WEEKLY JOURNAL 3

Network Administration

MAY 12, 2024

WEEKLY JOURNAL 3

(from week 7 to week 9)

Table of Contents

❖ Week 7

❖ Week 8

❖ Week 9

Week 7

➢ Key concepts

User account Template copies: Group Memberships, Home Directories, Profile Settings, Logon Scripts, Logon Hours, Password Settings, Department Name, Manager. The template should be named in a way that makes it stand out from the user account.

Bulk user account creation:

- **CSVDE**: import/export new user account details from a comma-separated value such as spreadsheet text.
- **LDIFDE**: import/export new user account details from an LDAP database. AD DS uses LDAP format to export user accounts and import them into a new domain using LDIFDE.

OU (Organizational Unit) allows a logical structure that speeds up locating objects, allows users to be delegated management privileges and allows configurations to be targeted using Group Policy. OU can be created by right-clicking in DSA or ADAC or typing the Powershell command: **New-AdOrganizationalUnit -name ICT -path "dc=swin,dc=local"**.

The **hierarchy of OUs** is determined by the Administrator and based on: location (e.g. USA, Aus), business unit (e.g. Sales, Marketing) and resource (e.g. server, PC)

The default AD containers Users and Computers are not OUs so GPOs can not link to them. To change the default locations using **redircmp** and **redirusr**.

E.g. **redircmp "ou=Melb,dc=swin,dc=local**" : redirect all new computers account to the Melb OU.

To run **Delegate Control Wizard**, right-click the OU.

Permissions assigned for an object are Explicit (black ticks) and permissions assigned for a parent object are inherited (grey ticks). Explicit permissions override Inherited permissions.

For **security Permissions** attached to an object:

- Explicit Deny overrides Explicit Allow
- Explicit Allow overrides Inherited Deny
- Inherited Deny overrides Inherited Allow

To confirm the effective access of a user or group, use the Effective Access tab in Advanced Security.

Role Based Access Control groups include Identity Groups (Account) and Access Groups (ACL). To be more specific:

- **Identity group** is used for grouping accounts that have similar requirements, Global groups fill this role (e.g. G_Sales: reflects the account).

- **Access group** is used to control access to resources, Domain Local groups fill this role (e.g. DL_SalesData_RW : reflects the resources and the permissions being given).

Nesting global groups (Second-level account groups) are made when needing to group multiple account groups. For example, a department made up of teams or a team is spread across numerous domains, yet has the same requirements.

- If the second-level account group collects groups within a single domain, it should be a Global group → **I G G DL A**
- If the second-level account collects groups from different domains, it should be a universal group → **I G U DL A**

Universal group membership lists are maintained in the Global Catalog, whereas other groups memberships are not.

It is important to remember to **share the resource**; otherwise, no one can access it over the network.

Access base enumeration is a property of the share that prevents users from seeing resources they do not have permission to.

There are some **groups** whose memberships are automatically generated:

- Everyone: All user accounts and guest accounts
- Authenticated users: All user accounts
- Anonymous Logon: All users including those without accounts
- Interactive: Users logged on locally
- Network: users accessing resources from a remote computer
- Creator Owner; the user account that created the file or the user/group allocated ownership. Creator/ Owner automatically has FC permissions for files they create.

The most restrictive applies when combining NTFS and Share permissions.

➢ Innovative ways to address business needs

There are some best practices for delegating control to OUs in business[1]:

Use good OU structure: *The well-structured OU design makes assigning specific administrative tasks to delegated administrators easier. It provides a clear hierarchy for the management and maintenance of permissions.*

Utilize nested OUs: *Nested OUs provide flexibility and scalability in delegation. Administrators can delegate control at different levels and manage resources more efficiently.*

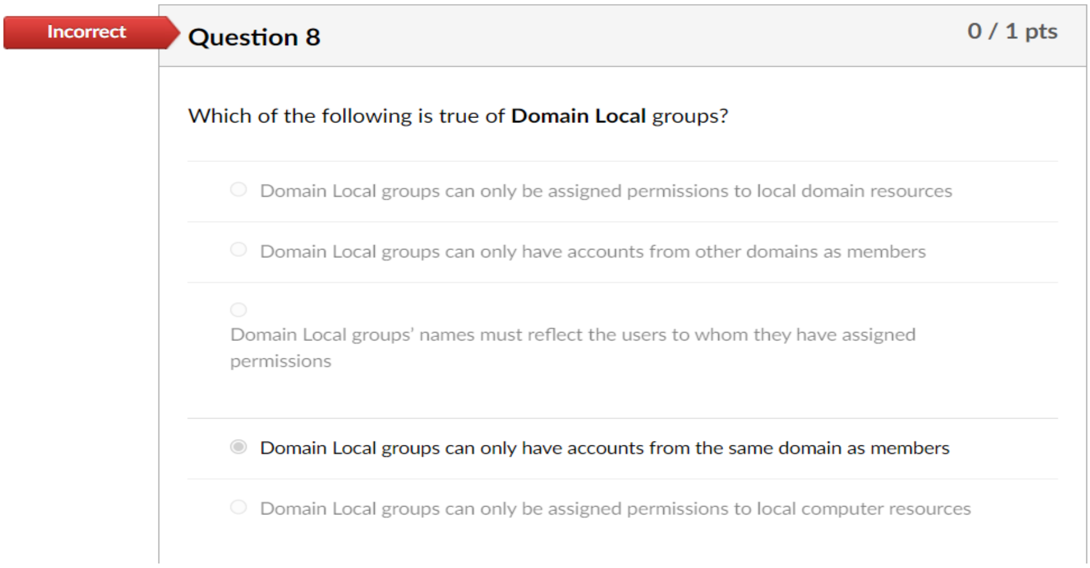
***Delegate control to groups, instead of users**: Delegate permissions to groups make managing membership and access rights easier, especially when there are changes in personnel or job roles.*

***Perform audits of privileged access**: Auditing privileged access can detect and mitigate unauthorized or excessive permissions granted to accounts that help identify security vulnerabilities.*

***Use Role-Based Access Control**: RBAC manages sensitive resources by assigning specific access rights to specific job roles and responsibilities.*

➢ Reflection and plan for further study

In this week, I still have problem with remembering all the memberships, resources and limitation of all group scopes. In the revision quiz, I made a mistake in the question about the membership of the Domain Local group.



Which of the following is true of **Domain Local** groups?

○ Domain Local groups can only be assigned permissions to local domain resources

○ Domain Local groups can only have accounts from other domains as members

○ Domain Local groups' names must reflect the users to whom they have assigned permissions

● Domain Local groups can only have accounts from the same domain as members

○ Domain Local groups can only be assigned permissions to local computer resources

Fig. 1 Revision quiz 7 question

To address this issue, I tried to review the table of Group scopes and their features in the active directory and practised answering more questions about the group scopes.

➢ Key configurations and commands

To **create user accounts**:

- Step 1: Right-click on the Users container and select **New → User**
- Step 2: Type the information such as first name, last name, user logon name and password

- Step 3: Clear the check box **User must change password at next logon** so that the administrator does not have to change password when that user logs on.

To **create computer accounts**: In **Active Directory Users and Computers**, right-click on the **Computer** container and select **New → Computer**. Then type the computer name.

To **configure user account properties**: In **Active Directory Users and Computers**, right-click on the user account created previously in the **Users** container and then select **Properties**. There are the following tabs that the settings can be configured:

- General: Type the **Display name**, **Description**, **Office** and **E-mail**.
- Address: Type the **Street**, **City**, **State**, **Post Code**, and **Country**
- Account: Change **Logon Hours** and **Logon To**.
- Profile: Change the **Home folder**
- Etc.

To **configure Computer Account Properties**: In **Active Directory Users and Computers**, right-click on the computer account created previously in the **Computers** container and then select **Properties**. Next, enter the description of the computer in the **Description** field on the **General** tab.

To **create an OU**, follow these steps:

- Step 1: In **Active Directory Users and Computers**, right-click on the domain root name
- Step 2: Choose **New → Organisational Unit**
- Step 3: Enter the name of the new OU
- Step 4: If the OU is temporary, remove the tick from **Protect container from accidental deletion**.

To **create group accounts**, right-click on the OU created before and select **New → Group**. Next, choose the group scope. Then name the group following the naming convention.

To **assign the NTFS permissions**: right-click on the folder and select **Properties**. Next, click on the **Security** tab. Finally, choose the permissions by ticking the checkboxes and clicking **OK**.

To **remove Inherited Permissions**, in the **Security** tab, click on the **Advanced** button. Next, click the **Disable inheritance** button, and select **Convert inherited permissions into explicit permissions on this object**.

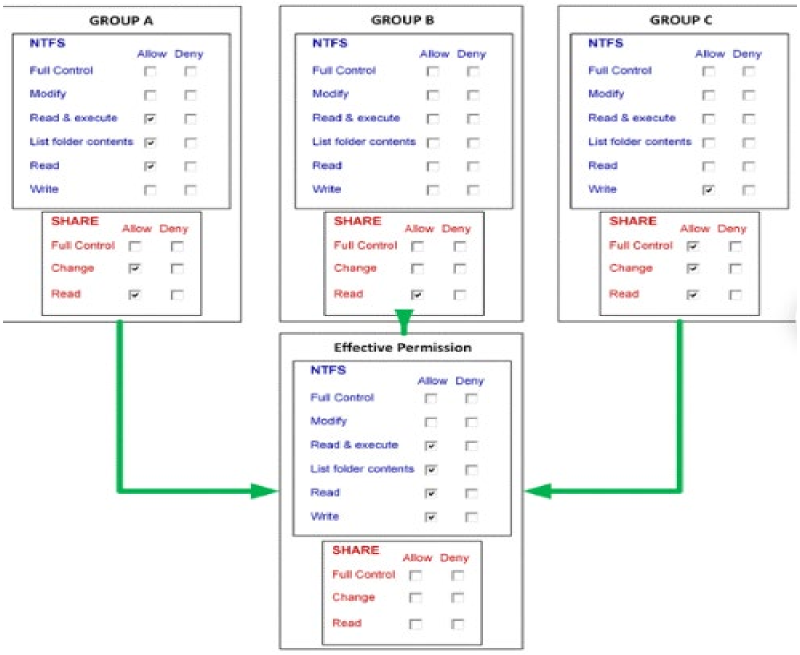
To **assign Share Permissions**, click on the **Security** tab and then the **Advanced Sharing** button. Now choose the sharing permissions.

Week 8

➢ Key Concepts

Permission combination:

- **Accessing the resource locally**: combine **NTFS allow** permissions from all ACL groups the account is a “member” of, deny overrides other permissions. Share permissions are not allowed with local access.



GROUP A

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

GROUP B

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

GROUP C

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	☑	□

SHARE	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

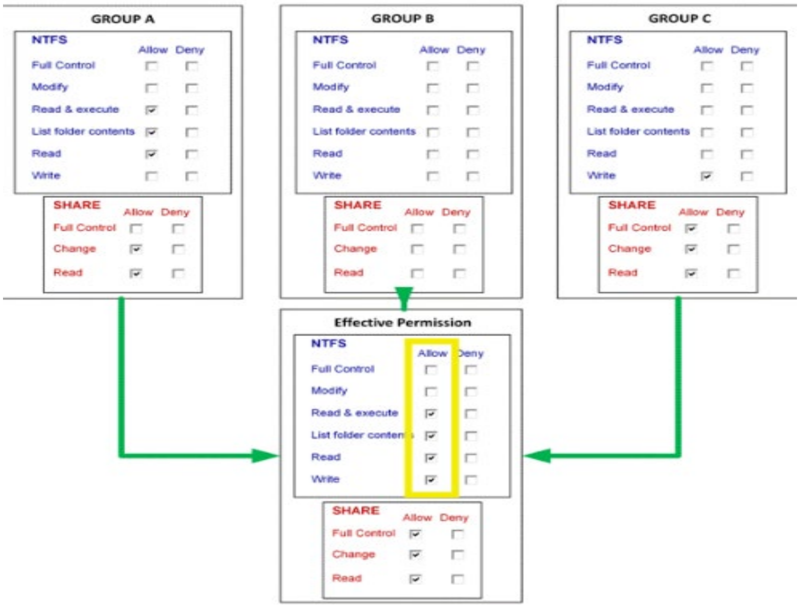
Effective Permission

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

SHARE	Allow	Deny
Full Control	□	□
Change	□	□
Read	□	□

Fig. 2 Share permissions and NTFS permission accumulation

- **Accessing the resource as the network user** (e.g. accessing the workstation): combine **NTFS allow** permissions and **Share permissions** from all ACL groups the account is a “member” of.



GROUP A

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

GROUP B

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	□	□
Read	□	□

GROUP C

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	☑	□

SHARE	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Effective Permission

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

SHARE	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Fig. 3 Share permissions and NTFS permission accumulation

Group policies:

Computer configuration	User configuration
Settings applied according to **computer account**	Settings applied according to **user account**
Deploy software for all users that use a specific computer	Deploy software to where the user logs on
Startup/Shutdown scripts	Logon/Logoff scripts
Deploy Printers	Deploy Printers
Control updates	

Group Policy can not be changed by the user and the application can be based on User Account or Computer Account. There are some components of Group policy:

Group Policy Container:

- Stored in AD
- Automatically replicated to other DCs in Domain
- Points to Group Policy Template (GPT) for settings

Group Policy Template:

- Contain the GPO settings
- Will not replicate if stored in wrong location
- Store in Sysvol (default location) (will replicate if in default location)

GPO settings include simple radio buttons, dropdown lists, spin boxes, and text boxes. Some GPO settings must be configured with other settings. These settings are recorded in the registry. Some settings apply only to Domain Controllers and remember to beware the Double Negative.

Preferences can be changed by the user, e.g. Setting is not grey out.

GPOs will apply when:

- Start up (Computer Configuration settings)
- Sign in (User Configuration settings)
- Typing these PowerShell commands:
  - GPUpdate /target: <computer/user>
  - GPUpdate /logoff
  - GPUpdate /boot
  - GPUpdate /force
- DC linked: update every 5 minutes and only applies settings that have changed
- Non-DC linked: update every 90 minutes (+0-30 minutes offset) and only applies settings that have changed

Default GPOs include:

- Default Domain Policy: is pre-linked to Domain, includes Default Security settings and Default Power settings
- Default Domain Controller Policy: is pre-linked to Domain Controllers OU: Default user rights
- Resetting default GPOs – DCGPOFix: DCGPOFix /target:Domain and DCGPOFix /target: DC

It is **important to remember**:

- GPO must be linked to: Site, Domain and OU.
- GPO can not be linked to: Groups, Users, Computers, Users or Computers containers in AD
- A container can have multiple GPOs linked and a GPO can be linked to many containers

Permission to link GPOs to an OU can be delegated using Delegation of Control Wizard.

Unlinking a GPO is a useful tip for quick troubleshooting as it prevents GPO from applying.

The **order of GPO application**: Local → Site → Domain → Parent OU → Child OU. The last applied wins.

The **GPO precedence**: Child OU → Parent OU → Domain → Site → Local

If GPOs are configuring different settings, the settings cumulate.

Blocking inheritance prevents GPOs linked to any parent container from applying to objects in the OU. It is impossible to block inheritance selectively.

Enforcing a GPO overrides Blocking Inheritance and conflicting settings. It allows the head office to override rogue branch administrators.

Security filtering allows GPO to apply to user and computer accounts in specific groups.

GPO permissions can be accessed via GPMC, Delegation tab and Advance button. The apply group policy permission must have read permission to work.

WMI Filtering has scripts that can assess the environment and apply settings accordingly. E.g. Only install software if RAM > 8 GB RAM.

There are two types of **Administrative Templates**:

- ADML: support other languages
- ADMX: XML files with code for the GPO settings that can be created for the developed software

There are some tools to **troubleshoot GPOs**:

- Group Policy Modelling: a GPMC wizard
- Group Policy Results: communicates with computer and incorporates the Local Computer Policy in the analysis.

- gpresult: a command line tool

Printer deployment with GPOs can be done via Print Management console.

GP preference level targeting (Item level targeting) allows preferences to be conditional. E.g. Only install a large format network printer if there is sufficient disk space and RAM.

➢ Innovative ways to address business needs

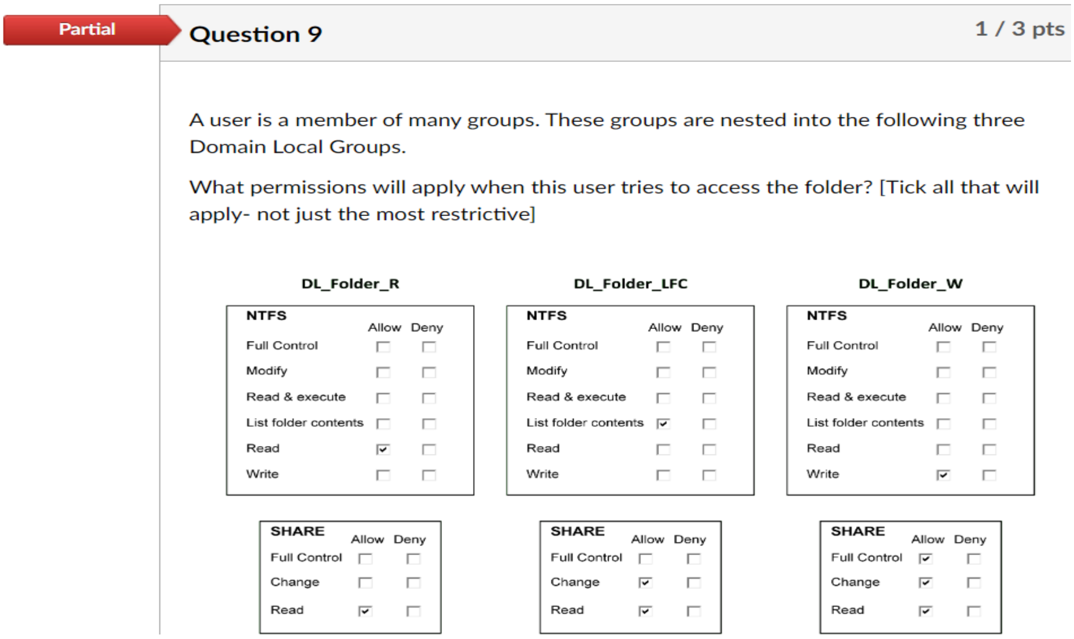
One of the best practices to prevent security breaches using group policy is **preventing Windows from Storing LAN Manager Hash**. *Windows creates and stores passwords for user accounts using "hashes", especially generating a LAN Manager hash (LM hash) and a Window NT hash (NT hash). These hashes are stored in either the local Security Accounts Manager (SAM) database or Active Directory (AD)* [2].

The LM hash is considered vulnerable to hacking so it is recommended to prevent Windows from storing LM hashes of passwords. Below are the steps to achieve this:

- Step 1: In Group Policy Management Editor, click **Computer Configuration → Window Settings → Local Policies → Security Options**.
- Step 2: In the right panel, double-click **Network security: Do not store LAN Manager hash value on the next password change** policy.
- Step 3: Select **Define this policy setting** checkbox and click **Enabled**.
- Step 4: Click **Apply** and **OK**.

➢ Reflection and plan for further study

This week, I have had difficulty accumulating the NTFS and share permissions. Therefore, I answered the questions about this accumulation incorrectly.



Partial

Question 9

1 / 3 pts

A user is a member of many groups. These groups are nested into the following three Domain Local Groups.

What permissions will apply when this user tries to access the folder? [Tick all that will apply- not just the most restrictive]

DL_Folder_R

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	☑	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

DL_Folder_LFC

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	☑	□
Read	□	□
Write	□	□

SHARE	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

DL_Folder_W

NTFS	Allow	Deny
Full Control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	☑	□

SHARE	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Fig. 4 Revision quiz 8 question

To address this problem, I re-read the theories of permission accumulations and practice with this question more frequently. Another problem that I should be more careful of is that explicitly deny will override explicitly allow.

➢ Key configurations and commands

Powershell commands:

Command	Use
New-AdUser	Creates user accounts
Set-AdUser	Modifies the properties of user accounts
Remove-AdUser	Delete user accounts
Set-AdAccountPassword	Resets the password of a user account
Set-AdAccountExpiration	Modifies the expiration date of a user account
Unlock-AdAccount	Unlocks a user account
Enable-AdAccount	Enables a user account
Disavle-AdAccount	Disables a user account

e.g. **New-AdUser -name Jill** : create a disabled account in the Users container

New-AdUser -name “Jack” -Path”ou=ICT,dc=SWin,dc=local” -accountPassword (ConvertTo-SecureString -AsPlainText “Pa55w.rd” -Force) -enable $True : Create an active user account in the ICT Organizational Unit.

To create an OU in PowerShell:

New-ADOrganizationalUnit -name Finance -path “dc=Wtnr,dc=sWin,dc=local”

To create groups using PowerShell:

New-ADGroup -name G_FinanceWtn -GroupCategory Security -GroupScope Global -path “ou=Finance,dc=Wtnr,dc=sWin,dc=local”

To set the membership and nesting:

Add-ADGroupMember G_AccPay Kim

Add-ADGroupMember G_FinanceWtn G_AccPay

To change the default location for the Computer Accounts, use **redircmp**:

Redircmp “ou=Finance,dc=Wtnr,dc=sWin,dc=local”

Week 9

➢ Key Concepts

Some **best practices for increasing security** are:

- Follow the principle of least privilege: Only provide the permission needed to do the job
- Use separate administrative accounts: Every administrator should have 2-3 user accounts. One unprivileged used to log on to computers, another with privileges.
- Restrict administrator console sign-in
- Restrict physical access
- Apply all available security updates quickly

Applying **Defense-in-depth** model to increase security:

Policies, procedures and awareness	Security documents, user education	Develop and communicate policy on the best security practice Test policies
Physical security	Guards, locks, tracking devices	Keep sensitive hardware in secure rooms, behind lock and key Keep backups in a safe Use RFID door locks to track access
Perimeter	Firewalls. network access quarantine control	
Networks	Network segments, IPsec	
Host (computer and server)	Hardening, authentication, update management	Keep computer secure with the latest security updates Configure password complexity Configure user rights Configure the host firewall Install antivirus software Prevent auto-running of devices
Application	Application hardening, antivirus	Close unused ports and ensure the security patches are up-to-date Centralise management with **WSUS***
Data	ACLs, EFS, BitLocker, backup/restore procedures	ACLs such as NTFS permissions Encrypted File System (EFS): encrypts file content, and should be used in conjunction with AD CS

		BitLocker encrypts whole volumes Recovery Certificates must be backed up

***WSUS** is a server role that centralises and manages updates. Administrators can test updates before approving them for deployment. GPO can be used to configure automatic updates.

Security Template categories are Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry, and File System.

User Rights Types: Privileges and Logon Rights. User Rights are configured via GPO. Some Common user rights are:

- Add workstations to domain
- Allow log on locally
- Allow log on through Remote Desktop Services
- Back up files and directories
- Change the system time
- Force shutdown from a remote computer
- Shut down the system

Difference between **User Rights** and **Permissions**:

User Rights restrict what a user can do to a computer system

Permissions restrict what a user can do to an object

Using **security auditing** to log security-related events to configure security auditing according to the company's security regulations and filter the **Security Event Log** in **Event Viewer** to find specific security-related events.

Group Policy can control group membership by configuring restricted groups. There are two options:

- **Members of this group**: Remove accounts not on list every time GPO is applied
- **This group is a member of**: Automatically make a group a member of other groups

Account Policy settings can mitigate the threat of brute force attacks:

Policies	Default settings
Password	Controls complexity and lifetime of passwords
Account Lockout	Controls how many incorrect attempts can

	be made

As Domain Accounts reside on DCs, Account Policies must apply to DCs.

A failed attempt to log on will be recorded in Event Viewer.

The process of **auditing object access**:

- Step 1: Configuring Auditing at GPO
- Step 2: Specify auditing details in Object SACL

Restricting software can be done by using **AppLocker** and **Software Restriction Policies** or not running specified Windows Applications.

Windows Firewall is a stateful, host-based firewall that allows or blocks network traffic according to its configuration.

Some Microsoft tools help establish a baseline of security:

- Best Practice Analyzer (Server Manager)
- Security Configuration and Analysis Wizard
- Security Compliance Manager (SCM)

➢ Innovative ways to address business needs

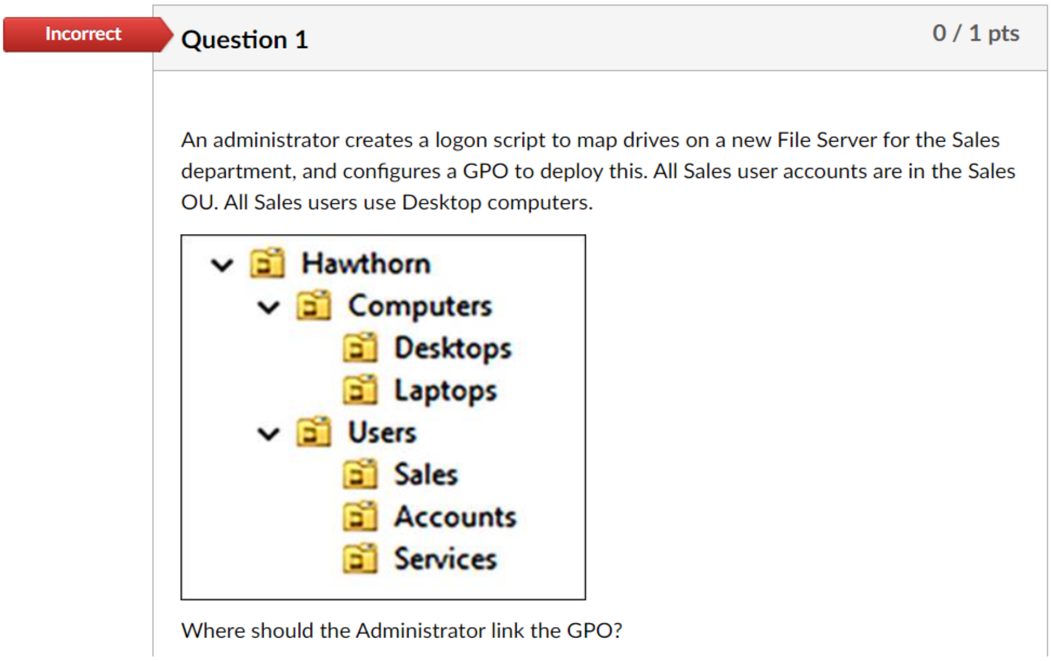
WSUS is configured for the update deployment using the HTTP protocol. However, this default deployment can be compromised by a Man-In-The-Middle attack. To mitigate the vulnerability, Microsoft advised the administrators to use HTTPS for the WSUS configuration that implements the encryption to clients and web server connections.

Some steps can be taken to secure the environment [3]:

- *Secure the WSUS environment with TLS/SSL protocol by configuring servers with HTTPS)*
- *Set up a system-based proxy for detecting updates if needed*
- *Enable the* ***Allow user proxy to be used as a fallback if detection using system fails*** *policy.*

➢ Reflection and plan for further study

One of the most common mistakes I usually make is where the GPOs can be linked to. Based on the theories I studied, GPOs can only be linked to site, domain, and OU. The example below is the question I had made a mistake in the revision quiz.



Incorrect Question 1 0 / 1 pts

An administrator creates a logon script to map drives on a new File Server for the Sales department, and configures a GPO to deploy this. All Sales user accounts are in the Sales OU. All Sales users use Desktop computers.

Where should the Administrator link the GPO?

Fig. 5 Revision quiz 9 question

To solve this problem, I plan on the revision of the theories in the lectures and read the questions more carefully before answering them.

Key configurations and commands

To harden a desktop using **Local Policies**:

- Step 1: Log on a PC as **Administrator**.
- Step 2: Typing gpedit.msc at the **Start screen** to run **Local Group Policy Editor**, then select **gpedit.msc (Microsoft Common Console Document)** to load the **Local Group Policy**.
- Step 3: In the **Computer Configuration** section, expand the **Administrative Templates** container, then expand the **Windows Components** container.
- Step 4: Double-click the **Autoplay Policies** container, and double-click the **Turn off Autoplay** Policy. Click on the **Enabled** option button.
- Step 5: Double-click on **Set the default behaviour for Autorun**, click the **Enabled** Option button and set the **Default Autorun Behaviour** option to **Do not execute any autorun commands**. Then, click **OK**.

To prohibit access to the Control Panel:

- Step 1: In gpedit, in the **User Configuration**, expand the **Administrative Templates**, then click on the **Control Panel** container.
- Step 2: Double-click on **Prohibit access to the Control Panel and PC settings.**
- Step 3: Click the **Enabled** option button, then **OK.**

To remove the Ctrl+Alt+Del Options, follow these steps:

- Step 1: In the **Local Group Policy Editor** console, find the **User Configuration → Administrative Templates → System → Ctrl+Alt+Del options** container
- Step 2: Click **Remove Lock Computer** option.
- Step 3: Double-click on the chosen option and **Enable** this setting → click **OK**.

To delegate Control of an OU, follow these steps:

- Step 1: Right-click on the OU
- Step 2: Select **Delegate Control…** to start the wizard and add the user account into the OU.
- Step 3: Delegate the tasks

To create a custom console:

- Step 1: Type **mmc** in the tool bar at the bottom left of the window
- Step 2: Click **Run as administrator** to launch the **MMC** (Microsoft Management Console)
- Step 3: In the **Console1 – [Console Root]** window, click **File** and then select **Add/Remove Snap-in**…
- Step 4: Select **Active Directory Users and Computers** snap-in, then click **Add** and click **OK**.
- Step 5: Right-click on the OU and select **New Window from Here**.
- Step 6: Click on the **Window** menu and select **Console Root** … window.
- Step 7: Save the console

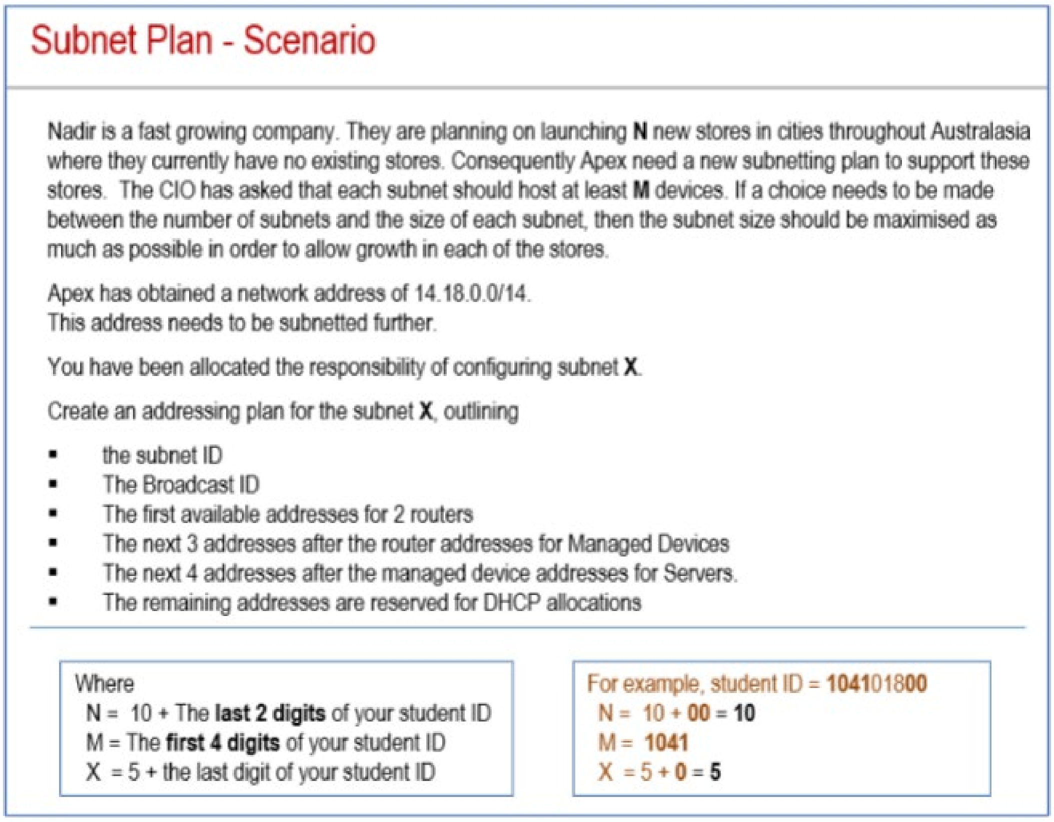
To create a Group Policy Objects:

- Step 1: Run gpmc.msc
- Step 2: Expand the **Domain** container and right-click on **Group Policy Objects**. Then select **New**.
- Step 3: Enter the name of the new GPO
- Step 4: Right-click on the new GPO and select **Edit**

To link GPOs to containers

- Step 1: In the **Group Policy Management** windows, right-click on the domain and select **Link to Existing GPO**… Select the GPO and click **OK**.
- Step 2: Run **gpupdate /force** on the PC.

Subnet Plan



Subnet Plan - Scenario

Nadir is a fast growing company. They are planning on launching **N** new stores in cities throughout Australasia where they currently have no existing stores. Consequently Apex need a new subnetting plan to support these stores. The CIO has asked that each subnet should host at least **M** devices. If a choice needs to be made between the number of subnets and the size of each subnet, then the subnet size should be maximised as much as possible in order to allow growth in each of the stores.

Apex has obtained a network address of 14.18.0.0/14.
This address needs to be subnetted further.

You have been allocated the responsibility of configuring subnet **X**.

Create an addressing plan for the subnet **X**, outlining

- the subnet ID
- The Broadcast ID
- The first available addresses for 2 routers
- The next 3 addresses after the router addresses for Managed Devices
- The next 4 addresses after the managed device addresses for Servers.
- The remaining addresses are reserved for DHCP allocations

Where
N = 10 + The **last 2 digits** of your student ID
M = The **first 4 digits** of your student ID
X = 5 + the last digit of your student ID

For example, student ID = **104101800**
N = 10 + **00** = **10**
M = **1041**
X = 5 + **0** = **5**

Fig. 6 Subnet Plan Scenario

Student ID: 103818400

According to the instructions in the Fig. above:

N = 10 + 0 = 10

M = 1038

X = 5 + 0 = 5

After applying the change, the scenario problem can be summarised as:

The company: Network Address: 14.18.0.0/14

Need: 10 new branches/subnets

Need: at least 1038 devices/available hosts for each subnet

Administrator: responsible for Subnet 5

Here is the subnet plan for this company:

Referring to the scenario in Fig. 4 above, the company demands to maximize the subnet size as much as possible in other to allow growth in each of the stores in the future rather than increasing the number of stores.

Currently, the company needs 10 more stores so 4 host bits need to be borrowed (2^3 = 8 < 10 so it must be 2^4 = 16 > 10).

The company needs 1038 devices for each subnet so 11 bits need to be borrowed (2^{10} - 2 = 1022 < 1038 so must be 2^{11} – 2 = 2046 > 1038).

The leftover bits = 32 – 14 – 4 – 11 = 3 bits. These 3 leftover bits should be added to the host portion due to the demand of the company. Therefore, the number of network bits after subnetting = 14 + 4 = 18 bits.

The subnet mask of the subnet address is 255.255.192.0 (slash notation: /18)

Number of host bits = 32 - 18 = 14 bits

Number of devices in each subnet = 2^{14} - 2 = 16382 devices (2 unusable addresses for network address and broadcast address)

Therefore, after the first time subnetting, the number of devices in each subnet will be 16382 devices and after the last time subnetting, the number of devices in each subnet will be 2046 devices >= the minimum required size of each subnet which is 1038.

The gap size will be 256 – 192 = 64. Every time the gap size is added to the next subnet ID, the gap size will be added to the third octet of the address as 248 is located in the third octet.

To find the first IP address of each subnet, increment the last octet value of that subnet ID by one.

To find the broadcast address of each subnet, decrement the third octet value of the next subnet ID by one and set the last octet value to 255.

To find the last IP address of each subnet, decrement the last octet value of that subnet's broadcast address by one.

After doing the subnetting the subnets information is displayed in the table below:

Subnet	Subnet ID	First Address	Last Address	Broadcast address
0	14.18.0.0/18	14.18.0.1	14.18.63.254	14.18.63.255
1	14.18.64.0/18	14.18.64.1	14.18.127.254	14.18.127.255
2	14.18.128.0/18	14.18.128.1	14.18.191.254	14.18.191.255
3	14.18.192.0/18	14.18.192.1	14.18.255.254	14.18.255.255
4	14.19.0.0/18	14.19.0.1	14.19.63.254	14.19.63.255
5	14.19.64.0/18	14.19.64.1	14.19.127.254	14.19.127.255

Based on the table above, subnet 5 has:

Subnet ID: 14.19.64.0/18

Broadcast address: 14.19.127.255

Subnet range: 14.19.64.1 - 14.19.127.254 → 2046 usable devices.

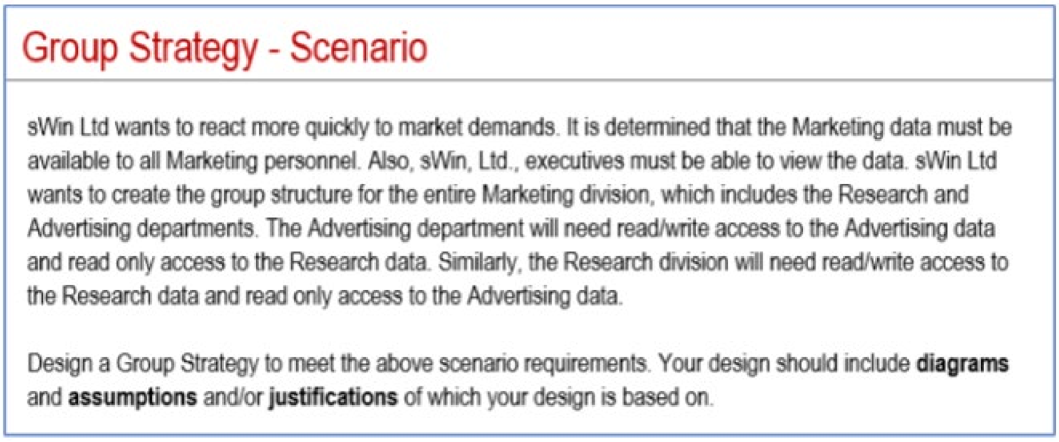
The **first 2 available** addresses for 2 routers: 14.19.64.1/18 and 14.19.64.2/18

The **next 3 addresses** after the router addresses for **Managed devices**: 14.19.64.3/18, 14.19.64.4/18, and 14.19.64.5/18

The **next 4 addresses** after the Managed devices addresses for **Servers**: 14.19.64.6/18, 14.19.64.7/18, 14.19.64.8/18, and 14.19.64.9/18

Remaining addresses reserved for DHCP allocations: from 14.19.64.10/18 to 14.19.127.254/18 → (16382 – 2 – 3 – 4) = 16373 usable addresses in total

Group Strategy



Group Strategy - Scenario

sWin Ltd wants to react more quickly to market demands. It is determined that the Marketing data must be available to all Marketing personnel. Also, sWin, Ltd., executives must be able to view the data. sWin Ltd wants to create the group structure for the entire Marketing division, which includes the Research and Advertising departments. The Advertising department will need read/write access to the Advertising data and read only access to the Research data. Similarly, the Research division will need read/write access to the Research data and read only access to the Advertising data.

Design a Group Strategy to meet the above scenario requirements. Your design should include **diagrams** and **assumptions** and/or **justifications** of which your design is based on.

Fig. 7 Group strategy Scenario

According to the scenario above, there should be 3 groups for 3 teams: the Executive group, the Researching department group and the Advertising department group.

All these groups are in the same domain so all of them are global groups.

Based on the group naming convention:

- Executives: **G_Executives**
- Researching department: **G_ Research**
- Advertising department: **G_Advertise**

There are 2 resources: research data and advertising data.

All these groups are domain local groups due to their responsibility for the resource access of their group members.

Based on the group naming convention:

- Executives must have **Read-only** access to all the data: **DL_AdvertisingData_R**, **DL_ResearchingData_R**
- The advertising department needs to have **Read/write** access to the advertising data: **DL_AdvertisingData_RW**
- The advertising department needs to have **Read-only** access to the researching data: **DL_ResearchingData_R**
- The researching department needs to have **Read/write** access to the researching data: **DL_ResearchingData_RW**
- The researching department needs to have **Read-only** access to the advertising data: **DL_AdvertisingData_R**

For this scenario, the strategy must be used is: **I → G → DL ← A**

- I: Identity
- G: Global group and
- DL: Domain Local group
- A: Access

The folder must be shared with the ruled group so both the interactive user and network user can access the resources.

The diagram below demonstrates all the information above:

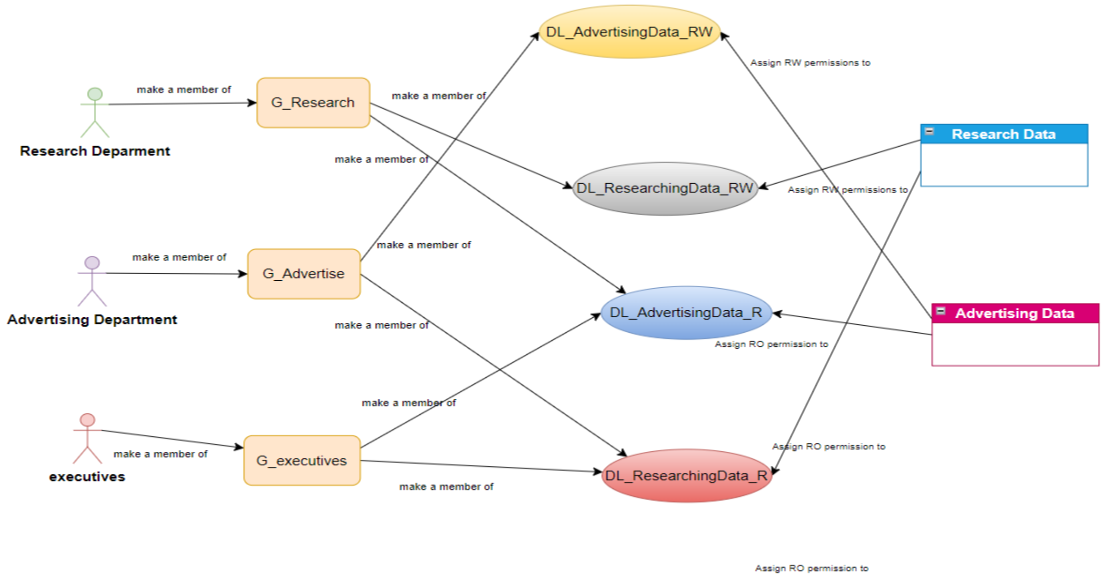


Fig. 8 Group strategy diagram

References

[1] A. Simister, “Active Directory Permissions Delegation Best Practices,” Lepide Blog: A Guide to IT Security, Compliance and IT Operations, Jun. 15, 2023. https://www.lepide.com/blog/ad-permissions-delegation-best-practices/#:~:text=Delegating%20control%20in%20Active%20Directory

[2] Danny Murphy, “Top 10 Most Important Group Policy Settings for Preventing Security Breaches - Lepide Blog: A Guide to IT Security, Compliance and IT Operations,” Lepide Blog: A Guide to IT Security, Compliance and IT Operations, Dec. 2017. https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

[3] “Microsoft WSUS vulnerable to attack,” Office of the Chief Information Security Officer. https://ciso.uw.edu/2020/09/10/microsoft-wsus-vulnerable-to-attack/

[4] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lecture-07-slide-presentation-ad-groups-and-permissions?module_item_id=3845570

[5] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lecture-08-slide-presentation-gpos?module_item_id=3845572

[6] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lecture-09-slide-presentation-security?module_item_id=3845574

[7] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lab-06-identity-and-access-control-using-ad-ds

[8] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lab-07-rbac-using-ad-ds-and-security-groups

[9] “Redirecting,” login.microsoftonline.com. https://swinburne.instructure.com/courses/57016/pages/lab-08-group-policy-objects