LAB JOURNAL

Network Administration

Abstract

This document serves as a lab journal for the Network Administration unit, documenting the weekly activities conducted within the lab sessions. The labs within this unit primarily delve into topics such as Active Directory, Windows Server Administration, and Group Policy Object. It covers key concepts, configurations, commands, and further study pertinent to each lab exercise.

Jade Hoang

Swinburne University of Technology

Table of Contents

Lab 01: Introduction to Network Administration lab

Key concepts

Hyper-V is a Microsoft virtualisation platform that allows hosting multiple virtual machines (VMs) on a single physical machine. It optimises hardware utilisation, reduces costs, and requires fewer physical servers, space, power, and setup work. A hypervisor manages hardware resources for each VM, enabling them to run independently. The host machine is the physical server, while the VMs are referred to as guests or virtual machines. It is best practice to revert all required VMs to "Starting Image" checkpoint at the start and end of each lab so that the VMs have the correct settings and configurations.

Key configurations and commands

Key steps	**Details**	**Notes**
Create virtual switches	*Create a virtual switch:* • Hyper V Manager, under Actions -> Virtual Switch Manager • "Create Virtual Switch" -> Add "Name" and "Notes". • "Connection type" -> "Private network" -> OK *Remove virtual switch:* • "Virtual Switch Manager", click on virtual switch, then "Remove".	
Change VM's network adapter	*Connect to a different virtual switch:* • Click on the VM, Settings, under "Hardware", select Network Adapter. • "Virtual switch:" -> choose the virtual switch -> OK.	
Launch VM	• Revert VM to "StartingImage" checkpoint. • Right-click VM -> "Start." -> Connect. • Enter password "**Pa55w.rd**"	
Shutdown VM	Right-click Win key -> Shutdown/Sign out -> Shutdown -> Continue	
Configure IP settings	*Verify IP settings:* • Start, Run, "cmd" -> "**ipconfig**" *Configure IP settings (for server only):* "Server Manager" -> "Local Server" -> "Properties" -> "Ethernet", "Network Connections" -> right click "Ethernet" -> "Properties" -> "Internet Protocol Version 4 (TCP/IPv4)" -> Properties button	

Revert VM to its previous (latest) checkpoint	Hyper-V manager -> right-click VM -> Revert -> Revert Virtual Machine -> Revert button *Apply checkpoint "Starting Image" to VM:* • Right-click "Starting Image" checkpoint -> Apply (in Actions pane) -> "Apply Checkpoint" -> Apply	

Further study

There are two types of hypervisors in virtualisation: type 1 ("bare metal") and type 2 ("hosted hypervisor"). Type 1 hypervisor runs directly on top of the hardware and is used mainly in data centre environments. Examples of type 1 hypervisors include VMware ESXi and Microsoft Hyper-V. Type 2 hypervisors run as a program or software on an operating system like a regular computer program (Bigelow & Kirsch 2021). Examples include VMware Workstation and Oracle VirtualBox. Although type 2 hypervisor is not common in data centres, it is commonly used on personal devices such as a MAC user who wants to run an application that is only supported on Windows.

Lab 02: Getting Familiar with Network Administration Labs

Key concepts

I examined VM communication within and across different switches and observed DHCP IP address assignment. To enable device communication within a network, layer 2 devices (such as switches) are used, while layer 3 devices (such as routers) are required for inter-network communication. Correct IP settings must also be configured for communication to occur.

I also learned about three types of virtual switches in Hyper-V:

- **Private**: allows communication only between guest VMs on the same host machine.
- **Internal**: allows communication between guest VMs on the same host machine and the host machine itself.
- **External**: allows communication between guest VMs and the physical network to which the Hyper-V host machine is connected.

Key configurations and commands

Key steps	**Details**	**Notes**
Verify communication between 2 devices	Cmd.exe, type: **ping <IPv4 address>**	
Connect a VM to a different virtual switch	• Hyper-V Manager, right-click VM -> Settings • Under Hardware, select "Network Adapter" -> pull down Virtual Switch and select desired switch	
Verify IP configurations including DHCP information	• Command Prompt, type "**ipconfig /all**" • Output: "DHCP enabled: No" -> IP address is manually configured. • "DHCP enabled: Yes" -> device obtains an IP address and related settings automatically from the DHCP server	**ipconfig /all** output displays DHCP server IP address, current client IP address, lease obtained, and expiration.
Configure VM to obtain IP settings from DHCP server	• Right-click Win key, Windows PowerShell (Admin). • **Netsh interface ip set address Ethernet dhcp**	Changing IP configuration requires admin rights.

Further study

Ethernet frame encapsulates the packet with a header and trailer. The size of the Ethernet header is typically 14 bytes, and the trailer is 4 bytes long. This makes up 18 bytes in total for both the Ethernet header and trailer. According to Lee (2014), "*Ethernet has a minimum frame size of 64 bytes, comprising an 18-byte header and a payload of 46 bytes. It also has a maximum frame size of 1518 bytes; in which case, the payload is 1500 bytes.*" The frame size is determined by the Type/length field of the header.

Lab 03: IPv4 & Subnetting

Key concepts

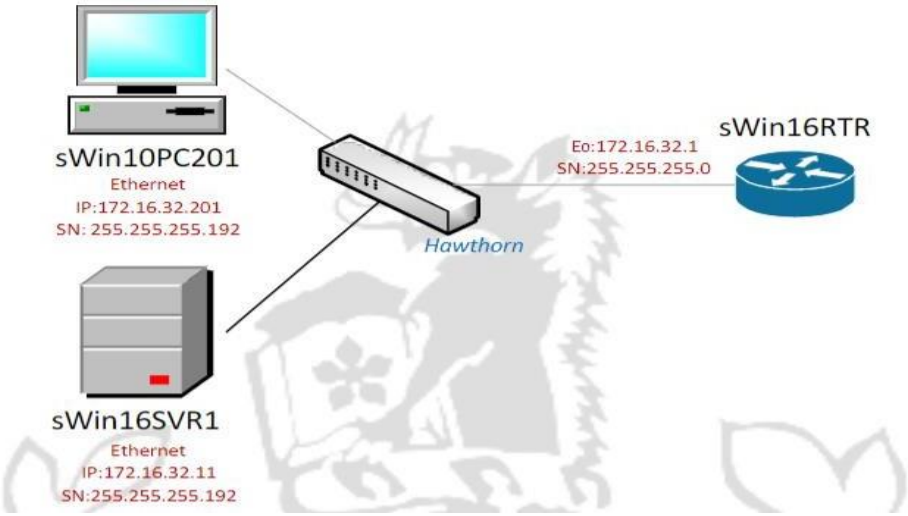
Today, I learned about IPv4 addresses, default gateway and subnet mask. Here are the main points:

- Default gateway address enables communication between devices in different subnets. Meanwhile, subnet mask determines the network and host portions of an IP address.
- Correctly configured IP address and subnet mask are sufficient for communication within the same subnet.
- Subnet mask is used to determine whether to use destination device or default gateway's MAC address as Layer 2 frame's destination address.
- Subnet masks are not exchanged between devices. Each device only knows its own subnet mask which it uses to calculate network address of the destination device.

Key configurations and commands

Key steps	**Details**	**Notes**
View network adapter	• File Explorer, right-click Network, Properties. • Network and Sharing Center -> Ethernet link -> double-click to Properties -> double-click Internet Protocol Version 4 (TCP/IPv4)	Can also type **ncpa.cpl** in cmd.
Configure default gateway	• Repeat “view adapter configuration” steps above. • Under **Internet Protocol Version 4 (TCP/IPv4) properties**, type IP address of the default gateway -> OK	
Display ARP table	• Load Windows PowerShell (Admin) • Type **arp -a**	Successful pings result in new entries being added to the ARP table with corresponding IP and MAC addresses.
Clear ARP cache	• Load Windows PowerShell (Admin) • Type **arp -d**	
Fixing revert VM error	• Hyper-V Manager, Actions pane, Stop Service • In Stop Virtual Machine Management Service, click Turn Off • After service stopped, click Start Service	Perform this if errors occurred when starting a VM, reverting a VM, or applying checkpoint Starting Image to a VM

Further study



Source: Lab 03 Part C – IPv4 Addressing, Question 22

sWin16SVR1 can ping sWIN16RTR (E0) even though they have different subnet masks because:

- sWin16SVR1 applies its subnet mask 255.255.255.192 to its IP address and gets subnet ID: 172.16.32.0
- sWin16SVR1 applies its subnet mask to the router's IP address and gets subnet ID: 172.16.32.0
- The two subnet IDs are identical so SVR1 will use the router's MAC address as Layer 2 destination MAC address. In this case, no default gateway is needed because devices are in the same subnet.
- SVR1 does not know the subnet mask of the router, thus SVR1 uses its own mask to calculate the router's subnet ID.

sWin16SVR1 cannot ping sWin10PC201 because:

- SVR1 applies its own subnet masks to its IP address and gets subnet ID: 172.16.32.0
- SVR1 applies its own subnet mask to PC201's IP address and gets subnet ID: 172.16.32.192
- These 2 subnet IDs are not identical, they are in different subnets. Without configuring the default gateway, the packet will be dropped.

Lab 04: DHCP & Further Subnetting

Key concepts

I learned about Dynamic Host Configuration Protocol (DHCP), which automatically assigns IP addresses and network configuration settings. DHCP simplifies network administration and allows flexibility in IP address management. Exclusion and reservation ensure unique IP addresses, with reservation being preferred as it guarantees the same IP address and offers centralised configuration. DHCP can be configured with additional options like default gateway and DNS server addresses, which can be set at various levels of the DHCP hierarchy.

If same setting is configured differently, the **order of precedence** from lowest to highest is:

1. Server level – apply for all devices from all scopes on the DHCP server e.g., DNS server used by all subnets
2. Scope level – apply to the pools in each scope and are typically associated with subnets e.g., default gateway.
3. Reservation level (reserved client) – apply to a specific device.

Key configurations and commands

Key steps	**Details**	**Notes**
Enable DHCP on a network interface	Right-click on Start -> Windows PowerShell (Admin) and type command: *Method 1:* • **Set-NetIPInterface –InterfaceAlias Ethernet –dhcp enabled.** *Method 2:* • **Netsh interface ip set address Ethernet dhcp**	Type **ipconfig /all** to verify
Install DHCP	• On SVR1, Server Manager -> Manage -> Add Roles and Features • Accept the defaults (click Next 3 times) and stop on "Select server roles" page. • Click check box next to DHCP -> Add Features -> Next 3 times. • "Confirm installation selections", verify adding the DHCP server tools -> Install. • When the text under blue lines read "Configuration required. Installation on sWin22SVR1", Close	• **Always launch Domain Controller (DC1) first before launching any other machines**. **Login as swin\Administrator.** • Install DHCP is not enough, we need to configure the role (i.e., authorise the DHCP server if it is part of the domain) • The Domain Controller can also be a DHCP server.
Post-deployment configuration	• In Server Manager, a yellow triangle alert appears (DHCP post-deployment flag) • Click on alert -> Complete DHCP configuration. *Authorise the new DHCP server with Domain Controller:* • DHCP Post-install configuration wizard, Next • Authorization page, accept defaults, click Commit. Note: select "Alternate Credentials" if logged in to the wrong account • Summary page, Close.	• Since SVR1 is Windows Domain sWin.Local -> must **Authorize new DHCP server with the Domain Controller** before any computer in the domain will accept a lease from it. -> must **login as domain administrator** (not local) i.e., **swin\Administrator.**

	Note: configure this step correctly otherwise we get a red arrow.	

Create a DHCP scope	• On server, Server Manager, Tools, DHCP.
	• Click on the server's name (sWin16SVR1) -> IPv4.
	• Right-click on IPv4 -> New Scope…
	• New scope wizard, click Next on the first page -> enter name Hawthorn and description (e.g., purpose) -> Next.
	• IP Address Range page -> enter the values -> Next
	• Add Exclusions and Delay page, click Next.
	• Lease Duration page, choose a lease period of:
	  ○ 8 days for devices on a cable
	  ○ 8 hours for devices on WiFi
	Then click Next.
	• "Configure DHCP Options" page, select No -> Next -> Finish
	
	Activate the scope:
	• DHCP Management console, a red down arrow in the icon of the new scope we just created and a blue exclamation mark with IPv4 container -> the Scope has not been activated.
	• Click on the Scope icon -> right-click Scope icon -> select Activate from the context menu.
	• Red down arrow and blue exclamation mark disappeared -> DHCP server is now ready to send out offers.	

Stop DHCP service of a server	• Server Manager, Tools, DHCP. • DHCP console, click on **swin16dc1.swin.local** -> right-click on **swin16dc1.swin.local** -> select All tasks, Stop	**Stop the service** to ensure that this DHCP server will **not** lease out any IP addresses
Test if DHCP server is working	PC -> PowerShell, type "**ipconfig /renew**", Enter	**Ipconfig /renew** command triggers the computer to send out a DHCP discover packet.
Configure exclusions	• On server, in DHCP management console, expand Hawthorn scope. • Right-click on the Address Pool container -> select New Exclusion Range… • Enter start IP address and End IP address -> Add.	Test if the exclusion is being applied by typing **ipconfig /release** then **ipconfig /renew** on the device e.g., sWin10CL101
Find a device's MAC address	• On a device e.g., sWinCL101, open Windows PowerShell (Admin) -> type **ipconfig /all** -> enter. • The MAC address is located on the line "Physical Address"	
Configure a reservation	• sWin16SVR1, DHCP Management, expand Ipv4 and Scope containers. • Right-click Reservations, New Reservation	

	• Reservation name -> enter name "sWin10CL101", IP address, MAC address (without the hyphens "-") of the reserved device. • *Verify*: Change to sWin10CL101 -> ipconfig /release -> ipconfig /renew	
DHCP options	• sWin16SVR1, DHCP Management console, expand the scope created before (in IPv4 section). • Click Server Options container -> right-click to bring the context menu. • Select Configure Options… -> the Options dialogue box appears.	3 common options: • 003 for router • 006 for DNS servers • 015 for DNS domain name
Server options	In **Server Options** dialog, configure: • 003 Router IP address setting -> Add. • 015 DNS Domain Name e.g., NetAdmin.edu -> OK • Release and renew IP address of the sWin10CL101 to verify new settings e.g., DNS suffix, IPv4 address, subnet mask, default gateway.	
Scope options	• On sWin16SVR1, expand Hawthorn scope, click **Scope Options** -> right-click -> Configure Options… -> configure 003 Router IP address & 015 DNS Domain Name e.g., ScopeSetDNS.com -> Add. • Release and renew IP address of sWin10CL101 to verify new settings.	
Reservation options	• On sWin16SVR1, expand Hawthorn scope -> expand **Reservations** container -> click on the IP address -> right-click to bring context menu up. • Select Configure Options…, configure 015 DNS Domain Name -> OK	

Further study

Address Resolution Protocol (ARP) is used to map a known Layer 3 IP address to an unknown Layer 2 MAC address for local network communication. ARP process has 2 messages: ARP request and ARP response. The ARP request is broadcast because the layer 2 address of the destination host is unknown and all devices on the same network will see the message, but only the intended device will respond with an ARP reply. The ARP reply is unicast, which is sent only to the host that sent the request (Harmoush 2021). Devices maintain ARP caches to optimise communication and the Windows command **arp -a** displays the ARP table. ARP caches can be deleted using **arp -d**.

Lab 05: Introduction to DNS

Key concepts

I have gained knowledge about DNS (Domain Name System). DNS is an essential technology that enables us to access websites, services, and internet resources using easy-to-remember domain names instead of complex IP addresses. It operates as a widely distributed database and serves various purposes such as translating fully qualified domain names (FQDNs) into IP addresses, locating domain controllers and global catalog servers, converting IP addresses back to host names, and assisting in mail server location for email delivery.

Key configurations and commands

Key steps	**Details**	**Notes**
Install DNS	• Launch DC1 • Log into sWin22SVR1, Server Manager -> Manage -> Add Roles and Features -> install DNS Server role, with all default settings. • Installation complete, close Add Roles and Features. • Server Manager, Tools, DNS to bring up DNS Manager console.	Launch DC first then network devices, including DHCP server before other machines.
Create a primary forward lookup zone	• DNS Manager -> sWin22SVR1 -> Forward Lookup Zones. • Right-click Forward Lookup Zones -> select New Zone... • Welcome screen -> Next. -> Zone Type page, select Primary zone -> Next -> Enter the Zone name -> Next -> accept the default Zone file name and location -> Next • Keep default *"Do not allow dynamic updates"* -> Next -> Finish. • Our DNS Manager should have a new primary zone under Forward Lookup Zone.	
Creating network resources – file server	• On SVR3, launch File Explorer -> navigate to This PC -> create a Folder by right-clicking Local Disk (C:) -> New -> Folder. • Name the new folder (e.g., Data). In this folder, create a New text document (e.g., TopSecret.txt), add some text and save it. *Share the folder for access over the network:* • Right-click folder -> Properties -> Sharing tab -> Advanced Sharing. • Check *"Share this folder'* -> limit the number of simultaneous users. • Permissions -> ensure Read permissions are configured for Everyone. -> Ok twice -> Close	File Server role is **installed by default i**n Windows Server 2016.

Create network resources – Web server	• SVR3, Server Manager, Add Roles and Features -> accept default options until we get to Select server roles page. • Add Web Server (IIS) role -> accept default options -> close. • Click Start, notepad -> **Run as administrator**. • Save as index.htm in **C:\inetpub\wwwroot** folder.	
Create DNS records	On SVR1, DNS Management, Forward Lookup Zone -> primary zone *Create records for www:* • Right-click primary zone -> New host • Name field, enter www (FQDN: www.burne.edu.) • IP address field, enter IP address -> Add Host. *Create records for File server (alias with CNAME record):* • Right-click on primary zone -> New Alias (CNAME) • Enter alias name. *Set the target host:* Click Browse button -> double-click SVR1 in Records pane -> double-click Forward Lookup Zones -> double-click burne.edu zone -> select www **Host (A) record** -> OK twice.	
Clear DNS cache	Open cmd/PowerShell, type **ipconfig /flushdns** on the machine (e.g., PC203)	Do this if made mistakes with DNS record
Test DNS	• Login to PC203 as Admin • Ethernet adapter -> add SVR1's IP address as PC203's preferred DNS server. • Microsoft Edge browser -> type in www.burne.edu in address bar -> should be directed to the web page created before. • File Explorer -> type \\FileSvr.burne.edu -> enter username: Administrator, password: Pa55w.rd • We can see Data folder created before.	
Zone transfers	*Create secondary zone on another machine e.g., DC1:* • Load DNS Management -> right-click Forward Lookup Zones -> choose New Zone... • On Zone name dialog, enter e.g., burne.edu -> click Next • On Master DNS server dialog, enter SVR1's IP address (server that hosts primary zone) -> click Next -> Finish. • Double-click on new zone (zone is not loaded) *Authorise zone transfer:*	After creating secondary/stub zone, authorise zone transfers on primary server before data is transferred. 2 options to authorise: • Name Servers tab -> List of all DNS servers in the domain, • Authorise DNS server individually.

	• On the primary server (SVR1), in DNS Management, right-click on burne.edu -> select Properties. • Click on Zone Transfers tab • Click on Name Servers tab -> Add sWin16DC1.swin.local -> Resolve -> error (because we do not have reverse lookup zone configure) -> OK • Click Zone Transfer tab -> Allow zone transfers, Only to servers listed on the name servers tab, OK • DC1, **refresh** new sWin.local secondary zone -> right-click burne.edu zone, select Transfer from Master	

Lab 06: Identity and Access control using AD DS

Key concepts

I learned about Active Directory Domain Services (AD DS), which centralises control over user accounts, computer accounts, and security policies for managing network resources (Lutkevich & Boger 2021). I learned how to create a domain, OU, user, computer, and group accounts. ACL (resource) groups help control access to resources and keep servers efficient by minimising the size of DACLs. Domain Local groups are the best fit for ACL groups, as they can be given permissions to local resources and can have members from any trusted domain. ACL groups can only give one set of permissions. Account groups streamline permission allocation to user or computer accounts based on similar requirements (e.g., same role/location), typically created using the Global group scope.

Key configurations and commands

Key steps	**Details**	**Notes**
Create a domain	*Configure DC:* • Log into DC as Administrator -> configure DNS address to be its own IP address • Server Manager -> Manage -> Add Roles and Features -> Active Directory Domain Services -> accepting default settings • Click on alert symbol -> *"Promote this server to be a domain controller."* • **Add a new forest** -> domain: sWin.Local -> choose domain & forest functional level -> accept default options for installing a DNS server & Global Catalog -> enter DSRM password (**Pa55w.rd**) -> accept defaults for the remainder. • Restart the computer -> login as **sWin\administrator**	• Make sure that both server & PC have IP addresses in the same subnet. • Match domain functional level to **oldest** DC for existing forests, set to **highest** for new forests with one DC.
Create resources	• On the DC, click File Explorer -> This PC -> Local Disk (C:)-> right-click -> New -> Folder *Share the folder:* • Right click folder -> Properties -> Sharing tab -> Advanced Sharing -> Share this folder -> Permissions button -> tick "Allow" according to the scenario.	
Join a PC to a domain	• From PC, login as local Administrator -> configure DNS address as DC's IP address • Search System (Control Panel) -> in System window -> Change Settings -> Click "Domain" radio button under "Member of" -> type sWin.Local (the name of domain that you want to join) -> OK • "Computer name/domain changes" -> enter username "sWin\Administrator" & password	Test DNS by **ping sWin.Local** or **nslookup sWin.Local ->** success if it **returns DC's IP address.**

	"Pa55w.rd" (account with administrative privileges) -> reboot the computer • *Validate if joining is successful*: in DC -> Server Manager -> Tools -> Active Directory Users and Computers (DSA) -> the new computer account is in **Computers** container	
Create user accounts	• On DC -> run Active Directory Users and Computers (or **dsa.msc**) -> right-click on Users container -> New... -> User • Enter first name, last name and logon name -> Next -> enter password -> untick User must change password at next logon -> OK -> can now logon as e.g., sWin\Jill in PC203	
Create computer accounts	• On DC -> dsa.msc -> right-click Computers container -> New... -> Computer • Enter computer name (1) -> Change... button -> type in username -> Check Names.	(1) Enter **PC's exact name** when creating **computer account** in DC
Configure account properties	*Set user account properties:* • DSA -> Users container -> right-click user account -> Properties -> configure settings in different tabs e.g., General, Address, Account (Logon hours, logon to, unlock account, user must change password at next logon, etc.), Profile (Home folder, Connect = Z: \\sWin22SVR3\Home\%username%), Member of. *Set computer account properties:* • DSA -> Computers container -> right-click on computer account -> Properties -> General tab (Description) or Location tab etc.	**%username%** is a dynamic system variable for **user's Home folder**, useful for creating account templates without manual path updates.
Create an OU	On DC -> DSA -> right-click sWin.Local -> New... -> Organisational unit -> Enter OU's name	Untick "Protect container from accidental deletion" if this is a temporary OU
Create group accounts	*Create resource group:* • Right-click on the OU -> New... -> Group • Click Domain local button -> Enter group name -> assign access to the group *Create account groups*: • Active Directory Users and Computers -> right-click OU -> New -> Group -> select group scope: Global -> enter group name -> OK • Right-click new group -> Properties -> Members tab -> add member.	Group name should follow a convention (e.g., DL_Data_RW; G_People)

Assign permissions for resources	*Assign NTFS permissions:* • Right-click the folder -> Properties -> Security tab -> Edit button -> Add button -> Enter the object names -> type in the resource group names -> Check Names -> click on the right DL group -> OK • Tick the permissions -> OK *Remove inherited permissions:* • Folder's properties -> Security tab -> Advanced button -> Disable Inheritance -> **"*Convert inherited permissions into explicit permissions on this object*"** • "Permission entries" list -> click on every entry for the User group -> Remove -> OK twice to back at Properties. *Assign Share permissions*: • Folder's properties -> Sharing tab -> Advanced Sharing... -> tick Share this folder -> accept default share name (1) • Permissions button -> assign needed permissions (e.g., Everyone group Full Control) (2) -> OK 3 times	• (1) Shares are advertised by default but can be hidden by adding **$** to share name. Hidden shares require full UNC path for access. • (2) Without at least one group having **Write** access to the files in the folder, the **default read-only share permission** prevents any user, including administrators, from writing to the files. *Best practice for sharing a folder*: Convert to explicit permissions -> remove User groups from NTFS -> Share Everyone = Full Control/Change -> allow NTFS permissions to control access
Nesting groups	*2 methods:* • *Method 1:* in DSA, right-click the DL group -> Properties -> **Members** tab -> add Global group as a member. • *Method 2:* Right-click the Global group -> Properties -> **Memberof** tab -> add DL group that the Global group belongs to.	
Test the configuration	Login as Jill on PC and confirm their access to the folder (e.g., RW/RO) using UNC path/network browsing.	Access tokens are created during user logins -> group membership changes require **logging off and back** on to generate new access tokens with updated SIDs.

Further study

UNC (Universal Naming Convention) path is a standard way of identifying shared network resources in Microsoft Windows environment. It allows users to access files, folders, and printers on remote servers by specifying two backslashes (\\), followed by the server's name or IP address, and the share name (**\\server\sharename**). For instance, the UNC path for a shared folder on a server named "Server1" with a share name "SharedFolder" would be "\\Server1\SharedFolder". UNC paths are commonly used in modern Windows environments for accessing shared network resources. In contrast, DOS paths (e.g., C:\Folder\File.txt) are more traditional and refer to the local file system path on a specific drive and folder of a Windows computer (Brans 2023).

Lab 07: RBAC using AD DS & Security Groups

Key concepts

This week, I learned about advanced group strategies, including the use of second-level account groups for efficient access management in Active Directory. Creating these groups with member groups allows for easy access provisioning, such as adding teams to higher-level groups like departments. In multi-domain forests, Universal groups can be used to group teams from different domains (**IGUDLA**), while Global groups can be used for groups within the same domain (**IGGDLA**). These strategies enhance scalability and flexibility in access management. The reason we do not use IGUDLA strategy extensively is because Universal group memberships are stored in the global catalog, which is replicated to every domain in the forest, and can result in additional replication overhead (Bertram 2020).

Key configurations and commands

Key steps	Details	Notes
Create a child domain	• Verify DNS configuration on SVR3: ping **sWin.local** • Add ADDS role to SVR3 (refer to Lab 6) • On a new server (SVR3), Server Manager -> click alert -> Promote this server to be a domain controller • Deployment Configuration -> **Add a new domain to an existing forest** -> Select... -> enter username (**sWin.local\Administrator**) and password (**Pa55w.rd**) -> Select domain type: *Child Domain* -> Parent domain name: *sWin.local* -> enter new domain name -> Next • "Domain Controller Options" -> Domain functional level: Windows Server 2016 -> ensure DNS server and GC checked -> Site name: Default-First-Site-Name -> enter DSRM password -> Next. • "DNS Options" -> ensure Create DNS delegation is checked & Credentials for delegation creation is sWin.local\Administrator -> Next -> Next 3 times -> ignore alert -> Install	For child domain's DC (SVR3) to function as primary DC in new child domain, install DNS server and copying forest information from parent domain.
Resolve existing DC replication issue	• On existing DC (DC1) -> Server Manager -> Active Directory Sites and Services -> expand and browse to SWIN16DC1 -> NTDS Settings -> right-click -> Replicate Now -> a confirmation box appeared if replication successes. • Do the same step for another DC (SVR2) • Promote the new DC again (SVR3)	Only perform this step if cannot promote SVR3 to be a DC and replication error message

Group Strategy	• *Create network resources on DC1:* Create folders -> share folders with Everyone = FC -> remove inherited permissions (1) (Refer to Lab 6) • *Create an OU on DC1*: Active Directory Users and Computers -> right-click sWin.local -> New -> OU -> name the OU • *Create sWin.local groups*: right-click new OU -> New -> Group -> name the group -> Group type: Security -> choose Group scope (2) • *Nest groups within domain*: refer to Lab 6 or use PowerShell • *Nest groups between domains*: On DC1 -> DSA -> double-click **Universal** group-> Members tab -> Add... -> Select Users, Contacts... -> Locations... -> expand sWin.local domain -> select different domain -> OK -> Enter the object names... -> type G_ -> Check Names -> select desired group.	• (1) This includes convert to explicit permissions + remove all permissions for **Users** group • (2) Use **Universal** groups for **multi-domain forests (IGUDLA)** and **Global** groups for **single-domain forests (IGGDLA).**
Fix group scope mistake	Change the group scope to Universal -> can now change to Global/Domain Local.	Default group scope is **Global ->** cannot change directly to Domain Local
Create user account template	• DC1 -> dsa.msc -> right-click OU -> New -> User -> enter first name & user logon name -> Next -> ensure that "User must change password at next logon" & "Account is disabled" are unchecked -> Next -> Finish • *Configure attributes to be copied for each new user account*: Profile, Memberof, Account tab, etc. *Copy this template:* • Right-click template -> Copy... -> Enter first name, last name, and user logon name -> Next -> enter password -> untick User must change password & Account is disabled • Change new user's groups as needed	A new user folder will appear in *C:\Home\folder* after copying from template
Verifying child domain creation success	• On SVR3 (child domain) -> logon as child domain admin (e.g., SRWK\Administrator) • Server Manager -> Tools -> **Active Directory Domains and Trusts** -> expand sWin.local -> verify that Srwk.sWin.local is added as a child domain	
Create domain	Domain example: Srwk.sWin.local	

objects in PowerShell	• *Create OU "Finance"*: on SVR3 -> PowerShell -> Type: ***new-ADOrganizationalUnit –name Finance –path "dc=Srwk,dc=sWin,dc=local"*** -> Enter • *Create new user account for Minh:* ***New-AdUser –name "Minh" –Path "ou=Mkt,dc=Vn,dc=sWin,dc=local" –accountPassword (ConvertTo-SecureString –AsPlainText "Pa55w.rd" –Force) –enable $True*** • *Create Groups:* *Create groups:* ***New-ADGroup –name G_Adv –GroupCategory Security –GroupScope Global –path "ou=Mkt,dc=Vn,dc=sWin,dc=local"*** *Set membership and nesting:* ***Add-ADGroupMember G_Adv Minh*** (add Minh as a member of G_Adv) *or* ***Add-ADGroupMember G_FinanceSrw G_AccPay*** (add G_Adv as member of G_MktVn)	
Join PC to new domain	• On SVR3 -> PowerShell -> type: ***redircmp "ou=Finance,dc=Wtnr,dc=sWin,dc=local"*** *Join PC203 to Wantirna domain (Finance OU):* • On PC203 -> test DNS by ping Wtnr.sWin.local -> if success -> join PC to this domain (refer to Lab 6) • Use credentials of Wtnr\Administrator -> skip "Add an account" -> reboot PC203 -> verify PC203's computer account appears in Finance OU in Wantirna domain	Use **redircmp** to change default location for computer accounts in AD when joining a **computer without an account** to the domain. By default, new computer accounts are created in the **Computer** container in AD.
Test access permission	• On PC203 login as Minh -> File Explorer -> enter UNC for shared resources on DC1: \\sWin16DC1.sWin.local\CustAccountData • Verify that user has correct access	If encounter error: "user cannot login remotely": • Login as Administrator on PC203 • Add **Everyone** group to **Remote Desktop Users** group on the DC. *Remember*: Group membership changes require **logging off** and **logging back** on to generate a new Access token with updated SIDs for the user.

Lab 08: Group Policy Objects (GPOs)

Key concepts

I explored the configuration and deployment of Group Policy Objects (GPOs) in Active Directory (AD) for centralised management of user and computer settings. Here are the key points:

- GPOs are applied in the order of **LSDON**: Local, Site, Domain, (parent) OU, and nested (child) OU.
- GPOs cannot be directly linked to groups or user/computer containers in AD, but they can be **filtered** to apply only to specific groups or users.
- 3 methods to **filter GPOs**: GPMC (security filtering), GPO permissions (delegation deny ACL), and WMI Filtering (based on computer attributes).
- 3 approaches to **restrict software execution**: Software Restriction Policies, AppLocker, and Don't run specified Windows applications. AppLocker can restrict all software versions and specific companies and offers Audit mode for tracking software usage and user access.

GPOs need to be linked to a container for application, and the objects that require the GPO settings must be located within that container. GPOs also require propagation to other computers before taking effect. By default, GPOs are reapplied every 5 minutes on domain controllers and within 90 ± 30 minutes on end devices.

Key configurations and commands

Key steps	Details	Notes
Shortcuts	**Win+R** or run **cmd**: • **Ncpla.cpl** - Network Adapter • **Gpmc.msc** - Group Policy Management Console • **Gpedit.msc** - Local Group Policy Editor	
Harden a desktop (Local policies)	• Logon to PC as local Administrator -> Win key -> Start -> **gpedit.msc** -> **Local Group Policy, Computer Configuration, Administrative Templates, Windows Components** • Double-click “Set the default behavior for Autorun” -> Enabled -> enter comment -> set “Default Autorun Behavior” to “Do not execute any autorun commands”	
Prohibit access to the Control Panel (Local policies)	• Check if you can access control panel: Start screen -> type Control panel -> select it to run • gpedit, **User Configuration, Administrative templates, “Control Panel”** container • Double-click “Prohibit access to the Control Panel and PC settings”, enter comment, Enabled, OK • Test: Start -> type Control Panel -> should not run.	

Ctrl+Alt+Del Options (Local polices)	• <u>Check if you have this option:</u> press Ctrl+Alt+Del. • Local Group Policy Editor (gpedit) -> **User Configuration, Administrative Template, System, "Ctrl+Alt+Del options",** Double-click "Remove Lock Computer", Enable, enter comment, OK	Same steps for "Remove Task Manager
Delegate control of an OU	Right-click OU, Delegate Control, add user account (that needs delegated control) to child OU -> choose the tasks they can perform	Delegate control of an OU to specific user/group for user account password and group management.
Create a custom console	*<u>Create custom console for a specific OU:</u>* • Launch MMC on DC-> File -> add/remove snap-in -> add Active Users and Computers snap-in • Expand swin.local domain -> OU needed to create a custom console for, right-click, New Window from here *<u>The initial console window still shows domain root and details:</u>* • Click on Window menu -> select Console Root\... -> close this inner window (not the whole console) • *<u>Test</u>*: should only have contents of desired OU in the console -> save console as "ICTSupportConsole"	• Type mmc on cmd.exe • Create a custom console to limit the visibility of the network structure for users with delegated access, displaying only the objects they are authorised to manage.
Create GPOs	• DC1 -> run **gpmc.msc** -> expand Domains, swin.local -> right-click Group Policy Objects -> New -> GPO's name: EnableTaskManager • Right-click new GPO -> Edit -> **User Configuration, Policies, Administrative Templates, System, Ctrl+Alt+Del options, "Remove Task Manager"** -> Disabled option	• Put **sWin** before the logon name • If cannot logon and error "*To sign in remotely, you need the right to sign in through Remote Desktop Services....*" -> on the PC -> View menu -> deselect Enhanced sessions
GPUpdate	In cmd, type: • **Gpudate /force** - applies all GPO settings (user + computer), even if they have not changed • **Gpupdate /target:user** (or **:computer**) - applies only user/computer configuration • **Gpudate /boot** - restarts the computer after GPO has been applied	After changing GPO setting, run "gpupdate" on both **DC** and **workstation** being tested.
Link GPOs to containers	• GPMC -> right-click domain/OU/site -> Link an Existing GPO -> select GPO • **gpupdate /force** on both DC1 and PC201 • Test on PC201 (Ctrl+Alt+Del options)	

Prevent Software Running Policies	• DC1 -> GPMC -> create and link GPO "RestrictRunningOfCalc" to swin.local domain. • Edit GPO -> browse to "***User Configuration\Policies\Administrative Templates\System\Don't run specified Windows applications***" • Add "calc.exe" to the list of disallowed applications. • <u>*Test*</u>: run **calc.exe** on SVR1 by browsing to "***C:\Windows\System32\calc.exe"*** in File Explorer -> should not run	• ***Don't run specified Windows*** only blocks programs launched through **File Explorer**. It does not restrict users from running programs through other system processes like Task Manager or cmd.exe. <u>2 other methods:</u> • **Software Restriction Polices** *(User configuration\Policies\Windows Settings\Security Settings)* -> right-click Software Restriction Policies -> New Software Restriction Policies • **AppLocker** (*Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker*) -> 3 steps
Link multiple GPOs	<u>*Change priority of GPOs:*</u> • GPMC -> ICTProcurement OU -> link **Remove Taks Manager** first -> then link **Enable Task Manager** GPO • On PC201 -> login as user in ICTProcurement OU -> **Remove Task Manager GPO** is applied <u>*Change link order of GPOs so Enable Task Manager is at position 1:*</u> • GPMC -> select Enable Task Manager -> click on the arrow -> test on PC201 -> **Enable Task Manager** GPO is applied	GPOs with **lower link order** numbers have **higher precedence**. -> Link order 1 win over link order 2
Filter GPOs	<u>*GPMC (Security) filtering:*</u> • GPMC -> link GPO to desired OU • **Group Policy Objects** container -> click GPO • Security Filtering -> default: **Authenticated Users** group -> Remove default permission of **Authenticated User** (**<u>Allow Read & blank Apply Group Policy</u>**) -> Remove -> Add... -> add desired group to Security Filtering -> make sure this group has **Allow Read** -> <u>*GPO Permissions:*</u> • GPMC, right-click GPO, Edit, right-click on GPO name, Properties. • Security tab -> Domain Admins group -> Permissions for... -> "**Apply group policy**" -> tick **Deny** -> this GPO will apply to everyone **except** those in Administrators group	<u>Important (for Security filtering):</u> Ensure targeted accounts have **read permissions** when filtering a GPO. • Security tab of GPO -> Authenticated Users -> ensure **Allow Read** permissions. • <u>Restrict GPO's scope:</u> ensure **Allow Apply group policy** is blank for "Authenticated Users" group -> GPO will only apply to members who are part of the specified group, and not to all authenticated users.

	• SVR1 -> log off -> log on as Administrator -> test if can run apps	
Modelling GPOs	• GPMC -> right-click Group Policy Modeling, Select defaults for Domain Controller Selection • User and Computer Selection -> specify the user and computer accounts to be modeled -> tick "Skip to the final page...", Next. • Ignore warnings -> On the report -> Details tab to see what GPOs are being applied	Group Policy Modeling is a troubleshooting tool that generates a report identifying which GPO settings are being applied to a selected container, user, or computer (**remember to enter the correct path**). <u>3 ways to troubleshoot GPOs:</u> • Group Policy Modelling • Rsop.msc • gpresult
Create a new printer	• GPMC -> create a new GPO "IctPrinterDeploy" -> link to OU *<u>Create a new printer:</u>* • Server manager, Tools, Printer Management -> expand Print Servers, sWin16DC1 (local) -> right-click Printers -> Add Printers • Printer Installation page -> Add a new printer using an existing port: -> port **LTP1,** Next • Printer Driver page -> Install a new driver -> next • Printer Installation -> select Brother Color Leg Type1... printer -> Next • Printer Name and Sharing Settings -> name: ICT_Printer -> share as ICT_Printer, next, Printer Found page, Next, Finish	
Set Permissions on printer	Right-click printer, Properties, Security tab -> give the group: Manage this printer & Manage documents permission -> **Apply,** OK	<u>Optional step</u>: Set printer permissions to delegate management and avoid being solely responsible for printer issues.
Deploy Printer using GPOs	• Print Management -> right-click ICT_Printer -> Deploy with Group Policy... • Browse (next to "GPO name")-> find ICTPrinterDeploy GPO, OK *<u>Deploy printer to Users ICT OU:</u>* • Check "The user that this GPO applies to (per user)" -> Add • Verify UNC for the printer in Printer Name, OK, success message, OK *<u>Test deployment</u>:* • Logon to SVR1 as users created above (or **gpupdate /force** if already logged in) -> verify that printer has been deployed (Settings\Services\Printers & Scanners)	• Printer deploys to Users, or to computers if GPO linked to OU with computer accounts. • If cannot find Print Management, install roles under "Tools".

Lab 09: Managing Security in AD

Key concepts

I learned how to improve the baseline security of a Windows Server Domain by configuring different security settings. Enhancing AD security is vital for protecting data, preventing breaches, and ensuring compliance. Here are the main points:

- Enforcing strong passwords and lockout settings via account policies, linked to the Default Domain Controllers Policy (DC).
- Utilising the Restricting Groups policy to remove unauthorised accounts from privileged groups.
- Implementing Encrypting File System (EFS) for file security.
- Monitoring account logon events and object access through auditing, with event logs retrieved via Event Viewer console.
- Leveraging tools like Best Practices Analyzer (BPA) and Security Compliance Manager (SCM) for compliance and security improvements.
- Centralising OS and application updates with Windows Server Update Services (WSUS), configured through GPOs.

Key configurations and commands

Key steps	**Details**	**Notes**
Configure account policies	• DC1 -> GPMC -> edit **Default Domain Controller Policy.** • ***"Computer configurations, Policies, Windows Settings, Security Settings, Account Policies, Password Policy"*** • Account Policies -> Account lockout policy -> configure each policy accordingly	Accept the defaults as necessary.
Configure user rights	• Create a GPO, link to OU. • Edit GPO -> "***Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment"*** -> Allow log on locally -> "*Define these policy settings*" is checked -> add groups • Deny log on locally -> add groups. • Test: **gpupdate /force** on DC -> login as denied user on CL101 -> can still login since CL101 computer account is in Computer container, not ICT OU. • Move sWin10CL101 from **Computers** container to OU -> reboot CL101.	If the GPO is not taking effect, ensure **computer account is in the container where GPO is linked**.
Troubleshoot GPO with **gpresult**	*Run apps with elevated privileges:* • CL101, Start, cmd, right-click, **Run as administrator,** enter credentials of swin\Administrator.	

	• Type: **cd c:\users\IPuser** (change to the IPuser's home folder) *Generate GPO settings report:* **gpresult /user <username> /h <filename>.htm** • File Explorer, browse to C:\Users\IPuser, double-click the html file, scroll down to see **Applied GPOs** section.	
Restricting groups	• SWin.local domain -> create and link GPO: RestrictAdminGroup -> Edit... -> **Computer Configuration, Policies, Windows Settings, Security Settings, Restricted Groups** -> Right-click -> Add Group... -> Browse to Administrators group. • Administrator Properties -> **Member of this group:** -> Add -> add user account: ISuser -> OK • DSA, Builtin container -> right-click Administrator -> Members tab -> Add -> add user accounts (ISuser,IPuser) -> OK • Run **gpupdate /force** -> **Members** tab of Administrators group -> IPuser should be removed, ISuser remain.	Restricting Groups policy **removes unauthorised user accounts added to privileged groups** (e.g., Administrators) during the next group policy application.
Auditing	• DC1 -> GPMC -> edit "***Default Domain Policy***" -> "***Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Audit Policy***" -> enable Audit Account Logon Events & Audit Object Access • **For Audit object access:** Go to file/folder -> Advanced Security -> Auditing tab -> Add -> Select a principal -> enter Authenticated Users -> Type: All -> OK twice • Test: Reboot CL101 -> login as ISuser -> browse to \\sWin22DC1\Data -> open file, make some changes, save • DC1 -> **Event Viewer** -> expand Windows Logs, Security **4656 -** object access events **4624 -** account logon events **4634 -** account logoff	For "audit object access" or "audit directory service access" -> need to configure **Properties** of file/folder + editing GPO.
Using EFS	Right-click file -> Properties -> General tab -> Advanced... -> Advanced Attributes dialog -> check Encrypt contents to secure data, OK, Apply	
WSUS with GPO	• DC1 -> edit **Default Domain Policy** -> **Computer Configuration, Policies,**	Remember to link GPO and **gpupdate /force**

	Administrative Templates, Windows Components, Windows Update • Specify intranet Microsoft update service location: Enabled -> set intranet update service & set intranet statistics server = http://172.16.32.1 (URL of WSUS server) • Configure Automatic Updates: Enabled -> Configure automatically updating; Scheduled install day, Schedule install time • Enable client-side targeting: Enabled -> target group name for this computer.	
GPO with Firewall	• Create new GPO "Firewall-AllowPing", link to the domain • Edit the GPO -> **Computer Configuration, Policies, Windows Settings, Security Settings, Windows Firewall with Advanced Security** -> right-click Inbound Rules -> New Rule... • Rule Type = custom; Program = all programs; Protocol = ICMPv4; Scope = any IP address; Action = allow; Profile = Domain and Private; Name = AllowPing;	Enable ping through GPO for troubleshooting purposes but remember to **unlink the GPO afterwards** to prevent potential misuse.
Best Practice Analyzer	Server Manager -> All Servers -> select DC1 -> scroll down to Best Practices Analyzer -> drop down TASKS -> Start BPA scan -> Start Scan -> wizard completes with a list of warnings	

Further study

Both "*Audit Account Logon Events*" and "*Audit Logon Events*" settings are used to audit the logon events into a computer, but they serve different purposes in monitoring user authentication events. "*Audit Account Logon Events*" focuses on tracking authentication events for domain user accounts on domain controllers, while "*Audit Logon Events*" tracks authentication events for all types of logons, including both local and domain accounts, on individual Windows systems (Morgan 2014). These settings help organisations monitor and log user authentication activities for security analysis and troubleshooting purposes.

Lab 10: Managing Quality & Risk with Disaster Recovery

Key concepts

Disaster recovery is important for protecting critical data and systems and resuming business operations after a disaster. Firstly, implementing volume redundancy through technologies like RAID 1 and RAID 5, created using Disk Management, offers fault tolerance by mirroring data across multiple drives or using distributed parity data across several drives (Hefner & Sullivan, 2023). Shadow copies capture changes to files on a volume for easy access to previous versions of a file, but they cannot replace backups. Backups should be stored on separate devices or locations. Access-based Enumeration enhances security and user experience by ensuring that individuals can only view and access files and folders they have explicit permission for within a shared folder, reducing confusion and unnecessary helpdesk inquiries.

Windows Server Backup is a valuable tool for backing up entire volumes or specific files/folders. While it is not installed by default, it can be easily added using Server Manager. Service recovery automatically restarts services or reboots computers in case of minor crashes, helping minimise downtime and quickly restore system functionality. Performance Logs are important for tracking system performance over time. They allow us to identify issues and optimise system performance. Lastly, NTFS Quotas offer a means to limit the disk space consumed by individual users on a volume, preventing any single user from monopolizing resources.

Key configurations and commands

Key steps	Details	Notes
Configure volume redundancy – mirrored volume (RAID1)	• Logon to SVR1 as **sWin\Administrator** • Right-click Start -> Disk Management • Right-click Disk 1, select Online -> Repeat for Disk 2 • Right-click Disk 1, Initialize disk -> select **GPT** (1) -> OK • *Create mirrored volume:* Right-click Unallocated Space, select "New Mirrored Volume" *During the wizard:* • Add Disk 2 to **Selected:** list. • Amount of space in MB = 2048MB • Mount volume in NTFS folder: C:\Backups • Volume labels: Backups, check "Perform a quick format" Finish -> "convert the disk to Dynamic disk," select Yes • SVR1 -> folder **C:\Backups** -> create new folder "**NetworkBackup**" -> share this as **Backup$**, share permission **Everyone = FC** -> remove inheritance, remove **Users** from NTFS -> give **Domain Admins** NTFS Allow FC	• (1) Older versions of Windows on the network -> select MBR. If use only up-to-date OS -> select GPT • The $ sign in "Backup$" creates a hidden share that is not visible to users browsing the network.

Configure Shadow Copies	• DC1, create Shared folder "C:\Data", create file "**ChangeALot**" in this folder, enter data, save. • Right-click **C:** drive, select **Configure Shadow Copies** • Click **Enable,** a warning pops up -> ignore this (as a low-use server), click Yes • Click Settings, we can set space to reserve for shadow copies, accept the defaults. • Click Schedule to schedule shadow copies. • Click Delete twice (to remove current schedule), New -> Schedule task: Daily, Start time: 8:00AM -> Advance, tick Repeat Task -> Every: 30 minutes, duration: 10 hours -> OK 3 times • *Create shadow copy*: Create Now -> Edit **ChangeALot.txt** file, Save. (2) • Previous versions -> right-click C: drive -> Restore previous versions (to recover all files on volume) • Right-click file -> Restore previous versions -> select older version-> Open -> recent changes are missing, we can either restore the file and overwrite current version or copy it with a new name to keep both versions.	• (1) Shadow copies reserve space for snapshots, default 10% of the volume size. When space runs out, older snapshots are deleted. • (2) Repeat this step for 2nd copy
Access-based enumeration	• DC1, Server Manager -> File and Storage Services (left pane) -> click Shares • Right-click Data -> Properties -> Settings -> Enable access-based enumeration • Pc201, reconnect to shared Data folder -> cannot see the file	
Install Windows Server backup	• DC1, Server Manager, Add roles and Features, skip to Select features page, scroll down, check Windows Server Backup -> Next, Install	
Perform backup once	• Sever Manager, Tools, Windows Server Backup • Local Backup (top-left), Backup Once (top-right), Next for 1st step of wizard. *Backup Data, Users folders:* • Select backup Configuration page, click Custom -> Select items -. expand Local disk (C:) -> checks Data, Users folder -> OK, Next *Tell backup software to backup our share:* • Click "Remote shared folder", enter UNC for backup share \\sWin22SVR1\Backup$	This performs backup over network to Mirrored Volume created on SVR1

	• **Inherit** should be selected as Access control, Next -> **Backup** to start the process, Close	
Configure NTFS Quotas	• SVR1, File Explorer, right-click mounted folder C:\Backups, create folder "*CentralFileStore*" -> share Everyone = FC • Right-click Backups (left), Properties • General tab, Properties -> Quota tab, "Enable quota management" should be checked. • Apply: "Deny disk space to users exceeding quota limit," "Limit disk space": 20MB, set warning limit: 15MB, check "Log events when users exceed their limit/warning level" -> Quota has been set up to limit all users (except Administrator) to 20MB. <u>*Configure individual quota for ITSnr:*</u> • Quota Entries button -> click menu item Quota -> New Quota Entry... for ITSnr -> Limit the disk usage: 300MB, warning level: 200MB • Logon to CL101 as ITJnr, use UNC path to the share folder • Copy some folder to CentralFileStore share • Load Event Viewer -> Windows Logs, System -> see NTFS source entries (event ID 36, 37) for ITJnr	• Event Viewer = **eventvwr.msc** • Event 36 - when user reaches the threshold • Events 37 - when user reaches the limit
Configure Service Recovery	• DC1 -> Start, type **Services.msc** -> Enter -> scroll down, right-click DNS Server -> Properties, Recovery tab • First and second failures: Restart the Service; Subsequent failures: Restart the Computer • Restart Computer Options button, ensure "Before restart, send this message" is enables -> Ok twice	
Configure Counter Logs	<u>*Real-time monitoring:*</u> • DC1, Start, Windows Administrative Tools, Resource Monitor -> overview of 4 primary sub-systems • Click Disk chart to view processes using the disk subsystem. • Click **Read (B/min)** to sort processes by disk read usage • Windows Administrative Tools, click Performance Monitor twice to get a real-	To observe the disk usage counter: • Open **cmd** -> **cd ** (change to root directory) -> **dir /s** (recursive directory) -> **CTRL+Z** or **CTRL+Break** to break the loop

	time, visual representation of **%Processor time** (counter) from **Processor** (performance object) • Top toolbar, click green plus icon, find object: **Physical Disk** -> add counter **%Idle Time** for **C:** drive -> double-click lines on the chart to change colour and width *Logged monitoring:* • Expand Data Collector Sets container -> right-click User Defined to create new Data Collector Set. • Name: SubsystemLog -> Create Manually (Advanced) -> Next • Select "Performance counter", Next and add desired counters -> sample interval: 3 secs -> accept default location for data storage -> Finish • Right-click **Subsystem Log** -> Properties, Schedule tab, create schedule so counter log starts in 5 mins. • Stop Condition tab, Overall duration: 2 minutes, Apply • Wait for the log to finish recording -> click Performance Monitor, View Log Data icon in toolbar (or CTRL+L) • Source tab -> **Log files:** add DataCollector01 from C:\Perflogs\Admin\SubsytemLog\000001 -> Ok • CTRL+N (or green plus icon) to add data for performance counters	
Restore file from backup	• Data folder, delete ChangeALot • Windows Server Backup, Recover... link in Actions -> This server -> click backup date to restore from, Next • Select recovery type, select Files and folders, Next • Expand DC1 container to find C:\Data\ChangeALot -> Next -> choose restore location e.g., Original	
Test Quota entry	• Delete files in CentralFileStore folder on SVR1 • Logon as the user with the quota entry (ITSnr) on client machine (CL101	

	• Copy a large file/folder from the local machine (C:\Program Files (x86)) to CentralFileStore share. • Event Viewer, System log on SVR1 to confirm that NTFS source entries (event ID 36, 37) are generated for user, indicating that they have reached or exceeded their quota limit or warning level.	
Task Manager	• DC1, CTRL+SHIFT+DEL -> Task Manager • Details tab to close non-responsive applications: right-click app name, End Task • Performance tab identifies CPU, memory, and network bottlenecks. • Run calc.exe, select View, Scientific, and calculate the factorial of 99999 to see CPU usage reach maximum. • While running the calculation, use the Details tab to set process priority to Low or end unimportant processes. • End calc.exe process to see CPU usage decrease.	

REFERENCES

Bertram, A 2020, 'Active Directory nesting groups strategy and implementation', *SearchWindowsServer*, viewed 18 May 2023, <https://www.techtarget.com/searchwindowsserver/tip/Active-Directory-nesting-groups-strategy-and-implementation>.

Bigelow, SJ & Kirsch, B 2021, 'What's the difference between Type 1 vs. Type 2 hypervisor?', *TechTarget*, viewed 9 March 2023, <https://www.techtarget.com/searchitoperations/tip/Whats-the-difference-between-Type-1-vs-Type-2-hypervisor>.

Brans, P 2023, 'What is the Universal Naming Convention? | A Definition from TechTarget.com', *WhatIs.com*, viewed 26 April 2023, <https://www.techtarget.com/whatis/definition/Universal-Naming-Convention-UNC>.

Harmoush, E 2021, 'Traditional ARP – Address Resolution Protocol', *Practical Networking*, viewed 17 March 2023, <https://www.practicalnetworking.net/series/arp/traditional-arp/>.

Hefner, K & Sullivan, E 2023, 'What is RAID 5? - Definition from WhatIs.com', *TechTarget*, viewed 14 May 2023, <https://www.techtarget.com/searchstorage/definition/RAID-5-redundant-array-of-independent-disks>.

Lee, G 2014, 'Minimum Frame Size - an overview | ScienceDirect Topics', *Science Direct* , viewed 17 March 2023, <https://www.sciencedirect.com/topics/computer-science/minimum-frame-size>.

Lutkevich, B & Boger, T 2021, 'What is Microsoft Active Directory Domain Services (AD DS)?', *SearchWindowsServer*, viewed 25 April 2023, <https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Active-Directory-Domain-Services-AD-DS>.

Morgan 2014, 'Group Policy: Account logon vs Logon events', *MorganTechSpace*, viewed 24 April 2023, <https://morgantechspace.com/2014/12/account-logon-vs-logon-events.html>.