

TNE10005

Lab Class Journal

Trac Duc Anh Luong - 103488117

Table of contents	1
Week 1	3
Week 2	4
Week 3	5
Week 4	6
Week 5	7
Week 6	10
Week 7	12
Week 8	16
Week 9	17
Week 10	19
Week 11	20
Week 12	22
References	23

Week 1

This is the first week of the semester, in which we spent most of the class section introducing the subject. This week served as an orientation week and did not have any lab work to work on.

First, we go through the necessary details in terms of what the unit is, what we will learn, and the desired learning outcome for students. Dr. Ngoc showed us where to see the unit schedule in the unit outline, the unit structure, or the time allocation for each class session (2 hours of live lecture and 2 hours for practical class - the lab). We also got introduced to the teaching team, which includes Dr. Ngoc as the lecturer and Mr. Huy Anh as the tutor. There were also recommended reading materials presented, as well as how we can utilize the Ed discussion session to make questions and further discuss the materials and assignments that we get. For this unit, I find the slide quiz and revision quiz helpful, as I get to study each topic over and over with detailed implementation and how we utilize and remember the key knowledge.

For the knowledge obtained, we studied network devices. The main components of a computer are the CPU and the Input/Output devices. Some other sub-components are RAM, hard disk, flash, and the input/output controller. These components are then assembled to create end-user devices, such as personal computers/workstations, servers, and misc. The media player contains elements like copper, glass, and air, which lead to several problems, including attenuation, and interference/noise. Network devices include a repeater, hub (which is a multiport repeater), bridge, switch (which is a multiport bridge), router, and server. Protocols can be understood as a pre-set of rules that network devices use when transferring data.

The next topic is the OSI (Open Systems Interconnection) and CPT (Current Procedural Terminology) models. The OSI has 7 layers, which is best illustrated by the figure below.

TCP/IP MODEL	OSI MODEL
Application Layer	Application Layer
Transport Layer	Presentation Layer
Internet Layer	Session Layer
Network Access Layer	Transport Layer
	Network Layer
	Data Link Layer
	Physical Layer

The TCP/IP model contains 4 layers, from 4 to 1, which are Application, Transport, Internet, and Network Access respectively. The TCP/IP model is a concise version of the OSI model, which is why there is close relevance between the 2 models.

Finally, we took a look at the number systems in IT, which is a binary number system of 1 and 0 for on and off protocols. We were also taught how to convert from decimal to binary, which was crucial to calculate IP addresses and subnet masks later in the course.

Week 2

Challenges appeared right in the first lab of the course, as we were required to install many components and large files to create virtual machines. Firstly, we needed to view our computer's configuration to see if it was compatible with the requirements of this unit. To create virtual machines, we need the Hyper-V Manager software, which is only available on Windows machines with the Pro version of windows. Luckily, we found a video tutorial on YouTube that showed us how we can enable the Hyper-V manager on Windows home with a simple bat script ([link](#)). After that, we need to download the disk image files (.iso) from the Azure Dev Tools for Teaching website. After choosing the directories for our virtual machines, we followed the remaining steps instructed in the lab material. We get to work with the Command Prompt to view the IP address and settings.

The step that I struggled with the most is Testing the network. First, we need to config the network by changing the properties of the IPv4 on both of the machines (sWin10PC203 and WindowsServer2016XX). This is a crucial step as it determines if you can later ping the Windows Server using the Windows 10 virtual machine. The 2 machines also have to be connected to a private switch, which we created in the Hyper-V Manager (in the Virtual Switch Manager) settings and named NetAdLab1SwitchXX as instructed. Initially, I failed to ping the Windows Server machine since I forgot to configure the Windows 10 machine like the topology given by our lecturer. After fixing that minor mistake, I got the lab to work as needed.

The lab was a clear demonstration of the lecture, which covered network addressing and an introduction to project management. There are 4 topologies for network addressing, which are bus topology, star topology, ring topology, and fully meshed topology - which is considered the safest and most significant redundancy and is being used in many network settings in buildings across the world. We also covered which layer our network operated at, and took a closer look at IP addresses and subnet masks. The addressing rules were initially quite confusing, but the lab showed us the IP configuration in a private network, which was helpful.

Project management was an area that we had to know of, as it satisfied the needs of the current IT job market state. Project managers are paid more, but that comes with strict requirements. Seniors IT professionals with years of experience and soft skills like communication, people management, management skills, and understanding of technology tend to become project managers. Different areas for management like integration, time, scope, and cost were also examined.

Week 3

This week we looked closely at project management and the TCP/IP model. Apart from the aforementioned areas for management, some other areas include quality, human, communications, risk, procure, and stakeholder management. The continuum of project life cycles includes agile, iterative, and hybrid-based projects. The lecture was intriguing as we had the chance to examine how each area can be applied in real life via both successful and unsuccessful examples. Dr. Ngoc later instructed us to form groups and start working on the task of designing our household network, which was related to the lecture, particularly in the IPv4 Addressing session. It was based on a binary session, which had logical constraints for subnet and multicast purposes. We use subnets to reduce network congestion, increase security, and reuse a single network address across multiple locations.

For the lab, we worked on a simple project on Microsoft Project 2019. The class had some difficulties in installing and using the software online via the Citrix workplace as instructed by the lab materials. However, I figured out the best way to do the lab was to download the software from Microsoft Azure Education and work on my local machine. This way, I was not prone to any software trouble like crashes or misclicks, while getting to save a copy of the project on my local machine.

Some of the main steps for the lab include: creating a breakdown structure, creating a Gantt chart, determining the critical path, managing resources and costs, and assigning resources.

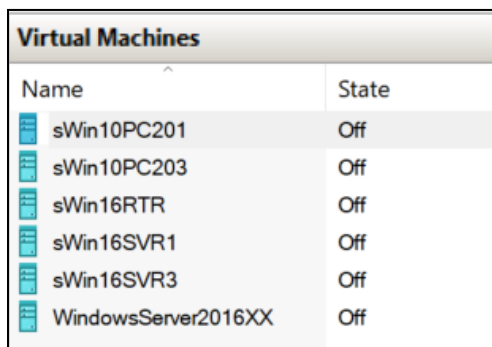
- First, I created a work breakdown structure by entering the task name and making a list of new tasks.
 - Each subtask could be marked with the right arrow button, or the critical combination of Alt + Shift + Right. Using this, we create a tree structure of tasks for easier management.
 - We outlined the task number on the adjacent left column, with 1 being the main task and 1.1 being the subtask (and so on).
 - Then, we entered the duration for each task, which consisted of hours or days.
- Second, we created a Gantt chart. The task was familiar as we had already covered this in the Problem solving with the ICT unit.
- After that, we determined the lead time, lag time, and critical path, as well as managed resources and costs.

Because it gives projects direction and leadership, project management is crucial. In other words, the goal of project management is to effectively plan and oversee a project such that its stated objectives and deliverables are met. It entails assessing and controlling risks, prudent resource allocation, astute budgeting, and open communication between various teams and stakeholders.

Week 4

In week 4, we did lab 3, which from my perspective is one of the most challenging labs so far. The lab was an introduction to IPv4 addressing and contained numerous tasks that required us to configure the IPv4 addresses and observe the purpose of the default gateway and subnet mask.

The preliminary settings instructed us to download and launch 4 additional virtual machines, including 3 windows server 2016 machines and a windows 10 machine. Creating these machines manually one by one can be time-consuming, therefore I came up with the method to export these machines into a folder, duplicate them and rename them as the lab instructed.



Virtual Machines	
Name	State
sWin10PC201	Off
sWin10PC203	Off
sWin16RTR	Off
sWin16SVR1	Off
sWin16SVR3	Off
WindowsServer2016XX	Off

Once the machines had been created, we turned them on one by one to configure the IP address via the control panel, which we used to do in lab 1. The topology was at first confusing, as I did not know how to turn the sWin16RTR machine into a router for our 3 remote switches. After some consultation, it returned to the Hyper-V manager, went to the settings of sWin16RTR, and added new network adapters that corresponded to the topology given. The default name for our Ethernet connections were 0, 1, and 2, which were later renamed to the switch for easy configurations and management.

Once the IP addresses had been set to the topology, pinging the Windows Server machines was an easy and approachable task. However, we did need to note that the firewall for VR3 had to be turned off to ping the machine successfully, otherwise only the allow files and printer sharing option in the panel would not work.

To get more practice with the subnet mask, we saw an illustration of how the destination MAC address was selected and used. As the source and destination of Frame 1 and 2, the MAC address changed first, with both the Source and Destination address staying the same.

SVR1 could ping the RTR but not PC201 because RTR is the router, which allowed communication between subnet masks. However, the subnet address for PC201 had changed. sWin16SVR1 and sWin16RTR(E0) could successfully ping, but they had different subnet masks because we had changed the host IP address.

Week 5

In week 5, we did lab 4, which was primarily related to the content of DHCP. The lab aimed to install and configure DHCP attributes, such as scopes, exclusions, reservations, options, and even an extension of high availability. The virtual machines required to execute this lab were sWin16DC1, a server of sWin16SVR1, and sWin10CL101.

We first launched the machines mentioned above and opened Powershell in CL101. We needed to start Powershell in admin mode. You would find the reason in the next step. At the prompt we typed the command “**Set-NetIPInterface –InterfaceAlias Ethernet –dhcp enabled**” and waited for the IP address, subnet mask, and default gateway, to be re-configured. This is a private IPv4 address.

```
PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-7FSON5P
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address. . . . . : 00-15-5D-38-01-1F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.219.7(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 83891549
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-D7-CF-D6-00-15-5D-38-01-1F
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

After that, we needed to install DHCP on SVR1 via “**Add Roles and Features**”. After downloading, some post-deployment configurations were needed. We could click on the flag next to Manage and Tools on the menu bar in the server manager. As SVR1 is a domain, we had to authorize our new DHCP server via a domain controller. The user account that could be used to carry out this action is the domain administrator. On the post-configuration page, we accepted the default section and committed.

Next, we were instructed to create a scope. DHCP served the purpose of allocating IP addresses automatically, however, those addresses still needed to be configured. We could select DHCP in the server manager window and click on the server name (in this case, SVR1) to expand the containers including IPv4 and IPv6 to create a new scope. As this unit mainly focused on IPv4 and related contents, we will choose IPv4. The new scope was named Hawthorn with a description so that it could be easier to manage, retrieve, and authorize. The IP address range was set to the requirements. After configuration, to ensure the server DC1 would not lease out any IP addresses, we needed to stop its service. The addresses prompted after we had entered **ipconfig /renew** are within the scope we had just configured.

```

PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6
    IPv4 Address. . . . . : 172.16.32.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

```

There will come times when we need to remove specific addresses from a Scope's pool. To do this we expanded the Hawthorn scope in the DHCP management window, right-clicked on the address pool, and chose New Exclusion Range. Before testing, we need to release the previous IP address by using the command "**ipconfig /release**" and "**/renew**". The output is shown below:

```

PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6
    IPv4 Address. . . . . : 172.16.32.160
    Subnet Mask . . . . . : 255.255.255.0

```

As we can see, the IPv4 addresses had changed.

To create new reservations, we could expand the scope of our domain and click on Reservations. Here, choose new reservations and enter a specific IP address.

The physical address was: 00-15-5D-38-01-1F

```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Microsoft Hyper-V Network Adapter
    Physical Address. . . . . : 00-15-5D-38-01-1F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6(Preferred)
    IPv4 Address. . . . . : 172.16.32.160(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Wednesday, October 19, 2022 11:22:54 AM
    Lease Expires . . . . . : Thursday, October 27, 2022 11:22:53 AM
    Default Gateway . . . . . : 
    DHCP Server . . . . . : 172.16.32.11
    DHCPv6 IAID . . . . . : 83891549
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-D7-CF-D6-00-15-5D-38-01-1F
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           : fec0:0:0:ffff::2%1
                           : fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

```

My address after renewing the IP configuration was

```

PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6
    IPv4 Address. . . . . : 172.16.32.199
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

```

Therefore, the IPv4 addresses have once again changed.

To communicate with devices outside of their subnet mask, a device needs a default gateway. We can access the server option and configure it to 003 as a router. The new address is 172.16.32.2. To clarify, we return to CL101 and record our new IP addresses after releasing and renewing:

```
C:\Users\Jack>ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : NetAdmin.edu
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6
    IPv4 Address. . . . . : 172.16.32.199
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.32.2
```

We once again configure the 003 router option to the 015 DNS domain name and add ScopeSetDNS.com

```
C:\Users\Jack>ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : ScopeSetDNS.com
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6
    IPv4 Address. . . . . : 172.16.32.199
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.32.1
```

We can see that the default gateway has changed but IP and subnet stay the same.

The option precedence calls us to add a new hostname as screenshotted below:

```
C:\Users\Jack>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-7F50N5P
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : ResSetDNS.com

Ethernet adapter Ethernet:

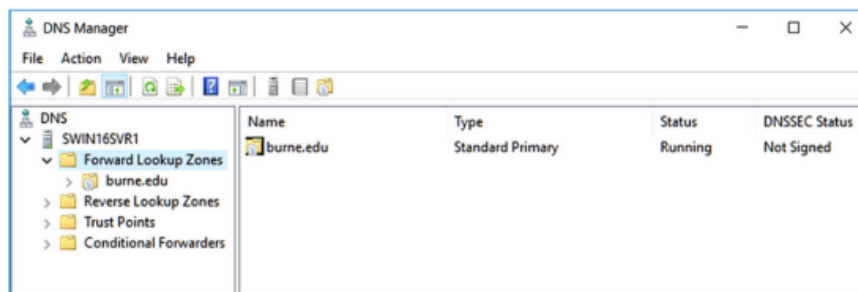
    Connection-specific DNS Suffix  . : ResSetDNS.com
    Description . . . . . : Microsoft Hyper-V Network Adapter
    Physical Address. . . . . : 00-15-5D-38-01-1F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::b088:fa13:c75e:db07%6(Preferred)
    IPv4 Address. . . . . : 172.16.32.199(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, October 20, 2022 12:21:31 AM
    Lease Expires . . . . . : Friday, October 28, 2022 12:21:31 AM
    Default Gateway . . . . . : 172.16.32.1
    DHCP Server . . . . . : 172.16.32.11
    DHCPv6 IAID . . . . . : 83891549
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-D7-CF-D6-00-15-5D-38-01-1F
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled
```

Week 6

In week 6, in addition to the network admin test 1, we also do lab 5, which is a detailed introduction to DNS. The lab aims to get to know what DNS is used for, as well as the installation process and configure zones, records, and zone transfers. The virtual machines needed for this lab are sWin16DC1, sWin16SVR1, sWin16SVR3, and sWin10PC203.

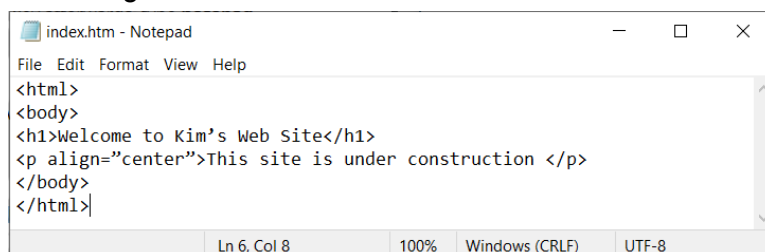
Similar to lab 4, we open the Add Roles and Features wizard to install new roles, in this case, DNS Server, with default settings. Once we have successfully installed DNS, we can move to the next section of creating a lookup zone.

In this section, we will create a forward lookup zone. Expand SVR1 and click on the forward lookup zone. We will create a zone named burne.edu and finish the setup. The new primary zone should look something like this:



In the next section, we will practice how to directly share resources (files) in the File Explorer application. The new data is shared via the properties settings in the Properties context menu.

In the following session, we learn how to share web pages via a server eternally. To do this, we need to save an index.htm file in the **C:\inetpub\wwwroot** folder. The content of the file looks something like this:



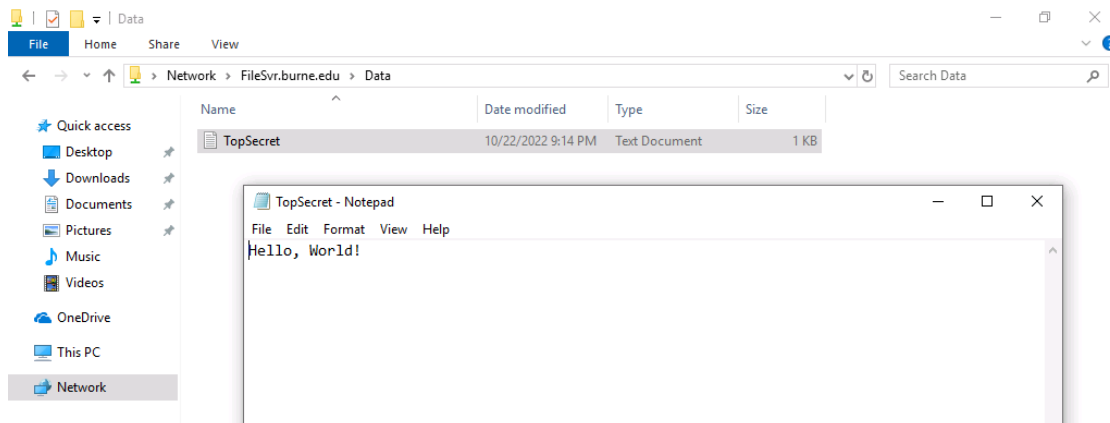
(remember to run Notepad in admin mode or else Windows would not allow us to save a file in this particular folder)

To view the file, we need to create DNS records, which is also the content of the next part. We need to create a new host for the burne.edu zone and add the name field www. To create a file server, we also create an alias by creating a CNAME record that points to burne.edu. We do need to note that we should enter the command **ipconfig /flushdns** on the client pc, in this case, PC203 to clear the DNS cache.

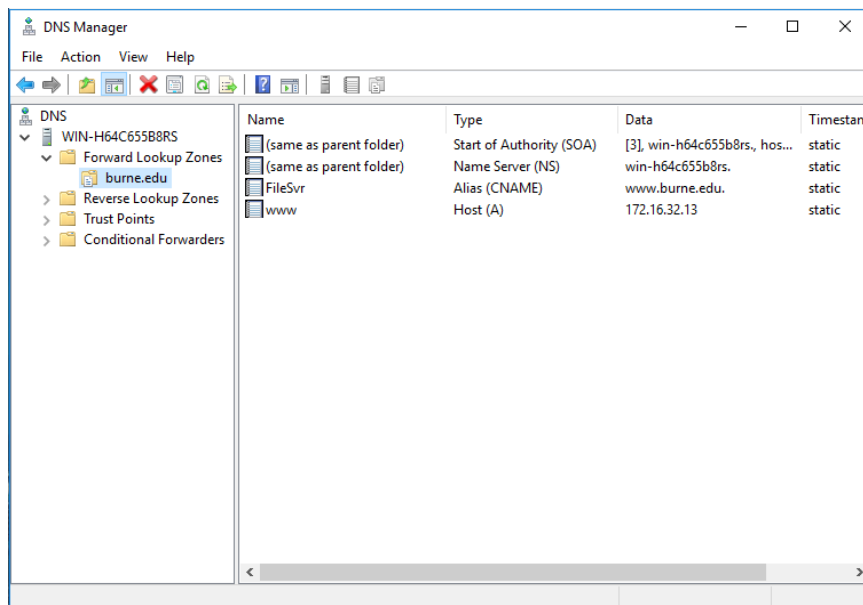
For testing, we need to log in to PC203 as Admin. After setting the IPv4 address to the SVR1 preferred DNS server, we can open a browser (Edge) and type in www.burne.edu, this will direct us to the web page that we have just created.



Enter the file server name as the File Explorer and we will get:



The last part of the lab is zone transfers. Here we will create a secondary zone and enter the SVR1 IP address. For security measurement, the zone will not be automatically loaded. Instead, we will need to approve and configure settings before data can be accessed. After refresh, burne.edu should load:



Week 7

This week, we do lab 6, which is about the configuration of a windows server domain. The goal of the lab is to practice domain-related materials and skills. First, we will use sWin16SVR3 as our server and install ADDS (Active Directory Domain Service). Next, we will use a client PC, which is sWinPC203 to join the server. In the following steps, we will create domain user, computer, and group accounts, as well as how to access and secure those accounts using sharing permissions, which include read-only, read and write, and full control.

First, to create a domain, we need to add the “Active Directory Domain Services” roles via the “Add Roles and Features” settings in the Server Manager. Next, we promote it to be a server and restart the SVR3 machine. After that, we can create some resources (data folders) to access from accounts created.

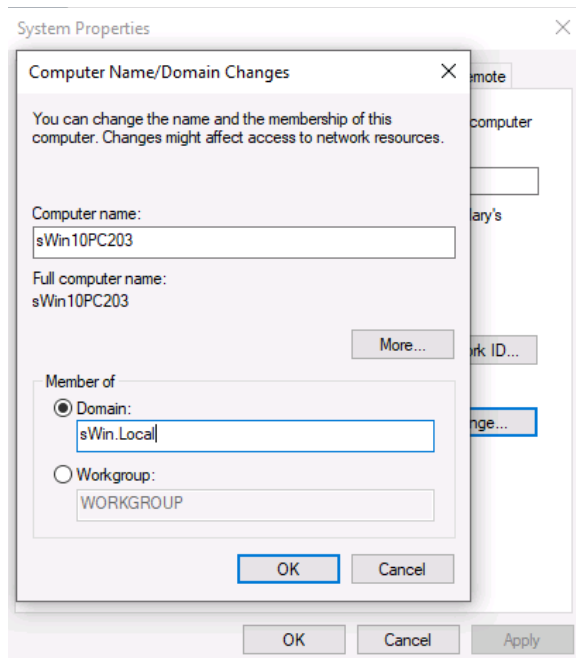
```
C:\> Command Prompt

C:\Users\Jack>ping sWin.Local

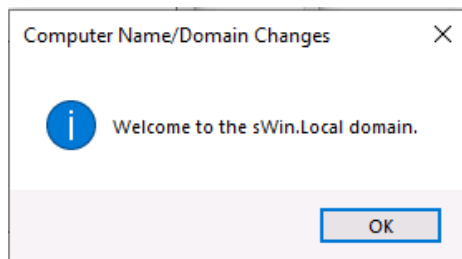
Pinging sWin.Local [192.168.100.13] with 32 bytes of data:
Reply from 192.168.100.13: bytes=32 time<1ms TTL=128
Reply from 192.168.100.13: bytes=32 time=1ms TTL=128
Reply from 192.168.100.13: bytes=32 time<1ms TTL=128
Reply from 192.168.100.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

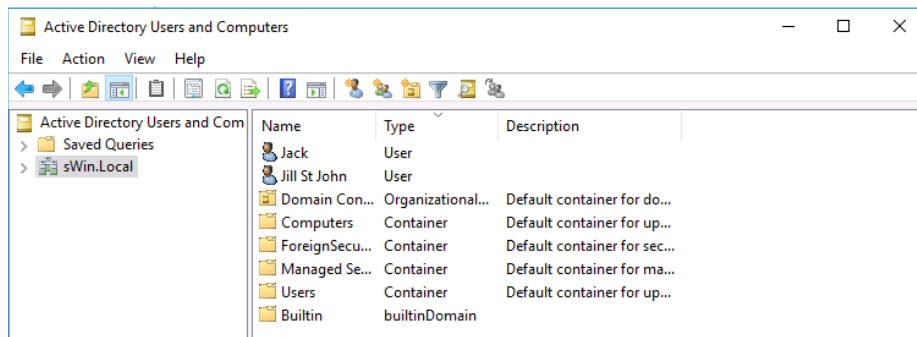
To join a domain, we switch to the client PC (PC203). We need to ensure that the IPv4 settings, including the IP address, subnet mask, and most importantly - the DNS are set correctly to the topology, otherwise, you cannot join the domain. Then, we access the advanced system settings to join the sWin.local domain and press ok.



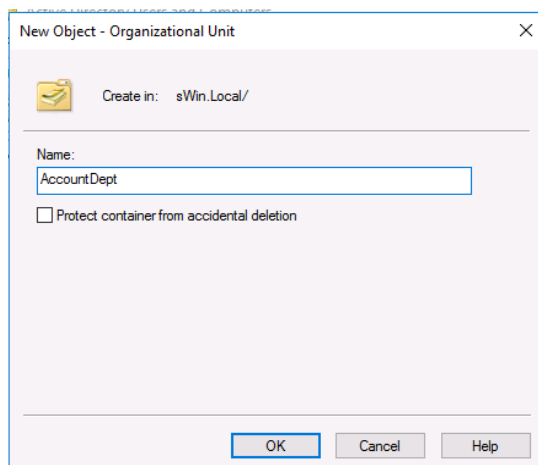
The computer should prompt a welcome screen and automatically restart the machine.



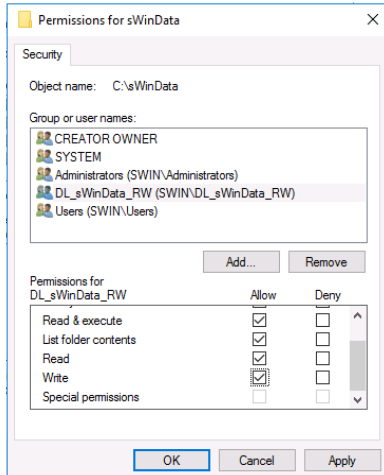
Next, we will learn how to create accounts. Normally if we log in to the client's PC using a local account, we can only access resources stored on that computer. However, if we log in to accounts created by ADDS, we can access the resources shared with the server via our permissions. Repeating the steps mentioned in the lab will create a new user account named Jack.



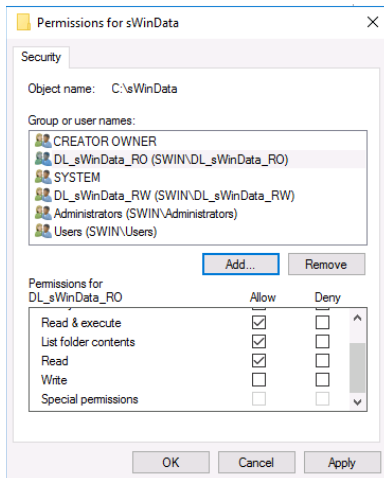
For the next step, we will create an OU, which stores the accounts and is an important step for the Skills Assessment.



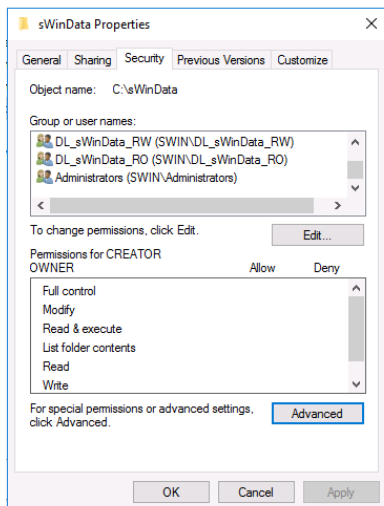
For the next step, we will create group accounts and assign permissions, including read, write, and full access to the resource created.



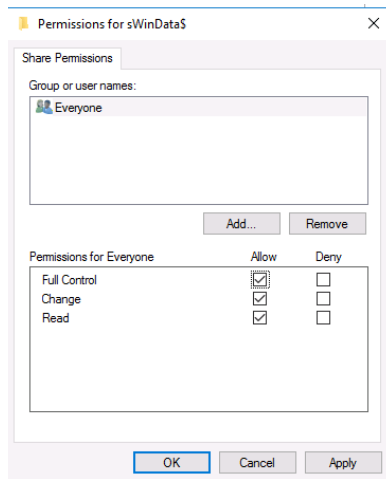
After adding the users, the permissions tab should look like this:



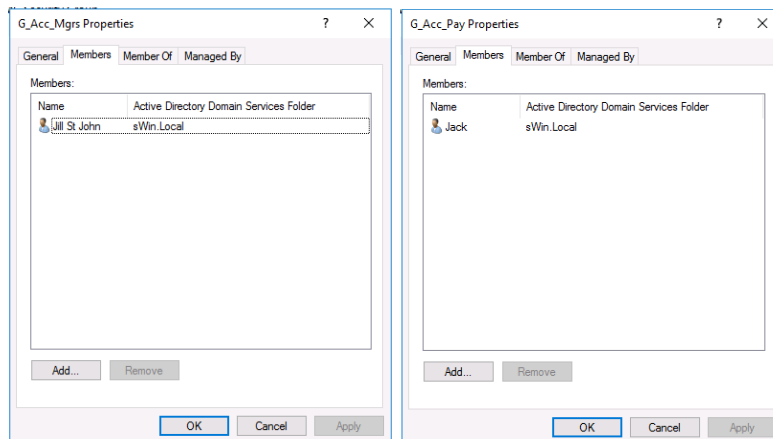
Another step is to remove inheritance so that there are no more User groups, making the resources protected against local unauthorized accounts.



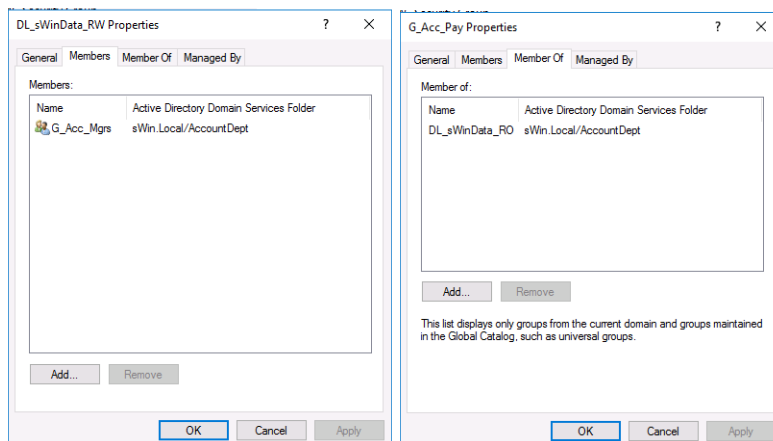
The first step to assigning permissions is to allow everyone = full control, then we can set individual groups later.



After adding Jack and Jill to their respective groups, here are what we will be ended with:



For the domain local, we should add G_Acc_Mgrs to the SWinData_RW



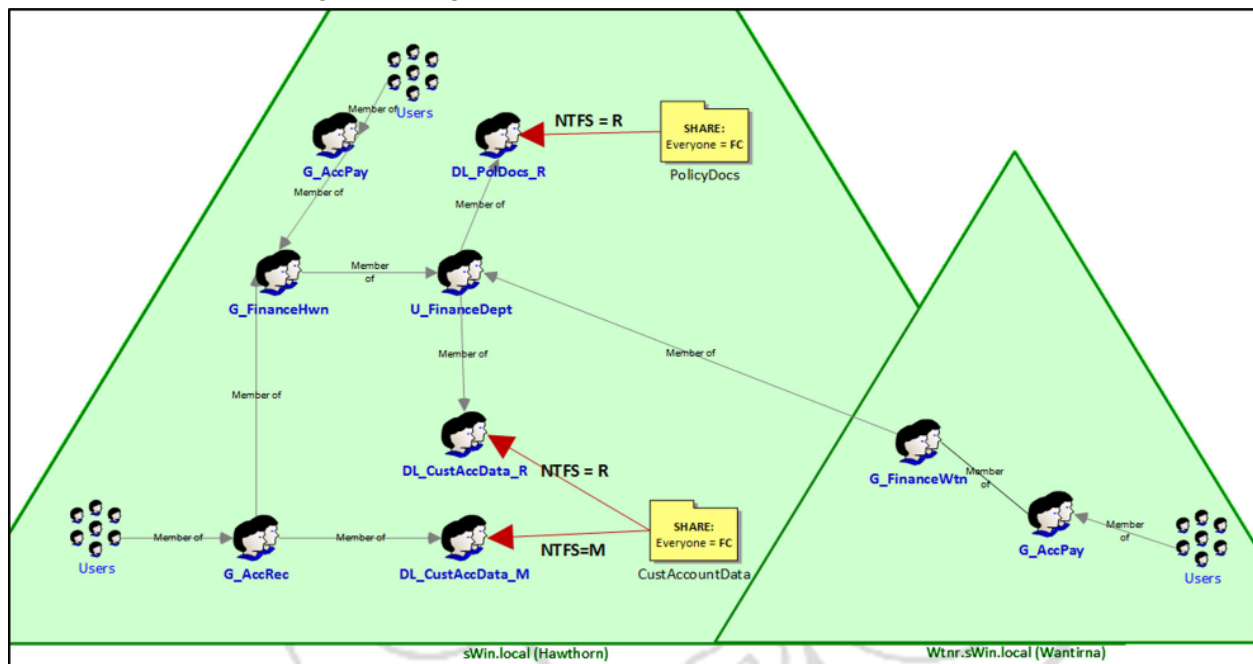
Week 8

This week, we do lab 7, which is challenging since it requires up to 6 virtual machines to be up and running at the same time, taking up a lot of resources from our computers. The machines needed are a domain controller (DC1), a router (RTR), 2 servers (SVR2 and SVR3), and 2 client PCs (CL101 and PC203).

The first step of the lab is to create a child domain. Before that, we need to log into SVR3, open the command prompt, and type “**ping sWin.Local**”. If there is a response, we can ensure that the DNS server address has been configured correctly with the topology. After adding ADDS, we need to add sWin.Local\Administrator as a new username.

Next, we need to create a delegation in the DNS Options windows and install it to promote SVR3 to become the main DC in the child domain.

For the group strategy, we need to create similar users, user groups, domain local entities, and resources similar to the given design:



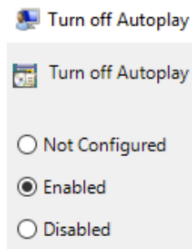
Next, we create the necessary folders in the C drive and share permission with Everyone with Full Control. In the following step, we need to create an OU named “Finance” and add a group with global scope and security type. This process will be repeated 6 times until we have created all necessary entities. The account template is essentially a temporary account that holds attributes like logon scripts, hours, password settings, etc.

The next part teaches us how to create new users, and groups, and join domains using PowerShell. This is useful as it is time-efficient and easier than doing those extra steps with the Graphical User Interface.

Week 9

In week 9, we do lab 8, in which the content focuses on group policies on a windows server domain. The main goal is to strengthen our understanding of how to set up and develop group policies with multiple accounts in the domain. For this lab, we use a domain controller (DC1), a Windows Server (SVR1), and a client PC (PC201).

For the first part, we will use the Microsoft Common Console Document to edit the local group policy and turn off the autoplay section.



Then, we will forbid access to the control panel in the user configuration part of the pgedit. After our settings have been enabled, we should be able to successfully launch it.

We will also want to remove the task manager option once we click Ctrl+Alt+Del. To do this, we simply go to the local group policy editor windows and remove the lock computer option in the settings.

The next step is to create an OU. This step has been done in the 2 previous labs, giving us beforehand experience. After creating the OU and child OU, we need to create a delegate to manage the account passwords and groups in the Support OU.

For the next step, we need to create a custom console by selecting the console root window. After that, we shall be able to advance to creating objects that belong to a group policy. Many GPO settings can only be turned on or off when configured, like light switches. Similar to a light switch, if one person enters a room and turns on the light, the next person enters and turns the light off, and the third person switches it on when they enter, the light will constantly be on or off depending on who last flicked the switch. The same applies to GPOs. The basic rule is that when GPOs disagree over a setting, the most recent GPO applied will control the setting, albeit an administrator may have some tricks up their sleeves to override this.

The GPOUpdate section introduces us to the reboot process of computer configuration settings. To modify the GPU update, we can use some of the following commands in the shell prompt:

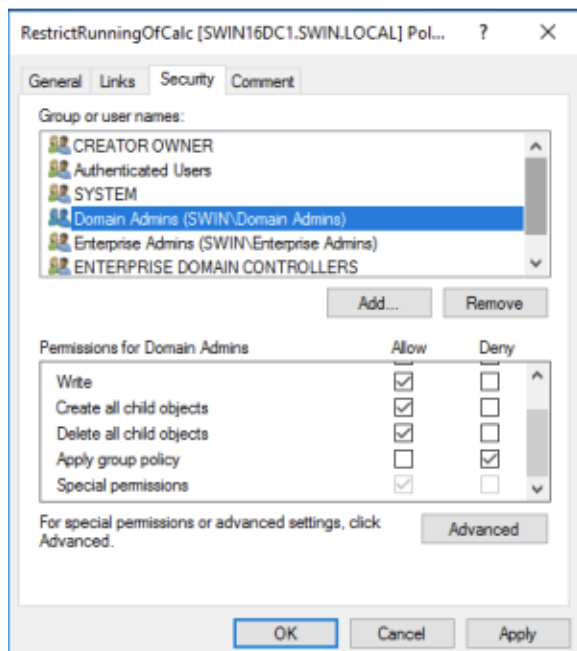
We can modify **gpupdate** by using the following switches:

gpupdate /force - Will apply all GPO settings both user and computer configurations whether they have changed or not.

gpupdate /target:user - Will apply all of the user configuration settings, the word user can be substituted with computer to apply all of the computer configuration settings.

gpupdate /boot - Will cause the PC to reboot after the GPO has been applied

The next part mainly focuses on linking GPOs to domains and containers. We can also link multiple GPOs to one single container to see if conflicts happen. WMI filtering allows us to use the Group Policy Management MMC snap-in to build and add WMI filters to the GPO to guarantee that each GPO connected with a group can only be applied to gadgets running the right version of Windows. Although each GPO can have a unique membership group, you would then need to oversee who belongs to each group. Instead, utilize only one membership group, and let WMI filters take care of applying the right GPO to each device automatically.

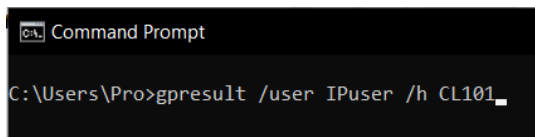


Week 10

In week 10, we will practice an interesting topic, which is managing security in the user active directory. The purpose of this lab is for students to get a better grasp of the security procedures in a Windows server domain. The virtual machines used for these labs are a domain controller (DC1) and a client PC (CL101).

For the preliminary settings, we need to reconfigure some of the last lab's work and ensure that the 2 machines are connected to the same virtual switch (Hawthorn).

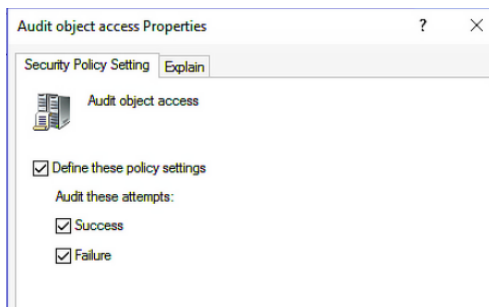
Next, we have to config the account policies and password policies on the server machine. You might recall that throughout the presentation we discussed the importance of having two user accounts for each administrator. A privileged account that administrators use to launch applications with enhanced access and an unprivileged account for logging on. In the following part, run as will be used. This is how you run an application with administrative rights. To generate a report on the GPO settings, we may use the command:



```
Command Prompt
C:\Users\Pro>gpresult /user IPuser /h CL101
```

After the command has been executed, an htm file will be reported, which we can open via Edge or Internet Explorer.

The following part of the lab is restricting groups, which is essentially a policy that allows the admin to curb the influence of membership or groups such as the Admin group. The part also contains auditing, where an administrator can keep track of events like who logs onto the network and who accesses crucial files. The event viewer console can be used to get these records.



Next, the encrypted file system is introduced. This is one of the most interesting parts as we learn the encryption of files and this can be linked to hackers and phishing where they attack your computers by encrypting your files and resources. In addition to that, the use of GPO is also highlighted as it is paired with the WSUS settings and Firewall. Finally, we practiced some good measurements on how to become an analyzer or Security Manager.

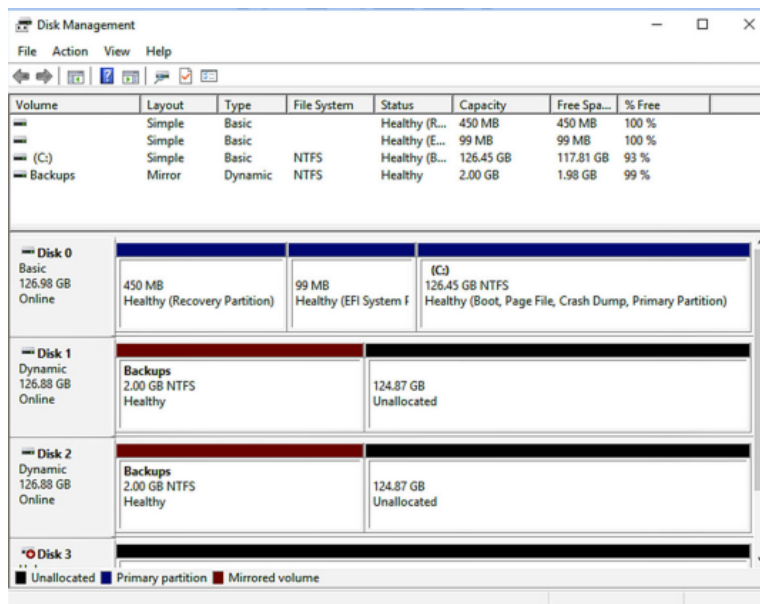
Week 11

In week 11, we would do lab 10, which was the last lab, and also did the Practice Skills Assessment 1. For the Skills Assessment, I find Part A and B quite comprehensible and could do it well with accuracy. Even though my methods for calculating the IPv4 settings were somewhat different from the given answer, the results were the same. It is Part C when it gets challenging as there are so many steps to configure the domain, and domain local groups with such a short window of time. Luckily, a peer in my class did a video tutorial on doing parts C and D, which helped us a lot in correcting our assessments and making them time-efficient.

For lab 10, we practiced using disaster recovery in a Windows Server domain to manage risks and improve quality. The goal of the lab was for students to get a more comprehensive perspective on volume redundancy, enumeration, backup, service recovery, and how we can monitor performance. The 3 virtual machines that we would be using were a domain controller (DC1), a Windows server (SVR1), and a client PC (CL101)

The first part is to use disk management to configure volume redundancy. Windows Disk Management system software gives you the ability to carry out sophisticated storage functions. Here are some applications for disk management:

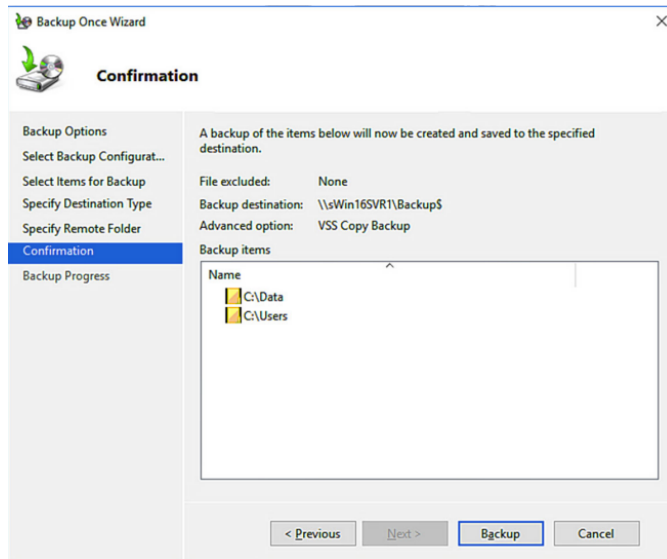
- Initializing a new drive can be used to set up a new drive.
- See Expand a basic volume to extend a volume into space that isn't already occupied by a volume on the same drive.
- See Shrink a basic volume for information on how to shrink a partition, usually so you can extend an adjacent partition.
- See Change a drive letter for information on how to modify or assign a new drive letter.



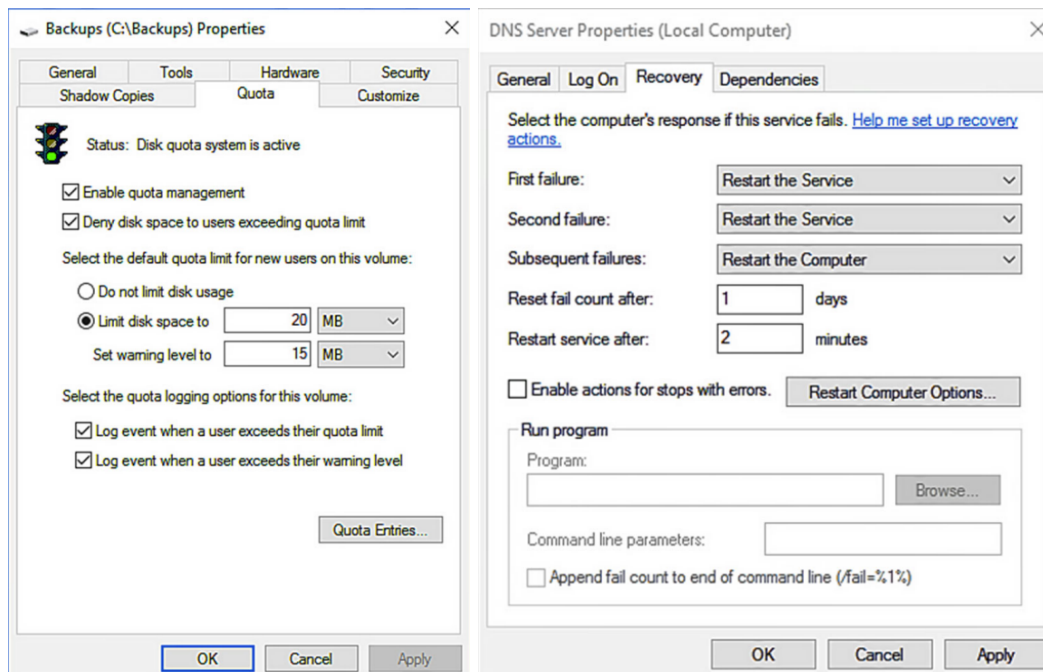
And to answer the question of why we use the dollar sign in the share name, that is because any network searchers are unable to find the share, making it hidden and secured.

Next, we learned about shadow copies. A shadow copy is a snapshot of a volume that duplicates every piece of information stored there at a specific point in time. Each shadow copy is assigned a persistent GUID by VSS.

Files and folders that users do not have the authorization to access are hidden via access-based enumeration. For DFS namespaces, this feature is not by default turned on. Using DFS Management, you can enable access-based enumeration of DFS folders. You must use Share and Storage Management to enable access-based enumeration on each shared folder to manage access-based enumeration of files and folders in folder targets.



The final sections were about installing a server backup and configuring NTFS Quotas, Service Recovery, and Counter Logs.



Week 12

There was no lab in web 12 but we did the Practice Theory Assessment and Practice Skills Assessment 2. This was crucial as it gave us some detailed practice on how we can perform in our final exam. For the theory part, it was manageable. However, I still needed some practice on the Design Quiz. The skills section was somewhat similar to the one we had in week 11, therefore it was also manageable by many students.

References

Tanenbaum, AS & Wetherall, D 2014, Computer networks, Pearson India Education Services Pvt, Limited, India, viewed 8 October 2022,

<<https://www.mbit.edu.in/wp-content/uploads/2020/05/Computer-Networks-5th-Edition.pdf>>.

Schwalbe, K 2015, Introduction to project management, 5th edn, Schwalbe Publishing, Minneapolis, Mn.

paolomatarazzo 2022, 'Create WMI Filters for the GPO (Windows)', learn.microsoft.com, viewed 3 December 2022,

<<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-wmi-filters-for-the-gpo>>.

JasonGerend 2021, 'Overview of Disk Management', learn.microsoft.com, viewed 3 December 2022,

<<https://learn.microsoft.com/en-us/windows-server/storage/disk-management/overview-of-disk-management>>.

JasonGerend 2021, 'Enable Access-based Enumeration on a Namespace', learn.microsoft.com, viewed 3 December 2022,

<<https://learn.microsoft.com/en-us/windows-server/storage/dfs-namespaces/enable-access-based-enumeration-on-a-namespace>>.

GrantMeStrength 2021, 'Shadow Copies and Shadow Copy Sets - Win32 apps', learn.microsoft.com, viewed 3 December 2022,

<<https://learn.microsoft.com/en-us/windows/win32/vss/shadow-copies-and-shadow-copy-sets>>.