Windows
PowerShell auditing configuration guide
# Table of Contents

Overview                                                                                   1

1. Configure PowerShell auditing in ADAudit Plus                                           1

2. Configure audit policies in your domain                                                 1
   2.1. Automatic configuration                                                            1
   2.2. Manual configuration                                                                2
       2.2.1. For module logging                                                            2
       2.2.2. For script block logging                                                      3

3. Configure the log size                                                                  4

4. Troubleshooting                                                                        5
Overview

Windows PowerShell is a scripting language that is used to automate system tasks. It can be used to gather data, steal system information, dump credentials, and more. This is why tracking PowerShell activity is imperative.

ADAudit Plus' PowerShell auditing reports help track PowerShell processes that run in your environment along with the commands executed in them.

ADAudit Plus enables you to audit the following versions of PowerShell:
- PowerShell version 5.0
- PowerShell version 4.0

1. Configure PowerShell auditing in ADAudit Plus

To configure PowerShell auditing on a domain controller (DC), configure the domain and the DC in ADAudit Plus. Click here to see how.

To configure PowerShell auditing on a Windows server, configure the Windows server in ADAudit Plus. Click here to see how.

2. Configure audit policies in your domain

Audit policies must be configured to log events whenever any activity occurs.

2.1. Automatic configuration

ADAudit Plus can automatically configure the required audit policies for PowerShell auditing. To learn how to enable audit policies automatically for PowerShell auditing on a:

- Domain controller, click here.
- Windows server, click here.
2.2. Manual configuration

2.2.1. For module logging

1. Log in to any computer that has the Group Policy Management Console (GPMC) with domain admin credentials.

2. Open the GPMC and, based on your setup, edit the:
   - **Default Domain Controllers Policy** to enable module logging on a DC.
   - **ADAuditPlusMSPolicy** to enable module logging on a Windows server.

3. In the Group Policy Management Editor, go to **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Powershell.** Navigate to the right pane, and right-click on **Turn on Module Logging > Enabled.**

4. In the Options pane, click on **Show.** In the **Module Names** window, enter * to record all modules, and press **OK.**
2.2.2. For script block logging

1. Log in to any computer that has the GPMC with domain admin credentials.

2. Open the GPMC and, based on your setup, edit the:
   - Default Domain Controllers Policy to enable module logging on a DC.
   - ADAuditPlusMSPolicy to enable module logging on a Windows server.

3. In the Group Policy Management Editor, go to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Powershell. Navigate to the right pane, and right-click on Turn on PowerShell Script Block Logging > Enabled.
3. Configure the log size

We recommend setting the maximum log size of PowerShell logs to 150MB. To do this, follow the steps outlined below.

1. Log in to any computer that has the GPMC with domain admin credentials.

2. Open the GPMC and, based on your setup, edit the:
   - Default Domain Controllers Policy to enable module logging on a DC.
   - ADAuditPlusMS Policy to enable module logging on a Windows server.

3. In the Group Policy Management Editor, go to Computer Configuration > Preferences > Windows Settings, and right-click Registry > New > Registry Item.

4. In Action field of the New Registry Properties wizard, select Update from the drop-down. In the Hive field, select HKEY_LOCAL_MACHINEM from the drop-down. In the Key Path field, enter: SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\ Channels\Microsoft-Windows-PowerShell\Operational. In the Value name field, uncheck the box beside Default, and type in MaxSize. In the Value type field, select REG_DWORD from the drop-down. In the Value data field, type in 153616384. In the Base field, select Decimal, and then click Apply.
4. Troubleshooting

1. How to verify if the desired events are getting logged?

   Open the Event Viewer on a computer where PowerShell auditing has been configured. Navigate to the left panel, and click on Application and Service Logs > Microsoft > Windows > PowerShell > Operational. Verify if events 4103 and 4104 are getting logged.