ManageEngine

Przewodnik po konfiguracji procesu inspekcji programu Windows PowerShell



www.adauditplus.com

Spis treści

Przegląd	1
1. Konfiguracja inspekcji programu PowerShell w ADAudit Plus	1
2. Konfiguracja zasad inspekcji w domenie	1
2.1. Konfiguracja automatyczna	1
2.2. Konfiguracja ręczna	2
2.2.1. Rejestrowanie modułu	2
2.2.2. Rejestrowanie bloku skryptu	3
3. Konfiguracja rozmiaru dziennika	4
4. Rozwiązywanie problemów	5

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

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

- 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.
- 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.

Group Policy Management Editor								
File Action View Help								
HomeGroup	Mindaux David Chall							
Internet Explorer	Windows Powershell							
Internet Information Services	Turn on PowerShell Script Block	Setting		State	Comment			
I ocation and Sensors	Logging	Turn on M	Andule Longing	Enabled	No			
Maintenance Scheduler		Turn on P	owerShell Script Block Logging	Not configured	No			
Mans	Edit policy setting	an rum on a	CIDUEXECUTION	Not configured	No			
MDM	Requirements:	Turn on P	owerShell Transcription	Not configured	No			
Microsoft Secondary Authentication Factor	At least Microsoft Windows 7 or	E Set the de	fault source nath for Undate-Help	Not configured	No			
Microsoft User Experience Virtualization	Windows Server 2008 family	in our me de	and source pair for opaate freep	Not configured				
NetMeeting			Turn on PowerShell Script Block L	oqqinq		— п х		
OneDrive	Description:		<u>~</u>					
Coline Assistance	This policy setting enables	alicy setting enables 🗮 Turp on PowerShell Script Block Logging						
Portable Operating System	logging of all PowerShell script input				Previous Setting Next Setting			
Presentation Settings	to the Microsoft-Windows-							
Remote Deskton Services	PowerShell/Operational event log. If		O Not <u>C</u> onfigured Comment:			~		
RSS Feeds	you enable this policy setting,		Enabled					
Search	processing of commands, script		C Lindbled					
Security Center	blocks, functions, and scripts -		O Disabled			~		
Shutdown Options	whether invoked interactively, or		Supported on:	At least Microsoft Window	s 7 or Windows Server 2008 family	~		
Smart Card	through automation.							
Software Protection Platform	Marian disable shis settion estimat					×		
Sound Recorder	logging of PowerShell script input is		Ontions:	Help				
Store	disabled.		options	(icipi				
Svnc your settings								
Tablet PC	If you enable the Script Block		Log script block invocation start / s	stop events: This	policy setting enables logging of all Po	werShell script		
Task Scheduler	additionally logs events when			input to f	he Microsoft-Windows-PowerShell/Op	perational event		
Windows Calendar	invocation of a command, script			log. If yo	u enable this policy setting,			
Windows Color System	block, function, or script			Wine	dows PowerShell will log the processing	J of commands,		
Windows Customer Experience Improvement Pr	starts or stops. Enabling			interactio	ecks, runctions, and scripts - whether in welv, or through automation	voked		
> 🦰 Windows Defender	Invocation Logging generates a high							
> 🦳 Windows Error Reporting	volume of event logs.			lf yo	u disable this policy setting, logging of	PowerShell		
> C Windows Hello for Business	Note: This policy setting exists			script inp	ut is disabled.			
Windows Ink Workspace	under both Computer Configuration			lf.ue	u anabla the Seriet Black Investiga La	aning		
Windows Installer	and User Configuration in the Group			PowerSh	ell additionally logs events when invoc	ation of a		
Windows Logon Options	Configuration policy ratting takes			comman	d, script block, function, or script			
Windows Mail	precedence over the User			start	s or stops. Enabling Invocation Loggin	g generates a		
Windows Media Digital Rights Management	Configuration policy setting.			high volu	ime of event logs.			
Windows Media Player				Note	This policy setting exists under both	Computer		
Windows Messenger				Configur	ation and User Configuration in the Gr	oup Policy Editor.		
Conter Windows Mobility Center				The Com	puter Configuration policy setting take	s precedence		
Windows PowerShell				over the	User Configuration policy setting.	~		
windows Kenability AnalySis								
> 🧮 Windows Remote Management (WinRM)					OK Canc	el <u>A</u> pply		
Windows Remote Shell								
> 📫 Windows Update								
Work Folders								
C All Settings								
> Preferences								
✓ K User Configuration								
> Policies								
> Preferences v								
< >	Extended Standard							

3. Konfiguracja rozmiaru dziennika

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

- 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.
- 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.

ManageEngine)

ManageEngine ADAudit Plus to działające w czasie rzeczywistym oprogramowanie do inspekcji i sprawozdawczości o następujących funkcjach:

Monitorowanie usługi Active Directory (AD), Azure AD, serwerów plików systemu Windows, serwerów członkowskich i stacji roboczych oraz pomoc w przestrzeganiu rozporządzeń, w tym HIPAA, RODO, oraz innych regulacji.

Zamiana surowych i niejasnych danych dziennika zdarzeń w praktyczne, generowane po kilku kliknięciach raporty, które informują o działaniach poszczególnych użytkowników oraz o czasie i miejscu ich wykonania w ekosystemie Windows.

Identyfikacja nieprawidłowej aktywności oraz wykrywanie potencjalnych zagrożeń dla przedsiębiorstwa za pomocą analizy zachowań użytkownika (User Behaviour Analytics, UBA).