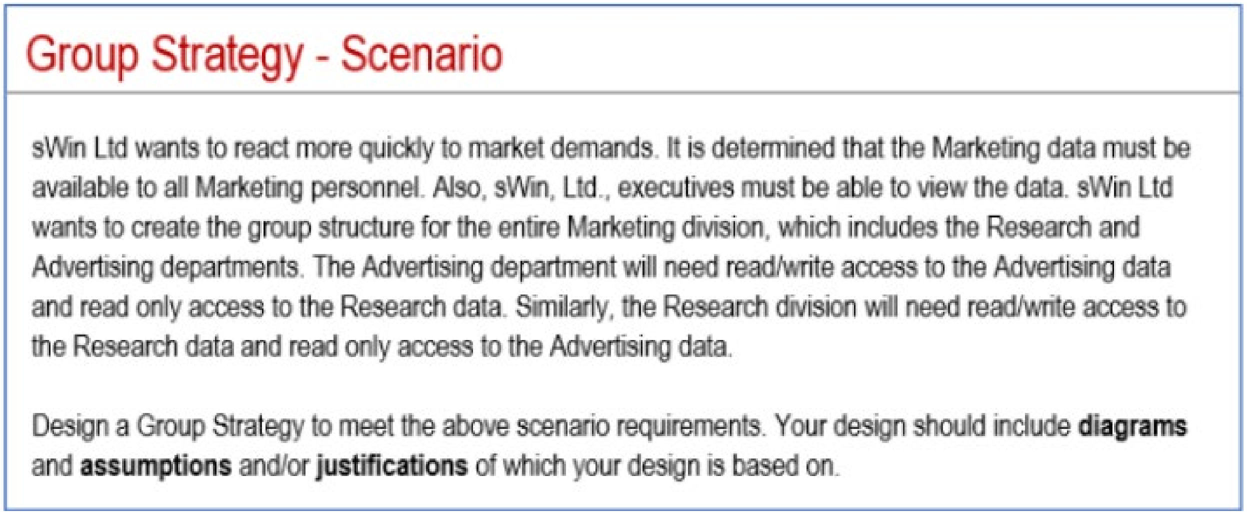
WEEKLY JOURNAL 3

Khoi Nguyen Pham – 104772183

Swinburne University of Technology

I. Table of Contents

II. 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.

Figure 1. Group Strategy Scenario in Weekly Journal 3 [1]

From my interpretation, since the Marketing division consists of the Research and Advertising departments, the Marketing data will include the Research and Advertising data. The executives must also be able to see the data, so they will also have a separate group.

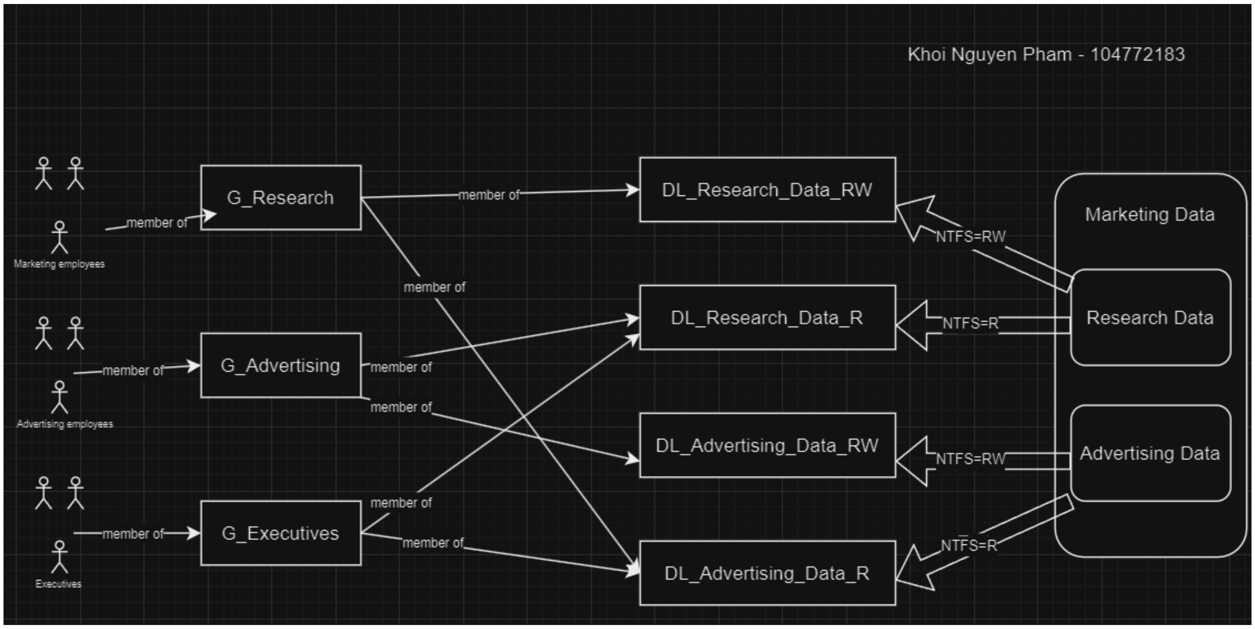
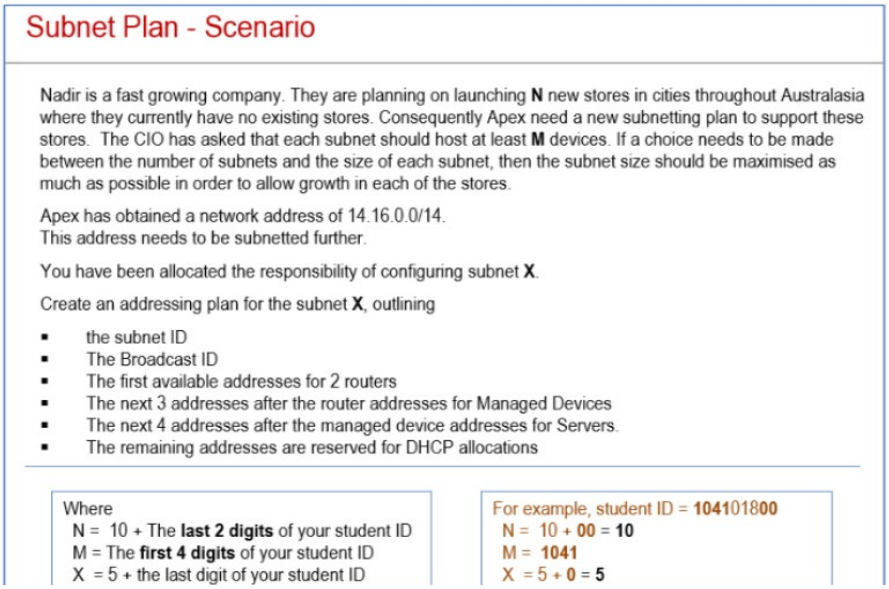


Figure 2. Group Strategy drawn on diagram.net [2]

There will be two domain local groups which have read and read-write permission for each data resource. The Research group has read-write access to the Research Data and read-only access to the Advertising Data, while the Advertising group has read-write access to the Advertising Data and read-only access to the Research Data. Additionally, the Executives group has read-only access to both data resources. Both data resources will assign the proper NTFS permissions to its corresponding domain local groups, ensuring access for the right users.

III. Subnet Design



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 14.16.0.0/14.
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 = 1041018**00**
N = 10 + **00** = **10**
M = **1041**
X = 5 + **0** = **5**

Figure 3. Subnet Design Scenario in Weekly Journal 3 [1]

Since my student ID is 104772183, the values for the scenario are:

- N = 10 + 83= 93 stores.
- M = 1047 devices
- X = 5 + 3 = subnet 8

The provided network address is 14.16.0.0/14:

- 93 branches => borrow 7 subnet bits since 2^7 = 128 > 93
- Calculate the subnet bits if borrow 7 bits: 14 + 7 = 21
- 1047 devices => 11 host bits since 2^{11} – 2 = 2046 > 1047
- Calculate the subnet bits for 11 host bits: 32 -11 = 21
- They want to maximize the subnet size, so I reserve the host bits. However, there're no extra bits => New subnet mask is /21.
- /21 in dotted-decimal notation is 255.255.248.0. Therefore, the subnet gap is in the 3rd octet: 256 – 248 = 8

Having found the subnet gap, now I'm going to create an addressing plan of 14.16.0.0/21 for subnet 8:

Table 1. Subnet Plan made on Word by Khoi Nguyen Pham:

Subnet 0	14.	16.	0.	0.
Subnet 1	14.	16.	8. (0 + 8)	0.
Subnet 2	14.	16.	16. (8 + 8)	0.
Subnet 3	14.	16.	24. (16 + 8)	0.
…	…	…	…	…
Subnet 8	14.	16.	64. (56 + 8)	0.
Subnet 9	14.	16.	72. (64 + 8)	0.

- Subnet ID 8 is 14.16.64.0
- The broadcast address is 14.16.71.255 (one address before subnet ID 9).
- The first available addresses for 2 routers are 14.16.64.1 and 14.16.64.2
- The next 3 addresses for Managed Devices are 14.16.64.3, 14.16.64.4 and 14.16.64.5
- The next 4 addresses for Servers are 14.16.64.6, 14.16.64.7, 14.16.64.8 and 14.16.64.9.

- The remaining addresses reserved for DHCP allocations are the remaining usable addresses: 14.16.64.10 – 14.16.71.254

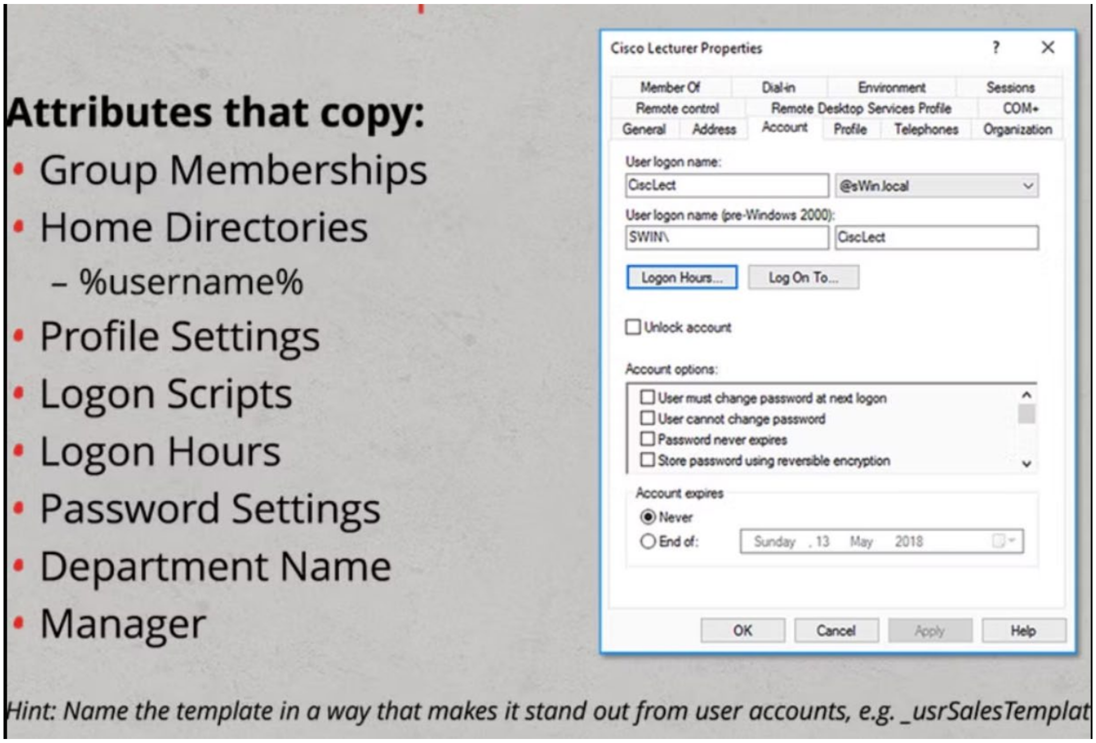
IV. Key Concepts

1. Week 7 (16/09 – 22/09)

1.1. Lectures

a. Organizing AD Accounts

This week's lecture introduces us how to create and organize multiple accounts and how we can use Organizational Unit (OU) to delegate control. Firstly, we got introduced to user account templates in Active Directory. They are predefined configurations that help network administrators quickly create new user accounts with consistent settings. These templates have multiple attributes which are automatically applied when creating accounts, making the process more efficient and consistent. This feature is crucial for businesses having to manage large amounts of users by providing a centralized way to control account configurations.



Attributes that copy:

- Group Memberships
- Home Directories
  - %username%
- Profile Settings
- Logon Scripts
- Logon Hours
- Password Settings
- Department Name
- Manager

Cisco Lecturer Properties

User logon name: CiscLect @sWin.local

User logon name (pre-Windows 2000): SWIN\ CiscLect

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Sunday , 13 May 2018

Hint: Name the template in a way that makes it stand out from user accounts, e.g. _usrSalesTemplat

Figure 4. Attributes of user account templates [3]

I've come up with a scenario to strengthen my understanding. Let's say a new employee named Nguyen joins the Programming department. A user account template for Programming employees could be configured as these:

- Group Memberships: Automatically add Nguyen to the Programming Team.
- Home Directories: Creates a personal directory for users as "\programming-server\home%username%"
- Profile Settings: Configure the OS to Windows 11, set the wallpaper as the logo of the company, and automatically installed Visual Studio.
- Logon Scripts: Used to map network drives to shared coding resources.
- Logon Hours: Allow logins Monday through Sunday, 9:00 – 21:00.

- Password Settings: Requires passwords to be at least 10 characters long with a combination of characters, numbers and symbols.
- Department Name: Set his department name to “Programming”.

We’ve also got to know about bulk user account creation. This process utilizes user account templates to ensure that all accounts created in bulk have consistent settings and configurations. There are two main methods for this process:

- CSVDE: Imports and exports account details from a CSV file. For instance, if Swinburne has 1000 new students, the administrator can create a CSV file with settings for each student and run a single command to create all accounts at once.
- LDFIFDE: Imports and exports account details in the LDAP format. Compared to CSVDE, it’s more flexible and can handle more complicated directory structures and attributes. For example, if Swinburne wants to move student accounts from another directory service to Active Directory, they can export the user data in LDIF format and then put it into Active Directory using LDIFDE.

Last week’s content [4] introduced us to Domain Terminology, specifically OU, which is a container that organizes users, computers, and other OUs. This week focuses on explaining why and how OUs are used. I’ve already written down how OUs allow a hierarchical structure and help managing large groups of people in Weekly Journal 2 [5], but I’ve just learned that OU structure can be based on various criteria, and they can target Group Policy for specific configurations for specific objects:

- Geographical location (e.g.: Australia, Canada): Allows businesses operate in different places to manage their own users and resources, meaning they can apply region-specific policies.
- Business units (e.g.: sales, marketing, designing): Allows companies with distinct departments to have their own policies.
- Resource management (e.g.: server, laptop, PC): Allows companies that manage various types of devices for configurations like security or maintenance.

b. Role Based Access Control

I’ve also gained a deeper understanding of permission inheritance. Inherited permissions are automatically passed down from a parent object to its child object. For example, if a folder has a write permission set for a group, all of the files and subfolders inside that folder will also have the write permission if there aren’t any overridden explicit permissions.

From what I understand from permission precedence, the system prioritizes permissions in this order: explicit Deny, explicit Allow, inherited Deny, inherited Allow. Let’s say that Folder A inherits read permission from Group X and if file B within folder A has set deny read permission, folder A can’t access file B because the system checks for file B’s deny permission first.

In large environments with multiple resources, permission inheritance is crucial since it simplifies the management and consistency of permissions. When applying to higher levels, the permissions automatically pass down to all contained objects, reducing the risk of misconfigurations.

Last week, we’ve gained basic concepts of group scopes and how we can apply I=>G=>DL<=A strategy to manage permissions effectively. In this week, I’ve had a deeper understanding of these groups, and how we can combine multiple first-level account groups within second-level groups to manage permissions in a more hierarchical way. As organizations are becoming more complex with larger amounts of users, this method is very efficient in simplifying access rights control across the environment and increasing security.

Second-level account groups in Active Directory are categorized based on their scope:

- If the second-level account group is aggregating groups from within a single domain, it should be a global group. Global groups offer a centralized measure to manage user permissions, hence reducing administrative overhead and enhancing efficiency. For example, in a game company like EA, a global group called “EA Sports Team” could be established, and it will include first-level groups, such as FIFA, NFL, or NBA.

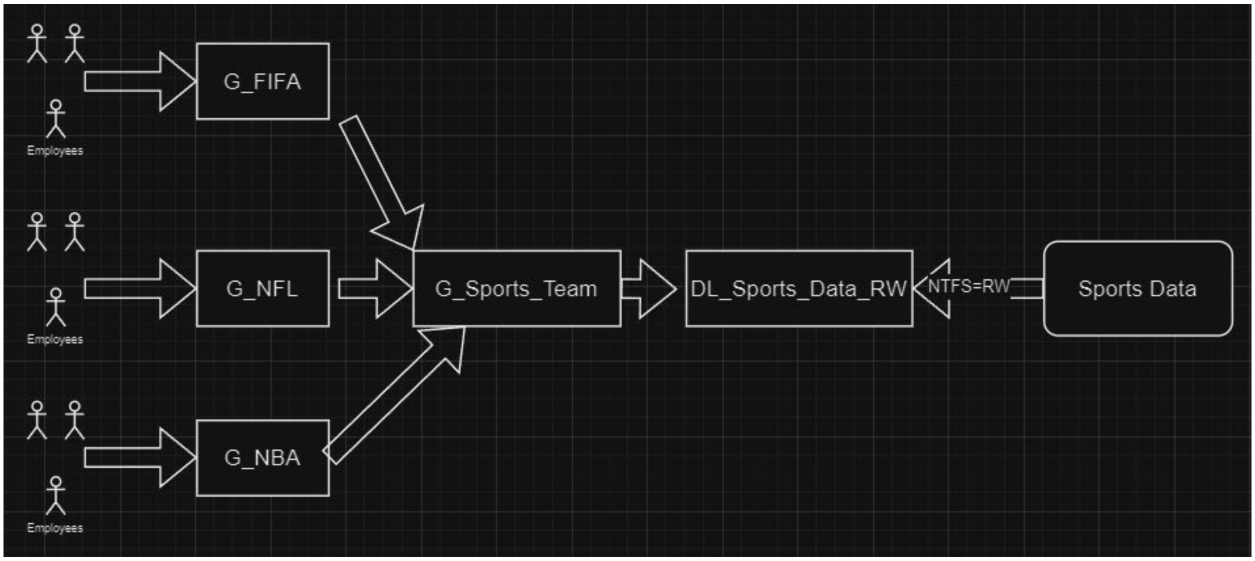


Figure 5. Drawn on diagram.net [2]

- Conversely, when the second-level account group is collecting groups from multiple domains, it is classified as a universal group. This enables businesses with multiple teams to collaborate and share resources across different domains within a forest. Let's say Steam has a universal group call "Game Marketing", it will aggregate first-level groups in different countries such as "EA Marketing Team", "Ubisoft Marketing Team", or "Capcom Marketing Team".

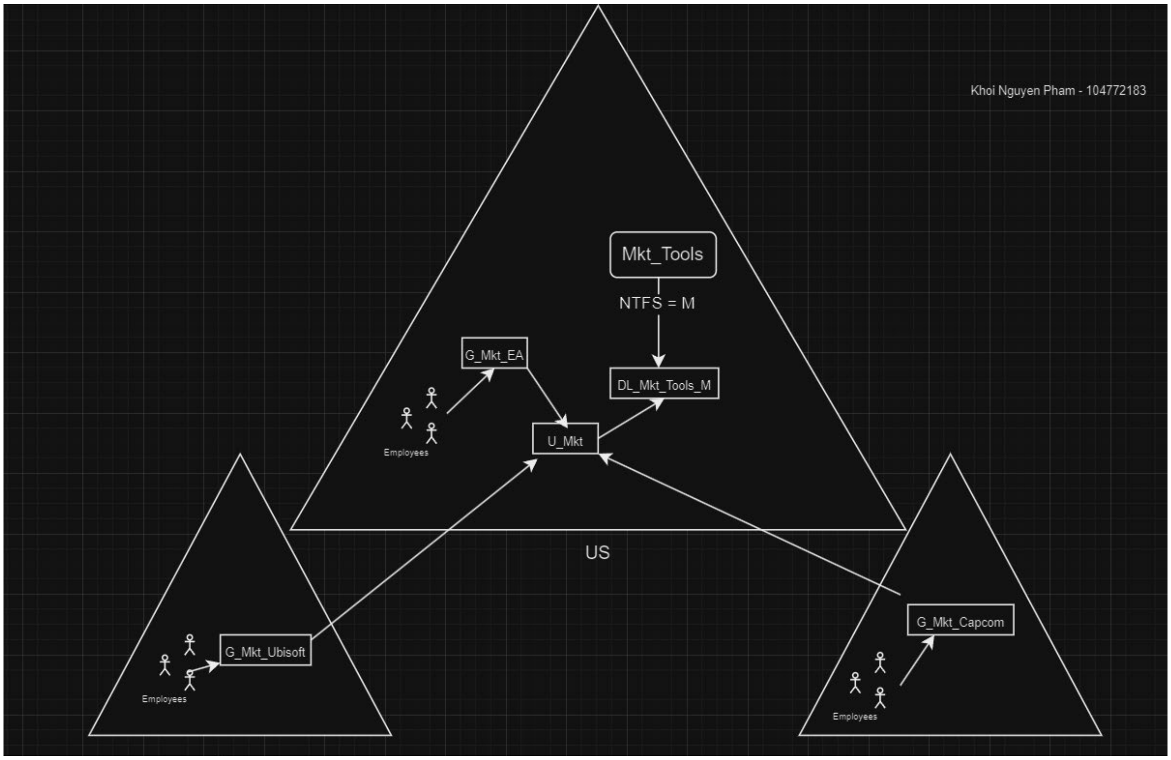


Figure 6. Drawn on diagram.net [2]

Since universal groups replicate changes across all domain controllers in the forest, this might affect performance due to overloading the network. On the other hand, global groups only replicate in their own domain. Therefore, it's important to know when to utilize which second-level account groups.

I've also learned about Access-Based Enumeration (ABE) and how it improves security and user experience. ABE ensures that users can't see resources they don't have permission to access. This enables companies to reduce the potential attack surface from malicious actors.

NTFS and Share permissions can be apply to predefined groups. This helps administrators to set permissions for broader categories without having to work with individual accounts. By utilizing this feature, we can control access as well as ensuring that permissions are applied appropriately with ABE, allowing for better security within organizations.

Coincidentally, in my Weekly Journal 2 [5], I've looked up on how NTFS and share permissions can be combined, and this week's content furtherly explained this concept. I've learned that it only applies when accessing a shared folder over the network. However, if accessed locally, share permissions don't apply and only NTFS permissions take control. When a user belongs to multiple groups, both NTFS and share permissions can accumulate within each permission type. For example, if group A has NTFS Read, group B has NTFS Write, and group C has NTFS Modify, they will accumulate. The user will then inherit all three permissions: Read, Write, and Modify until there's any explicit "Deny" for one of the permissions.

1.2. Lab 6: Configuring a Windows Server Domain

This week's lab gave us hands-on experience to install AD DS, join computers to a domain, create user, computer, and group account. Finally, we learned how to control access to resources in a domain.

As we've already known, AD DS can be used by businesses to centralize management. Joining Windows 10 computers to the domain enhances security and ensures that administration is simplified.

Creating user, computer, and group accounts within a domain are crucial for efficient management and security in a business environment. Domain user accounts enable employees to manage their own resources, whereas domain computer accounts allow network administrators to monitor and manage all devices within the network. Lastly, group accounts can be used to assign access rights to multiple users at once, therefore, saving time and reducing misconfigurations.

2. Week 8 (23/09 – 29/09)

2.1. Lectures

a. Introduction to GPOs

In this week's lecture [6], I've gain deeper understanding in Group Policy Options (GPOs). First of all, I've known that configuring settings manually (e.g.: change screen saver settings) will make change in the registry, which is not the ideal way since it's not efficient and error-prone. Therefore, using Local Computer Policies is a friendlier way to modify the registry due to its consistency and centralized nature.

Group Policies are similar to Computer Policies but configured in a domain. They can be applied to two main objects:

- Computer: Applied on the computer itself, regardless of the users. For example, a Swinburne's computer is enforced with a firewall policy for all the teachers or students who log on.
- User: Affect the user's environment to any computer they log on. For instance, my student account is configured with the Swinburne's wallpaper regardless of the computer I log into.

Group Policies can only be modified by administrators and not the end users, ensuring that devices within organizations (e.g.: Swinburne) are secured and consistent.

I've also learned about Group Policy Container (GPC) and its purpose of storing settings of a GPO. It is located in Active Directory to centralize management. Changes in one container are replicated to another Domain Controller, enabling better consistency. Businesses can utilize this to manage devices more time-efficiently and reduce misconfigurations on a larger scale.

Another component of GPOs is Group Policy Template (GPT). GPC points to GPT, which contains the actual settings of GPO to further policy enforcement.

Let's say a company wants to enforce a screensaver password policy. GPC will store the metadata (e.g.: version and links) of the policy whereas GPT contains the actual settings like password requirements and timeout in SYSVOL, and it will replicate across all DCs.

Unlike standard GPO which are strictly implied, GPO Preferences allow users to modify the settings, offering better flexibility. An example of how we can utilize this is setting default printers for users in the office. Administrators can use Preferences to configure a user to a specific printer but allowing the user to switch to another printer if needed.

The lecture also briefly introduced Default GPOs, such as Default Domain Policy and Default Domain Controller Policy. The Default Domain Policy is pre-linked to the domain and manages security and power settings, whereas the Default Domain Controller Policy is pre-linked to OUs to manage user rights for DCs. These default GPOs automatically provide initial baseline configurations to reduce setup time.

b. Controlling GPO Scope

Crucially, GPOs have to be linked to apply the settings, and a single GPO is able to link to multiple containers. GPOs can only be linked to Site, Domain, and OU, and cannot be linked to Groups, Users, Computers, Users or Computers containers in AD.

GPOs apply in a specific order: Local > Site > Domain > Parent OU > Child OU. If multiple conflicting GPOs are applied at the same level, the last GPO wins. GPOs linked to higher levels are inherited by sub-levels, and administrators can prevent this by blocking inheritance. The downside of this is that you cannot selectively block inheritance but have to block all.

By linking GPOs at appropriate levels, businesses can have consistent security policies while allowing specific settings for individual departments. Let's say an administrator wants to enforce password protection to all users across the company, they can link the GPO to the domain that contains all these users. However, there are special service accounts that don't require passwords, therefore administrators can block inheritance on these accounts.

If we want to give someone permission to manage and link GPOs without granting them full domain control, we can use Delegate Control wizard. For instance, if an administrator wants a helpdesk team member to help with policies management in the Marketing department, they can use Delegate Control wizard to allow the member to only be able to reset passwords for all users to this OU only.

GPO can be set to "Enforced" to ensure that settings will be guaranteed applied, despite block inheritance or conflicting settings. Let's get back to our example. Later, due to a data breach, the company decides that all accounts must have a password protection policy, and to do that, administrators must enforce the password GPO.

As stated earlier, GPO cannot be linked to Groups or objects like Users or Computers. However, we can still achieve this by using Filtering. Filtering allows us to control which groups, users or computers a GPO can apply to. There are 2 types of filtering:

- Security Filtering: Specified which users or groups can apply to the GPO. For example, a university has a "Remote Desktop Access" GPO linked to "All Students" OU, but the administrator only wants the online students to have remote access, so they can use security filtering to grant Apply Group Policy permission to the online students group.
- WMI Filtering: Specified GPO based on the system such as OS or hardware requirements. For example, we can use this to apply a policy to a desktop with more than 4GB of RAM.

GPOs can use Administrative Templates to define settings that can be managed:

- ADMX: Provide code for settings like installing ADMX for Microsoft Office.
- ADML: Display GPO in multiple languages.

2.2. Lab 7: Securing resources in a domain

This week's lab focuses on providing better security and scalability by creating child domains and implementing strategic group nesting and permission controls.

Firstly, we've learned to add a new domain to an existing forest to create a child domain. Businesses can use this to improve scalability. Then, I applied for the appropriate permissions for the resources. After that, I've deployed a secure and scalable strategy by nesting groups within a second-level group and storing all of them into an OU. For me, this is the most important part of this lab, as it successfully demonstrates how administrators can effectively manage access rights to resources. I've also learned a second way to create a new user by using User Account Template. By using the template, we can effectively create accounts with the same settings to avoid misconfigurations and better time management. Lastly, I've troubleshooted by testing access from different accounts as this is a crucial step for a network administrator.

3. Week 9 (30/09 – 06/10)

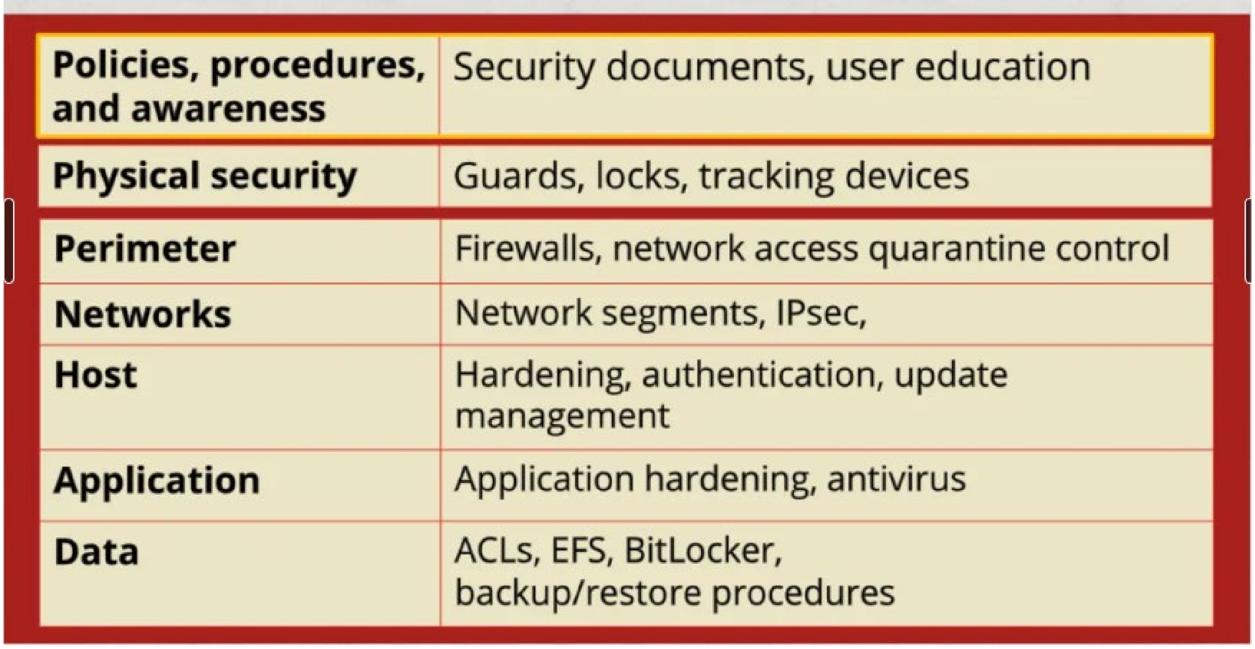
3.1. Lectures

a. The Defense-in-Depth model

I've learned some of the best practices to increase security in the lecture [7]:

- Follow the principle of lease privilege: User and administrator should be only granted the minimum permissions to do the job. This helps businesses to reduce the risk of malicious activity or potential data breaches.
- Use separate administrative accounts: For example, Justin - a lecturer has a standard account used for daily activities like uploading lectures, checking emails and interacting with students. He can also have another account used for administrative tasks such as modifying course settings and managing students enrollment.
- Restrict administrator console sign-in: Let's say Justin wants to change some course settings, he should log in with his standard account and use "Run-As" to perform the tasks. Justin should avoid logging in with administrators unless absolutely necessary.
- Restrict physical access: Companies can use methods such as locks or ID cards to control access to data rooms.
- Apply all available security updates quickly: This can minimize some potential weaknesses that attackers can exploit. However, it's also good for a balanced approach as updates must be tested carefully before implementation. This was evident in the recent Microsoft and CrowdStrike incident, where multiple flights around the world are cancelled due to the new update from CrowdStrike [8].

Another security approach is to apply defense-in-depth concepts. This approach applies multiple layers to enhance security and reduce potential data breach for businesses.



Policies, procedures, and awareness	Security documents, user education
Physical security	Guards, locks, tracking devices
Perimeter	Firewalls, network access quarantine control
Networks	Network segments, IPsec,
Host	Hardening, authentication, update management
Application	Application hardening, antivirus
Data	ACLs, EFS, BitLocker, backup/restore procedures

Figure 7. Layers of Defense-in-depth [7]

I've found some different examples from the lectures for these layers:

- Policies, procedures and awareness: Ablett suggests "all employees to clean up their table to prevent unwanted access". [9]
- Host: One paper suggests "configure Endpoint Detection and Response to detect malicious activities and initiate automatic defenses". [10]
- Application: Boyd and Keromytis recommend "setting up input validation mechanisms on a web application to prevent SQL injection attacks". [11]

I've also learned about WSUS, which is a Microsoft server role to manage updates and patches across the network in a controlled and centralized way. In a corporation with multiple devices, WSUS makes sure all of them are successfully updated with the new patches. It can also deploy the updates to test environments to prevent any instability and potential issues to the company.

b. Using GPOs to Secure a Network

As we all know, GPOs can be used to enhance security. GPOs can configure user rights to control system-level access such as logon rights, whereas permissions function on individual objects like files or folders. Understanding these rights and permissions enables administrators to prevent unauthorized access.

Security templates are default configurations that can be applied through GPOs to enforce security consistently across multiple devices. Administrators can implement this to reduce vulnerabilities and make it easier for management.

GPOs can also be used to audit, by allowing organizations to monitor events within the network. Administrators can audit events such as account logons or object access, ensuring the activities are authorized. To enhance this process, SACLs can be configured to observe and determine access of specific events, therefore administrators can detect and take preventive measures quickly.

We can use GPOs to restrict the privilege of the administrator to manage a group and control the services their devices run. They can also be used to block access to specific applications and software (e.g. calculator). Window Firewall can be deployed to further protect the system. All of these features enable companies with large scales to manage the network more effectively and reduce malware risks.

Lastly, I've learned that Microsoft has provided some baseline security tools to use alongside GPOs, such as Server Manager to check if the server follows best practices, Security Configuration and Analysis Wizard to compare current settings with baseline, and SCM to create and enforce security baselines. Mastering these tools enables administrators to secure the system efficiently.

3.2. Lab 8: Configuring Group Policies in a Domain

In this lab, I've gained practical knowledge on how to create and link GPOs to containers. Specifically, I've tested linking around different GPOs to understand how they are applied (e.g.: local, domain, OU) and how precedence affects conflicting settings within the same level. I've applied further to groups and users using the filtering features. I've also got to deploy printers to users. These are important skillset for administrators to control policies that are applied appropriately and effectively across the entire organization.

V. Further Study

1. Week 7 (16/09 – 22/09)

In the revision quizzes, the most challenging questions I found were related to the Domain Terminology. I've understood how they can be implemented in practice, but when it comes to specific technical terms in the lectures and the quizzes, I had trouble remembering them. One of my friends also had a hard time memorizing these terms, so we've decided to break down the concept into simpler terms, and explain them to each other, since teaching is the best way to reinforce our understanding.

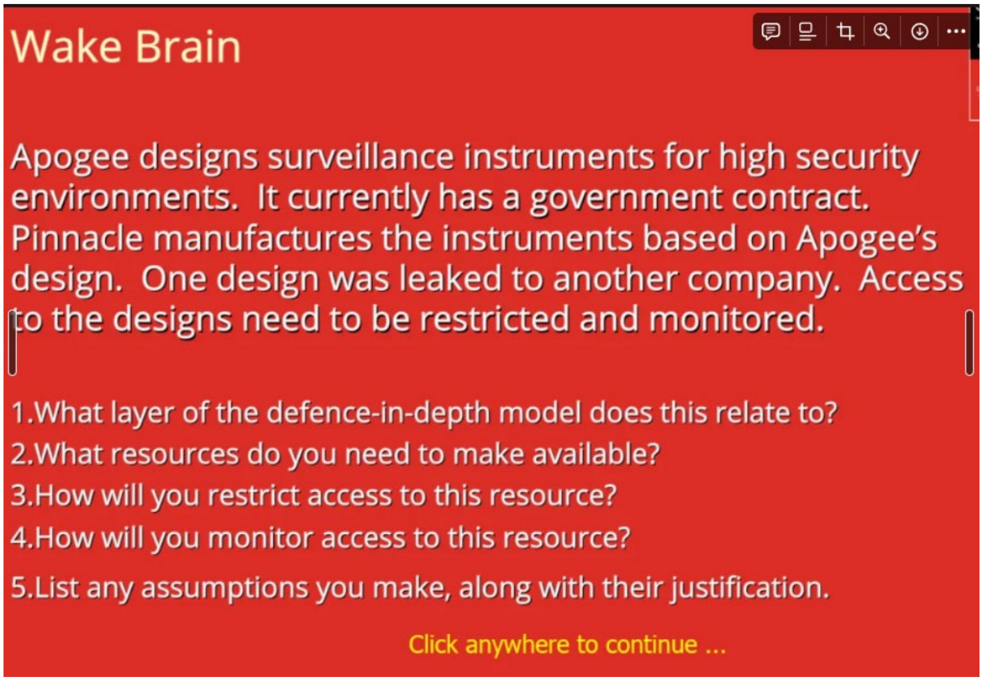
I was interested in ABE, so I've decided to dive deeper into this feature, and found some drawbacks with it. The configuration often encounters performance overhead because the server has to constantly evaluate which permissions should be visible [12]. Therefore, administrators often combine ABE with permissions to limit who can see the share resources in the first place.

2. Week 8 (23/09 – 29/09)

There were no challenges in this week's quizzes, however I've made several misconfigurations in the lab which leads to inaccessibility using different accounts. These mistakes were mostly from the nesting process, where I wasn't careful enough to correctly nest the appropriate groups. Therefore, I spent additional time reviewing and practicing the lab again more thoroughly and at a slower pace to ensure there's no error in the process.

3. Week 9 (30/09 – 06/10)

In this week's lecture, there are some questions without answers to solidify our understanding of security [7]. I've referred to the lectures and my knowledge to answer these questions.



Wake Brain

Apogee designs surveillance instruments for high security environments. It currently has a government contract. Pinnacle manufactures the instruments based on Apogee's design. One design was leaked to another company. Access to the designs need to be restricted and monitored.

1.What layer of the defence-in-depth model does this relate to?
2.What resources do you need to make available?
3.How will you restrict access to this resource?
4.How will you monitor access to this resource?
5.List any assumptions you make, along with their justification.

Figure 8. Questions from Lecture 9 [7]

1. This relates to the Data layer since one design which is critical data was leaked.
2. Resources to make available are:
   - Identity and Access Management (IAM) tools to control and manage user access.
   - Monitoring tools for auditing access to the designs and logging user activity.
3. I will use GPO to control and configure appropriate policies to prevent unauthorized access.
4. I will use GPOs to configure SACLs to log who accesses the resources.

VI. Key Configurations and Commands

1. Week 7 (16//09 – 22/09)

- Install AD DS: In ***Add Roles and Features*** => ***Install***
- Promote: Click on yellow triangle => ***Promote this server to a domain controller*** => ***Add a new forest*** => Set both level to ***Windows Server 2016*** => ***DSRM password***
- Create Accounts: ***Tools*** => ***Active Directory Users and*** Computers => right-click ***Users/Computers*** => ***New Users/Computers***
- Create Group Accounts: Right-click OU => ***New…*** => ***Group***.
- Share permissions: Right-click the folder => ***Properties*** => ***Sharing*** => ***Advanced Sharing*** => check ***Share this folder*** => ***Permissions***.
- Create OUs: ***Active Directory Users and Computers*** => right-click on the domain (sWin.Local) => ***New*** => ***Organizational Unit***.
- Create Domain Local Groups: Right-click OU => ***New*** => ***Group*** => ***Domain Local***.
- NTFS permissions: Right-click (sWinData) folder => ***Properties*** => ***Security*** => ***Edit*** => ***Add*** => enter the group names => set permissions.

- Join a domain: Search ***System*** => ***Change Settings*** => ***Change*** => ***Domain***.
- Remove inherited permissions: ***Properties*** => ***Security*** => ***Advanced*** => ***Disable Inheritance*** => ***Convert inherited permissions into….*** => ***Convert…*** => ***Remove***

2. Week 8 (23/09 – 29/09)

- Create Child Domain: After installing AD DS => ***Promote this server to be a domain controller*** => ***Add a new domain to an existing forest.***
- Nesting: Right-click on objects => ***Properties*** => ***Member of*** => ***Add.***
- User Account Template: Right-click on accounts => ***Copy…*** => Enter required settings.

3. Week 9 (30/09 – 06/10)

- Prohibit Control Panel: In ***gpedit*** => ***User Configuration*** => ***Administrative templates*** => ***Control Panel*** => ***Prohibit access to the Control Panel and PC settings*** => ***Enabled***.
- Create Custom Console: Search ***mmc*** => ***Run as administrator*** => In ***Console1 – [Console Root]*** => ***File*** => ***Add/Remove Snap-in….*** => ***Active Directory Users and Computers*** => ***Add***. ***Right-click OU*** => ***New Window from Here*** => ***Window*** => ***Console Root\ …***
- Create, link and edit GPOs: Right-click ***Group Policy Objects*** => ***New***. Select container => ***Link an Existing GPO…*** Right-click new GPO => ***Edit… => Expand User Configuration => Policies => Administrative Templates= > System.***
- gpupdate /force: Apply GPO settings.
- Security Filtering: Right-click GPO => ***Edit..*** => Right-click GPO name => ***Properties*** => ***Security*** tab.
- Modelling GPOs: Right-click ***Group Policy Modeling => Enter user and computer*** => ***Next*** => ***Details.***
- Deploy Printers: Add ***Print and Document Services***. ***Tools*** => ***Printer Management*** => ***Right-click Printers*** => ***Add Printers…*** => ***Add a new printer using an existing port: LTP1*** => ***Printer Driver*** => ***Install a new driver*** => ***select MS Publisher Color Printer***. Back in ***Print Management*** => right-click ***GPO*** => ***MS Publisher Color Printer*** => ***Browse*** => Check ***The users that this GPO applies to (per user).***

VII. References

[1] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Portfolio Task - Weekly Journal 3,” 2024.

[2] "diagrams.net," JGraph Ltd. [Online]. Available: https://app.diagrams.net.

[3] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Lecture 07 Slide Presentation – AD, Groups & Permissions,” Sep. 2024.

[4] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Lecture 06 Slide Presentation – ADDS,” Sep. 2024.

[5] Khoi Nguyen Pham, “TNE10005/TNE60002 - Network Administration Weekly Journal 2,” 2024.

[6] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Lecture 08 Slide Presentation – GPOs,” Sep. 2024.

[7] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Lecture 09 Slide Presentation – Security,” Oct. 2024.

[8] G. Fraser and J. da Silva, “Microsoft apologizes after thousands report new outage,” BBC News, 30-Jul-2024. [Online]. Available: https://www.bbc.com/news/articles/c903e793w74o.

[9] J. Ablett, “Clean Desk Policy in 2024: Benefits, How-To, Examples,” Adelia Risk, 02-Mar-2022. [Online]. Available: https://adeliarisk.com/clean-desk-policy/.

[10] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, “Endpoint detection & response: A malware identification solution,” in 2021 International Conference on Cyber Warfare and Security (ICCWS), Nov. 2021, pp. 1-8.

[11] S. W. Boyd and A. D. Keromytis, “SQLrand: Preventing SQL injection attacks,” in Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004. Proceedings 2, Springer Berlin Heidelberg, 2004, pp. 292-302.

[12] W. Murphy, "Access-Based Enumeration: Enhancing Security but at a Performance Cost," Microsoft TechCommunity, 2023. [Online]. Available: https://techcommunity.microsoft.com.