Name : Tarikul Islam Apon
ID : 1288503
Batch : NSA-65/IBCS-Primax

Project Name : Security Hardening in Windows Server-based DNS, DHCP, and IPAM Management

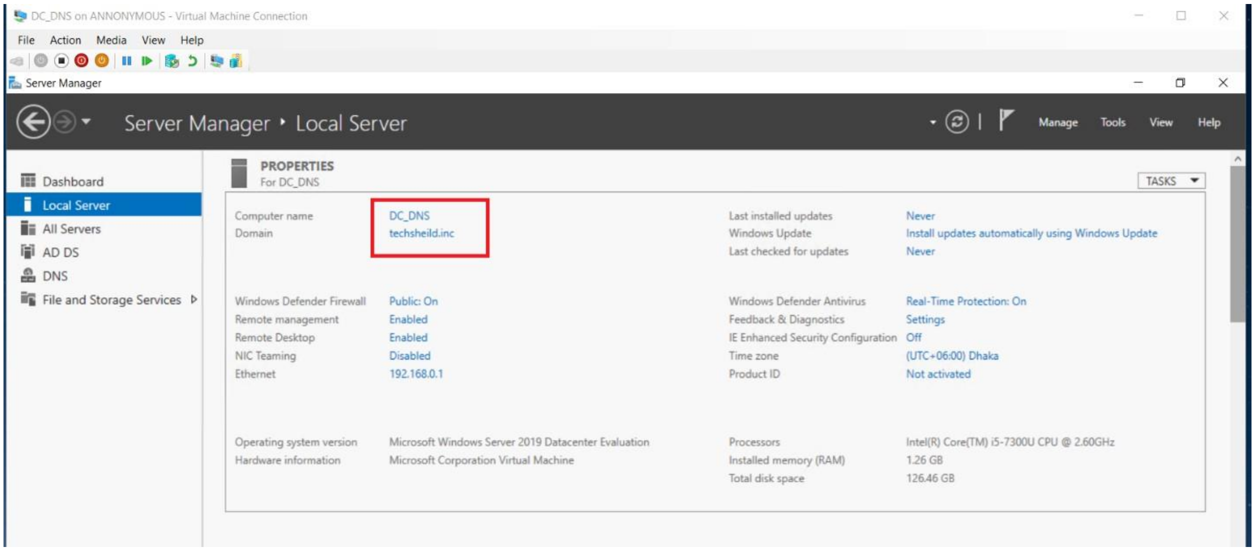
Objective:

Through this lab, you will be able to design and implement a secure network based on Windows Server.
It will also demonstrate how DNS, DHCP, and IPAM can work together in a secure and integrated manner.

Project Work :

At first should ready our machines and those are domain joined . **(techsheild.inc).**

DC +DNs


DC_DNS on ANNONYMOUS - Virtual Machine Connection
File
Action
Media
View
Help
Server Manager
Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
TASKS

PROPERTIES
For DC_DNS

Computer name DC_DNS
Domain techsheild.inc

Last installed updates Never
Windows Update Install updates automatically using Windows Update
Last checked for updates Never

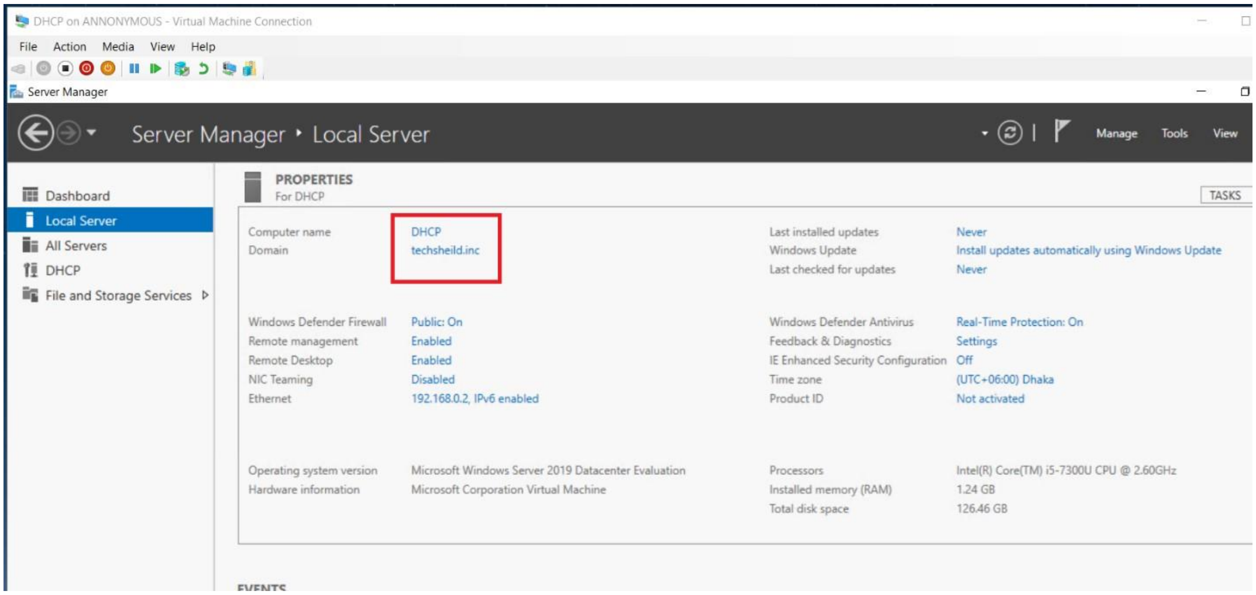
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.0.1

Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC+06:00) Dhaka
Product ID Not activated

Operating system version Microsoft Windows Server 2019 Datacenter Evaluation
Hardware information Microsoft Corporation Virtual Machine

Processors Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz
Installed memory (RAM) 1.26 GB
Total disk space 126.46 GB

DHCP Server


DHCP on ANNONYMOUS - Virtual Machine Connection
File
Action
Media
View
Help
Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Dashboard
Local Server
All Servers
DHCP
File and Storage Services
TASKS
EVENTS

PROPERTIES
For DHCP

Computer name DHCP
Domain techsheild.inc

Last installed updates Never
Windows Update Install updates automatically using Windows Update
Last checked for updates Never

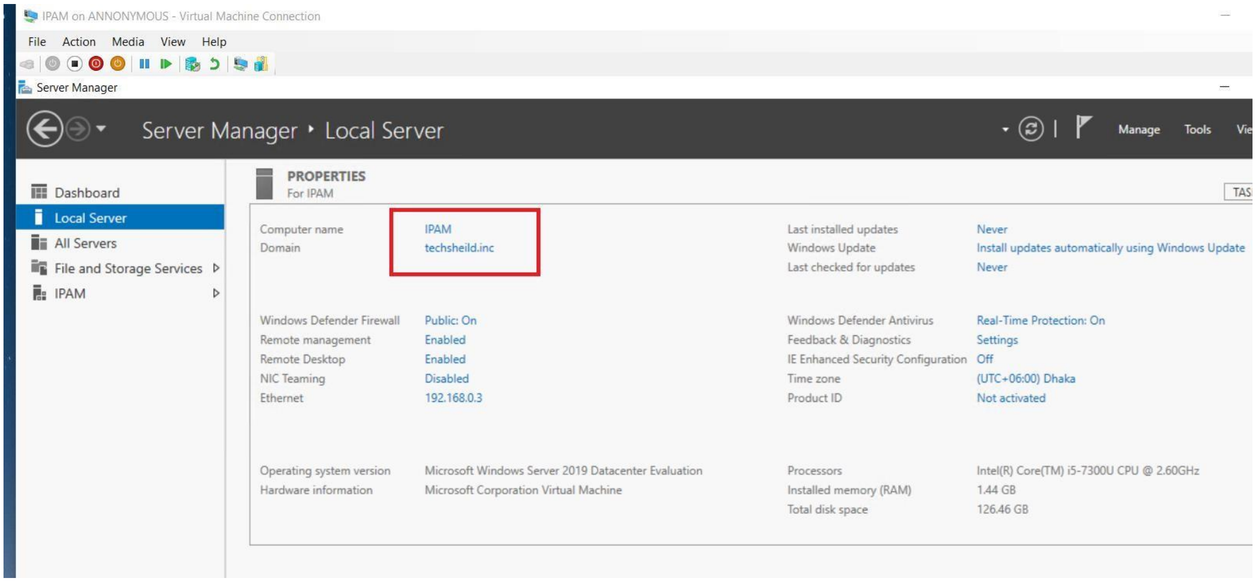
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.0.2, IPv6 enabled

Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC+06:00) Dhaka
Product ID Not activated

Operating system version Microsoft Windows Server 2019 Datacenter Evaluation
Hardware information Microsoft Corporation Virtual Machine

Processors Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz
Installed memory (RAM) 1.24 GB
Total disk space 126.46 GB

IPAM Server


IPAM on ANNONYMOUS - Virtual Machine Connection
File
Action
Media
View
Help
Server Manager
Server Manager ‣ Local Server
Manage
Tools
Vie
Dashboard
Local Server
All Servers
File and Storage Services
IPAM
TAS

PROPERTIES
For IPAM

Computer name IPAM
Domain techsheild.inc

Last installed updates Never
Windows Update Install updates automatically using Windows Update
Last checked for updates Never

Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.0.3

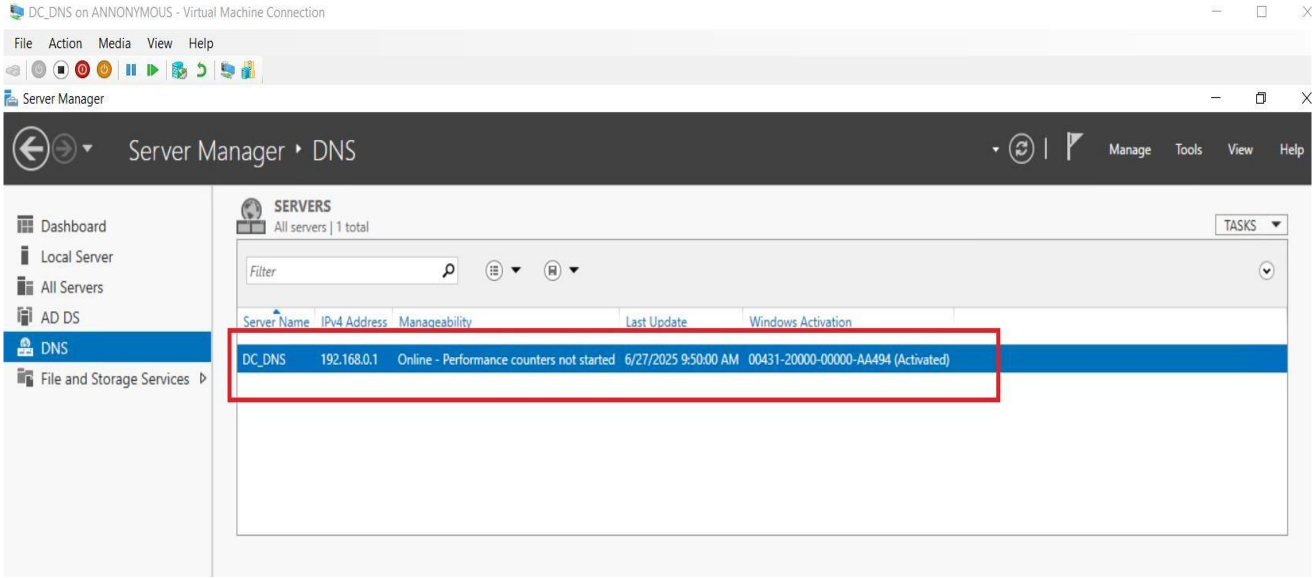
Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC+06:00) Dhaka
Product ID Not activated

Operating system version Microsoft Windows Server 2019 Datacenter Evaluation
Hardware information Microsoft Corporation Virtual Machine

Processors Intel(R) Core(TM) i5-7300U CPU @ 2.60GHz
Installed memory (RAM) 1.44 GB
Total disk space 126.46 GB

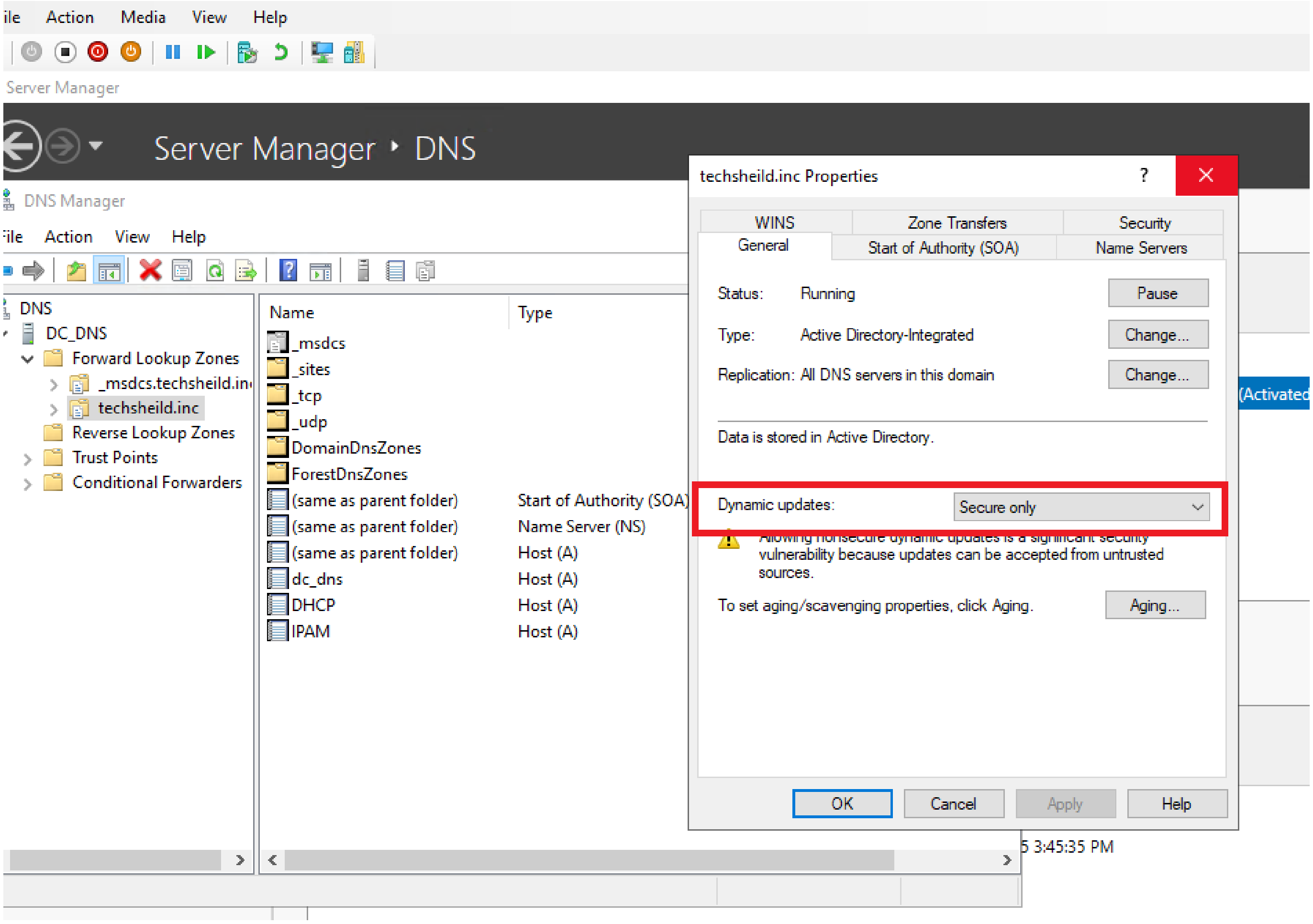
1. DNS Security:

a) Configure Dns Server named Dc_Dns.



Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC_DNS	192.168.0.1	Online - Performance counters not started	6/27/2025 9:50:00 AM	00431-20000-00000-AA494 (Activated)

b) Prevent Unauthorized Dynamic Updates and Configure Secure Dynamic Update. And We should select **Secure only** Option. And Sign DNSec Zone for more security .



Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
dc_dns	Host (A)
DHCP	Host (A)
IPAM	Host (A)

techsheild.inc Properties

Status: Running

Type: Active Directory-Integrated

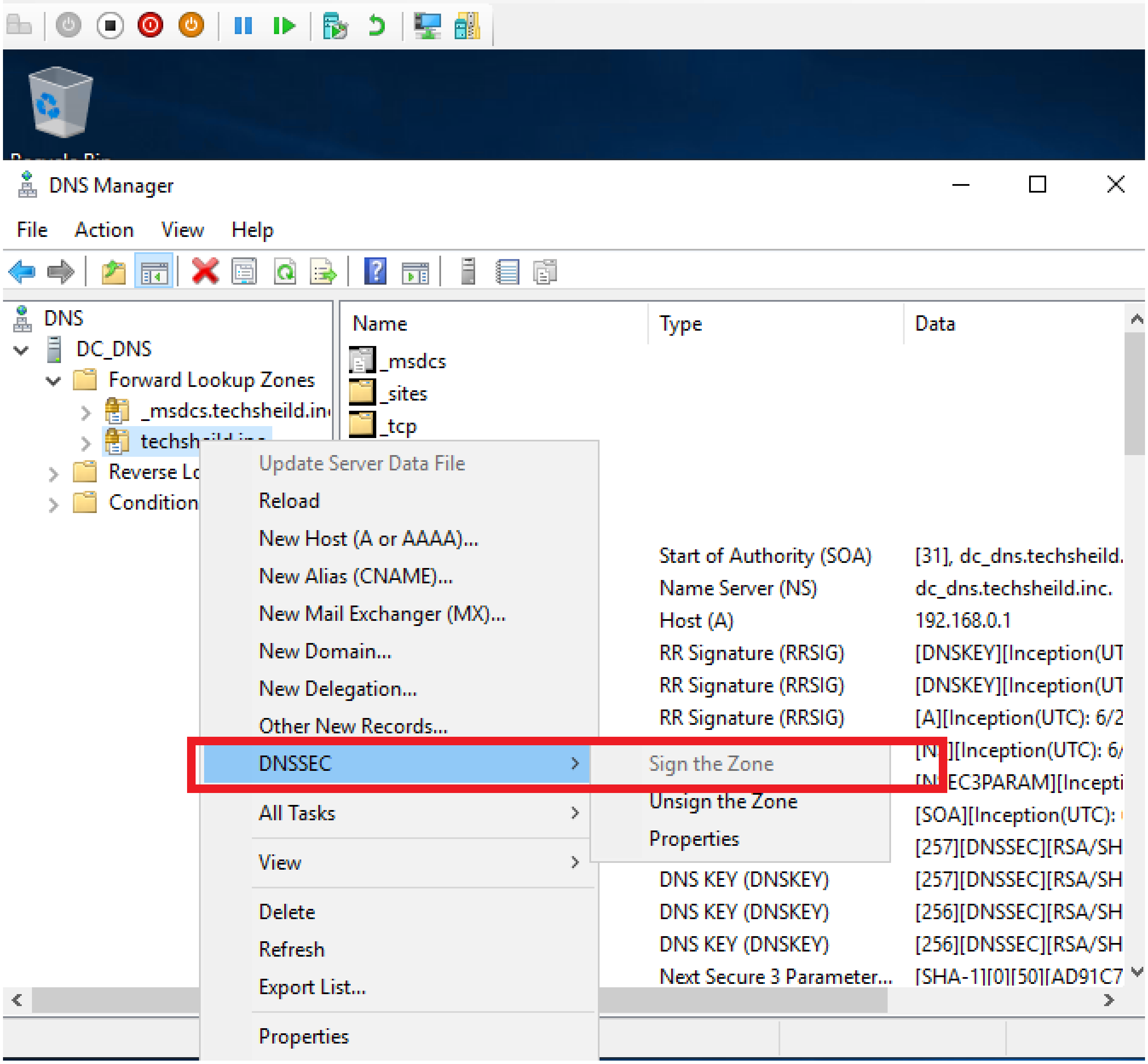
Replication: All DNS servers in this domain

Data is stored in Active Directory.

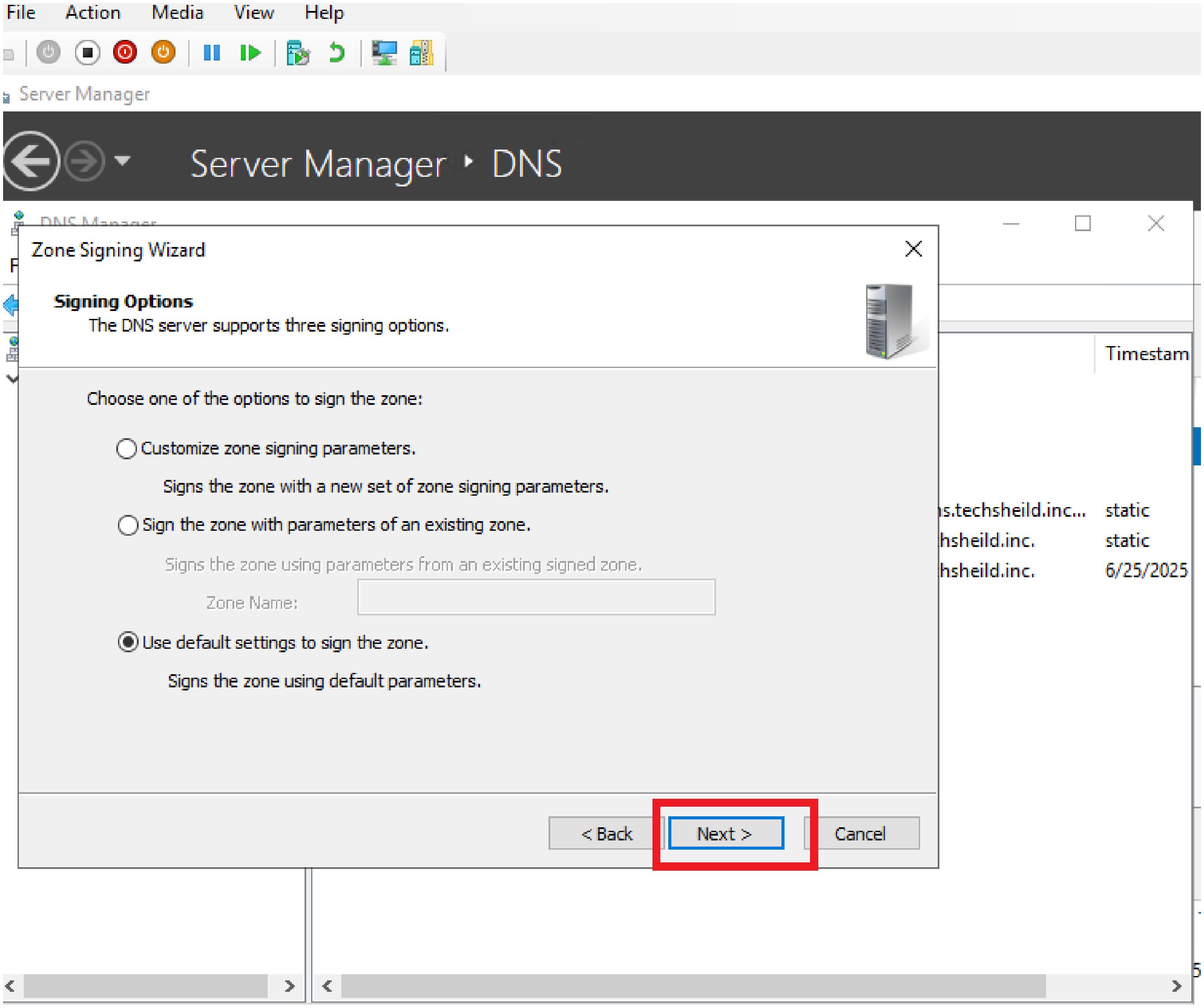
Dynamic updates: Secure only

Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

To set aging/scavenging properties, click Aging.



Name	Type	Data
_msdcs		
_sites		
_tcp		
	Start of Authority (SOA)	[31], dc_dns.techsheild.
	Name Server (NS)	dc_dns.techsheild.inc.
	Host (A)	192.168.0.1
	RR Signature (RRSIG)	[DNSKEY][Inception(UT
	RR Signature (RRSIG)	[DNSKEY][Inception(UT
	RR Signature (RRSIG)	[A][Inception(UTC): 6/2
		[N][Inception(UTC): 6/
		[N EC3PARAM][Incepti
		[SOA][Inception(UTC):
		[257][DNSSEC][RSA/SH
	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SH
	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SH
	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SH
	Next Secure 3 Parameter...	[SHA-1][0][50][AD91C7



Zone Signing Wizard

Signing Options

The DNS server supports three signing options.

Choose one of the options to sign the zone:

○ Customize zone signing parameters.

Signs the zone with a new set of zone signing parameters.

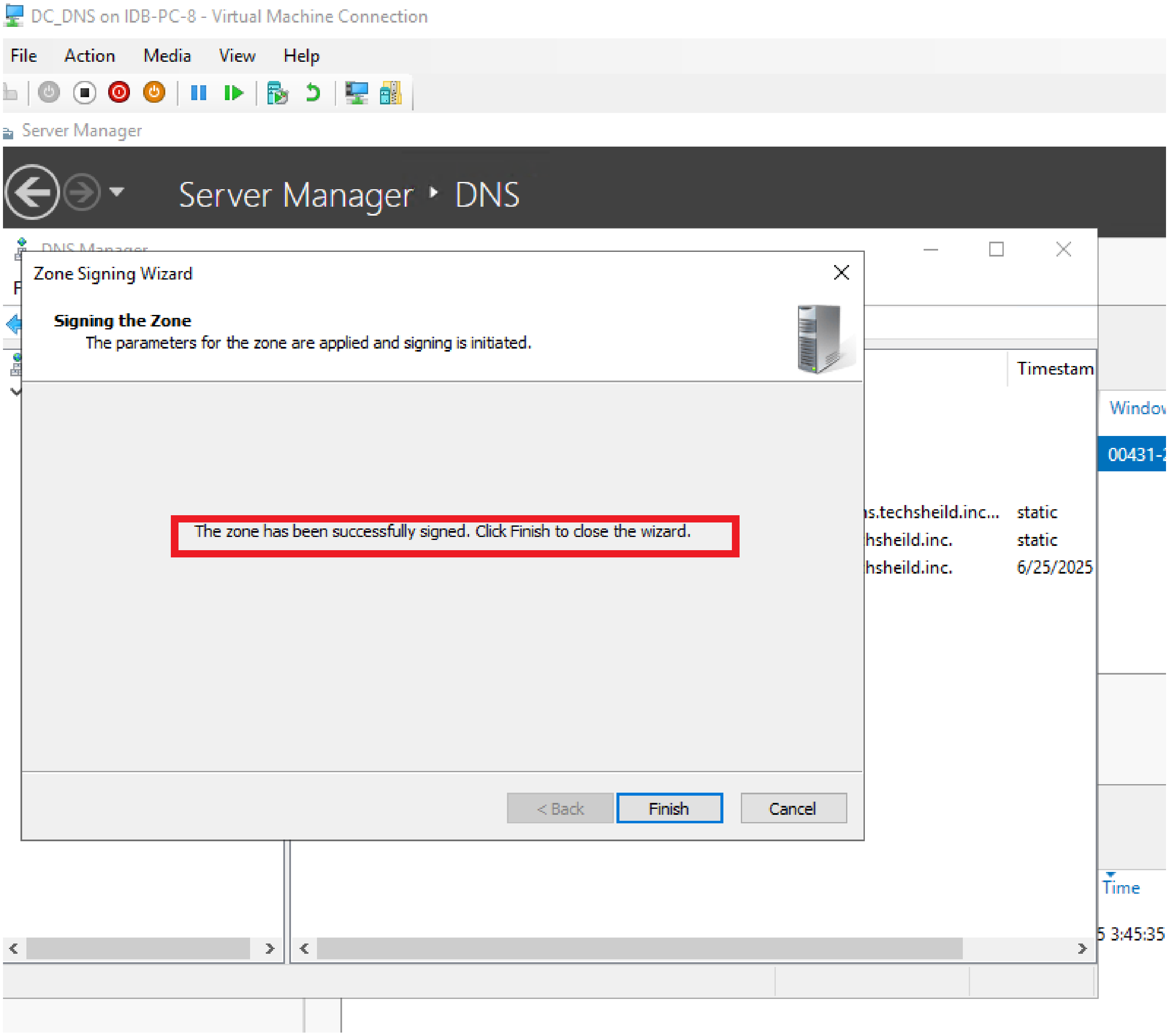
○ Sign the zone with parameters of an existing zone.

Signs the zone using parameters from an existing signed zone.

Zone Name:

● Use default settings to sign the zone.

Signs the zone using default parameters.



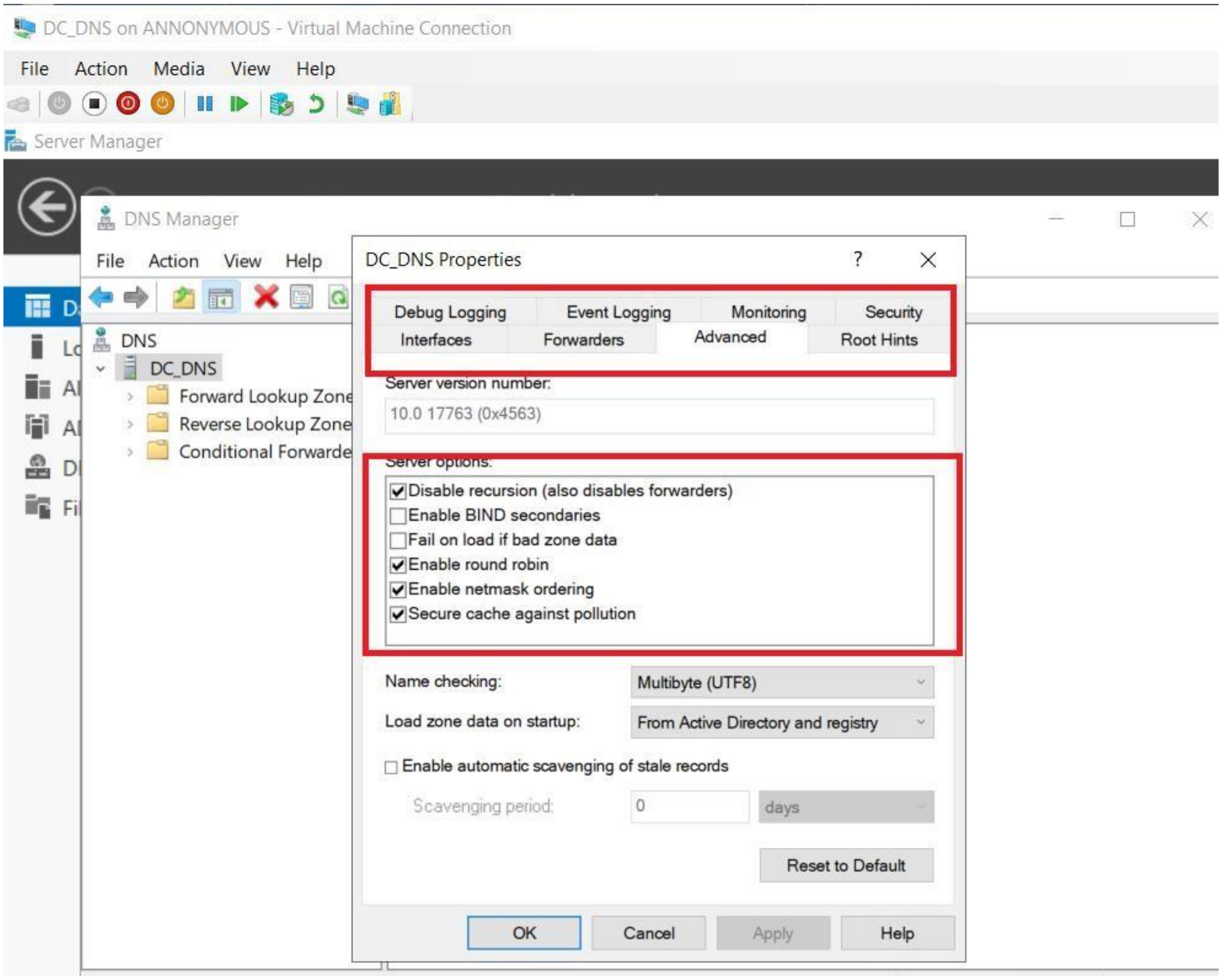
Zone Signing Wizard

Signing the Zone

The parameters for the zone are applied and signing is initiated.

The zone has been successfully signed. Click Finish to close the wizard.

c) Configure appropriate Logging and Recursion Control for prevent DNS Cache Poisoning.



Server version number:
10.0 17763 (0x4563)

Server options:

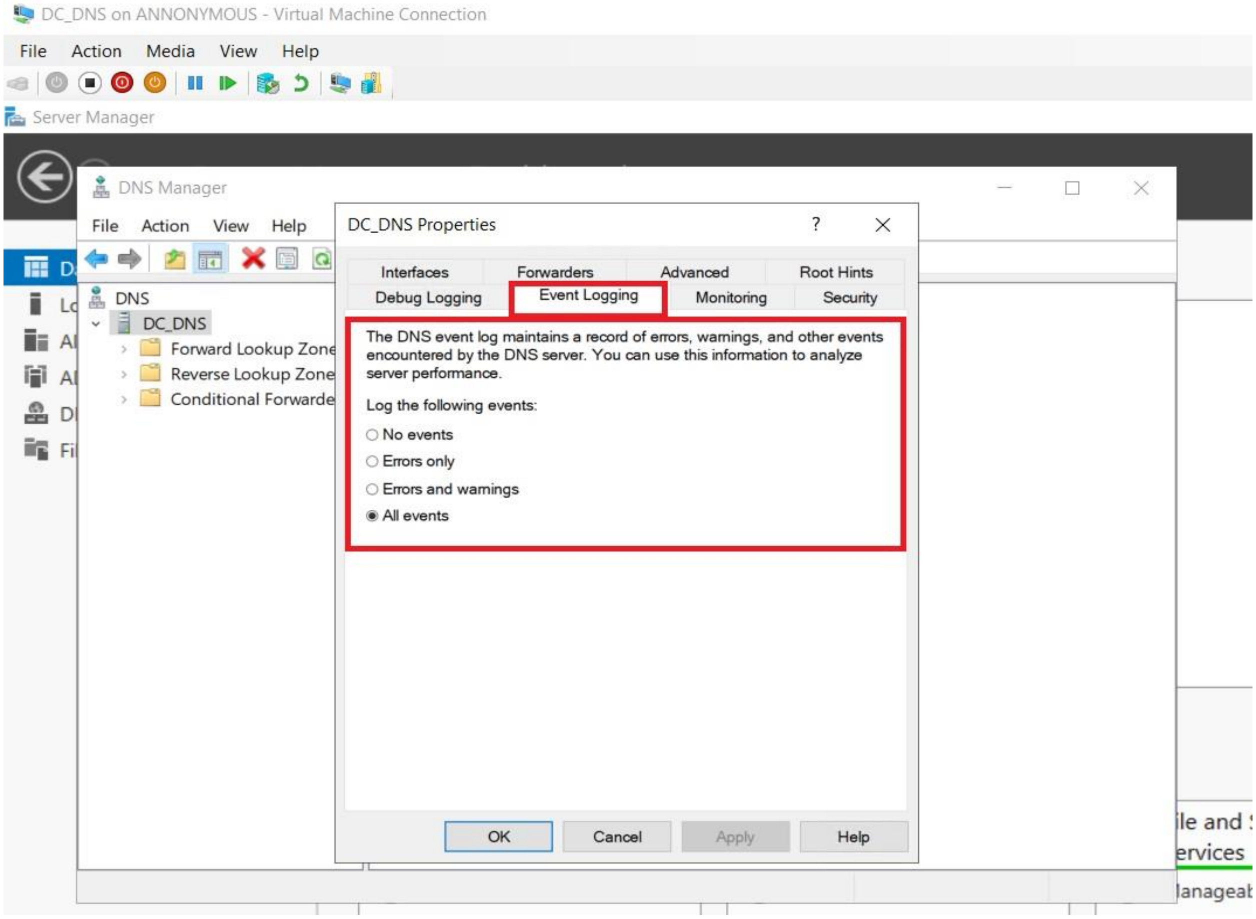
- ☑ Disable recursion (also disables forwarders)
- □ Enable BIND secondaries
- □ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

□ Enable automatic scavenging of stale records

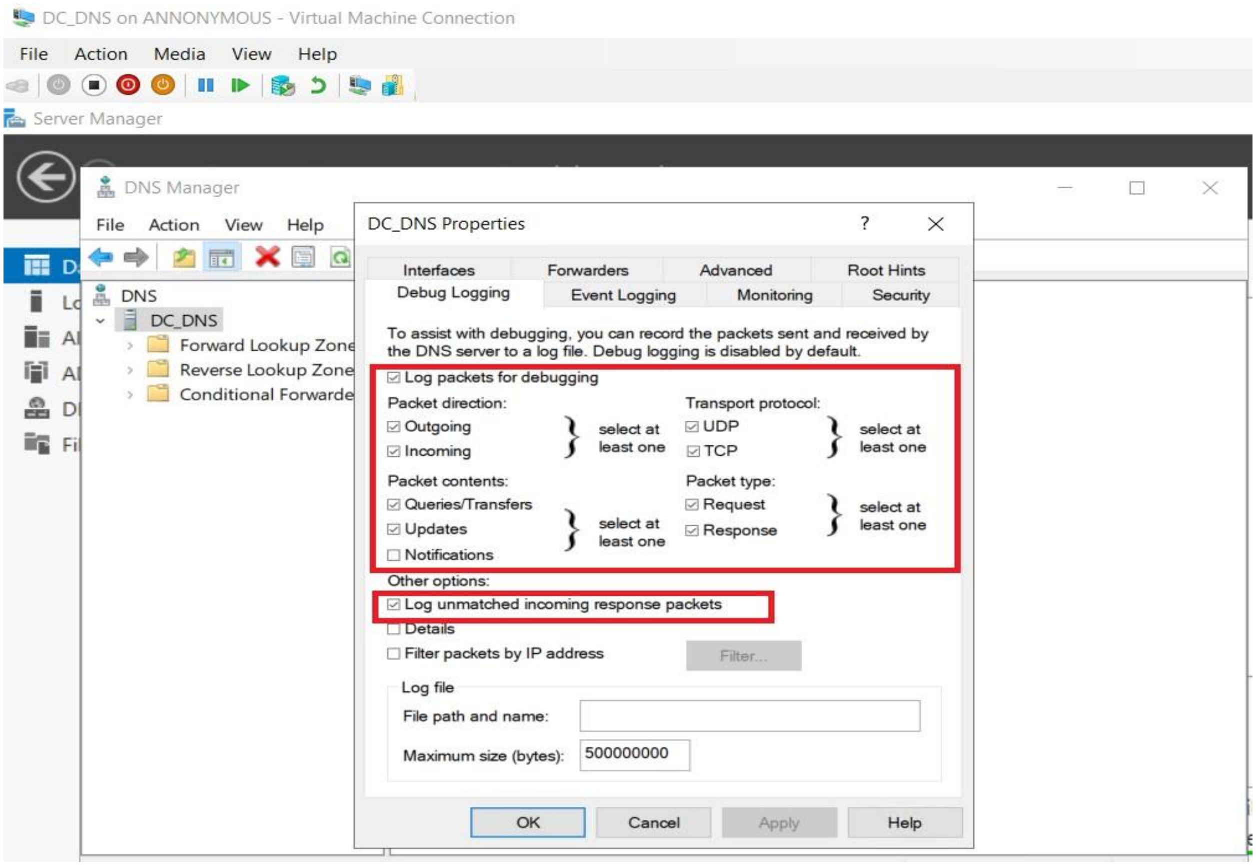
Scavenging period: 0 days



The DNS event log maintains a record of errors, warnings, and other events encountered by the DNS server. You can use this information to analyze server performance.

Log the following events:

○ No events
○ Errors only
○ Errors and warnings
● All events



To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction: ☑ Outgoing ☑ Incoming } select at least one

Transport protocol: ☑ UDP ☑ TCP } select at least one

Packet contents: ☑ Queries/Transfers ☑ Updates □ Notifications } select at least one

Packet type: ☑ Request ☑ Response } select at least one

Other options:

☑ Log unmatched incoming response packets

□ Details

□ Filter packets by IP address Filter...

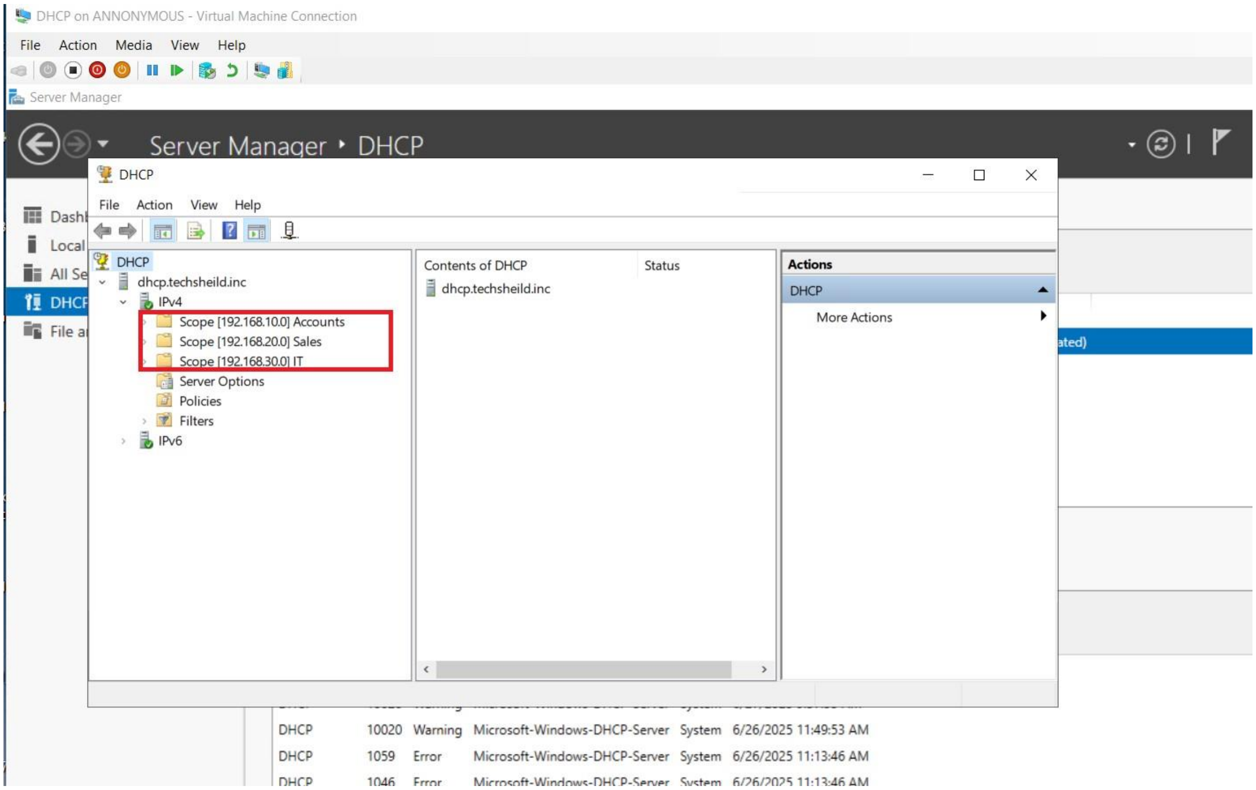
Log file

File path and name:

Maximum size (bytes): 500000000

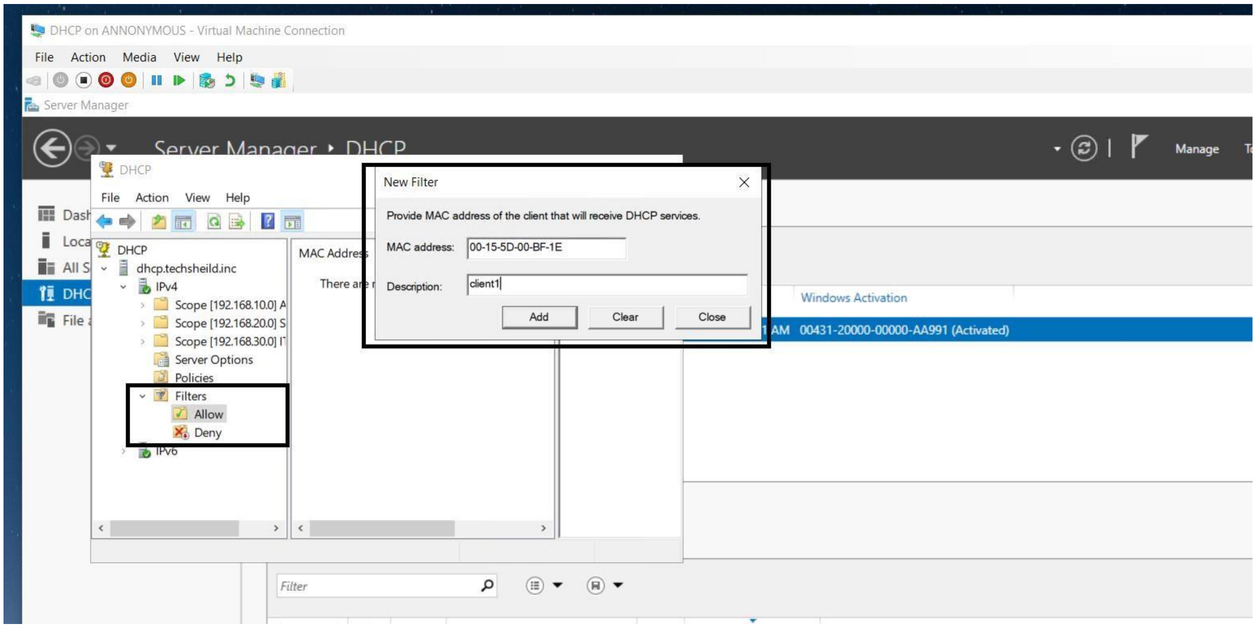
2.DHCP Security :

a) First of all I create scops or subnets named Accounts, Sales ,IT.



```
DHCP   10020  Warning  Microsoft-Windows-DHCP-Server  System  6/26/2025 11:49:53 AM
DHCP   1059   Error    Microsoft-Windows-DHCP-Server  System  6/26/2025 11:13:46 AM
DHCP   1046   Error    Microsoft-Windows-DHCP-Server  System  6/26/2025 11:13:46 AM
```

b) I configure **DHCP MAC address filtering** to allow only authorized clients to receive IP addresses



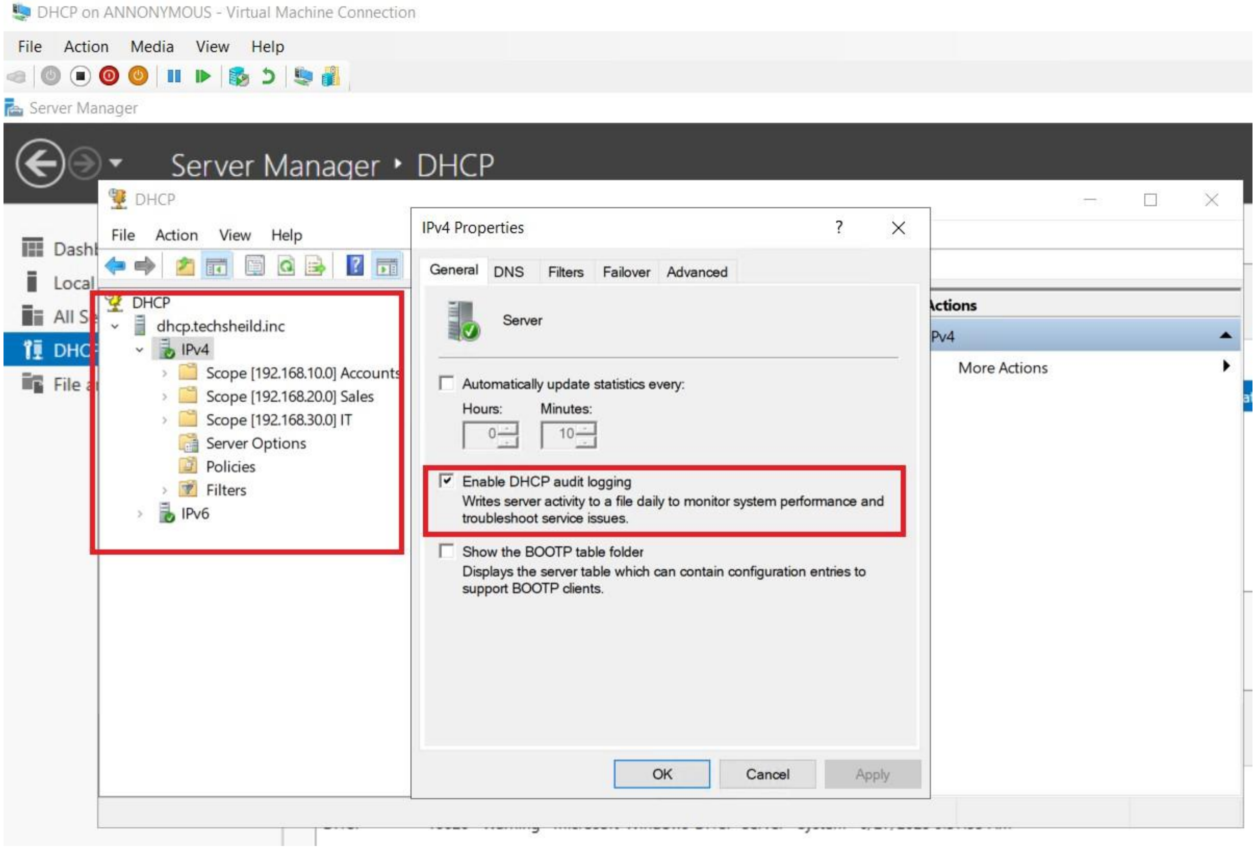
Provide MAC address of the client that will receive DHCP services.

MAC address: 00-15-5D-00-BF-1E

Description: client1

AM 00431-20000-00000-AA991 (Activated)

c) I enable **DHCP audit logging** for detect and prevent **DHCP starvation attacks**



IPv4 Properties

General | DNS | Filters | Failover | Advanced

Server

☐ Automatically update statistics every:

Hours: 0 Minutes: 10

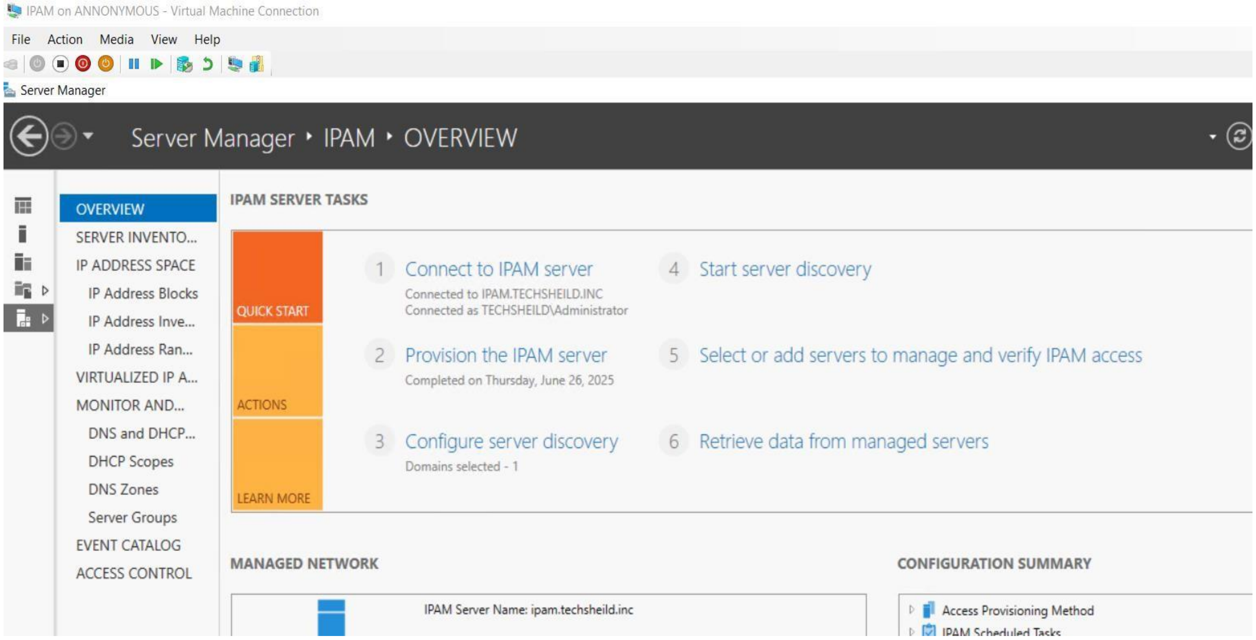
☑ Enable DHCP audit logging
Writes server activity to a file daily to monitor system performance and troubleshoot service issues.

☐ Show the BOOTP table folder
Displays the server table which can contain configuration entries to support BOOTP clients.

OK Cancel Apply

3. IPAM Configuration :

a) **Install and configure** the **IPAM Server role** in Windows Server.



IPAM SERVER TASKS

1 Connect to IPAM server
Connected to IPAM.TECHSHEILD.INC
Connected as TECHSHEILD\Administrator

2 Provision the IPAM server
Completed on Thursday, June 26, 2025

3 Configure server discovery
Domains selected - 1

4 Start server discovery

5 Select or add servers to manage and verify IPAM access

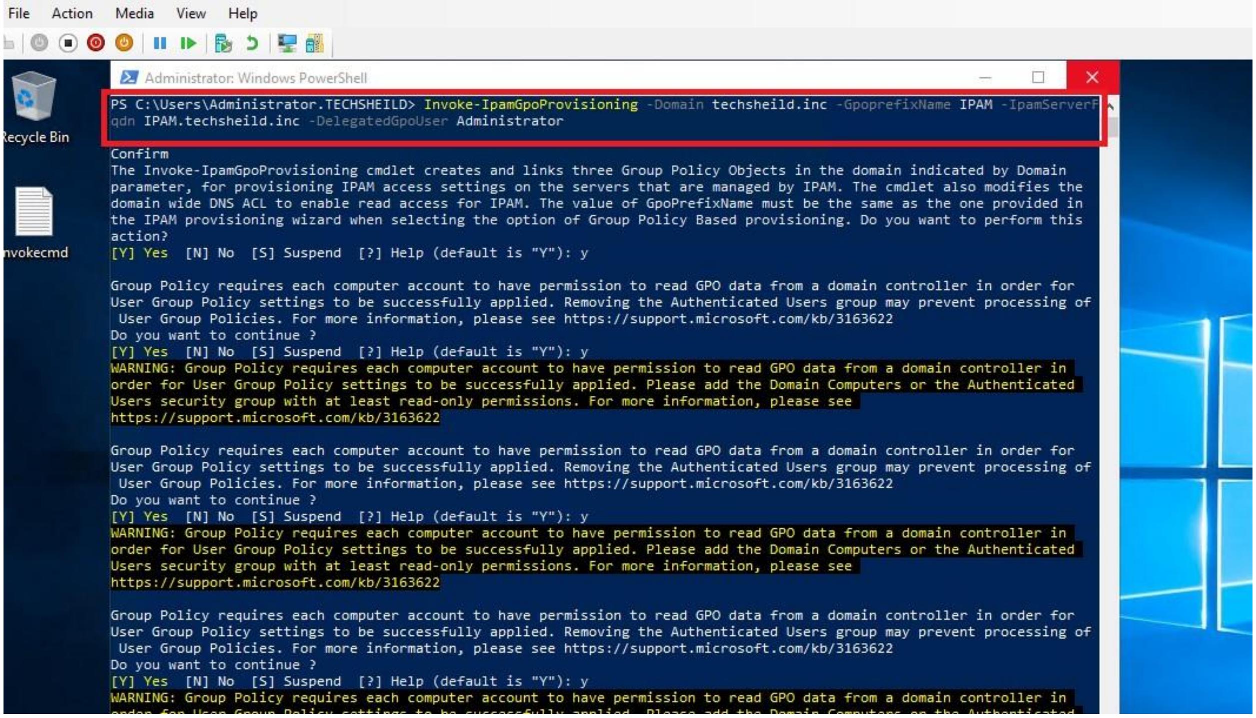
6 Retrieve data from managed servers

MANAGED NETWORK

IPAM Server Name: ipam.techsheild.inc

CONFIGURATION SUMMARY

Access Provisioning Method
IPAM Scheduled Tasks


File Action Media View Help
Recycle Bin
nvokecmd
Administrator: Windows PowerShell

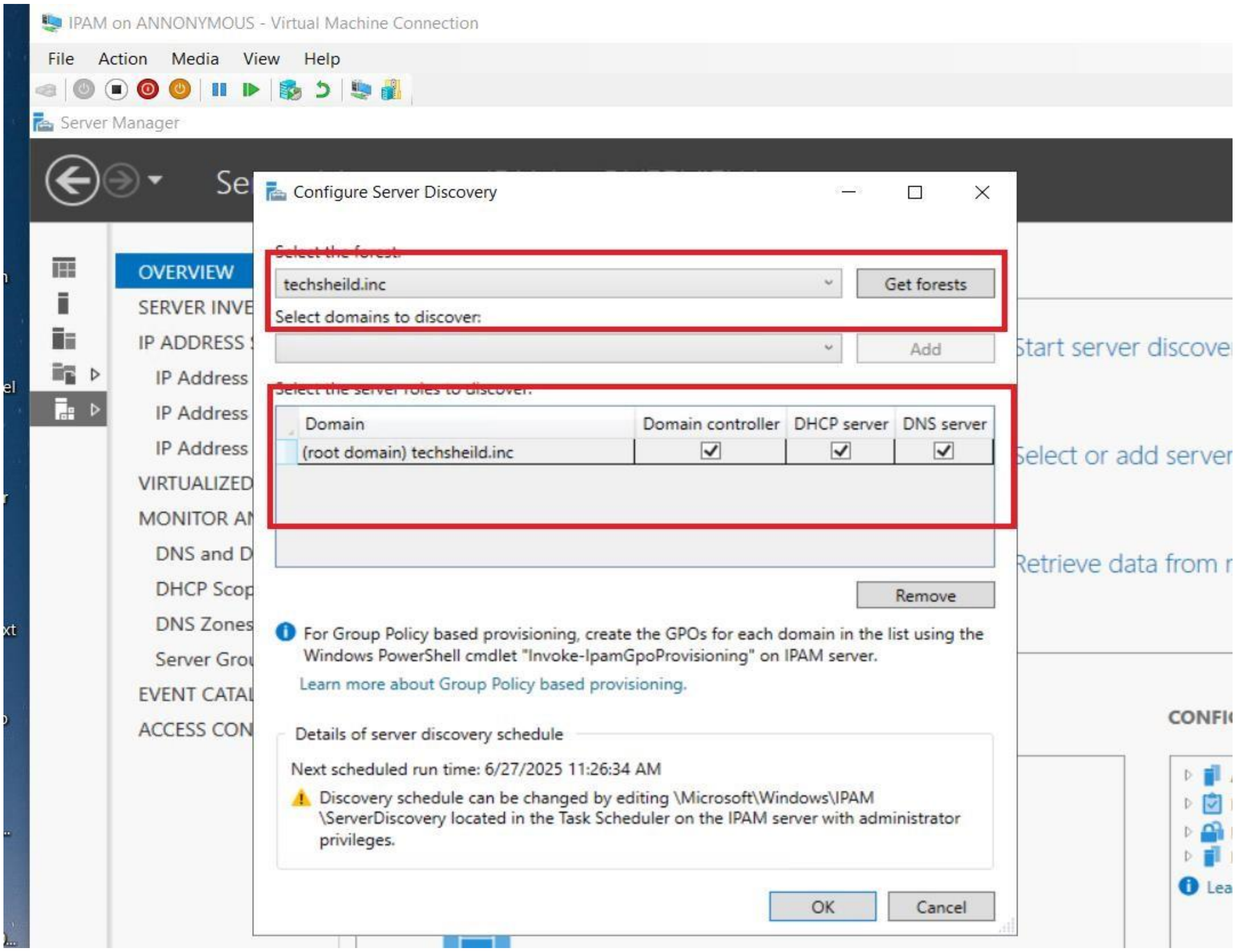
```
PS C:\Users\Administrator.TECHSHEILD> Invoke-IpamGpoProvisioning -Domain techsheild.inc -GpoprefixName IPAM -IpamServerF
qdn IPAM.techsheild.inc -DelegatedGpoUser Administrator

Confirm
The Invoke-IpamGpoProvisioning cmdlet creates and links three Group Policy Objects in the domain indicated by Domain
parameter, for provisioning IPAM access settings on the servers that are managed by IPAM. The cmdlet also modifies the
domain wide DNS ACL to enable read access for IPAM. The value of GpoPrefixName must be the same as the one provided in
the IPAM provisioning wizard when selecting the option of Group Policy Based provisioning. Do you want to perform this
action?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Group Policy requires each computer account to have permission to read GPO data from a domain controller in order for
User Group Policy settings to be successfully applied. Removing the Authenticated Users group may prevent processing of
 User Group Policies. For more information, please see https://support.microsoft.com/kb/3163622
Do you want to continue ?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
WARNING: Group Policy requires each computer account to have permission to read GPO data from a domain controller in
order for User Group Policy settings to be successfully applied. Please add the Domain Computers or the Authenticated
Users security group with at least read-only permissions. For more information, please see
https://support.microsoft.com/kb/3163622

Group Policy requires each computer account to have permission to read GPO data from a domain controller in order for
User Group Policy settings to be successfully applied. Removing the Authenticated Users group may prevent processing of
 User Group Policies. For more information, please see https://support.microsoft.com/kb/3163622
Do you want to continue ?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
WARNING: Group Policy requires each computer account to have permission to read GPO data from a domain controller in
order for User Group Policy settings to be successfully applied. Please add the Domain Computers or the Authenticated
Users security group with at least read-only permissions. For more information, please see
https://support.microsoft.com/kb/3163622

Group Policy requires each computer account to have permission to read GPO data from a domain controller in order for
User Group Policy settings to be successfully applied. Removing the Authenticated Users group may prevent processing of
 User Group Policies. For more information, please see https://support.microsoft.com/kb/3163622
Do you want to continue ?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
WARNING: Group Policy requires each computer account to have permission to read GPO data from a domain controller in
```



Configure Server Discovery

Select the forest:

techsheild.inc | Get forests

Select domains to discover:

Add

Select the server roles to discover:

Domain	Domain controller	DHCP server	DNS server
(root domain) techsheild.inc	☑	☑	☑

Remove

For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.

Learn more about Group Policy based provisioning.

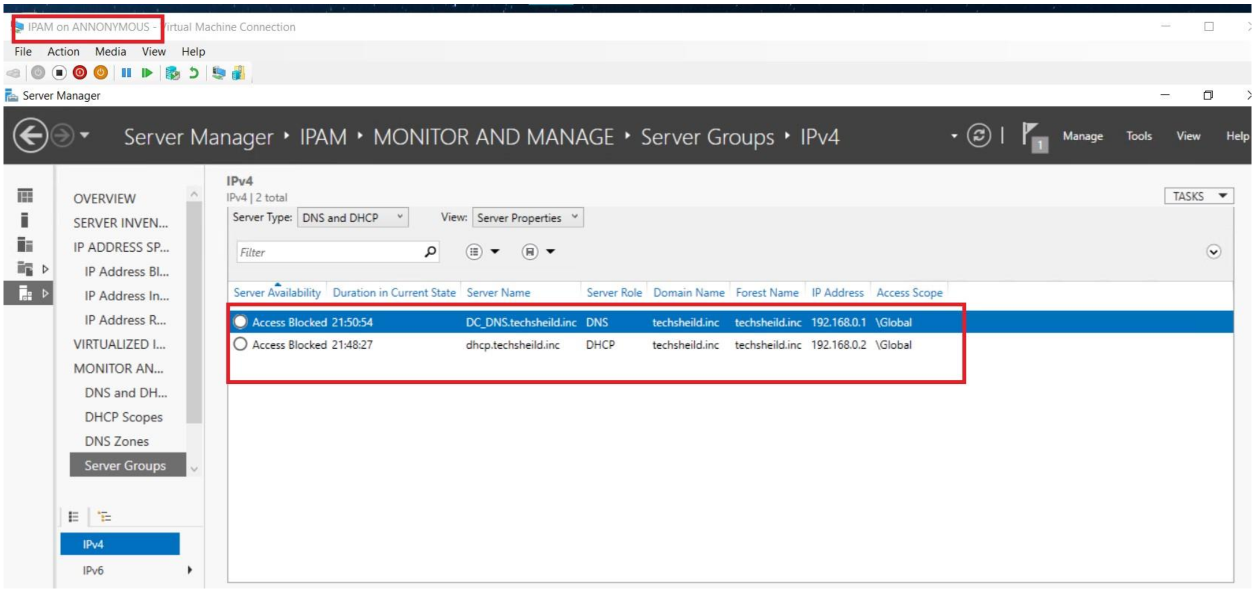
Details of server discovery schedule

Next scheduled run time: 6/27/2025 11:26:34 AM

Discovery schedule can be changed by editing \Microsoft\Windows\IPAM \ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.

OK | Cancel

b) I configure IPAM to **centrally manage DHCP and DNS servers**.



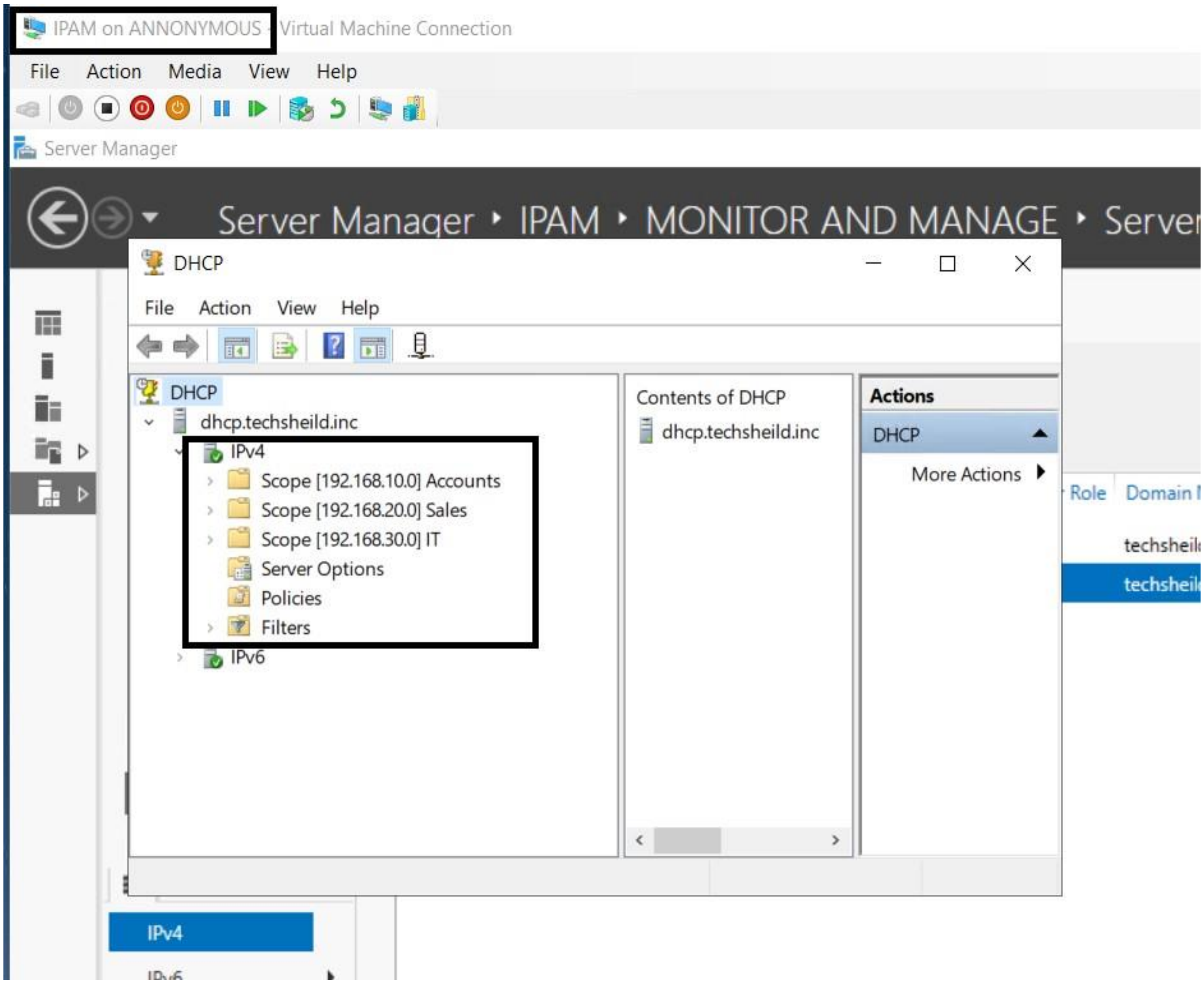
IPv4

IPv4 | 2 total

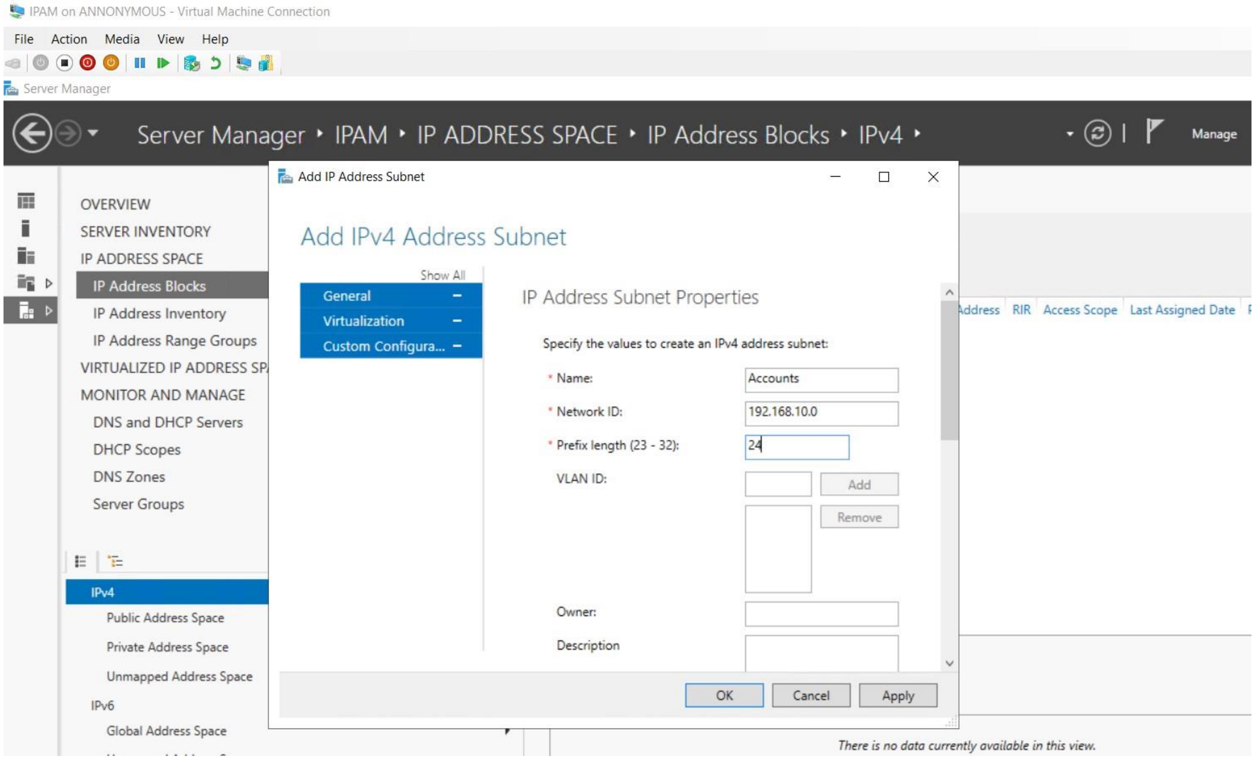
Server Type: DNS and DHCP

View: Server Properties

Server Availability	Duration in Current State	Server Name	Server Role	Domain Name	Forest Name	IP Address	Access Scope
○ Access Blocked	21:50:54	DC_DNS.techsheild.inc	DNS	techsheild.inc	techsheild.inc	192.168.0.1	\Global
○ Access Blocked	21:48:27	dhcp.techsheild.inc	DHCP	techsheild.inc	techsheild.inc	192.168.0.2	\Global



c) Enable IP Utilization Monitoring and ensure IP Conflict Reporting .

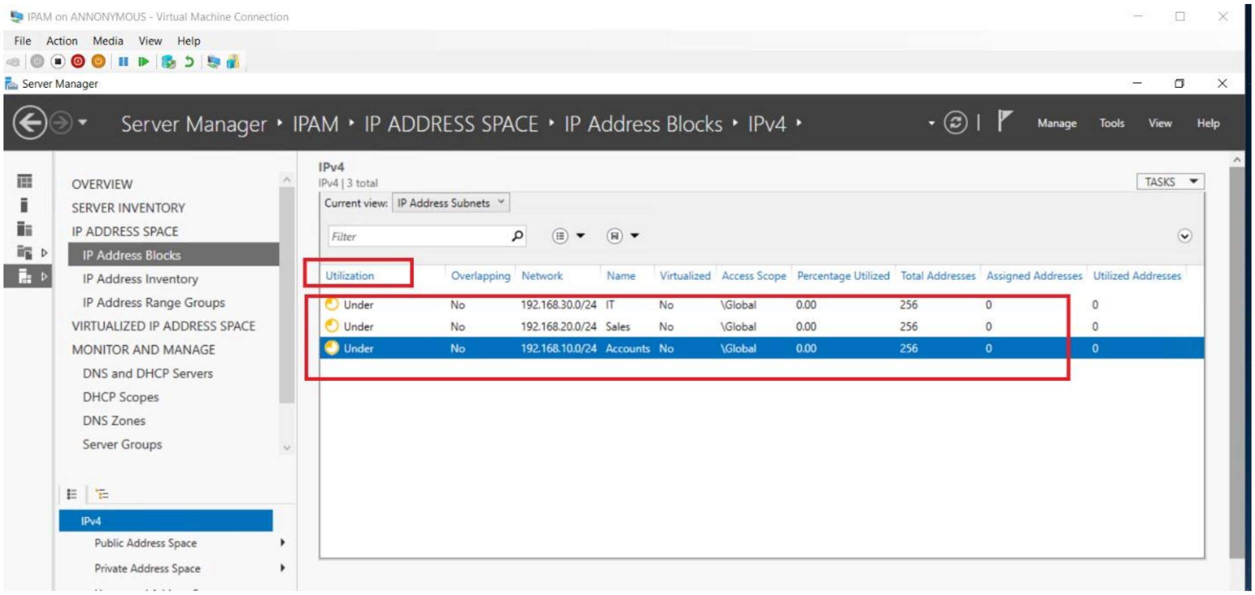


Add IPv4 Address Subnet

IP Address Subnet Properties

Specify the values to create an IPv4 address subnet:

- Name: Accounts
- Network ID: 192.168.10.0
- Prefix length (23 - 32): 24



IPv4

IPv4 | 3 total

Current view: IP Address Subnets

Utilization	Overlapping	Network	Name	Virtualized	Access Scope	Percentage Utilized	Total Addresses	Assigned Addresses	Utilized Addresses
Under	No	192.168.30.0/24	IT	No	\Global	0.00	256	0	0
Under	No	192.168.20.0/24	Sales	No	\Global	0.00	256	0	0
Under	No	192.168.10.0/24	Accounts	No	\Global	0.00	256	0	0

Conclusion : In this lab, we have successfully demonstrated the design and implementation of a secure, domain-based network using Windows Server. The core services—DNS, DHCP, and IPAM— wereconfigured with enhanced security practices toensure data integrity, prevent unauthorized access, and maintain IP address management accuracy.