LDAP-Signierung und Kanalbindung: Ereignisse 2889 und 3039 auswerten



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

BERATUNG
LDAP-Härtung ohne Ausfall am Montagmorgen? Wir planen sie mit dir.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Ereignisse lesen, Verursacher finden, Härtung testen: praxisnah für dein Team.
› **Schulung zum NTLM Diagnostiker**

Jeder Domain Controller schreibt dir einmal am Tag einen Brief. Er trägt die Nummer 2887, steht im Protokoll Directory Service und sagt sinngemäß: „Gestern haben sich hier jede Menge Clients ohne Signierung angemeldet. Wer, verrate ich nicht.“ Die meisten Administratoren lesen diesen Brief seit Jahren nicht mehr, ungefähr so, wie man die Warnleuchte im alten Firmenwagen irgendwann für Dekoration hält. Mit der NTLM-Ablösung lohnt sich ein zweiter Blick, denn ungeschützte LDAP-Bindungen sind eines der Lieblingsziele für NTLM-Relay. Die wirst du nicht los, indem du nur NTLM-Anmeldungen zählst.

Dieser Beitrag dreht sich um ldap channel binding und Ereignis 2889: wie du die Ereignisse 2889 (unsignierte und Klartext-Bindungen) und 3039 (fehlende Kanalbindung) auf deinen Domain Controllern zum Reden bringst, wie du sie liest, wie du aus einer IP-Adresse einen Verursacher machst und in welcher Reihenfolge du die Härtung angehst, ohne dass am Montag die Kopierer streiken. Die Grundlagen zum Relay-Schutz stehen in NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz, den großen Zeitplan findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Der Hintergrund ist bekannt: Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, und mit der nächsten Windows-Server-Version soll NTLM standardmäßig abgeschaltet sein. Bis dahin bleibt NTLM in vielen Netzen im Spiel. Solange es im Spiel ist, entscheidet die LDAP-Härtung darüber, ob ein abgefangener NTLM-Austausch am Domain Controller etwas anrichten kann oder ins Leere läuft.

FAKTEN · Das Wichtigste in Kürze

2889 protokolliert je Client eine Bindung auf Port 389 ohne Signierung (SASL) oder eine einfache Bindung über eine unverschlüsselte Verbindung, mit IP-Adresse und Identität des Clients.

3039 protokolliert je Client eine Bindung über SSL/TLS, die an der Prüfung des Kanalbindungstokens (CBT) gescheitert ist. Das Ereignis erscheint nur, wenn die Kanalbindung auf „Wenn unterstützt“ oder „Immer“ steht.

Beide Einzelereignisse brauchen die Diagnosestufe 2 im Registrierungswert „16 LDAP Interface Events“ unter HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics.

Die Tageszusammenfassungen 2887 (Signierung) und 3040 (Kanalbindung) kommen ohne Diagnose, nennen aber nur Zahlen, keine Clients.

Neue Bereitstellungen ab Windows Server 2025 verlangen LDAP-Signierung standardmäßig und setzen die Kanalbindung auf „Wenn unterstützt“. Bei In-place-Upgrades bleiben vorhandene Einstellungen erhalten.

Was 2889 und 3039 eigentlich messen

LDAP-Signierung und Kanalbindung werden gern in einen Topf geworfen. Das ist verständlich, denn beide stehen in der Gruppenrichtlinie direkt untereinander. Geschützt werden aber verschiedene Wege. Signierung betrifft SASL-Sitzungen ohne TLS, also das klassische LDAP auf Port 389. Kanalbindung betrifft SASL-Sitzungen über TLS, also LDAPS auf Port 636 oder StartTLS auf Port 389. Und die einfache Bindung, bei der ein Client Benutzername und Kennwort schickt, schützt keiner der beiden Mechanismen. Die braucht TLS, sonst geht das Kennwort im Klartext über die Leitung.

Welche Bindung schützt was?

Signierung gilt für Port 389, Kanalbindung für TLS. Die einfache Bindung schützt keins von beiden.

Bindungsart	Was das bedeutet	Ergebnis	Ereignis
Port 389, einfache Bindung	Kennwort im Klartext	kein Schutz	2889
Port 389, SASL ohne Signierung	manipulierbar, NTLM relaybar	kein Schutz	2889
Port 389, SASL mit Signierung	Integrität, NTLM-Relay nicht verhindert	teilweise	-
LDAPS, SASL ohne CBT	verschlüsselt, NTLM relaybar	teilweise	3039
LDAPS, SASL mit CBT	an die TLS-Sitzung gebunden	geschützt	-

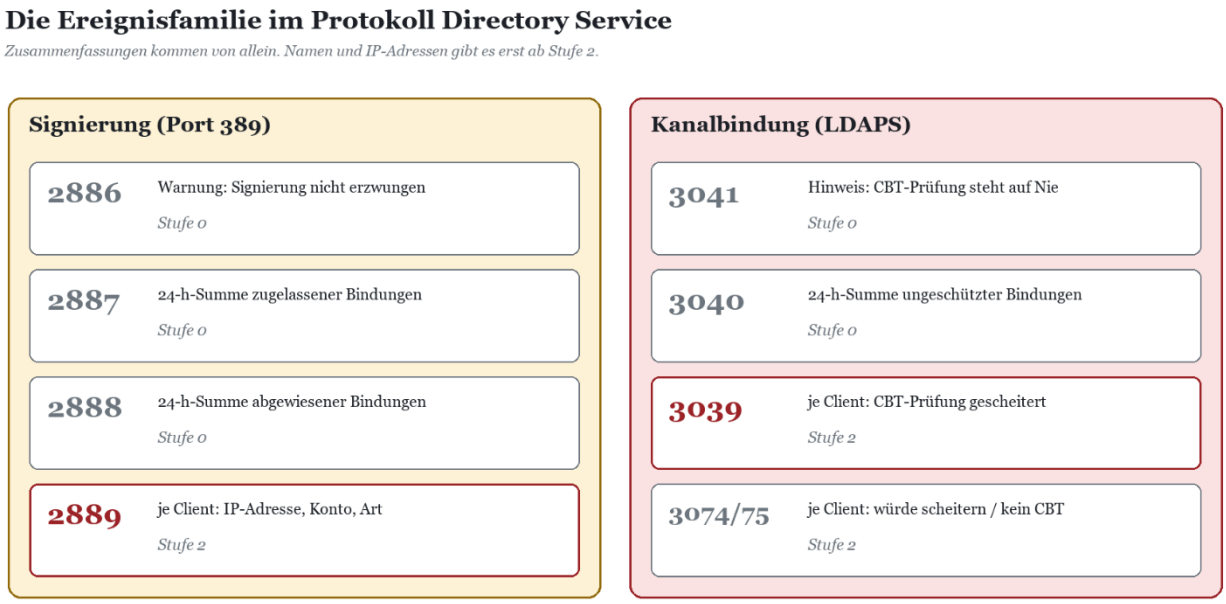
Skizze: nach Microsofts Übersicht zu LDAP-Signierung und Kanalbindung, stark vereinfacht

Für die NTLM-Ablösung ist das der springende Punkt: Microsoft schreibt in der Übersicht zur Kanalbindung ausdrücklich, dass das Hauptrisiko, gegen das CBT schützt, NTLM-Relay ist. Ein Angreifer fängt einen NTLM-Austausch ab, baut eine eigene TLS-Sitzung zum Domain Controller auf und reicht die Anmeldung weiter. Ohne Kanalbindung kann der Domain Controller die weitergereichte Anmeldung nicht von der echten unterscheiden. Signierung auf Port 389 erkennt

Manipulationen an einer Sitzung, verhindert NTLM-Relay laut Microsoft aber nicht. Kerberos mit gegenseitiger Authentisierung plus Kanalbindung über TLS nennt Microsoft als stärkste Kombination. Mehr zu Kerberos findest du im Kompetenzbereich Microsoft Kerberos.

Die ganze Familie auf einen Blick

2889 und 3039 sind nicht allein, beide gehören zu einer kleinen Familie im Protokoll „Anwendungs- und Dienstprotokolle > Directory Service“, Quelle Microsoft-Windows-ActiveDirectory_DomainService. Ein Teil davon meldet sich ohne Zutun, der interessante Teil erst nach dem Hochdrehen der Diagnose.



Skizze: Ereignis-IDs und Mindeststufen laut KB4520412 und Microsoft Learn; Texte gekürzt

Ereignis	Bedeutung	Wann es erscheint	Mindeststufe
2886	Domain Controller weist unsignierte SASL- und Klartext-Bindungen nicht ab	beim Start und alle 24 Stunden, wenn Signierung auf „Keine“ steht	0
2887	Anzahl zugelassener unsignierter und Klartext-Bindungen	alle 24 Stunden, wenn es Treffer gab	0
2888	Anzahl abgewiesener Bindungen, weil Signierung erforderlich ist	alle 24 Stunden, wenn es Treffer gab	0
2889	einzelner Client mit unsignierter oder Klartext-Bindung	bei jeder solchen Bindung	2
3039	einzelner Client, dessen LDAPS-Bindung die CBT-Prüfung nicht besteht	nur bei Kanalbindung „Wenn unterstützt“ oder „Immer“	2
3040	Anzahl ungeschützter LDAPS-Bindungen der letzten 24 Stunden	wenn Kanalbindung auf „Nie“ steht und es Treffer gab	0
3041	Empfehlung, die CBT-Prüfung zu erzwingen	beim Start und alle 24 Stunden bei „Nie“	0
3074 / 3075	Client würde bei Erzwingung scheitern beziehungsweise liefert kein CBT	nur bei „Wenn unterstützt“ oder „Immer“, ab bestimmtem Updatestand	2

WICHTIG · 3039 ist nicht der Zwilling von 2889

Bei der Signierung bekommst du die Einzelereignisse 2889, solange die Signierung nur optional ist. Bei der Kanalbindung ist es anders: 3039 entsteht nur, wenn die Kanalbindung bereits auf „Wenn unterstützt“ (1) oder „Immer“ (2) steht. Steht sie auf „Nie“ (0), siehst du nur die Summe in 3040.

„Wenn unterstützt“ ist deshalb nicht nur eine Härtungsstufe, sondern auch dein Messinstrument. Clients, die CBT nicht kennen, werden dabei laut Microsoft weiterhin zugelassen.

Was in einem 2889-Ereignis steht

Ein 2889 ist erfreulich kurz. Es nennt die IP-Adresse des Clients samt Quellport, die Identität, als die sich der Client anmelden wollte, und die Art der Bindung. Typ 0 steht für eine SASL-Bindung ohne angeforderte Signierung, Typ 1 für eine einfache Bindung über eine unverschlüsselte Verbindung. Typ 1 ist der unangenehmere Fall, denn hier lag ein Kennwort im Klartext auf dem Netz. Ein Name oder Prozess des Clients steht nicht im Ereignis. Die Werte liegen im EventData-Block als durchnummerierte Einträge vor. Deine Auswertung greift deshalb über die Position zu, nicht über den Meldungstext, der bei weitergeleiteten Ereignissen ohnehin leer sein kann.

Angabe	Beispiel (Musterwerk GmbH)	Was du daraus machst
Client-IP-Adresse:Port	10.20.30.41:51544	Gerät per DNS, DHCP oder Inventar zuordnen; Port ignorieren
Identität	MUSTERWERK\svc-scan	Dienstkonto, Benutzer oder Computerkonto? Wer ist verantwortlich?
Bindungsart	1	0 = SASL ohne Signierung, 1 = einfache Bindung im Klartext

WARNUNG · 2889 sagt nicht, ob NTLM im Spiel war

Eine SASL-Bindung kann Kerberos oder NTLM verwenden. Das 2889 verrät dir nicht, welches von beiden. Für die NTLM-Sicht brauchst du die NTLM-Ereignisse am Domain Controller: 4030 bis 4033 beim erweiterten Auditing, 8004 in der klassischen Überwachung oder 4776 im Sicherheitsprotokoll. Wie du 4776 liest, steht in

Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll. Erst wenn IP-Adresse, Konto und Zeit in beiden Quellen zusammenpassen, weißt du, dass hier NTLM ungeschützt über LDAP lief.

Diagnoseprotokollierung einschalten, ohne den DC zu fluten

Der Schalter sitzt in der Registrierung jedes Domain Controllers. Microsoft dokumentiert in KB4520412 den Wert „16 LDAP Interface Events“ vom Typ REG_DWORD unter HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics. Stufe 2 genügt für 2889 und 3039. Die Details stehen im Microsoft-Artikel 2020, 2023, and 2024 LDAP channel binding and LDAP signing requirements for Windows (KB4520412).

```
# auf jedem Domain Controller, in einer Konsole mit Administratorrechten
reg add "HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" /v "16 LDAP Interface Events"
/t REG_DWORD /d 2 /f

# nach der Erfassung wieder zurück auf 0
reg add "HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" /v "16 LDAP Interface Events"
/t REG_DWORD /d 0 /f
```

Das ist der einfache Teil. Der schwierige Teil ist das Volumen. Ein Domain Controller, an dem ein schlecht konfigurierter Monitoring-Agent alle 30 Sekunden eine Klartext-Bindung macht, schreibt dir in einer Woche das Protokoll voll. Microsoft empfiehlt ausdrücklich, die Diagnose nach der Untersuchung wieder abzuschalten, um Leistungseinbußen zu vermeiden.

TIPP · Erst Protokollgröße, dann Diagnose

Vergrößere das Protokoll Directory Service vor dem Hochdrehen, sonst überschreibt der DC die spannenden Ereignisse, bevor du sie liest. Mit wevtutil geht das ohne Klickstrecke:

wevtutil sl "Directory Service" /ms:536870912

Das setzt die Höchstgröße auf 512 MB. Prüfe vorher den freien Platz auf dem Systemlaufwerk. Für mehrere Domain Controller lohnt eine zentrale Sammlung per Windows Event Forwarding, siehe NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.

Kanalbindung auf „Wenn unterstützt“ stellen

Damit 3039 überhaupt entsteht, muss die Gruppenrichtlinie „Domain controller: LDAP server channel binding token requirements“ (in der deutschen Oberfläche „Domänencontroller: Anforderungen an das LDAP-Server-Kanalbindungstoken“) mindestens auf „Wenn unterstützt“ stehen. Dahinter steckt der Registrierungswert LdapEnforceChannelBinding unter HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters mit den Werten 0 (Nie), 1 (Wenn unterstützt) und 2 (Immer). Setze die Richtlinie über die GPO der Domain Controller, nicht per Hand in der Registrierung einzelner Server, sonst hast du nach dem nächsten DC-Neubau eine Überraschung.

Einstellung	Signierung (LDAPServerIntegrity)	Kanalbindung (LdapEnforceChannelBinding)
Richtlinie	Domain controller: LDAP server signing requirements	Domain controller: LDAP server channel binding token requirements
Werte	1 = Keine, 2 = Signatur erforderlich	0 = Nie, 1 = Wenn unterstützt, 2 = Immer
Standard bis Server 2022	optional, unsignierte Bindungen erlaubt	Nie (Auditing seit den Updates von 2023)
Neue Bereitstellung Server 2025	Signierung erzwungen (Enforcement-Richtlinie)	Wenn unterstützt
Einzelereignis bei Stufe 2	2889	3039 (dazu 3074 und 3075)

Mit Windows Server 2025 kam außerdem die Richtlinie „Domain controller: LDAP server signing requirements enforcement“ hinzu. Microsoft beschreibt sie als bei Neuinstallationen aktiv; wenn sie greift, hat sie Vorrang vor der klassischen Signaturrichtlinie. Wer seine Domain Controller per In-place-Upgrade auf 2025 gehoben hat, behält dagegen seine alten Einstellungen. Prüfe also, was bei dir wirklich gilt, statt dich auf den Standard zu verlassen.

AUS DER PRAXIS · Die zwei Domain Controller der Musterwerk GmbH

dc01 wurde neu mit Windows Server 2025 aufgesetzt, dc02 per Upgrade von Server 2019 gehoben. Die Folge: dc01 verlangt Signierung, dc02 nimmt weiterhin alles an. Der Kopierer im Lager war seit Monaten fest auf dc02 eingestellt und lieferte dort brav seine Klartext-Bindungen ab. Niemand hatte es bemerkt, bis dc02 außer Betrieb gehen sollte. Merke: Ein uneinheitlicher Stand ist die beste

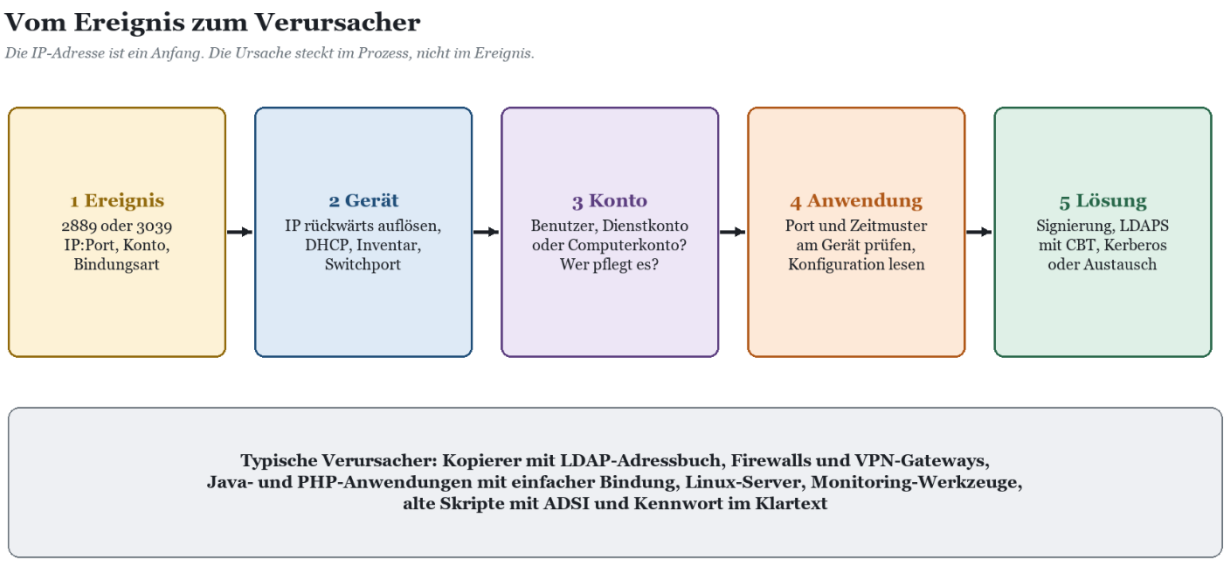
Tarnung für Altlasten.

Clients finden: aus der IP-Adresse wird ein Verursacher

Sobald die Diagnose läuft, liest du die Ereignisse am besten nicht in der Ereignisanzeige, sondern per PowerShell. Das folgende Rezept fasst die 2889-Ereignisse eines Domain Controllers nach IP-Adresse, Konto und Bindungsart zusammen. Die Positionen der Werte im EventData-Block prüfst du einmal an einem echten Ereignis mit Format-List, bevor du dich auf die Zuordnung verlässt.

```
$dc = 'dc02.musterwerk.local'
Get-WinEvent -ComputerName $dc -FilterHashtable @{
    LogName = 'Directory Service'; Id = 2889; StartTime = (Get-Date).AddDays(-7) } |
  ForEach-Object {
    [pscustomobject]@{
      IP    = ($_.Properties[0].Value -split ':')[0]
      Konto = $_.Properties[1].Value
      Art   = $_.Properties[2].Value   # 0 = SASL ohne Signierung, 1 = Klartext
    } } |
  Group-Object IP, Konto, Art | Sort-Object Count -Descending |
  Select-Object Count, Name -First 25
```

Für 3039 funktioniert dasselbe mit Id = 3039. Die Anzahl der Werte unterscheidet sich, deshalb auch hier: einmal anschauen, dann verallgemeinern. Mehr Rezepte für Get-WinEvent, auch für die NTLM-Ereignisse und für mehrere Domain Controller, findest du in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.



Skizze: Vorgehen beispielhaft für die Musterwerk GmbH

Die üblichen Verdächtigen

Nach ein paar Tagen Sammeln ergibt sich meist ein vertrautes Bild. Es sind selten die Windows-Arbeitsplätze, denn Windows-Clients fordern Signierung standardmäßig an, und Windows 11 ab 24H2 verschlüsselt LDAP-Verbindungen laut Microsoft sogar standardmäßig. Es sind die Geräte und Anwendungen, die irgendwann jemand „mal schnell ans AD angebunden“ hat.

Verursacher	Typisches Muster	Typischer Lösungsweg
Multifunktionsgerät mit	2889 Typ 1, Dienstkonto, Port	LDAPS mit gültigem Zertifikat

LDAP-Adressbuch	389	konfigurieren; Firmware prüfen
Firewall, VPN-Gateway, WLAN-Controller	2889 Typ 1 bei jeder Benutzeranmeldung	auf LDAPS umstellen oder anders anbinden; Herstellerdoku prüfen
Java- oder PHP-Webanwendung	2889 Typ 1, technisches Konto, regelmäßig	ldaps:// statt ldap://, Zertifikatsvertrauen einrichten
Linux-Server, SSSD, Samba	2889 Typ 0 oder 3039	Signierung oder Sealing aktivieren, Kerberos nutzen
Monitoring- und Inventarwerkzeuge	viele 2889 im Minutentakt	Konfiguration auf LDAPS, Abfrageintervall prüfen
Alte Skripte mit ADSI und Kennwort	2889 Typ 1 zu festen Uhrzeiten	Skript auf integrierte Anmeldung umbauen
Ältere Bibliotheken von Drittanbietern	3039 bei LDAPS-Bindungen	Bibliothek oder Laufzeit aktualisieren, Hersteller fragen

Zu mehreren Gerätegruppen gibt es eigene Beiträge der Serie: NAS, Drucker und Scanner: NTLM bei Geräten ohne Windows, Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden, Java-Anwendungen und NTLM: Kerberos mit SPNEGO, Linux und Samba in der Domäne: Kerberos statt NTLM und Backup-, Monitoring- und Inventaragenten als NTLM-Quelle. Steckt hinter einer Identität ein Dienstkonto, das gleichzeitig per NTLM auffällt, hilft Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen.

Wo Bordmittel an ihre Grenzen kommen

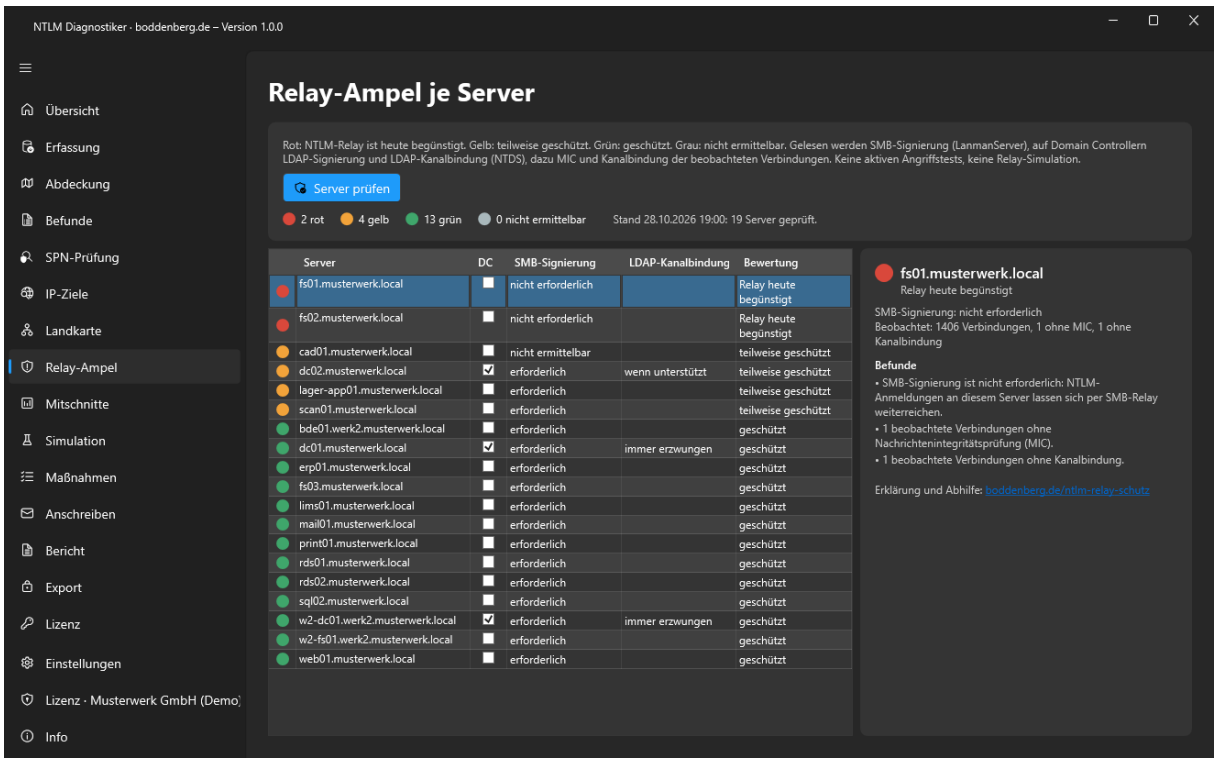
In einer Umgebung mit zwei Domain Controllern und zwanzig Treffern erledigst du das alles an einem Nachmittag. Bei sechs Standorten, vierzehn Domain Controllern und einem Protokoll, das alle zwei Tage überläuft, sieht es anders aus. Die IP-Adresse aus dem 2889 sagt dir nicht, welcher Prozess die Bindung aufgebaut hat. Ob dieselbe Gegenstelle auch NTLM ohne Kanalbindung oder ohne MIC benutzt, steht in ganz anderen Protokollen, nämlich in den NTLM-Ereignissen 4020 bis 4023 mit den Feldern ChannelBindingStatus und „Mic Status“. Und welche Domain Controller schon „Immer“ eingestellt haben und welche noch „Nie“, musst du Server für Server nachsehen.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Die Relay-Ampel zeigt dir den Stand je Server

Der NTLM Diagnostiker liest auf den Domain Controllern die Einstellungen zu LDAP-Signierung und LDAP-Kanalbindung aus der NTDS-Konfiguration, auf allen geprüften Servern die SMB-Signierung, und verknüpft das mit den beobachteten NTLM-Verbindungen: Wie viele kamen ohne Nachrichtenintegritätsprüfung (MIC), wie viele ohne Kanalbindung, wie viele ohne Sitzungsschlüssel?

Daraus entsteht je Server eine Bewertung: Rot heißt „Relay heute begünstigt“, Gelb „teilweise geschützt“, Grün „geschützt“, Grau „nicht ermittelbar“. In den Demodaten landet ein Domain Controller mit Kanalbindung „wenn unterstützt“ bei Gelb, einer mit „immer erzwungen“ bei Grün. Rechts siehst du die Befunde zum markierten Server samt Verweis auf die passende Erklärung.

Der Diagnostiker arbeitet ausschließlich lesend. Er führt keine Angriffstests aus, simuliert kein Relay und ändert keine Einstellung. Was zu tun ist, entscheidest und erledigst du.

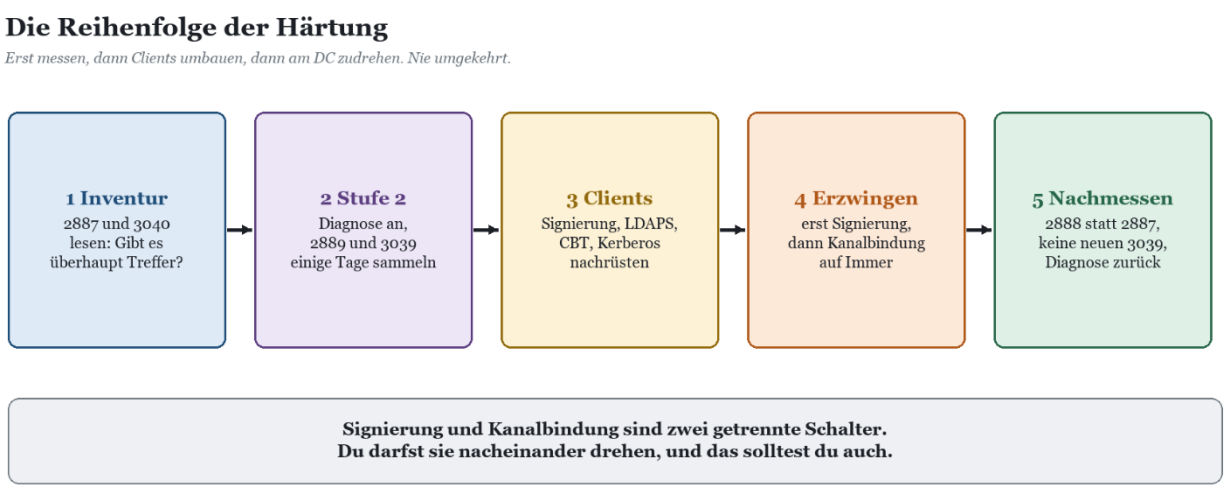


So siehst du in der Relay-Ampel je Server, ob SMB-Signierung und LDAP-Kanalbindung greifen und wie viele NTLM-Verbindungen ohne MIC oder Kanalbindung kamen (Demodaten der Musterwerk GmbH).

Das ersetzt das Lesen von 2889 und 3039 nicht, es ordnet sie ein: Du siehst, an welchem Domain Controller die Härtung noch fehlt, und über die Top-10-Verursacher, die Ursachen-Engine und die Kommunikationsmatrix, welche Prozesse und Konten NTLM ohne Kanalbindung verwenden. Wie der NTLM Diagnostiker Ereignisse direkt vom DC, über einen Windows Event Collector, per Direktabfrage oder Datei-Import einsammelt, steht auf der Produktseite. Die kostenlose Express-Edition liefert dir den Fünf-Minuten-Befund vom DC mit Readiness-Ampel, Abdeckungskarte und Top-10-Verursachern; den vollen Funktionsumfang kannst du sieben Tage lang je Domäne testen.

Die Reihenfolge der Härtung

Der häufigste Fehler bei der LDAP-Härtung ist kein technischer, sondern ein zeitlicher: Jemand stellt an einem Dienstagnachmittag die Signierung auf „erforderlich“, weil der Penetrationstest das empfohlen hat, und am Mittwochmorgen druckt, scannt und authentifiziert die halbe Firma nicht mehr. Der Domain Controller hat dann alles richtig gemacht. Er hat nur vorher niemanden gefragt.



Skizze: Reihenfolge beispielhaft für die Musterwerk GmbH

Schritt	Was du tust	Woran du den Erfolg erkennst
1 Inventur	2887 und 3040 der letzten Wochen lesen, Einstellungen aller DCs vergleichen	Du weißt, ob und wie viele ungeschützte Bindungen es gibt
2 Messen	Diagnosestufe 2, Kanalbindung auf „Wenn unterstützt“, mindestens eine Woche sammeln, möglichst mit Monatsabschluss	Liste aller Clients mit 2889 und 3039
3 Nachrüsten	Geräte und Anwendungen auf Signierung, LDAPS mit CBT oder Kerberos umstellen	Die Zahl der Clients in 2889 und 3039 sinkt
4 Signierung erzwingen	Signaturrichtlinie auf „Signatur erforderlich“, erst ein DC, dann alle	2888 statt 2887; meldet 2888 Abweisungen, hast du jemanden übersehen
5 Kanalbindung erzwingen	Kanalbindung auf „Immer“, wieder schrittweise	keine neuen 3039
6 Aufräumen	Diagnosestufe zurück auf 0, Protokollgröße normalisieren, Ergebnis dokumentieren	Härtung im Normalbetrieb, Rückfälle sichtbar über 2888

WARNUNG · Einfache Bindungen über TLS bleiben erlaubt

„Signatur erforderlich“ weist einfache Bindungen über unverschlüsselte Verbindungen ab, nicht aber einfache Bindungen über LDAPS. Kanalbindung gilt laut Microsoft nur für SASL über TLS, nicht für einfache Bindungen. Ein Gerät, das auf ldaps:// mit Benutzername und Kennwort umgestellt wurde, fällt also aus beiden Ereignissen heraus. Das ist besser als Klartext, aber kein Kerberos. Führe solche Konten in einer eigenen Liste, mit langen Kennwörtern und eingeschränkten Rechten.

TIPP · Erfolgskontrolle über die Tageszusammenfassungen

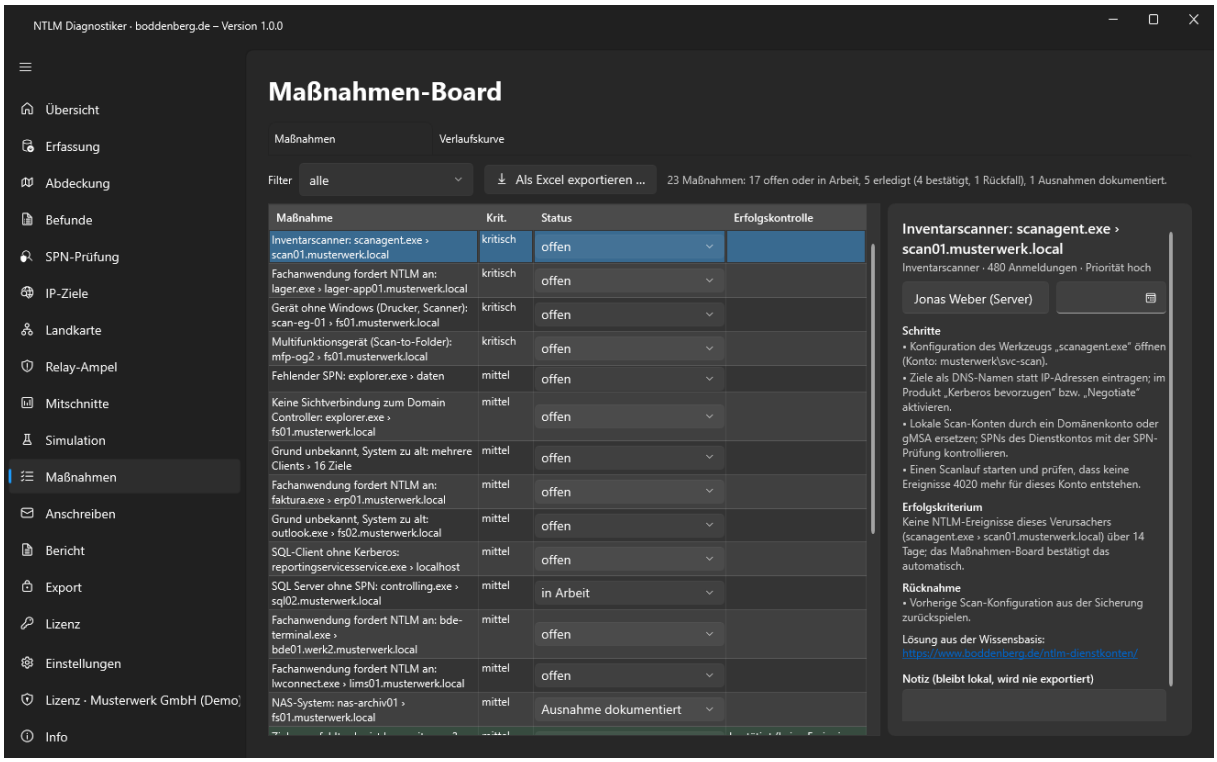
Nach dem Erzwingen ist 2888 dein bester Freund. Das Ereignis zählt, wie viele Bindungen der DC in 24 Stunden abgewiesen hat. Steht dort plötzlich eine Zahl, gibt es einen Client, der es nicht mehr schafft. Kurz die Diagnose auf Stufe 2, und du hast IP-Adresse und Konto. Wie du generell erkennst, ob nach einer Härtung jemand zurückfällt, steht in

Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben.

Wie das zur NTLM-Ablösung passt

LDAP-Härtung und NTLM-Ablösung laufen parallel, nicht nacheinander. Kanalbindung schließt die Relay-Lücke für NTLM über LDAPS heute schon, auch wenn du NTLM noch Monate brauchst. Umgekehrt hilft jede Anwendung, die du von NTLM auf Kerberos umstellst, auch der LDAP-Sicherheit. Behandle beide Listen deshalb als ein gemeinsames Maßnahmenpaket: Wer in 2889 auftaucht, steht oft auch in deiner NTLM-Liste, und umgekehrt. Damit du die Clients auch im NTLM-Teil siehst, brauchst du das erweiterte NTLM-Auditing auf den Domain Controllern, siehe Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; das NTLM-Audit-GPO-Skript nimmt dir die Klickarbeit in der Gruppenrichtlinie ab.

Im NTLM Diagnostiker landen beide Themen im selben Maßnahmen-Board. Jede Maßnahme hat Kritikalität, Status, Verantwortlichen, Rücknahme und ein Erfolgskriterium mit Erfolgskontrolle. So wird aus „Kopierer Lager auf LDAPS umstellen“ ein nachvollziehbarer Punkt mit Häkchen, nicht ein Zettel am Monitor.



So verfolgst du im Maßnahmen-Board jede Umstellung mit Kritikalität, Status und Erfolgskontrolle (Demodaten der Musterwerk GmbH).

Wenn du die Härtung für viele Standorte oder mit vielen Fremdgeräten planen musst, begleitet dich unsere Beratung zur NTLM-Ablösung. Wer die Ereignisse im Team selbst sicher lesen will, findet das passende Format in der Schulung zum NTLM Diagnostiker.

FAQ zu Ereignis 2889, 3039 und LDAP-Kanalbindung

Warum sehe ich kein Ereignis 2889, obwohl 2887 Treffer meldet?

Weil 2889 erst ab Diagnosestufe 2 im Wert „16 LDAP Interface Events“ protokolliert wird. 2887 kommt auch ohne Diagnose, zählt aber nur.

Warum sehe ich kein Ereignis 3039?

3039 entsteht nur, wenn die Kanalbindung auf „Wenn unterstützt“ oder „Immer“ steht und die Diagnosestufe mindestens 2 beträgt. Bei „Nie“ meldet der DC nur die Summe in 3040.

Wie lange sollte die Diagnosestufe 2 aktiv bleiben?

So lange, bis du alle regelmäßigen Clients gesehen hast, in der Regel ein bis zwei Wochen einschließlich Monatswechsel. Danach stellst du sie wieder auf 0, wie Microsoft es empfiehlt.

Bricht etwas, wenn ich die Kanalbindung auf „Wenn unterstützt“ stelle?

Clients, die CBT nicht unterstützen, werden laut Microsoft weiterhin zugelassen. Abgewiesen werden Clients, die CBT unterstützen, aber keins oder ein fehlerhaftes schicken. Genau die zeigt dir 3039. Teste die Einstellung trotzdem zuerst an einem Domain Controller.

Was bedeutet Bindungsart 1 im Ereignis 2889?

Eine einfache Bindung über eine unverschlüsselte Verbindung. Benutzername und Kennwort gingen im Klartext über das Netz. Typ 0 ist eine SASL-Bindung ohne angeforderte Signierung.

Zeigt 2889, ob ein Client NTLM benutzt hat?

Nein. Für die NTLM-Sicht brauchst du die NTLM-Ereignisse am DC, etwa 4030 bis 4033, 8004 oder 4776, und gleichst IP-Adresse, Konto und Zeit ab.

Ist Windows Server 2025 von Haus aus abgesichert?

Bei neuen Bereitstellungen ist die Signierung erzwungen und die Kanalbindung auf „Wenn unterstützt“ gesetzt. Bei Upgrades bleiben die alten Einstellungen erhalten. Prüf den tatsächlichen Stand jedes Domain Controllers.

Wo finde ich die offizielle Ereignisliste zur Kanalbindung?

In der Microsoft-Übersicht LDAP Channel Binding in Active Directory und im Artikel KB4520412.

Fazit: Erst zuhören, dann zudrehen

2889 und 3039 sind zwei der ehrlichsten Ereignisse, die ein Domain Controller schreiben kann. Beide sagen dir genau, wer sich ohne Signierung oder ohne Kanalbindung anmeldet, mit IP-Adresse und Konto. Du musst sie nur einschalten, eine Woche zuhören und die Antworten ernst nehmen. Danach ist die Härtung keine Mutprobe mehr, sondern eine Liste: Clients nachrüsten, Signierung erzwingen, Kanalbindung erzwingen, Diagnose zurückdrehen.

Und wenn am Ende doch ein Kopierer übrig bleibt, der weder signieren noch LDAPS kann: Dann hast du immerhin den Beleg, um mit dem Hersteller oder der Geschäftsführung über seinen wohlverdienten Ruhestand zu reden. Die komplette Liste der Prüfpunkte vor dem Stichtag findest du in Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz
› Ereignis 4776 auf dem Domain Controller: NTLM-Anmeldungen im Sicherheitsprotokoll
› NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NAS, Drucker und Scanner: NTLM bei Geräten ohne Windows
› Java-Anwendungen und NTLM: Kerberos mit SPNEGO
› Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen
› Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben
› Microsoft Kerberos