Lab Assignment

Cybersecurity Professional Program

Microsoft Security

Security Policies & Authentication

MS-10-L1 Hardening LLMNR, NetBIOS & SMB

Lab Objective

Understand the fundamentals of service hardening and the importance of securing services against potential exploits.

Lab Mission

Disable the functionality of the LLMNR and NetBIOS services to prevent legacy name resolution and harden SMB security.

Lab Duration

30–45 minutes

Requirements

- Basic working knowledge of Windows Server
- Basic working knowledge of Windows client
- Basic understanding of LLMNR, NetBIOS, and SMB

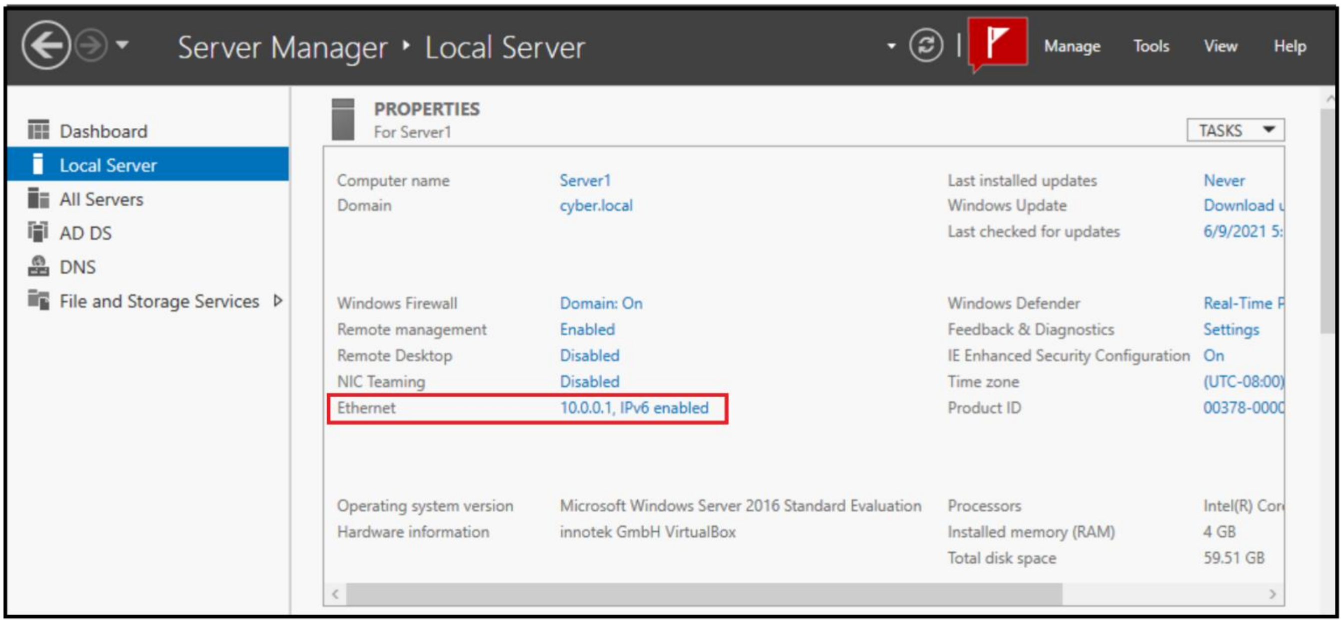
Resources

- Environment & Tools
    - VirtualBox
        - Windows Server 2016
        - Windows 7

Lab Task 1: Disable NetBIOS

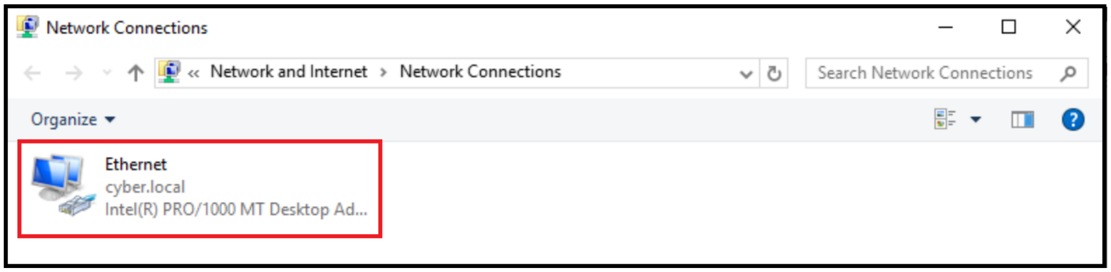
In this task, you will disable NetBIOS to prevent it from establishing connections.

1 On Server1, click on the ethernet section to open the network connections.



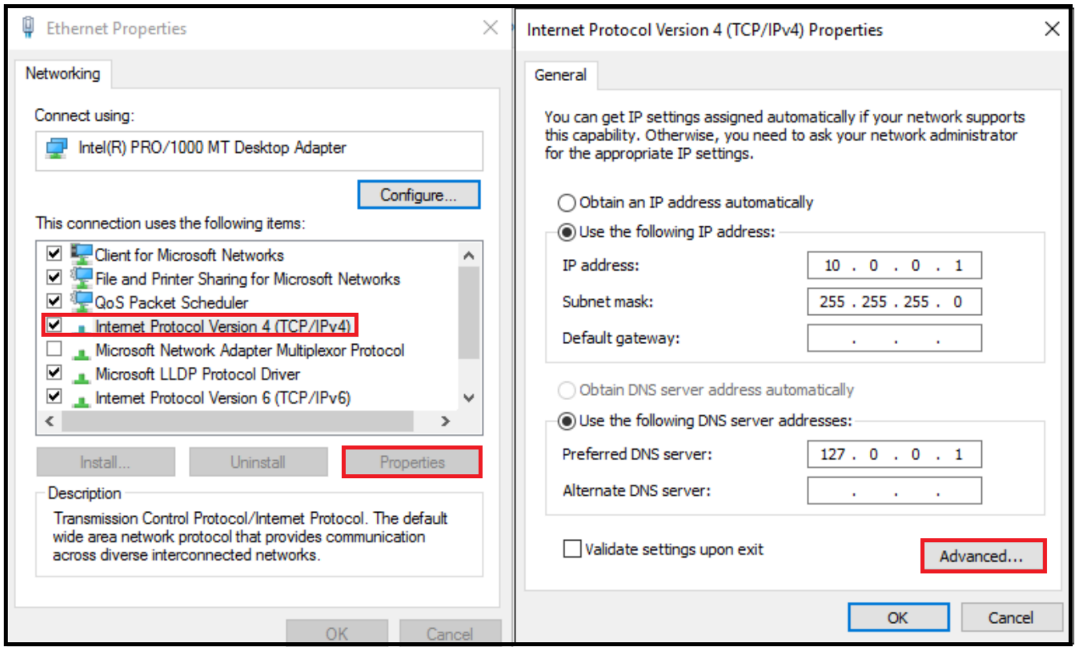
Computer name	Server1	Last installed updates	Never
Domain	cyber.local	Windows Update	Download u
		Last checked for updates	6/9/2021 5:
Windows Firewall	Domain: On	Windows Defender	Real-Time P
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00)
Ethernet	10.0.0.1, IPv6 enabled	Product ID	00378-0000
Operating system version	Microsoft Windows Server 2016 Standard Evaluation	Processors	Intel(R) Cor
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)	4 GB
		Total disk space	59.51 GB

2 Right click **Ethernet** and open its properties.


Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize

Ethernet
cyber.local
Intel(R) PRO/1000 MT Desktop Ad...

3 Double-click ***Internet Protocol Version 4 (TCP/IPv4)*** and click ***Advanced...***



Ethernet Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 0 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

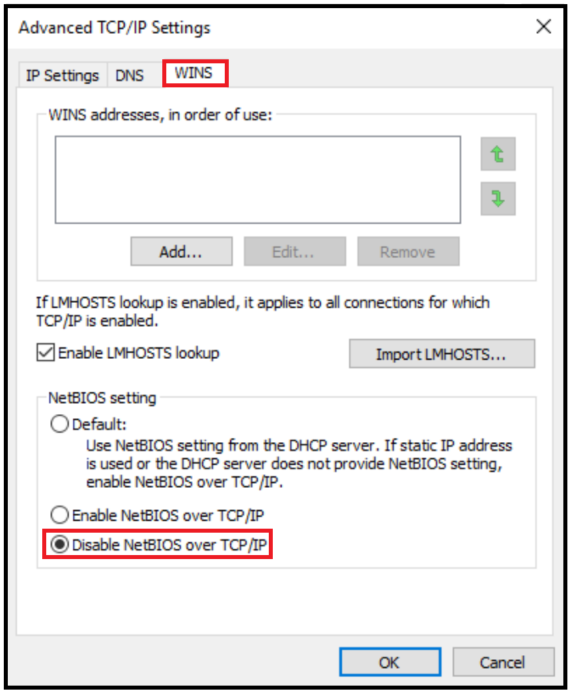
Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK Cancel

4 Navigate to **WINS** and select ***Disable NetBIOS over TCP/IP***. This option prevents the computer from using NetBIOS.



Advanced TCP/IP Settings

IP Settings DNS WINS

WINS addresses, in order of use:

Add... Edit... Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

Import LMHOSTS...

NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

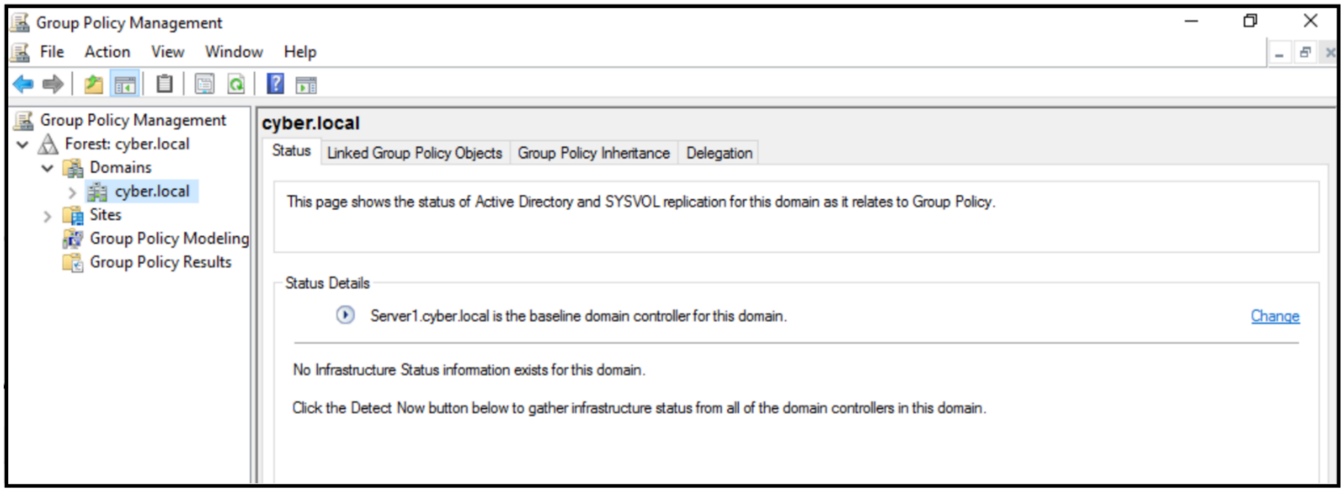
○ Enable NetBIOS over TCP/IP
● Disable NetBIOS over TCP/IP

OK Cancel

Lab Task 2: Disable LLMNR

In this task, you will disable LLMNR activity using a GPO.

1 On Server1, open the **Group Policy Management** tool.



cyber.local

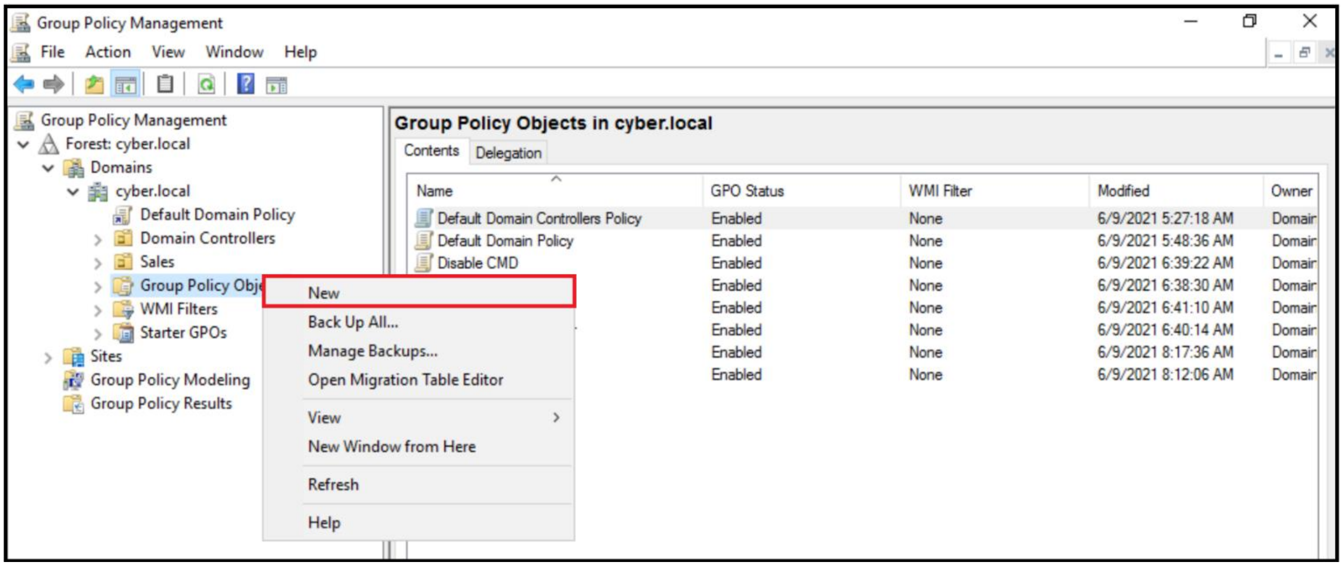
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

Server1.cyber.local is the baseline domain controller for this domain.

No Infrastructure Status information exists for this domain.

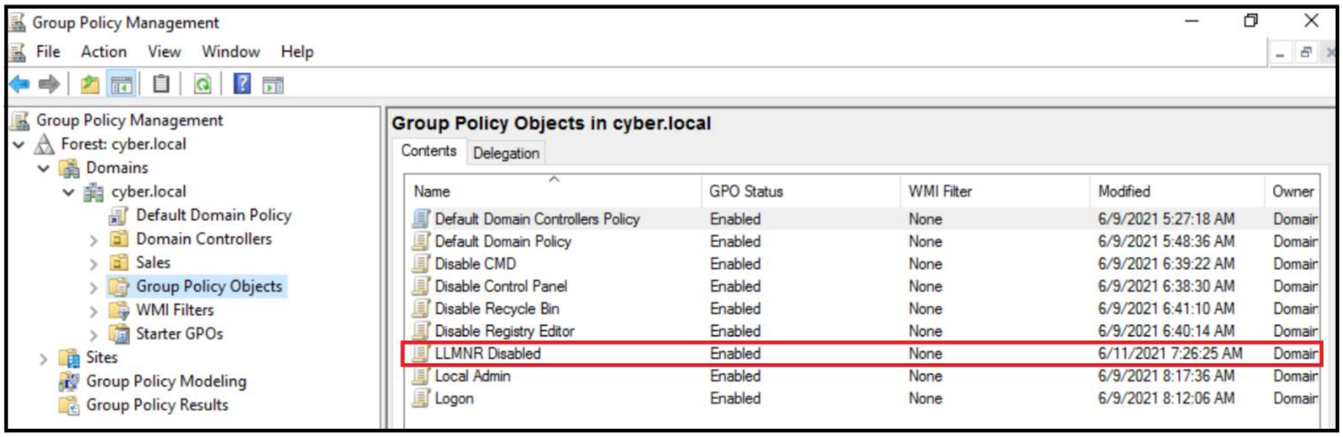
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

2 In ***cyber.local***, create a new GPO named **LLMNR Disabled** in the ***Group Policy Objects*** folder.



Group Policy Objects in cyber.local

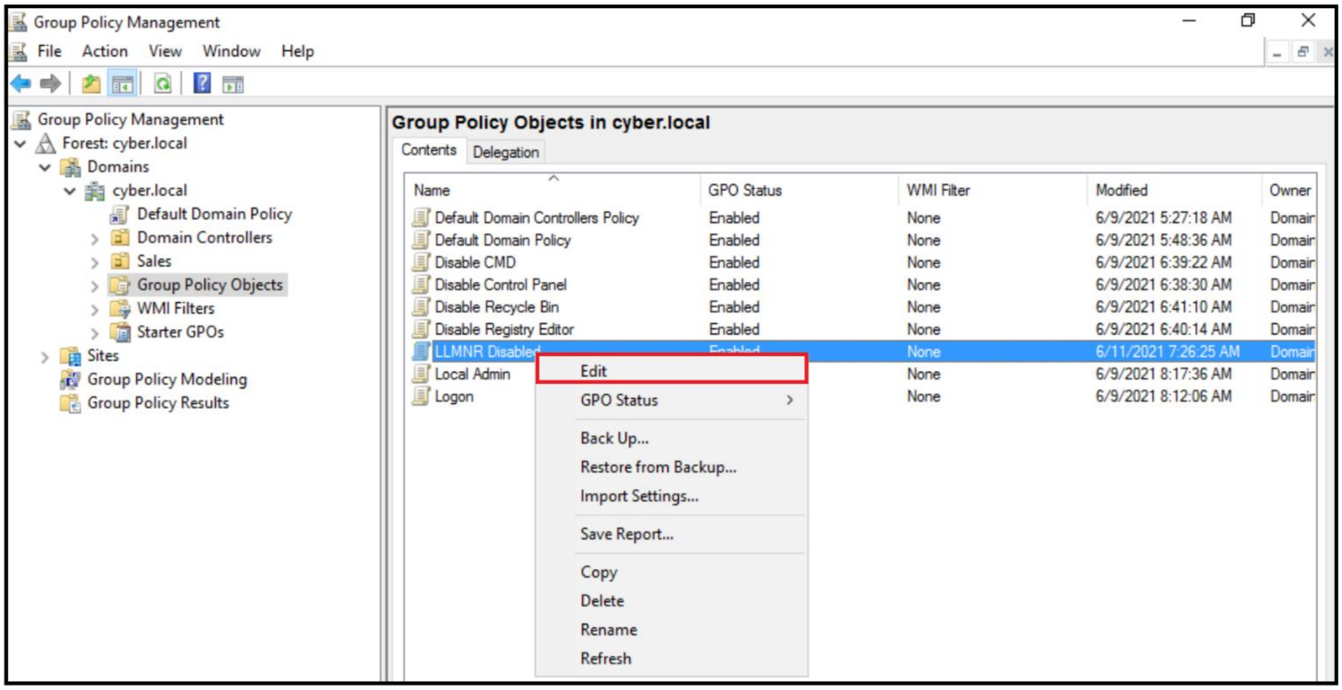
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
	Enabled	None	6/9/2021 6:38:30 AM	Domair
	Enabled	None	6/9/2021 6:41:10 AM	Domair
	Enabled	None	6/9/2021 6:40:14 AM	Domair
	Enabled	None	6/9/2021 8:17:36 AM	Domair
	Enabled	None	6/9/2021 8:12:06 AM	Domair



Group Policy Objects in cyber.local

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
Disable Control Panel	Enabled	None	6/9/2021 6:38:30 AM	Domair
Disable Recycle Bin	Enabled	None	6/9/2021 6:41:10 AM	Domair
Disable Registry Editor	Enabled	None	6/9/2021 6:40:14 AM	Domair
LLMNR Disabled	Enabled	None	6/11/2021 7:26:25 AM	Domair
Local Admin	Enabled	None	6/9/2021 8:17:36 AM	Domair
Logon	Enabled	None	6/9/2021 8:12:06 AM	Domair

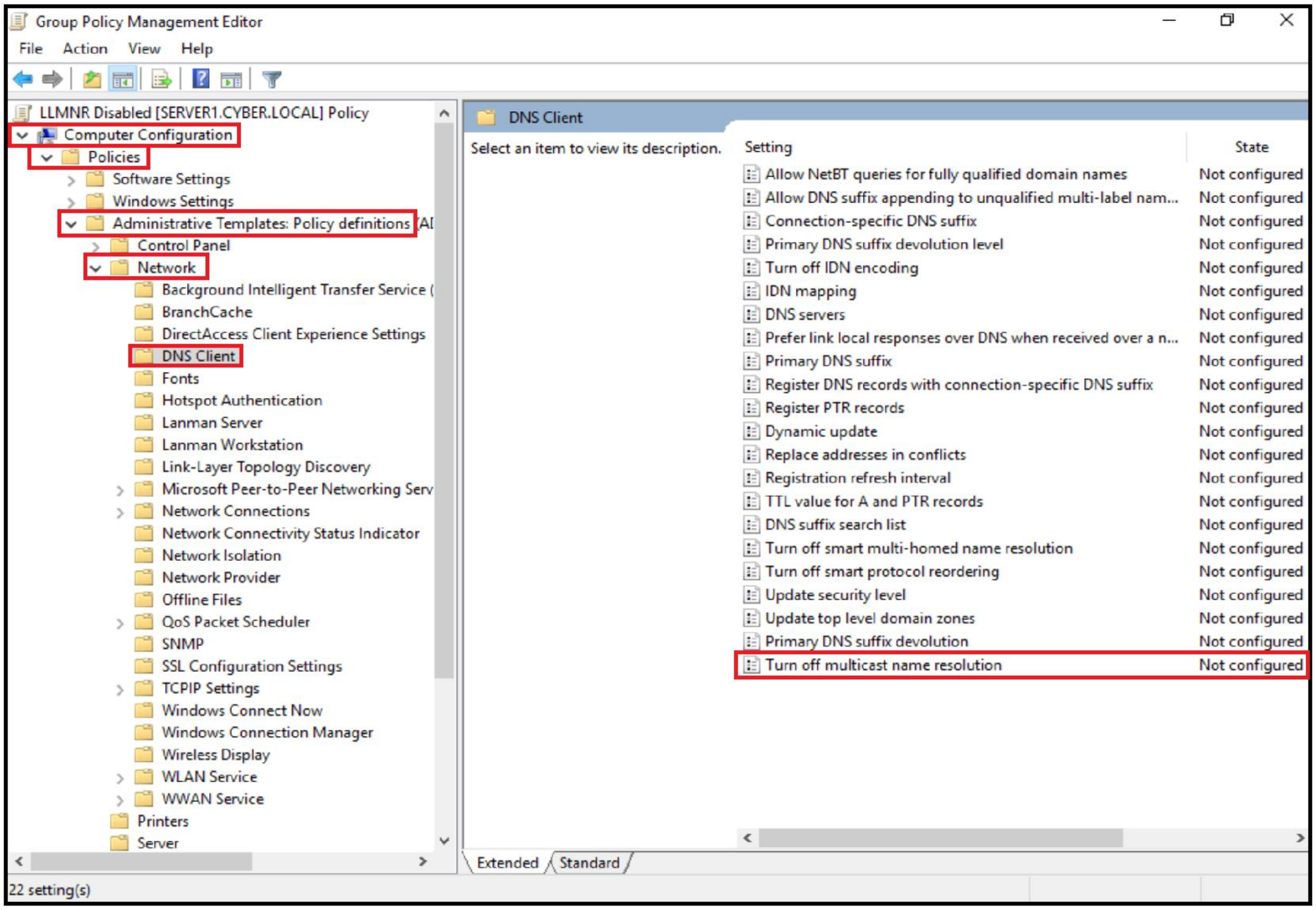
3 Right-click the ***LLMNR Disabled*** GPO and enter its editor.



Group Policy Objects in cyber.local

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
Disable Control Panel	Enabled	None	6/9/2021 6:38:30 AM	Domair
Disable Recycle Bin	Enabled	None	6/9/2021 6:41:10 AM	Domair
Disable Registry Editor	Enabled	None	6/9/2021 6:40:14 AM	Domair
LLMNR Disabled	Enabled	None	6/11/2021 7:26:25 AM	Domair
Local Admin		None	6/9/2021 8:17:36 AM	Domair
Logon		None	6/9/2021 8:12:06 AM	Domair

4 Navigate to ***Computer Configuration*** > ***Policies*** > ***Administrative Templates*** > ***Network*** > ***DNS Client***.



LLMNR Disabled [SERVER1.CYBER.LOCAL] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (AI
      - Control Panel
      - Network
        - Background Intelligent Transfer Service (
        - BranchCache
        - DirectAccess Client Experience Settings
        - DNS Client
        - Fonts
        - Hotspot Authentication
        - Lanman Server
        - Lanman Workstation
        - Link-Layer Topology Discovery
        - Microsoft Peer-to-Peer Networking Serv
        - Network Connections
        - Network Connectivity Status Indicator
        - Network Isolation
        - Network Provider
        - Offline Files
        - QoS Packet Scheduler
        - SNMP
        - SSL Configuration Settings
        - TCPIP Settings
        - Windows Connect Now
        - Windows Connection Manager
        - Wireless Display
        - WLAN Service
        - WWAN Service
      - Printers
      - Server

DNS Client

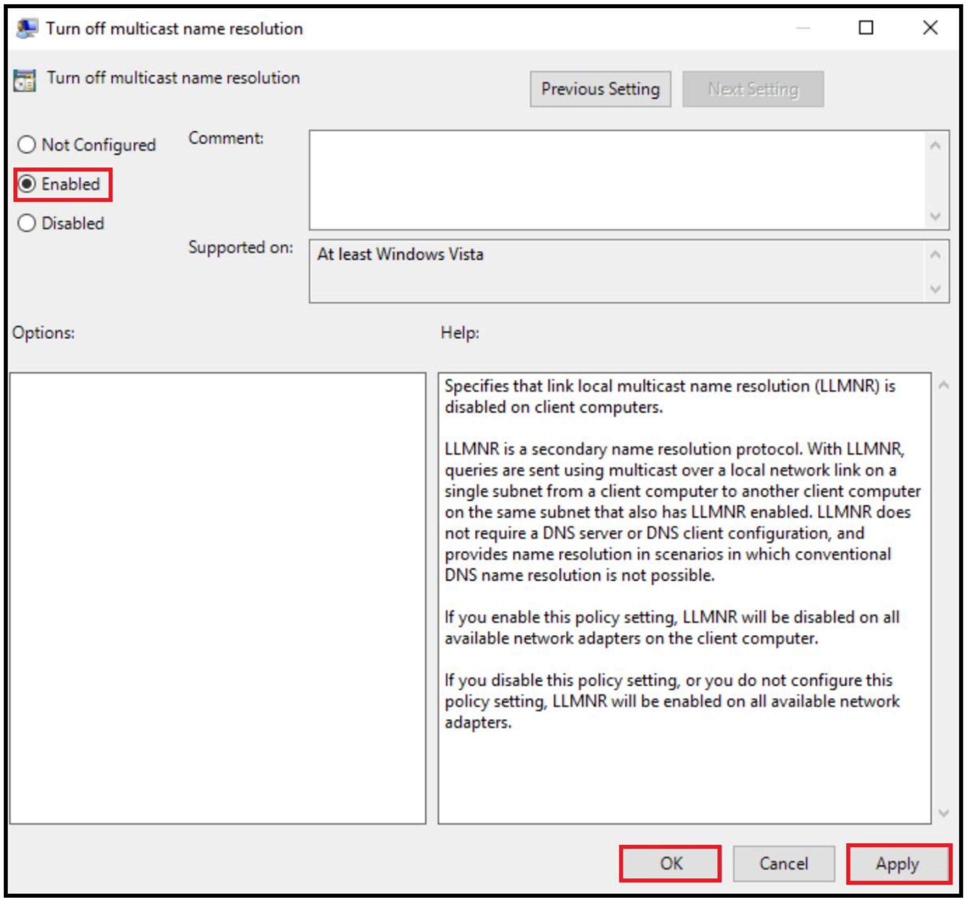
Select an item to view its description.

Setting	State
Allow NetBT queries for fully qualified domain names	Not configured
Allow DNS suffix appending to unqualified multi-label nam...	Not configured
Connection-specific DNS suffix	Not configured
Primary DNS suffix devolution level	Not configured
Turn off IDN encoding	Not configured
IDN mapping	Not configured
DNS servers	Not configured
Prefer link local responses over DNS when received over a n...	Not configured
Primary DNS suffix	Not configured
Register DNS records with connection-specific DNS suffix	Not configured
Register PTR records	Not configured
Dynamic update	Not configured
Replace addresses in conflicts	Not configured
Registration refresh interval	Not configured
TTL value for A and PTR records	Not configured
DNS suffix search list	Not configured
Turn off smart multi-homed name resolution	Not configured
Turn off smart protocol reordering	Not configured
Update security level	Not configured
Update top level domain zones	Not configured
Primary DNS suffix devolution	Not configured
Turn off multicast name resolution	Not configured

22 setting(s)

]

5 Right click to edit the ***Turn off multicast name resolution*** policy.



Turn off multicast name resolution

Turn off multicast name resolution

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

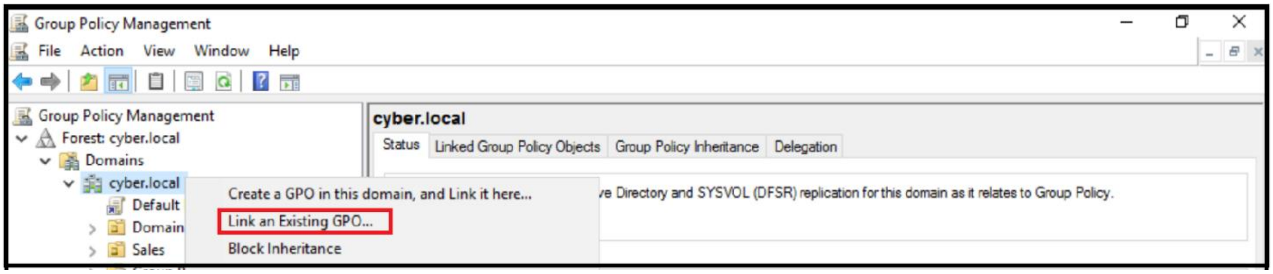
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

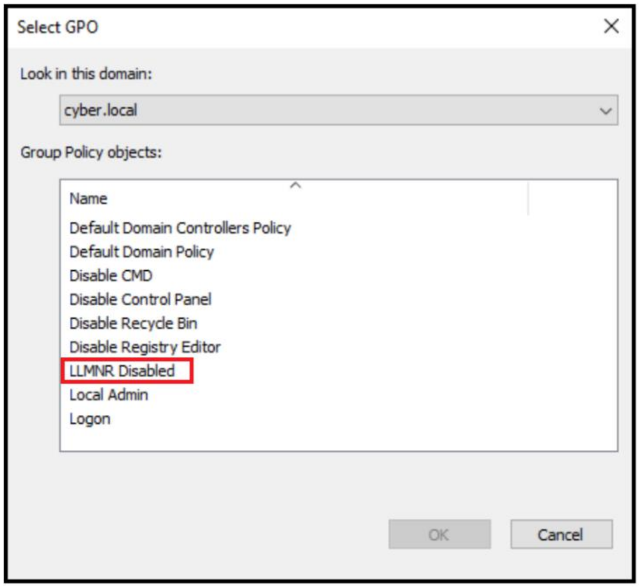
If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer.

If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.

6 In **Group Policy Management**, link the GPO **LLMNR Disabled** to the domain ***cyber.local***.



ve Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.



Look in this domain:

cyber.local

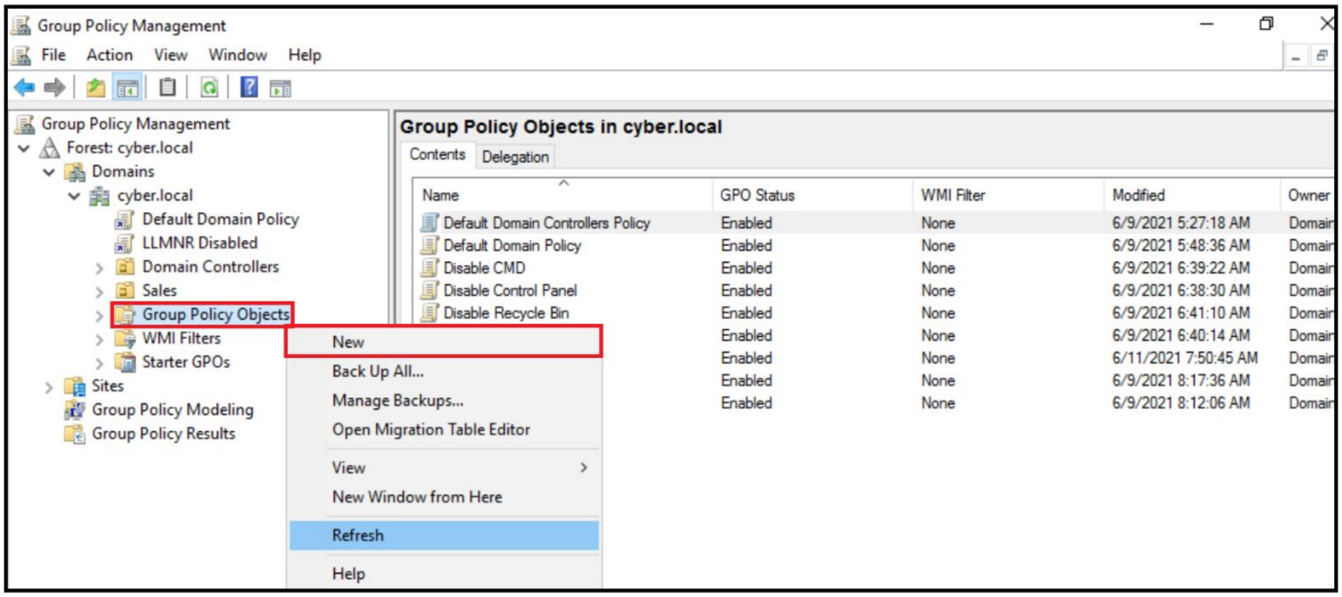
Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Disable CMD
Disable Control Panel
Disable Recycle Bin
Disable Registry Editor
LLMNR Disabled
Local Admin
Logon

Lab Task 3: SMB Signing

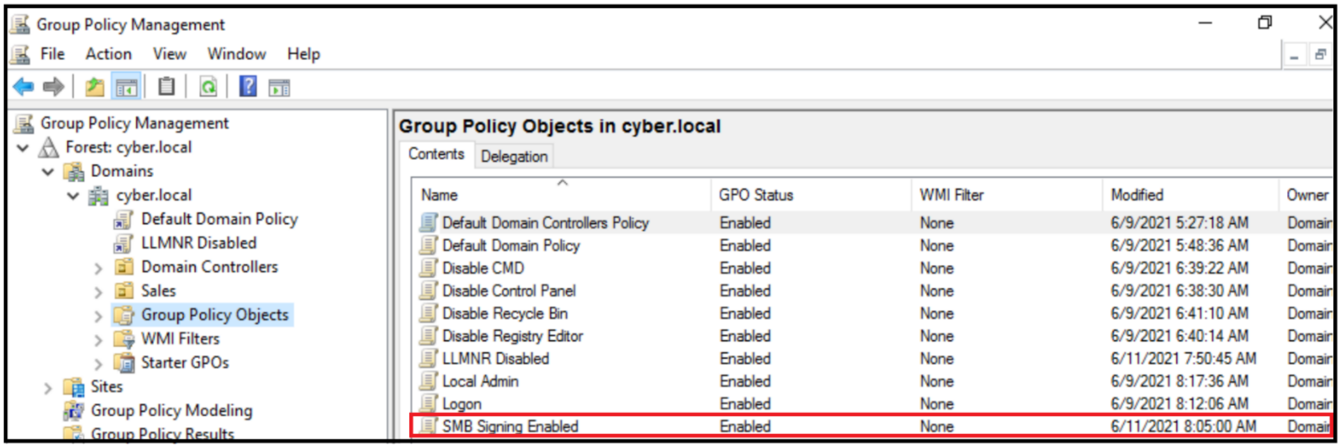
In this task, you will enable SMB signing in the organization using a GPO.

1 On Server1, open the **Group Policy Management** tool. Under ***cyber.local***, create a new GPO named **SMB Signing Enabled** in the ***Group Policy Objects*** folder.



Group Policy Objects in cyber.local

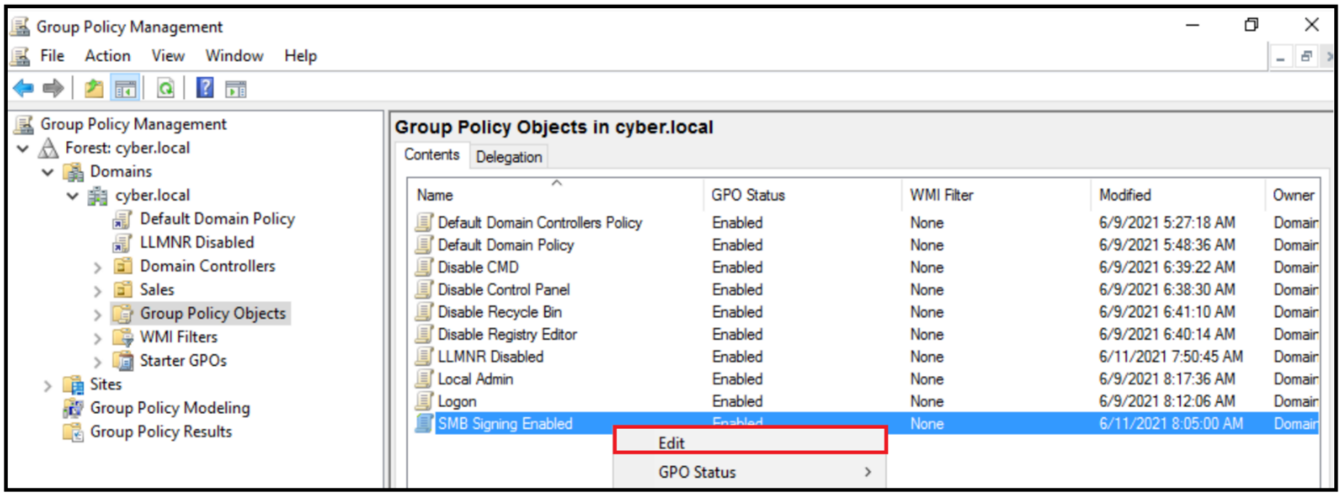
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
Disable Control Panel	Enabled	None	6/9/2021 6:38:30 AM	Domair
Disable Recycle Bin	Enabled	None	6/9/2021 6:41:10 AM	Domair
	Enabled	None	6/9/2021 6:40:14 AM	Domair
	Enabled	None	6/11/2021 7:50:45 AM	Domair
	Enabled	None	6/9/2021 8:17:36 AM	Domair
	Enabled	None	6/9/2021 8:12:06 AM	Domair



Group Policy Objects in cyber.local

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
Disable Control Panel	Enabled	None	6/9/2021 6:38:30 AM	Domair
Disable Recycle Bin	Enabled	None	6/9/2021 6:41:10 AM	Domair
Disable Registry Editor	Enabled	None	6/9/2021 6:40:14 AM	Domair
LLMNR Disabled	Enabled	None	6/11/2021 7:50:45 AM	Domair
Local Admin	Enabled	None	6/9/2021 8:17:36 AM	Domair
Logon	Enabled	None	6/9/2021 8:12:06 AM	Domair
SMB Signing Enabled	Enabled	None	6/11/2021 8:05:00 AM	Domair

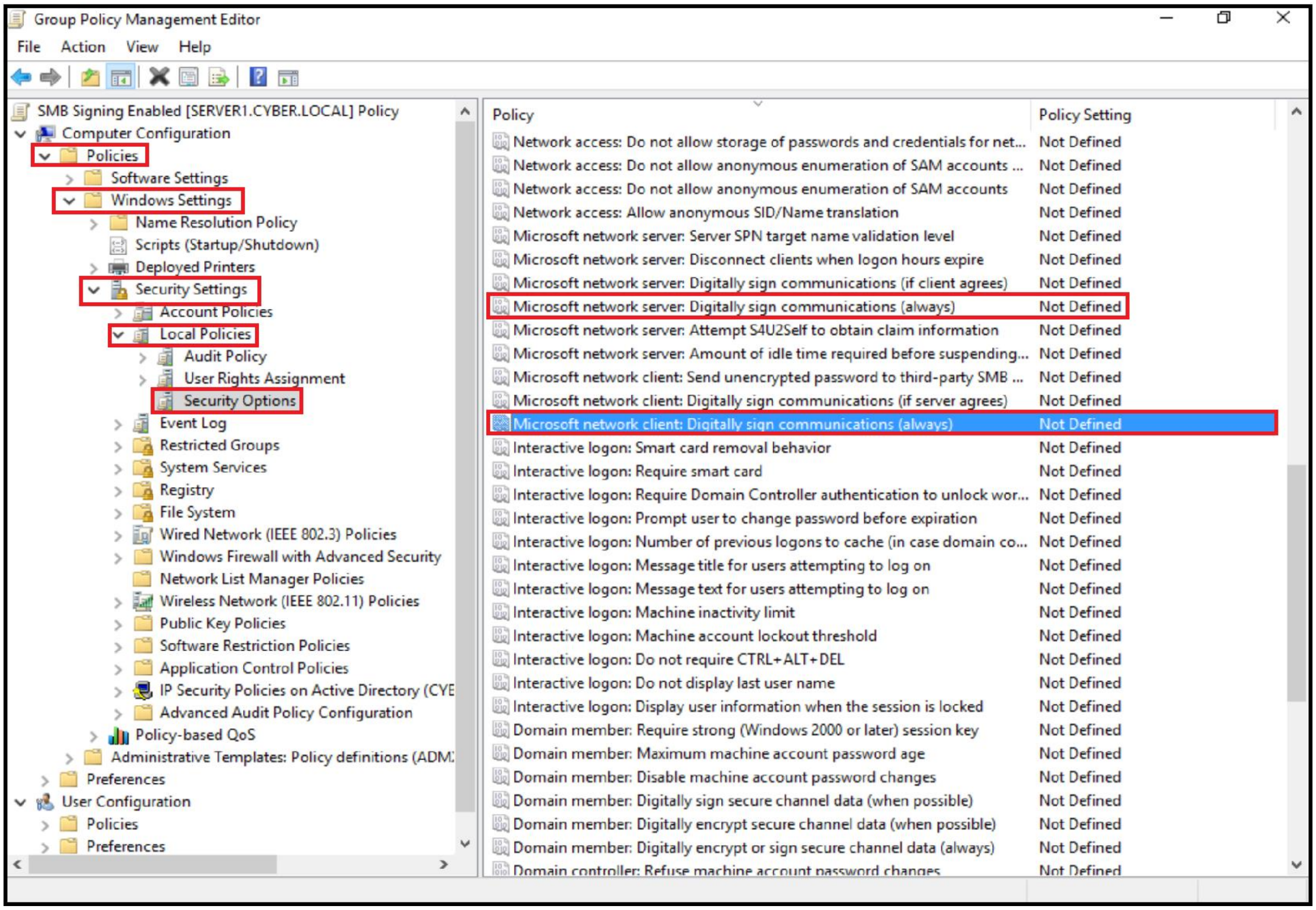
2 Right-click the **SMB Signing Enabled** GPO and enter its editor.



Group Policy Objects in cyber.local

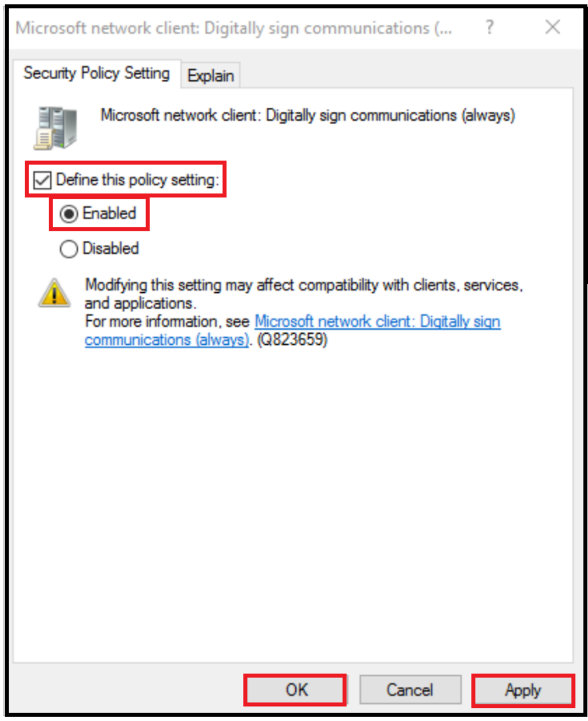
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	6/9/2021 5:27:18 AM	Domair
Default Domain Policy	Enabled	None	6/9/2021 5:48:36 AM	Domair
Disable CMD	Enabled	None	6/9/2021 6:39:22 AM	Domair
Disable Control Panel	Enabled	None	6/9/2021 6:38:30 AM	Domair
Disable Recycle Bin	Enabled	None	6/9/2021 6:41:10 AM	Domair
Disable Registry Editor	Enabled	None	6/9/2021 6:40:14 AM	Domair
LLMNR Disabled	Enabled	None	6/11/2021 7:50:45 AM	Domair
Local Admin	Enabled	None	6/9/2021 8:17:36 AM	Domair
Logon	Enabled	None	6/9/2021 8:12:06 AM	Domair
SMB Signing Enabled	Enabled	None	6/11/2021 8:05:00 AM	Domair

3 Navigate to ***Computer Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***Security Options*** and enable both **Microsoft network server and client: Digitally signed communications (always)**.


Group Policy Management Editor
File Action View Help
SMB Signing Enabled [SERVER1.CYBER.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (CYE
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM)
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Network access: Do not allow storage of passwords and credentials for net...	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts ...	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Amount of idle time required before suspending...	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB ...	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Digitally sign communications (always)	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Require Domain Controller authentication to unlock wor...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Number of previous logons to cache (in case domain co...	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined
Domain controller: Refuse machine account password changes	Not Defined

4 Enable ***Microsoft network client: Digitally sign communications (always)*** and ***Microsoft network server: Digitally sign communications (always)***.


Microsoft network client: Digitally sign communications (... ? ×

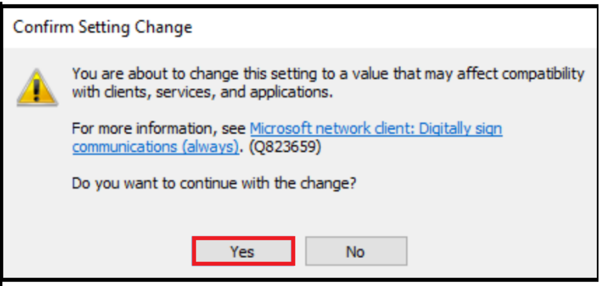
Microsoft network client: Digitally sign communications (always)

☑ Define this policy setting:

● Enabled

○ Disabled

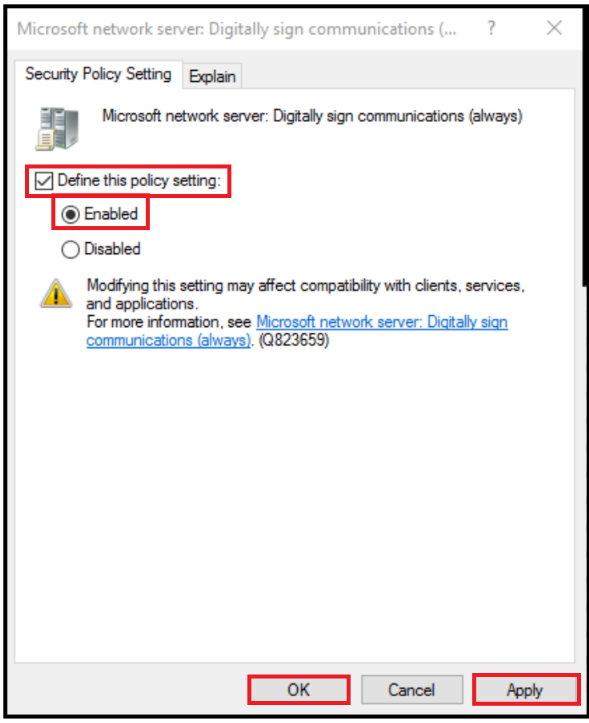
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Microsoft network client: Digitally sign communications (always). (Q823659)


Confirm Setting Change

You are about to change this setting to a value that may affect compatibility with clients, services, and applications.

For more information, see Microsoft network client: Digitally sign communications (always). (Q823659)

Do you want to continue with the change?


Microsoft network server: Digitally sign communications (... ? ×

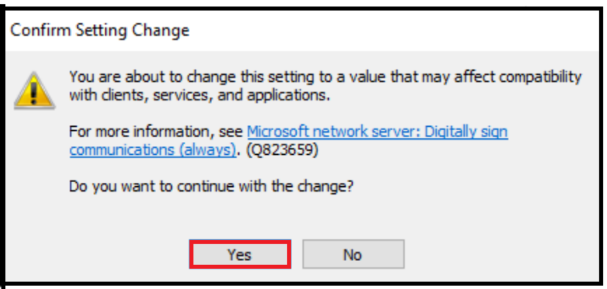
Microsoft network server: Digitally sign communications (always)

☑ Define this policy setting:

● Enabled

○ Disabled

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Microsoft network server: Digitally sign communications (always). (Q823659)

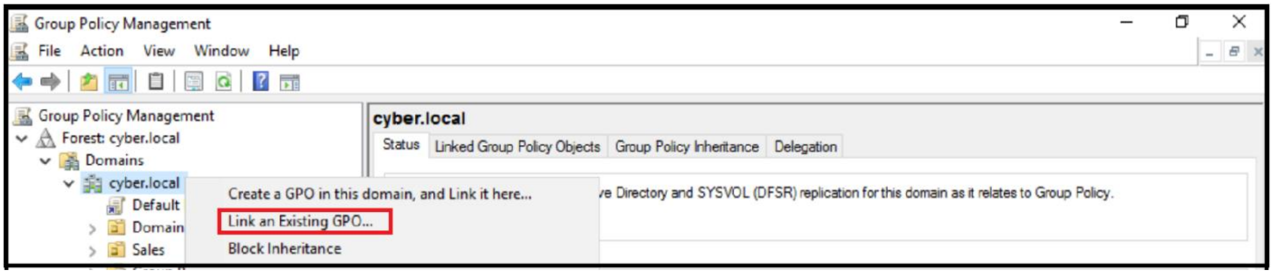

Confirm Setting Change

You are about to change this setting to a value that may affect compatibility with clients, services, and applications.

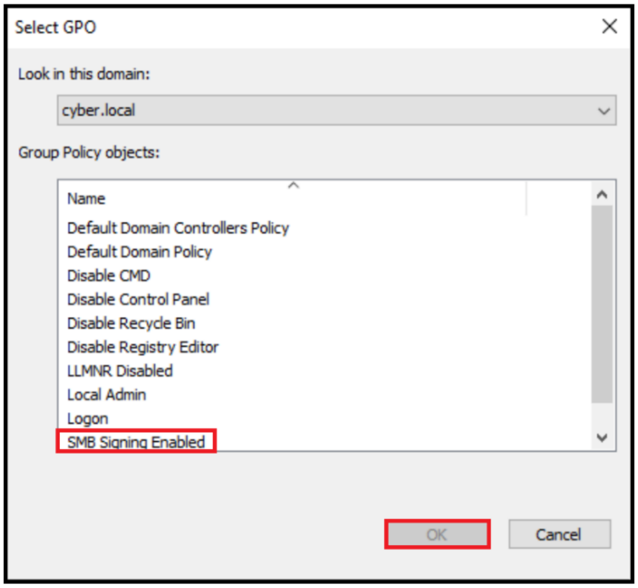
For more information, see Microsoft network server: Digitally sign communications (always). (Q823659)

Do you want to continue with the change?

5 Link the GPO **SMB Signing Enabled** to the domain ***cyber.local***.



ve Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.



Look in this domain: cyber.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Disable CMD
Disable Control Panel
Disable Recycle Bin
Disable Registry Editor
LLMNR Disabled
Local Admin
Logon
SMB Signing Enabled