

SMW ASSIGNMENT REPORT



School of Computing

Diploma in Cybersecurity and Digital Forensics

Securing Microsoft Windows (ST2612)

DCDF/FT/2B/23

Group 3

Group Member	Admission Number
Tan Yi Jie Kayden	2424303
Lee Jiayi	2424329
Justin Myo Lwin	2424220
Ivan Kong Yu Yao	2423836

Lecturer's Name: Muhammad Iruan KARAMAN

ST2612_Assignment

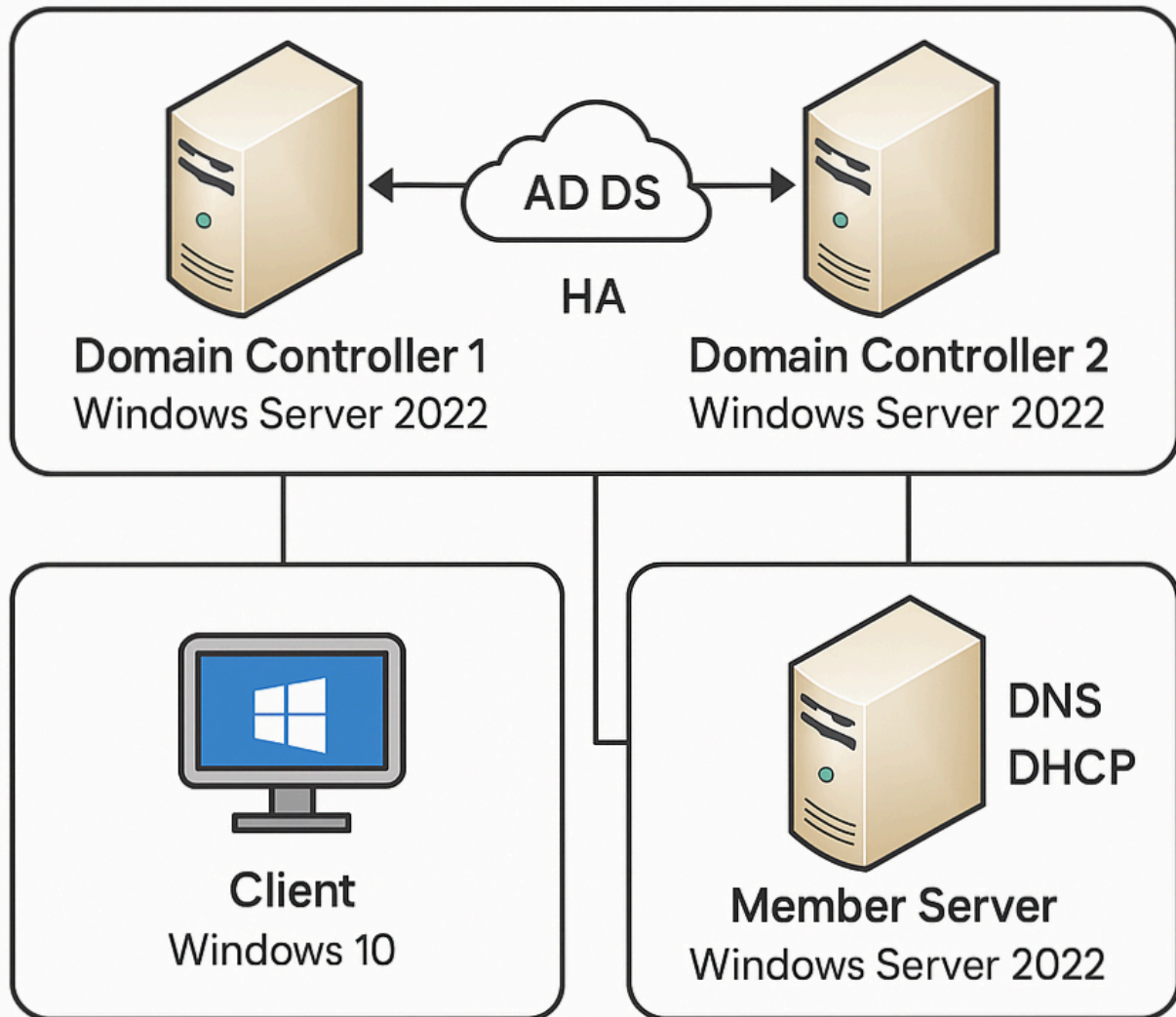
Securing Windows and Active Directory

Tables of Content

● Introduction	3
● Infrastructure	4
○ 2.1. Setting Up Domain Controllers and Services	
○ 2.2. Setting Up DNS	
○ 2.3. Setting Up DHCP	
○ 2.4. Setting Up Member Server and Client	
● CIS Benchmarks Applications	14
○ 3.1. CIS Benchmarks for Server and Client	
○ 3.2. CIS Benchmarks for Active Directory (Domain Controller)	
● Additional Security Measures	20
○ 4.1. Secure DNS	
○ 4.2. Enable DNS Logging	
○ 4.3. Restrict Zone Transfers	
○ 4.4. Secure Remote Desktop	
● Demonstration Agenda	28
○ 5.1. DNS High Availability	
○ 5.2. DHCP High Availability	
○ 5.3. Active Directory High Availability	
○ 5.4. CIS Benchmark Testing	
○ 5.5. Additional Security Testing	
● Recommendations	33
● Task Allocation	34
● Individual Reflection	35
● References	36

Introduction

This report documents the planning, setup, and implementation of a secure and highly available Windows Server and Active Directory (AD) environment. The assignment required our team to design and configure a resilient network architecture consisting of multiple domain controllers, DNS and DHCP services, and a client machine, with an emphasis on high availability. Additionally, we also have to implement CIS benchmarks for our servers, client and active directory while also implementing additional security measures.



Report Body

Infrastructure

Setting up Domain Controllers and Services

1. Set static Ip for DC1

IP address: **192.168.81.30**

Subnet mask: **255.255.255.0**

Default gateway: **192.168.81.2**

Preferred DNS: **192.168.81.29**

Alternate DNS: **192.168.81.30**

1. Install ADDS on DC1
2. Promote it to a new forest in server manager in post installation
3. Install DNS on DC1 in server manager after installation of ADDS
4. Install DHCP on DC1 in server manager

Use default settings for post installation configuration

1. Set static Ip for DC2

i. Ip address: **192.168.81.31**

ii. Subnet mask: **255.255.255.0**

iii. Default gateway: **192.168.81.2**

iv. Preferred DNS: **192.168.81.30**

v. Alternate DNS: **192.168.81.31**

2. Join DC2 to the domain in system properties
3. Install ADDS on DC2
4. Add it to the existing domain in post installation
5. Install DNS on DC2 in server manager during the post installation of ADDS
6. Install DHCP on DC2 in server manager

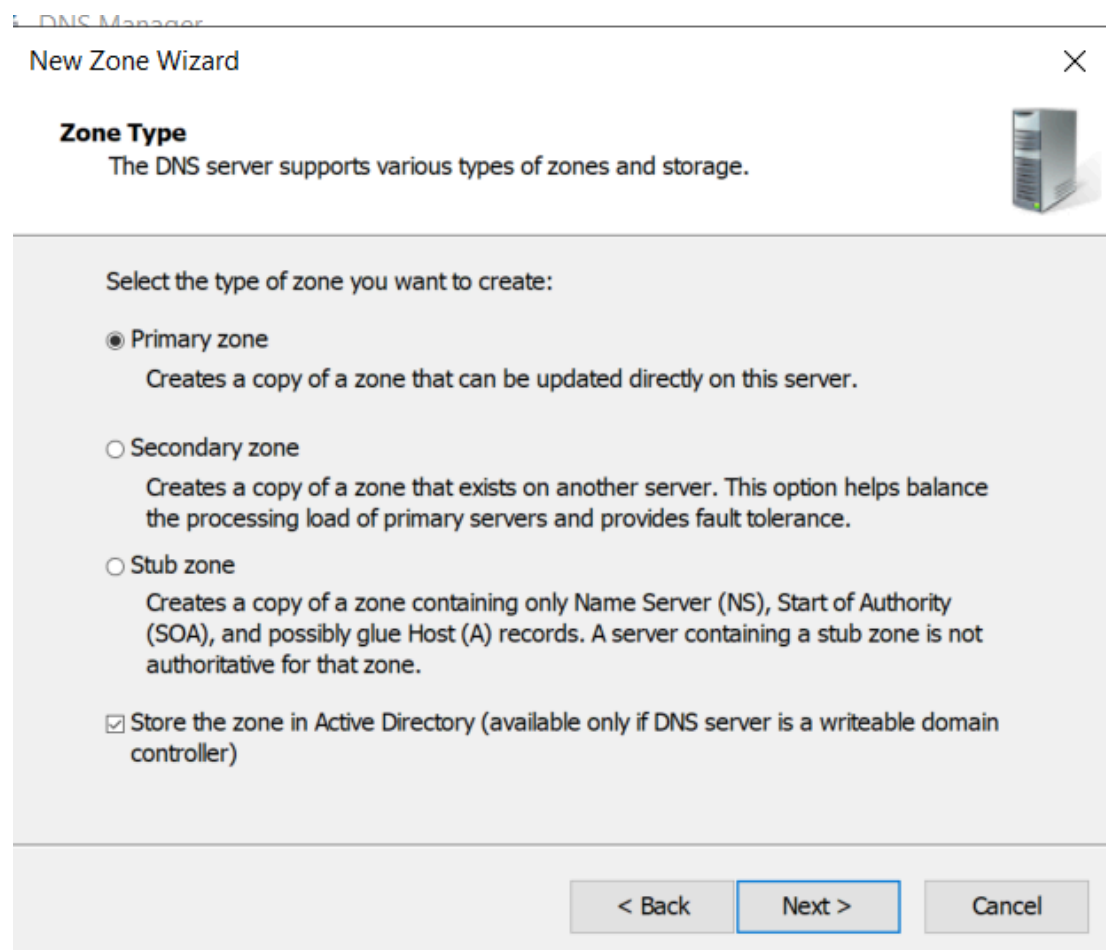
Use default settings for post installation configuration

Setting up DNS

Verify the DNS forward lookup zones in DC1 have been copied over to DC2 in the DNS manager for both DCs, this should be done automatically at this point

Create a reverse lookup zone in DC1 using DNS manager

Zone Type: Primary zone



DNS Manager

New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

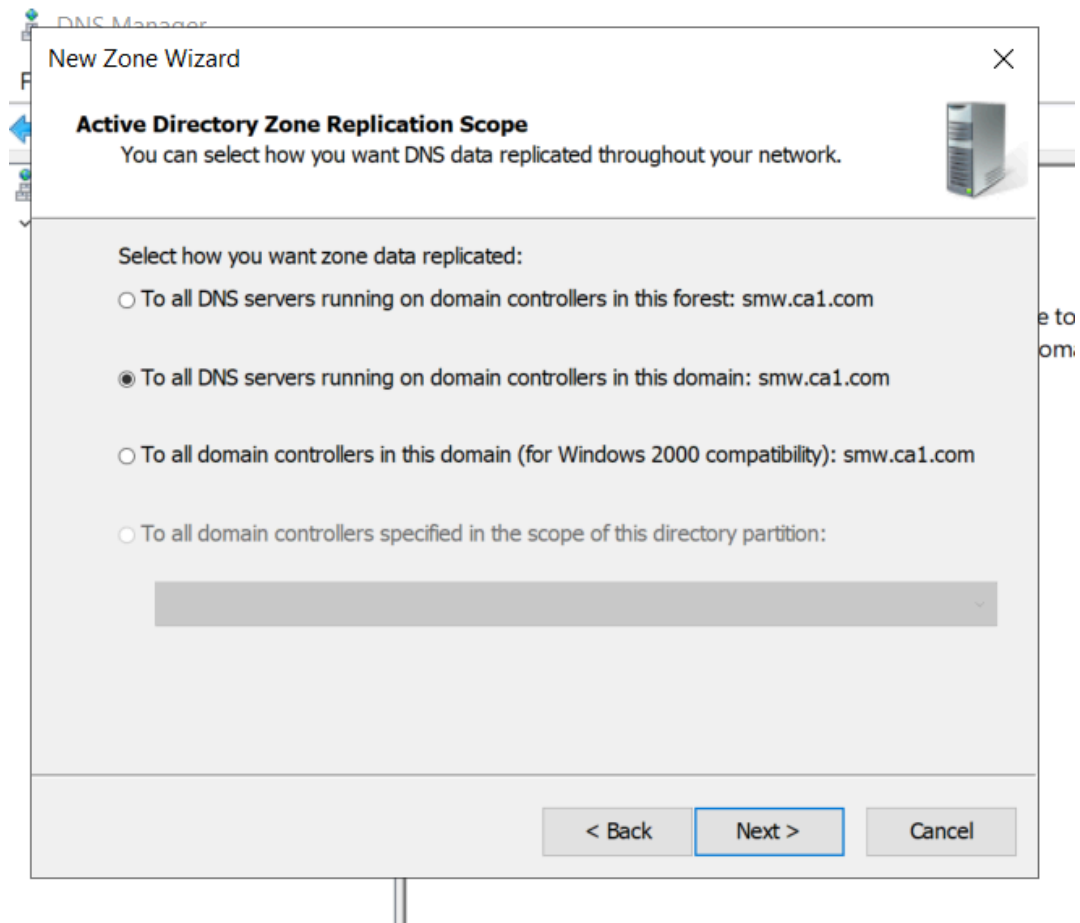
Select the type of zone you want to create:

- ☒ Primary zone
Creates a copy of a zone that can be updated directly on this server.
- ☐ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

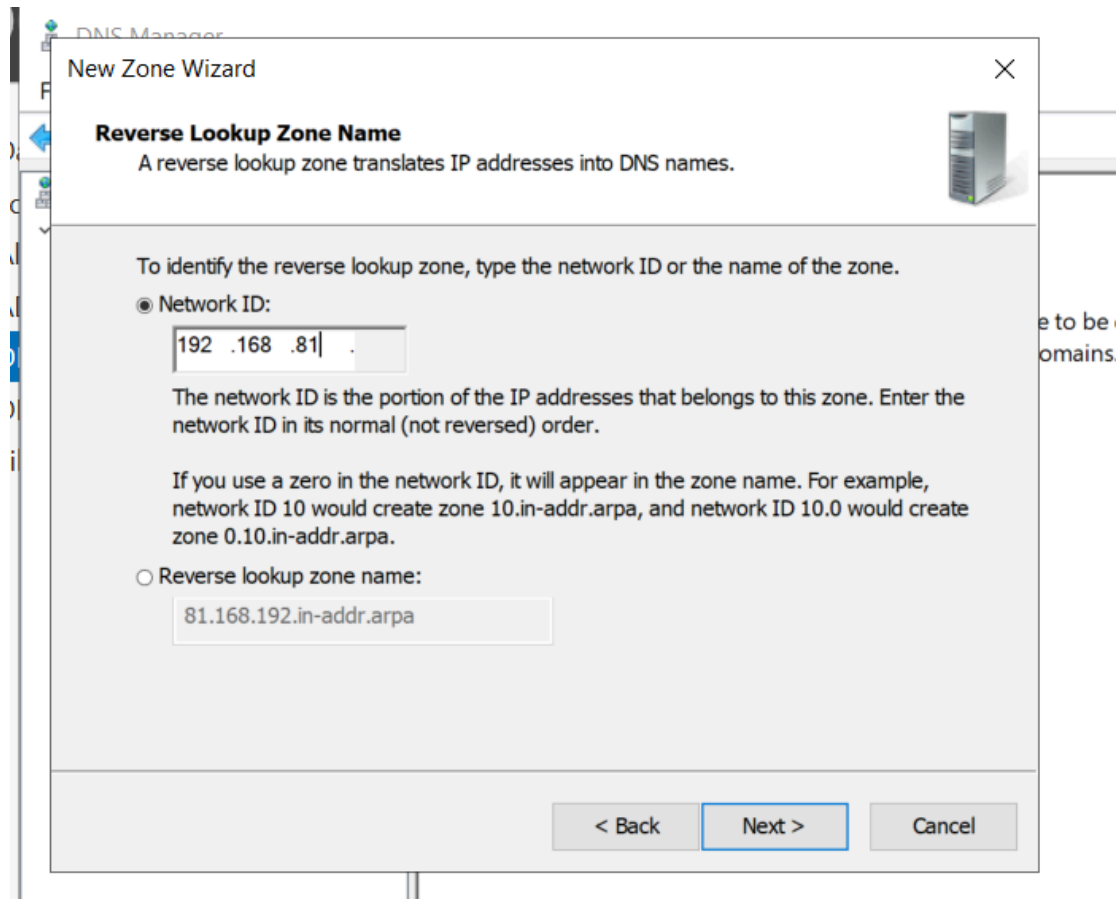
☒ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back Next > Cancel

Replication: To all DNS servers running on domain controllers in this domain



Network ID: 192.168.81



Dynamic updates: Allow only secure dynamic updates (means that only authenticated domain-joined clients (or authorized servers) can automatically register or update their DNS records)

Right click the smw.ca1.com zone in forward lookup zones

Click properties

Click name servers

Click add and add the ip addresses: 192.168.81.30, 192.168.81.31

Do this for both DC1 and DC2

Setting up DHCP

Create a DHCP scope in DC1 using DHCP manager

Create new scope in IPv4

Enter name and description

Start IP address: 192.168.81.100

End IP address: 192.168.81.150

... a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 81 . 100

End IP address: 192 . 168 . 81 . 150

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Skip add exclusions and delay

Leave the lease duration as default

dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

Minutes:

3

0

0

< Back

Next >

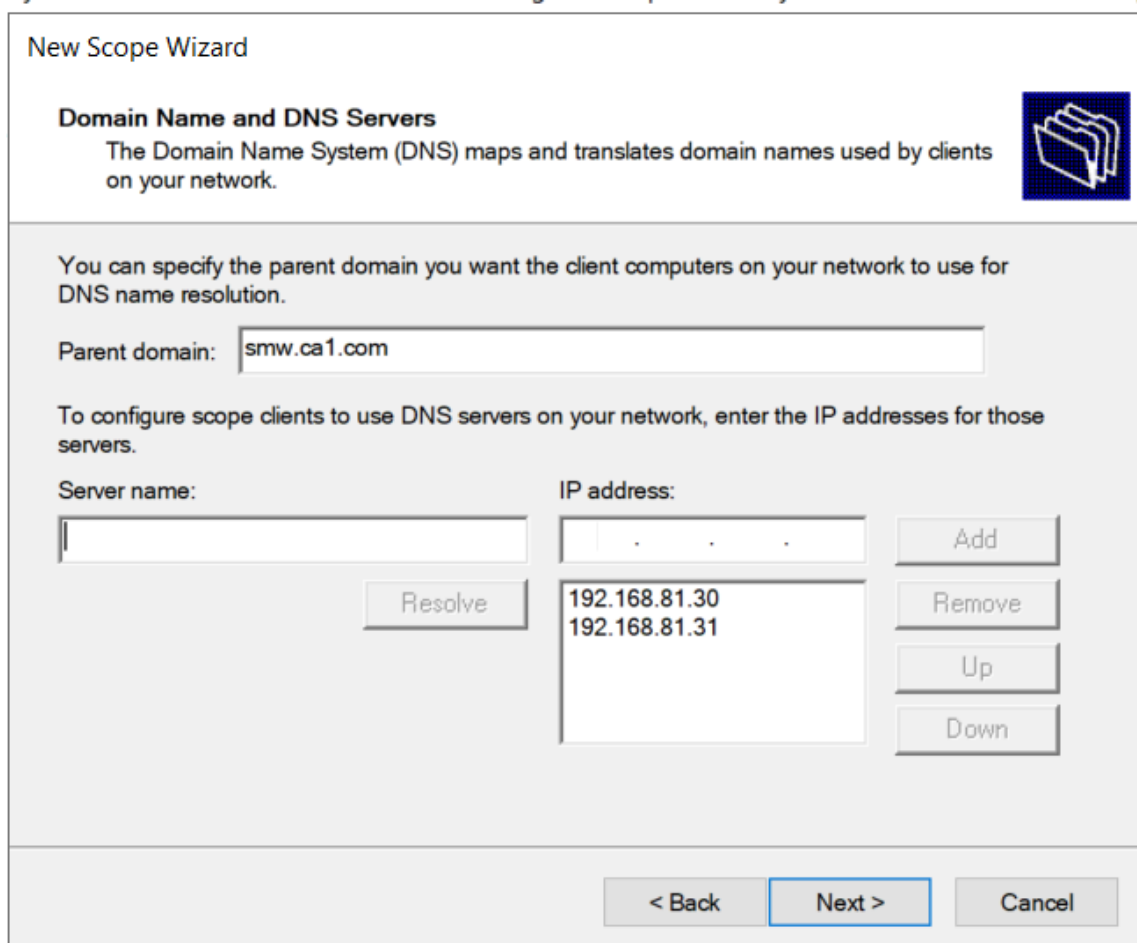
Cancel

Configure DHCP options:

Select: Yes, I want to configure these options now

Router: 192.168.81.2

DNS servers: 192.168.81.30, 192.168.81.31



The image shows a screenshot of the 'New Scope Wizard' window, specifically the 'Domain Name and DNS Servers' step. The window has a title bar and a main content area. At the top, the title 'New Scope Wizard' is displayed. Below it, the section 'Domain Name and DNS Servers' is highlighted, with a sub-header 'Domain Name and DNS Servers' and a description: 'The Domain Name System (DNS) maps and translates domain names used by clients on your network.' To the right of this text is a small icon of a folder. Below the description, there is a text box for 'Parent domain:' containing the value 'smw.ca1.com'. Further down, a paragraph explains that the user can specify the parent domain for client computers. Below this, there is a section for configuring DNS servers. It includes a 'Server name:' label and an empty text box, a 'Resolve' button, and an 'IP address:' label. To the right of the 'IP address:' label is a list box containing the IP addresses '192.168.81.30' and '192.168.81.31'. To the right of the list box are four buttons: 'Add', 'Remove', 'Up', and 'Down'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

Resolve

IP address:

Add
Remove
Up
Down

< Back Next > Cancel


Skip the WINS server configuration and proceed to finish the configuration

Select: Yes, I want to activate this scope now

Configure failover in IPv4 in DC1

Click add server

Select DC2 to be the server added

Description	Failover Relationship
<div><h3>Configure Failover</h3><p>Specify the partner server to use for failover</p><p>Provide the host name or IP address of the partner DHCP server with which failover should be configured.</p><p>You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.</p><p>Alternatively, you can type the host name or IP address of the partner server.</p><p>Partner Server: <input type="text" value="dc2.smw.ca1.com"/> <input type="button" value="Add Server"/></p><p><input type="checkbox"/> Reuse existing failover relationships configured with this server (if any)</p></div>	
<div><input type="button" value=" < Back"/> <input type="button" value=" Next > "/> <input type="button" value=" Cancel"/></div>	

Configure Failover

Create a new failover relationship

Create a new failover relationship with partner dc2.smw.ca1.com

Relationship Name: win2k22std.smw.ca1.com-dc2.smw.ca1.com

Maximum Client Lead Time: 1 hours 0 minutes

Mode: Load balance

Load Balance Percentage

Local Server: 50%

Partner Server: 50%

☒ State Switchover Interval: 5 minutes

☒ Enable Message Authentication

Shared Secret: *****

< Back Next > Cancel

Configure failover relationship

Maximum client lead time: 1h (maximum amount of time that a DHCP client can use a lease without needing confirmation from the partner serve)

Mode: load balance (both DHCP servers actively lease IP addresses at the same time and)

Load balance percentage: Local server 50%/Partner server 50% (lease requests are distributed between the 2 servers equally at 50%/50% for each server)

State switch interval: 5min (optional timer that controls how long a DHCP server should wait before automatically taking over the responsibility of leasing IP addresses when the partner server is unreachable)

AD:

1. On DC2, in command prompt, use the command `repadmin /replsummary`

This should show success

2. Make sure networking discovery has been turn on for both the client and member server

3. Shut down DC1

4. On client, login to a domain user account with domain credentials

Username: test

Password: 1qwer\$#@!

5. Try to access a shared domain resource created on the member server

Network Path: `\\MEMBER-SERVER\testfolder2`

6. In command prompt, use the command `gpupdate /force`

7. Repeat steps 4-6 by turning on DC1 and shutting down DC2 to check that you get the same results

If all of the above are successful on top of the HA for the DNS, this proves that HA for AD is working

Setting up member server and client

On the member server

Set static Ip for member server

Ip address: 192.168.81.32

Subnet mask: 255.255.255.0

Default gateway: 192.168.81.2

Preferred DNS: 192.168.81.30

Alternate DNS: 192.168.81.31

Join the member server to the domain in system properties

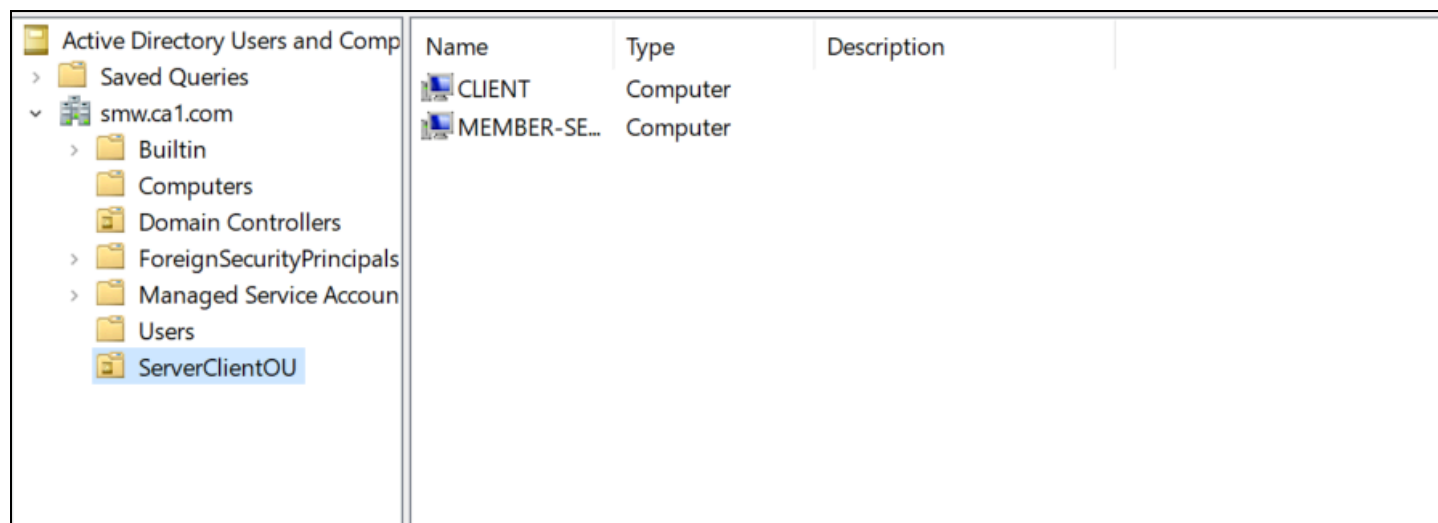
On the client

Join the client join the domain in system properties

CIS Benchmarks Applications

CIS Benchmarks for server and client

1. Put Client and Server into the same OU



2. Right click on the OU and click create GPO in this domain, and link it here.

3. Name the GPO (I named it CIS Password Policy)

4. Right click the created GPO and click edit

5. Go to Computer Configuration > Policies > Windows Settings > Security Settings > Password Policy

6. Setting 6 password policies for Server and Client

1. GPO → Enforce password history (Set to 24 password remembered)
2. GPO → Maximum password age (Set to 60 days)
3. GPO → Minimum password age (Set to 1 day)
4. GPO → Minimum password length (Set to 14 characters)
5. GPO → Password must meet complexity requirements (Set to Enabled)
6. GPO → Store passwords using reversible encryption (Set to Disabled)

7. Make another GPO (I name it CIS Account Lockout Policy)

8. Edit newly created GPO and go to > Computer Configuration > Policies > Windows Settings > Security Settings > Account Lockout Policy

9. Setting 4 account lockout policies for server and client

1. GPO → Account lockout duration (Set to 15 minutes)

2. GPO → Account lockout threshold (Set to 5 invalid logon attempt)
 3. GPO → Allow Administrator account lockout (Set to Enabled)
 4. GPO → Reset account lockout counter after (Set to 15 minutes)
-
10. Go to your server and client machine
 11. Windows + R
 12. Type in “cmd”
 13. Type “gpupdate /force”

After completing all the steps, 10 CIS Benchmarks would have been applied to Server and Client.

CIS Benchmarks for Active Directory (Domain Controller)

1. Right click on the OU and click create GPO in this domain, and link it here.
2. Name the GPO (I named it CIS Active Directory Policy)

>	Domain Control	2	CIS Active Directory ...	No	Yes	Enabled
---	----------------	---	--------------------------	----	-----	---------

3. Right click the created GPO and click edit
4. Setting 10 CIS benchmarks for Active Directory (Domain Controller)

Setting GPO for user rights assignment (1)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment
2. Double-click Access this computer from the network.
3. Remove Everyone, Authenticated Users if present.
4. Add only required groups (e.g. Administrators, Domain Admins)

Access this computer from the network	SMW\Domain Admins
---------------------------------------	-------------------

Setting GPO Deny access to this computer from the network (2)

1. Double-click Deny access to this computer from the network
2. Check 'Define these policy settings'
3. Add accounts that should not have access to DC (e.g. Guests, local accounts)
4. Click 'Ok'

Deny access to this computer from the network	Guests
---	--------

Setting GPO Enable Windows Firewall – Domain Profile (3)

1. Computer Configuration → Policies → Administrative Templates → Network → Network Connections → Windows Defender Firewall → Domain Profile
2. Double click Defender Firewall: Protect all network connections
3. Click 'Enabled'
4. Click 'Ok'

Windows Defender Firewall: Protect all network connections	Enabled
--	---------

Setting GPO to Enable Audit Directory Service Access (4)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → DS Access
2. Double click Audit Directory Service Access
3. Click 'Configure' and enable 'Success' and 'Failure'
4. Click 'Ok'

	Audit Directory Service Access	Success and Failure
--	--------------------------------	---------------------

Setting GPO to Prevent Disabling Windows Defender AV (5)

1. Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus
2. Double click Turn off Microsoft Defender Antivirus
3. Click 'Disabled'
4. Click 'Ok'



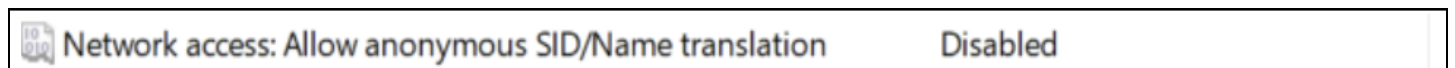
Setting GPO to Audit the Group Policy Objects (GPOs) (6)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → DS Access
2. Double click Audit Directory Service Changes
3. Click 'Configure' and enable 'Success' and 'Failure'
4. Click 'Ok'



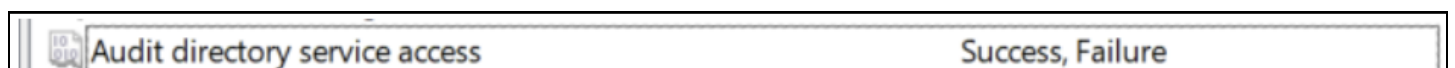
Setting GPO 'Network access: Allow anonymous SID/Name translation' (7)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options
2. Double click Network access: Allow anonymous SID/Name translation
3. Click 'Define' and click Disabled
4. Click 'Ok'



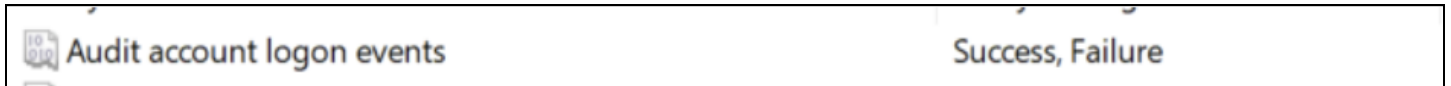
Setting GPO 'Audit directory service access' (8)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy
2. Double click Audit directory service access
3. Click 'Define' and enable 'success' and 'failure'
4. Click 'Ok'



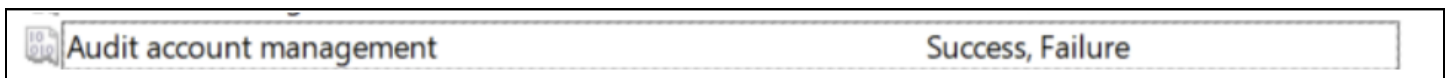
Setting GPO ‘Audit account logon events’ (9)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy
2. Double click Audit account logon events
3. Click ‘Define’ and enable ‘success’ and ‘failure’
4. Click ‘Ok’



Setting GPO ‘Audit account management’ (10)

1. Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy
2. Double click Audit account management
3. Click ‘Define’ and enable ‘success’ and ‘failure’
4. Click ‘Ok’

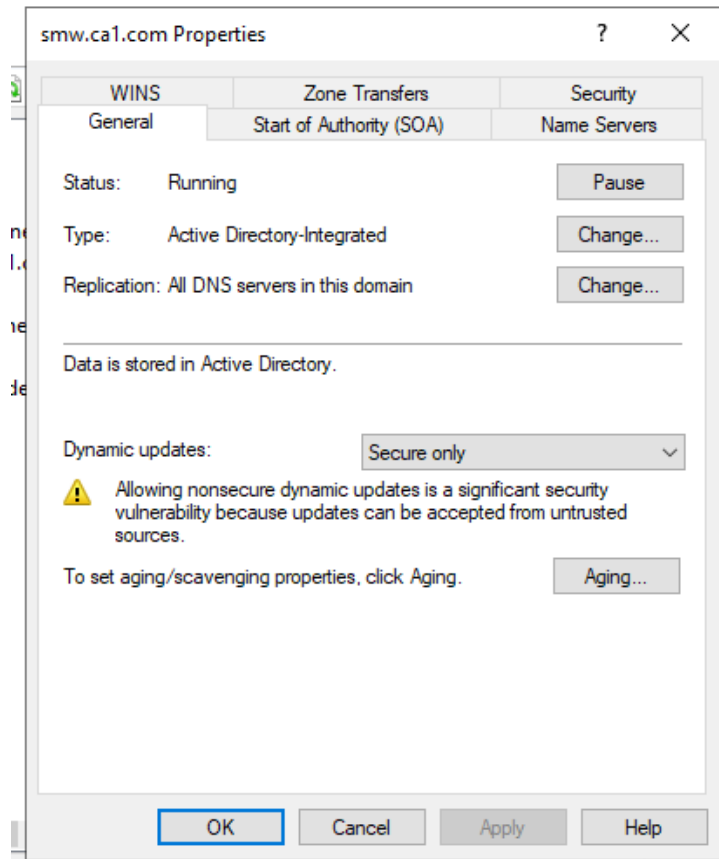


Additional Security Measures

Secure DNS

Secure Dynamic Updates

1. Open DNS Manager on each DC
2. Right-click your zone (e.g. yourdomain.local) and go to properties
3. Under Dynamic Updates, select: Secure only



Enable DNS Logging

1. Open DNS Manager
2. Right-click DNS server and go to properties
3. Go to the Debug Logging tab
4. Enable Log packets for debugging and tick options
 - Queries
 - Updates
 - Notifications
 - Transfers

The screenshot shows the 'WIN2K22STD Properties' dialog box with the 'Debug Logging' tab selected. The dialog has four main tabs: 'Interfaces', 'Forwarders', 'Advanced', and 'Root Hints'. Under 'Advanced', there are sub-tabs: 'Debug Logging', 'Event Logging', 'Monitoring', and 'Security'. The 'Debug Logging' sub-tab is active. It contains a text box explaining that debug logging is disabled by default and can be used to record packets sent and received. Below this, there are several sections of checkboxes and selection options:

- ☒ Log packets for debugging
- Packet direction:**
 - ☒ Outgoing } select at least one
 - ☒ Incoming } select at least one
- Transport protocol:**
 - ☒ UDP } select at least one
 - ☒ TCP } select at least one
- Packet contents:**
 - ☒ Queries/Transfers } select at least one
 - ☒ Updates } select at least one
 - ☒ Notifications
- Packet type:**
 - ☒ Request } select at least one
 - ☒ Response } select at least one
- Other options:**
 - ☐ Log unmatched incoming response packets
 - ☐ Details
 - ☐ Filter packets by IP address (with a 'Filter...' button)
- Log file:**
 - File path and name: [text box]
 - Maximum size (bytes): 500000000

At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Restrict Zone Transfers

Prevent DNS zone data from being leaked or copied by unauthorized servers.

1. DNS Manager → Right-click zone → Properties
2. Zone Transfers tab:
 - Uncheck Allow zone transfers OR choose “Only to servers listed on the Name Servers tab”





















Use Access Control Lists (ACLs)

Restrict who can query or modify DNS records.

1. Open DNS Manager → Right-click a zone → Properties
2. Click Security tab
3. Configure permissions:
 - Remove “Everyone” if present
4. Allow only:
 - Authenticated Users (Read)
 - Domain Admins (Full Control)
 - DNS Admins (as needed)

Group	Access to Allow
Domain Admins	Full control
DnsAdmins	Full control (or Special, if desired)
Authenticated Users	Read & Create All Child Objects
Enterprise Admins	Full control
SYSTEM	Full control
SELF	Validated write to computer objects
ENTERPRISE DOMAIN CONTROLLERS	Special

Permission entries:

	Type	Principal	Access	Inherited from	Applies to
	Allow	Domain Admins (SMW\Domain Admins)	Full control	None	This object only
	Allow	Authenticated Users	Create all child objects	None	This object only
	Allow	SYSTEM	Full control	None	This object only
	Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object and all descendant objects
	Allow	DnsAdmins (SMW\DnsAdmins)	Special	cn=MicrosoftDNS,DC=Domain...	This object and all descendant objects
	Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	cn=MicrosoftDNS,DC=Domain...	This object and all descendant objects
	Allow	Pre-Windows 2000 Compatible Access ...	Special	DC=DomainDnsZones,DC=s...	Descendant InetOrgPerson objects
	Allow	Pre-Windows 2000 Compatible Access ...	Special	DC=DomainDnsZones,DC=s...	Descendant Group objects
	Allow	Pre-Windows 2000 Compatible Access ...	Special	DC=DomainDnsZones,DC=s...	Descendant User objects
	Allow	SELF		DC=DomainDnsZones,DC=s...	This object and all descendant objects
	Allow	SELF	Special	DC=DomainDnsZones,DC=s...	This object and all descendant objects
	Allow	Enterprise Admins (SMW\Enterprise Ad...	Full control	DC=DomainDnsZones,DC=s...	This object and all descendant objects
	Allow	Pre-Windows 2000 Compatible Access ...	List contents	DC=DomainDnsZones,DC=s...	This object and all descendant objects
	Allow	Administrators (SMW\Administrators)	Special	DC=DomainDnsZones,DC=s...	This object and all descendant objects
	Allow	CREATOR OWNER	Validated write to computer at...	DC=DomainDnsZones,DC=s...	Descendant Computer objects
	Allow	SELF	Validated write to computer at...	DC=DomainDnsZones,DC=s...	Descendant Computer objects
	Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=DomainDnsZones,DC=s...	Descendant Computer objects
	Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=DomainDnsZones,DC=s...	Descendant Group objects
	Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=DomainDnsZones,DC=s...	Descendant User objects
	Allow	SELF		DC=DomainDnsZones,DC=s...	Descendant Computer objects

Secure Remote Desktop

Unbind any previously Assigned RDP Certificate

1. Open PowerShell as Administrator
2. Paste the following commands into the terminal:
 - a. `$ts = Get-WmiObject -Namespace "root\cimv2\TerminalServices" -Class "Win32_TSGeneralSetting" -Filter "TerminalName='RDP-Tcp'"`
 - b. `$ts.SSLCertificateSHA1Hash = $null`
 - c. `$ts.Put()`
3. Restart the RDP service with: `Restart-Service TermService -Force`

Delete the existingG domain controller certificate

This step removes the certificate issued from the DomainController template, which is not appropriate for RDP over TLS.

1. Paste the following command into the terminal
 - a. `certutil -delstore My <Thumbprint>`
 - i. Replace <Thumbprint> with the SHA1 hash of the DomainController certificate
(In this case: 5329b903dfba3f430a683541a8b0ba228d5d9a2e)

Generate a new self-signed RDP Certificate

Use PowerShell to manually create a self-signed certificate with the correct EKU

Paste the following command:

`New-SelfSignedCertificate ``

`-DnsName "$env:COMPUTERNAME", "$env:COMPUTERNAME.$env:USERDNSDOMAIN" ``

`-CertStoreLocation "cert:\LocalMachine\My" ``

`-KeyExportPolicy NonExportable ``

`-KeySpec KeyExchange ``

`-Provider "Microsoft RSA SChannel Cryptographic Provider" ``

`-NotAfter (Get-Date).AddYears(5) ``

`-TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")`

```
PS C:\Users\Administrator> New-SelfSignedCertificate `
>> -DnsName "$env:COMPUTERNAME", "$env:COMPUTERNAME.$env:USERDNSDOMAIN" `
>> -CertStoreLocation "cert:\LocalMachine\My" `
>> -KeyExportPolicy NonExportable `
>> -KeySpec KeyExchange `
>> -Provider "Microsoft RSA SChannel Cryptographic Provider" `
>> -NotAfter (Get-Date).AddYears(5) `
>> -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.1)"
```

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint	Subject
-----	-----
DEE0A9E71FC01178D9880221F1C8607A78B5E1F9	CN=WIN2K22STD

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object {
>> $_.Subject -like "*$env:COMPUTERNAME*" -and $_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.1"
>> } | Select-Object Subject, Thumbprint
```

Subject	Thumbprint
-----	-----
CN=WIN2K22STD	DEE0A9E71FC01178D9880221F1C8607A78B5E1F9

Restart Remote Desktop Service

Restart the service with: `Restart-Service TermService -Force`

Verify Certificate Binding

Run the following to confirm RDP is using the correct cert:

```
Get-WmiObject -Class Win32_TSGeneralSetting -Namespace root\cimv2\terminalservices | select  
SSLCertificateSHA1Hash
```

Then compare with:

```
certutil -store My
```

Look for a certificate:

Subject = Hostname (CN=WIN2K22STD)

Issuer = Same as Subject (self-signed)

EKU = Server Authentication (1.3.6.1.5.5.7.3.1)

SHA1 hash matches the bound cert

```
PS C:\Users\Administrator> Restart-Service TermService -Force
PS C:\Users\Administrator> certutil -store My
My "Personal"
===== Certificate 0 =====
Serial Number: 465dccbdd734cd914658a6e9a9841f6f
Issuer: CN=smw-WIN2K22STD-CA, DC=smw, DC=ca1, DC=com
NotBefore: 7/24/2025 5:25 PM
NotAfter: 7/24/2030 5:35 PM
Subject: CN=smw-WIN2K22STD-CA, DC=smw, DC=ca1, DC=com
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): f17d6fe2ea8a69ca8716bb905a2e9ab861ded116
Key Container = smw-WIN2K22STD-CA
Unique container name: 98c8f0fed6551c4e6dadb4839e2fc1c1_b951f56a-3c38-4382-8328-38e1ebbb0ad3
Provider = Microsoft Software Key Storage Provider
Signature test passed
```

```
===== Certificate 1 =====
Serial Number: 120b771c61d7c2944fc4b3f1dc213baa
Issuer: CN=WIN2K22STD
NotBefore: 7/31/2025 4:07 PM
NotAfter: 7/31/2030 4:17 PM
Subject: CN=WIN2K22STD
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): dee0a9e71fc01178d9880221f1c8607a78b5e1f9
  Key Container = 54cb97cfdbe476681a268f3c1c707a52_b951f56a-3c38-4382-8328-38e1ebbb0ad3
  Simple container name: te-6495ad2f-dd1d-49f3-9a16-89ee0c46d535
  Provider = Microsoft RSA SChannel Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
PS C:\Users\Administrator> Get-WmiObject -Class Win32_TSGeneralSetting -Namespace root\cimv2\t
SLCertificateSHA1Hash

SSLCertificateSHA1Hash
-----
DEE0A9E71FC01178D9880221F1C8607A78B5E1F9
```

Demonstration Agenda

Infrastructure

DNS:

1. Shut down DC1
2. On client, open command prompt and use the command `ipconfig /all`

Under DNS servers there should be the ip address of DC1 and DC2

3. `Ipconfig /flushdns`
4. Use a nslookup command like `nslookup win2k22std.smw.ca1.com`: there should be a response
5. Try to access the internet and it should be successful
6. Repeat steps 2-5 by turning on DC1 and shutting down DC2 to check that you get the same results

This proves that HA for DNS is working

DHCP:

1. Shut down DC1
2. On client, open command prompt and use the command `ipconfig /release`
3. Run `ipconfig /all` it is no longer being assigned an ip address from the dhcp
4. Then use the command `ipconfig /renew`

This will release the current dhcp assigned ip address and request a new ip address from the dhcp server.

5. Now use the command `ipconfig /all`

The client should still be receiving an ip address from the DHCP scope that has been set

6. Repeat steps 2-5 by turning on DC1 and shutting down DC2 to check that you get the same results

This proves that HA for DHCP is working

CIS Benchmarks:

For Server/Client side

GPO → Account lockout threshold (Set to 5 invalid logon attempt)

1. Power up Windows Client machine
2. Log in with invalid passwords (5 times)
3. Account should be locked out after

After the 5th invalid attempt, you should see:

“The referenced account is currently locked out and may not be logged on to.”

For AD/DC

Setting GPO to Prevent Disabling Windows Defender AV

1. Open Windows Security.
2. Go to Virus & threat protection.
3. Click “Manage settings” under “Virus & threat protection settings”
4. Look for “Real-time protection”

The outcome should show the button under “Real-time protection” should be grayed out and locked, thus showing the GPO is working correctly

Additional Security Measures

Secured Remote Desktop

1. Confirm Secure Certificate Is Bound to RDP

Run this on WIN2K22STD (DC):

```
Get-WmiObject -Class Win32_TSGeneralSetting -Namespace root\cimv2\terminalservices | Select  
SSLCertificateSHA1Hash
```

Output should show a valid SHA1 thumbprint:

[SSLCertificateSHA1Hash](#)

[DEE0A9E71FC01178D9880221F1C8607A78B5E1F9](#)

Then verify that it matches one of the certificates issued by your CA in: certutil -store My

Look for matching Cert Hash(sha1) and confirm the cert includes:

DNS Name = win2k22std.smw.ca1.com

Template = DomainControllerAuthentication

2. From Client, Connect via RDP Using FQDN

Open Remote Desktop Connection (mstsc) on your client (Win + R)

In the Computer field, enter: win2k22std.smw.ca1.com

Click Connect

Log in using a domain admin account

3. Confirm Login Works Without a Certificate Warning

If secure RDP is working:

You will connect directly to the server

Secured DNS

DNS Debug Logging Test

On a domain client (e.g., 192.168.81.127), run: `nslookup win2k22std.smw.ca1.com`

On the DNS Server (WIN2K22STD), run this PowerShell command:

```
Get-Content "C:\Windows\System32\Dns\dns.log" | Select-String 192.168.81.127
```

You should see the log entry showing that the client queried the server.

Zone Transfers Block Test

Goal: Show unauthorized zone transfers are denied.

On a different client, open Command Prompt and type: `nslookup`

In the nslookup prompt, type:

```
server 192.168.81.30
```

```
ls -d smw.ca1.com
```

Expected output: Can't list domain smw.ca1.com: Query refused

Recommendations

1. Export the self-signed cert and install it in clients' Trusted Root Certification Authorities to prevent trust warnings
2. Use firewall rules or a VPN to restrict RDP access
3. Limit RDP logins to specific security groups via Group Policy
4. Ensure Network Level Authentication (NLA) is enabled
5. Apply OS-specific GPOs only where relevant using WMI filters to prevent misapplied policies that may disrupt client machines or older systems
6. Enable Logging for Windows Defender Firewall to identify malicious connection attempts or misconfigured applications trying to communicate

Task Allocation

Tan Yi Jie Kayden

CIS Benchmarks

- Selected and implemented CIS Benchmark controls for both Active Directory and member servers/clients using Group Policy Objects (GPOs).
- Configured security-related policies including Account Lockout, Firewall, UAC, and Audit Policies

Jiayi

Infrastructure

- responsible for the infrastructure setup and contributed to implementing additional security measures.

Justin

Infrastructure

- responsible for the infrastructure setup

Ivan

Additional Security Measures

- responsible for the set up of the additional security measures

Individual Reflection

Tan Yi Jie Kayden:

During this assignment, I learned about High availability and how to set it up as well as security measures like CIS benchmark and the implementation of these measures to secure DNS and Remote Desktop. My primary responsibility was to research and apply CIS Benchmark controls across servers, clients and AD (DC). Through this, I became more proficient in using Group Policy Management in Server Manager. Additionally, working in a team requires good communication especially when multiple people were configuring different services and implementing different security measures. Thus, I learned how to communicate my progress and troubleshoot collaboratively. Overall, this assignment gave me practical exposure to Windows Server management and has strengthened my confidence in system hardening on Windows.

Jiayi:

In this project, I was mainly responsible for setting up the infrastructure. I configured the domain controllers, managed DNS, and ensured proper connectivity between client and server machines. This helped me strengthen my skills in Active Directory, DNS, and Remote Desktop setup. I also helped implement secure RDP access by manually configuring certificate-based authentication using PowerShell and a self-signed certificate. Overall, the experience improved my technical skills and gave me valuable exposure to real-world infrastructure deployment.

Justin:

I was responsible for doing the part related to setting up the infrastructure and this has given me a better understanding of managing a domain with high availability features for Active Directory, DNS and DHCP with a member-server and client. This has made me explore options in the DNS and DHCP management among other things and reinforced previous knowledge to strengthen my overall ability in dealing with windows domains.

Ivan:

I implemented two key additional security measures: Secure DNS and Secure Remote Desktop. I understood the importance of securing name resolution services in a network. This process gave me practical experience in reducing the attack surface of commonly targeted services and deepened my understanding of securing remote access in real-world environments. This has given me the experience to improve my skills in using windows server management.

References and Appendices

Microsoft Learn. (n.d.). *Active Directory Domain Services Overview*.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Microsoft DHCP high availability options

<https://www.youtube.com/watch?v=TKgm2Dxj-YM>

Microsoft Docs. *DHCP failover overview*

<https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-failover>

Configure DHCP for failover

<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831385%28v%3Dws.11%29>

CIS Benchmarks

https://www.cisecurity.org/benchmark/microsoft_windows_server