



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Network Operating Systems and Services (NOSS)

(ACCA5023)

Worksheet 3

MANAGING AND MAINTAINING NETWORK RESOURCES
USING NETWORK POLICY AND SECURITY PRACTICES

Objectives

- In this part of the assessment, you are tasked with creating local drive/file and folder (*NTFS*) permissions and *understanding the use of (Sharing permissions)* for network deployed access control to these resources. To demonstrate this basic local file access control will be demonstrated before then investigating the major difference to deploying these files for shared network access.
- Furthermore the ability to manage network environment settings and security policies via *Group Policy Objects* is investigated. Utilising *the Group Policy Management Console (GPMC snap-in)* is a critical part of network policy management. It determines how security and environment settings can be created and applied to the most critical resources inside the network directory service. A number of both Computer and User Configurations will be setup in our host network.

NB: YOU ARE REQUIRED TO SCREEN CAPTURE THE COMPLETION OF THESE TASKS IN EVERY WORKSHEET AS YOUR EVIDENCE OF UNDERTAKING THE TASKS REQUIRED. PRACTICE USING THE SNIPPET TOOL AND CAPTURE EVIDENCE AND BUILD YOUR WORKSHEETS USING A WORD PROCESSING PACKAGE SUCH AS MICROSOFT WORD.

YOU SHOULD READ EVERY ELEMENT IN THE WORKSHEETS 'VERY CAREFULLY' AS THERE ARE PRE-REQUISITE SNIPPETS OF INFORMATION YOU WILL NEED TO UNDERSTAND, BEFORE UNDERTAKING EACH TASK.

YOU SHOULD PROVIDE SUITABLE NARRATIVE ALONGSIDE THE SCREEN CAPTURES TO IMPROVE THE QUALITY OF YOUR PRACTICAL TASKS.

Task 1: Understanding NTFS and Share Permissions.

NTFS

Recall that NTFS permissions can only be set, on drives partitioned with the NT File System. NTFS permissions can be set on Drives, Folders and Files, all resources part of the operating system.

All NTFS permissions take effect at the local OS level, which means they are bound to the local operating system and its user. NTFS permissions govern who has access to a particular drive/file or folder. The permissions themselves are more granular than those of Share permissions in that they offer more than simply Read, Change (Modify) and Full Control level of permissions.

Firstly to demonstrate how local/NTFS permissions apply, it is necessary to create a simple text file, inside of a folder. The first part of the task will involve creating different sets of permissions for two different users. One user will have administrator like privileges to the file and the other will have only read access.

[On the Client 1 VM]:

- o Login to the Windows 10 Client with an account that belongs to the Administrators group on the nwtraders.msft domain.
- o In the search bar, type in This PC, click on the icon.
- o In the right section of this window under Devices and Drives, double click the Windows (C:) drive
- o Again, in the right hand window, right click away from any files or folders in the whitespace and choose New – Folder
- o Rename the folder **Dept_Important_Docs**
- o Within this folder, right click in the whitespace and choose New – Text Document
- o Again if you right click on the file, you can rename it to something similar to Important_File
- o In order to set NTFS (local) permissions, we will need to set these on the folder and file.
- o So right click on the Dept_Important_Docs folder, and choose Properties.
- o Now click on the Security tab.

- o We are looking to set access permissions, so that one of your network users has Full Control permissions and the other network users have only read access. This will stop them from accidentally or otherwise destroying the contents of the file.
- o Click on the Edit button to change these permissions.
- o You will see under the Groups or User names section that there are roughly 4 access entries listed, Authenticated Users, SYSTEM etc.
- o We will need to tighten down our permissions so we need to delete these Inherited permissions from the file system.
- o Click on Authenticated Users and Choose the Remove button, note that you are presented with a Windows Security error dialog saying that the permissions on this folder are being inherited. Therefore, we need to turn off inherited permissions on this folder.
- o Click Cancel in this window, Click on the Advanced button.
- o Click on the Disable Inheritance button then click Remove all inherited permissions from this object.
- o Click on the Apply button, then choose Yes and Click on the Ok button to close this window.
- o We can now add the permissions we require on the folder, so choose Edit again.
- o Click on Add button, in the “Enter object names to select field, type in the username of the account you are logged in with. Click Check Names, the account should underline to signify its verification. Choose Ok
- o In the bottom part of the window, the specific types of permissions are listed and they are categorised into an Allow or Deny column.
- o Check the Full Control option on under the Allow category.
- o Click Apply, this will give the current user, recall the administrative level user the full access required.
- o Now right click the File within this folder and choose Properties. Note the access control settings are inheriting from the folder to which the file belongs. This is fine for our example.
- o Go back to the folder level and right click and choose Properties again,
- o Click on the Security tab, this time we’re going to add in another user from our network with a more restricted set of permissions.

- o Click Edit, then Add, find the user and click Check Names. Choose Ok.
- o Grant this user everything underneath and including Read and Execute, note that there is no Modification allowed on the folder or its contents.
- o One these settings are applied close down the folder view and open up the file inside.
- o **Type some text into the file and save the file, does the action permit you to do so successfully?**
- o **Logoff, login as the other (non-admin) user, try opening the folder and modifying the file, are you permitted to do so?**

Share Permissions

Share permissions enable controls over resource access within a networked environment. When a file or folder is created on a system in the network, it is not shared by default. Files/Folders and Drives that are specifically shared on a system can be viewed by searching for a PC on your network and expanding the available shares this system has provided, unless the share is specifically hidden by the administrator.

Network shares need to be carefully managed alongside NTFS permissions as making a resource available over the network can compromise local resources if access control is not properly secured locally.

NTFS permissions work by granting access to files, folders and drives to individual user accounts or groups, regardless of where they are connecting from.

In the event of any conflicting rules set between the share permissions and the NTFS permissions, the most restrictive rules always take preference; e.g. A network user may have full control NTFS access to a particular file but it may reside in a network share where that user does not have appropriate share permissions. If the file is in a network share therefore the user will not be able to access it.

Share permissions are less granular and more straightforward than NTFS/local permissions.

Shares are usually stored on Servers, the appropriate role for this is a File Server.

[On the Server 1 VM]:

- o Click search and enter Server manager, load Server Manager. Now click File and Storage Services then click Shares>Tasks>New share to create a folder share on the server.
- o The first dialog you're prompted with is the Share Profile page, here different types of profiles based on the share are offered. The SMB Share – Quick option is suitable for what we need, but read through the other listed profile options *SMB Share – Advanced*, *SMB Share – Applications*, *NFS Share – Quick*, *NFS Share – Advanced*. These other options offer more advanced options such as creating shares that can be accessed via other operating systems than Windows, e.g. Linux.
- o When the profile is selected, at the Select a server for this path and share, choose the Select by volume option – click Next.
- o Now a share name needs to be specified, enter the name *DeptNetShare\$* and take note of the options *Local path to share* – it will say *C:\shares\DeptNetShare* and the *Remote Path to share* which should say something like *\\YourServerName\DeptNetShare\$*
- o The latter option is very important since we will need this in order to access the files over the network from a different machine or to Map a network drive to the file server, we will do this later.
- o Choose Next – At the *Configure Share Settings* dialog window, choose/check on the **Enable access-based enumeration** and **Allow caching of share options**.
- o Access based enumerations means that the share will only display the files and folders that a particular user has rights to access. This is important as you may have a departmental share where different people are allowed to access different folders and the files that reside within them. Caching of share will enable users to still see the files they have access to if they go offline. It works by caching the files on that user's local machine that they are using to access the share.
- o At the Specify permissions to control access screen – we will add Administrators with full control and **two members** of our nwtraders.msft domain with read and execute access. Click Next when these have been added.

- o At the Confirm Selections page, take note of the options we have configured and verify they are okay. Choose **Create** to create our network file share on the server.

Accessing the file share/server over the network.

There are a few ways you could access the share, one is through File Explorer by entering the path to the network share. Another method is by browsing the computers on the network and seeing if there are any shares associated with that Server/Computer. The second option isn't suitable for us since we have enabled a hidden share. By using the \$ (dollar sign) in our share name, we have denoted that the share is hidden for security purposes. This acts as a preventative measure for any would be snoopers who might be browsing our network. We will instead access the file share by another method known as creating a **Mapped Drive**. A network mapped drive offers a persistent connection to the share, which means it appears as another local drive on the network computer that is trying to access the network share. It also means we don't have to browse to the share or search for it every time we want to access the files stored there.

[On the Client 1 VM]:

- o Search for This PC – right click and choose **Map Network Drive**
- o Accept the default drive letter, note that this feature adds a local drive to our machine that it reserves for the network share we are mapping to. This means that the network share is permanently stored on our machine, until we disconnect from it.
- o The network folder we are connecting to needs the server name and the full file share name, e.g.

[\\YourServerName\DeptNetShare\\$](#)

Choose Finish to complete the Mapped drive and verify you can see the share

Task 2: Utilising Group Policy Management Console to better facilitate network object management.

Group Policy

Recall that Group Policy is a built in tool (snap-in) part of the Microsoft Windows Server operating system that provides Systems administrators with the ability to centrally manage the two main types of objects within an Active Directory, *domain joined Computers* and *User accounts*.

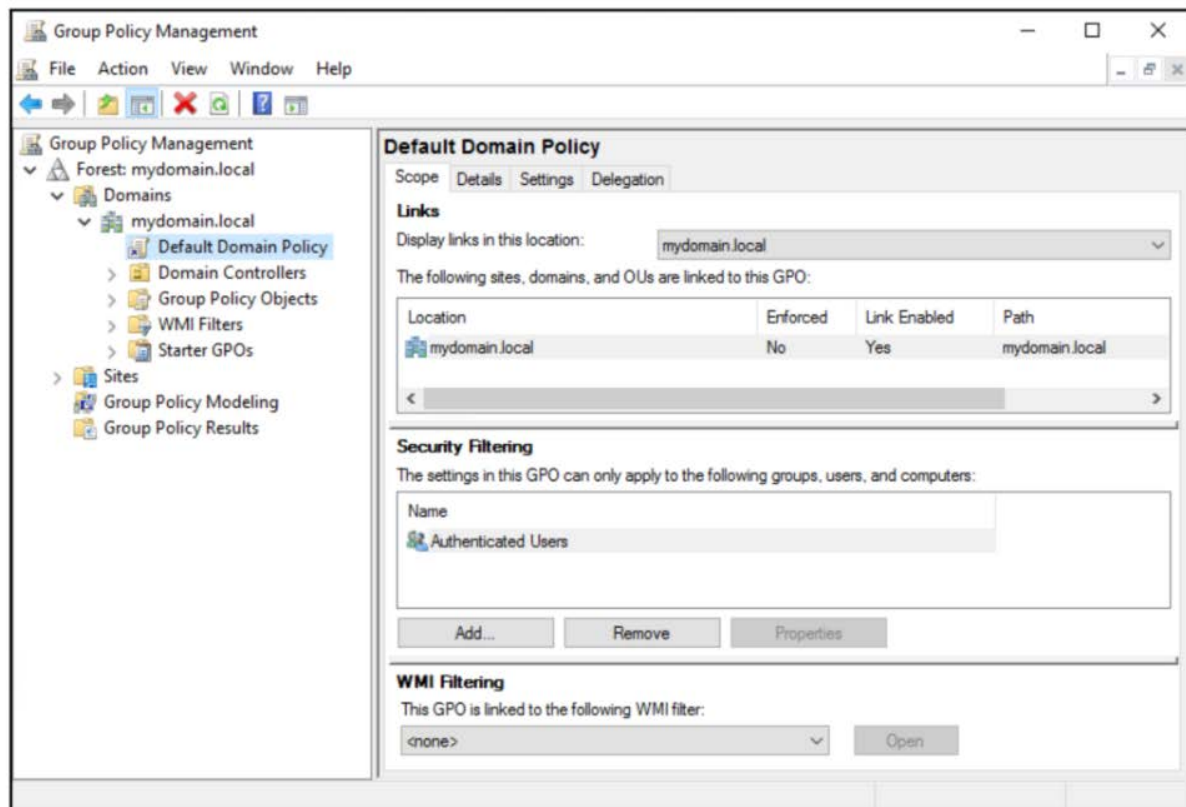
The principal purpose of Group Policy management, is to automate the process of rolling out, often times organisational or departmental wide settings to the machines and users that belong to the domain. This obviously saves time in terms of manual configurations, but it also provides a means to centrally manage security settings to ensure that all required systems are affected as required, without omission.

Local group policy is a different technology to Group policy in that is available to configure only locally on every Microsoft Windows System. The main reason local group policy isn't used over Group Policy is that it would require an administrator to configure the settings on an individual basis on every machine in the network. Some critical systems require local group policy, e.g. domain controllers as a very small number of users should be responsible for administering them, for security purposes. With Group Policy, any system admin can be assigned to manage a department/organisational wide setting.

Group Policy Management Console – GPMC.

Group Policy Objects are created within the Group Policy Management Console, often referred to as *GPMC*. *Fig A: Shows the GPMC view:*

Fig A: GPMC Editor.



Note, that is critical to understand the Hierarchy of Processing in Group Policy Management. This is because it is possible to filter out policies specific to the level of where you need them to apply. The domain structure is shown on the left of the window and the GPOs (Group Policy Objects themselves that are active at that organisational level are shown on the right hand side of the window.

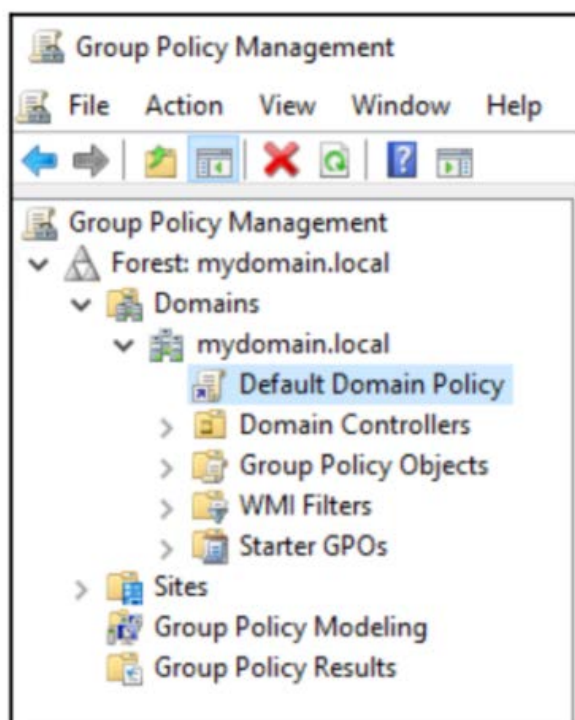
Local Policies – as discussed available to administer on all systems, but infrequently used because of manual configuration required.

Site Policies – An Active Directory can expand more than one site (or one physical location e.g. Offices and their resources at Swansea, Cardiff, Newport and Bristol may all belong to one Active Directory (*for more details research Active Directory Sites and Services*). Site level policies are configured via the Sites container in the console tree

view on the left hand side of the window and provide the ability to administer different policies to different physical sites .

Domain Level Policies – Typically settings that an administrator wants to deploy organisation wide. Group policy objects are created at the top of the organisational tree, by right clicking the domain name in the left hand side of the console window and creating a group policy object at this level. See fig B below where the *gpo: default domain policy* has been created at domain level. All organisational units and containers with their objects will 'inherit' these settings by default, unless Inheritance Blocking is setup on the Organisational Unit/Container.

Fig B: Domain Level Policy: Default Domain Policy.



Organisational Unit Level Policies.

Recall that an Organisational Unit (OU) is an object which acts like a storage folder/container for organising and holding other objects, typically computers or users of a particular category e.g. Computing Student Users or Engineering Dept PCs.

Applying GPOs at OU level is the most common way of applying Group Policy in organisations, as it allows for more control and better management of resources.

Configuring User Environment and Computer Environment, 'Network Group Policy Objects':

[On the Server 1 VM]:

GPO 1: Moderating Access to the Control Panel.

- o Restricting access to the Control panel is a good way of safeguarding users from making administrative changes to the settings of systems in your network. We will first need to create an OU for Non admin users, do this by going into Active Directory Users and Computers,
- o Right click the nwtraders.msft domain in the left hand side of the console and choose New – Organisational Unit. Call the OU **Non Admin Users**
- o **Now right click this OU and create a new user inside, refer to the previous worksheet where instructed how to create users.**
- o We already have users in our domain who are administrators, namely the administrator account!
- o After we complete the GPO we will need to test the policy is working by logging onto a workstation in the domain and verifying that the policy works.
- o To create the GPO – Search for Group Policy Management Console and load the program.
- o In GPMC, expand the domain and find the Non Admin Users OU you have just created. Right click this and choose New – Group Policy Object. Name the object **NoCtrlPanAccess**. Now right click the GPO itself (it resembles a small scroll as shown in Fig B above and choose Edit.
- o You are now brought into the Group Policy Object Editor - expand 'User Configuration' - Administrative Templates - Control Panel.
- o Now double-click "Prohibit access to Control Panel and PC settings" policy in to open its properties.
- o Choose the Enabled option, Click Apply, then click Ok.

There is a command that system administrators can run in order to force the Active Directory to look at any new settings or policies that have been applied. This is useful when you want to force AD so that you can test the settings, as in our example here.

- o Search for Command Prompt, right click and choose Run as Administrator.
- o Now in the command prompt window, type: `gpupdate /force`
- o Note that there is a space after the word `gpupdate`

The window will notify you of settings being updated. We now need to test that the Non admin user cannot access the Control Panel.

[On the Client 1 VM]:

- o Login to the Client 1 VM as the user you created above.
- o Test that you cannot access the Control Panel, you should provide screenshots to validate this task.

GPO 2: Removing Access to the Command Prompt.

A command prompt can be used to run commands that override system settings and give high level access to users looking to circumvent security policies. In the wrong hands (e.g. Programmers, Network Hackers) it could prove a problem.

[On the Server 1 VM]:

We already have our Non Admin OU and user that we want the settings to apply to, so as before:

- o To create the GPO – Search for Group Policy Management Console and load the program.
- o In GPMC, expand the domain and find the Non Admin Users OU you have just created. Right click this and choose New – Group Policy Object. Name the object **NoCmdPrmptAccess**
- o Now right click the GPO itself (it resembles a small scroll as shown in Fig B above and choose Edit.
- o You are now brought into the Group Policy Object Editor - expand 'User Configuration' - Windows Settings – Policies - Administrative Templates – System.
- o In the right side window, double click 'Prevent Access to the Command Prompt' - choose the Enabled option. Click Apply then Ok.
- o Search for Command Prompt, right click and choose Run as Administrator.
- o Now in the command prompt window, type: `gpupdate /force`

[On the Client 1 VM]:

- o Login to the Client 1 VM as the user you created above.
- o Test that you cannot access the Command Prompt, the system should display a message that says some settings have been disabled or something similar.
- o Screenshot to validate the policy in effect.

GPO 3: Restricting Access to Removable Media Drives.

Removable Media Drives are one of the most common transport mediums of viruses and malware in a network/domain. Therefore it is recommended to **deny all accesses to these** for all groups of users other than the domain admins.

[On the Server 1 VM]:

We already have our Non Admin OU and user that we want the settings to apply to, so as before:

- o To create the GPO – Search for Group Policy Management Console and load the program.
- o In GPMC, expand the domain and find the Non Admin Users OU you have just created. Right click this and choose New – Group Policy Object. Name the object **NoRemDriveAccess**
- o Now right click the GPO itself and choose Edit.
- o In the Group Policy Object Editor - expand User Configuration
- o Expand Policies - Administrative Templates – System - Removable Storage Access.
- o In the right pane, double-click “All removable storage classes: Deny all accesses” policy
- o Click Enabled, Click Apply then click OK.

[On the Client 1 VM]:

- o Login to the Client 1 VM as the non admin user.
- o Verify that access to Removable Storage has been disabled, as before provide screenshots.

[On the Server 1 VM]:

GPO 4: Restricting Software Installs

One major source of threat inside a network is 'unauthorised software installations' onto systems that are more accessible than perhaps the Servers stored in Datacenters. Apps and plug ins can be installed on client PCs, which could then be used to exploit vulnerabilities and attack vectors in the network. Therefore it is wise to restrict software installations only to authorised system admins.

Here the GPO will need to apply to a Computer object as opposed to a User configuration. Therefore we will need to apply the object to an OU that contains our WS1 computer object.

- o In Active Directory Users and Computers – Right click the nwtraders.msft domain and choose New Organisational Unit, name the OU **NWClient Computers**.
- o We need to locate the Computer Object and move it to this OU. This is done by right clicking the Computer Object for the client – click Move to and then select the NWTClient Computers OU.
- o Now that the computer object is within the proper OU, we can configure the software installation restriction GPO.
- o In Group Policy Management – right click on the NWTClient Computers OU and choose New – Group Policy Object – Name the object **NounauthSoftInstalls**
- o Right click the GPO and choose Edit
- o In Group Policy Editor – expand Computer Configuration”
- o Then expand Administrative Templates - Windows Component - Windows Installer.
- o In the right hand side of the console window double click the “Prohibit User Install” policy.
- o Click Enable
- o Now click Apply and Ok.
- o Search for Command Prompt, right click and choose Run as Administrator.
- o Now in the command prompt window, type: gpupdate /force

[On the Client 1 VM]:

- o Login to the Client 1 VM as a non-administrative user.
- o Try to install a program, screen capture the results.

GPO 5: Enforcing Password Policy in the 'nwtraders.msft' domain.

We have seen both User and Computer configuration policies applied at OU Level to objects within our domain. There are certain settings however that require Domain level enforceable policies.

Password Policy is a critical requirement for enhancing security across the network. Stronger attributes associated with values reduce the likelihood of passwords being cracked, and provide the ability to follow sound password security principles for example such as 'passphrases'. By setting a longer predetermined value length as a minimum requirement, 'passphrases' (*e.g. using the first letter of a word in a structured sentence that is easy to remember as a user's password*) can be used in conjunction with minimum complexity requirements to enforce stronger password policy.

[On the Server 1 VM]:

- o In Group Policy manager, expand the nwtraders.msft domain, right click the on the Default Domain Policy GPO – choose Edit.
- o Expand Computer Configuration – Policies – Windows Settings – Security Settings
- o Click on Account Policies
- o Click on Password Policy

Ensure that the predefined settings are changed to the following values:

Enforce password history:	8 passwords
Maximum Password Age:	31 days
Minimum Password Age:	1 day
Minimum Password Length:	10 Characters
Passwords must meet complexity Requirements:	Enabled

Store Passwords using reversible encryption:	Disabled
---	-----------------

- o Close down Group Policy Manager
- o Search for Command Prompt, right click and choose Run as Administrator.
- o Now in the command prompt window, type: `gpupdate /force`

- o Now create a new user account, try and enter a password for the account that is less than the predefined 10 characters just set in the policy. You should now instead use a passphrase for this account.
- o The settings we have used, mean that passwords must be changed after no more than a month (31 days) and passwords/passphrases must still use special characters as part of their structure.

Task 3: Observational Tasks

NB: You should use a proper referencing style here when submitting your answers.

- 3 a) Explain the main differences between local permissions and file shares.
- 3 b) Describe the role of Group Policy Management in the network environment, you can use example policies in your answer.
- 3 c) Give some examples of sound 'password' principles in modern network environments.