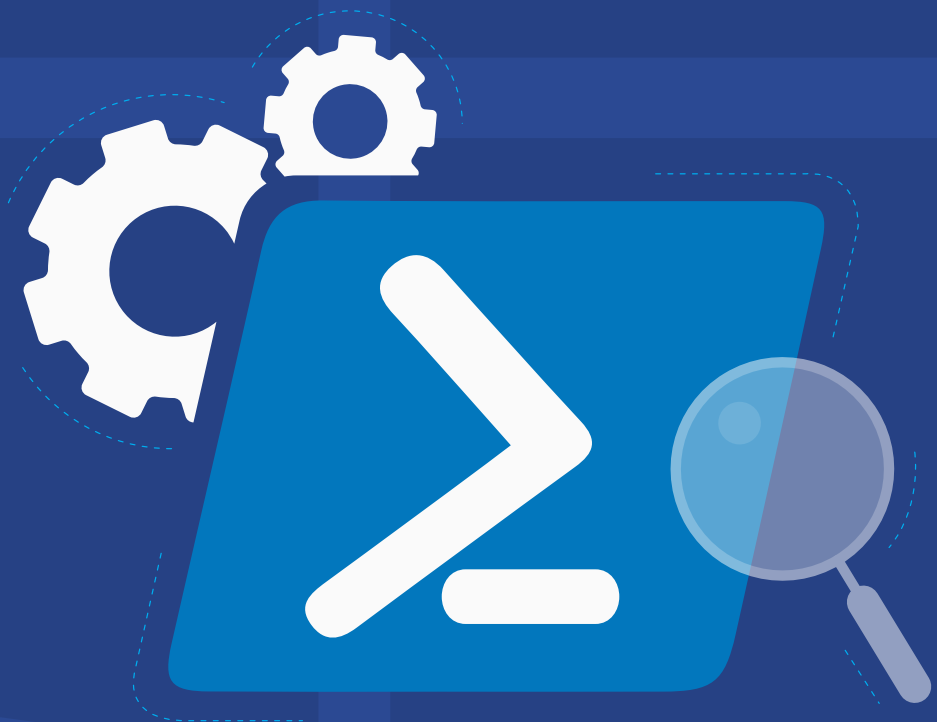
ManageEngine
ADAudit Plus

Przewodnik po konfiguracji procesu inspekcji programu Windows PowerShell



www.adauditplus.com

Spis treści

Przegląd

Windows PowerShell to język skryptowy używany do automatyzacji zadań systemowych. Może być używany do zbierania danych, przechwytywania informacji o systemie, wykonywania kopii zapasowej poświadczeń i nie tylko. Dlatego monitorowanie aktywności w programie PowerShell jest takie ważne.

Oferowane w ADAudit Plus raporty z inspekcji PowerShell pomagają śledzić procesy PowerShell, które przebiegają w środowisku użytkownika wraz z poleceniami wykonanymi w ramach tych procesów.

ADAudit Plus pozwala poddać inspekcji następujące wersje programu PowerShell:

- PowerShell, wersja 5.0
- PowerShell, wersja 4.0

1. Konfiguracja inspekcji programu PowerShell w ADAudit Plus

Aby skonfigurować inspekcję PowerShell w kontrolerze domeny (DC), skonfiguruj domenę oraz kontroler DC w ADAudit Plus. Kliknij tutaj, aby zobaczyć jak.

Aby skonfigurować inspekcję PowerShell na serwerze Windows, skonfiguruj serwer Windows w ADAudit Plus. Kliknij tutaj, aby zobaczyć jak.

2. Konfiguracja zasad inspekcji w domenie

Zasady inspekcji należy konfigurować, aby rejestrować zdarzenia związane z każdą aktywnością.

2.1. Konfiguracja automatyczna

ADAudit Plus pozwala automatycznie skonfigurować wymagane zasady inspekcji na potrzeby inspekcji programu PowerShell.

Aby dowiedzieć się, jak automatycznie włączyć zasady inspekcji na potrzeby inspekcji programu PowerShell w:

- kontrolerze domeny, kliknij tutaj;
- serwerze Windows, kliknij tutaj.

2.2. Konfiguracja ręczna

2.2.1. Rejestrowanie modułu

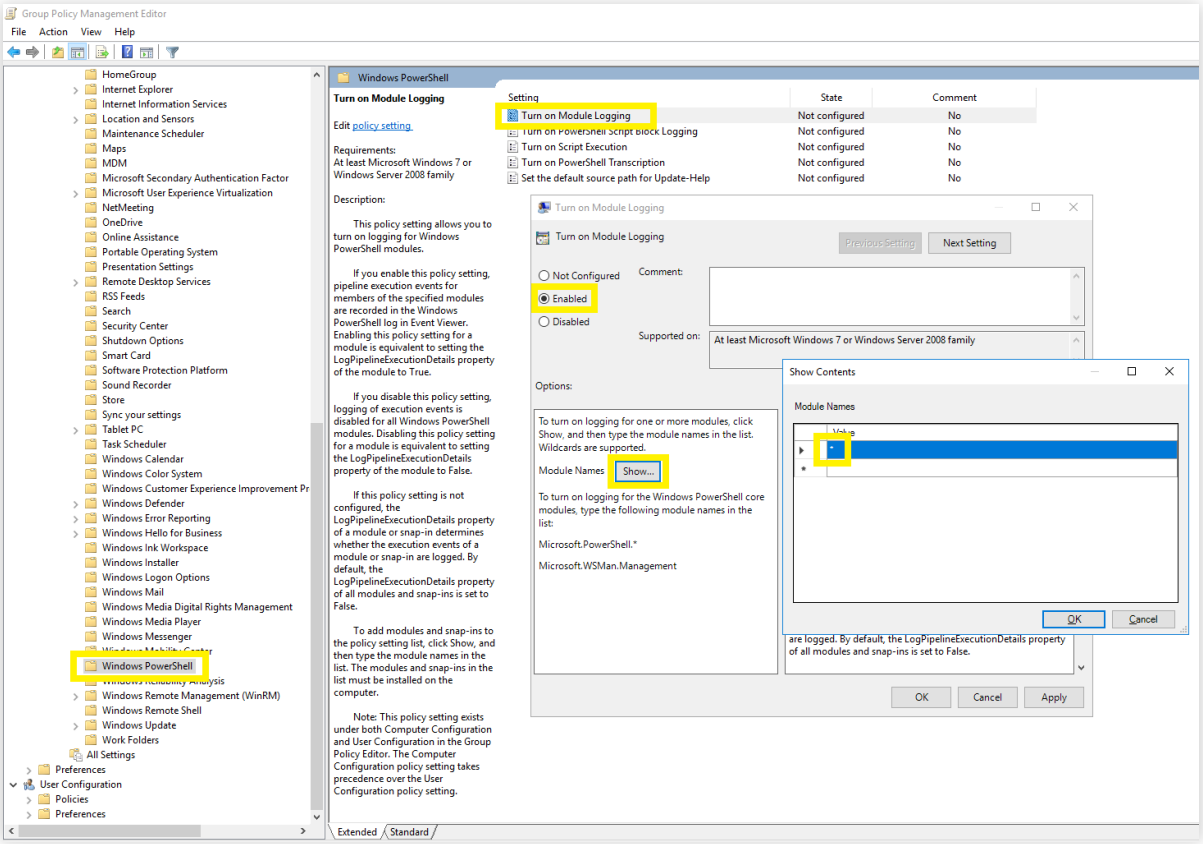
1. Zaloguj się do dowolnego komputera z e Group Policy Management Console (GPMC), używając poświadczeń administratora domeny.

2. Otwórz konsolę GPMC i, w zależności od konfiguracji, edytuj:

   - Default Domain Controllers Policy, aby włączyć rejestrowanie modułu w kontrolerze DC.
   - ADAuditPlusMSPolicy, aby włączyć rejestrowanie modułu w serwerze Windows.

3. WGroup Policy Management Editor przejdź do obszaru Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Powershell.. Przejdź do prawego panelu i prawym przyciskiem kliknij opcję Turn on Module Logging > Enabled

4. W panelu Options kliknij opcję Show. W oknie Module Names wpisz *, aby zarejestrować wszystkie moduły i naciśnij **OK.**



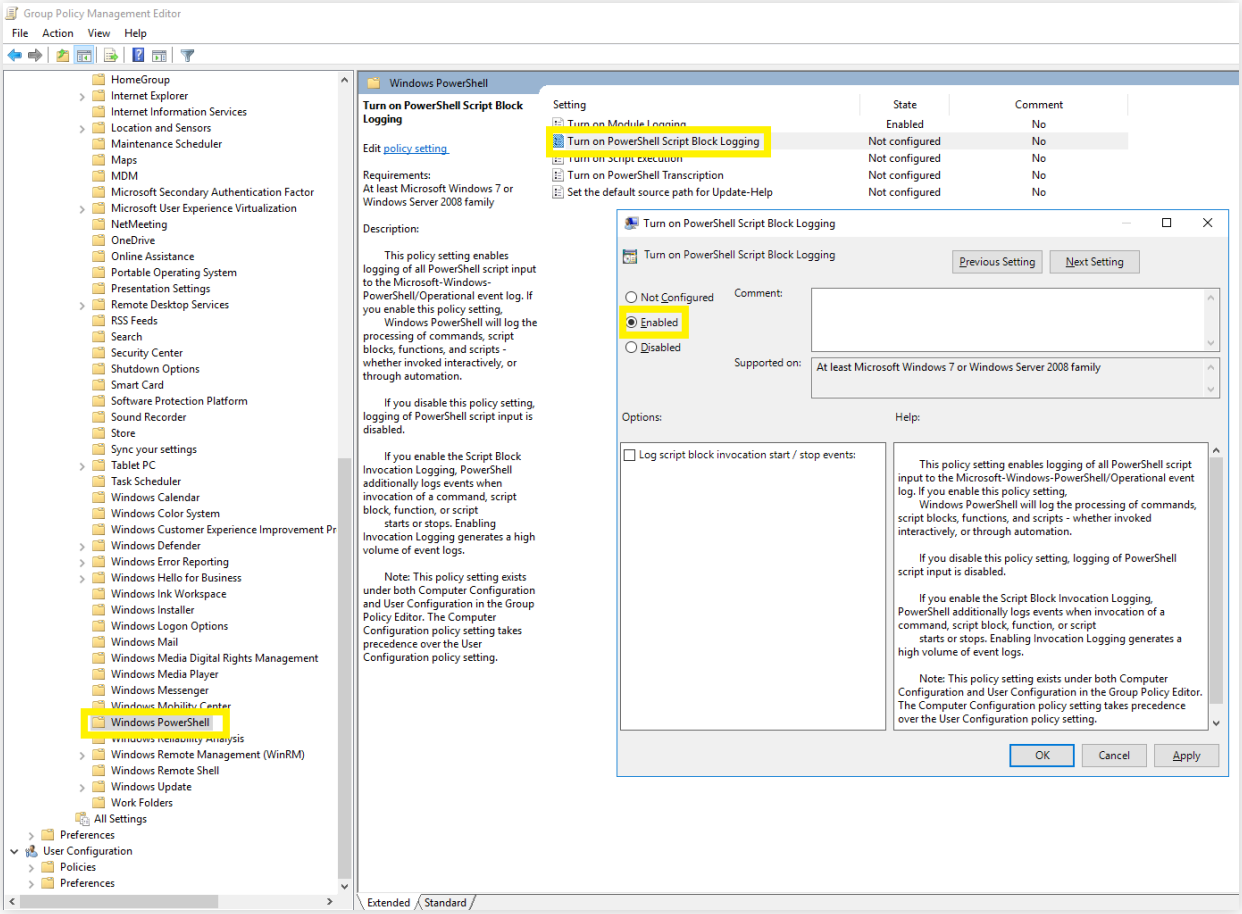
2.2.2. Rejestrowanie bloku skryptu

1. Zaloguj się do dowolnego komputera z konsolą GPMC, używając poświadczeń administratora domeny.

2. Otwórz konsolę **GPMC** i, w zależności od konfiguracji, edytuj:

   - Default Domain Controllers Policy, aby włączyć rejestrowanie modułu w kontrolerze DC.
   - ADAuditPlusMSPolicy, aby włączyć rejestrowanie modułu w serwerze Windows.

3. W Group Policy Management Editor przejdź do obszaru Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Powershell. Przejdź do prawego panelu i prawym przyciskiem kliknij opcję Turn on PowerShell Script Block Logging > Enabled.



3. Konfiguracja rozmiaru dziennika

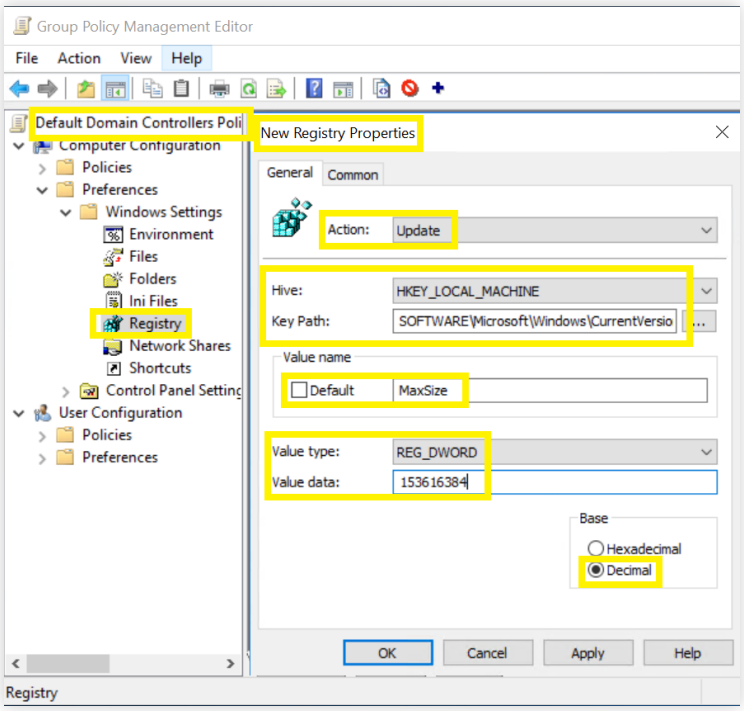
Zalecamy ustawienie maksymalnego rozmiaru dziennika PowerShell na 150 MB. Aby to zrobić, wykonaj niżej opisane czynności.

1. Zaloguj się do dowolnego komputera z konsolą GPMC, używając poświadczeń administratora domeny.

2. Otwórz konsolę GPMC i, w zależności od konfiguracji, edytuj:
   - Default Domain Controllers Policy, aby włączyć rejestrowanie modułu w kontrolerze DC.
   - ADAuditPlusMSPolicy, aby włączyć rejestrowanie modułu w serwerze Windows.

3. W Group Policy Management Editor przejdź do obszaru Computer Configuration > Preferences > Windows Settings, i prawym przyciskiem myszy kliknij k Registry > New > Registry Item.

4. W polu Action kreatora New Registry Properties wybierz Update z listy rozwijanej.
   W polu Hivewybierz **HKEY_LOCAL_MACHINE** z listy rozwijanej. W polu Key Path wpisz: **SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-PowerShell\Operational.** W polu *Value wartości* usuń zaznaczenie pola obok opcji **Default** i podaj **MaxSize**. W polu *Typ wartości* wybierz **REG_DWORD** z listy rozwijanej.
   W polu *Value type* wpisz **153616384.** W polu Base wybierz **Decimal**, a następnie kliknij **Apply.**



4. Rozwiązywanie problemów

1. **Jak zweryfikować, czy pożądane zdarzenia są rejestrowane?**

   Otwórz **Event Viewer** w komputerze, w którym skonfigurowano inspekcję PowerShell. Przejdź do lewego panelu i kliknij opcję Application and Service Logs > Microsoft > Windows > PowerShell > Operational. Sprawdź, czy zdarzenia **4103** oraz **4104** są rejestrowane.