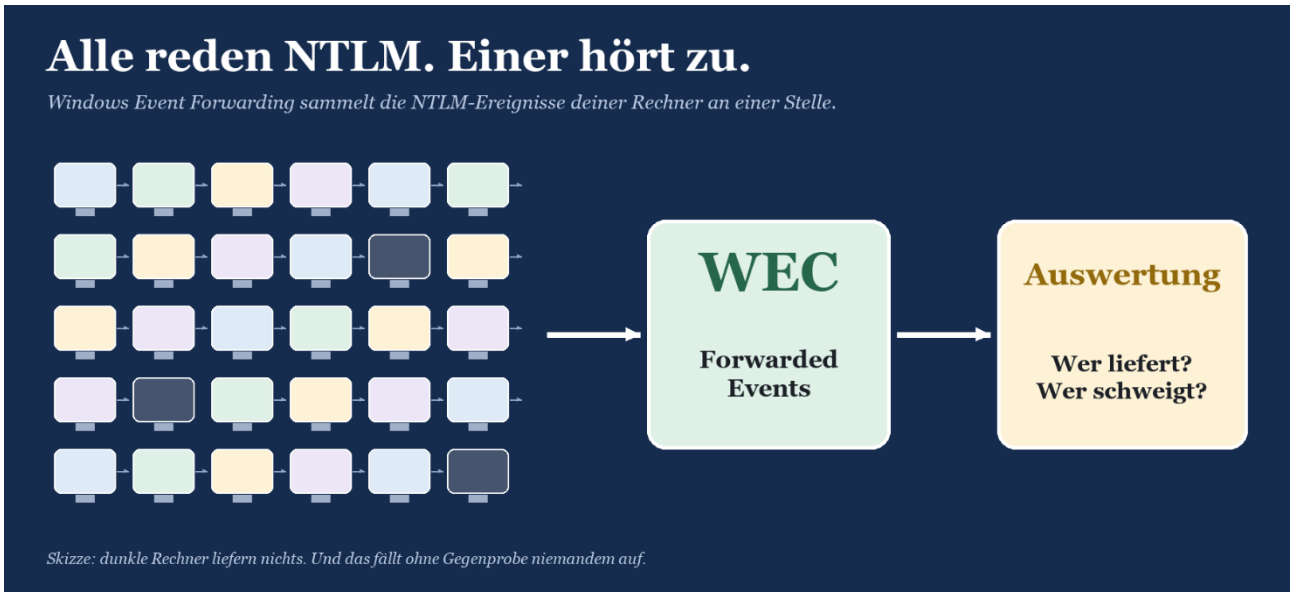
NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding



WISSEN
Was der NTLM Diagnostiker aus deinem Event Collector herausliest und was er kostet.
› NTLM Diagnostiker

BERATUNG
Collector planen, Abonnements aufsetzen, Lücken schließen: mit Erfahrung aus vielen Netzen.
› Beratung zur NTLM-Ablösung

SCHULUNG
WEF, Auditing und Auswertung so lernen, dass dein Team es selbst betreibt.
› Schulung zum NTLM Diagnostiker

Das erweiterte NTLM-Auditing hat ein Problem, das Microsoft nicht lösen wollte: Es schreibt die Wahrheit dorthin, wo sie entsteht. Die Reason ID steht auf dem Client, der NTLM benutzt hat, das eingehende 4022 auf dem Server, das 4031 auf dem Domain Controller. Bei 400 Rechnern sind das 400 kleine Wahrheiten, verstreut über das ganze Haus, und jede einzelne wird irgendwann vom Protokollumlauf still beerdigt. Wer die NTLM-Ablösung ernst nimmt, braucht diese Ereignisse an einer Stelle. Genau dafür gibt es Windows Event Forwarding, und zwar seit Windows Vista, ohne Lizenz und ohne Agent.

Der Zeitdruck ist bekannt: Seit dem Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1 standardmäßig, Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Die Details stehen in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Bis dahin musst du wissen, wer noch NTLM spricht, und vor allem: warum.

Dieser Beitrag ist die Anleitung für windows event forwarding ntlm. Du bekommst das Konzept in fünf Minuten, eine Faustregel für die Zahl der Collector, ein fertiges Abonnement, das nur NTLM-Ereignisse einsammelt, die zwei Stolperfallen, an denen fast jede Einrichtung zuerst scheitert (Leserecht und Protokollgröße), und am Ende die unbequeme Frage, wie du eigentlich merkst, dass ein Rechner nichts schickt.

FAKTEN · Windows Event Forwarding in 30 Sekunden

WEF ist die Weiterleitungsfunktion im Windows-Client, WEC (Windows Event Collector) der Dienst

auf dem Sammelserver. Beides ist in Windows enthalten.

Transport: WinRM (WS-Management), standardmäßig HTTP auf Port 5985. In der Domäne ist die Verbindung trotzdem per Kerberos authentifiziert und verschlüsselt.

Quelleninitiiert (Push): Die Rechner erfahren per Gruppenrichtlinie, wo der Collector steht, holen sich dort das Abonnement und schicken selbst. Das ist die skalierbare Variante.

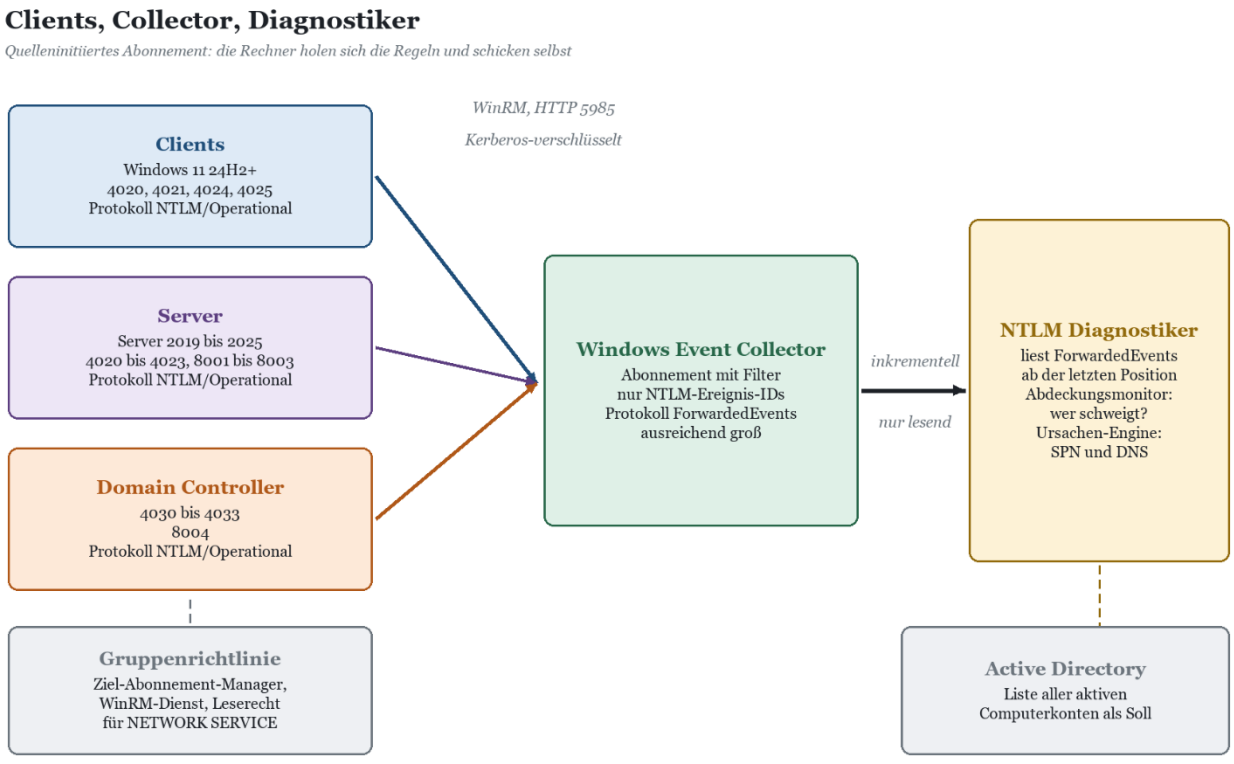
Ziel: Weitergeleitete Ereignisse landen standardmäßig im Protokoll „ForwardedEvents“ (deutsch „Weitergeleitete Ereignisse“) auf dem Collector.

Die NTLM-Ereignisse stehen auf allen Quellen im Protokoll Microsoft-Windows-NTLM/Operational: 4020 bis 4023 auf Clients und Servern, 4024 und 4025 für NTLMv1, 4030 bis 4033 auf DCs, 8001 bis 8004 aus der klassischen Restrict-NTLM-Überwachung.

WEF ist passiv: Es schaltet weder Auditing ein noch vergrößert es Protokolle oder ändert Rechte. Das musst du selbst erledigen.

WEF und WEC in fünf Minuten: wer schickt, wer sammelt

Event Forwarding ist eines dieser Windows-Features, die seit fünfzehn Jahren zuverlässig funktionieren und trotzdem von kaum jemandem benutzt werden, weil die Oberfläche so wirkt, als hätte sie ein Praktikant an einem Freitagnachmittag gebaut. Das Prinzip ist simpel: Ein Abonnement auf dem Collector beschreibt, welche Ereignisse er haben möchte. Die Quellen lesen das Abonnement, filtern ihre eigenen Protokolle lokal und schicken nur das, was passt.



Skizze: vereinfachte Architektur, ein Collector, alle Quellen per Gruppenrichtlinie angebunden

Quelleninitiiert oder collectorinitiiert

Es gibt zwei Bauformen, und für NTLM gewinnt fast immer dieselbe. Microsoft beschreibt die quelleninitiierte Variante selbst als die einfachste und am besten skalierende, weil du keine Rechnerlisten pflegen musst. Wer neu in die Domäne kommt und die Gruppenrichtlinie bekommt, ist dabei.

Merkmal	Quelleninitiiert (Push)	Collectorinitiiert (Pull)
Wer baut die Verbindung auf?	die Quelle	der Collector
Rechnerliste	keine, Zugriff über Computergruppen in der Abonnement-ACL	jeder Rechner wird im Abonnement einzeln eingetragen
Konfiguration der Quellen	Gruppenrichtlinie „Ziel-Abonnement-Manager konfigurieren“	Leserecht für das Abfragekonto auf jeder Quelle
Notebooks, VPN, Homeoffice	schicken nach, sobald sie den Collector wieder erreichen	nur erreichbar, wenn der Collector sie gerade findet
Typischer Einsatz	alle Rechner der Domäne	wenige ausgewählte Server, gezielte Beobachtung
Empfehlung für NTLM	ja	nur als Ergänzung

WinRM, Kerberos und ein kleiner Witz am Rande

WEF benutzt WinRM. In der Domäne authentifizieren sich Quelle und Collector gegenseitig per Kerberos, mit NTLM als Rückfallebene. Ja, richtig gelesen: Wer den Collector in der Gruppenrichtlinie per IP-Adresse oder Kurznamen einträgt, erzeugt beim Einsammeln der NTLM-Ereignisse womöglich neue NTLM-Ereignisse. Das ist die Sorte Humor, über die man nur lacht, wenn es im Netz des Nachbarn passiert. Trage deshalb immer den vollqualifizierten Namen ein, also etwa weco1.musterwerk.local. Warum IP-Adressen Kerberos verhindern, erklärt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen; die Grundlagen der Gegenseite findest du im Kompetenzbereich Microsoft Kerberos.

ForwardedEvents: das Sammelbecken

Auf dem Collector landen alle weitergeleiteten Ereignisse im Protokoll ForwardedEvents. Jedes Ereignis behält dabei seinen Ursprungsrechner im Feld „Computer“ der Systemdaten, das ist der vollqualifizierte Name der Quelle. Das klingt banal, ist aber der Schlüssel für alles, was später kommt: Nur so kannst du zählen, wer liefert, und daraus ableiten, wer nicht liefert.

> **TIPP · Englisches Gebietsschema im Abonnement**
>
> Im Abonnement legst du fest, in welcher Sprache der Meldungstext gerendert wird. Mit Locale Language="en-US" heißen die Felder im Text überall gleich, also „Reason ID“, „Target Machine“ und „NTLM Version“, egal ob die Quelle ein deutsches oder englisches Windows ist. Wer später mit PowerShell auswertet, spart sich damit zwei Sätze regulärer Ausdrücke.

Den Collector planen: Anzahl, Größe, Platz

Bevor du irgendetwas klickst, beantworte drei Fragen: Wie viele Collector brauchst du, wie groß wird ForwardedEvents, und wo steht der Server? Die gute Nachricht: Für reine NTLM-Abonnements sind die Antworten deutlich entspannter als für ein volles Sicherheitsmonitoring.

Faustregel: 2.000 bis 4.000 Clients pro Collector

Microsoft nennt für einen stabilen Collector auf gewöhnlicher Hardware rund 3.000 Ereignisse pro Sekunde im Mittel über alle Abonnements. Begrenzend sind Schreibleistung der Platte, die Zahl der gleichzeitigen TCP-Verbindungen und die Größe der Registrierung, in der der Collector für jede Quelle Lesezeichen und Heartbeat speichert. In der Praxis hat sich daraus die Faustregel 2.000 bis 4.000 Clients pro Collector bewährt. Ein reines NTLM-Abonnement liegt meist am oberen Ende, weil es pro Rechner nur einen Bruchteil der Ereignisse eines Sicherheitsprotokolls erzeugt.

Umgebung	Rechner	Empfehlung
Sparfuchs & Partner Steuerberatungs GmbH	60	ein Collector, gern als Zweitrolle eines Verwaltungsservers
Musterwerk GmbH	450	ein eigener Collector
Trendforge Digital GmbH	1.800	ein Collector, zweiter für Ausfallsicherheit sinnvoll
Klinikverbund mit mehreren Häusern	6.000 bis 9.000	zwei bis vier Collector, je Standort oder je Computergruppe ein Abonnement

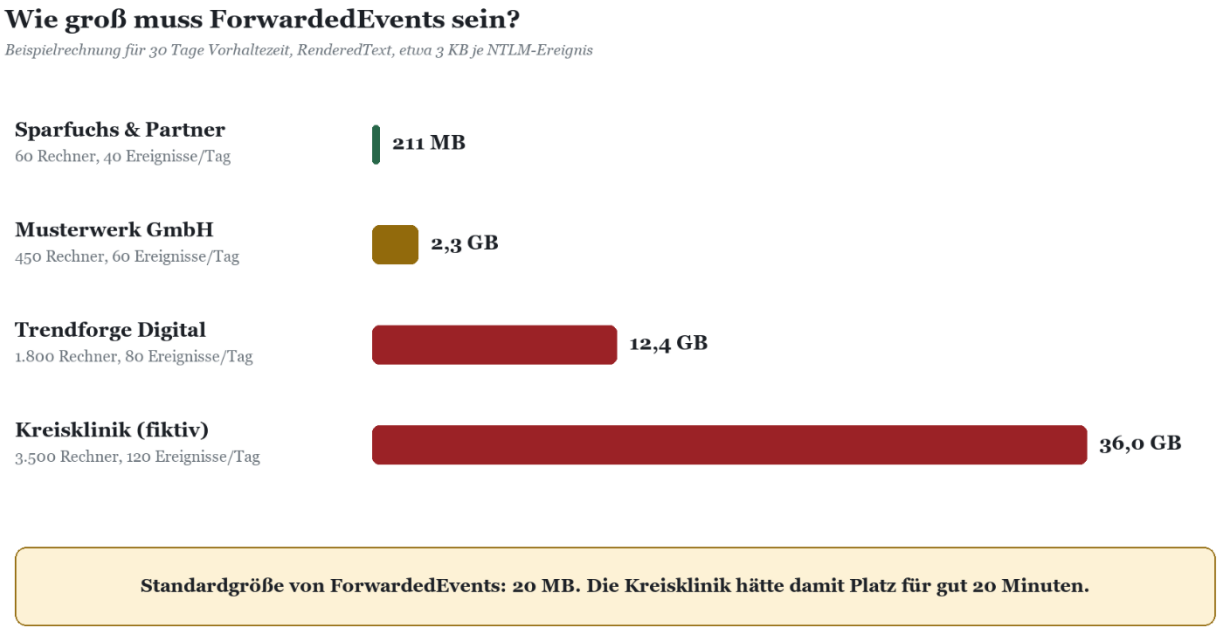
Weitere Grenzwerte aus der Microsoft-Dokumentation, die du kennen solltest: Ab etwa 1.000 Quellen, die sich im Lauf der Zeit an einem Abonnement gemeldet haben, wird die Ereignisanzeige beim Klick auf „Abonnements“ für einige Minuten zäh. Ab 50.000 bleibt nur noch wecutil.exe, ab 100.000 ist die Registrierung nicht mehr lesbar und der Collector ein Fall für die Neuinstallation. Wer Rechner regelmäßig neu aufsetzt, sammelt diese Lebenszeit-Quellen schneller, als man denkt. Nachlesen kannst du das in Use Windows Event Forwarding to help with intrusion detection.

WARNUNG · Kein Collector auf dem Domain Controller

Technisch geht es, praktisch nicht. Ein DC hat genug mit Anmeldungen zu tun, und ein voll laufendes ForwardedEvents auf der Systempartition des DC ist eine Störung, die du dir selbst gebaut hast. Nimm einen Mitgliedsserver mit eigener Datenplatte für die Protokolle.

Größe von ForwardedEvents

Hier scheitern die meisten Einrichtungen, ohne es zu merken. ForwardedEvents ist standardmäßig 20 MB groß und überschreibt bei Bedarf die ältesten Einträge. Das ist ungefähr so, als würdest du die Patientenakten einer Klinik in einer Schuhschachtel ablegen und dich wundern, warum die Befunde vom Dienstag fehlen. Rechne grob: Rechner mal NTLM-Ereignisse pro Tag mal Ereignisgröße mal gewünschte Vorhaltezeit in Tagen.



Skizze: Zahlen fiktiver Beispiele; miss dein eigenes Volumen in der ersten Woche

Die Ereignisgröße hängt am Format. Im Standardformat „RenderedText“ schickt die Quelle den Meldungstext mit, was das Volumen laut Microsoft etwa verdoppelt bis verdreifacht. Das Format

„Events“ überträgt nur das XML und ist deutlich kompakter, dann rendert aber der Collector den Text selbst und braucht dafür die Ereignisdefinitionen der neuen NTLM-Ereignisse. Für NTLM empfehle ich RenderedText, solange der Collector nicht selbst auf Windows Server 2025 oder einem aktuell gepatchten Server 2022 läuft; der Platz ist billiger als ein leeres Meldungsfeld.

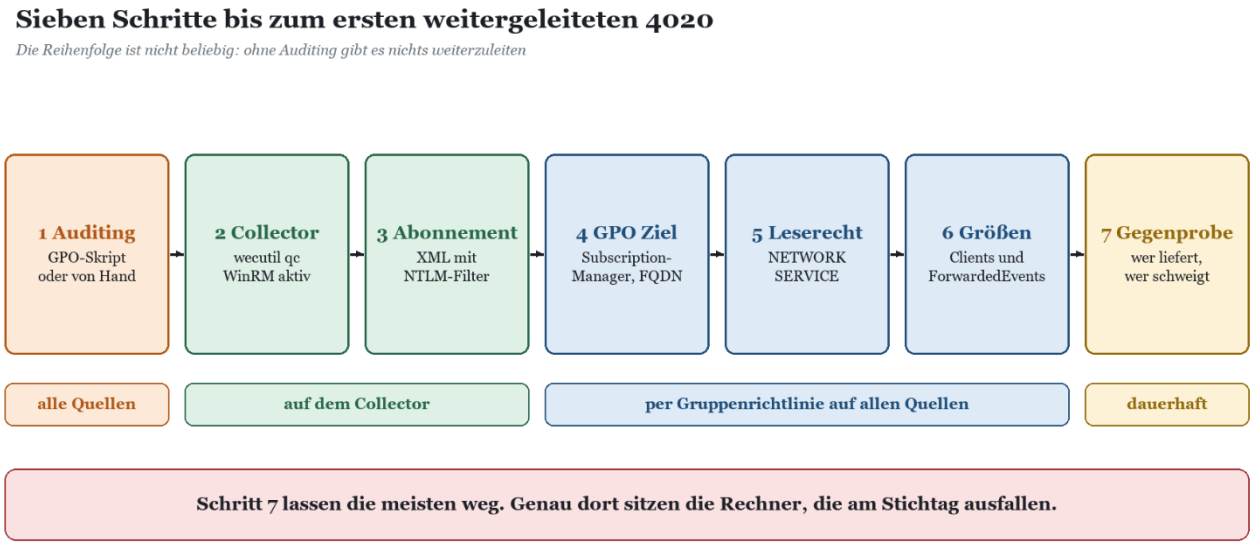
```
# Auf dem Collector: ForwardedEvents auf 8 GB vergrößern und eigenen Pfad setzen
wevtutil sl ForwardedEvents /ms:8589934592
wevtutil sl ForwardedEvents /lfn:D:\Logs\ForwardedEvents.evtx

# Kontrolle
wevtutil gl ForwardedEvents
```

Und denk an die andere Seite: Das lokale Protokoll Microsoft-Windows-NTLM/Operational jeder Quelle ist der Puffer für die Zeit, in der der Collector nicht erreichbar ist. Läuft es über, sind die Ereignisse weg, und der Collector erfährt davon nichts. Microsoft sagt das ausdrücklich: Es gibt weder eine Meldung noch eine Markierung für die Lücke.

Schritt für Schritt: ein Abonnement nur für NTLM

Jetzt wird es handfest. Die folgende Reihenfolge funktioniert in Domänen von zehn bis zehntausend Rechnern. Rechne für eine saubere Einrichtung mit einem halben Tag, für die Fehlersuche bei den ersten zwanzig Rechnern, die nicht wollen, mit einem weiteren.



Skizze: Ablauf der Einrichtung, Details in den Abschnitten unten

Schritt 1: Auditing einschalten

WEF leitet nur weiter, was da ist. Ohne aktiviertes NTLM-Auditing bleibt ForwardedEvents leer, und du hältst die Stille für ein gutes Zeichen. Die erweiterten Ereignisse 4020 bis 4023 und 4030 bis 4033 entstehen auf Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026; die Einzelheiten stehen in Overview of NTLM auditing enhancements in Windows 11, version 24H2 and Windows Server 2025. Die klassischen Ereignisse 8001 bis 8004 der Restrict-NTLM-Überwachung liefern auch ältere Systeme. Wie du alles per Gruppenrichtlinie einschaltest, zeigt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt. Wenn du dir das Klicken sparen willst: Das NTLM-Audit-GPO-Skript legt die nötigen Audit-Einstellungen als fertige Gruppenrichtlinie an.

Schritt 2: den Collector vorbereiten

Auf dem Sammelserver aktivierst du WinRM und den Dienst Windows-Ereignissammlung. Beides erledigen zwei Befehle in einer Eingabeaufforderung mit Administratorrechten.

```
winrm quickconfig -q
wecutil qc /q

# Prüfen, ob der Collector auf 5985 lauscht
winrm enumerate winrm/config/listener
```

Schritt 3: das Abonnement mit NTLM-Filter anlegen

Die Ereignisanzeige kann Abonnements anlegen, aber das Abonnement als XML-Datei ist nachvollziehbar, versionierbar und in fünf Sekunden auf einem zweiten Collector wiederholt. Der Filter holt ausschließlich die NTLM-Ereignis-IDs aus Microsoft-Windows-NTLM/Operational, nichts sonst. Speichere die Datei als ntlm-abo.xml und lege das Abonnement mit wecutil cs an.

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
  <SubscriptionId>NTLM-Audit</SubscriptionId>
  <SubscriptionType>SourceInitiated</SubscriptionType>
  <Description>NTLM-Ereignisse 4020-4025, 4030-4033, 8001-8004</Description>
  <Enabled>true</Enabled>
  <Uri>http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
  <ConfigurationMode>Normal</ConfigurationMode>
  <Query><![CDATA[
    <QueryList>
      <Query Id="0" Path="Microsoft-Windows-NTLM/Operational">
        <Select Path="Microsoft-Windows-NTLM/Operational">*[System[
          (EventID &gt;= 4020 and EventID &lt;= 4025) or
          (EventID &gt;= 4030 and EventID &lt;= 4033) or
          (EventID &gt;= 8001 and EventID &lt;= 8004)]]</Select>
      </Query>
    </QueryList>]]></Query>
  <ReadExistingEvents>true</ReadExistingEvents>
  <TransportName>HTTP</TransportName>
  <ContentFormat>RenderedText</ContentFormat>
  <Locale Language="en-US"/>
  <LogFile>ForwardedEvents</LogFile>
  <AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>

<AllowedSourceDomainComputers>O:NSG:BAD:P(A;;GA;;;DC)(A;;GA;;;DD)S:</AllowedSourceDomainComputers
>
</Subscription>

wecutil cs ntlm-abo.xml
wecutil gs NTLM-Audit
```

Drei Zeilen verdienen einen zweiten Blick. **ReadExistingEvents** sorgt dafür, dass die Quellen auch die Ereignisse schicken, die schon vor dem Abonnement im Protokoll standen; standardmäßig werden nur neue weitergeleitet. **AllowedSourceDomainComputers** erlaubt Domänencomputer (DC) und Domänencontroller (DD). Die Domain Controller stehen nämlich nicht in der Gruppe Domänencomputer, und wer DD vergisst, wundert sich drei Wochen später, warum kein einziges 4031 ankommt. Wenn du nur einen Teil der Rechner anbinden willst, nimmst du statt DC und DD die SID einer eigenen Computergruppe. **ConfigurationMode Normal** reicht für NTLM völlig; Minimize Latency mit 30 Sekunden Verzögerung brauchst du für Alarme, nicht für eine Bestandsaufnahme.

WICHTIG · Filter schmal halten

Die Versuchung ist groß, gleich noch das Sicherheitsprotokoll mitzunehmen, wo man schon mal dabei ist. Lass es. Ein schmales Abonnement hält ForwardedEvents klein, die Auswertung schnell

und die Diskussion mit dem Datenschutz kurz. Ein Sicherheitsmonitoring ist ein eigenes Projekt mit eigenem Collector.

Schritt 4: den Quellen sagen, wo der Collector steht

In einer Gruppenrichtlinie, die auf alle Rechner und die Domain Controller wirkt, öffnest du Computerkonfiguration, Richtlinien, Administrative Vorlagen, Windows-Komponenten, Ereignisweiterleitung und aktivierst „Ziel-Abonnement-Manager konfigurieren“. Als Wert trägst du die Adresse des Collectors ein:

```
Server=http://wec01.musterwerk.local:5985/wsman/SubscriptionManager/WEC,Refresh=60
```

Refresh gibt in Sekunden an, wie oft die Quelle nach geänderten Abonnements fragt. Für die Einführung sind 60 Sekunden angenehm, im Dauerbetrieb reichen größere Werte. Hast du zwei Collector, trägst du zwei Zeilen ein; die Quellen schicken dann an beide, sofern sie die Berechtigung haben.

Schritt 5: WinRM-Dienst und Leserecht für NETWORK SERVICE

Auf den Quellen muss der Dienst Windows-Remoteverwaltung (WS-Verwaltung) laufen. Das stellst du in derselben Gruppenrichtlinie unter Computerkonfiguration, Richtlinien, Windows-Einstellungen, Sicherheitseinstellungen, Systemdienste auf „Automatisch“. Einen WinRM-Listener auf den Clients brauchst du für das quelleninitiierte Abonnement nicht, denn die Clients bauen die Verbindung selbst auf.

Und jetzt der Klassiker. Der Weiterleitungsdienst läuft auf der Quelle als NETWORK SERVICE, und NETWORK SERVICE muss das Protokoll lesen dürfen. Microsoft empfiehlt für die Mindestkonfiguration, NETWORK SERVICE in die lokale Gruppe Ereignisprotokollleser (Event Log Readers) aufzunehmen. Das geht per Gruppenrichtlinie über „Eingeschränkte Gruppen“ oder Gruppenrichtlinien-Einstellungen für lokale Benutzer und Gruppen. Ob das Protokoll Microsoft-Windows-NTLM/Operational diese Gruppe in seiner Zugriffsliste hat, prüfst du an einem Referenzrechner:

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

# In der Ausgabe auf die Zeile channelAccess achten:
#   (A;;0x1;;;S-1-5-32-573)  = Leserecht für Event Log Readers
#   (A;;0x1;;;NS)            = Leserecht direkt für NETWORK SERVICE

# Fehlt beides: bestehende Zeichenfolge übernehmen und ergänzen, zum Beispiel
wevtutil sl Microsoft-Windows-NTLM/Operational /ca:"<bisheriger Wert>(A;;0x1;;;NS)"
```

WARNUNG · /ca ersetzt, es ergänzt nicht

wevtutil sl /ca schreibt die komplette Zugriffsliste neu. Wer nur (A;;0x1;;;NS) übergibt, nimmt allen anderen das Recht weg, auch den Administratoren. Kopiere den bisherigen Wert aus wevtutil gl, hänge den neuen Eintrag an und verteile das Ergebnis per geplanter Aufgabe oder Startskript. Und teste es an drei Rechnern, bevor du es auf dreihundert loslässt.

Merkst du ein fehlendes Leserecht, dann im Protokoll Microsoft-Windows-Eventlog-ForwardingPlugin/Operational auf der Quelle. Dort protokolliert der Weiterleitungsdienst Erfolg, Warnungen und Fehler. Der Benutzer bekommt davon nichts mit, keine Meldung, kein Fenster. Das ist schön für den Benutzer und schlecht für dich, weil es eben auch niemand meldet.

Schritt 6: lokale Protokolle vergrößern

Das lokale NTLM-Protokoll ist der Puffer für Notebooks, die eine Woche auf Dienstreise waren. Vergrößere es per geplanter Aufgabe in der Gruppenrichtlinie, so wie Microsoft es für andere Kanäle beschreibt:

```
%SystemRoot%\System32\wevtutil.exe sl Microsoft-Windows-NTLM/Operational /ms:104857600
```

100 MB sind für Clients ein vernünftiger Startwert, für Dateiserver und Domain Controller darf es mehr sein. Auf den DCs entstehen 4030 bis 4033 und 8004 für die ganze Domäne; die Besonderheiten dort beschreibt NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

Schritt 7: die Gegenprobe

Nach dem nächsten Gruppenrichtlinienabgleich melden sich die ersten Quellen. Auf dem Collector zeigt wecutil gr den Laufzeitstatus des Abonnements mit jeder Quelle, ihrem Zustand, dem letzten Fehler und dem letzten Heartbeat. Eine Quelle, die nichts zu senden hat, meldet sich trotzdem regelmäßig mit einem Heartbeat. Das ist wertvoll, denn so unterscheidest du „hat kein NTLM“ von „ist gar nicht angebunden“.

```
wecutil gr NTLM-Audit

# Stichprobe: Was ist in der letzten Stunde angekommen?
Get-WinEvent -FilterHashtable @{ LogName='ForwardedEvents'; StartTime=(Get-Date).AddHours(-1) }
|
  Group-Object MachineName, Id | Sort-Object Count -Descending | Select-Object Count, Name -
First 20
```

AUS DER PRAXIS · Musterwerk GmbH: der Collector, der alles hatte

Bei der Musterwerk GmbH lief WEF seit Wochen, ForwardedEvents war gut gefüllt, alle waren zufrieden. Dann der Abgleich mit dem Active Directory: 450 aktive Computerkonten, Ereignisse von 381. Von den 69 Schweigern standen 31 in einer OU, auf die die WEF-Richtlinie nicht wirkte, 17 waren Windows-10-Rechner, die 4020 gar nicht schreiben können, 12 hatten das Leserecht nicht, weil das Startskript an einer Firewallregel scheiterte, und 9 waren Notebooks, die seit dem Sommer niemand mehr gesehen hatte. Ohne Gegenprobe hätte die IT-Leitung einen Bericht über 381 Rechner bekommen und ihn für 450 gehalten.

Auswerten und Lücken finden: wer liefert, wer schweigt

Ein gefüllter Collector ist ein guter Anfang, aber noch keine Antwort. Zwei Fragen musst du regelmäßig beantworten: Was steht in den Ereignissen, und wer fehlt? Die erste Frage behandeln die Beiträge zu den einzelnen Ereignissen, also Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen, Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern und Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen. Die zweite ist das eigentliche Thema dieses Abschnitts.

Mit PowerShell: Soll gegen Ist

Das Soll liefert das Active Directory, das Ist der Collector. Das folgende Skript vergleicht beides. Es nimmt nur Computerkonten, die sich in den letzten 14 Tagen angemeldet haben, damit Leichen im AD nicht als Lücke zählen.

```
Import-Module ActiveDirectory
$seit = (Get-Date).AddDays(-14)

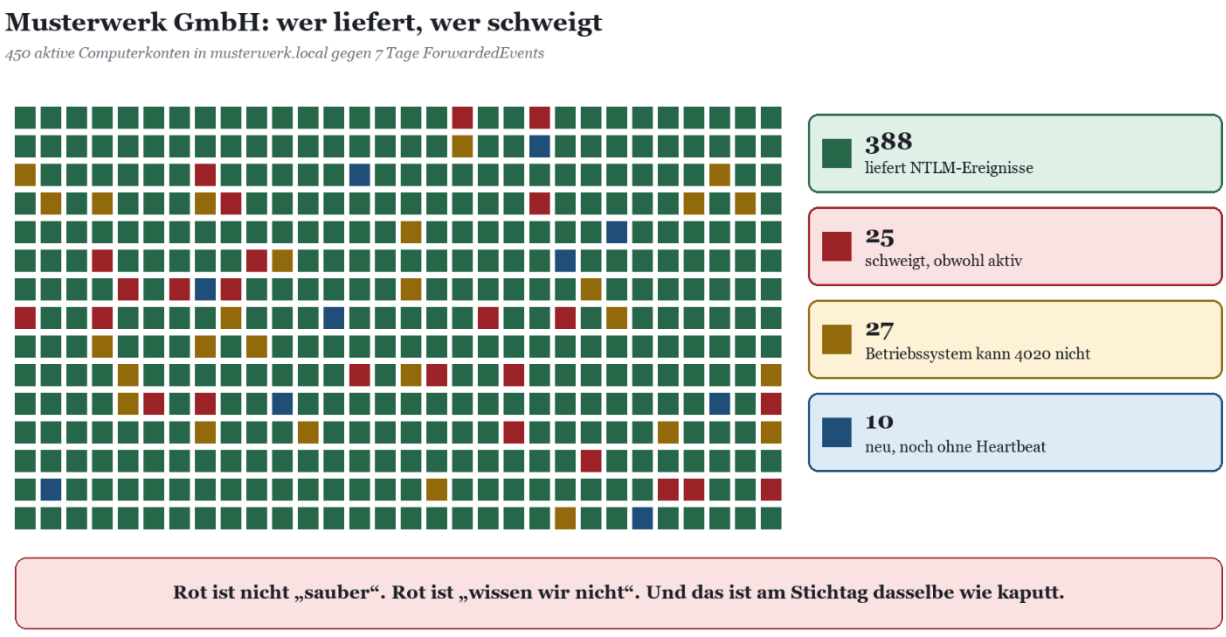
# Ist: wer hat in 14 Tagen etwas geschickt?
```

```
$liefern = Get-WinEvent -FilterHashtable @{ LogName='ForwardedEvents'; StartTime=$seit } |
  Select-Object -ExpandProperty MachineName -Unique

# Soll: aktive Computerkonten
$soll = Get-ADComputer -Filter 'Enabled -eq $true' -Properties LastLogonTimestamp,
OperatingSystem,
  OperatingSystemVersion | Where-Object { [DateTime]::FromFileTime($_.LastLogonTimestamp) -gt
$seit }

# Schweiger mit Betriebssystem, damit du siehst, wer gar nicht liefern kann
$soll | Where-Object { $liefern -notcontains $_.DNSHostName } |
  Select-Object Name, OperatingSystem, OperatingSystemVersion |
  Sort-Object OperatingSystem | Export-Csv .\schweiger.csv -NoTypeInformation -Encoding UTF8
```

Das funktioniert, mit drei Haken. Erstens liest Get-WinEvent bei jedem Lauf das ganze Zeitfenster von vorn; bei ein paar Millionen Ereignissen kannst du dir dabei einen Kaffee kochen, ihn trinken und die Tasse spülen. Zweitens bedeutet „hat nichts geschickt“ nicht automatisch „ist kaputt“: Ein Rechner ohne NTLM-Nutzung schickt eben nichts. Die saubere Unterscheidung kommt erst aus dem Heartbeat in wecutil gr, und den musst du für jede Quelle einzeln aus der Ausgabe fischen. Drittens weiß das Skript nicht, welche Windows-Version welche Ereignisse überhaupt schreiben kann. Ein Windows-10-Rechner liefert keine 4020, so gut du ihn auch anbindest.



Skizze: fiktive Verteilung, jedes Kästchen ein Computerkonto

Was WEF grundsätzlich nicht sieht

Event Forwarding sammelt Windows-Ereignisse von Windows-Rechnern. Drucker, Scanner, NAS-Systeme, Medizingeräte und Linux-Server haben kein NTLM/Operational-Protokoll. Ihre NTLM-Anmeldungen siehst du nur indirekt auf dem Zielserver als 4022 oder auf dem DC, und ohne Reason ID. Wie du diesen Teil abdeckst, steht in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

Lücke	Woran du sie erkennst	Was hilft
Richtlinie greift nicht	kein Heartbeat, kein Eintrag in wecutil gr	OU-Verknüpfung und Sicherheitsfilter prüfen, gpresult auf der Quelle
Leserecht fehlt	Quelle verbunden, aber keine NTLM-Ereignisse; Fehler im ForwardingPlugin-	Event Log Readers oder channelAccess

	Protokoll	prüfen
Betriebssystem zu alt	nur 8001 bis 8004, nie 4020 bis 4023	Update oder bewusst als Lücke führen
Auditing aus	Heartbeat ja, Ereignisse nie	Audit-Richtlinie prüfen
Puffer übergelaufen	Lücken im Zeitverlauf einer Quelle	lokales Protokoll vergrößern
Gerät ohne Windows	taucht nur als Ziel in 4022 oder auf dem DC auf	Mitschnitt, Gerätekonfiguration, Herstellerangaben

Wo es mühsam wird

Bis hierhin ist alles mit Bordmitteln lösbar, und bei 60 Rechnern einer Steuerberatung ist das auch völlig in Ordnung. Bei 1.800 Rechnern der Trendforge Digital GmbH sieht die Woche anders aus: Montag Skript laufen lassen, Dienstag die Schweiger nach Betriebssystem sortieren, Mittwoch die Reason-IDs aus den Meldungstexten ziehen, Donnerstag SPN und DNS für die Top-Ziele prüfen, Freitag die Excel-Tabelle für die IT-Leitung bauen. Und am nächsten Montag fängt alles von vorn an, weil das Skript nicht weiß, was es letzte Woche schon gelesen hat. Einen ehrlichen Vergleich, wann Skripte genügen und wann nicht, findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Den Collector lesen, statt ihn abzuarbeiten

Ereignisquelle Windows Event Collector: Der Diagnostiker liest ForwardedEvents inkrementell, also ab der Stelle, an der er zuletzt aufgehört hat. Alternativ liest er direkt vom Domain Controller oder fragt einzelne Rechner direkt ab, etwa die, die noch nicht angebunden sind.

Abdeckungsmonitor und OS-Landkarte: Sie stellen die aktiven Computerkonten den liefernden Quellen gegenüber und zeigen, welche Maschinen schweigen und welche wegen ihrer Windows-Version gar keine erweiterten Ereignisse schreiben können. Die Readiness-Ampel fasst das Lagebild zusammen.

Ursache statt Ereignis: Die Ursachen-Engine verbindet Reason ID und Ziel und prüft SPN und DNS. Die NTLMv1-Hitliste zeigt, wer noch v1 spricht, Kommunikationsmatrix und Konten-Sicht zeigen, wer mit wem und mit welchem Konto. Sicherheitsflaggen markieren Auffälliges. Für Geräte ohne Ereignisprotokoll gibt es den Wireshark-Import.

Entscheiden: Die Abschalt-Simulation zeigt, wen eine Abschaltung treffen würde. Ergebnis als Word-Bericht für die IT-Leitung, als Excel- oder CSV-Export für die Tickets.

Ausschließlich lesend: Der Diagnostiker ändert weder Abonnements noch Richtlinien, Protokolle oder Konten. Er liest, was dein Collector ohnehin hat.

Editionen: Express ist kostenlos und liefert den Fünf-Minuten-Befund. Die Vollversion testest du 7 Tage, lizenziert wird pro aktivem Computerkonto. Anwendungskatalog, Ausnahmelisten- und Skript-Generator, Phasenplan, Kerberos-Gegencheck und Verlauf sind geplant.

Der Collector, den du in diesem Beitrag aufgebaut hast, ist damit keine Sackgasse, sondern genau die Datenquelle, die der NTLM Diagnostiker erwartet. Du richtest WEF einmal sauber ein, der Diagnostiker liest regelmäßig nach und sagt dir, welche Rechner fehlen. Wenn du Unterstützung beim Aufbau der Collector, bei Abonnements für mehrere Standorte oder bei der Bewertung der Lücken brauchst, hilft dir die Beratung zur NTLM-Ablösung. Systemhäuser, die das bei vielen Kunden gleich machen wollen, finden das Vorgehen in NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

HINWEIS · Benutzernamen im Collector

NTLM-Ereignisse enthalten Konto- und Rechnernamen. Ein zentraler Collector macht daraus eine Sammlung, die Datenschutz und Betriebsrat interessieren wird, und zwar besser vorher als nachher. Zweckbindung, Vorhaltezeit und Zugriffsrechte auf den Collector gehören in die Dokumentation. Worauf es ankommt, steht in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

FAQ zu Windows Event Forwarding für NTLM

Brauche ich für WEF eine zusätzliche Lizenz?

Nein. Weiterleitung und Collector sind Bestandteil von Windows. Du brauchst nur einen Server für die Collector-Rolle, idealerweise einen Mitgliedsserver mit eigener Datenplatte.

Wie viele Clients schafft ein Collector?

Als Faustregel 2.000 bis 4.000 Clients pro Collector. Microsoft nennt als Richtwert rund 3.000 Ereignisse pro Sekunde für einen stabilen Collector. Ein reines NTLM-Abonnement erzeugt deutlich weniger Last als ein volles Sicherheitsmonitoring.

Warum kommen keine Ereignisse von den Domain Controllern an?

Meist fehlt DD in der Zugriffsliste des Abonnements, weil Domain Controller nicht Mitglied der Gruppe Domänencomputer sind. Prüfe außerdem, ob die WEF-Gruppenrichtlinie auch auf die OU Domain Controllers wirkt.

Warum ist ForwardedEvents leer, obwohl die Quellen in wecutil gr stehen?

Die drei häufigsten Gründe: Das NTLM-Auditing ist nicht aktiv, NETWORK SERVICE darf Microsoft-Windows-NTLM/Operational nicht lesen, oder es gibt schlicht noch kein NTLM auf diesen Rechnern. Das Protokoll Eventlog-ForwardingPlugin/Operational auf der Quelle verrät, welcher Fall vorliegt.

Kann ich die Ereignisse 4024 und 4025 im selben Abonnement sammeln?

Ja. Sie stehen ebenfalls in Microsoft-Windows-NTLM/Operational, der Filter oben schließt sie mit ein. Was sie bedeuten, erklärt Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen.

HTTP auf Port 5985, ist das nicht unsicher?

In der Domäne wird die Verbindung per Kerberos authentifiziert und verschlüsselt, auch bei HTTP. HTTPS brauchst du nur, wenn Quellen ohne Domänenmitgliedschaft per Zertifikat angebunden werden.

Leitet WEF auch alte Ereignisse weiter?

Nur, wenn im Abonnement ReadExistingEvents auf true steht. Standardmäßig schicken die Quellen nur Ereignisse, die nach dem Empfang des Abonnements entstanden sind.

Ändert der NTLM Diagnostiker etwas an meinem Collector?

Nein. Er arbeitet ausschließlich lesend und liest ForwardedEvents inkrementell. Abonnements, Richtlinien und Protokolle bleiben, wie du sie eingerichtet hast.

Was mache ich mit Rechnern, die gar nicht angebunden werden können?

Notiere sie als bewusste Lücke, frage sie bei Bedarf direkt ab und prüfe ihre Spuren auf Zielservern und Domain Controllern. Den Gesamtüberblick über alle Quellen gibt NTLM-Nutzung ermitteln: der komplette Leitfaden.

Fazit: Ein Collector ist schnell gebaut, die Gegenprobe macht ihn wertvoll

Windows Event Forwarding ist das unterschätzte Werkzeug der NTLM-Ablösung. Es kostet nichts, ist in einem halben Tag eingerichtet und holt die Ereignisse dorthin, wo du sie auswerten kannst. Die Fallstricke sind überschaubar und gut bekannt: quelleninitiiertes Abonnement mit schmalem Filter, Collector per FQDN, Domain Controller in der Zugriffsliste, Leserecht für NETWORK SERVICE, ForwardedEvents deutlich größer als 20 MB und lokale Protokolle als Puffer.

Der wichtigste Schritt ist der, den die meisten weglassen: die Frage, wer nicht liefert. Ein Collector voller Ereignisse beweist nur, dass einige Rechner reden. Die anderen schweigen, und Schweigen ist bei der NTLM-Ablösung keine Zustimmung, sondern ein Ticket, das am Stichtag von allein aufgeht. Wer die Gegenprobe jede Woche macht, mit Skript oder mit dem Diagnostiker, weiß vorher, wer ausfallen wird. Alle anderen erfahren es vom Helpdesk.

WEITERLESEN · Weiter in dieser Serie

› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Audit-GPO-Skript
› 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-Nutzung ermitteln: der komplette Leitfaden
› NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker