SOC ONBOARDING WINDOWS EVENT LOGS

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Author** |
| 0.1 | 29-JUL-2021 | Luk Schoonaert |
| 0.2 | 11-AUG-2021 | Luk Schoonaert |
|  |  |  |

**WINDOWS (AD) GROUP POLICIES**

1. Open Group Policy Management Console (GPMC) and open the Default Domain Policy (right-click and select “edit”) and make all the changes made below listed in this document.

Graphical user interface, text, application, email

Description automatically generated

Make sure this GPO is linked to all servers (Domain Computers domain controllers, servers – as shown above) – we won’t be collecting all these logs from all systems – but having these events logged on all systems will provide us with forensic evidence in case of a security incident.

2. Open the GPO and expand **Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Advanced Audit Policy Configuration 🡪 Audit Policies.**

Clicking on each category like **Account Logon**, **DS Access** and **System**, for example, will provide more granular categories in the righthand pane as you can see below.

Graphical user interface, text

Description automatically generated

For more information please go to this website :

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

You can search for specific Windows Event-ID’s on the left-hand side (red square in the screenshot)

Graphical user interface, text

Description automatically generated

**Kerberos tickets (Authentication on DC’s, service tickets)**

will cover the use-cases/event-ids specified below. Please refer to the screenshot on how to configure the GPO.

**4768: A Kerberos authentication ticket (TGT) was requested**

**4769: A Kerberos service ticket was requested**

**4770: A Kerberos service ticket was renewed**

**4776: The domain controller attempted to validate the credentials for an account (NTLM)**

Go to the Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies and click on Account Logon.

1. Enable “Audit Credential Validation”, Success and Failure.
2. Enable “Audit Kerberos Authentication Service”, Success and Failure.
3. Enable “Audit Kerberos Service Ticket Operations”, Success and Failure.

Make sure to configure all 3 subcategories as shown in the screenshot

Graphical user interface, application

Description automatically generated

**GPO Account Management**will cover the use-cases/event-ids specified below. Please refer to the screenshot on how to configure the GPO.

**4727: A security-enabled global group was created**

**4728: A member was added to a security-enabled global group**

**4729: A member was removed from a security-enabled global group**

**4730: A security-enabled global group was deleted**

**4731: A security-enabled local group was created**

**4732: A member was added to a security-enabled local group**

**4733: A member was removed from a security-enabled local group**

**4734: A security-enabled local group was deleted**

**4735: A security-enabled local group was changed**

**4737: A security-enabled global group was changed**

**4754: A security-enabled universal group was created**

**4755: A security-enabled universal group was changed**

**4756: A member was added to a security-enabled universal group**

**4757: A member was removed from a security-enabled universal group**

**4758: A security-enabled universal group was deleted**

Go to the Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies and click on Account Management.

1. Enable “Audit Security Group Management”, Success and Failure.
2. Enable “Audit Other Account Management Events”, Success and Failure.

Graphical user interface, text, application

Description automatically generated

**GPO User Account Management**

**4720: A user account was created**

**4722: A user account was enabled  
4723: An attempt was made to change an account's password**  
**4724: An attempt was made to reset an accounts password**

**4725: A user account was disabled**

**4726: A user account was deleted  
4740: A user account was locked out**

Go to the Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies and click on “Account Management”.

1. Enable “Audit User Account Management”, Success and Failure.

**Graphical user interface, application

Description automatically generated**

**GPO Account logon**

**4624: An account was successfully logged on**

**4625: An account failed to log on**

**4648: A logon was attempted using explicit credentials**

**4672: Special privileges assigned to new logon**

**4740: A user account was locked out**

Go to the Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies and click on “Logon/Logoff”.

1. Enable “Audit Account Lockout”, Success and Failure.
2. Enable “Audit Account Logoff”, Success and Failure.
3. Enable “Audit Account Logon”, Success and Failure.
4. Enable “Audit other Logon/Logoff Events”, Success and Failure.
5. Enable “Audit Special Logon”, Success and Failure.

Graphical user interface

Description automatically generated

**RDP CONNECTION Logs**

EventID : 1149

LogSource : Microsoft-Windows-Terminal-Services-RemoteConnectionManager

**Enabled by default** – no GPO configuration required – validate if you find these logs in eventviewer.

**SERVICE CREATION Logs**

EventID : 7045

LogSource : SYSTEM

**Enabled by default** – no GPO configuration required – validate if you find these logs in eventviewer.

**WMI Activity Logs**

EventID : 5861

LogSource : Microsoft-Windows-WMI-Activity/Operational

**Enabled by default** – no GPO configuration required – validate if you find these logs in eventviewer. Not always present, depends on WMI activity.

**Event Log Clearing Logs**

EventID : 1102

LogSource : Security

**Enabled by default** – no GPO configuration required – validate if you find these logs in eventviewer. Not always present, only when event logs have been cleared.

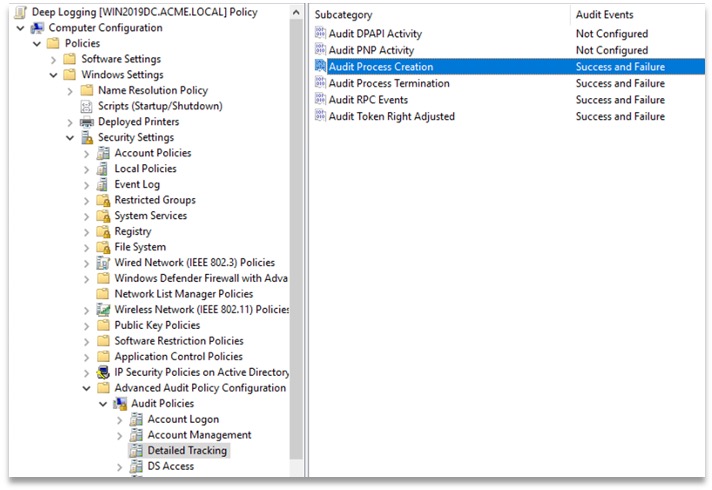
**PROCESS EXECUTION AND COMMAND LINE Logs**

EventID : 4688

LogSource : Security

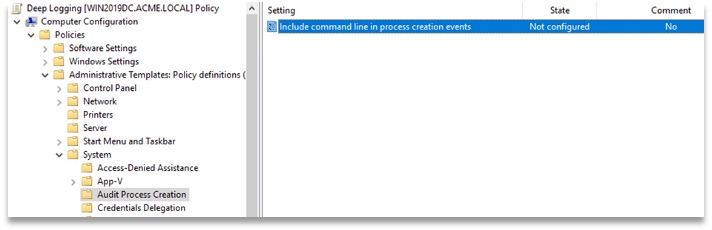
To enable **process creation** logging, go to Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking

* Double-click ***"Audit Process Creation"***
* Check the box "***Configure the following audit events"***
* Check the box ***"Success" and "Failure"***



Then enable the **command line arguments** logging by going to Computer Configuration\Administrative Templates\System\Audit Process Creation

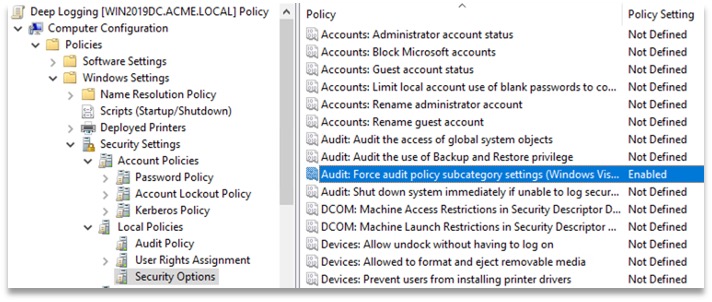
* Double-click ***"Include command line in process creation events"*** and set to ***Enabled***



Finally when you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings.

Go to Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

* Double-click ***AUDIT***: ***"Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings"***, then click ***"Define this policy setting"*** and set to ***Enabled***



**APPLOCKER Logs**

EventID : 8003, 8006

LogSource : Microsoft-Windows-WMI-Activity/Operational

8003: Applied only when the **Audit only** enforcement mode is enabled. Specifies that the .exe or .dll file would be blocked if the **Enforce rules** enforcement mode were enabled.

8006: Applied only when the **Audit only** enforcement mode is enabled. Specifies that the script or .msi file would be blocked if the **Enforce rules** enforcement mode were enabled.

* BE CAREFUL THAT YOU PUT THIS IN “AUDIT ONLY” MODE AND NOT IN ENFORCED MODE!!!

Go to the Computer Configuration -> Windows Settings -> Security Settings -> Application Control Policies -> Applocker and click on “Configure Rule Enforcement” check the configured box for these 3 options:

1. Executable Rules, AUDIT ONLY
2. Windows Installer Rules, AUDIT ONLY
3. Script Rules, AUDIT ONLY

Graphical user interface, application, email

Description automatically generated

Then to the Computer Configuration -> Windows Settings -> Security Settings -> System Services and click on “Application Identity”.

1. Set the service to start up automatically.

Graphical user interface, text, application

Description automatically generated

**4673: A privileged service was called**

Graphical user interface

Description automatically generated

**NEW -> 4663: An attempt was made to access an object**

Used to monitor file access on

Security

Event ID: 4663

(see screenshot below)

**NEW -> 5140: A network share object was accessed**

Used to monitor file access on servers

Security

Event ID: 5140

(see screenshot below)

**NEW -> 5145: A network share object was checked to see whether client can be granted desired access**

**\*VERY NOISY\***

Used to monitor file access on servers

Security

Event ID: 5145

(see screenshot below)

Graphical user interface, application

Description automatically generated

A picture containing text

Description automatically generated

Then go to the servers you want to log file activity on, select the directory and apply what needs to be logged :

Graphical user interface, application

Description automatically generated

When you have made all the GPO changes run the following command from an elevated command prompt (runas Administrator):

* gpupdate /force

This will force GPO replication.

The following command will show you which GPO’s are applied on the machine you execute this command on (if you want to make sure the GPO is actually applied to the machine)

* gpresult /r

To check if the GPO’s settings have been applied – check on your DC’s and a few servers, endpoints of choice and run this command:

* auditpol.exe /get /category:\*

You should see the GPO’s have been applied as below.

A picture containing text, screenshot, newspaper, plaque

Description automatically generated