

Audit-GPO-Skript für die NTLM-Ablösung: kostenlos und ohne Risiko

Bevor du NTLM abschalten kannst, musst du wissen, wer es benutzt. Und bevor du das weißt, muss Windows es erst einmal protokollieren und die Ereignisse an einer Stelle sammeln. Klingt nach einer Stunde Klickarbeit in der Gruppenrichtlinienverwaltung, ist es auch, und genau an dieser Stelle schleichen sich die Fehler ein, die einem später die halbe Auswertung verhageln.

Deshalb gibt es dieses PowerShell-Skript kostenlos. Es legt ein vollständiges Gruppenrichtlinienobjekt für das NTLM-Auditing samt Ereignisweiterleitung an und erzeugt die passende Subscription-Datei für deinen Windows Event Collector. Es blockiert nichts und verknüpft nichts. Wann und wo das GPO wirkt, entscheidest du.

Produkt

Die Ereignisse auswerten: wer, wohin, warum, was tun.

[Zum NTLM Diagnostiker](#)

Beratung

Hilfe bei Einrichtung, Analyse und Abschaltung.

[Zur Beratung NTLM-Ablösung](#)

Schulung

Auditing, Ereignisse und Kerberos im Workshop.

[Zum Schulungsangebot](#)

Das Skript auf einen Blick

Name	New-NtlmAuditGpo.ps1
Download	New-NtlmAuditGpo.ps1 herunterladen
Preis	kostenlos, ohne Registrierung
Was es tut	legt ein GPO mit NTLM-Auditing und Ereignisweiterleitung an, erzeugt die Subscription-Datei für den Collector
Was es nicht tut	nichts blockieren, nichts verknüpfen, nichts auf Clients oder Servern direkt ändern
Voraussetzung	Windows PowerShell 5.1 oder neuer, RSAT mit Gruppenrichtlinienverwaltung, Rechte zum Anlegen von GPOs
Prüfsumme (SHA-256)	29d4adc414cb413caf546a66db9c409bfb3036662057267d7b952813053f8bfa

Was das Skript einstellt

Das Skript legt ein einziges GPO an, standardmäßig mit dem Namen „NTLM-Audit“. Es ist für die Verknüpfung auf Domänenebene gedacht, sodass Clients, Server und Domain Controller dieselbe Richtlinie bekommen. Die Einstellung für die domänenweite Überwachung wirkt ohnehin nur auf Domain Controllern.

Einstellung	Wert	Wirkung
Eingehenden NTLM-Datenverkehr überwachen	Überwachung für alle Konten	Server protokollieren eingehende NTLM-Anmeldungen
Ausgehenden NTLM-Datenverkehr zu Remoteservern einschränken	Alle überwachen	Clients protokollieren ausgehende Anmeldungen, ohne sie zu blockieren

Einstellung	Wert	Wirkung
NTLM-Authentifizierung in dieser Domäne überwachen	Alle aktivieren	Domain Controller protokollieren alle NTLM-Anmeldungen der Domäne
Ereignisweiterleitung (Zielabonnement-Manager)	Adresse deines Collectors	Maschinen schicken ihre NTLM-Ereignisse an den Collector
Dienst Windows-Remoteverwaltung (WinRM)	Automatisch	Voraussetzung für die Weiterleitung
Protokoll Microsoft-Windows-NTLM/Operational	aktiviert, 32 MB, Lesezugriff für NETWORK SERVICE	genug Puffer, und die Weiterleitung darf das Protokoll lesen

Wichtig: Überwachen heißt nicht blockieren

Alle Restrict-NTLM-Werte stehen auf Überwachung. Kein einziger Wert verweigert NTLM. Prüfe vor dem Verknüpfen trotzdem, ob ein anderes GPO mit höherer Rangfolge NTLM bereits einschränkt, denn sonst überschreibt dieses Audit-GPO womöglich eine strengere Einstellung.

Welche Ereignisse die Subscription sammelt

Die Subscription-Datei filtert ausschließlich das Protokoll Microsoft-Windows-NTLM/Operational und darin nur diese Ereignisse:

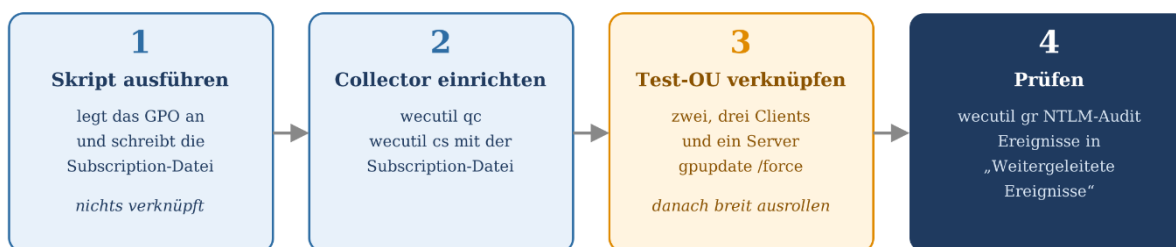
- **4020 bis 4023:** erweiterte Client- und Server-Ereignisse mit Reason-ID
- **4024 und 4025:** NTLMv1 bei der einfachen Anmeldung überwacht beziehungsweise blockiert
- **4030 bis 4033:** domänenweite Ereignisse der Domain Controller
- **8001 bis 8004:** klassische Restrict-NTLM-Überwachung, auch von älteren Systemen

Was die einzelnen Ereignisse bedeuten und welche Systeme welche liefern, steht in Microsofts [Übersicht zum erweiterten NTLM-Auditing](#). Die Reason-IDs erklärt der Artikel [NTLM-Reason-IDs erklärt](#).

So setzt du das Skript ein

Vom Skript zu den ersten Ereignissen

Vier Schritte, keiner davon blockiert etwas



Danach liest der NTLM Diagnostiker den Collector und sagt dir, warum NTLM benutzt wurde

Skizze 1: Vom Skript zu den ersten Ereignissen

Schritt 1: Skript ausführen

Führe das Skript als Domänen-Admin auf einem Rechner mit Gruppenrichtlinienverwaltung aus, am besten auf Windows 11 ab 24H2 oder Windows Server 2025. Dort kennt Windows das NTLM-Protokoll

bereits, und das Skript kann die Leseberechtigung für die Weiterleitung sauber übernehmen. Auf älteren Systemen bekommst du eine Warnung, und die Berechtigung musst du anders lösen (siehe Fehlersuche).

```
.\New-NtlmAuditGpo.ps1 -CollectorFqdn wec01.musterwerk.local
```

Optional: **-GpoName** für einen eigenen Namen, **-LogMaxSizeMB** für die Protokollgröße, **-RefreshSeconds** für das Abfrageintervall. Mit **Get-Help .\New-NtlmAuditGpo.ps1 -Full** siehst du alle Parameter.

Schritt 2: Collector einrichten

Auf dem Collector-Server richtest du den Sammeldienst ein und importierst die Subscription-Datei, die das Skript erzeugt hat:

```
wecutil qc /q
wecutil cs NTLM-Audit-Subscription.xml
wevtutil sl ForwardedEvents /ms:1073741824
```

Die letzte Zeile vergrößert das Protokoll „Weitergeleitete Ereignisse“ auf 1 GB. Bei großen Umgebungen gern mehr. Wie viele Maschinen ein Collector schafft und worauf du achten musst, steht im Artikel [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#).

Schritt 3: Erst eine Test-OU, dann die Domäne

Verknüpfe das GPO zuerst mit einer kleinen Test-OU, etwa zwei, drei Clients und ein Server, gern auch ein älteres System zum Vergleich. Auf den Testmaschinen gpupdate /force ausführen und ein paar Minuten warten. Wenn alles ankommt, verknüpfst du das GPO auf Domänenebene.

Schritt 4: Prüfen

```
wecutil gr NTLM-Audit
```

Die Testmaschinen sollten als „Active“ erscheinen. In der Ereignisanzeige des Collectors findest du die Ereignisse unter „Weitergeleitete Ereignisse“.

Schritt 5: Erweitertes Logging kontrollieren

Die erweiterten Ereignisse sind laut Microsoft standardmäßig aktiv. Hat jemand sie bewusst abgeschaltet, kommen nur die klassischen 8001 bis 8004 an. Kontrolliere deshalb im GPO die beiden Richtlinien „NTLM Enhanced Logging“ (Administrative Vorlagen > System > NTLM) und „Log Enhanced Domain-wide NTLM Logs“ (Administrative Vorlagen > System > Netlogon) und setze sie bei Bedarf auf „Aktiviert“. Dafür brauchst du aktuelle ADMX-Vorlagen im zentralen Speicher. Mehr dazu im Artikel [Erweitertes NTLM-Auditing einschalten](#).

Wenn nichts ankommt: Fehlersuche

Symptom	Wahrscheinliche Ursache	Abhilfe
Maschine erscheint nicht in wecutil gr	GPO noch nicht angewendet oder WinRM läuft nicht	gpupdate /force, Dienst WinRM prüfen, gpresult /r
Maschine ist „Active“, aber keine Ereignisse	NETWORK SERVICE darf das NTLM-Protokoll nicht lesen	Skript auf Windows 11 24H2 oder Server 2025 erneut ausführen oder NETWORK SERVICE in die Gruppe „Ereignisprotokollleser“ aufnehmen

Symptom	Wahrscheinliche Ursache	Abhilfe
Nur Ereignisse 8001 bis 8004	System zu alt oder erweitertes Logging abgeschaltet	Updatestand prüfen, Richtlinien aus Schritt 5 kontrollieren
Verbindungsfehler zum Collector	Port 5985 gesperrt oder falscher Name	Firewall prüfen, Collector-FQDN im GPO kontrollieren
Collector wird langsam	zu viele Clients oder zu kleines Protokoll	Protokoll vergrößern, ab einigen tausend Clients einen zweiten Collector einplanen

Rückgängig machen

Weil das Skript nichts blockiert, gibt es auch nichts zu reparieren. Wenn du das Auditing wieder entfernen willst:

- GPO-Verknüpfung entfernen oder das GPO „NTLM-Audit“ löschen
- Auf dem Collector: `wecutil ds NTLM-Audit`
- Beim nächsten Gruppenrichtlinien-Abgleich fallen die Einstellungen auf den vorherigen Stand zurück

Und dann? Vom Ereignis zur Lösung

Nach ein paar Tagen hast du Tausende Ereignisse im Collector. Jedes einzelne ist aufschlussreich, alle zusammen sind erst mal eine Wand. Genau hier setzt der NTLM Diagnostiker an: Er liest den Collector, ordnet jeder Verbindung eine Ursache zu, prüft gegen DNS und SPNs, findet NTLMv1 und simuliert, was eine Abschaltung treffen würde.

So geht es weiter

Starte mit dem kostenlosen Express des [NTLM Diagnostikers](#). Er braucht nicht einmal den Collector und liefert dir in fünf Minuten ein erstes Lagebild direkt von den Domain Controllern. Für die vollständige Auswertung nimmt er dann die Ereignisse, die dieses Skript einsammelt.

Häufige Fragen

Ist das Skript wirklich kostenlos?

Ja, ohne Registrierung und ohne Haken. Es ist der erste Schritt jeder NTLM-Ablösung, und den soll niemand von Hand zusammenklicken müssen.

Kann das Skript etwas kaputt machen?

Es legt nur ein GPO an und verknüpft es nicht. Alle Werte stehen auf Überwachung. Prüfen solltest du lediglich, ob ein anderes GPO NTLM bereits strenger einschränkt.

Brauche ich einen eigenen Server als Collector?

Ein Mitgliedsserver mit genug Plattenplatz reicht. Ein Domain Controller muss es nicht sein und sollte es auch nicht.

Wie lange sollte ich sammeln?

Mindestens 30 Tage, damit Monatsabschlüsse und Quartalsjobs mit drin sind.

Funktioniert das auch mit älteren Systemen?

Ja, Windows 10 und Server 2016 liefern die klassischen Ereignisse 8001 bis 8004, allerdings ohne Reason-ID. Die erweiterten Ereignisse gibt es ab Windows 11 24H2, Server 2025 sowie Server 2022 und 2019 mit Updates ab 13. Oktober 2026.

Wozu die Prüfsumme?

Damit du sicher sein kannst, dass die heruntergeladene Datei unverändert ist: Get-FileHash .\New-NtlmAuditGpo.ps1 muss denselben SHA-256-Wert liefern wie oben angegeben.