LAB JOURNAL

Enterprise Network Server Administration

Abstract

This document serves as a lab journal for Enterprise Network Server 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: Implementing DNS & DHCP 3

Key concepts 3

Key configurations and commands 3

Further study 6

Lab 02: Installing and Configuring AD DS 6

Key concepts 6

Key configurations and commands 7

Further study 9

Lab 03: Implementing Distributed AD DS & Sites Replication 10

Key concepts 10

Key configurations and commands 10

Further study 13

Lab 04: Implementing Group Policy Infrastructure & Managing User Desktops with Group Policy 14

Key concepts 14

Key configurations and commands 14

Further study 17

Lab 05: Implementing a simple VPN solution 18

Key concepts 18

Key configurations and commands 18

Further study 19

Lab 06: Quota, File Screening using FSRM & Implementing DFS 20

Key concepts 20

Key configurations and commands 20

Further study 23

Lab 07: Configuring Network Load Balancing 24

Key concepts 24

Key configurations and commands 24

Further study 25

Lab 08: Implementing Update Management 26

Key concepts 26

Key configurations and commands 26

Further study 27

Lab 09: Implementing Active Directory Certificate Services........28
Key concepts........28
Key configurations and commands........28
Further study........30
Lab 10: Implementing Active Directory Right Management Services........31
Key concepts........31
Key configurations and commands........31
Further study........33

Lab 01: Implementing DNS & DHCP

Date: 09/03/2024

Key concepts

Domain Name System (DNS) has 3 zone types: **primary zone** (read-write copy of DNS zone), **secondary zone** (read-only copy), and **stub zone** (read-only subset copy of DNS zone - contains only SOA and NS records). Secondary zone can be used to load balance DNS queries and optimise the resolution performance. Additionally, **Active Directory-integrated zone** is used for DNS servers on Domain Controllers, storing zone data in Active Directory Domain Services (AD DS) rather than a traditional text zone file. This integration offers improved security and availability as the zone data is replicated among Domain Controllers. **Conditional Forwarder** and **Stub zone** optimise name resolution for regular access by a business partner.

DNS Zone Delegation is used to delegate subdomains to be hosted in different DNS server other than the parent domain. This delegation enhances DNS zone performance by distributing traffic across multiple servers.

Regarding Dynamic Host Configuration Protocol (DHCP) priority in terms of Option Type: the priority order is **Server**, **Scope**, **Class**, and **Reservation**. The latest configuration will take precedence in case of conflicts.

Key configurations and commands

Key steps	Details	Notes
Implementing DNS		
Create Reverse Lookup Zone	• Server Manager, Tools, DNS -> Right-click Reverse Lookup Zone -> New zone. • Select zone type -> enter Reverse Lookup Zone ID & IP address -> Accept other default values.	Reverse lookup zone resolves IP address to FQDN.
Create PTR record	• DNS Manager -> Reverse Lookup Zone -> right-click reverse zone -> New Pointer (PTR). • Type the server's IP address and FQDN (e.g., sWin16DC1.sWin.Local) in "Host IP Address" and "Hostname" fields respectively.	
Install DNS server role	• Server Manager -> Add roles and features -> Next -> check "DNS server" -> Add Features -> Install.	
Enable and configure Zone transfers	• On master DNS server, DNS Manager -> right-click Forward Lookup Zones, Properties • Zone Transfer tab, check "Allow zone transfer" -> select "Only to the following servers" -> Edit -> type secondary server's IP address under the box -> Enter -> OK • An error resolving secondary server IP addresses to their FQDN will not disrupt DNS functionality (since we have not created Reverse Lookup Zone). • Click Notify button -> type the secondary server's IP address under "The following servers" -> OK	Zone transfer occurs from master DNS servers to secondary DNS servers. 3 zone transfer options: • To any server • Only to servers listed on the Name Server tab (for secondary servers) • Only to the following servers

		(authorise each server individually)
Create secondary zone	• On secondary DNS server, DNS Manager -> right-click the zone -> New zone, Secondary zone -> enter zone name & master DNS server's IP address.	
Configure TTL, aging & scavenging	*Set minimum TTL*: • On primary DNS server, DNS Manager -> expand server name -> right-click domain name -> Properties, Start of Authority (SOA) tab -> Set Minimum (default) TTL value. *Set Aging and Scavenging value*: • DNS Manager, right-click DNS server's name -> Set Aging/Scavenging for All Zones -> Check "Scavenging stale resource records" -> review "No-refresh interval" & "Refresh interval" (default is 7 days) -> OK • Check "Apply these settings to the existing…." -> OK	Set TTL value to automatically flush resolved records from the DNS resolver cache upon TTL expiration. Aging and scavenging, which automate stale record cleanup, are **disabled** by default in DNS service.
Configure Conditional Forwarder	• On the partner company's DNS server: create a primary zone and add necessary records (e.g., MX, A, CNAME) • On company's DNS server: DNS Manager -> right-click Conditional Forwarder -> New Conditional Forwarder. • DNS Domain: Enter partner company's domain name. • Enter partner company's DNS server IP address.	
Test DNS Configuration	• On DNS client machine, open Windows PowerShell. *Verify DNS Queries*: confirm that the client is sending DNS queries to the intended DNS server: • Type **nslookup**. • Type **exit** -> press Enter to exit **nslookup.** *Verify SOA resource record for a domain zone*: • Type **resolve-dnsname -name Bume.com -type SOA** *Verify A Resource Record for an Application Server*: • Type **resolve-dnsname -name Lync-Svr1.Bume.com -type A** *Verify Alias (CNAME) for a Server*: • Type **resolve-dnsname –name <alias name e.g., SkypeServer.Bume.com> -type A**	
Implementing DHCP		
Install DHCP server role	• Server Manager, Add roles and features, Next, select DHCP Server role -> accept the defaults. • Back to Server Manager -> click yellow alert to open the DHCP post-install config wizard • *Authorise DHCP server with DC*: Authorisation page, accept defaults -> Commit. • Select "Alternate Credentials" if not already logged in as **domain admin**.	
DHCP scope and options	• Server Manager, Tools, DHCP, right-click IPv4 -> New scope	Do not forget post-deployment

	• Enter scope's name, IP address range, length, subnet mask, and exclusions range. • *Scope options*: Select checkboxes and input values (e.g., 03 Router for default gateway address or 015 DNS Domain Name) • Right-click the scope -> **Activate the scope**	configuration after DHCP role installation to avoid red arrow error.
Configure DHCP client	• Client machine's Ethernet adapter -> double-click Internet Protocol Version 4 (TCP/IPv4) • Select "Obtain an IP address automatically" and "Obtain DNS server address automatically" • Open Command Prompt, type **ipconfig /renew** • *Verify*: type **ipconfig /all**	
Configure reservation	• On DHCP server, DHCP manager, select Scope name -> right-click Reservations -> New reservation • Enter desired IP address and corresponding physical address (**without dashes**). • On DHCP client, **ipconfig /release** to release current IP address -> **ipconfig /renew** to verify the new reserved address.	Obtain DHCP client's MAC address using **ipconfig /all** command.
DHCP relay agent		
Install a DHCP relay agent	• On router, Server Manager, Tools, Routing and Remote Access • *Add DHCP relay agent to the router on the server*: expand RTR (local), IPv4 -> right-click General -> New routing protocol -> select "DHCP relay agent" from the list.	
Configure DHCP relay agent	*On local DHCP server:* • Right-click DHCP relay agent -> New Interface • Select Ethernet 2 (i.e., interface connected to end-devices, LAN network) -> OK twice. • Right-click DHCP relay agent -> Properties -> Add **DHCP server's IP address you want to relay requests to.** *On remote DHCP server:* • Create a new scope for network, configure Router options -> Activate the scope.	
Test DHCP relay agent	• *Stop DHCP service on the local DHCP server:* DHCP console -> right-click domain name -> All Tasks -> Stop • On client machine, Command Prompt, type **ipconfig /release** then **ipconfig /renew**	
Advanced DHCP settings – **Superscope**	• *Create a new extended scope*: On DHCP server, DHCP Manager -> click DHCP server's name -> right-click IPv4 -> New Scope -> enter scope details & scope options but do not activate it. • *Create a superscope*: right-click IPv4 -> New Superscope -> Next -> type the superscope's name -> Next	• DHCP scope that has **not** been activated yet will have **red down arrow** icon displayed. • A superscope is created when the

	• Select **Scopes** -> select old scope & new extended scope (hold **Ctrl** key) -> Finish.	current scope exhausts addresses, combining an extended scope with the old one to expand available addresses.
Create a user class	• *Add a user class*: Open DHCP, click on the DHCP server -> right-click IPv4 -> Define User Classes -> Add button -> name the user class and its ASCII value • *Add a policy*: Right-click Policies -> New Policy -> enter Policy Name -> Add • *Add Condition*: In the "Configure Conditions for the policy" -> Add button -> Set **Criteria** to User class, **Operator** to Equals, and Add **Value** to the name of the user class -> Add button. • Click Next -> set "**Vendor class**" dropdown list to **DHCP Standard Options** and configure desired DHCP options (e.g., default gateway & DNS domain name). • *Set classID for DHCP client:* On the DHCP client machine, open Command Prompt -> type **ipconfig /setclassid <NIC name (e.g., ethernet0)> "<User class ID e.g., SpecialProject>"** then **ipconfig /renew** to verify the class configurations • You can verify the DHCP classID on the DHCP client machine by typing **ipconfig /all** and look at the **DHCPv4 Class ID** line.	• The user class name ID (**ASCII**) should match the DHCP class ID string set on DHCP clients (when typing in the **ipconfig** command). It is case-sensitive. • Ensure DHCP client is set to **Obtain Ip address automatically.**

Further study

The Start of Authority (SOA) record in DNS identifies the primary server in DNS zone and it contains zone-wide settings, including TTL, aging, and scavenging. **TTL** value instructs the DNS client to automatically flush the record out of its cache once the TTL expires. **Aging** eliminates expired DNS records, maintaining the accuracy of the zone database. **Scavenging** further cleans up old records by grooming the DNS server resource records, cleaning up stale records that have not been removed through normal aging processes.

Lab 02: Installing and Configuring AD DS

Date: 16/03/2024

Key concepts

AD DS is a technology that allows organisations to centralise the Authentication, Authorisation, and Auditing (AAA) process from a single location. Authentication validates user identities; Authorisation controls their access levels to resources; and Auditing tracks and monitors user activities and resource usage. AD DS comprises both **physical** and **logical** components, and understanding their roles is essential for administrators to maintain smooth business operations.

The **AD Recycle Bin** feature allows for the recovery of accidentally deleted objects, such as user accounts. By default, this feature is disabled, requiring administrators to enable it to take advantage of its functionality. If the Recycle Bin is not enabled and an object is deleted, administrators may need to perform a non-authoritative or authoritative restore from backup media, potentially causing downtime.

Key configurations and commands

Key steps	**Details**	**Notes**
Install ADDS	• Server Manager, Add roles and features, select ADDS role -> accept default settings. *Promote a machine to be a new DC*: • Server Manager, yellow alert symbol -> Promote this server to be a DC • On “Deployment Configuration”, ensure “Add a DC to an existing domain” is checked, **Domain** field is filled with sWin.local -> Next -> accept default options for installing DNS server and GC -> Type DSRM password (i.e., Pa55w.rd) -> Next • On “Prerequisites Check” page, verify “All prerequisite checks passed successfully” -> Install -> the computer will restart.	
Install and configure RODC	*Verify RODC installation requirements:* • On DC1, Server Manager -> Tools -> Active Directory Users and Computers • Right-click domain name -> Raise domain functional level -> ensure that “Current domain functional level” is set to “Windows Server 2016” -> Cancel *Pre-stage a computer account for the new RODC*: • Expand domain name -> right-click **Domain Controllers** container -> Pre-create Read-only Domain Controller account • In “Active Directory Domain Services Installation Wizard”, click Next twice to accept current credentials • Enter **RODC server’s name** (e.g., sWin22SVR3) in the “Computer name” field -> Next • Click Next on both “Select a site” and “Additional Domain Controller options” pages *Delegate local admin permission on RODC to user:* • On “Delegation of RODC installation and Administration” page, type **username or group with users permitted to attach the server to the RODC computer account** (e.g., sWin\Apple) -> Next -> Finish *Install RODC on target server:* • On to-be RODC server (e.g., SVR3), Server Manager, Add roles and features -> add AD DS role -> Accept default settings -> Promote this server to a DC • **Domain** field: enter domain name (swin.local) -> Change button (for “No credentials provided”) -> type **above username (user that is allowed to attach RODC)** for Username -> OK -> Next	The **minimum** domain functional level for RODC support is Windows Server 2003.

	• "Domain Controller Options" page, ensure "Use existing RODC" is selected. • "Type the DSRM password": enter password and confirm password -> Next • "Additional Options": "Replicate from" dropdown, choose DC1 (i.e., DC as the replication source) -> Next 3 times -> "Prerequisites Check" page, Install -> RODC will restart	
Configure password replication policy	*Verify default settings*: • On DC1, DSA -> click **Users** container -> double-click "Allowed RODC Password Replication Group" -> Members tab -> verify nothing is listed. • Click **Domain Controllers** container -> right-click RODC's name -> Properties -> Password Replication Policy tab -> verify that both "Allowed RODC Password Replication" and "Denied RODC Password Replication" groups are listed. • *Create a Global security group for branch users* -> add relevant users and computers to this group *Configure Password Replication Policy for the RODC*: • On DC1, DSA, navigate to **Domain Controllers** OU -> right-click RODC's name -> Properties -> **Password Replication Policy** tab -> double-click "Allowed RODC Password Replication Group" -> Members tab -> Add the branch user Global group & computer (check Computer as object type when searching) -> Check names -> Apply *Evaluate the resulting policy, to ensure correct settings for specific users and administrators*: • On "Password Replication Policy" tab -> click Advanced -> Resultant Policy tab -> Add a user in branch users Global group -> Check names -> OK -> confirm that the Resultant Setting for that user is *Allow* -> Clear • Add **Administrator** -> Check Names -> OK -> confirm that the Resultant Setting is *Deny (explicit)* *Test authentication and caching*: • Sign out of the branch computer (also in the Global security group, e.g., CL101) -> sign in as branch user (e.g., swin\Apple) • *Confirm password caching on the RODC*: On writable DC, RODC's name Properties tab -> Password Replication Policy tab -> Advanced -> verify that user's password has been cached on RODC (click the dropdown list) *Prepopulate credentials*: • On RODC's Properties, "Password Replication Policy" tab -> Advanced -> Prepopulate Passwords -> type user & computer accounts whose credentials should be cached without prior authentication -> Check names -> OK -> Yes -> OK	2 methods for authenticating on an RODC: 1. Authenticate user and computer credentials with a writable DC before caching. 2. Prepopulate credentials without prior DC authentication.
Configure Password Policy and Account lockout settings		

Configure a domain-based password policy (GPO)	- DC1, GPMC -> edit Default Domain Policy -> **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy** -> configure necessary settings	Domain-wide policies (*Default Domain Policy),* apply to **all domain users**.
Configure domain-based account lockout policy (GPO)	- DC1, GPMC -> edit Default Domain Policy -> **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy** -> configure necessary settings	
Configure a fine-grained password policy (PSO)	- Server Manager, Tools, Active Directory Administrative Centre -> click local domain name (*sWin (local)*) -> double-click **System** container -> right-click **Password Settings Container** -> New -> Password Settings - "Create Password Settings", create a new PSO with desired settings. - "Directly Applies To": add Global security group -> Check Names.	To accommodate **varying password policy needs for different user groups**, Windows Server 2008 domain functional level introduces **Password Settings Objects (PSO)**.
AD Recycle Bin		
Enable AD Recycle Bin	- Active Directory Administrative Centre, click local domain name (*swin (local)*) -> click **Enable Recycle Bin** -> OK to refresh ADAC - Press F5 to refresh ADAC.	Once enabled, Recycle Bin **cannot** be disabled.
Create and delete test users	- ADAC, click *swin (local)* -> double-click **Users** container -> click **New** (in Tasks pane) -> click User -> create 2 new users - Delete the 2 users by right-click them -> Delete -> Yes	User account deletions will be replicated to all DCs within the domain.
Restore deleted users	- ADAC, click *swin (local)*, double-click **Deleted Objects** -> right-click the deleted users -> **Restore** (restore accounts to their **original location**) or optionally, **Restore To** (recover account to a different OU)	

Further study

RODCs provide authentication services in locations lacking physical security, with a read-only copy of the Active Directory database. Authentication on an RODC occurs via two methods: **caching user and computer credentials** (requiring prior authentication by a writable DC) or **prepopulating credentials** (the preferred method). Managing cached credentials involves setting up a **Password Replication Policy** and employing two Domain Local groups: **Allowed RODC Password Replication Group** (initially empty) and **Denied RODC Password Replication Group** (with default members: Domain Admins, Enterprise Admins, and Group Policy Creator Owners).

Lab 03: Implementing Distributed AD DS & Sites Replication

Date: 23/03/2024

Key concepts

A domain is an administrative unit for managing users, computers, and other objects. Implementing a distributed AD DS infrastructure with child domains allows for efficient management of resources across different regions or branches within an organisation. Trust relationships must be established between forests before allowing access to resources between businesses. There are 3 levels of trust authentication: **Forest-wide authentication**, **Domain-wide authentication**, and the most restrictive **Selective authentication**, which permits only certain users from *Trusted forests* to access specific server resources in the *Trusting forest*.

AD DS site is a logical grouping of multiple IP subnets connected by low-latency, reliable links. It serves 2 main purposes: to provide localised services and to manage replication for DCs within a forest. It can also be used for group policy application. A **Site Link Bridge** is used when the IP network is not fully routed so it is used for failover and redundancy and used for more control over replication.

Key configurations and commands

Key steps	Details	Notes
Deploying a new child domain		
Install AD DS on the new child domain's DC	• *On parent domain's DC*: ensure the DC's **Ethernet** adapter is showing the domain name. Otherwise, Right-click **Ethernet** adapter -> Disable -> Enable • On the designated child DC, install ADDS role *Promote to be the first DC in the new child domain (on child domain's DC)*: • Select "Add a new domain to an existing forest"; Domain type: Child Domain, specify Parent domain name • **Select** button (next to "Domain") -> "Credentials for deployment option", login as **swin.local\Administrator** -> select **swin.local** • Provide new domain name: child's domain name (e.g., Wantirna) • Domain functional level: Windows Server 2016 • Check both DNS and GC options • Enter DSRM password and accept default settings.	• Child domain DC defaults to **Default-First-Site-Name** if AD DS Sites not implemented. • Ensure child DC's DNS is pointing to DC1. • **Existing DCs within the forest and the Router need to be up first.**
Verify new child domain & DC deployment	*Confirm DC status:* • Log in to the new DC as **Wantirna\Administrator** • Server Manager -> Local Server -> verify **Domain** is the child domain name (Wantirna.sWin.Local) • Network Connections -> ensure "Ethernet" shows "sWin.Local". Otherwise, Disable then Enable it *Validate trust configuration between parent-child domain*: • Active Directory Domains and Trusts -> navigate to the **Properties** of the child domain -> **Trusts** tab.	

	• Confirm two-way trust relationship with parent domain (swin.local) under "**Domain trusted by this domain (outgoing trusts)**" and "**Domain that trusts this domain (incoming trusts)**"	
Implementing Forest Trusts		
Configure DNS name resolution	*For one forest, create a **Conditional Forwarder** pointing to the DNS server of the other forest:* • On sWin22DC1, launch DNS -> right-click Conditional Forwarder -> specify DNS domain (Training.edu) & master server to the IP address of the other forest's DNS server (TRN16DC1's IP address) *For the other forest, create a **Stub zone** pointing to the first forest's DNS server:* • On TRN16DC1, launch DNS -> new Stub zone -> AD zone replication scope: "**To all DNS servers running on DCs in this forest**: Training.Edu" -> Swin's domain name as Zone name -> IP address of Swin forest's DNS server as "Master server"	To enable forest trust creation, **both companies' DNS** setups must facilitate DNS requests between their forests, achievable via **Conditional Forwarder** OR **Stub zone.**
Configure one-way forest trust with **selective authentication**	*Configure outgoing forest trust:* • On trusting domain's DC, launch "AD Domain and Trusts" -> right-click domain name, Properties, Trusts tab -> New trust • Domain name: trusted domain name -> Trust type: Forest trust -> Direction of Trust: One-way: outgoing -> Sides of trust: "Both this domain and the specified domain" -> provide **Administrator**'s credentials for Username & Password -> Outgoing trust authentication level: Local Forest Selective authentication -> accept default settings. *Validate newly created trust:* • In trusting domain's Properties -> Trust tab -> under "Domains trusted by this domain (outgoing trusts)" -> click trusted domain -> Properties -> Validate -> should have "The trust has been validated. It is in place an active" message.	**Trusted** domain can access **Trusting** domain's resources. Therefore, the trusting domain needs to establish an **outgoing** trust to the trusted domain.
Configure server for selective authentication	*Explicitly configure trusted users the right to authenticate at trusting domain's resource server:* • On trusting domain's DC, DSA -> Computer container -> right-click the **resource server** -> Properties -> Security tab -> Add -> click Locations -> choose the trusted domain's name -> OK • In "Enter the object name to select", type Global security group's name in the trusted domain that requires access to resources (G_IT) -> Check names -> enter trusted domain's Administrator credentials -> OK twice. • In the resource server's Properties, click Global group -> check Allow in "**Allowed to authenticate**", OK.	If cannot see **Security** tab in the computer's Properties -> View menu -> **Advanced Features**.

Test forest trust configuration	*Create data on the resource server:* - On resource server (in trusting domain), File Explorer -> Create a folder in C drive -> right-click the folder -> Share with, Specific People -> In "File Sharing" dialog box, type trusted domain's Global group -> Add -> click Read/Write -> Share -> Done. *Test access to resources*: - Sign in as Trusted domain's user, who is a member of the IT group (Training\Alice) on trusted domain's computer -> File Explorer, enter UNC path to shared folder (\\ResourceServer\SharedFolder) -> user should be able to create and view files.	
AD DS Sites		
Modify default site	- On DC, ensure Ethernet adapter displays domain name. Otherwise, right-click Ethernet -> Disable -> Enable. - AD Sites and Services -> expand Sites -> right-click **Default-First-Site-Name** -> Rename -> type site's new name.	
Create new site	- AD Sites and Services -> right-click Sites -> New site -> type the new site's name - Select a site for this site: DEFAULTIPSITELINK -> OK	**DEFAULTIPSITELINK** is the default site link for all sites, with default Cost of 100, Replication interval of 180 minutes. It is used for inter-site communication.
Create subnets for sites	- AD Sites and Services -> right-click Subnets -> New Subnet… - Enter subnet range used for computers in a location in the **Prefix** box - Select a site object for this prefix: click the according site (e.g., HQ) - When installing a new DC for the newly created site, choose newly created **site name**. -> To verify: AD Sites and Services -> expand the new site -> expand **Servers** -> verify that the new DC is in the site.	**Subnets connected by fast links are typically consolidated within a single site.** If DCs were deployed before implementing Sites, manual allocation to appropriate sites based on their IP addresses is needed.
Site replication between 2 sites	- On a site's DC, AD Sites and Services -> expand Sites, **Inter-Site Transports** -> right-click **IP** -> New Site Link - Enter site link's name (HQ-Branch) - Ensure both sites are included in "Sites in this site link" -> OK.	In "Change Schedule," mark the time range and select "Replication Not Available" to prevent replication during specific

	• Right-click newly created Site Link -> Properties -> change value of “Replication Every”, “Change Schedule” accordingly.	times, like business peak hours.

Further study

A particular **Forest/Domain Functional Level** is required to have certain domain/forest-wide features. The functional level is determined by the **lowest** version of the Operating System running on the DCs, with the lowest version determining the highest functional level. Currently, Windows Server 2016 is the most recent forest/domain functional level.

For facilitating authentication and resource **access between an AD DS domain and a non-Windows Kerberos v5 realm**, **Realm Trust** is employed. To **improve performance** during authentication and resource access **within an internal forest**, **Shortcut Trust** is used, enabling direct authentication between child domains of different trees.

Lab 04: Implementing Group Policy Infrastructure & Managing User Desktops with Group Policy

Date: 30/03/2024

Key concepts

Group Policy Object (GPO) is extensively used in businesses and organisations for **security enforcement** and **desktop standardisation**. It allows administrators to restrict access to certain programs, hide specific tools or software, and enforce desktop configurations such as wallpaper settings and folder redirection.

Starter GPOs are templates storing Administrative Template settings for creating new GPOs. They're ideal for junior administrators and can be exported to .cab files for easy replication via GPMC.

By default, GPO applies User Configuration based on the user's location in AD DS. To change this and base settings on the computer object's location, use **Loopback Processing** in Group Policy. This feature allows administrators to control computer behaviour based on location, useful for scenarios like kiosks or public library computers. It offers two modes: **Replace** (ignores and replaces user configurations) and **Merge** (combines user and computer settings).

Key configurations and commands

Key steps	Details	Notes
Create and configure GPO		
Enable/Disable Screen Saver	• On DC, GPMC -> right-click Group Policy Objects -> New -> enter GPO's name • Edit the GPO -> **User Configuration\Policies\Administrative templates\Control Panel\Personalisation** -> double-click **Screen saver timeout** -> Enable/Disable -> OK	Remember to **apply/link** GPO to Site, Domain or OU after creation.
Prevent running a program/software	• GPMC, right-click Group Policy Objects -> New -> enter GPO's name ->edit the GPO -> **User Configuration\Policies\Administrative Templates\System\Don't run specified Windows applications** -> Enabled • Under "**Options: List of disallowed applications**" -> Show -> Value: type the program, (e.g., notepad.exe) -> OK twice	
Managing GPO scope	*<u>Option 1: apply an opposite GPO to the Exception OU:</u>* • Link the opposite GPO to the narrower scope (e.g., OU has a narrower scope than Domain) *<u>Option 2: Create an exception for the Exception group:</u>* • GPMS, Click the desired policy -> Delegation tab -> Advanced -> Add -> type the Global security group (e.g., G_IT) under "Enter the object names to select" -> Check Names -> OK • Permission for Global group: **Deny Apply Group Policy**	• In this example, the Exception Group is exempted from GPO application. • Ensure Global group has Read

		permission. Deny.
Verify/ Troubleshooting GPO	*Option 1: Login as user* • Log in to the domain member computer as designated user. Ensure computer is activated and log in as a domain admin first to prevent errors. • Start icon -> search for Lock screen -> click “Screen saver settings”. Notice various fields are disabled, indicating that changes cannot be made. *Option 2: Group Policy Modelling:* • GPMC, right-click Group Policy modelling -> Select User -> Browse -> type the username -> Check Names -> OK -> Finish • Review Group Policy modelling page for the user -> Details tab. Notice GPOs listed under the Denied/Allowed GPOs list. • *Save the report*: right-click the page -> Save Report -> Save	This example verifies whether Screen Saver settings are enabled or not.
Apply GPO immediately	*Option 1:* • For User Configurations, logout and login as domain user. • For Computer Configurations, restart the computer. *Option 2:* • On domain member computer, Command Prompt (Run as Administrator), use domain admin’s credentials, type **gpupdate /force** (to reapply **all** settings).	
Loopback Processing	• GPMC, right-click the OU -> Create a GPO in this domain, and Link it here -> type GPO’s name • Edit the GPO -> **User Configurations\Policies\Administrative Templates\Control Panel\Personalization** -> configure necessary settings • **Computer Configurations\Policies\Administrative templates\System\Group Policy** -> Double-click “**Configure user Group Policy Loopback processing mode**” -> Enabled -> Choose Mode (Replace/Merge) • DSA, move the computer account to the applied OU • Either **restart the computer** or run **gpupdate /force** as Domain Administrator -> verify that Loopback policy settings override normal GPOs (e.g., Wait time of Screen saver is 27000 seconds instead of 600 seconds).	In Merge mode, non-conflicting User Configuration settings from other GPOs still apply.
Implementing drive mappings by GP preferences	• *Create a shared data folder*: DC1, File Explorer -> create new folder in (C:) -> right-click the folder (IT_Data) -> Share with, Specific people -> drop-down list: Everyone -> Add -> Permission: Read/Write -> Share -> Done -> add software package (.msi) to the folder. *Create GPO to map network drive for the users*:	

	• DC1, GPMC, right-click the OU -> create a GPO and link -> type GPO's name (IT-MapDrive) -> right-click the GPO -> Edit -> **User Configuration\Preferences\Windows Settings** -> right-click Drive Maps -> New -> Mapped Drive • In "New Drive Properties", Action: Create • Location: type UNC path to shared folder created above -> Drive: Z -> OK *Create GPO to create Shortcut for all Domain users:* • DC1, create and link GPO (e.g., Notepad Shortcut) to the domain -> **User Configuration\Preferences\Windows Settings** -> right-click Shortcuts -> New -> Shortcut -> Action: Create; Name: Notepad; Location: Desktop; Target path: C:\Windows\System32\Notepad.exe • **Common** tab, check Item-level targeting -> Targeting -> New Item -> Security Group -> click (…) button next to Group -> type Global group (e.g., G_IT) -> OK. *Test the Preferences:* • On domain member computer, sign out and sign in as member of G_IT group -> verify the Notepad shortcut on user's Desktop. • Open File Explorer, This PC -> verify Z: drive mapped to shared folder (e.g., \\sWin22DC1\IT-Data)	
Folder Redirection	*Create a shared data folder to store redirected folders:* • DC1, File Explorer -> Create a new folder in (C:) (IT-Redirect) -> right-click folder -> Share with, Specific people -> Add Everyone -> Permission: Read/Write -> Share -> Done. *Create GPO to redirect IT users's Document folders:* • DC1, GPMC, create a GPO and link it to IT OU (IT-Redirect) ->edit the GPO -> **User Configuration\Policies\Windows Settings\Folder Redirection** -> right-click Documents -> Properties -> Target tab -> Setting: Basic – Redirect everyone's folder to the same location -> Target folder location: Create a folder for each user under the root path -> Root Path: UNC path to the shared folder (\\sWin22Dc1\IT-Redirect) -> OK. *Test Folder Redirection:* • Sign out and sign in to domain member computer as G_IT user -> File Explorer -> right-click Documents -> Properties -> verify location of folder is now the network share located in a subfolder named after the user (sWin22DC1\IT-Redirect\Irene).	
Deploy software by using Group Policy	*Create GPO to deploy XML Notepad:* • DC1, GPMC -> create and link a GPO to domain (Deploy XML Notepad) -> Edit -> **Computer**	

	Configuration\Policies\Software Settings -> right-click Software installation -> New -> Package -> browse to the shared folder that contains **.msi** file -> Open • Deploy Software: Assigned mode. • *Verify XML Notepad was deployed:* On domain member computer, right-click Start -> Shutdown/sign out -> Restart -> sign in as domain member -> verify that XML Notepad 2007 is on user's Desktop.	

Further study

If a particular OU has **Block Inheritance**, all GPOs linked to its parent OU will be ignored, although this can be overridden with **Enforcement** at the parent level. By default, **without Enforcement**, GPOs are applied in the order of **LSDON (Local, Site, Domain, parent OU, and nested OU),** with the last applied GPO wins when there are settings conflicts.

When **Enforcement** is applied, **the order of GPO application** is reversed: **nested OUs, parent OU, Domain, and Site**. When performing exercises asking for the **order of application**, it's important to consider the **GPO link set without enforcement** first, followed by the **GPO link set with enforcement**.

Lab 05: Implementing a simple VPN solution

Date: 13/04/2024

Key concepts

A **Virtual Private Network** (VPN) is a remote access service that establishes point-to-point connections over a public network like the Internet, providing authentication, encryption, and encapsulation. Common **VPN tunnelling protocols** include **PPTP**, **L2TP/IPsec**, **SSTP**, and **IKEv2**. **Authentication protocols** for VPNs include **PAP**, **CHAP**, **MS-CHAPv2**, and **EAP** (strongest security).

Organisations can streamline VPN deployment and management with the **Connection Manager Administration Kit (CMAK)**. It simplifies VPN profile creation, packaging predefined connections on remote servers as executable files. This minimises help desk requests, reduces user errors, and expedites problem resolution through standardised configurations.

DirectAccess (DA) is an alternative to VPN, offering seamless remote access where clients can not differentiate between local and remote resources. **DA tunnelling options** include **ISATAP**, **6to4**, **Teredo**, and **IP-HTTPS**.

Another option for remote access is **Web Application Proxy** enables Internet users to access internal web applications without deploying VPN or DA.

Key configurations and commands

Key steps	Details	Notes
Configuring Routing and Remote Access Service (RRAS) – VPN server	• *Disable router function*: On RTR (i.e., VPN server), Server Manager -> Routing and Remote Access -> right-click swin22RTR -> Disable Routing and Remote Access -> Yes • Right-click swin22RTR -> Configure and Enable Routing and Remote Access -> Next -> Remote Access (dial-up or VPN) -> Next -> select VPN check box -> Next -> clear “Enable security on the selected interface…” • Select external interface (VPN client-facing -> Next -> select internal interface (for corporate network) -> select “From a specified range of addresses” -> Next -> New -> enter address range for VPN clients (172.16.32.200-249) -> OK -> Next. • Managing Multiple Remote Access Servers: Keep default “No, use Routing and Remote Access to authenticate connection requests” to use VPN server (not RADIUS server) to authenticate -> Next -> Finish. • Ignore DHCP relay warning as IP addresses for VPN clients have been manually assigned.	In "Managing Multiple Remote Access Servers," we can configure the VPN server as a RADIUS client to specify DC for authentication.
Configure Network Policy	• On VPN server, Routing and Remote Access -> right-click **Remote Access Logging & Policies** -> Launch NPS • *Disable the two default policies*: In NPS (local), click Network Policies -> right-click each policy with red cross -> Disable. *Configure new policy for VPN connection:*	• This is to allow remote connection. • PPTP is the simplest tunnelling

	• Right-click Network Policies -> New -> type Policy name (e.g., SimpleVPN) -> Type of network access server: Remote Access Server (VPN-Dial up) -> Next • Create a tunnel for encryption: On "Specify Conditions", Add -> select **Tunnel Type** -> Add. • Specify Access Permission page, ensure "Access granted" is selected. -> Next • Configure Authentication Methods: clear MS-CHAP, only keep MS-CHAP-v2 -> Next • Configure Constraints: can set restrictions on when users can connect remotely -> Next. • Configure Settings: can add restrictions for VPN users, like limiting access to protocols such as HTTP using IP filters. -> Next -> Finish.	protocol, does not require certificates. • Common configurations may include adding conditions, such as Windows or User Groups, to restrict VPN access to specific users.
Configure VPN client	• On PC, Control Panel -> Network and Internet -> Network and Sharing Centre -> Set up a new connection or network -> Next -> Connect to a workplace -> Next -> Use my Internet connection (VPN) -> I'll set up an Internet connection later • On "Connect to a Workplace", enter IP address of VPN server's interface facing the VPN client -> give the VPN a unique name -> Create *Configure VPN authentication:* • Network and Sharing Centre, Change adapter settings -> in "Network Connections", right-click the newly created VPN connection -> Properties -> Security tab -> Type of VPN: PPTP -> Allow these protocols -> ensure only MS-CHAP-v2 is selected -> OK *Connect to VPN server from VPN client:* • Right-click the VPN connection -> Connect/Disconnect -> In "Settings", click the VPN connection -> Connect -> enter admin's credentials. • Open CMD, type **ipconfig /all** -> the VPN client's IP address should change to the one assigned in corporate network • *Test*: Ping DC1's IP	

Further study

Network Policy Server (NPS) acts as a centralised location for AAA purposes, operating either as a **RADIUS server** or **proxy**. When functioning as a **RADIUS server**, NPS centralises AAA, whereas a **RADIUS proxy** acts as an intermediate between the RADIUS clients and RADIUS servers. The **RADIUS clients** are the **network access points** such as Remote access servers (VPN, or DA), wired/wireless access points. **NPS policies**, comprising **Network Policies** and **Connection Request Policies**, determine access privileges and the processing of connection attempts. **Network Policies** control whether access should be granted or denied, while **Connection Request Policies** control how servers handle incoming connection requests from remote clients.

Lab 06: Quota, File Screening using FSRM & Implementing DFS

Date: 20/04/2024

Key concepts

Distributed File System (DFS) organises multiple distributed SMB file shares into a unified file system on Windows servers. With DFS, users can access shared folders without needing to remember server locations, as DFS transparently manages replicas across multiple servers, ensuring redundancy and accessibility. DFS consists of two primary technologies: **DFS Namespace** and **DFS Replication**.

File Server Resource Manager (FSRM) facilitates capacity management on file servers, providing control over the quantity and types of data stored. Its key features include:

1. **Quota management**, allowing for the limitation of disk space allocated to volumes or folders with options for **hard** or **soft quotas**.
2. **File screening**, enabling the determination of allowed or blocked file types or extensions.
3. **Storage reports** for comprehensive insights into storage usage.
4. **File classifications** for organising and categorising files based on predefined criteria (e.g., large files, files have expired after a year).
5. **File management tasks** to automate administrative actions (e.g., archiving files that have remained unused for one year).

Key configurations and commands

Key steps	Details	Notes
Install FSRM role & Create testing folders	• *Install FSRM role:* On SVR1, Server Manager, Add roles and features -> on “Select server roles”, expand “File and Storage Services” -> Files and iSCSI Services -> select File Server Resource Manager -> Add Features -> Install • *Create a new Simple Volume*: on SVR1, Server Manager, Tools, Computer Management, Disk Management -> “Details” pane, right-click “Disk 1” -> Online -> right-click Disk 1 -> Initialise Disk -> right-click “Unallocated” next to Disk 1 -> New Simple Volume -> Next -> “Specify Volume Size in Mb”: 500 -> “Volume Label”: Data -> Finish • *Create Data folder for testing*: File Explorer -> This PC, Data (E:) -> New folder -> name: Users -> right-click Users folder -> Share with -> Specific people -> drop-down list: Everyone -> Add -> Permission: Read/Write -> Share.	
Configure FSRM Quotas	• *Create quota template:* SVR1, Server Manager, Tools, File Server Resource Manager -> expand Quota Management, right-click Quota Templates -> Create Quota Template -> Template name: “100Mb Limit Log to Event Viewer” -> Add (Notification thresholds) -> Event log tab -> check “Send warning to event log” -> “Generate notification when usage reaches (%)”: 100 -> OK.	
	Configure a Quota based on the Quota template: • FSRM console, Quotas -> right-click -> Create Quota -> Quota path: E:\Users -> select “Auto apply template and	

	create quotas on existing and new subfolders" -> "Derive properties from this quota template (recommended)": select the quota template -> Create -> "Details" pane: verify "E:\Users\*" quota entry (refresh as needed) • File Explorer -> Users folder -> create a new folder (e.g., Max) -> FSRM console, Action menu -> Refresh -> Details pane, Max should appear. *Test Quota*: • SVR1, CMD, type: **E:** -> **cd \Users\Max** -> **fsutil file createnew file1.txt 89400000** (generates a file exceeding 85 MB, triggering a warning in Event Viewer) • Server Manager, Tools, Event Viewer -> expand Windows Logs, Application -> Details pane, **Event ID 12325.** • CMD, type: **fsutil file createnew file2.txt 16400000** -> error: file cannot be created (since it exceeds quota limit) -> Event Viewer, **Event 12325** (100% exceeded quota)	
Configure File Screening	• *Create a file screen:* SVR1, FSRM, expand File Screening Management -> File Screens -> right-click -> Create File Screen -> "File screen path": E:\Users -> "Derive properties from this file screen template (recommended)": "Block Audio and Video Files" -> Create. *Create file group:* • SVR1, FSRM, right-click File Server Resource Manager (Local) -> Configure Options, File Screen Audit tab -> check "Record file screening activity in auditing database". • FSRM tree, right-click File Groups -> Create File Group -> File group name: "MPx Media Files" -> Files to include: *.mp* -> Add -> Files to exclude: *.mpp -> Add. • FSRM tree, File Screen Templates -> right-click Block Audio and Video files -> Edit Template Properties -> Settings tab, File groups, uncheck "Audio and Video files", check "MPx Media Files" -> OK -> Yes. • *Test file screen*: SVR1, File Explorer, View menu -> check "File name extensions" -> Data (E:) -> right-click -> create a new .mp3 (rename txt file) -> copy this file to E:\Users\Max folder -> should be unable to copy file • Event Viewer, **event ID 8215** – file saved by user is not permitted	• Configure file screening to block media files within user home folders while permitting unrestricted storage of Microsoft Project files (.mpp) in those directories. • File group to specify included files for file screening.
Generate Storage Reports	• *Generate on-demand storage report:* FSRM, Storage Reports Management -> right-click -> Generate Reports Now -> "Select reports to generate": File Screening Audit -> Scope tab -> Add -> Browse for Folder: E:\Users -> OK -> a HTML report is generated.	
DFS		
Install DFS role	• *Install DFS role on both SVR1 and SVR4:* Server Manager, Add roles and features -> expand "File and Storage	

	Services", "Files and iSCSI Services" -> select "DFS Namespaces" and "DFS Replication" -> Install.	
Configure domain-based DFS namespace	• *Create domain-based namespace:* on SVR1, Server Manager, Tools, DFS Management -> right-click Namespaces -> New Namespace -> Server: type first Namespace server's name -> Next -> Namespace Type: "Domain-based namespace" -> ensure "Enable Windows Server 2008 mode" is chosen -> Next -> Create • *Add another namespace server (SVR4):* right-click namespace -> Add Namespace Server -> Server: type sWin22SVR4 -> OK • *Enable access-based enumeration for BranchDocuments namespace:* navigation, Namespaces -> right-click the namespace -> Properties -> Advanced tab -> check "Enable access-based enumeration for this namespace". • *Add **DataFiles** folder to namespace on SVR1:* DFS Management, right-click namespace -> New Folder -> Name: DataFiles -> Add -> **Path to folder target:** type \\swin22SVR1\DataFiles as folder target -> OK -> Yes for warning -> Local path of shared folder: C:\BranchDocuments\DataFiles -> click "All users have read and write permission" -> OK -> Create some files in this folder target. • *Add **ResearchTemplates** folder to namespace on SVR4*: same as above • *Verify namespace*: on DC1, File Explorer -> address bar: \\swin.local\BranchDocuments\ -> both folders should be there • *Create second folder target for both DataFiles & ResearchTemplates:* SVR1, DFS Management, right-click **DataFiles** -> Add folder target -> same as before but on different namespace server (SVR4).	
Configure DFS replication	• Once add folder target for **DataFiles**, Replication dialogue box -> Yes -> "Replication Eligibility" page, select both folder targets -> Primary Member: select SVR1 -> Topology: Full mesh -> Create -> do the same for **ResearchTemplates** folder. *Verify DFS replication:* ***Method 1: via File Explorer*** • DC1, File Explorer, right-click Network, Map network drive -> type \\SWin.Local\BranchDocuments -> Finish. • Right-click namespace (BranchDocuments), Properties -> DFS tab -> Referral list: should have 2 *Active* servers. ***Method 2: via DFS console (can also force replication now)*** • SVR1, DFS Management, expand Replication, click any folder -> Connections tab -> Sending Member: swin22SVR1 to swin22SVR4 -> Replicate Now -> Override	• Replication group ensures synchronisation of folder targets. • All namespace servers are equal once the replication group is established (no primary server).

	schedule -> OK -> Verify file replication on both namespace servers from both folders.	

Further study

BranchCache is used to cache information on branch computers or local servers, particularly documents accessed from local branch offices. This technology resolves the issues encountered by users accessing files over **slower WAN links in branch offices with limited connectivity and infrastructure**, leading to delays when opening files. Moreover, **BranchCache** is preferred over DFS in situations where **physical security cannot be guaranteed**. BranchCache operates in two modes: **Hosted Cache** and **Distributed Cache**.

Lab 07: Configuring Network Load Balancing

Date: 27/04/2024

Key concepts

Network Load Balancing (NLB) provides fault tolerance and improved performance by transparently distributing traffic among multiple servers using virtual IP addresses and a shared name. NLB is most effective when applied to **stateless applications** like **web servers**. NLB offers three cluster operation modes: **unicast** (assigns the same MAC address to all hosts, potentially causing layer 2 problems), **multicast** (each host has two MAC addresses including the original and shared virtual MAC address, potentially causing layer 3 routing issues), and **IGMP multicast** (similar to multicast mode, but uses IGMP to handle multicast traffic more efficiently).

Failover clustering comprises a group of two or more computers (nodes) running the same application, functioning as a single entity to deliver high availability and scalability to clients. In the event of a node failure, another node takes over to provide services. Failover clustering is typically best suited for **stateful applications relying on a single data source**. Examples of stateful applications include **database applications, file servers,** and **DHCP services**.

Key configurations and commands

Key steps	Details	Notes
Install IIS role & NLB feature	On all NLB nodes, Server Manager, Add roles and features, install **IIS role** and **NLB feature.**	
Configure NLB cluster	• On NLB node (SVR1), launch Network Load Balancing Manager, right-click Network Load Balancing Clusters -> New cluster -> Host textbox: sWin22SVR1. • Select interface with virtual IP address and receive client traffic to load balance: Ethernet (172.16.32.11), Next. • Set a unique host identifier (Priority). • Add the shared cluster IP address and subnet mask (e.g., 172.16.32.40/24). Ensure that IP addresses are static as NLB disables DHCP on configured interfaces. • Full Internet name: specify the cluster name and choose the appropriate operation mode (Multicast). Port rules -> Next • *Add second host to the cluster:* NLB manager, expand Network Load Balancing Clusters, right-click SWIN-NLB (172.16.32.40) -> Add Host to Cluster -> Host: second node's name (sWin22SVR4), Connect, Next -> Finish.	• Host with lowest numerical priority handles unassigned network traffic (default is 1). • Opt for Multicast mode due to single NIC per server and no routing.
Validate NLB cluster	*Create DNS host record for the NLB cluster to enable access via name:* • On DC1, DNS, create host record for "SWIN-NLB" in the sWin.Local forward lookup zone with NLB cluster's IP address (172.16.32.40). *Verify NLB configurations*:	All cluster nodes must offer clients identical data for hosted services.

	• On SVR1, NLB Manager, ensure both nodes are in “Converged” status. • Right-click cluster’s name, Cluster Properties -> Cluster Parameters tab, ensure “Multicast operations mode” • Port rules tab, ensure only one port rule “All” (port 0-65535, both TCP/UDP, Single Affinity) • Test connectivity by pinging the cluster IP address and access cluster services via the configured DNS name (URL: http://SWIN-NLB.sWin.Local)	

Further study

NLB clusters rely on **heartbeats**, messages exchanged between hosts **every second**, to ensure all members are functional. If a host misses sending **five consecutive heartbeats**, it is removed from the cluster to maintain overall system health. Similarly, failover clusters use heartbeats to keep nodes informed about each other's status.

Quorum in failover clusters prevents a cluster from being split into two separate entities, each potentially running independently. If the cluster fails to achieve quorum, typically by not obtaining the **majority of votes**, it stops. Each voting element (usually a node) maintains a synchronised cluster configuration. And if there is **an even number of voters**, a special type called a **witness** helps break ties. **Witness types** include **Disk Witness**, **File Share Witness**, and **Cloud Witness**, providing additional votes for cluster stability.

Lab 08: Implementing Update Management

Date: 04/05/2024

Key concepts

Windows Server Update Services (WSUS) is used to centrally manage and distribute updates for Windows and other Microsoft software within a corporate network. Its key architectural components **include WSUS server** (upstream, downstream in autonomous/replica mode, and disconnected), **WSUS client** (implemented via Group Policy Objects for client-side targeting), and **WSUS computer groups**.

Windows Deployment Services (WDS) facilitates mass OS deployment by automatically deploying image files. It comprises two types of images: **boot image**, which is a scaled-down version of the Windows OS (Windows Pre-installation Environment), and **install image**, which mirrors the hard drive of a WDS client computer, including the OS, applications, updates, roles, and settings configured on the original computer that created the image.

Key configurations and commands

Key steps	Details	Notes
Implement WSUS Server Role	*Install WSUS server role:* • On SVR1, install **Windows Server Update Services role**. Select role services: select **WID Connectivity** & **WSUS Services** -> Next. • Content location selection page, textbox: C:\WSUSUpdates (folder created on SVR1), Next, Install. • Server Manager, Tools, WSUS, click Run. *Configure WSUS to synchronise with an upstream WSUS server:* • On "WSUS Configuration Wizard", Next twice -> Choose Upstream Server, click "Synchronize from another Windows Server Update Services server" -> Server name: type upstream server's name (sWin22SVR4.Swin.Local) -> Next -> Start Connecting -> select "Begin initial synchronisation", Finish. • Update Services navigation pane, SVR1, Options -> click Computers, select "Use Group Policy or registry settings on computers", OK.	SVR1 is downstream server (at branches), downloading updates from SVR4 (upstream server at head office). SVR1 uses Windows Internal Database for deployment.
Configuring Update Settings	• *Configure WSUS groups:* SVR1, WSUS console, double-click SVR1, double-click Computers, click All Computers, click Add Computer Group (Actions pane) -> Name: Research -> Add. *Configure GPO to deploy WSUS settings:* • DC1, GPMC, create a GPO linked to Research OU named "WSUS Research". Edit the GPO: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update -> **Configure Automatic**	• Configure GPO to deploy WSUS settings to **Research** client computers. Organise client groups in WSUS. Direct OU client computers to

	Updates: Enabled; **Configure automatic updating**: 4 – Auto download and schedule the install • **Specify intranet Microsoft update service location**: Enabled; **Set the intranet update service for detecting updates** & **Set the intranet statistics server**: http://sWin22SVR1.Swin.Local:8530 (downstream server's name) • **Enable client-side targeting**: Enabled; **Target group name for this computer**: Research. • Open DSA, move sWin10CL101 from Computers container to Research OU. *Verify GPO settings application:* • Restart sWin10CL101 (client), log as Domain Administrator -> open CMD (Run as Administrator) and type: **gpresult /r** -> ensure **WSUS Research** GPO is listed under Computer Settings (Applied GPO). *Initialise Windows Update:* • On sWin10CL101's CMD: **wuauclt.exe /reportnow** • On SVR1 (WSUS downstream server), Update Services console, Computers, All Computers, Research -> ensure client appears in Research group.	WSUS server for updates. • Resolve WSUS clients failed to report to WSUS issue: **wuauclt.exe /reportnow /detectnow** or **wuauclt.exe /resetauthorization /detectnow** or **UsoClient.exe startscan**
Approve & deploy an update by using WSUS	• *Approve WSUS updates for Research computer group*: SVR1, Update Services, Updates, All Updates, right-click "**Security Update for Microsoft Office 2016 KB4011628), 64-bit**", Approve -> Research: Approved for Install, OK. • *Deploy updates to client:* CL101, CMD: **wuauclt.exe /detectnow** -> Start screen, type Windows update, under Search, click "**Check for updates**" -> install new updates. • *Verify update deployment to client:* CL1010, Event Viewer, View event logs -> **Applications and Services Logs\Microsoft\Windows\WindowsUpdateClient/Operational** -> ensure update events are logged.	Approve, deploy, and verify update on sWin10CL101 (in Research department) to validate WSUS setup.

Further study

The **WSUS upstream server** connects directly to the Microsoft Update website, while **downstream servers** fetch updates from the upstream server instead of going to the Microsoft website. **Downstream servers** can operate in **two modes**: **autonomous** mode, where local administrators handle update evaluation and approval, suited for setups with enough manpower and specific site needs; or **replica** mode, suitable for environments lacking manpower or resources for update evaluation.

Disconnected mode is employed in branch offices with limited internet connectivity, allowing updates to be offline-mounted and shipped to remote sites.

To control which WSUS clients on the network receive specific updates, **WSUS computer groups** are used. These groups differ from ADDS security groups and Windows local groups. When updates are approved for deployment, administrators select the groups that should receive them.

Lab 09: Implementing Active Directory Certificate Services

Date: 11/05/2024

Key concepts

Active Directory Certificate Services (ADCS) is used for managing **digital certificates** within an organisation's network. It enables the **issuance, renewal, and revocation of digital certificates**, which are used to establish secure communication, authenticate users, and encrypt data. Organisations use ADCS to enhance security by implementing **Public Key Infrastructure (PKI)**.

ADCS role services include:

- **Certification Authority (CA)**: responsible for issuing, validating, and revoking digital certificates.
- **Certificate Enrolment Web Service**: allows computers **at least** to request and retrieve digital certificates via a web interface.
- **Certificate Enrolment Policy Web Service**: provides a customisable policy interface for certificate enrolment.
- **Certification Authority Web Enrolment**: offers a means to issue and renew certificates for computers that are running **non-Windows OS/non-ADDS domain members**, or **not directly connected to the organisation's network**.
- **Network Device Enrolment Service**: allows network devices (routers, switches) to request and obtain digital certificates.
- **Online Responder**: allows the management of Online Certificate Status Protocol (OCSP) responders, which provide real-time revocation status for digital certificates.

Key configurations and commands

Key steps	Details	Notes
Deploying Enterprise Root CA	• *Install and configure ADCS on SVR1:* SVR1, install ADCS role; **role services**: CA. *Configure destination server (SVR1) as CA*: • Use domain admin credentials. • Choose Enterprise CA, Root CA type. • Set up a new private key **with RSA#Microsoft Software Key Storage Provider**, 4096-bit key length. • Define CA common name (sWinRootCA), 5-year validity. • Default certificate database location (C:\Windows\system32). *View Root CA properties:* SVR1, Tools, Certification Authority -> sWinRootCA's Properties, General tab, View Certificate. *Backup Root CA certificate:* General tab, View Certificate, Details tab, Copy to File, Next. Export settings: **file format**: DER encoded binary X.509 (.CER). *Install Root CA certificate to Trusted Root Certification Authority of all domain computers (GPO):*	SVR1 is CA server. In practice, use a dedicated backup location for root CA certificates rather than local drive.

	• DC1, GPMC, edit Default Domain Policy, **Computer Configuration\Policies\Windows Settings\Security** • **Settings\Public Key Policies** -> right-click Trusted Root Certification Authorities, Import, Next -> **File to** import: **\sWin22SVR1\C$\RootCA.cer** (previously backed up Root CA file).	
Deploy & manage certificates	*Creating new template for sWin Web Servers:* Certification Authority on sWin22SVR1, expand sWinRootCA, right-click Certificate Templates, Manage -> right-click Web Server template, Duplicate Template. o **General tab**: Template display name to "sWinWebServer", Validity period: 3 years. o **Superseded Templates tab**: Add Web Server template. o **Request Handling tab**: Allow private key to be exported. o **Security tab**: Click Authenticated Users, **Allow Read and Enrol**. *Create new template for sWin users:* Certificate Templates console, right-click User template, Duplicate Template. o **General tab**: Template display name to "sWinUser". o **Superseded Templates tab**: Add User template. o **Security tab**: Authenticated Users, **Allow Read, Enrol, and Autoenroll**. o **Subject name tab**: Clear **Include e-mail name in the subject name** & **E-mail name**. • *Configuring sWinUser and sWinWebSrv Templates for Issuance*: Certification Authority on SVR1, right-click Certificate Templates, New, Certificate Template to Issue -> Enable both templates. *Configuring Autoenrollment for User Accounts*: • DC1 GPMC, **User Configuration\Policies\Windows Settings\Security Settings**, Public Key Policies. • Double-click Certificate Services Client – Auto-Enrolment, **Configuration Model**: Enabled; check "***Renew expired certificates, update pending certificates, and remove revoked certificates***" & "***Update certificates that use certificate templates***". • Double-click Certificate Services Client – Certificate Enrolment Policy, Enrollment Policy tab, **Configuration Model**: Enabled -> ensure "***Active Directory Enrollment Policy***" is selected and enabled. *Verify Autoenrolment:* • SVR1, open PowerShell, run **gpupdate /force** -> **mmc** -> Console 1, click File, Add/Remove Snap-in, Add	

	“**Certificates**”. -> expand Certificates – Current User, Personal, click Certificates -> verify issued certificate for Administrator based on sWinUser template. • *Installing IIS on SVR4*: install IIS role -> create **index.html** file in **C:\inetpub\wwwroot** folder. *Updating the Web Server Certificate on SVR4*: • Run **gpupdate /force** on SVR4 -> Server Manager, Tools, **Internet Information Services (IIS) Manager** -> double-click **Server Certificates** -> click **Create Domain Certificate**, fill **Distinguished Name** Properties; **Online Certification Authority**: sWinRootCA, **Friendly name**: sWin22SVR4. • Expand Sites, Default Web Site, click Bindings -> Add -> Type: https -> IP address & Host name: SVR4’s IP and FQDN; SSL certificate: sWin22SVR4 -> remote **http** row. *Test browsing to SVR4 web:* • Internet Explorer, http://sWin22SVR4.sWin.Local should display Security alert& error message, whereas **https** displays normal content.	

Further study

The difference between **Certification Authority Web Enrolment** and **Certificate Enrolment Web Service**: while both services facilitate certificate enrolment, the **Certification Authority Web Enrolment** is a user-facing web interface for manual certificate requests, whereas the **Certificate Enrolment Web Service** is a programmable interface primarily used for automated certificate enrolment in machine-to-machine interactions.

CA types can be **Standalone** (no AD required, manual certificate requests via web or other manual means, requires administrator approval, offline root CA) or **Enterprise CA** (AD-stored configurations, supports various enrolment methods including manual/web/auto-enrolment, offers **Certificate Templates**); **Root CA** (highest in hierarchy, singular, trusted by all clients) or **Subordinate CA** (number based on geographical and client factors).

Lab 10: Implementing Active Directory Right Management Services

Date: 18/05/2024

Key concepts

Active Directory Right Management Services (AD RMS) is used to protect sensitive information by controlling who can access, modify, print, and forward documents/emails. Organisations use AD RMS to **minimise unauthorised data transmission/leakage** and ensure confidential information **stays within the organisation**. AD RMS includes **5 components**: AD RMS server, AD RMS client, AD RMS Apps, Database, and PKI.

Active Directory Federation Services (AD FS) facilitates secure **single sign-on (SSO)** and authentication across organisational boundaries. With AD FS, users can conveniently access multiple applications and services using a single set of credentials. It enables resource sharing between organisations by establishing trust relationships through federation (**federation trusts**) and implementing a scalable **claim-based** authentication method.

Key configurations and commands

Key steps	Details	Notes
Install & configure AD RMS	<u>*DNS & AD RMS service account:*</u> • On DC1, DSA, create "Service Accounts" OU, create user account named "ADRMSSVC" within this OU (enable "password never expire" & "user cannot change password"). • Create Global security group: G_ADRMS_SuperUsers in **Users** container with email. • Create host record named "adrms" for SVR1's IP address in DNS. <u>*Install & configure AD RMS role:*</u> • SVR1, install AD RMS role with default options. • **Perform additional configuration**: Create a new AD RMS root cluster, Use Windows Internal Database on this server; Service account: sWin\ADRMSSVC; Cryptographic mode 2; Use AD RMS centrally managed key storage; Default Website, Use an unencrypted connection, FQDN: http://adrms.swin.local, port 80; Licensor Certificate: swinADRMS; Register SCP now. • Launch IIS Manager, **SWIN16SVR1(sWin\Administrator)\Sites\Default Web Site**, **_wmcs** -> double-click **Authentication**, **Anonymous Authentication**, Enable -> **Connections** pane, **_wmcs**, licensing -> do the same for **/_wmcs/licensing Home** (IIS section). -> sign out of SVR1. <u>*Configure AD RMS Super Users group:*</u> • Sign in back to SVR1 as domain admin, ADRMS console, expand sWin16SVR1 (local), Security Policies, right-click Super Users, Enable Super Users	In this example, SVR1 is AD RMS server.

	• Click Change super user group, **Super user group:** ADRMS_SuperUsers@swin.local, OK • *Configure email addresses for testing users in AD RMS deployment*: DC1, DSA, Development OU, **Chris Developer**, Properties, set email as chris@sWin.local -> do the same for **Apple Developer** and **Sam Researcher**.	
Configure AD RMS templates	*Configure new rights policy template:* • ADRMS console, Rights Policy Template, Create Distributed Rights Policy Template..., click Add. • Create a ReadOnly template for Developers@sWin.Local with View rights and specified settings. *Configure rights policy template distribution:* • SVR1, File Explorer, create C:\RmsTemplates folder, Share to swin\ADRMSSVC (Full Control), remove Everyone group. • Create and share C:\DocShare folder to Everyone (Ful Control). • In ADRMS console, Rights Policy Templates, click Change distributed rights policy templates file location, select “Enable export”. Specify Templates File Location (UNC): “*SWIN16SVR1\RMSTEMPLATES*” -> Review C:\rmstemplates\ReadOnly.xml file. • *Configure an exclusion policy:* ADRMS console, click Exclusion Policies, Manage application exclusion list -> Enable Application Exclusion -> Exclude Application -> enter application filename, min/max version -> Finish.	
Verify AD RMS on a Client	*Create rights-protected document:* • CL101, File Explorer, right-click This PC, Properties, Remote settings, Select Users, Add -> Enter object names to select: Chris; Apple; Sam -> OK -> Sign out and sign in as sWin\Chris -> in IE, URL: http://adrms.swin.local -> Security tab, Local intranet, Sites button, Advanced, Add, Close, OK twice (**this needs to be done for every user**). • Launch Word, create a document "NewProd_Developers Only." -> File, Protected Document, Restrict Access, Connect to Digital Rights Management Servers and get templates -> Protect Document and Restrict Access -> Restricted Access. • Permission: enable “*Restrict Permission to this document*”, Read: Apple@swin.local -> save as \SWin16SVR1\DocShare\NewProd_DevelopersOnly. -> signout. • *Verify access*: Sign in as another developer (Apple) on sWin10CL101 and configure Internet Explorer settings -> Access the saved document and verify permissions.	Chris and Apple are Developers, Sam is researcher.

	• Attempt to access the document as Sam (unauthorised user) and verify lack of permission.	

Further study

In an AD RMS environment, we have 4 types of certificates:

- **Machine certificate**: identify a trusted computer/device.
- **Rights account certificate**: identify an individual user within the AD RMS system.
- **Publishing licenses**: determine the specific rights and permissions that are applied to the content, such as viewing, editing, printing, or forwarding.
- **End-user license**: granted to authorised users so that they are allowed to access protected content.

Together, these certificates ensure that only authorised users and trusted devices can access and interact with protected content while maintaining control over usage rights and permissions.