Erweitertes NTLM-Auditing einschalten: Schritt für Schritt



WISSEN
Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er kostet.
› NTLM Diagnostiker

BERATUNG
Auditing einrichten, Ergebnisse bewerten, Abschaltung planen: mit Begleitung.
› Beratung zur NTLM-Ablösung

SCHULUNG
NTLM-Auditing einrichten und Ereignisse lesen: für dein ganzes Team.
› Schulung zum NTLM Diagnostiker

NTLM ist wie der Wasserschaden hinter der Badezimmerfliese: Solange du nicht hinschaust, ist alles in Ordnung. Viele Domänen laufen seit Jahren genau nach diesem Prinzip. Das ging gut, bis Microsoft einen Termin daraus gemacht hat. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten standardmäßig, und mit der nächsten Windows-Server-Version soll NTLM insgesamt standardmäßig abgeschaltet sein. Den Zeitplan dazu findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Bevor du irgendetwas abschaltest, musst du wissen, wer NTLM überhaupt noch benutzt. Dafür gibt es das erweiterte NTLM-Auditing. Es schreibt nicht nur auf, dass NTLM benutzt wurde, sondern auf dem Client auch, warum Windows nicht Kerberos genommen hat. Dieser Beitrag zeigt dir, wie du NTLM-Auditing aktivieren kannst, ohne dabei versehentlich etwas zu sperren: welche Systeme es können, welche Gruppenrichtlinien du setzt, warum die klassische Restrict-NTLM-Überwachung trotzdem dazugehört, wie groß das Protokoll sein muss und wie du am Ende prüfst, ob überhaupt etwas ankommt. Der letzte Punkt ist der, an dem die meisten Projekte unbemerkt scheitern.

FAKTEN · NTLM-Auditing aktivieren: das Wichtigste in Kürze

Erweitertes Auditing nach Microsoft KB5064479: Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Windows-Updates ab dem 13.10.2026.

Ereignisse 4020 und 4021 (Client), 4022 und 4023 (Server), 4030 bis 4033 (Domain Controller), alle im Protokoll Microsoft-Windows-NTLM/Operational.

Steuerung über zwei administrative Vorlagen: „NTLM Enhanced Logging“ unter System › NTLM und

„Log Enhanced Domain-wide NTLM Logs“ unter System › Netlogon.

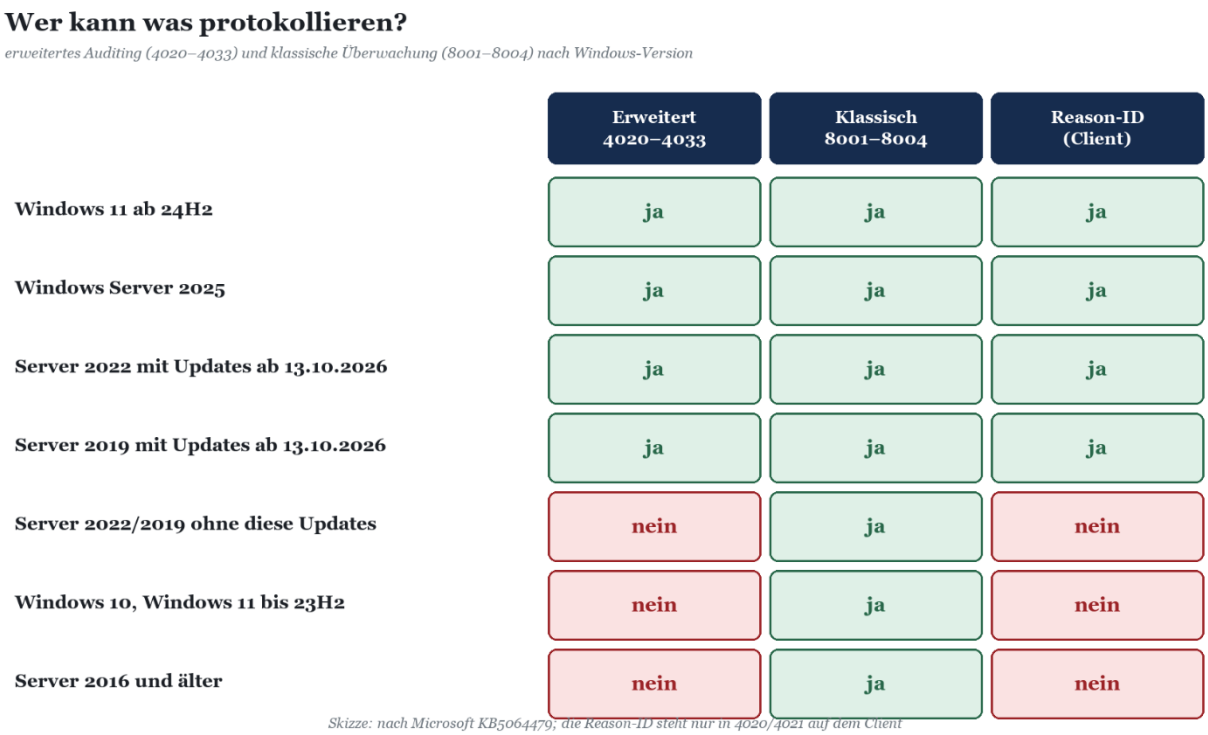
Laut Microsoft sind die neuen Ereignisse standardmäßig eingeschaltet. Die Richtlinien legen den Zustand verbindlich fest, damit du dich nicht auf Vermutungen verlassen musst.

Die klassischen Ereignisse 8001 bis 8004 bleiben erhalten und funktionieren auch auf älteren Systemen, liefern aber keine Ursache.

Bevor du klickst: welche Systeme was können

Das erweiterte Auditing ist keine neue Gruppenrichtlinie, die du einfach überall verteilst. Es ist eine Funktion des Betriebssystems, und die gibt es nur auf bestimmten Versionen mit bestimmtem Update-Stand. Ein Rechner ohne diese Funktion ignoriert die Richtlinie höflich und schreibt einfach nichts. Er beschwert sich nicht, er meldet keinen Fehler. Er schweigt, und du hältst ihn für sauber.

Erweitertes Auditing: die Systemvoraussetzungen



Betriebssystem	Erweitertes Auditing	Klassisch 8001–8004	Bemerkung
Windows 11 24H2, 25H2, 26H1, 26H2	ja	ja	volle Client-Sicht mit Reason ID
Windows Server 2025	ja	ja	auch als Domain Controller
Windows Server 2022	ja, mit Updates ab 13.10.2026	ja	Microsoft nennt KB5126655 als Beispiel
Windows Server 2019	ja, mit Updates ab 13.10.2026	ja	Microsoft nennt KB5126651 als Beispiel
Windows 10, Windows 11 bis 23H2	nein	ja	nur Restrict-NTLM-Überwachung
Windows Server 2016 und älter	nein	ja	nur Restrict-NTLM-Überwachung

Die genaue Liste pflegt Microsoft im Supportartikel Overview of NTLM auditing enhancements in Windows 11 and Windows Server 2025. Schau dort vor dem Rollout noch einmal hinein, denn die Angaben zu den unterstützten Serverversionen sind im Änderungsprotokoll des Artikels nicht ganz einheitlich formuliert.

Zwei Generationen von Ereignissen

Du hast es künftig mit zwei Familien zu tun, die friedlich im selben Protokoll Microsoft-Windows-NTLM/Operational nebeneinander wohnen. Microsoft betont ausdrücklich, dass das erweiterte Auditing die bisherigen Ereignisse nicht verändert: Was du heute schon mit 8001 bis 8004 protokollierst, läuft weiter.

Ereignis	Rolle	Gesteuert durch	Besonderheit
4020 / 4021	Client	NTLM Enhanced Logging	ausgehend, mit Reason ID, Target Machine, Process Name, NTLM Version
4022 / 4023	Server	NTLM Enhanced Logging	eingehend, mit Client Machine, Client IP, NTLM Version
4030 / 4031	Domain Controller	Log Enhanced Domain-wide NTLM Logs	Anfrage domänenübergreifend, Quelle Security-Netlogon
4032 / 4033	Domain Controller	Log Enhanced Domain-wide NTLM Logs	Anfrage aus derselben Domäne, mit Server Name und Server OS
8001	Client	Restrict NTLM: ausgehend	ausgehende NTLM-Anmeldung, ohne Ursache
8002 / 8003	Server	Restrict NTLM: eingehend	eingehende NTLM-Anmeldung, ohne Ursache
8004	Domain Controller	Restrict NTLM: in dieser Domäne	vom DC geprüfte Anmeldung

Die jeweils ungerade Nummer ist die Warnung: Dort markiert Windows Anmeldungen mit Sicherheitsabstufung, etwa NTLMv1. Was in den einzelnen Feldern steht, beschreiben Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen, Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern und NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

WARNUNG · Windows 10 und Server 2016 schweigen

Auf Windows 10, Windows 11 bis 23H2 und Windows Server 2016 gibt es kein 4020, kein 4022 und kein 4032, egal welche Richtlinie du setzt. Auch ein Server 2019 oder 2022, der seit Monaten keine Updates gesehen hat, bleibt stumm. Für diese Systeme brauchst du die klassische Restrict-NTLM-Überwachung. Sonst hast du eine Abdeckung wie ein Schweizer Käse, nur ohne Geschmack.

Bestand und Update-Stand prüfen

Bevor du Richtlinien verteilst, verschaff dir einen Überblick. Die Betriebssystemversion steht im Computerkonto in Active Directory:

```
Get-ADComputer -Filter 'Enabled -eq $true' -Properties OperatingSystem, OperatingSystemVersion
|
  Group-Object OperatingSystem, OperatingSystemVersion | Sort-Object Count -Descending |
  Select-Object Count, Name
```

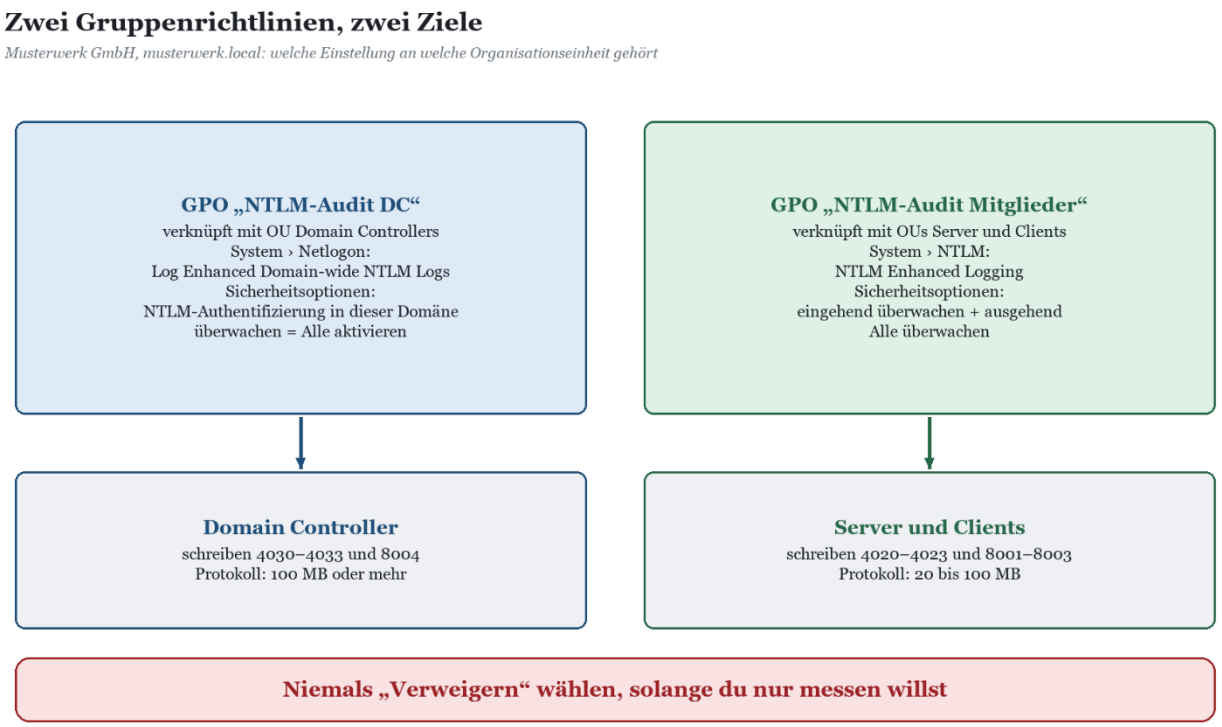
Der Update-Stand steht dort leider nicht. Für Server 2019 und 2022 prüfst du ihn am System selbst, zum Beispiel über die zuletzt installierten Updates:

```
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5 HotFixID, InstalledOn
```

Steht dort kein Update vom 13.10.2026 oder später, schreibt der Server keine erweiterten Ereignisse. Das ist der Moment, an dem du entweder Updates einspielst oder dir notierst, dass du dich bei diesem System auf 8001 bis 8004 verlassen musst.

Schritt für Schritt: die Gruppenrichtlinien einrichten

Jetzt geht es ans Eingemachte. Du brauchst die Gruppenrichtlinienverwaltung (gpmc.msc), Domänen-Admin-Rechte oder delegierte Rechte auf die betroffenen Organisationseinheiten und etwa eine halbe Stunde, in der niemand anruft. Letzteres ist erfahrungsgemäß die schwierigste Voraussetzung.



Skizze: empfohlene Aufteilung; Namen der Gruppenrichtlinienobjekte frei gewählt

Schritt 1: Vorlagen aktualisieren und Gruppenrichtlinienobjekte anlegen

Die beiden neuen Einstellungen tauchen im Gruppenrichtlinien-Editor nur auf, wenn die administrativen Vorlagen aktuell sind. Arbeitest du mit dem zentralen Speicher (PolicyDefinitions im SYSVOL), aktualisiere ihn mit den Vorlagen eines Systems, das bereits auf dem passenden Stand ist, etwa eines Windows 11 24H2 oder Windows Server 2025 mit aktuellen Updates. Findest du unter System › NTLM nichts, ist fast immer der zentrale Speicher veraltet.

Lege danach zwei Gruppenrichtlinienobjekte an: eines für die Domain Controller, eines für Server und Clients. Du kannst alles in ein Objekt packen, aber getrennte Objekte machen die Fehlersuche leichter und verhindern, dass DC-Einstellungen auf 800 Notebooks landen, wo sie nichts zu suchen haben.

Schritt 2: NTLM Enhanced Logging für Clients und Server

Öffne das Gruppenrichtlinienobjekt für Server und Clients und navigiere zu:

```
Computerkonfiguration › Richtlinien › Administrative Vorlagen › System › NTLM
  NTLM Enhanced Logging = Aktiviert
```

Diese Einstellung steuert die Ereignisse 4020 bis 4023. Microsoft schreibt, dass die Ereignisse standardmäßig eingeschaltet sind. Warum also die Mühe? Weil „standardmäßig“ in jeder Domäne mit zwanzig Jahren Gruppenrichtliniengeschichte etwas anderes bedeutet. Mit einer aktiv gesetzten Richtlinie weißt du, welcher Zustand gilt, und kannst es mit gpresult belegen. Verknüpfe das Objekt mit den Organisationseinheiten für Server und Clients.

TIPP · Erst eine Pilotgruppe

Verknüpfe das Objekt zuerst mit einer kleinen Organisationseinheit oder filtere es per Sicherheitsgruppe auf zehn bis zwanzig Rechner aus verschiedenen Abteilungen. Nach ein bis zwei Tagen siehst du, wie viele Ereignisse pro Tag entstehen, und kannst die Protokollgröße für die Fläche realistisch festlegen.

Schritt 3: Log Enhanced Domain-wide NTLM Logs für Domain Controller

Im Gruppenrichtlinienobjekt für die Domain Controller setzt du:

```
Computerkonfiguration › Richtlinien › Administrative Vorlagen › System › Netlogon
  Log Enhanced Domain-wide NTLM Logs = Aktiviert
```

Damit schreiben die Domain Controller die Ereignisse 4030 bis 4033 mit der Quelle Security-Netlogon. Sie sehen jede NTLM-Anmeldung mit Domänenkonto, die über sie geprüft wird, inklusive Server Name und Server OS des Zielsystems. Verknüpfe das Objekt mit der Organisationseinheit Domain Controllers, und zwar mit allen Domänen der Gesamtstruktur, nicht nur mit der, in der du gerade sitzt.

FAKTEN · Was der DC nicht sieht

Anmeldungen mit lokalen Konten erreichen den Domain Controller nie. Und die Ursache, also die Reason ID, steht ausschließlich im Client-Ereignis 4020 oder 4021. Wer nur die Domain Controller überwacht, hat einen guten Überblick, aber keine Erklärung.

Schritt 4: die klassische Restrict-NTLM-Überwachung dazunehmen

Für alle Systeme, die das erweiterte Auditing nicht können, nimmst du die altbekannten Sicherheitsoptionen dazu. Sie liegen unter Computerkonfiguration › Richtlinien › Windows-Einstellungen › Sicherheitseinstellungen › Lokale Richtlinien › Sicherheitsoptionen. Auf aktuellen Systemen schaden sie nicht, sie liefern die Ereignisse 8001 bis 8004 zusätzlich.

Richtlinie	Wert zum Messen	Ziel	Ereignis
Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Datenverkehr zu Remoteservern	Alle überwachen	Server und Clients	8001
Netzwerksicherheit: NTLM einschränken: Eingehenden NTLM-Datenverkehr überwachen	Überwachung für alle Konten aktivieren	Server und Clients	8002, 8003
Netzwerksicherheit: NTLM einschränken: NTLM-Authentifizierung in dieser Domäne überwachen	Alle aktivieren	Domain Controller	8004

WARNUNG · Ein Klick daneben, und der Montag ist gelaufen

Die Richtlinie für ausgehenden Datenverkehr kennt drei Werte: Alle zulassen, Alle überwachen und

Alle verweigern. Daneben gibt es die Schwesterrichtlinien „Eingehender NTLM-Datenverkehr“ und „NTLM-Authentifizierung in dieser Domäne“ ohne das Wort „überwachen“ im Namen. Die verweigern, wenn man sie lässt. Wer beim Messen versehentlich dort landet, ermittelt die NTLM-Nutzung über das Ticketsystem. Kontrolliere jede Einstellung zweimal.

Wie Überwachen, Ausnahmen und Verweigern zusammenspielen, erklärt Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern.

Schritt 5: das Protokoll vergrößern

Das Protokoll Microsoft-Windows-NTLM/Operational ist ab Werk eher auf Diät gesetzt. Auf einem Dateiserver mit erweitertem Auditing ist es schneller voll, als du „Reason ID“ sagen kannst, und dann überschreibt Windows die ältesten Einträge. Genau die, die du am Montag auswerten wolltest. Prüfe Größe und Zustand so:

```
wevtutil gl Microsoft-Windows-NTLM/Operational

# Größe auf 100 MB setzen (Angabe in Bytes)
wevtutil sl Microsoft-Windows-NTLM/Operational /ms:104857600

# Falls das Protokoll deaktiviert ist
wevtutil sl Microsoft-Windows-NTLM/Operational /e:true
```

In der Ausgabe von wevtutil gl achtest du auf enabled (muss true sein) und maxSize. Für die Verteilung in der Fläche packst du die Zeile in ein Startskript der Gruppenrichtlinie oder in deine Softwareverteilung. Als Richtwerte haben sich folgende Größen bewährt; sie sind unsere Empfehlung, keine Microsoft-Vorgabe:

Rolle	Empfohlene Größe	Begründung
Arbeitsplatz	20 bis 50 MB	wenige ausgehende Anmeldungen, Reason IDs wichtig
Mitgliedsserver	50 bis 100 MB	viele eingehende Anmeldungen, je nach Last
Dateiserver, Druckserver	100 bis 200 MB	fünfstellige Ereignismengen pro Tag möglich
Domain Controller	100 MB oder mehr	sieht alle Domänenanmeldungen, unbedingt zentral sammeln

Ein großes lokales Protokoll ist ein Puffer, kein Archiv. Für eine Auswertung über Wochen brauchst du eine zentrale Sammlung. Wie das mit Bordmitteln geht, zeigt NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

Schritt 6: verteilen und anwenden

Gruppenrichtlinien kommen von allein, nur eben nicht dann, wenn du darauf wartest. Für den Pilotrechner beschleunigst du das, für ganze Organisationseinheiten hilft Invoke-GPUpdate:

```
gpupdate /force

# Remote für eine Organisationseinheit
Get-ADComputer -SearchBase 'OU=Pilot,OU=Clients,DC=musterwerk,DC=local' -Filter * |
  ForEach-Object { Invoke-GPUpdate -Computer $_.Name -RandomDelayInMinutes 0 -Force }
```

TIPP · Die Abkürzung: das kostenlose Audit-GPO-Skript

Wenn du die Schritte 2 bis 5 nicht für jede Domäne von Hand durchklicken willst, nimm das NTLM-

Audit-GPO-Skript. Es ist kostenlos und legt die Überwachungsrichtlinien für dich an, sodass du dich auf das konzentrieren kannst, was danach kommt: prüfen und auswerten. Gerade wenn du als Systemhaus viele Kundendomänen betreust, spart das Zeit und Tippfehler. Ein einheitliches Vorgehen über viele Kunden hinweg beschreibt NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

WICHTIG · Vorher mit Datenschutz und Betriebsrat sprechen

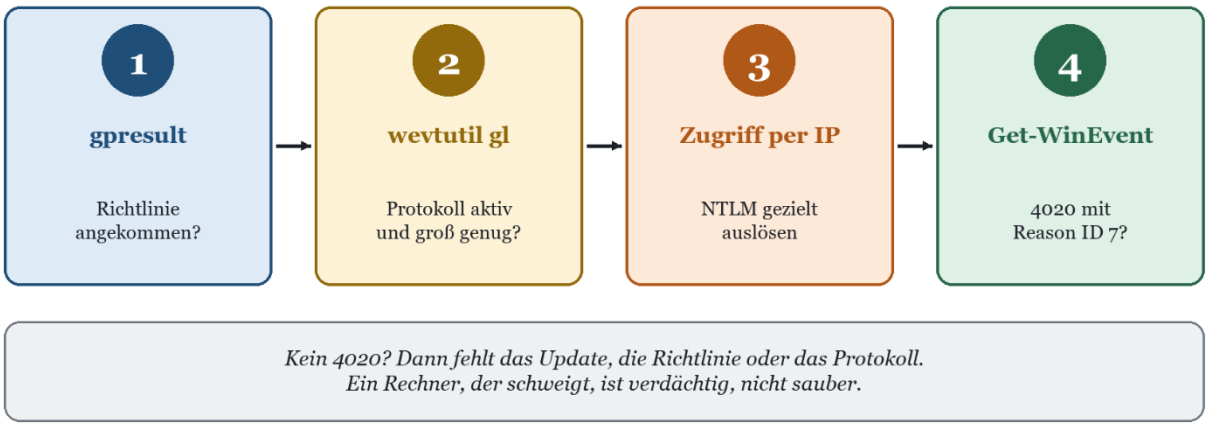
NTLM-Ereignisse enthalten Benutzernamen, Rechnernamen und Zeitstempel, also personenbezogene Daten. Kläre Zweck, Aufbewahrungsdauer und Zugriff, bevor du flächendeckend protokollierst. Worauf es ankommt, beschreibt NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Prüfen, ob es wirkt

Die Richtlinie ist verteilt, das Protokoll ist groß. Feierabend? Leider nein. Ein Auditing, das du nicht geprüft hast, ist ein Rauchmelder ohne Batterie: Er hängt an der Decke, er sieht beruhigend aus, und er wird dich im entscheidenden Moment im Stich lassen.

Der Rauchtest: wirkt das Auditing?

Trendforge Digital GmbH, trendforge.local: vier Prüfungen auf einem Pilotrechner



Skizze: Prüfablauf auf einem Client mit Windows 11 24H2; Firmenname frei erfunden

Der Rauchtest auf einem Pilotrechner

Zuerst prüfst du, ob die Richtlinie angekommen ist. gpresult zeigt die angewendeten Gruppenrichtlinienobjekte; im HTML-Bericht findest du auch die einzelnen Einstellungen:

```
gpresult /r /scope computer
gpresult /h C:\Temp\gpresult.html /scope computer
```

Dann löst du gezielt eine NTLM-Anmeldung aus. Der einfachste Weg: Greif auf eine Freigabe über die IP-Adresse statt über den Namen zu. Kerberos braucht einen Namen, also fällt Windows auf NTLM zurück, und das erweiterte Auditing muss ein 4020 mit Reason ID 7 schreiben, weil der Zielname eine IP-Adresse ist:

```
dir \\<IP-Adresse-des-Dateiservers>\<Freigabe>

Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational'; Id=4020,4021 }
  -MaxEvents 5 | Format-List TimeCreated, Id, Message
```

Im Meldungstext findest du „Target Machine“, „Reason ID“, „Reason“ und „NTLM Version“. Steht dort Reason ID 7, funktioniert das erweiterte Auditing auf diesem Client. Auf dem Dateiserver sollte zur selben Zeit ein 4022 erscheinen, auf dem zuständigen Domain Controller ein 4032. Wie du Reason ID 7 in der Praxis loswirst, steht in NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen; die übrigen Werte erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

TIPP · Gegenprobe mit dem Namen

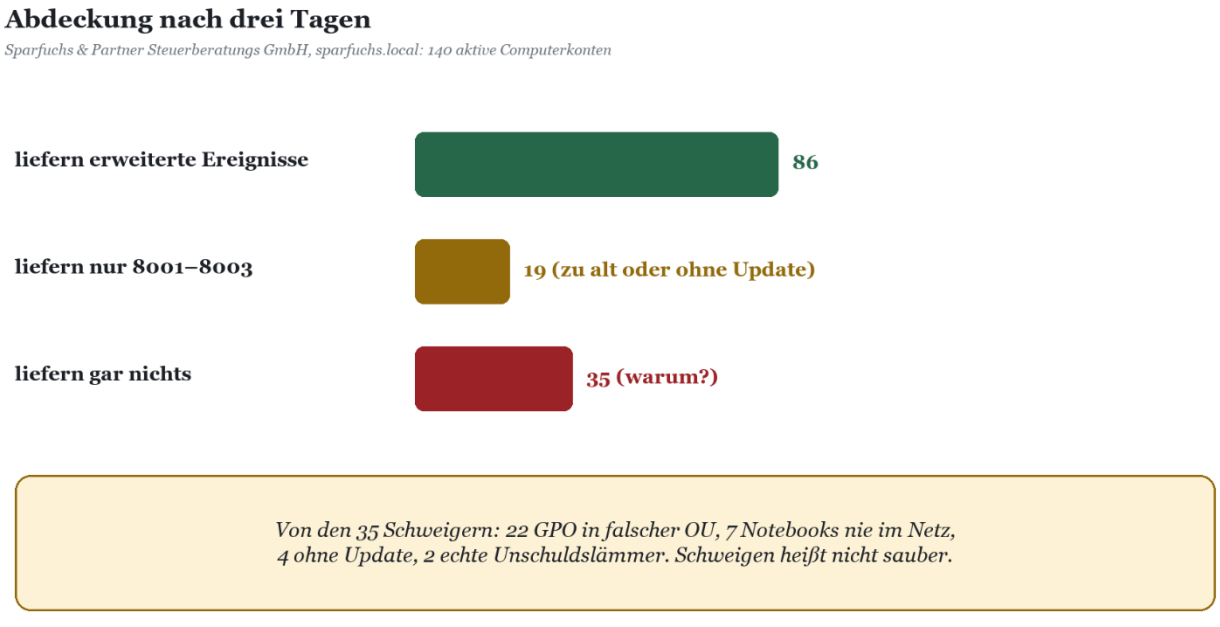
Greif danach auf dieselbe Freigabe über den vollständigen DNS-Namen zu, etwa \\srv-datei-02.musterwerk.local\daten. Dann sollte kein neues 4020 entstehen, weil Kerberos greift. Entsteht doch eines, hast du deinen ersten echten Befund, meist mit Reason ID 6 oder 8. Dann lohnt ein Blick auf SPN und DNS, etwa mit setspn -Q cifs/srv-datei-02.musterwerk.local.

Die Abdeckung in der Fläche prüfen

Ein funktionierender Pilotrechner beweist nur, dass die Technik geht. Die eigentliche Frage lautet: Liefern alle Rechner, die liefern sollten? Mit Bordmitteln heißt das, jeden Rechner einzeln zu fragen und das Ergebnis mit dem Bestand abzugleichen:

```
$pcs = (Get-ADComputer -Filter 'Enabled -eq $true' -SearchBase
'OU=Clients,DC=musterwerk,DC=local').Name
Invoke-Command -ComputerName $pcs -ErrorAction SilentlyContinue -ScriptBlock {
  $n = (Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational';
        Id=4020,4021,8001; StartTime=(Get-Date).AddDays(-3) } -ErrorAction
SilentlyContinue).Count
  [pscustomobject]@{ Ereignisse = $n }
} | Select-Object PSComputerName, Ereignisse | Sort-Object Ereignisse
```

Rechner, die gar nicht antworten, fehlen in der Ausgabe ganz. Die musst du gesondert ermitteln, indem du die Liste der Antworten gegen $pcs abgleichst. Und dann beginnt die Detektivarbeit: Ist der Rechner aus? Hängt er in der falschen Organisationseinheit? Fehlt das Update? Oder benutzt er tatsächlich kein NTLM? Nur die letzte Antwort ist eine gute Nachricht.



Skizze: Zahlen frei erfunden, aber typische Verteilung bei der ersten Auswertung

AUS DER PRAXIS · Sparfuchs & Partner: die stillen 25 Prozent

Bei der Sparfuchs & Partner Steuerberatungs GmbH lief das Auditing nach drei Tagen auf dem Papier vollständig. Die Auswertung zeigte etwas anderes: 35 von 140 Rechnern hatten kein einziges Ereignis geschrieben. 22 davon steckten in einer Organisationseinheit „Clients-alt“, mit der das Gruppenrichtlinienobjekt nie verknüpft war. Sieben Notebooks waren seit Wochen nicht im Büro, vier Server hatten das Oktober-Update noch nicht. Übrig blieben zwei Rechner, die wirklich kein NTLM sprachen. Ohne den Abgleich hätte die Kanzlei 35 Rechner als „sauber“ abgehakt.

Typische Fehler und ihre Ursachen

Symptom	Wahrscheinliche Ursache	Abhilfe
Einstellung unter System › NTLM fehlt im Editor	zentraler Speicher veraltet	PolicyDefinitions mit aktuellen Vorlagen aktualisieren
Nur 8001 bis 8004, kein 4020	Betriebssystem zu alt oder Update fehlt	Version und Update-Stand prüfen
Gar keine NTLM-Ereignisse	GPO nicht verknüpft, Filter falsch, Protokoll deaktiviert	gpresult, wevtutil gl
Ereignisse nur der letzten Stunden	Protokoll zu klein, Einträge werden überschrieben	maxSize erhöhen, zentral sammeln
4020 ohne Gegenstück 4022 auf dem Server	Server zu alt für erweitertes Auditing	dort auf 8002 und 8003 ausweichen
Benutzer melden plötzlich Zugriffsfehler	Verweigern statt Überwachen gewählt	Richtlinie sofort zurück auf Überwachen

Wo die Prüfung mit Bordmitteln mühsam wird

Bei einer Handvoll Server und einer Pilotgruppe ist das alles gut machbar. Ehrlich. Bei 300 Rechnern, drei Standorten und Notebooks, die nur dienstags im Netz sind, wird die Abdeckungsprüfung zum Dauerprojekt. Invoke-Command scheitert an der Firewall, das Skript liefert jede Woche eine andere Liste, und die IT-Leitung fragt, ob man „jetzt schon abschalten kann“. Darauf gibt es mit einer CSV-Datei keine überzeugende Antwort.

Genau hier setzt der NTLM Diagnostiker an. Er beantwortet die beiden Fragen, die nach dem Einschalten des Auditings offen bleiben: Liefert überhaupt jeder, der soll? Und wie weit bin ich von einer Abschaltung entfernt? Er arbeitet dabei ausschließlich lesend. Er setzt keine Richtlinie, ändert keinen SPN und fasst kein Konto an. Das Einschalten des Auditings bleibt deine Aufgabe, die Auswertung nimmt er dir ab.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Prüfen, ob das Auditing wirkt

Readiness-Ampel: Für jede Maschine siehst du auf einen Blick, wie es um ihre NTLM-Nutzung steht. Das ist die Antwort für die IT-Leitung, ohne Pivot-Tabelle.

Abdeckungsmonitor und OS-Landkarte: Sie zeigen, welche Rechner Ereignisse liefern, welche schweigen und welche wegen ihrer Windows-Version gar keine erweiterten Ereignisse schreiben können. Genau die Liste, die du oben mühsam per Invoke-Command zusammengesucht hast.

Ereignisquellen: direkt von den Domain Controllern, von einem vorhandenen Windows Event Collector oder per Direktabfrage der Rechner. Bestehendes Event Forwarding wird weiterverwendet.

Danach geht es an die Ursachen: Ursachen-Engine mit SPN- und DNS-Prüfung, NTLMv1-Hitliste, Kommunikationsmatrix und Konten-Sicht, Sicherheitsflaggen, Abschalt-Simulation sowie Word-

Bericht und Excel/CSV-Export. Ein Verlauf über mehrere Auswertungen ist geplant.

Einstieg: Die kostenlose Edition Express liefert einen Fünf-Minuten-Befund. Die Vollversion kannst du 7 Tage testen; lizenziert wird pro aktivem Computerkonto. Und alles passiert lesend.

› NTLM Diagnostiker

Wenn du beim Einrichten oder bei der Bewertung der ersten Ergebnisse Unterstützung willst, begleiten wir dich in der Beratung zur NTLM-Ablösung. Wer das Wissen ins eigene Team holen möchte, findet in der Schulung zum NTLM Diagnostiker den passenden Rahmen. Und was du mit den Ereignissen danach anfängst, beschreibt NTLM-Nutzung ermitteln: der komplette Leitfaden.

FAQ: NTLM-Auditing aktivieren

Ist das erweiterte NTLM-Auditing nicht ohnehin schon eingeschaltet?

Laut Microsoft sind die neuen Ereignisse standardmäßig aktiviert, sofern Betriebssystem und Update-Stand passen. Mit den Richtlinien „NTLM Enhanced Logging“ und „Log Enhanced Domain-wide NTLM Logs“ legst du den Zustand verbindlich fest und kannst ihn mit gpresult nachweisen.

Kann ich das erweiterte Auditing auf Windows 10 nachrüsten?

Nein. Es steht auf Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026 zur Verfügung. Auf Windows 10 nutzt du die Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8003.

Brauche ich die klassischen Restrict-NTLM-Richtlinien noch?

Ja, für alle Systeme ohne erweitertes Auditing. Auf aktuellen Systemen liefern sie zusätzliche Ereignisse, ohne zu stören. Wichtig ist nur, dass du ausschließlich die Überwachungswerte wählst.

Wo finde ich die Ereignisse in der Ereignisanzeige?

Unter Anwendungs- und Dienstprotokolle › Microsoft › Windows › NTLM › Operational. Dort stehen sowohl 4020 bis 4033 als auch 8001 bis 8004.

Wie groß sollte das NTLM-Protokoll sein?

Als Faustregel 20 bis 50 MB auf Arbeitsplätzen und 100 MB oder mehr auf Domain Controllern und Dateiservern. Entscheidend ist, dass die Einträge nicht schneller rotieren, als du sie auswertest oder zentral einsammelst.

Muss ich nach dem Einschalten neu starten?

Microsoft nennt dafür keinen Neustart. Notwendig ist das passende Windows-Update, das in der Regel ohnehin einen Neustart mitbringt. Die Gruppenrichtlinie selbst greift mit der nächsten Aktualisierung oder nach gpupdate /force.

Wie prüfe ich am schnellsten, ob es funktioniert?

Greif auf eine Freigabe über die IP-Adresse zu und suche im Protokoll nach Ereignis 4020 mit Reason ID 7. Erscheint es, funktioniert das erweiterte Auditing auf diesem Client.

Und was ist mit den NTLMv1-Ereignissen 4024 und 4025?

Die gehören zur Blockade von NTLMv1 für Single Sign-on, nicht zum erweiterten Auditing. Was sie bedeuten, steht in Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen; die zugehörige Steuerung über BlockNtlmv1SSO erklärt BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme.

Hat das Auditing etwas mit Kerberos zu tun?

Indirekt ja: Jede NTLM-Anmeldung in der Domäne ist eine Anmeldung, bei der Kerberos nicht funktioniert hat. Die Reason ID sagt dir, warum. Für die Fehlersuche auf der Kerberos-Seite lohnt der Kompetenzbereich Microsoft Kerberos.

Fazit: Einschalten ist leicht, Nachsehen ist die Arbeit

NTLM-Auditing aktivieren ist in einer halben Stunde erledigt: aktuelle Vorlagen, zwei Gruppenrichtlinienobjekte, „NTLM Enhanced Logging“ für Server und Clients, „Log Enhanced Domain-wide NTLM Logs“ für die Domain Controller, die Restrict-NTLM-Überwachung für die Altsysteme und ein Protokoll, das groß genug ist. Wer es noch schneller will, nimmt das Audit-GPO-Skript.

Die eigentliche Arbeit beginnt danach. Ein Auditing ist erst dann eingeschaltet, wenn du nachgewiesen hast, dass jeder Rechner liefert, der liefern kann, und du weißt, warum der Rest schweigt. Denn der Rechner, den du übersehen hast, meldet sich garantiert. Am Morgen nach der Abschaltung, kurz vor der Monatsabrechnung, mit einem Anrufer, der „es ging doch gestern noch“ sagt.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Nutzung ermitteln: der komplette Leitfaden
› Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen
› Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet