





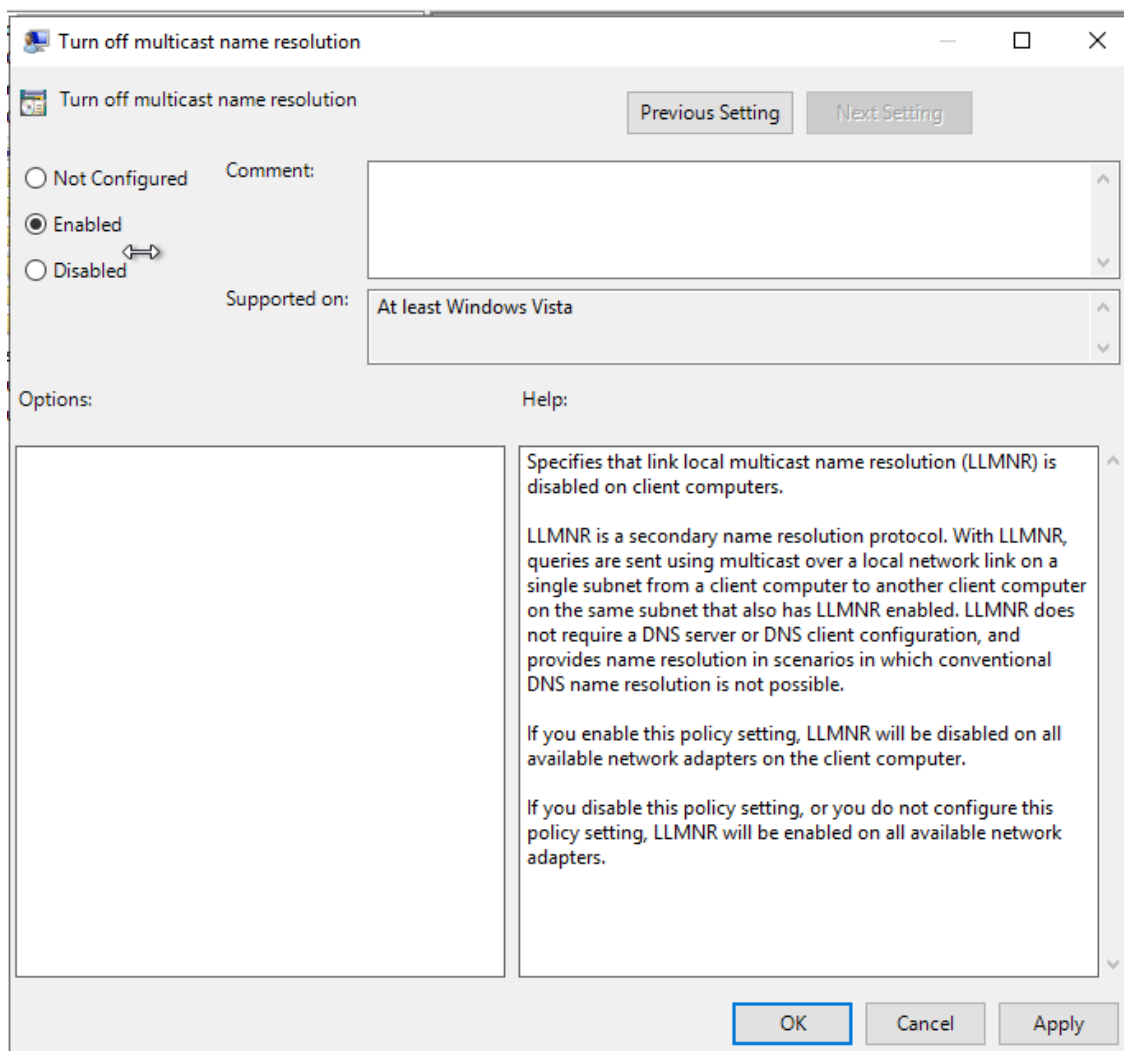
A Day in the Life of a Windows Sysadmin

Task 1: Create a GPO: Disable Local Link Multicast Name Resolution (LLMNR)

Creating a Group Policy Object called No LLMNR

Group Policy Objects in GOODCORP.NET		
Contents	Delegation	
Name	GPO Status	WMI Filter
 Default Domain Controllers Policy	Enabled	None
 Default Domain Policy	Enabled	None
 Limited Settings	Enabled	None
 No LLMNR	Enabled	None

Enabling the policy: Turn Off Multicast Name Resolution



The screenshot shows the 'Turn off multicast name resolution' Group Policy configuration window. The window title is 'Turn off multicast name resolution'. It has a 'Previous Setting' button and a 'Next Setting' button. The configuration options are:

- ☐ Not Configured
- ☒ Enabled
- ☐ Disabled

There is a 'Comment:' text box and a 'Supported on:' dropdown menu set to 'At least Windows Vista'. Below these are 'Options:' and 'Help:' sections. The 'Help:' section contains the following text:

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.

At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Linking No LLMNR GPO to GC Computers OU

GC Computers								
Linked Group Policy Objects		Group Policy Inheritance		Delegation				
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain	
1	No LLMNR	No	Yes	Enabled	None	4/27/202...	GOODC...	

Task 2: Create a GPO: Account Lockout

Group Policy Objects in GOODCORP.NET					
Contents		Delegation			
Name	GPO Status	WMI Filter	Modified	Owner	
Account Lockout	Enabled	None	4/27/2022 6:12:21 AM	Domain Admins (G	
Default Domain Controllers Policy	Enabled	None	9/22/2020 8:37:10 PM	Domain Admins (G	
Default Domain Policy	Enabled	None	2/5/2021 7:44:12 PM	Domain Admins (G	
Limited Settings	Enabled	None	4/27/2022 5:53:19 AM	Domain Admins (G	
No LLMNR	Enabled	None	4/27/2022 6:08:06 AM	Domain Admins (G	

Edited the Account Lockout using the following path:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

The image shows a screenshot of the 'Group Policy Management Editor' window. The title bar at the top reads 'Group Policy Management Editor' with standard window controls (minimize, maximize, close) on the right. Below the title bar is a menu bar with 'File', 'Action', 'View', and 'Help'. A toolbar with various icons is located below the menu bar. The main content area is divided into two panes. The left pane shows a tree view with 'Computer Configuration' expanded, followed by 'Policies', 'Software Settings', and 'Windows Settings'. The right pane displays the 'Policy' list with three items: 'Account lockout duration' (15 minutes), 'Account lockout threshold' (10 invalid logon attempts), and 'Reset account lockout counter after' (15 minutes). The 'Policy Setting' column is visible on the far right.

Link Account Lockout GPO to GC Computers OU

GC Computers								
Linked Group Policy Objects		Group Policy Inheritance		Delegation				
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain	
1	No LLMNR	No	Yes	Enabled	None	4/27/202...	GOODC...	
2	Account Lockout	No	Yes	Enabled	None	4/27/202...	GOODC...	

Task 3: Create a GPO: Enabling Verbose PowerShell Logging and Transcription

Creating GPO Powershell Logging

Group Policy Objects in GOODCORP.NET		
Contents Delegation		
Name	GPO Status	WMI Filter
Account Lockout	Enabled	None
Default Domain Controllers Policy	Enabled	None
Default Domain Policy	Enabled	None
Limited Settings	Enabled	None
No LLMNR	Enabled	None
<u>Powershell Logging</u>	Enabled	None

Enabling the Turn on Module Logging using * for Module Name

Windows PowerShell		
Select an item to view its description.	Setting	State
	Turn on Module Logging	Enabled
	Turn on PowerShell Script Block Logging	Not configured
	Turn on Script Execution	Not configured
	Turn on PowerShell Transcription	Not configured
	Set the default source path for Update-Help	Not configured

Turn on Module Logging

Turn on Module Logging

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 Comment:

Show Contents

Module Names

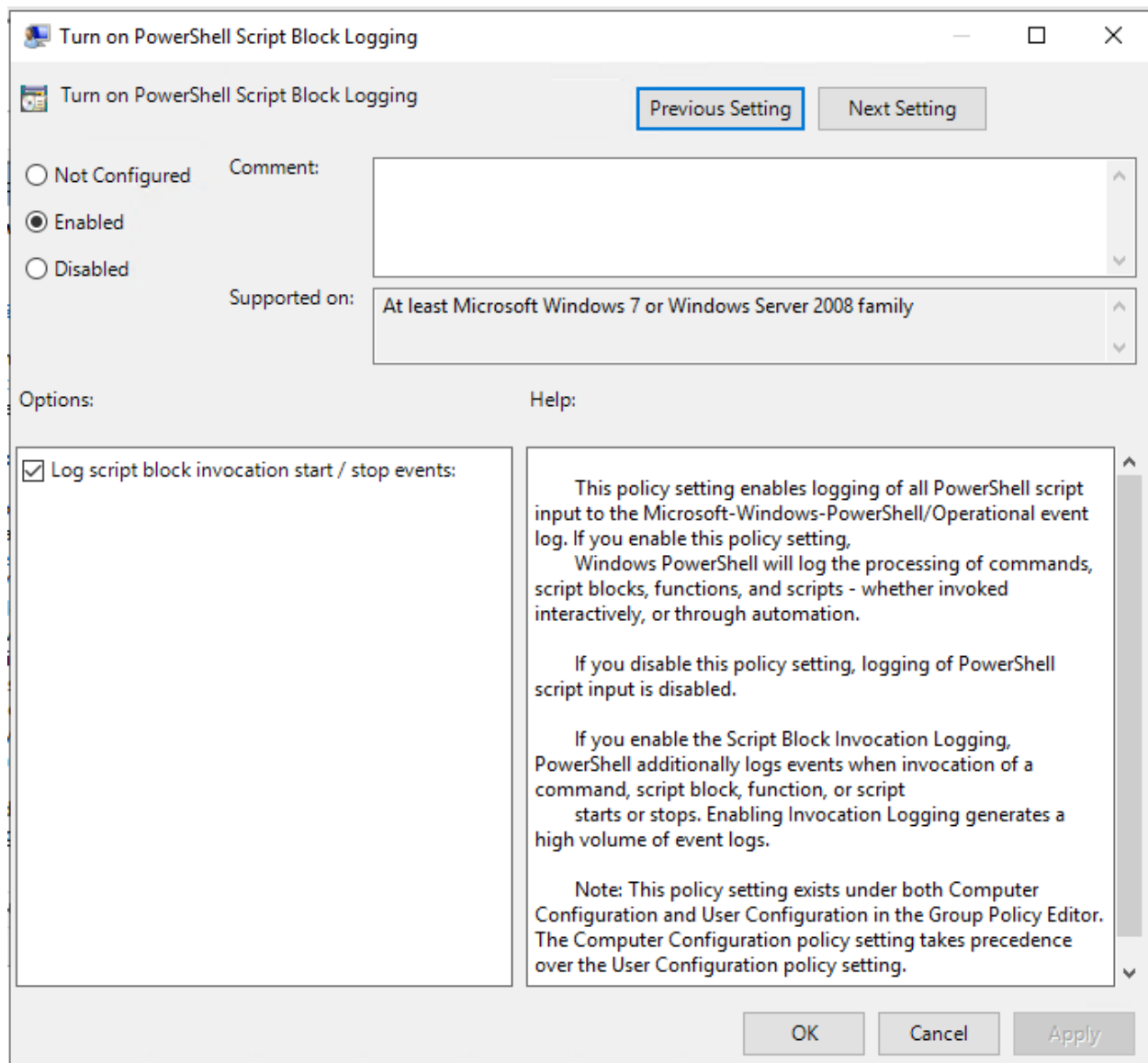
	Value
▶	*
*	

OK Cancel

If this policy setting is not configured, the LogPipelineExecutionDetails property of a module or snap-in determines whether the execution events of a module or snap-in are logged. By default, the LogPipelineExecutionDetails property of all modules and snap-ins is set to False.

OK Cancel Apply

Enabling Turn on PowerShell Script Block Logging



Turn on PowerShell Script Block Logging

Turn on PowerShell Script Block Logging [Previous Setting](#) [Next Setting](#)

☐ Not Configured **Comment:**

☒ **Enabled**

☐ Disabled

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

☒ Log script block invocation start / stop events:

Help:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting, Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.

If you disable this policy setting, logging of PowerShell script input is disabled.

If you enable the Script Block Invocation Logging, PowerShell additionally logs events when invocation of a command, script block, function, or script starts or stops. Enabling Invocation Logging generates a high volume of event logs.

Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.

[OK](#) [Cancel](#) [Apply](#)

Enabling Turn on Script Execution

Turn on Script Execution

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Execution Policy

Allow all scripts

Help:

This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.

If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.

The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.

The "Allow local scripts and remote signed scripts" policy setting allows any local scripts to run; scripts that originate from the Internet must be signed by a trusted publisher.

The "Allow all scripts" policy setting allows all scripts to run.

If you disable this policy setting, no scripts are allowed to run.

Note: This policy setting exists under both "Computer Configuration" and "User Configuration" in the Local Group Policy Editor. The "Computer Configuration" has precedence over "User Configuration."

OK Cancel Apply

Enabling Turn on PowerShell Transcription

Turn on PowerShell Transcription

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Transcript output directory

☒ Include invocation headers:

Help:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this policy setting, Windows PowerShell will enable transcribing for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.

If you disable this policy setting, transcribing of PowerShell-based applications is disabled by default, although transcribing can still be enabled through the Start-Transcript cmdlet.

OK Cancel Apply

Setting	State
Turn on Module Logging	Enabled
Turn on PowerShell Script Block Logging	Enabled
Turn on Script Execution	Enabled
Turn on PowerShell Transcription	Enabled
Set the default source path for Update-Help	Not configured

Linking PowerShell Logging

GC Computers					
Linked Group Policy Objects					
Group Policy Inheritance					
Delegation					
	Link Order	GPO	Enforced	Link Enabled	GPO Status
	1	No LLMNR	No	Yes	Enabled
	2	Account Lockout	No	Yes	Enabled
	3	PowerShell Logging	No	Yes	Enabled

Task 4: Create a Script: Enumerate Access Control Lists

Creating a PowerShell script that enumerate ACL of each file within the current working directory

```
enum_acls.ps1 X
1 $directory = Get-ChildItem
2 foreach ($item in $directory) {
3     Get-Acl $item
4 }
```

Results in C:\Windows

```
PS C:\Windows> C:\Users\sysadmin\Documents\enum_acls.ps1

Directory: C:\Windows

Path                Owner                Access
----                -
addins              NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
appcompat           NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
apppatch            NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
AppReadiness        NT AUTHORITY\SYSTEM      NT AUTHORITY\Authenticated Users Allow Read, Synchroni
assembly           BUILTIN\Administrators   BUILTIN\Administrators Allow FullControl...
bcastdvr            NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Boot                NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow -1610612736...
Branding            NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
CbsTemp            BUILTIN\Administrators   BUILTIN\Administrators Allow FullControl...
Containers          NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
CSC                 NT AUTHORITY\SYSTEM      NT AUTHORITY\SYSTEM Allow FullControl
Cursors            NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
debug              NT AUTHORITY\SYSTEM      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES
diagnostics         NT SERVICE\TrustedInstaller NT AUTHORITY\SYSTEM Allow -1610612736...
DiagTrack           NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
DigitalLocker       NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
Downloaded Program Files NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
en-US               NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Fonts               NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
GameBarPresenceWriter NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Globalization       NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
Help                NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
IdentityCRL         NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
IME                 NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
ImmersiveControlPanel NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
INF                 NT SERVICE\TrustedInstaller CREATOR OWNER Allow 268435456...
InputMethod         NT AUTHORITY\SYSTEM      NT SERVICE\TrustedInstaller Allow FullControl...
```

Bonus Task 5: Verify Your PowerShell Logging GPO

```
PS C:\Users\sysadmin\Documents\20220502> get-content .\PowerShell_transcript.DESKTOP-SITPOTH.HYDBexok.20220502093101.t
*****
Windows PowerShell transcript start
Start time: 20220502093102
Username: DESKTOP-SITPOTH\sysadmin
RunAs User: DESKTOP-SITPOTH\sysadmin
Configuration Name:
Machine: DESKTOP-SITPOTH (Microsoft Windows NT 10.0.19041.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 8104
PSVersion: 5.1.19041.1
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Command start time: 20220502093117
*****
PS C:\Users\sysadmin> cd .\Documents\
*****
Command start time: 20220502093119
*****
PS C:\Users\sysadmin\Documents> ls

Directory: C:\Users\sysadmin\Documents


Mode                LastWriteTime         Length Name
----                -
d-----          5/2/2022   9:19 AM             20220502
-a----          5/2/2022   8:36 AM             87 enum_acls.ps1
```