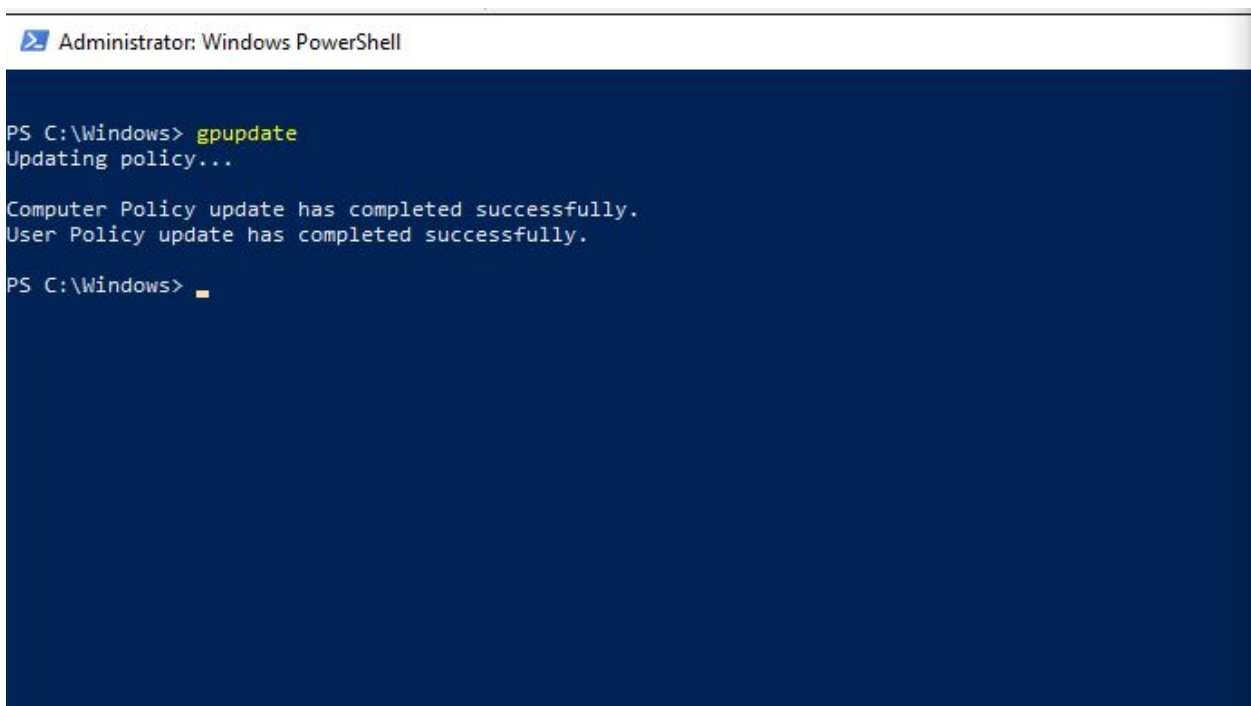


Bonus Task 5: Verify Your PowerShell Logging GPO

Solution:

Log into the **Windows 10** machine.

Run gpupdate in an administrative **PowerShell** window to pull the latest Active Directory changes.

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The command prompt shows the following sequence of text: "PS C:\Windows> gpupdate" in green, followed by "Updating policy..." in white, then "Computer Policy update has completed successfully." and "User Policy update has completed successfully." in white, and finally "PS C:\Windows> " with a white cursor.

```
Administrator: Windows PowerShell

PS C:\Windows> gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Windows> 
```

Close and relaunch **PowerShell** into an administrative session.

Navigate to a directory you want to see the ACLs in.

For the purpose of this project we navigate to **C:\Windows**, and then run the **enum_acls.ps1** script using the full file path and file name as shown below.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\sysadmin> cd 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, Synchroniz...
assembly            BUILTIN\Administrators   BUILTIN\Administrators Allow FullControl...
ocastdvr            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...
ESC                 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 Den...
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...
```

Checking the **C:\Users\sysadmin\Documents** for new logs:

Navigate to the directory **20200928** containing the log files and open the log files.

```
Windows 10 on ML-REFVM-447521 - Virtual Machine Connection
File Action Media View Help
Select Administrator: Windows PowerShell

PS C:\Windows> cd C:\Users\sysadmin\Documents\
PS C:\Users\sysadmin\Documents> ls

Directory: C:\Users\sysadmin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          9/27/2020   11:56 PM             20200927
d-----          9/28/2020   12:56 AM             20200928
-a----          9/28/2020    1:06 AM              79 enum_acls.ps1
-a----          2/20/2020    1:35 AM             1651 microsoftbloat.csv

PS C:\Users\sysadmin\Documents> cd .\20200928\
PS C:\Users\sysadmin\Documents\20200928> ls

Directory: C:\Users\sysadmin\Documents\20200928

Mode                LastWriteTime         Length Name
----                -
-a----          9/28/2020    1:22 AM             27033 PowerShell_transcript.DESKTOP-U3FCUKI.7xgl03ml.20200928005626.txt
-a----          9/28/2020    1:24 AM              0 PowerShell_transcript.DESKTOP-U3FCUKI.mYiYCqgw.20200928012445.txt

PS C:\Users\sysadmin\Documents\20200928> type .\PowerShell_transcript.DESKTOP-U3FCUKI.7xgl03ml.20200928005626.txt
*****
Windows PowerShell transcript start
Start time: 20200928005626
Username: DESKTOP-U3FCUKI\sysadmin
RunAs User: DESKTOP-U3FCUKI\sysadmin
Configuration Name:
Machine: DESKTOP-U3FCUKI (Microsoft Windows NT 10.0.18363.0)
```

copy of one of the logs.

```
*****
Command start time: 20200928010337
*****
PS C:\Users\sysadmin> Get-ChildItem ./

Directory: C:\Users\sysadmin

Mode                LastWriteTime         Length Name
----                -
d-r---          2/20/2020   12:44 AM             3D Objects
d-r---          2/20/2020   12:44 AM             Contacts
d-r---          2/20/2020    1:36 AM             Desktop
d-r---          9/28/2020   12:56 AM             Documents
d-r---          2/20/2020   12:44 AM             Downloads
d-r---          2/20/2020   12:44 AM             Favorites
d-r---          2/20/2020   12:44 AM             Links
d-r---          2/20/2020   12:44 AM             Music
d-r---          9/26/2020    6:09 PM             OneDrive
d-r---          2/20/2020   12:45 AM             Pictures
d-r---          2/20/2020   12:44 AM             Saved Games
d-r---          2/20/2020   12:45 AM             Searches
d-r---          2/20/2020    1:02 AM             Videos
-a----          9/28/2020   12:29 AM              52 .bash_history

*****
```