**Group Policies to Set**

### **Prevent Windows from Storing LAN Manager Hash**

Windows generates and stores user account passwords in “hashes.” Windows generates both a LAN Manager hash (LM hash) and a Windows NT hash (NT hash) of passwords. It stores them in the local Security Accounts Manager (SAM) database or Active Directory.

The LM hash is weak and prone to hacking. Therefore, you should prevent Windows from storing an LM hash of your passwords. Perform the following steps to do so:

1. In Group Policy Management Editor window (opened for a custom GPO), go to “Computer Configuration” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Network security: Do not store LAN Manager hash value on next password change” policy.
3. Select “Define this policy setting” checkbox and click “Enabled.
4. Click “Apply” and “OK”.

### **Disable Anonymous SID Enumeration**

Active Directory assigns a unique number to all security objects in Active Directory; including Users, Groups and others, called Security Identifiers (SID) numbers. In older Windows versions, users could query the SIDs to identify important users and groups. This provision can be exploited by hackers to get unauthorized access to data. By default, this setting is disabled, ensure that it remains that way. Perform the following steps:

1. In Group Policy Management Editor window, go to “Computer Configuration” “Policies” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Network Access: Do not allow anonymous enumeration of SAM accounts and shares” policy setting.
3. Choose ‘Enabled’ and then click ‘Apply’ and ‘OK’ to save your settings.

**For advanced Microsoft CommandLine and PowerShell module logging, make the following changes to group policy.**

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking > Audit Process Creation > Enable

Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation > Include command line in process creation events > Enable

User Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell > Enable and set module names to \*

If you also want to audit WMIC activity, you must run the following command on hosts that you want to collect WMIC tracing logs from. This must be run in an elevated prompt.

Wevtutil.exe sl Microsoft-Windows-WMI-Activity/Trace /e:true /q:true

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation - Disabled

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares -enabled

**Install Sysmon via Group Policy**

**Step1:** Create sysmon install batch file

First create a batch file that will be placed on the root domain folder that is accessible to each domain client.

Here’s the batch file. (This file will always write to C:\Windows and replace whatever configuration file is already there)

copy /z /y "\\domain.com\apps\config.xml" "C:\windows\"

sysmon -c c:\windows\config.xml

sc query "Sysmon" | Find "RUNNING"

If "%ERRORLEVEL%" EQU "1" (

goto startsysmon

)

:startsysmon

net start Sysmon

If "%ERRORLEVEL%" EQU "1" (

goto installsysmon

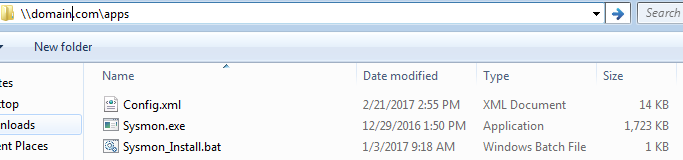
)

:installsysmon

"\\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml

**Step 2:** Create a folder on your domain that will be replicated with other domain controllers (in my example: **apps**), and copy the following:

* **sysmon.bat**
* [**sysmon.exe**](https://technet.microsoft.com/en-us/sysinternals/sysmon) (<https://technet.microsoft.com/en-us/sysinternals/sysmon>)
* **config.xml** (This is the configuration file that will be used by sysmon when you first deploy it, you may use [SwiftOnSecurity’s](https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml) own configuration to get you started)



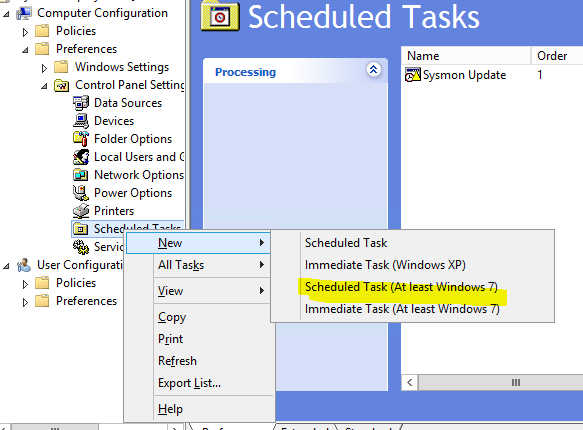
Now that you have the prerequisites, let’s move on.

**Step 3:** Creating a Scheduled Task

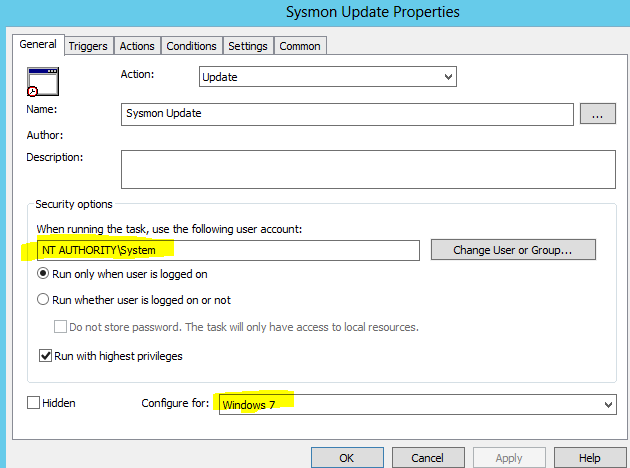
Launch your group policy utility and perform the following:

**Right click** your domain OU and

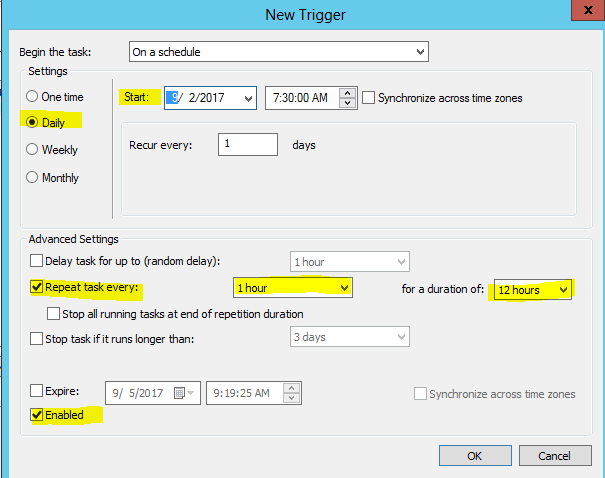
1. **Create GPO in this domain, and link it here**
2. Provide a name (**Sysmon Deployment) ,** hit OK
3. Right click your newly created GPO **Sysmon Deployment** and select **Edit**
4. Navigate to **Computer configuration > Preferences > Scheduled Tasks**
5. Right click **Scheduled Tasks** and click on **Scheduled Tasks (At Least Windows 7)** (This should work for Windows 7,10 Server 2008/2012)



6. Under the General Tab set the following:



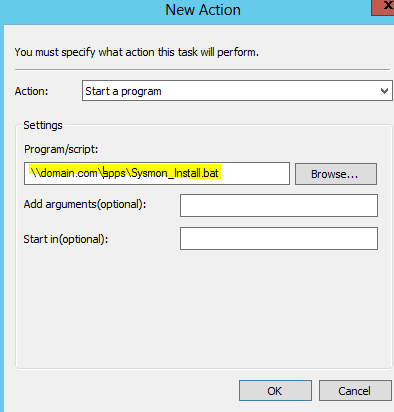
7. Under the Trigger Tab click on **New**

****

Hit **OK** when done.

(This will check your sysmon configuration every hour after 7:30 a.m, until 7:30 p.m, set to your own production hours when you expect to make changes to your sysmon config). This will allow all of your clients to constantly check for an updated version of sysmon config. This is helpful when you have hundreds or thousands of systems and you need a way to deploy the same configuration file.

8. Under the Actions tab click on **new**

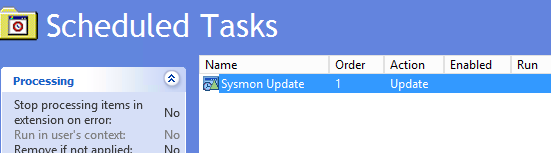
****

Browse to your sysmon.bat file and hit **OK** when done.

9. Optional step: Under the Settings tab, you can check the

**Allow task to be run on demand** (This will allow you to manually trigger the scheduled task on an endpoint when you login. It helps with initial testing).

10. Once done, click **OK.**

****