Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll



WISSEN
Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er dir zeigt.
› **NTLM Diagnostiker**

BERATUNG
Vom 4776-Ereignisberg zur belastbaren Liste der Verursacher: mit Begleitung.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Sicherheitsprotokoll und NTLM-Ereignisse richtig lesen: für dein ganzes Team.
› **Schulung zum NTLM Diagnostiker**

Ereignis 4776 ist das Klemmbrett des Türstehers. Jedes Mal, wenn ein Domain Controller ein Kennwort per NTLM prüft, macht er einen Strich: Konto, Herkunftsrechner, Ergebnis. Fertig. Wohin der Gast eigentlich wollte, welches Programm ihn geschickt hat und warum er nicht durch die Kerberos-Drehtür gegangen ist, notiert der Türsteher nicht. Er ist ja nicht die Polizei.

Trotzdem ist ereignis 4776 für viele Administratorinnen und Administratoren der erste Kontakt mit dem NTLM-Problem. Es steht im Sicherheitsprotokoll, das ohnehin jeder sammelt, es existiert seit Windows Server 2008, und es taucht in jedem SIEM-Dashboard auf, meist als rote Kurve mit dem Titel „NTLM-Anmeldungen“. Und genau diese Kurve wird gerade wichtig: Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 Single Sign-on mit NTLMv1 standardmäßig, und mit der nächsten Windows-Server-Version ist NTLM ab Werk abgeschaltet. Wer bis dahin nicht weiß, wer die Kurve füllt, erfährt es am Montagmorgen vom Helpdesk.

In diesem Beitrag gehen wir 4776 Feld für Feld durch, sortieren die Fehlercodes, richten die Überwachungsrichtlinie „Überprüfung der Anmeldeinformationen“ ein, sammeln die Ereignisse mit Get-WinEvent von allen Domain Controllern ein und klären, warum dir 4776 die Ursache niemals liefern wird. Wie sich das Ereignis in den großen Zusammenhang der NTLM-Bestandsaufnahme einfügt, steht in NTLM-Nutzung ermitteln, der Zeitplan der Abschaltung in Der Fahrplan zur NTLM-Abschaltung.

FAKTEN · Ereignis 4776 in 30 Sekunden

Titel: „Der Computer hat versucht, die Anmeldeinformationen für ein Konto zu überprüfen.“

(englisch „The computer attempted to validate the credentials for an account.“)

Protokoll: Sicherheit, Anbieter Microsoft-Windows-Security-Auditing, Erfolg und Fehler.

Unterkategorie: „Überprüfung der Anmeldeinformationen“ in der Kategorie Kontoanmeldung.

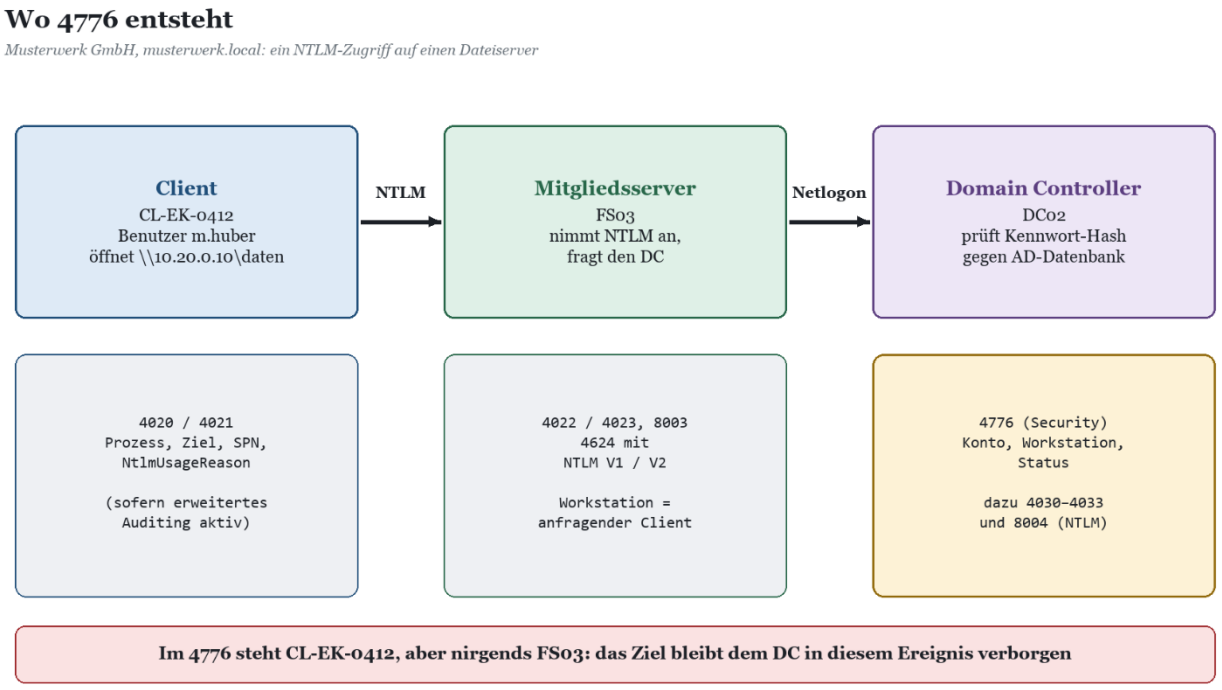
Entsteht nur auf dem Rechner, der für das Konto zuständig ist: bei Domänenkonten auf dem Domain Controller, bei lokalen Konten auf dem Rechner selbst.

Nur NTLM. Kerberos-Anmeldungen landen in 4768, 4769 und 4771, nicht in 4776.

Datenfelder: PackageName, TargetUserName, Workstation, Status. Kein Zielserver, kein Prozess.

Was in Ereignis 4776 steht und was nicht

Microsoft beschreibt 4776 knapp: Das Ereignis entsteht bei jeder Überprüfung von Anmeldeinformationen mit NTLM, und zwar nur auf dem Computer, der für diese Anmeldeinformationen maßgeblich ist. Für ein Domänenkonto ist das ein Domain Controller. Greift also ein Client per NTLM auf einen Dateiserver zu, nimmt der Dateiserver die NTLM-Antwort entgegen, reicht sie per Netlogon an einen DC weiter, und dort entsteht 4776. Auf dem Dateiserver selbst steht dann ein 4624 mit dem Authentifizierungspaket NTLM, das dir sogar die Version verrät; wie du das ausliest, zeigt Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen.



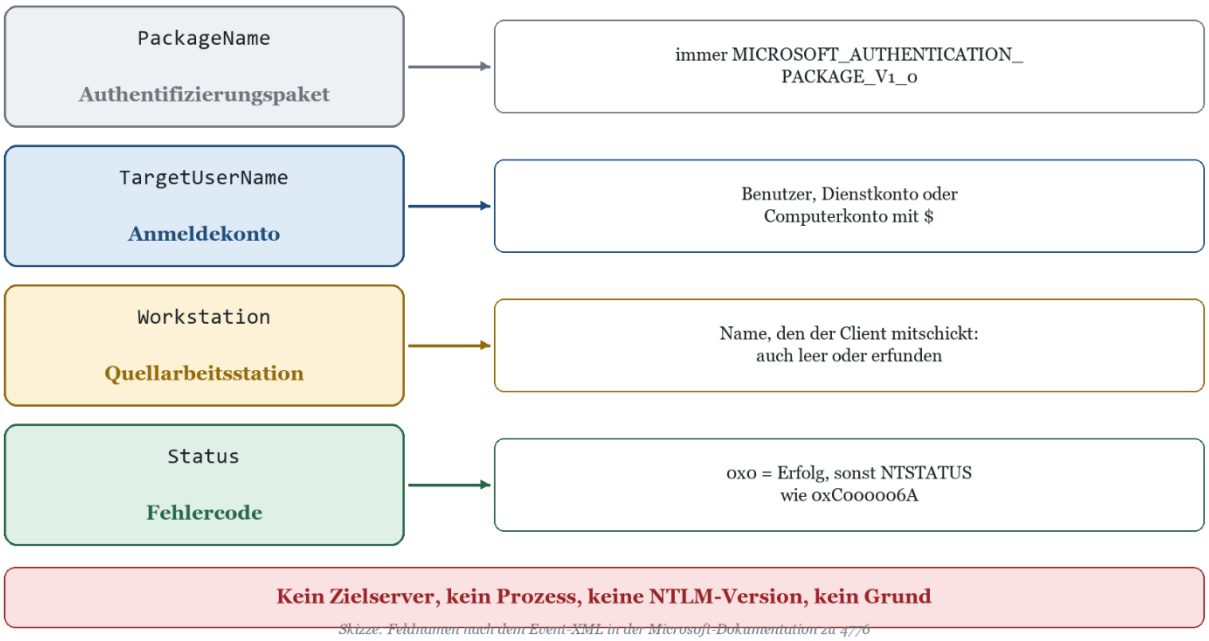
Skizze: Namen fiktiv; 4776 entsteht nur auf dem Rechner, der das Konto verwaltet

Die vier Felder

Im Meldungstext heißen die Felder Authentifizierungspaket, Anmeldekonto, Quellarbeitsstation und Fehlercode. Im Event-XML, und nur das zählt für jede Auswertung, heißen sie PackageName, TargetUserName, Workstation und Status. Wer mit Textsuche im Meldungstext arbeitet, hat spätestens beim ersten englischen DC neben dem deutschen ein Problem, und bei weitergeleiteten Ereignissen ist der Meldungstext manchmal schlicht leer.

Anatomie eines 4776-Ereignisses

Vier Datenfelder, mehr nicht. Die Kunst liegt im Zusammenzählen.



Skizze. Feldnamen nach dem Event-XML in der Microsoft-Dokumentation zu 4776

Feld (XML)	Anzeige im Meldungstext	Was es dir sagt	Fallstricke
PackageName	Authentifizierungspaket	Laut Microsoft immer MICROSOFT_AUTHENTICATION_PACKAGE_V1_0, also MSV1_0, der NTLM-Anbieter.	Sagt nichts über NTLMv1 oder NTLMv2.
TargetUserName	Anmeldekonto	Das geprüfte Konto: Benutzer, Dienstkonto oder Computerkonto (mit $ am Ende).	Ohne Domänenteil; bei Vertrauensstellungen genau hinsehen.
Workstation	Quellarbeitsstation	Name des Rechners, von dem die Anmeldung ausging.	Vom Client mitgeschickt, nicht geprüft: kann leer, veraltet oder frei erfunden sein.
Status	Fehlercode	0x0 bei Erfolg, sonst ein NTSTATUS-Code.	Fehlgeschlagene Anmeldungen haben oft eine Kette von Folgeereignissen.

WARNUNG · Das Ziel fehlt, und zwar absichtlich

Microsoft schreibt es selbst in die Dokumentation: Meldet sich ein Benutzer von CLIENT-1 an SERVER-1 an, steht im 4776 CLIENT-1 als Quellarbeitsstation. SERVER-1 taucht nicht auf. Du siehst also, dass m.huber sich von CL-EK-0412 per NTLM angemeldet hat, aber nicht, ob beim Dateiserver, beim Drucker oder bei der Zeiterfassung. Für die NTLM-Ablösung ist das die halbe Miete, und zwar die falsche Hälfte.

Was 4776 außerdem auslöst

Ein paar Eigenheiten, die dir beim Zählen begegnen werden:

- **Bildschirm entsperren:** Laut Microsoft entsteht 4776 auch beim Entsperren einer Arbeitsstation. Ein Teil deiner Kurve ist also Kaffeepausen-Rauschen und kein Netzwerkzugriff.
- **Lokale Konten:** Prüft ein Mitgliedsserver ein lokales Konto, steht 4776 im Sicherheitsprotokoll dieses Servers, nicht auf dem DC. Für lokale Konten empfiehlt Microsoft ohnehin 4624.
- **Lokale Anmeldung am DC:** Meldet sich ein Domänenkonto direkt am Domain Controller an, entsteht kein 4776.
- **Computerkonten:** Konten mit $ am Ende sind Maschinen. Viele davon in 4776 deuten auf Dienste, die als LocalSystem oder Netzwerkdienst per NTLM auf andere Rechner zugreifen.
- **RADIUS und WLAN:** Ein NPS, der MSCHAPv2 gegen das AD prüft, erzeugt ebenfalls NTLM-Prüfungen auf dem DC, auch wenn kein Mensch vor einem Rechner sitzt.

Zum letzten Punkt gibt es einen eigenen Beitrag: MSCHAPv2, NPS und WLAN: die versteckte NTLM-Abhängigkeit. Und Anmeldungen über Vertrauensstellungen sind ein Kapitel für sich, das NTLM über Vertrauensstellungen: Gesamtstrukturen, Domänen und Kerberos ausleuchtet.

Fehlercodes in 4776: vom Tippfehler bis zum Angriff

Steht im Feld Status etwas anderes als 0x0, ist die Prüfung fehlgeschlagen. Die Codes sind NTSTATUS-Werte, und Microsoft listet für 4776 die häufigsten. Die Kurzfassung mit unserer Einordnung für die NTLM-Ablösung:

Status	Bedeutung laut Microsoft	Typischer Hintergrund
0x0	Kein Fehler	Erfolgreiche NTLM-Prüfung, der Normalfall und der Hauptteil deiner Zählung.
0xC0000064	Benutzername existiert nicht	Tippfehler, gelöschtes Konto in einer alten Konfiguration oder jemand probiert Namen durch.
0xC000006A	Falsches Kennwort	Gespeichertes Altkennwort in Skript, Laufwerkszuordnung oder Gerät; in Serie auch Passwortraten.
0xC000006D	Allgemeiner Anmeldefehler	Ungültige Anmeldedaten oder abweichende LAN-Manager-Authentifizierungsebene zwischen Quelle und Ziel.
0xC000006F	Anmeldung außerhalb der erlaubten Zeiten	Anmeldezeiten am Konto greifen.
0xC0000070	Anmeldung von nicht erlaubter Arbeitsstation	Einschränkung „Anmelden an“ am Konto passt nicht zur Quellarbeitsstation.
0xC0000071	Kennwort abgelaufen	Dienstkonto mit Ablaufdatum, das niemand verlängert hat.
0xC0000072	Konto deaktiviert	Ausgeschiedenes Konto, das irgendwo noch eingetragen ist.
0xC0000193	Konto abgelaufen	Befristetes Konto, etwa für Externe.
0xC0000224	Kennwort muss bei nächster Anmeldung geändert werden	Neues oder zurückgesetztes Konto, an dem ein Dienst hängt.
0xC0000234	Konto gesperrt	Folge einer Serie von 0xC000006A, oft durch ein einziges vergessenes Gerät.
0xC0000371	Lokaler Kontospeicher enthält kein Geheimnis für das Konto	Selten; bei lokalen Konten zu prüfen.

Die ausführliche Deutung, inklusive der Frage, warum 0xC000006D so gern als Sammelbecken dient, steht in Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten. Hängt 0xC000006D mit einer unterschiedlichen LAN-Manager-Authentifizierungsebene zusammen, hilft LmCompatibilityLevel richtig setzen: NTLMv2 erzwingen ohne Ausfall weiter.

AUS DER PRAXIS · Die Sperr-Kaskade bei der Musterwerk GmbH

Montag, 7:12 Uhr: Das Dienstkonto svc-scan der Musterwerk GmbH ist gesperrt, der Scanner im zweiten Obergeschoss legt keine PDFs mehr ab, und die Buchhaltung hält das für Sabotage. Im Sicherheitsprotokoll von DC01 stehen ab 6:58 Uhr im Minutentakt 4776 mit 0xC000006A, dann eines mit 0xC0000234. Quellarbeitsstation: leer. Das Kennwort war am Freitag rotiert worden, das Multifunktionsgerät hatte davon nichts mitbekommen.

Gefunden hat das Team den Scanner am Ende über die Client-IP in den Anmeldeereignissen des Dateiservers, nicht über 4776. Lehre: 4776 sagt dir, dass es brennt. Wo, steht woanders.

TIPP · Fehlerserien zählen statt einzeln lesen

Ein einzelnes 0xC000006A ist ein Tippfehler. Hundert in zehn Minuten für dasselbe Konto sind entweder ein Gerät mit Altkennwort oder ein Angriff. Gruppiere deshalb nach TargetUserName, Workstation und Status pro Zeitfenster, nicht nach einzelnen Ereignissen. Microsoft empfiehlt genau diese Art der Überwachung für hochprivilegierte Konten, deaktivierte Konten und Konten, die nie benutzt werden sollten.

Überwachungsrichtlinie „Überprüfung der Anmeldeinformationen“ einrichten

4776 erscheint nur, wenn die Unterkategorie „Überprüfung der Anmeldeinformationen überwachen“ (englisch Audit Credential Validation) auf den Domain Controllern aktiv ist. Ob das bei dir schon so ist, hängt von Baselines, Altlasten und dem Mut früherer Kolleginnen und Kollegen ab. Prüfe es, statt es anzunehmen.

Per Gruppenrichtlinie

Der Pfad in der Gruppenrichtlinienverwaltung, verknüpft mit der OU Domain Controllers:

```
Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen >
  Erweiterte Überwachungsrichtlinienkonfiguration > Überwachungsrichtlinien >
  Kontoanmeldung > Überprüfung der Anmeldeinformationen überwachen
    [x] Erfolg   [x] Fehler
```

Erfolg brauchst du für die NTLM-Bestandsaufnahme, Fehler für Sperrungen und Angriffe. Wichtig: Wer erweiterte Überwachungsrichtlinien benutzt, sollte sie nicht mit den alten Kategorien unter „Lokale Richtlinien > Überwachungsrichtlinie“ mischen. Sonst gewinnt am Ende die Richtlinie, mit der du nicht gerechnet hast. Wenn du ohnehin das NTLM-Auditing einrichtest, nimmt dir das NTLM-Audit-GPO-Skript die Klickarbeit für die NTLM-Richtlinien ab; die Einzelheiten zum erweiterten NTLM-Auditing erklärt Erweitertes NTLM-Auditing einschalten.

Wirksamkeit prüfen

Auf jedem DC zeigt auditpol, was tatsächlich gilt. Die GUID ist sprachunabhängig, das erspart dir das Raten, ob dein DC deutsch oder englisch spricht:

```
auditpol /get /subcategory:"{0CCE923F-69AE-11D9-BED3-505054503030}"
```

Steht dort „Erfolg und Fehler“, bist du fertig. Steht dort „Keine Überwachung“, obwohl die GPO verknüpft ist, lohnt ein Blick in gpresult /h und auf die Sicherheitsoption, die den Unterkategorien Vorrang vor den alten Kategorien gibt (englisch „Audit: Force audit policy subcategory settings to override audit policy category settings“).

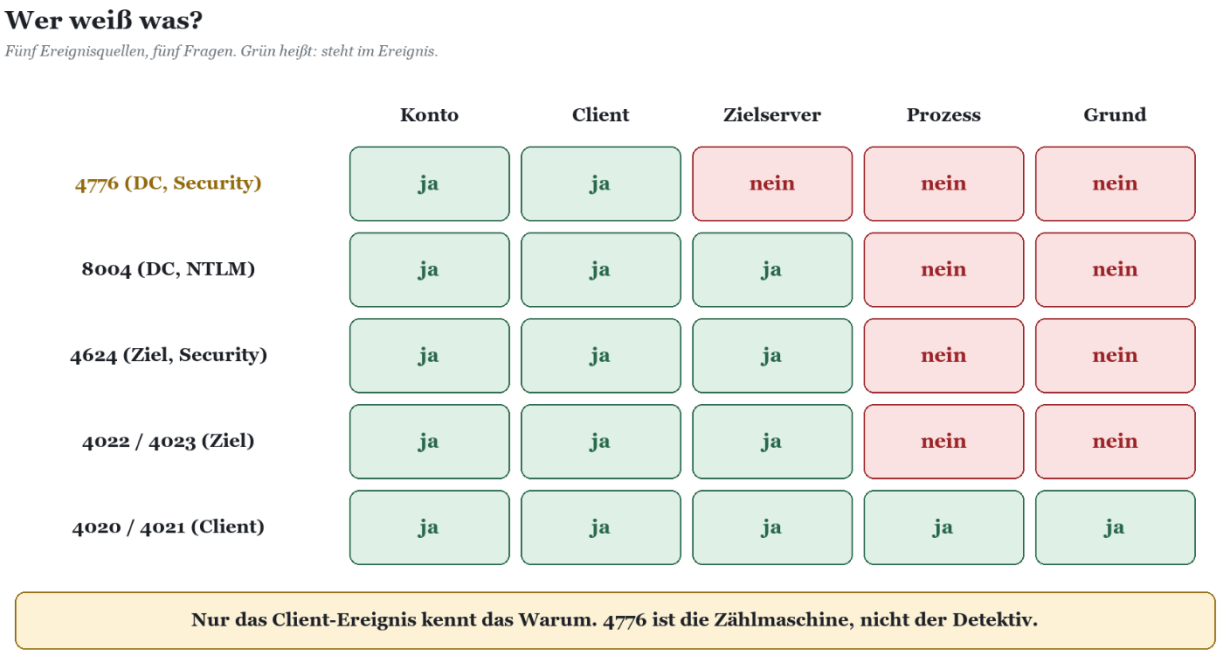
WICHTIG · Größe des Sicherheitsprotokolls

4776 ist gesprächig. Auf einem DC mit ein paar Tausend Clients kommen schnell Hunderttausende Ereignisse pro Tag zusammen. Mit der Standardgröße des Sicherheitsprotokolls überlebt ein Ereignis dann manchmal nur Stunden. Vergrößere das Protokoll oder sammle zentral, bevor du Wochenauswertungen planst. Wie das Sammeln über Windows Event Forwarding funktioniert, steht in

NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

4776 und die NTLM-Ereignisse: wer weiß was?

Neben dem Sicherheitsprotokoll gibt es das Protokoll Microsoft-Windows-NTLM/Operational. Dort stehen die klassischen Überwachungsereignisse 8001 (ausgehend), 8002 (eingehend), 8003 (eingehende Anmeldung am Server, mit dem anfragenden Client im Feld Workstation, auch auf Mitgliedsservern) und 8004 (Domain Controller) sowie die Ereignisse des erweiterten Auditings: 4020 und 4021 auf dem Client, 4022 und 4023 auf dem Server, 4024 und 4025 für NTLMv1-SSO und 4030 bis 4033 auf dem Domain Controller. Das erweiterte Auditing gibt es ab Windows 11 24H2 und Windows Server 2025 sowie auf Server 2022 und 2019 mit den Updates ab dem 13.10.2026.



Merkmal	4776	8004 / 4030–4033	4020 / 4021
Protokoll	Sicherheit	Microsoft-Windows-NTLM/Operational	Microsoft-Windows-NTLM/Operational
Entsteht auf	DC (bzw. Rechner mit lokalem Konto)	Domain Controller	Client
Voraussetzung	Überprüfung der	NTLM-Überwachung bzw.	Erweitertes Auditing auf dem

	Anmeldeinformationen	erweitertes Auditing	Client
Konto	ja	ja	ja
Anfragender Client	ja, ungeprüft	ja	ist selbst der Client
Zielserver	nein	ja, beteiligter Server	ja, TargetMachine und TargetService
Prozess	nein	nein	ja, ProcessName
Grund für NTLM	nein	nein	ja, NtlmUsageReason
Taugt für	Zählen, Sperren, Angriffe	Wer spricht mit welchem Server	Ursache finden

Der Kern: Nur das Client-Ereignis weiß, warum Windows nicht Kerberos benutzt hat. Dort steht im Feld NtlmUsageReason ein Begründungstext und daneben eine Nummer, die NtlmUsageId. Microsoft dokumentiert in KB5064479 die Reason-IDs 0 bis 11, in der Praxis taucht auch 12 auf, und Nummer und Text passen nicht immer zueinander. Maßgeblich ist deshalb der Text, die Nummer ist nur ein Hinweis. Mehr dazu in NTLM-Reason-IDs erklärt.

Warum 4776 allein keine Ursache liefert

Stell dir vor, die Trendforge Digital GmbH sieht in 4776 jeden Tag 30.000 erfolgreiche Prüfungen für das Konto svc-backup von der Quellarbeitsstation BKP01. Was weißt du? Dass der Backup-Server viel per NTLM spricht. Was weißt du nicht? Mit welchen Zielen, über welchen Prozess, per Name oder IP-Adresse, ob ein SPN fehlt oder ob der Agent schlicht nur NTLM kann. Für jede dieser Ursachen gibt es eine andere Lösung, und 4776 entscheidet zwischen keiner davon.

- **Kein Ziel:** Ohne Zielserver kannst du weder SPN noch DNS prüfen.
- **Kein Prozess:** Ob explorer.exe, ein Inventaragent oder eine Fachanwendung, bleibt offen.
- **Keine Version:** NTLMv1 und NTLMv2 sehen in 4776 gleich aus. Die Version liefern 4624 auf dem Ziel und die NTLM-Ereignisse.
- **Unzuverlässige Quelle:** Die Quellarbeitsstation ist eine Behauptung des Clients. Linux-Clients, Geräte und manche Bibliotheken schicken nichts oder Fantasienamen.

Zum ersten Punkt: Wie ein fehlender SPN NTLM erzwingt und wie du ihn findest, steht in Fehlender SPN als NTLM-Ursache. Für Dienstkonten wie svc-backup lohnt Dienstkonten als NTLM-Quelle.

FAKTEN · Was 4776 trotzdem gut kann

Es ist auf jedem unterstützten DC vorhanden, braucht kein Update und kein neues Protokoll.

Es zeigt dir in Summe, welche Konten und welche Quellrechner überhaupt NTLM benutzen.

Es ist dein Frühwarnsystem für Sperrungen, Passwortraten und vergessene Altkennwörter.

Nach der Abschaltung zeigt es dir als Gegenprobe, ob die NTLM-Prüfungen wirklich weniger werden.

4776 mit Get-WinEvent auf allen Domain Controllern auswerten

Jede Anmeldung landet auf genau einem DC, nämlich dem, den der Server gerade per Netlogon erreicht. Wer nur DC01 auswertet, sieht nur einen Teil. Das folgende Skript holt die Ereignisse der letzten 24 Stunden von allen DCs der Domäne und liest die Felder aus dem XML, nicht aus dem Meldungstext. Es braucht das AD-PowerShell-Modul und das Recht, das Sicherheitsprotokoll der DCs zu lesen, etwa über die Gruppe Ereignisprotokollleser.

```
$start = (Get-Date).AddHours(-24)
$dcs   = (Get-ADDomainController -Filter *).HostName

$events = foreach ($dc in $dcs) {
  try {
    Get-WinEvent -ComputerName $dc -ErrorAction Stop -FilterHashtable @{
      LogName = 'Security'; Id = 4776; StartTime = $start } |
    ForEach-Object {
      $d = @{}
      ([xml]$_.ToXml()).Event.EventData.Data | ForEach-Object { $d[$_.Name] = $_.'#text' }
      [pscustomobject]@{
        DC          = $dc
        Zeit        = $_.TimeCreated
        Konto       = $d.TargetUserName
        Workstation = if ($d.Workstation) { $d.Workstation } else { '(leer)' }
        Status      = $d.Status
      }
    }
  } catch { Write-Warning "$dc: $($_.Exception.Message)" }
}
```

Danach wird gezählt. Die erste Frage ist fast immer: Welche Paare aus Konto und Quellrechner machen den Großteil aus?

```
# Top 20 Paare Konto + Workstation (nur Erfolg)
$events | Where-Object Status -eq '0x0' |
  Group-Object Konto, Workstation | Sort-Object Count -Descending |
  Select-Object -First 20 Count, Name

# Fehlerserien je Konto und Status
$events | Where-Object Status -ne '0x0' |
  Group-Object Konto, Status | Sort-Object Count -Descending |
  Select-Object -First 20 Count, Name

# Verteilung auf die DCs
$events | Group-Object DC | Select-Object Count, Name

$events | Export-Csv .\4776.csv -NoTypeInformation -Encoding UTF8
```

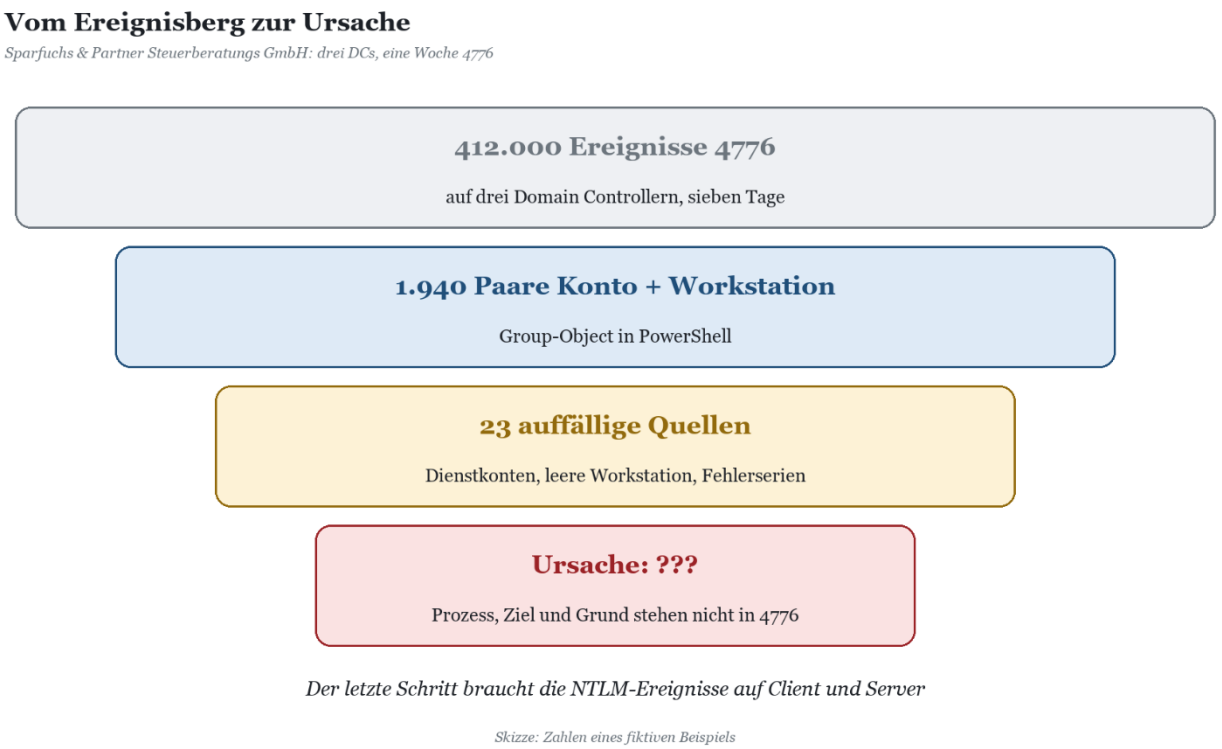
TIPP · Schneller mit XPath und parallel

Get-WinEvent -ComputerName holt jedes Ereignis über das Netz. Bei großen Protokollen ist es deutlich schneller, das Skript per Invoke-Command auf den DCs selbst laufen zu lassen und nur die fertigen Objekte zurückzugeben. Und wenn du nur Fehler willst, filtere schon beim Lesen, etwa mit einem XPath-Ausdruck wie *[System[EventID=4776] and EventData[Data[@Name='Status']!='0x0']]. Weitere Rezepte, auch für die NTLM-Ereignisse, sammelt

NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

Wo es mühsam wird

Für eine Domäne mit drei DCs und ein paar Hundert Clients reicht das Skript. In echten Umgebungen kippt es an vier Stellen:

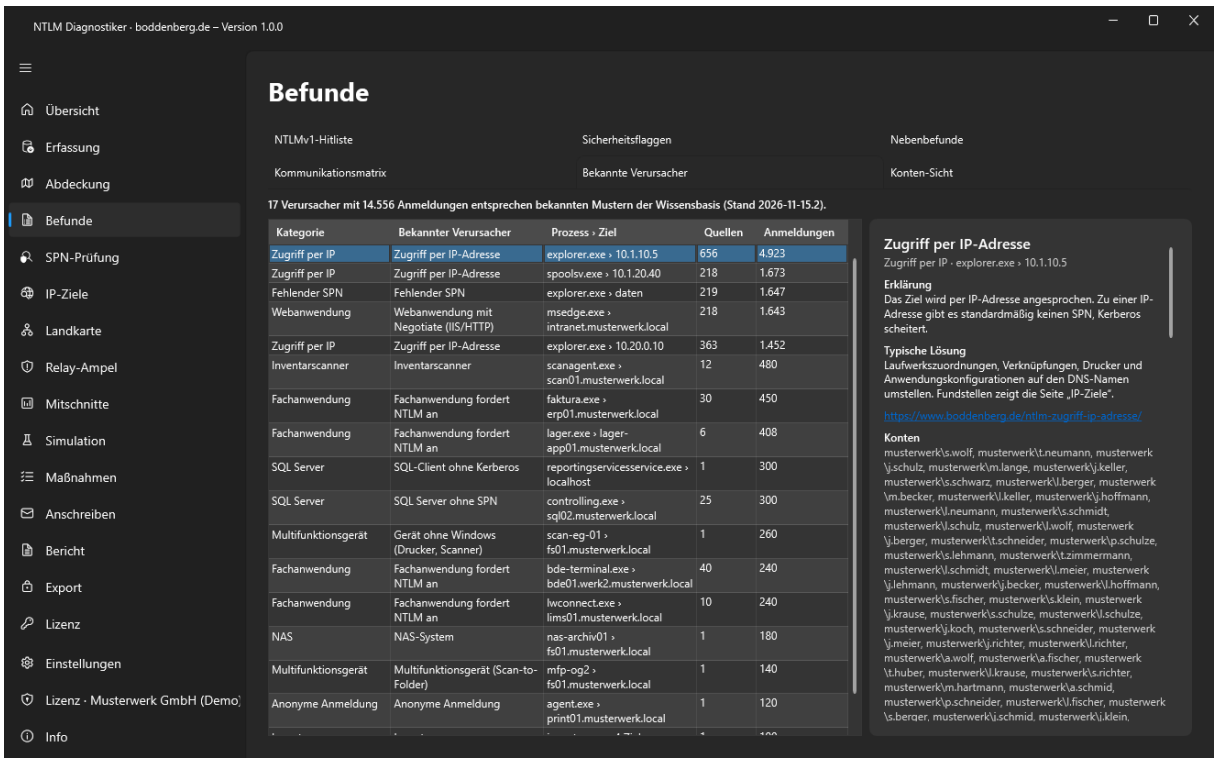


Hürde	Was passiert	Folge
Menge	Hunderttausende 4776 pro Tag und DC; das Protokoll rollt über, bevor du liest.	Lücken, die du nicht bemerkst.
Verteilung	Jeder DC sieht nur seinen Teil; ein DC ist gerade nicht erreichbar.	Verzerrte Hitlisten.
Fehlende Ursache	Konto und Quellrechner sind bekannt, Ziel, Prozess und Grund nicht.	Du musst auf jedem Quellrechner einzeln nachforschen.
Stille Quellen	Leere Workstation, Linux, Geräte, Appliances.	Die schwierigsten Fälle bleiben anonym.

An dieser Stelle hört 4776 auf, nützlich zu sein, und die NTLM-Ereignisse fangen an. Sie verraten Prozess, Ziel und Begründung, aber sie kommen von Hunderten Clients und Servern, und sie müssen zusammengeführt, gruppiert und gedeutet werden. Genau dafür haben wir den NTLM Diagnostiker gebaut.

Vom Zählen zur Ursache mit dem NTLM Diagnostiker

Der Diagnostiker sammelt die NTLM-Ereignisse dort ein, wo sie anfallen: direkt vom Domain Controller, über einen vorhandenen Windows Event Collector, per Direktabfrage der Rechner oder per Datei-Import. Er wertet die Felder aus, nicht den Meldungstext, und fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen. Aus 30.000 Strichen auf dem Klemmbrett werden so ein paar Zeilen mit Namen: Zugriff per IP-Adresse, fehlender SPN, SQL Server ohne SPN, Inventaragent. Er arbeitet dabei ausschließlich lesend und ändert nichts an deiner Umgebung.



Hier siehst du in den Befunden, welcher Verursacher mit welchem Prozess und Ziel hinter den NTLM-Anmeldungen steckt, samt Erklärung und typischer Lösung (Demodaten).

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Vom anonymen 4776 zum benannten Verursacher

Reiter „Befunde" öffnen: Die Tabelle „Verursacher" zeigt je Zeile eine Kategorie, den erkannten Verursacher, das Paar aus Prozess und Ziel, die Zahl der Quellen und die Zahl der Anmeldungen. Das ist genau die Information, die dir 4776 vorenthält.

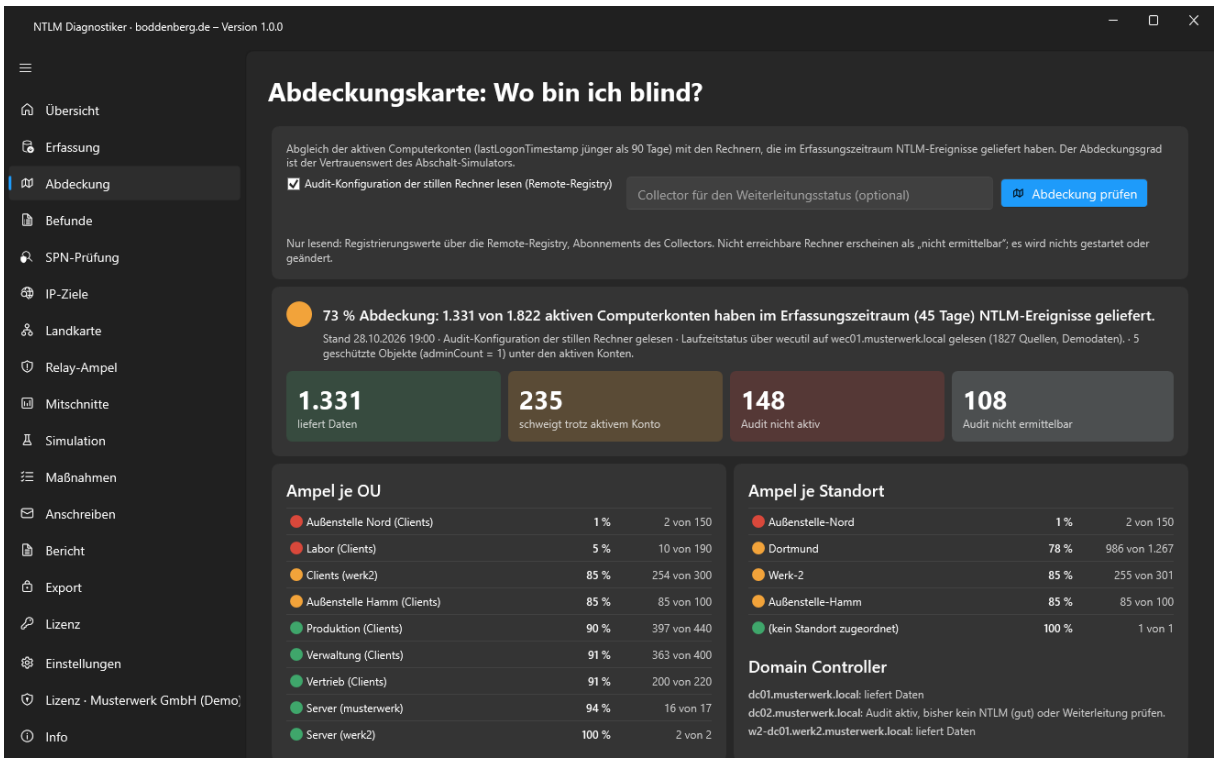
Zeile auswählen: Im Detailbereich stehen eine Erklärung aus der Wissensbasis bekannter Verursacher, die typische Lösung und die betroffenen Konten. Taucht dort svc-backup auf, hast du die Brücke zu deiner 4776-Hitliste.

Begründung lesen: Die Ursachen-Engine wertet den Begründungstext aus NtlmUsageReason aus, nicht nur die Nummer, und prüft bei Bedarf SPN, Aliasnamen und IP-Ziele.

Befehle übernehmen: Wo ein SPN fehlt, zeigt der Diagnostiker den passenden setspn-Befehl zum Kopieren an. Ausführen tust du ihn selbst.

Abdeckung prüfen: Die Abdeckungskarte zeigt je OU und Betriebssystem, welche Rechner Ereignisse liefern und welche schweigen, damit die Hitliste nicht nur die lauten Rechner kennt.

› NTLM Diagnostiker



In der Abdeckungskarte siehst du, welche Rechner NTLM-Ereignisse liefern, welche trotz aktivem Konto schweigen und wie es um die Domain Controller steht (Demodaten).

Zum Ausprobieren reicht die kostenlose Edition Express: Sie liefert unbegrenzt einen Fünf-Minuten-Befund direkt vom DC mit Readiness-Ampel, Abdeckungskarte, Top-10-Verursachern, Hinweisen aus der Wissensbasis, NTLMv1-Alarm mit Anzahl und Top 5 sowie einem Kurzbefund als PDF. Einmal pro Domäne kannst du sieben Tage lang fast den ganzen Funktionsumfang testen, lizenziert wird pro aktivem Computerkonto für 18 Monate, für beliebig viele Domänen. Ein Kerberos-Gegencheck und eine Phase-3-Bereitschaftsprüfung sind geplant.

Wenn du lieber mit jemandem zusammen von der 4776-Kurve zur Maßnahmenliste gehst, unterstützt dich die Beratung zur NTLM-Ablösung. Soll dein Team Sicherheitsprotokoll und NTLM-Ereignisse künftig selbst lesen, ist die Schulung zum NTLM Diagnostiker der kürzere Weg. Und wie die Kerberos-Seite funktioniert, auf die du am Ende umstellst, erklärt der Kompetenzbereich Microsoft Kerberos.

FAQ zu Ereignis 4776

Was bedeutet Ereignis 4776?

Ein Computer hat versucht, die Anmeldeinformationen eines Kontos per NTLM zu prüfen. Bei Domänenkonten passiert das auf dem Domain Controller. Status 0x0 heißt Erfolg, jeder andere Wert ist ein Fehlercode.

Wird 4776 auch bei Kerberos geschrieben?

Nein. 4776 steht für NTLM-Prüfungen. Kerberos-Anmeldungen protokolliert der DC in 4768, 4769 und 4771.

Warum steht der Zielserver nicht im Ereignis?

Weil 4776 nur die Prüfung des Kontos beschreibt. Microsoft dokumentiert ausdrücklich, dass nur die Quellarbeitsstation erscheint. Den Zielserver findest du in 4624 auf dem Ziel, in den NTLM-Ereignissen 8004 und 4030 bis 4033 auf dem DC und in 4020 und 4021 auf dem Client.

Warum ist die Quellarbeitsstation leer?

Der Name wird vom Client mitgeschickt. Manche Clients, Geräte und Bibliotheken lassen ihn weg oder setzen einen eigenen Wert. Dann hilft nur die IP-Adresse aus anderen Ereignissen, etwa 4624 auf dem Zielserver.

Erkenne ich NTLMv1 an 4776?

Nein. Das Authentifizierungspaket ist immer MICROSOFT_AUTHENTICATION_PACKAGE_V1_0, unabhängig von der Protokollversion. Die Version steht in 4624 auf dem Zielserver und in den NTLM-Ereignissen; Einzelheiten in Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen.

Welche Überwachungsrichtlinie brauche ich für 4776?

Die erweiterte Unterkategorie „Überprüfung der Anmeldeinformationen überwachen“ in der Kategorie Kontoanmeldung, für Erfolg und Fehler, auf allen Domain Controllern.

Reicht es, 4776 auf einem DC auszuwerten?

Nein. Jede Prüfung landet auf dem DC, den der Server gerade erreicht. Für ein vollständiges Bild brauchst du alle DCs der Domäne, am besten zentral gesammelt.

Kann ich 4776 nach der Abschaltung zur Erfolgskontrolle nutzen?

Ja, als grobe Gegenprobe ist es gut geeignet: Sinkt die Zahl der erfolgreichen 4776, wird weniger NTLM geprüft. Wie du Rückfälle zuverlässig erkennst, beschreibt Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben.

Wo steht das bei Microsoft?

In der Ereignisreferenz 4776(S, F): The computer attempted to validate the credentials for an account. Dort findest du Event-XML, Feldbeschreibungen und die Tabelle der Fehlercodes.

Fazit: Das Klemmbrett zählt, die Ursache steht woanders

Ereignis 4776 ist das robusteste NTLM-Signal, das du hast: auf jedem DC vorhanden, mit einer einzigen Überwachungsrichtlinie eingeschaltet und mit vier Feldern schnell gezählt. Es sagt dir, welche Konten und Quellrechner NTLM benutzen, und es warnt dich vor Sperr-Kaskaden und Passwortraten. Für die NTLM-Ablösung ist es der Einstieg, nicht das Werkzeug: Ziel, Prozess, Version und Begründung fehlen.

Nimm 4776 also als Zählmaschine und Frühwarnsystem, sammle es von allen DCs ein und werte es über die XML-Felder aus. Für die Frage nach dem Warum brauchst du die NTLM-Ereignisse von Clients und Servern, ob du sie mit eigenen Skripten zusammenführst oder vom Diagnostiker zusammenführen lässt. Der Türsteher hat seinen Job gemacht. Den Rest musst du selbst ermitteln, bevor der Stichtag die Tür für alle zumacht.

WEITERLESEN · Weiter in dieser Serie

› Ereignis 4624: NTLM V1 und V2 im Anmeldeprotokoll erkennen
› Fehlercodes 0xC000006D und Co.: fehlgeschlagene NTLM-Anmeldungen deuten
› NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte
› NTLM-Nutzung ermitteln
› NTLM-Reason-IDs erklärt
› Erweitertes NTLM-Auditing einschalten
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte