Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren



WISSEN
Wie der NTLM Diagnostiker belegt, welche Ziele in deiner Umgebung tatsächlich noch NTLM brauchen.
› **NTLM Diagnostiker**

BERATUNG
Ausnahmen bewerten, eng fassen und in einen Pflegeprozess bringen, bevor das Verweigern scharf geschaltet wird.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Ereignisse, Reason IDs und Ausnahmelisten so lesen, dass dein Team die Entscheidungen selbst trifft.
› **Schulung zum NTLM Diagnostiker**

Jede NTLM-Ablösung hat einen Moment, in dem jemand sagt: „Dann machen wir für den eine Ausnahme." Der Satz fällt meist gegen 16:40 Uhr, kurz bevor das Wartungsfenster schließt, und er ist völlig in Ordnung. Problematisch wird er erst drei Jahre später, wenn die Ausnahmeliste 47 Einträge hat, von denen 30 auf Server zeigen, die längst im Wertstoffhof liegen, und einer davon schlicht „*" heißt. Niemand weiß mehr, wer ihn eingetragen hat. Aber alle wissen, dass man ihn besser nicht anfasst.

Ausnahmen werden in den nächsten Monaten wichtiger, nicht unwichtiger. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig, gesteuert über den Registrierungswert BlockNtlmv1SSO und protokolliert mit den Ereignissen 4024 und 4025. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Den Zeitplan erklärt NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Wer NTLM vorher selbst kontrolliert einschränkt, braucht für den Rest, der noch nicht umgestellt ist, Ausnahmen. Und genau da entscheidet sich, ob du Fenster einbaust oder Löcher bohrst.

Dieser Beitrag zeigt, wann eine Ausnahme gerechtfertigt ist, wie eng du sie fasst, wie du sie dokumentierst und wie du sie regelmäßig überprüfst, damit aus der Übergangslösung kein Denkmal wird. Die Technik der Restrict-NTLM-Richtlinien selbst, also welche Option was bewirkt, steht in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern. Hier geht es um die Pflege.

FAKTEN · NTLM-Ausnahmen auf einen Blick

Es gibt zwei Ausnahmelisten: „Netzwerksicherheit: NTLM einschränken: Remoteserverausnahmen für die NTLM-Authentifizierung hinzufügen“ auf Clients und „Netzwerksicherheit: NTLM einschränken: Serverausnahmen in dieser Domäne hinzufügen“ auf Domänencontrollern.

Beide wirken nur, wenn die zugehörige Richtlinie verweigert: ausgehend zu Remoteservern beziehungsweise „NTLM-Authentifizierung in dieser Domäne“. Ohne Verweigern ist die Liste wirkungslos, aber nicht harmlos: Sie wird beim Scharfschalten sofort aktiv.

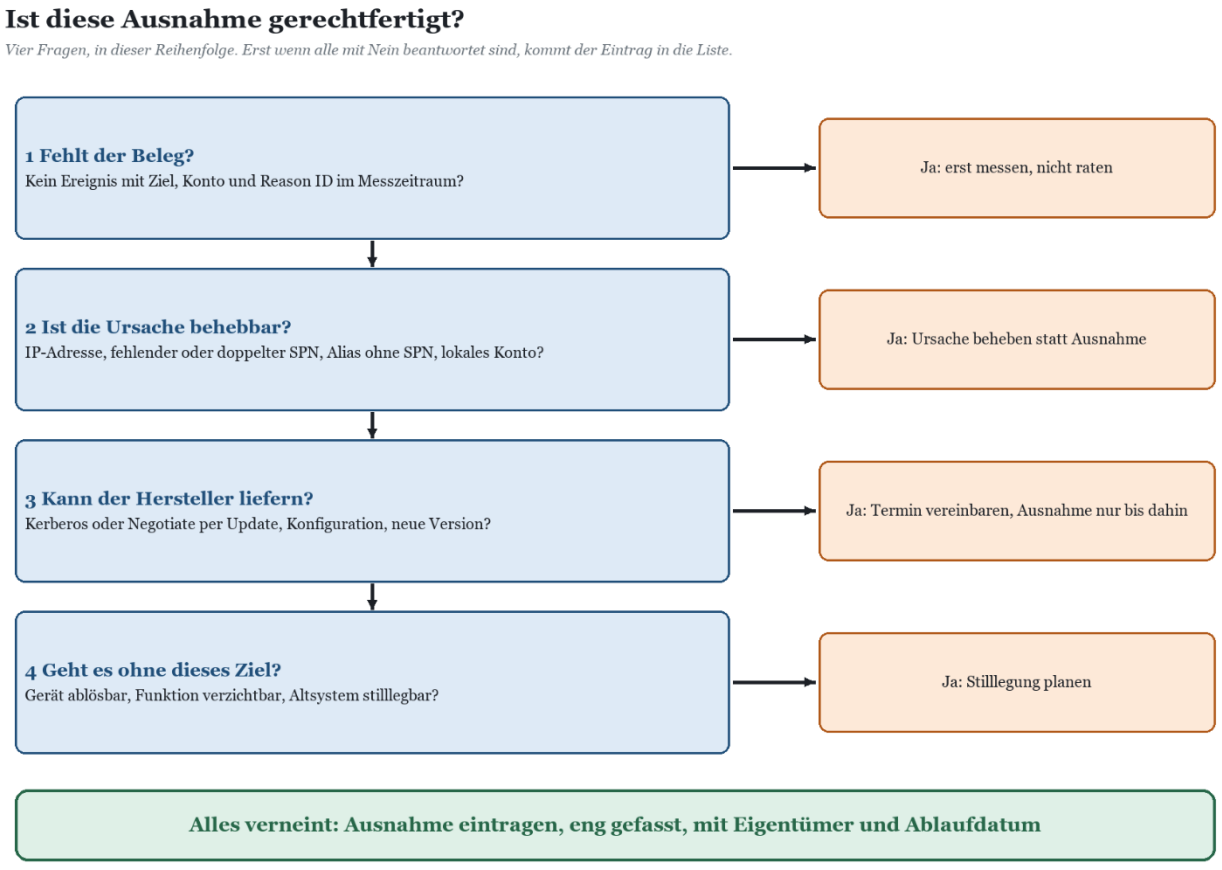
Format laut Microsoft: NetBIOS-Name des Servers, ein Eintrag pro Zeile, ein Stern als Platzhalter an beliebiger Stelle. Bei den Remoteserverausnahmen zählt der Name, den die Anwendung tatsächlich verwendet, also gegebenenfalls auch der FQDN.

Die eingehende Richtlinie am Server hat keine Ausnahmeliste. Einen Server nimmst du dort aus, indem du ihn aus dem Wirkungsbereich der Verweigern-GPO herausnimmst.

Änderungen greifen laut Microsoft ohne Neustart. Ob die Liste wie gewünscht wirkt, zeigt das Protokoll Microsoft-Windows-NTLM/Operational.

Wann eine Ausnahme gerechtfertigt ist

Eine Ausnahme ist eine Entscheidung, NTLM für ein bestimmtes Ziel weiter zuzulassen, obwohl du es sonst verweigerst. Microsoft formuliert das in der Referenz zur DC-Ausnahmeliste nüchtern: Der Verkehr zu Servern auf der Liste bleibt angreifbar für alles, was die Schwächen von NTLM ausnutzt. Jede Ausnahme ist also ein kalkuliertes Risiko. Kalkuliert setzt voraus, dass jemand gerechnet hat.



Skizze: Prüfreihenfolge für einen Ausnahmeantrag

Erst die Ursache, dann die Ausnahme

Der häufigste Fehler ist, eine Ausnahme für ein Problem einzutragen, das sich in zehn Minuten beheben ließe. Das erweiterte NTLM-Auditing nach Microsoft KB5064479 liefert in den Ereignissen 4020 bis 4023 (Client und Server) und 4030 bis 4033 (DC) eine Reason ID von 0 bis 11, die erklärt, warum nicht Kerberos benutzt wurde. Das erweiterte Auditing läuft ab Windows 11 24H2 und Windows Server 2025 sowie auf Windows Server 2022 und 2019 mit den Updates ab 13.10.2026. Auf älteren Systemen bleiben die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004, allerdings ohne Ursache. Die Bedeutung jeder einzelnen Reason ID steht in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

Für die Ausnahmefrage reicht eine grobe Sortierung: Ist die Ursache in deiner Hand, gehört sie behoben, nicht ausgenommen.

Ursache im Befund	Ausnahme sinnvoll?	Was stattdessen hilft
Zugriff per IP-Adresse	nein	Laufwerke, Skripte und Geräte auf DNS-Namen umstellen
Zielname nicht auflösbar oder SPN fehlt	nein	SPN registrieren, DNS-Eintrag oder Alias korrigieren
Doppelter SPN	nein	Duplikat mit setspn -X finden und bereinigen
Lokales Konto am Ziel	selten	Domänenkonto oder gMSA verwenden, lokale Altlasten entfernen
Keine Sichtverbindung zum DC	vorübergehend	Netzwerkpfad klären, IAKerb und lokales KDC einplanen
Anwendung spricht nur NTLM	ja, befristet	Hersteller nach Kerberos/Negotiate fragen, Termin festhalten
Gerät ohne Kerberos-Unterstützung	ja, befristet	Firmware prüfen, Ablösung im Budget einplanen

Für die drei häufigsten Fälle gibt es eigene Beiträge: NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen, Reason-ID 6: wenn der Zielname nicht auflösbar ist und Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten. Bleibt danach ein Rest, ist er ehrlich. Mit dem kannst du arbeiten.

Die vier legitimen Gründe

In der Praxis bleiben fast immer dieselben vier Kategorien übrig. Alles, was hier nicht hineinpasst, solltest du noch einmal anschauen.

- Fachanwendung mit fest eingebautem NTLM, für die der Hersteller ein Update zugesagt hat oder ausdrücklich keines liefern wird. Wie du richtig nachfragst, zeigt der Beitrag zur Herstellerfrage.
- Geräte ohne Kerberos-Unterstützung: Multifunktionsdrucker, Scanner, ältere NAS, Steuerungen in der Produktion, Medizintechnik im Krankenhaus mit Zulassung, an der niemand schrauben darf.
- Übergangsphasen mit Termin: Migration eines Dateiservers, Ablösung einer Fachanwendung, Zusammenlegung zweier Domänen.
- Verbindungen ohne Sichtverbindung zum DC, bis IAKerb und lokales KDC aus Phase 2 in deiner Umgebung angekommen sind.

Für die Herstellerseite lohnt sich Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen, für Drucker und Co. NAS, Drucker und Scanner: NTLM bei Geräten ohne

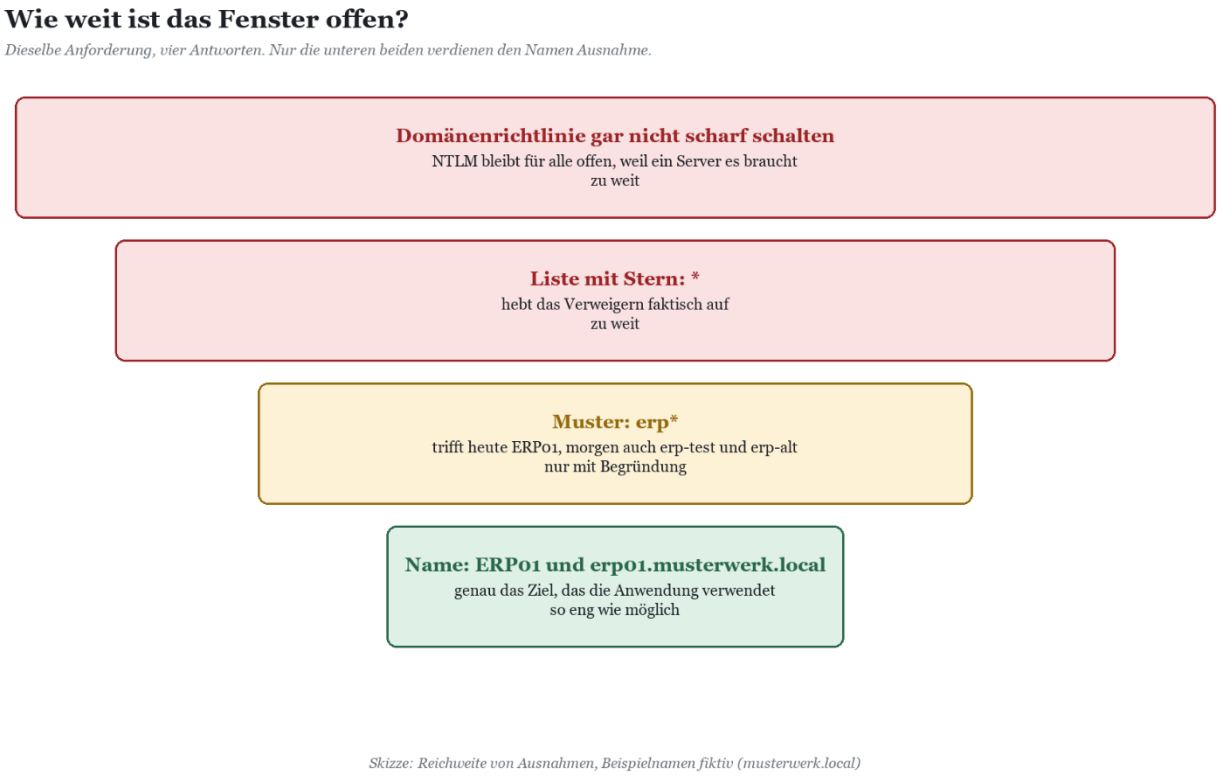
Ereignisprotokoll. In Kliniken ist die Liste der Geräte mit Zulassung oft der größte Brocken; dazu mehr in NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen.

WARNUNG · „Hat bisher immer funktioniert“ ist keine Begründung

Eine Ausnahme ohne Ereignis-Beleg ist eine Vermutung mit Gruppenrichtlinie. Trag nichts ein, was du nicht im Protokoll gesehen hast, mit Quelle, Ziel, Konto und, wo verfügbar, Reason ID. Und trag nichts „vorsichtshalber“ ein. Vorsichtshalber eingetragene Ausnahmen sind die, die nie wieder jemand entfernt, weil keiner weiß, ob sie gebraucht werden.

Wie eng du eine Ausnahme fasst

Die Grundregel ist simpel: so eng wie möglich, so weit wie nötig. In der Praxis heißt das Server statt Domäne, Namen statt Platzhalter und so wenige Geräte im Wirkungsbereich wie möglich. Die Restrict-NTLM-Richtlinien geben dir dafür mehr Stellschrauben, als die meisten nutzen.



Skizze: Reichweite von Ausnahmen, Beispielnamen fiktiv (musterwerk.local)

Server statt Domäne

Die bequemste Ausnahme ist gar keine: Man schaltet das Verweigern einfach nicht ein, weil ein einziger Server noch NTLM braucht. Damit bleibt NTLM für die gesamte Domäne offen, für ein Problem auf einer Maschine. Das ist, als würdest du das ganze Haus unverschlossen lassen, weil der Schlüssel zum Kellerfenster klemmt. Die saubere Lösung: Verweigern einschalten und genau diesen einen Server auf die Liste setzen. Am DC heißt das „Serverausnahmen in dieser Domäne“, auf Clients „Remoteserverausnahmen“.

Dasselbe gilt für den Wirkungsbereich der GPO. Brauchen nur die zwölf Rechner im Labor das Analysegerät, gehört die Ausnahme nicht in eine GPO für alle Clients, sondern in eine GPO, die per OU oder Sicherheitsfilter nur das Labor erreicht. Die übrigen 900 Clients dürfen dann überhaupt kein NTLM mehr sprechen, auch nicht zum Analysegerät.

Namen statt Platzhalter

Ein Stern ist an jeder Stelle des Eintrags erlaubt. Das ist praktisch und gefährlich zugleich. Ein Eintrag „scan*“ trifft heute die drei Scanner, die du kennst, und morgen auch den Testserver, den ein Kollege „scan-test-alt“ genannt hat. Ein Eintrag „*“ allein hebt das Verweigern vollständig auf und ist damit keine Ausnahme mehr, sondern eine Kapitulation mit Formular.

Trage deshalb konkrete Namen ein, und zwar genau die Schreibweise, die die Anwendung benutzt. Ruft eine Anwendung den Server über seinen FQDN auf, steht der FQDN in der Liste. Ruft sie ihn über einen Alias auf, steht der Alias drin, und du solltest dir bei der Gelegenheit gleich ansehen, warum für den Alias kein SPN existiert. Muster sind dann vertretbar, wenn eine Namenskonvention verbindlich ist und die Begründung ausdrücklich das Muster nennt.

```
# Remoteserverausnahmen, Musterwerk GmbH, GPO "NTLM Ausnahmen Clients"
ERP01
erp01.musterwerk.local
LAB-ANALYSE02

# Serverausnahmen in dieser Domäne, GPO "NTLM Ausnahmen DC"
LEGACY-APP01
```

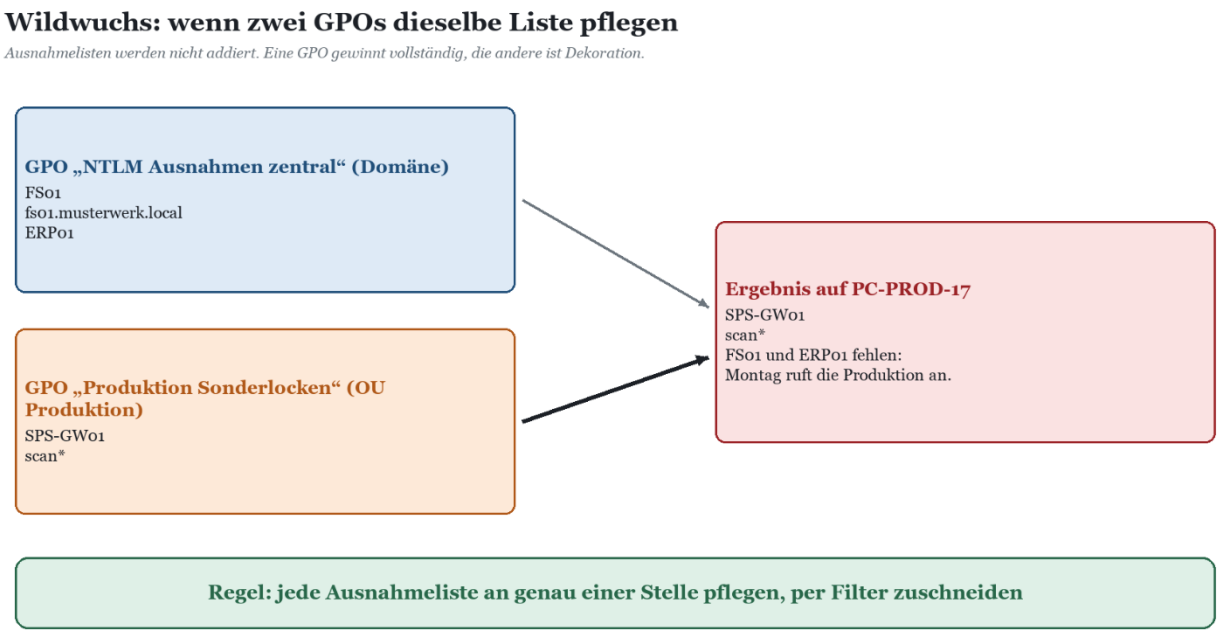
Was eng in der Praxis bedeutet

Stellschraube	Weit (vermeiden)	Eng (anstreben)
Richtlinie	Verweigern gar nicht einschalten	Verweigern ein, einzelne Ziele ausnehmen
Eintrag	* oder srv*	ERP01, erp01.musterwerk.local
Wirkungsbereich	GPO an der Domäne	GPO an der OU oder mit Sicherheitsfilter
Dauer	unbefristet	Ablaufdatum, Verlängerung nur mit Beleg
Pflegeort	mehrere GPOs mit eigenen Listen	eine GPO pro Liste und Zielgruppe
Begleitschutz	keiner	SMB-Signierung, Kanalbindung, erweiterter Schutz am Ziel

Der letzte Punkt wird gern vergessen: Ein Server, der weiter NTLM annimmt, sollte wenigstens gegen Relay geschützt sein. Wie das geht, beschreibt NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

Wildwuchs vermeiden: eine Liste, ein Pflegeort

Die Ausnahmelisten sind Sicherheitsoptionen. Konfigurieren zwei GPOs dieselbe Liste, werden die Einträge nicht zusammengeführt, sondern die GPO mit der höheren Priorität gewinnt vollständig. Das führt zu einem der hinterhältigsten Fehlerbilder der ganzen Ablösung.



Skizze: Gruppenrichtlinien-Rangfolge bei Sicherheitsoptionen, Namen fiktiv

Die Regel daraus: Jede Liste wird an genau einer Stelle gepflegt. Unterschiedliche Zielgruppen bekommen unterschiedliche GPOs, deren Wirkungsbereiche sich nicht überschneiden. Wer eine Liste ändert, prüft vorher mit gpresult auf einem Zielrechner, welche GPO dort tatsächlich gewinnt.

Dokumentation: Begründung, Verantwortlicher, Ablaufdatum

Die Gruppenrichtlinie kennt keine Kommentarspalte. In der Liste steht „LEGACY-APP01“ und sonst nichts. Alles, was diesen Eintrag später verständlich macht, muss deshalb woanders stehen: in einem Ausnahmeregister. Das kann eine Tabelle sein, ein Abschnitt im Wiki oder eine Kategorie im Ticketsystem. Hauptsache, es gibt genau eins, und jeder Eintrag in der GPO hat dort eine Zeile.

Die Pflichtfelder im Ausnahmeregister

Feld	Inhalt	Beispiel (Musterwerk GmbH)
Eintrag	exakter Text in der Liste	ERP01, erp01.musterwerk.local
Liste und GPO	welche Ausnahmeliste, welche GPO	Remoteserverausnahmen, GPO „NTLM Ausnahmen Clients“
Quelle	welche Geräte oder OU die Ausnahme brauchen	OU Buchhaltung, 14 Clients
Konto	Benutzer- oder Dienstkonto im Ereignis	svc-erp-client
Beleg	Ereignis-ID, Reason ID, Zeitraum	4020, Reason ID laut Befund, 01.09. bis 30.09.2026
Begründung	warum nicht behebbar	Client der ERP-Software nutzt fest NTLM
Verantwortlicher	eine Person, kein Team	Leitung Anwendungsbetrieb ERP
Ablaufdatum	festes Datum	31.03.2027
Ausweg	Ticket, Herstellertermin, Projekt	Update 7.2 mit Kerberos, Herstellerzusage Q1/2027
Letzte Überprüfung	Datum und Ergebnis	01.11.2026, weiter genutzt

TIPP · Ein Verantwortlicher ist eine Person

„IT“ ist kein Verantwortlicher, „Systemhaus“ auch nicht. Trag eine konkrete Person ein, die sagen

kann, ob die Ausnahme noch gebraucht wird, und die einen Anruf bekommt, wenn das Ablaufdatum naht. Bei Fachanwendungen ist das oft nicht die Administration, sondern die Leitung der Fachabteilung. Die Administration pflegt die Liste, die Fachabteilung verantwortet den Bedarf.

Ablaufdatum: die wichtigste Spalte

Ohne Ablaufdatum ist jede Ausnahme unbefristet, und unbefristete Übergangslösungen haben in der IT eine Lebenserwartung, von der Schildkröten nur träumen. Setze das Datum an einem echten Ereignis fest: dem zugesagten Update, dem Ende der Migration, dem Austausch des Geräts. Gibt es so ein Ereignis nicht, setz ein festes Datum für die nächste Überprüfung, höchstens sechs Monate in der Zukunft. Spätestens mit der nächsten Windows-Server-Version, die NTLM standardmäßig abschaltet, hast du ohnehin ein Ablaufdatum, ob es im Register steht oder nicht.

AUS DER PRAXIS · Sparfuchs & Partner: die Ausnahme, die keiner kannte

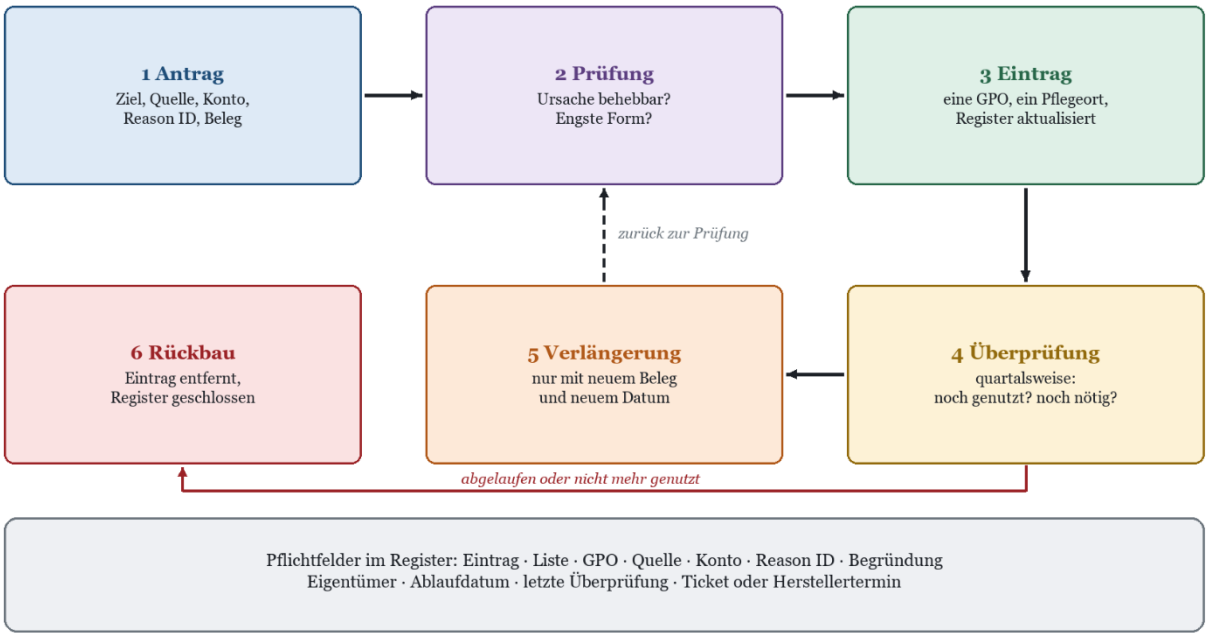
Bei der Sparfuchs & Partner Steuerberatungs GmbH stand in der Liste der DC-Serverausnahmen ein Eintrag „DMS*“. Begründung: keine. Verantwortlich: niemand. Bei der Aufräumaktion stellte sich heraus, dass der Stern drei Server traf, von denen zwei seit Jahren abgeschaltet waren und der dritte, der aktuelle Dokumentenserver, längst sauber per Kerberos angesprochen wurde. Der Eintrag stammte aus einer Migration 2019. Die Kanzlei hatte also jahrelang ein Fenster offen, durch das niemand mehr hereinkam, außer vielleicht jemand, der es nicht sollte.

Regelmäßige Überprüfung: Ausnahmen müssen sterben dürfen

Eine Ausnahmeliste ist kein Dokument, sondern ein Prozess. Sie braucht einen Rhythmus, in dem jeder Eintrag einmal auf den Prüfstand kommt. Bewährt hat sich ein Quartalstermin, an dem die Verantwortlichen zwei Fragen beantworten: Wird die Ausnahme noch genutzt? Wird sie noch gebraucht? Beides ist nicht dasselbe.

Der Lebenszyklus einer Ausnahme

Jede Ausnahme wird geboren, überprüft und stirbt. Die ohne Sterbedatum werden Denkmäler.



Skizze: Pflegeprozess für NTLM-Ausnahmen, Intervalle als Richtwert

Wird die Ausnahme noch genutzt?

Das beantwortet das Protokoll. Mit Bordmitteln heißt das: Ereignisse sammeln und nach dem Ziel filtern. Die erweiterten Ereignisse nennen das Ziel im Meldungstext, etwa als „Target Machine“, dazu „Reason ID“ und „NTLM Version“. Für einen einzelnen Server reicht eine Abfrage per PowerShell; für eine ganze Domäne brauchst du die Ereignisse zentral, etwa per Windows Event Forwarding, wie in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding beschrieben. Die passende Überwachungs-GPO legt das NTLM-Audit-GPO-Skript reproduzierbar an.

```
# Aktuelle Ausnahmelisten auf diesem Gerät auslesen
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0' `
  -Name ClientAllowedNTLMServers -ErrorAction SilentlyContinue
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters' `
  -Name DCAllowedNTLMServers -ErrorAction SilentlyContinue   # nur auf DCs

# NTLM-Ereignisse der letzten 30 Tage, die ein bestimmtes Ziel nennen
Get-WinEvent -FilterHashtable @{
  LogName   = 'Microsoft-Windows-NTLM/Operational'
  Id        = 4020, 4021, 8001
  StartTime = (Get-Date).AddDays(-30)
} | Where-Object { $_.Message -match 'ERP01' } |
  Group-Object Id | Select-Object Name, Count
```

Taucht ein Ziel im Messzeitraum gar nicht mehr auf, ist das ein starkes Indiz für den Rückbau. Ein Indiz, kein Beweis: Vielleicht lief der Monatsabschluss nicht im Zeitraum, vielleicht war der einzige Rechner, der das Ziel anspricht, drei Wochen im Urlaub. Bevor du streichst, prüfe deshalb die Abdeckung, also ob die relevanten Quellen im Zeitraum überhaupt Ereignisse geliefert haben.

> **WICHTIG · Ein leeres Protokoll ist keine Entwarnung**
>
> Stille kann bedeuten: kein NTLM mehr. Sie kann aber auch bedeuten: Protokoll übergelaufen, Weiterleitung kaputt, Gerät ausgeschaltet, Auditing nie angekommen. Microsoft weist bei der Domänenüberwachung ausdrücklich darauf hin, die Größe des Operational-Protokolls im Blick zu behalten. Prüf also immer zuerst, ob die Quelle liefert, bevor du ihr Schweigen interpretierst. Was auf DCs ankommt, beschreibt NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

Wird die Ausnahme noch gebraucht?

Das beantwortet nicht das Protokoll, sondern der Verantwortliche. Ist das Update inzwischen da? Ist der Dateiserver migriert? Hat der Hersteller geliefert oder vertröstet? Eine Verlängerung gibt es nur mit neuem Beleg und neuem Datum. Eine Ausnahme, deren Verantwortlicher nicht mehr im Haus ist, bekommt einen neuen oder wird zurückgebaut, nach einer Überwachungsphase mit dem Eintrag entfernt und dem Verweigern aktiv.

Rückbau ohne Montagsdrama

Der Rückbau ist der eigentliche Zweck jeder Ausnahme. Er folgt demselben Muster wie das Verweigern selbst: erst in einer Pilotgruppe, dann flächig, mit dokumentiertem Rückweg. Den gesamten Ablauf beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

Rhythmus	Was passiert	Wer
monatlich	Nutzung je Ausnahme aus dem Protokoll ziehen, Abdeckung prüfen	Administration
quartalsweise	Register durchgehen: genutzt, gebraucht, Datum aktuell?	Administration mit Verantwortlichen
bei Ablauf	Verlängerung mit Beleg oder Rückbau einleiten	Verantwortlicher

jährlich	Liste gegen Register abgleichen, verwaiste Einträge entfernen	IT-Leitung
bei jedem Release	Prüfen, was die neue Windows-Version am NTLM-Standard ändert	IT-Leitung

Wenn die Liste belegt sein soll, nicht geschätzt

Mit Bordmitteln kommst du bei einer kleinen Umgebung durch. Ab einer gewissen Größe kippt es: Tausende Ereignisse pro Tag, Hunderte Maschinen, von denen ein Teil keine erweiterten Ereignisse liefert, Geräte ohne Ereignisprotokoll, die nur im Netzwerkmitschnitt auftauchen, und zu jedem Ziel die Frage, ob die Ursache nicht doch behebbar wäre. Am Ende sitzt du vor einer Tabellenkalkulation mit 80 000 Zeilen und rätst, welche davon eine Ausnahme rechtfertigen.

Genau hier setzt der NTLM Diagnostiker an. Er liefert die belegte Liste der Ziele, die in deiner Umgebung tatsächlich noch NTLM brauchen, mit Quelle, Konto und Ursache. Damit trennt er die Fälle, die du beheben kannst, von denen, für die eine Ausnahme ehrlich ist. Und er zeigt, wo dein Messzeitraum Lücken hat, bevor du auf Basis dieser Lücken eine Ausnahme streichst.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Von der Ereignisflut zur belegten Ausnahmeliste

Der NTLM Diagnostiker arbeitet ausschließlich lesend. Er trägt keine Ausnahme ein, ändert keine Gruppenrichtlinie und keinen Registrierungswert. Er liefert die Belege, entscheiden tust du.

Ereignisse holt er direkt vom DC, über einen vorhandenen Windows Event Collector oder per Direktabfrage. Die Kommunikationsmatrix und die Konten-Sicht zeigen, welche Quelle mit welchem Ziel unter welchem Konto NTLM spricht. Das ist die Rohfassung deiner Ausnahmeliste, belegt statt geschätzt.

Die Ursachen-Engine mit SPN- und DNS-Prüfung sortiert aus, was gar keine Ausnahme braucht: fehlende oder doppelte SPNs, nicht auflösbare Namen, Zugriffe per IP-Adresse. Die NTLMv1-Hitliste zeigt, welche Ziele noch NTLMv1 bekommen, die Sicherheitsflaggen markieren riskante Kombinationen.

Abdeckungsmonitor und OS-Landkarte zeigen, welche Maschinen Ereignisse liefern und welche schweigen. So erkennst du, ob eine scheinbar ungenutzte Ausnahme wirklich ungenutzt ist. Für Geräte ohne Ereignisprotokoll gibt es den Wireshark-Import.

Die Readiness-Ampel und die Abschalt-Simulation zeigen, was bei aktivem Verweigern ausfallen würde, mit und ohne den Eintrag, den du gerade streichen willst.

Das Ergebnis geht als Word-Bericht an die IT-Leitung und als Excel/CSV-Export in dein Ausnahmeregister.

Ein automatischer Vorschlag für Ausnahmelisten, ein Ausnahmelisten- und Skript-Generator sowie ein Verlauf für den Vergleich zwischen zwei Messungen sind als Ausbaustufen geplant. Heute pflegst du die Liste selbst, aber auf Basis von Belegen.

Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund, der volle Umfang lässt sich sieben Tage testen. Lizenziert wird pro aktivem Computerkonto.

Bei der Trendforge Digital GmbH ergab der erste Lauf 23 Ziele mit NTLM-Verkehr. Die Administration hatte mit rund 20 Ausnahmen gerechnet. Nach der Ursachenprüfung blieben vier übrig: zwei Multifunktionsgeräte, eine Zeiterfassung mit fest eingebautem NTLM und ein Altsystem, dessen Abschaltung ohnehin geplant war. Die übrigen 19 waren SPN-Lücken, Laufwerkszuordnungen per IP-Adresse und ein vergessener Alias. Vier Ausnahmen mit Namen,

Verantwortlichem und Datum statt zwanzig Bauchgefühle: Das ist der Unterschied zwischen Fenster und Loch.

Wenn du Ausnahmen, Pflegeprozess und Rückbauplan mit Begleitung aufsetzen willst, hilft dir die Beratung zur NTLM-Ablösung. Wie die Ausnahmepflege in das Gesamtprojekt passt, beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand; für Systemhäuser mit vielen Kundenumgebungen lohnt NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen.

FAQ: NTLM-Ausnahmen

Wirkt eine Ausnahmeliste, wenn ich gar nicht verweigere?

Nein. Beide Listen greifen nur zusammen mit ihrer Verweigern-Richtlinie. Solange du nur überwachst, hat die Liste keine Wirkung. Sie wird aber in dem Moment aktiv, in dem du verweigerst, deshalb sollte sie schon vorher gepflegt sein.

Kann ich für eingehenden NTLM-Verkehr am Server eine Ausnahme eintragen?

Nein, die eingehende Richtlinie hat keine Ausnahmeliste. Einen Server nimmst du aus, indem du ihn aus dem Wirkungsbereich der Verweigern-GPO herausnimmst, etwa über eine eigene OU oder einen Sicherheitsfilter. Das gehört genauso ins Register wie ein Listeneintrag.

NetBIOS-Name oder FQDN?

Microsoft nennt den NetBIOS-Namen als Format. Bei den Remoteserverausnahmen zählt aber der Name, den die Anwendung tatsächlich verwendet. Ruft sie den FQDN oder einen Alias auf, gehört genau diese Schreibweise in die Liste. Im Zweifel trägst du beide ein und prüfst im Protokoll, welche greift.

Ist ein Platzhalter grundsätzlich verboten?

Nein, aber er braucht eine Begründung, die das Muster ausdrücklich nennt, und eine verbindliche Namenskonvention. Ein Stern allein ist tabu, er hebt das Verweigern faktisch auf.

Wie lange sollte eine Ausnahme höchstens gelten?

So lange wie das Ereignis, das sie beendet: Update, Migration, Gerätetausch. Fehlt ein solches Ereignis, setz eine Überprüfung nach spätestens sechs Monaten fest. Die nächste Windows-Server-Version mit standardmäßig abgeschaltetem NTLM ist ohnehin die natürliche Obergrenze.

Hilft eine Ausnahme auch gegen die NTLMv1-Blockade seit Oktober 2026?

Die Restrict-NTLM-Ausnahmelisten und die Blockade von NTLMv1 für Single Sign-on sind getrennte Mechanismen. Ein Eintrag in der Remoteserverliste hebt die NTLMv1-Blockade nicht auf. Wie BlockNtlmv1SSO arbeitet, steht in BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme.

Trägt der NTLM Diagnostiker die Ausnahmen für mich ein?

Nein. Er arbeitet ausschließlich lesend und liefert die belegte Liste der tatsächlich benötigten Ziele samt Ursache. Ein automatischer Vorschlag für Ausnahmelisten ist als Ausbaustufe geplant, aber heute nicht vorhanden.

Was hat Kerberos mit Ausnahmen zu tun?

Jede Ausnahme, die du zurückbaust, muss danach per Kerberos funktionieren. SPNs, DNS-Namen und Sichtverbindung zum DC entscheiden darüber. Hintergründe findest du im Kompetenzbereich Microsoft Kerberos.

Fazit: Fenster einbauen, nicht Löcher bohren

Ausnahmen sind kein Versagen der NTLM-Ablösung, sondern ihr Werkzeug. Sie erlauben dir, das Verweigern früh einzuschalten und den Rest gezielt offen zu lassen, statt die ganze Domäne zu schonen, weil ein Gerät noch nicht so weit ist. Gute Ausnahmen sind belegt, eng gefasst, an genau einer Stelle gepflegt, mit Begründung, Verantwortlichem und Ablaufdatum dokumentiert und werden regelmäßig überprüft. Schlechte Ausnahmen sind ein Stern, den keiner mehr erklären kann.

Die nächste Windows-Server-Version wird NTLM standardmäßig abschalten, ob deine Liste aufgeräumt ist oder nicht. Wer bis dahin jede Ausnahme kennt, verantwortet und befristet hat, erlebt den Umstieg als Termin im Kalender. Alle anderen erleben ihn als Überraschungsparty, nur ohne Kuchen. Wenn dein Team die Befunde selbst lesen und bewerten soll, hilft die Schulung zum NTLM Diagnostiker.

WEITERLESEN · Weiter in dieser Serie

› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen
› Reason-ID 6: wenn der Zielname nicht auflösbar ist
› Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen
› NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt