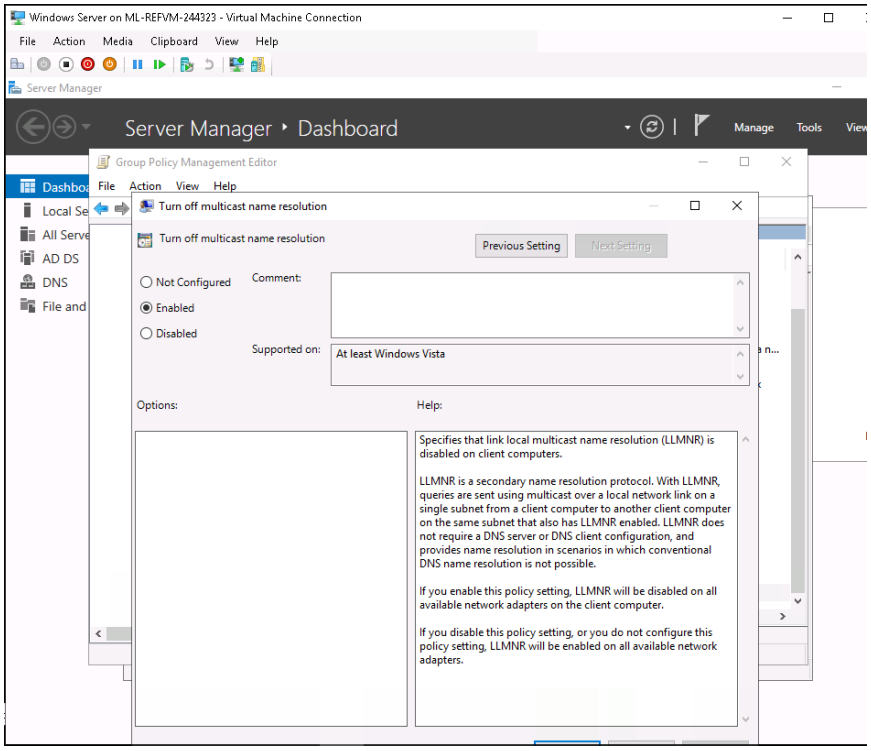
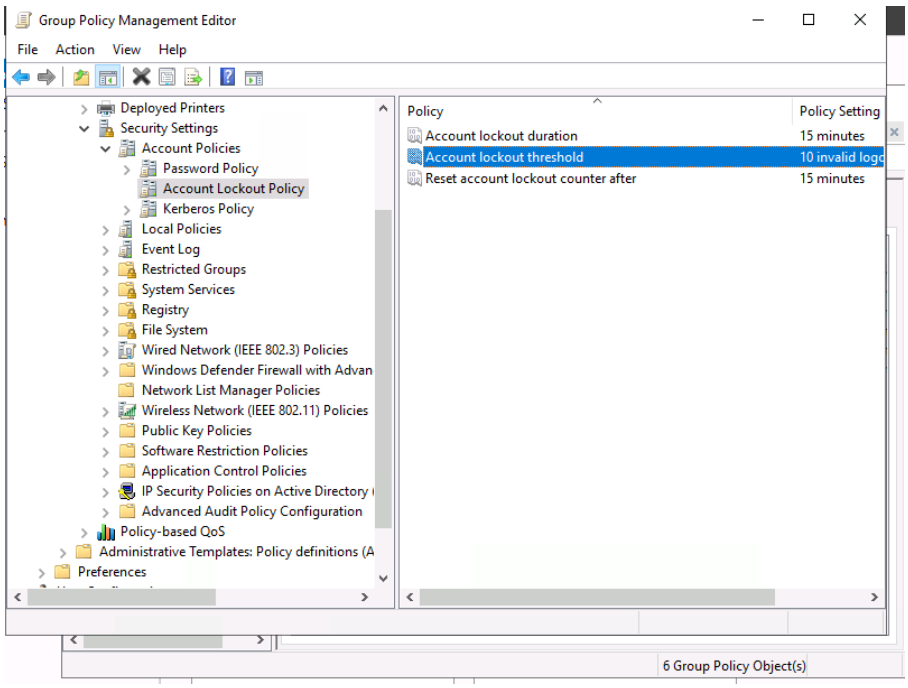
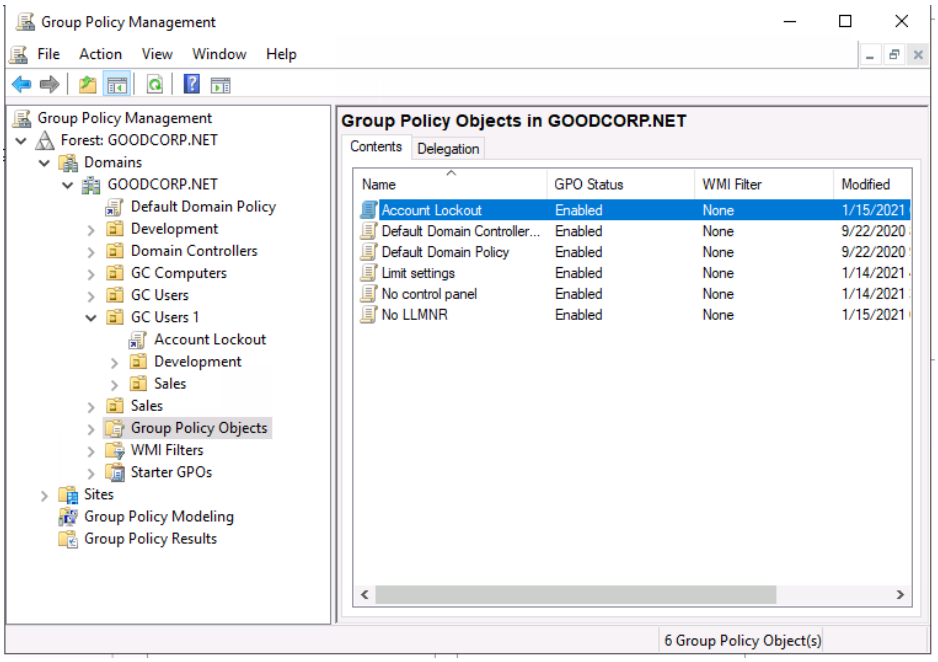
Week 7 Homework: A Day in the Life of a Windows Sysadmin

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

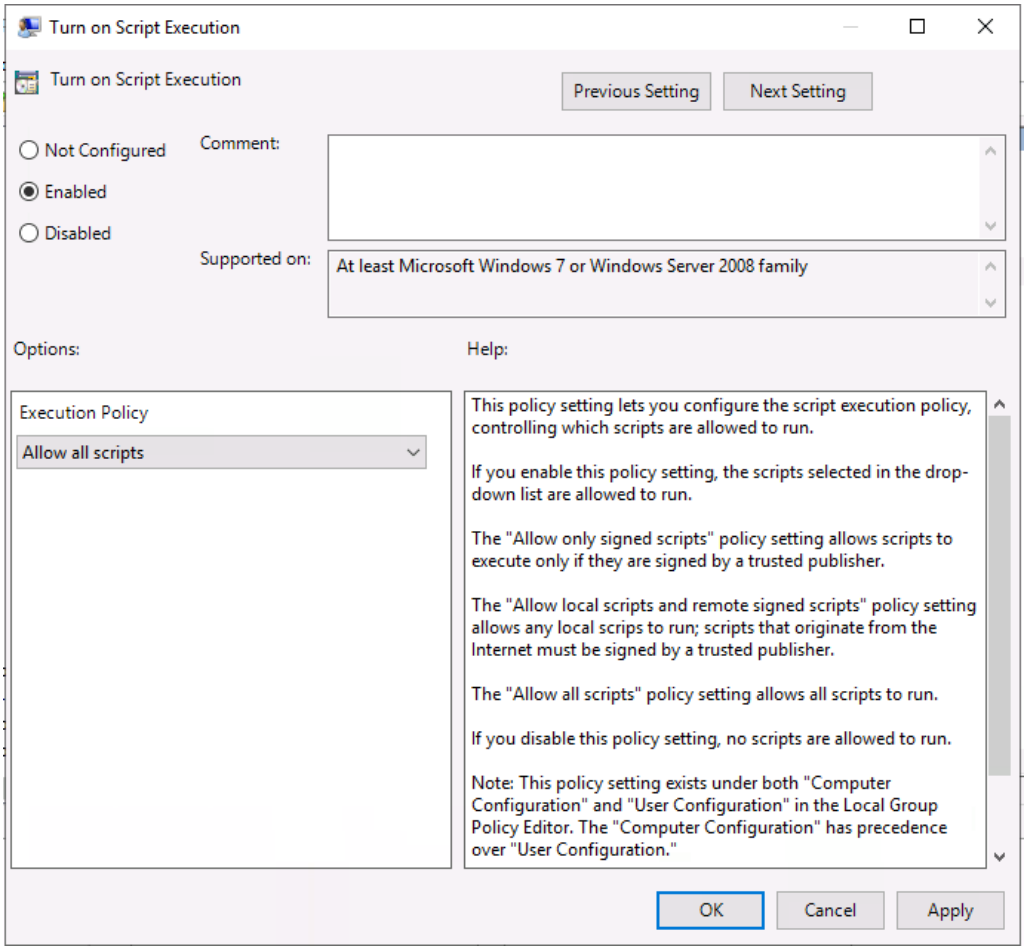


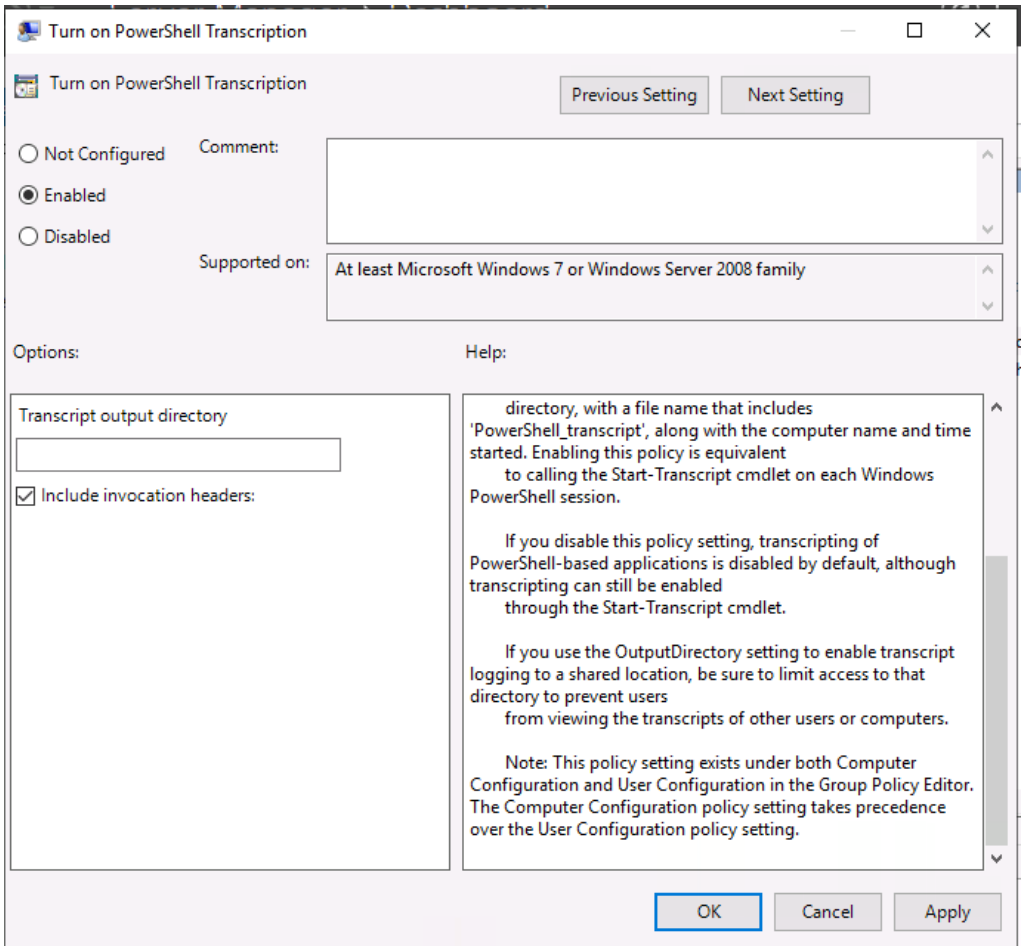
Task 2: Create a GPO: Account Lockout

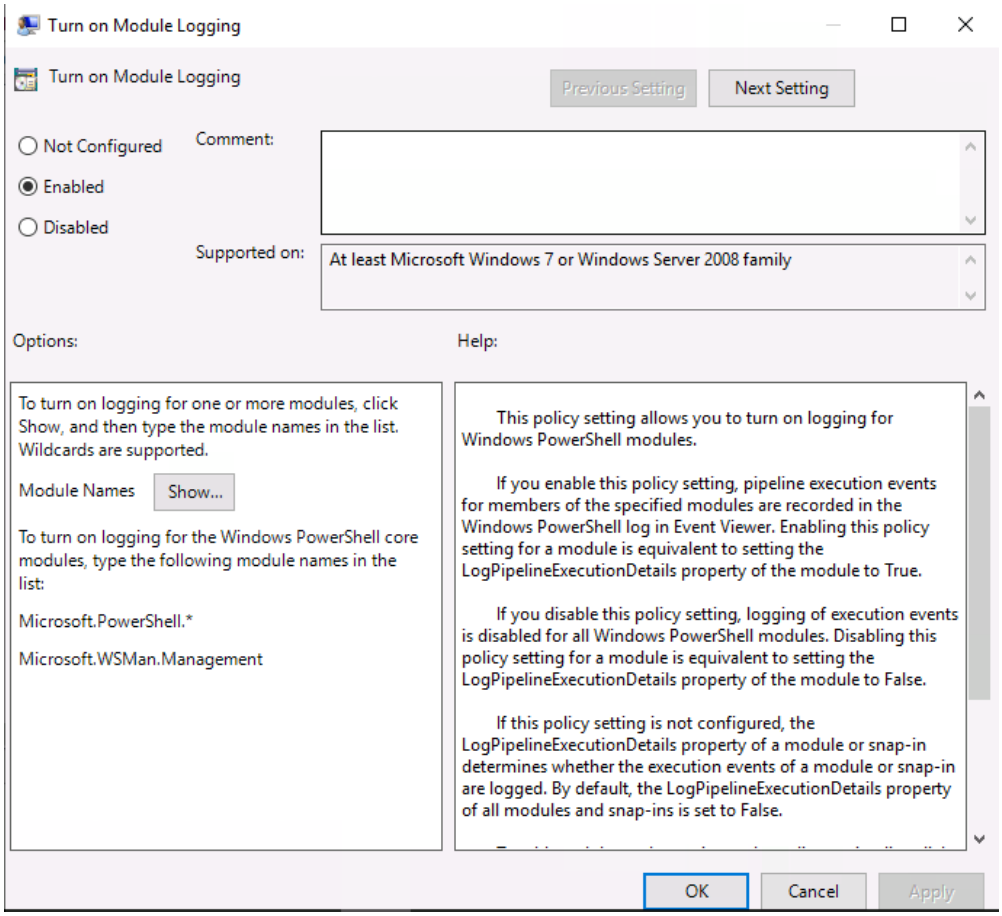


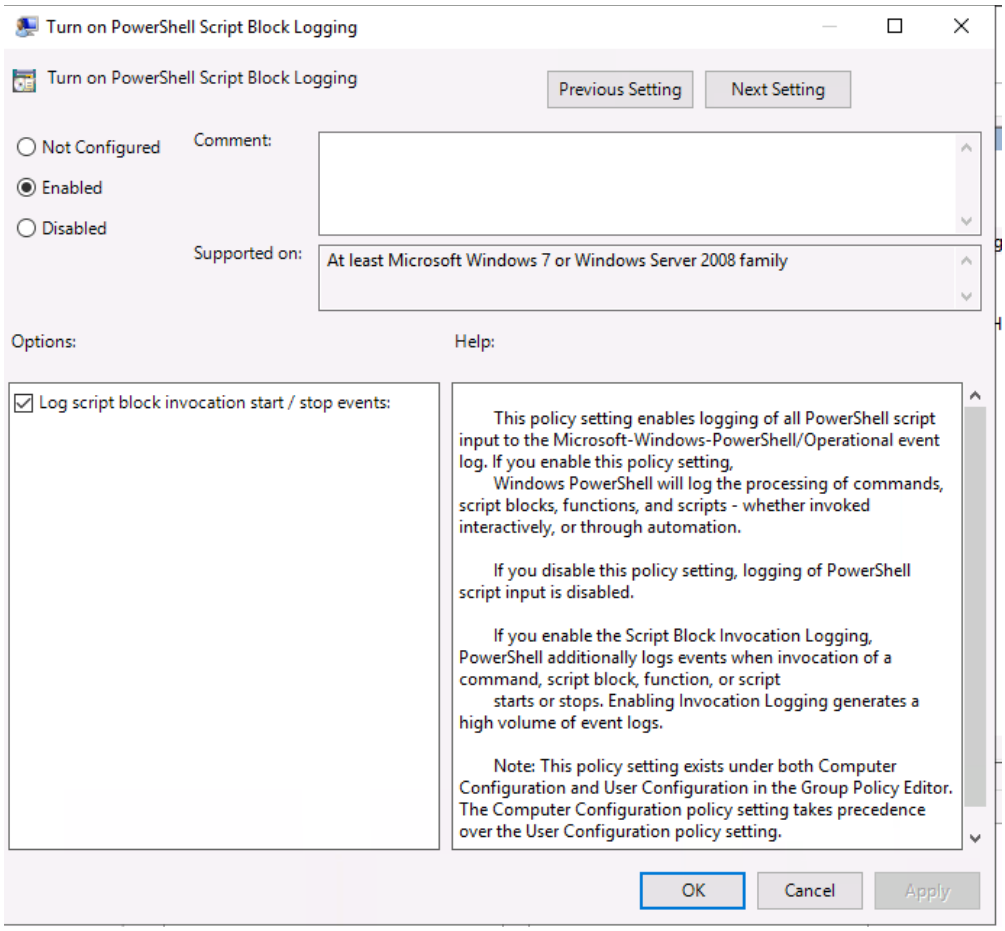


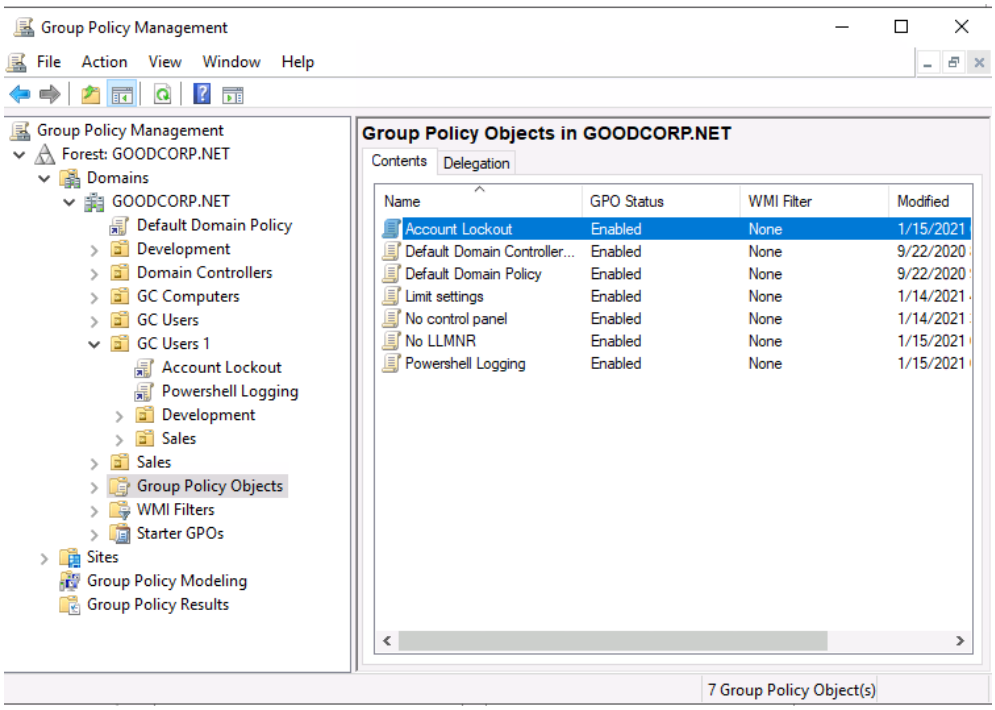
Task 3: Create a GPO: Enabling Verbose PowerShell Logging and Transcription

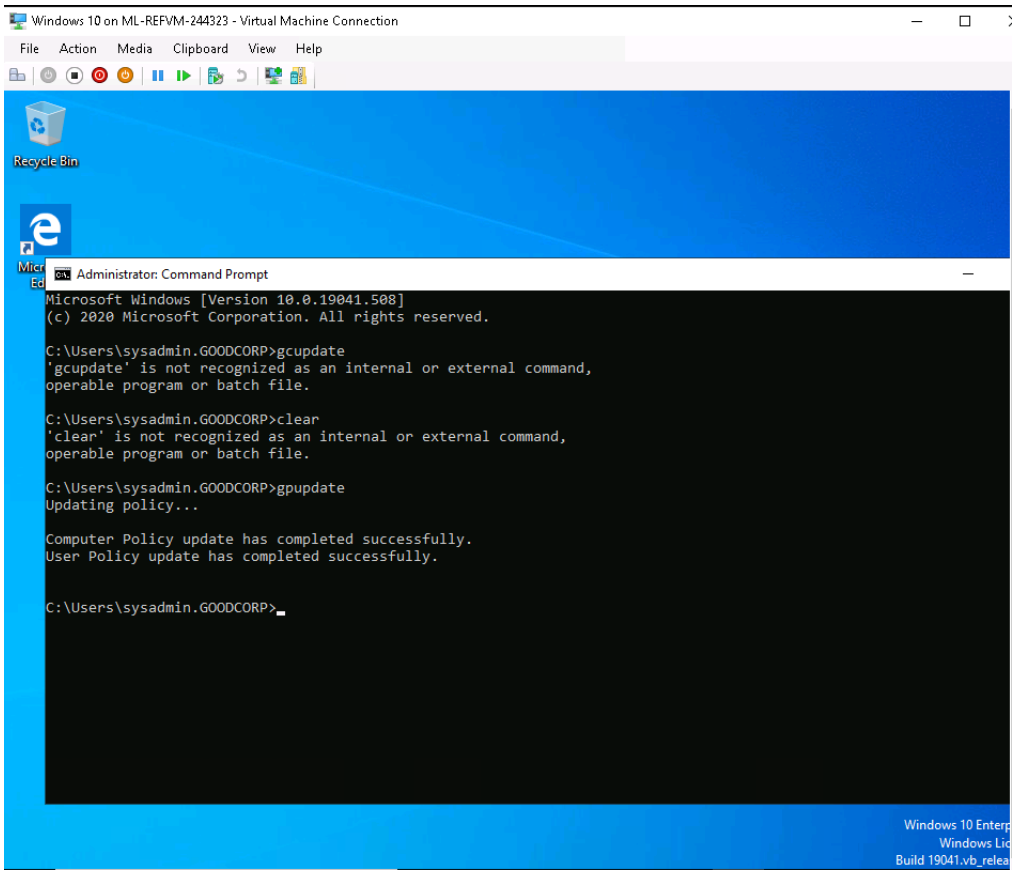



Turn on PowerShell Transcription
Turn on PowerShell Transcription
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Transcript output directory
Include invocation headers:
directory, with a file 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, transcripting of PowerShell-based applications is disabled by default, although transcripting can still be enabled through the Start-Transcript cmdlet.
If you use the OutputDirectory setting to enable transcript logging to a shared location, be sure to limit access to that directory to prevent users from viewing the transcripts of other users or computers.
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

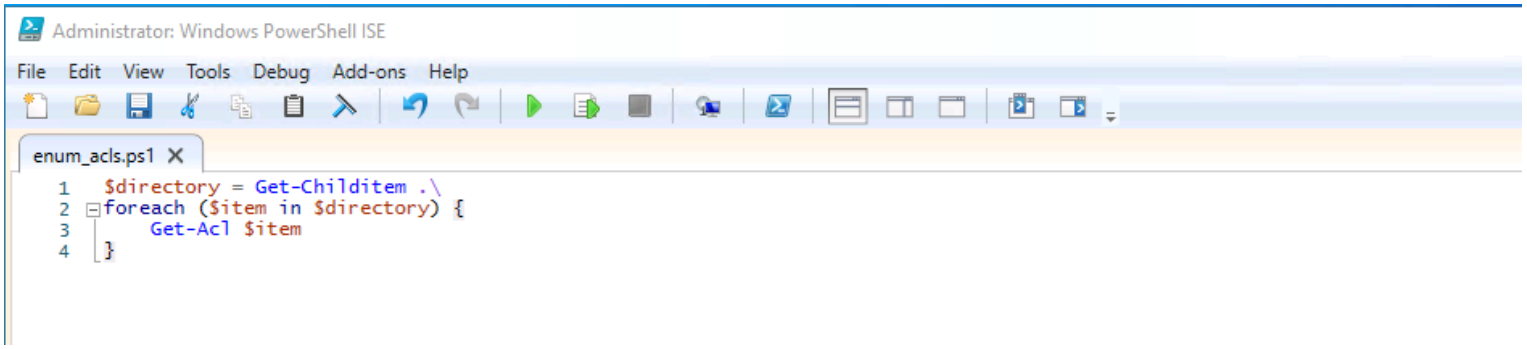

Turn on Module Logging
Turn on Module Logging
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
To turn on logging for one or more modules, click Show, and then type the module names in the list. Wildcards are supported.
Module Names
Show...
To turn on logging for the Windows PowerShell core modules, type the following module names in the list:
Microsoft.PowerShell.*
Microsoft.WSMan.Management
This policy setting allows you to turn on logging for Windows PowerShell modules.
If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.
If you disable this policy setting, logging of execution events is disabled for all Windows PowerShell modules. Disabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to False.
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


Turn on PowerShell Script Block Logging
Turn on PowerShell Script Block Logging
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Log script block invocation start / stop events:
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


Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: GOODCORP.NET
Domains
GOODCORP.NET
Default Domain Policy
Development
Domain Controllers
GC Computers
GC Users
GC Users 1
Account Lockout
Powershell Logging
Development
Sales
Sales
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in GOODCORP.NET
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Account Lockout
Enabled
None
1/15/2021
Default Domain Controller...
Enabled
None
9/22/2020
Default Domain Policy
Enabled
None
9/22/2020
Limit settings
Enabled
None
1/14/2021
No control panel
Enabled
None
1/14/2021
No LLMNR
Enabled
None
1/15/2021
Powershell Logging
Enabled
None
1/15/2021
7 Group Policy Object(s)



Task 4: Create a Script: Enumerate Access Control Lists




```
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, Synchronize...
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
```