Domain local
- ☒ Global
- ☐ Universal

☐ Protect from accidental deletion

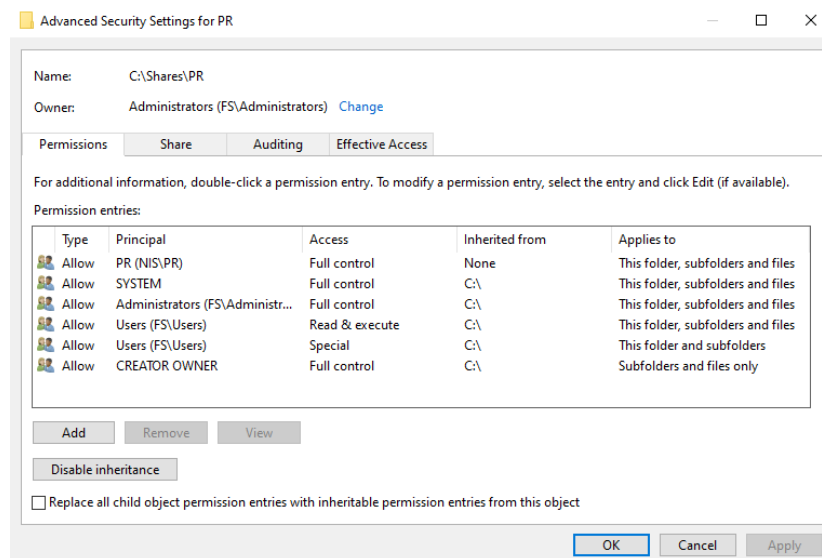
- Now let's add each employee to the corresponding group. Right click a user Hala for example and select add to group. Write the name of the groups and click check names select and verify.



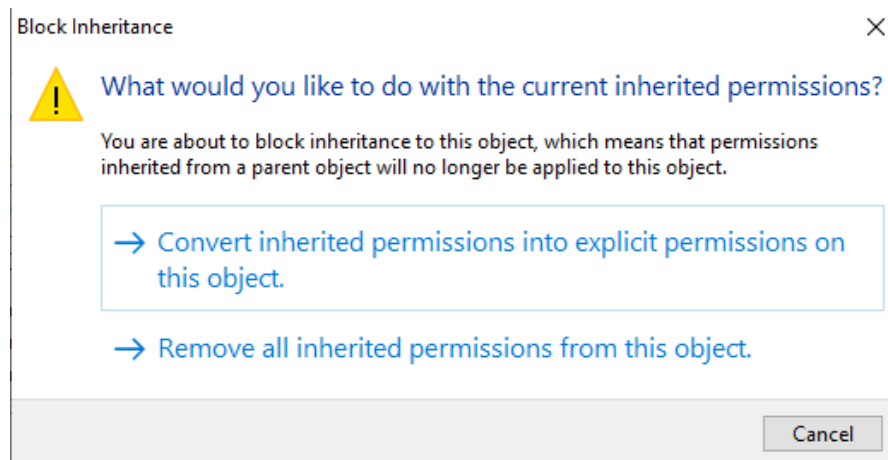
- After adding all users to their respective groups login to the file server using the FSadmin account.
- In File and storage services\shares , right click the Sales shared folder and choose properties.
- Click Permissions then customize permissions.
- Click add then click select a principal and write 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.
- Do the same for PR share and PR user group.



10. Now let's test this on our client machines. Log in to one of the clients using a PR user and to the other machine using a sales user and open the file server share and notice the permissions for both users.
11. To fix the problem we need to change our permissions on the two folders. Open the share properties of both shares and remove permissions that were inherited by others: click Disable Inheritance in the below screen:



12. Choose Remove all inherited permissions from this object in the pop up screen:

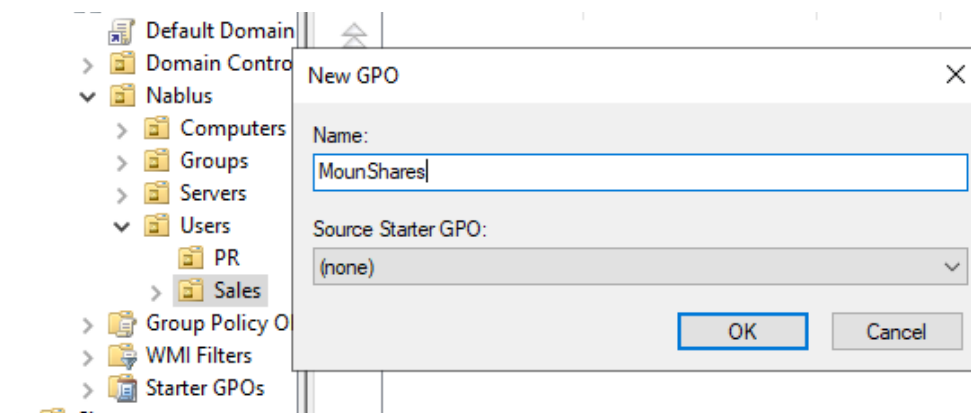


13. Confirm all boxes and then check what are the permissions on the client machines for both departments. And verify that a user that is not part on any of the two department cannot access the two shares.

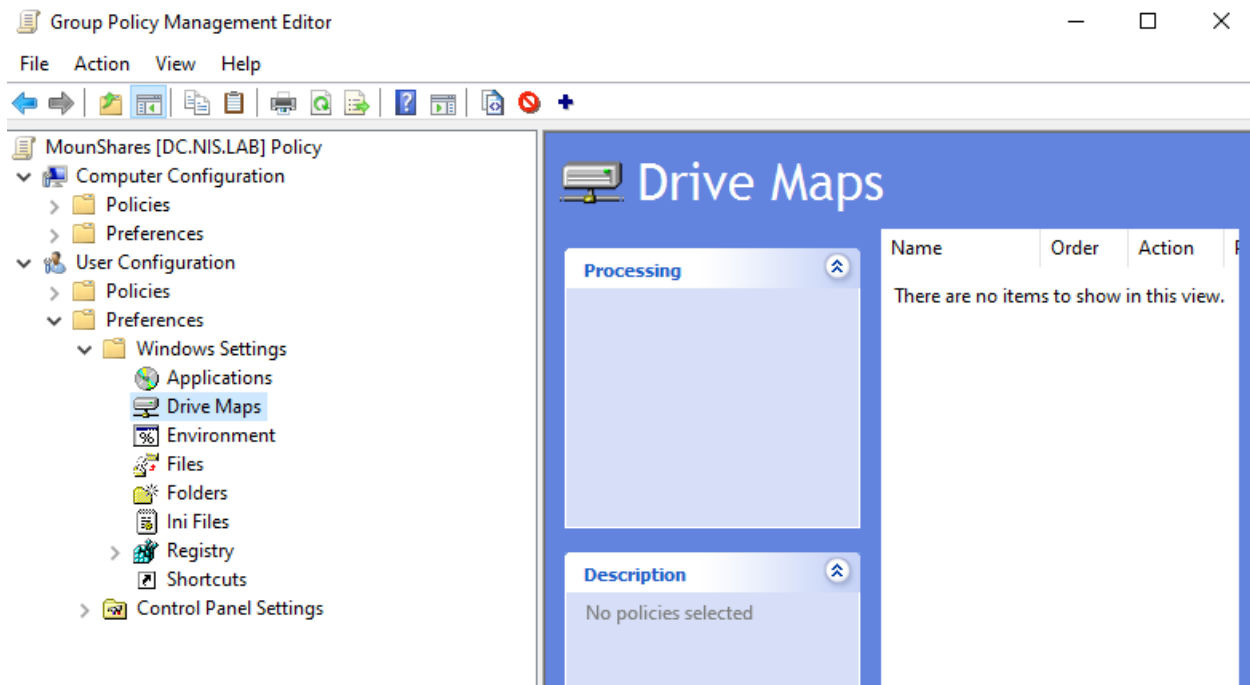
Group Policy

Opening the shares the way we have been using since we started using the file server during the labs is not practical especially with not so technical users. To make accessing the shares easier we need to make the system automatically mount the share as a network drive that the user can access from the windows explorer easily.

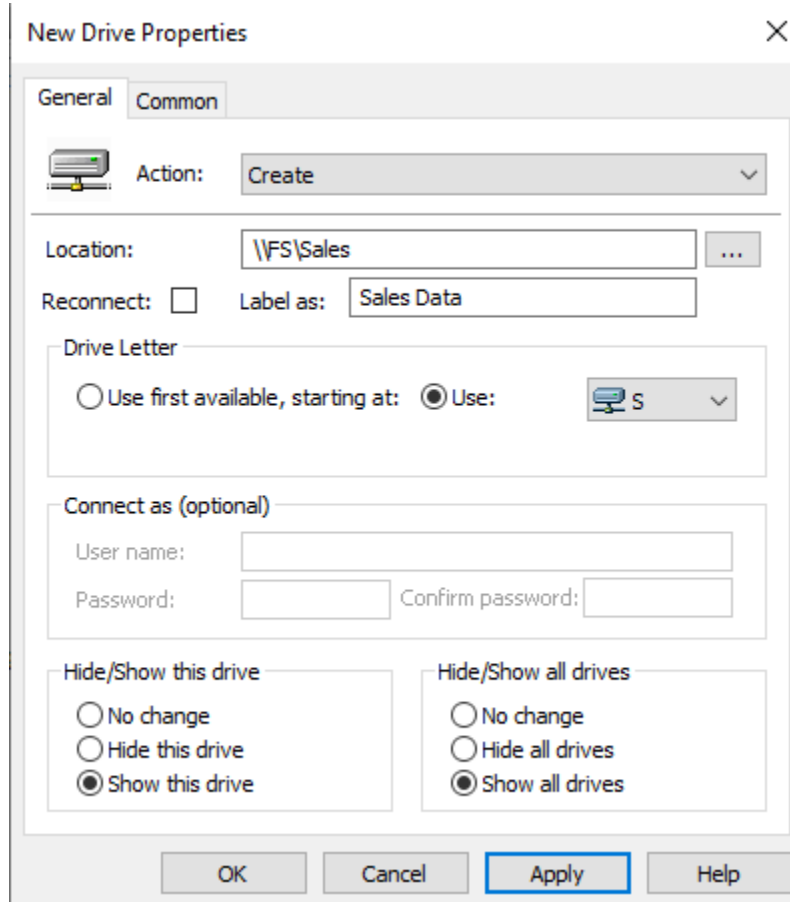
To do this we will use Group Policy. On the Server Manager app of your domain controller open group policy management from the Tools menu. Right click the sales OU and choose “ Create a GPO in this domain and link it here”. Name it MountShares:



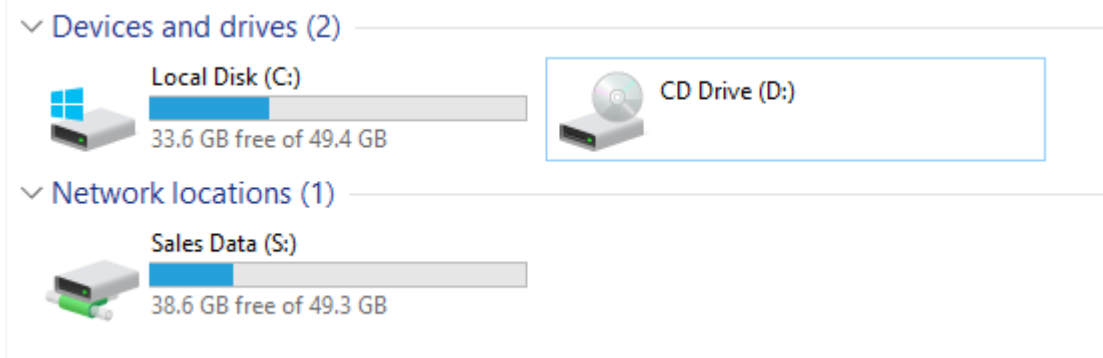
Right click the GPO called MountShares and choose edit. Navigate to User Configuration > Preferences > Windows Settings > Drive Maps.



Right click Drive Maps and Create a new Mapped Drive. Fill the fields as follows (FS is the file server name in my case remember to use yours):



Do the same thing for the PR shared folder and the PR group. Now test the new configuration by logging in as a sales user to one machine and as a PR user to another machine. When logging in as y.saeed who is a sales user he should be able to see the following when he open This PC in the windows explorer:



This is a simple example of Group policy objects that can be used to enforce policies in the organization. Explore other GPOs.

DONE