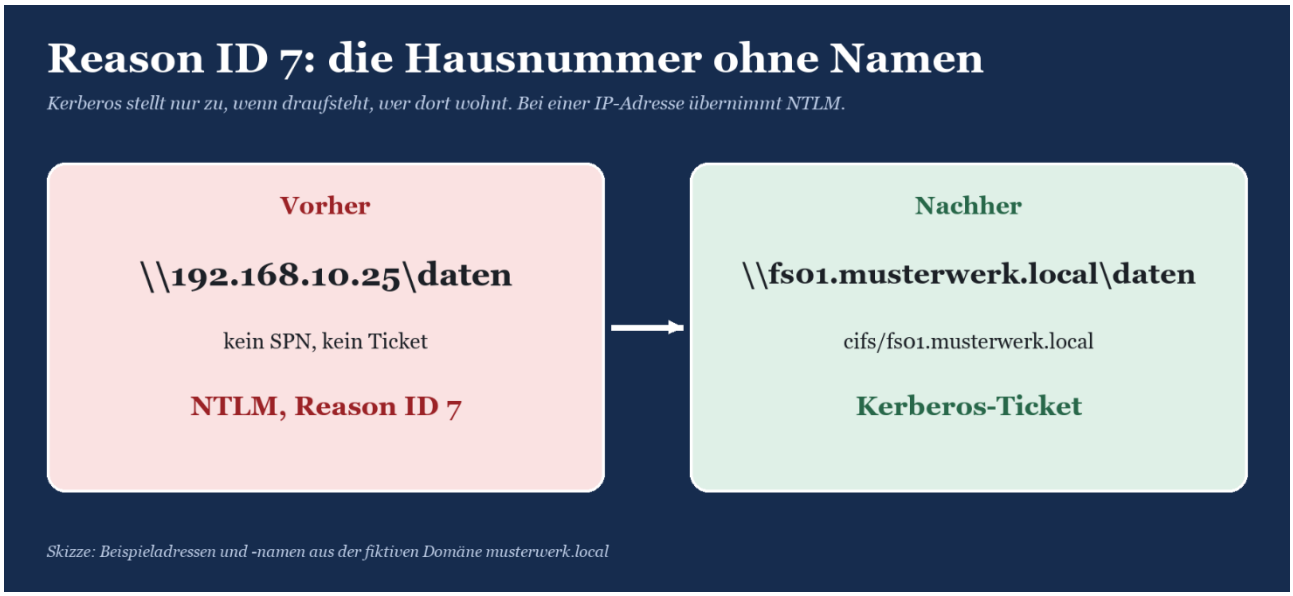
NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen



WISSEN
Was der NTLM Diagnostiker erfasst, wie er IP-Zugriffe findet und was er kostet.
› NTLM Diagnostiker

BERATUNG
IP-Zugriffe finden, Namen klären, Umstellung planen, ohne dass der Montag ausfällt.
› Beratung zur NTLM-Ablösung

SCHULUNG
Ereignisse lesen, Reason-IDs deuten, Skripte und GPOs durchsuchen: für dein ganzes Team.
› Schulung zum NTLM Diagnostiker

Es gibt in jeder Domäne diesen einen Satz, der irgendwann in einem Anmeldeskript gelandet ist und seitdem niemandem mehr aufgefallen ist: net use S: \\192.168.10.25\daten. Geschrieben vor zwölf Jahren, von jemandem, der längst in Rente ist, weil „das mit dem Namen damals nicht ging“. Seitdem läuft jede Anmeldung an dieser Freigabe über NTLM. Jeden Morgen, bei jedem Rechner, bei jedem Benutzer. Kerberos stand die ganze Zeit daneben und durfte nicht mitspielen.

Im erweiterten NTLM-Auditing hat dieses Muster eine eigene Nummer: Reason ID 7, „The target name contains an IP address.“ Neben fehlenden SPNs ist sie in der Praxis die häufigste Ursache, warum Windows nicht Kerberos benutzt. Und sie ist die dankbarste, denn die Lösung ist fast immer dieselbe: Die Adresse kommt raus, der DNS-Name kommt rein. Mühsam wird es nur beim Finden. Die Kombination ntlm ip adresse kerberos taucht eben nicht an einer Stelle auf, sondern an zwanzig.

Warum das jetzt drängt: 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. Eine IP-Adresse im Anmeldeskript ist dann kein Schönheitsfehler mehr, sondern ein Laufwerk, das am Stichtag einfach nicht mehr verbindet. Den ganzen Fahrplan findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

In diesem Beitrag erfährst du, warum Kerberos mit IP-Adressen nicht funktioniert, wo IP-Zugriffe typischerweise stecken, wie du sie mit Bordmitteln findest und wie du sie sauber auf DNS-Namen umstellst. Und, der Ehrlichkeit halber, ab wann das Suchen von Hand keinen Spaß mehr macht.

FAKTEN · Reason ID 7 auf einen Blick

Meldungstext laut Microsoft KB5064479: „The target name contains an IP address."

Fundort: Client-Ereignisse 4020 (Information) und 4021 (Warnung) im Protokoll Microsoft-Windows-NTLM/Operational, Abschnitt „NTLM Usage", Felder „Reason ID" und „Reason".

„Client" ist der Rechner, der zugreift. Das kann auch ein Server sein, etwa ein Anwendungsserver, der per IP auf eine Freigabe schreibt.

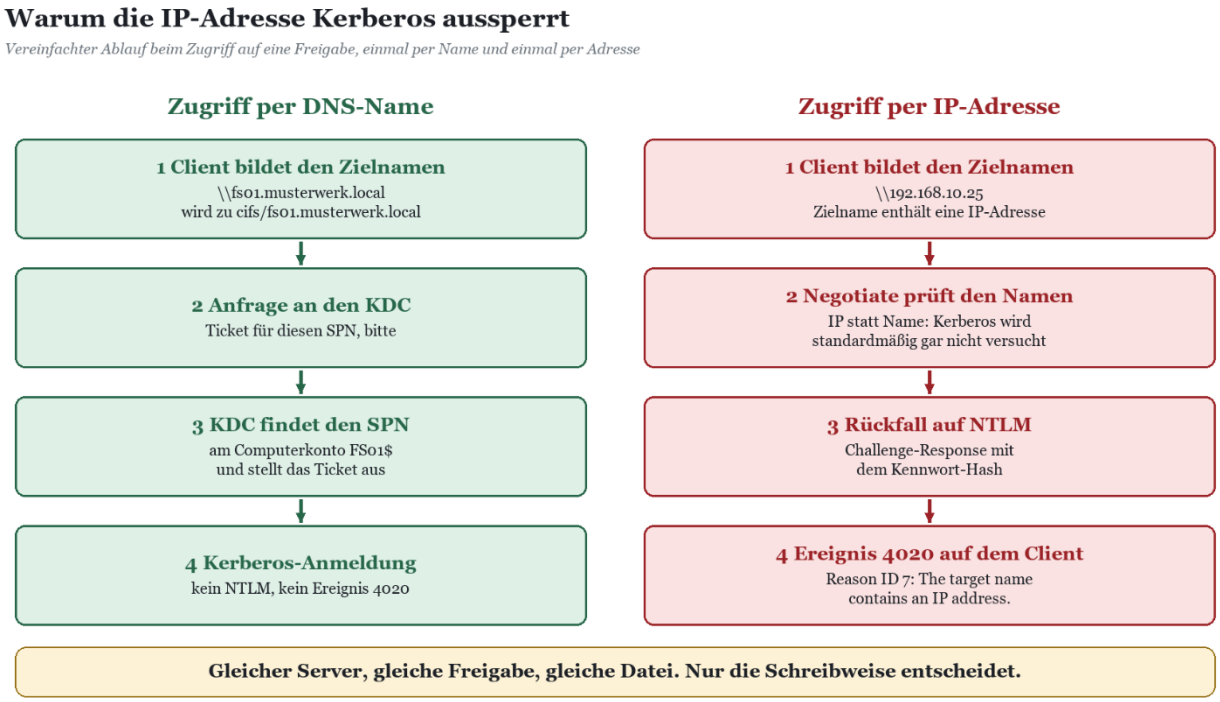
Systeme mit erweitertem Auditing: Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026.

Nicht sichtbar in den Server-Ereignissen 4022/4023, den DC-Ereignissen 4030 bis 4033 und den klassischen Restrict-NTLM-Ereignissen 8001 bis 8004. Die kennen keine Reason ID.

Warum Kerberos mit IP-Adressen nicht funktioniert

Kerberos ist ein Ticketsystem. Der Client bittet den Key Distribution Center auf dem Domain Controller um ein Ticket für einen bestimmten Dienst, und zwar über dessen Service Principal Name, kurz SPN. Für eine Dateifreigabe auf fs01.musterwerk.local heißt der SPN cifs/fs01.musterwerk.local. Der KDC sucht im Active Directory das Konto, an dem dieser SPN hängt, und verschlüsselt das Ticket mit dessen Schlüssel. Ohne passenden SPN weiß der KDC schlicht nicht, für wen er das Ticket ausstellen soll.

Eine IP-Adresse ist kein SPN. Windows-Computer registrieren beim Domänenbeitritt SPNs für ihren Kurznamen und ihren DNS-Namen, aber nicht für ihre Adressen. Und Windows versucht es standardmäßig gar nicht erst: Steht im Ziel eine IP-Adresse, verzichtet der Client auf Kerberos und nimmt direkt NTLM. Microsoft beschreibt das in Configuring Kerberos for IP Address ausdrücklich so. Das ergibt Sinn, denn Adressen wechseln, DHCP-Leases laufen ab, und ein Ticket an „wer auch immer gerade 192.168.10.25 hat" wäre eine schlechte Idee.



Skizze: didaktisch vereinfacht, ohne DNS-Abfragen und Sitzungsaufbau im Detail

So sieht Reason ID 7 im Ereignis aus

Damit du die Fälle überhaupt siehst, muss das erweiterte NTLM-Auditing laufen. Wie du es per Gruppenrichtlinie einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; das NTLM-Audit-GPO-Skript setzt die nötigen Einstellungen in einem Rutsch. Ein gekürztes Ereignis 4020 sieht dann ungefähr so aus:

```
Process Information:
    Process Name:        C:\Windows\explorer.exe
Client Information:
    Username:            m.mueller
    Domain:              MUSTERWERK
Target Information:
    Target Machine:      192.168.10.25
    Target Resource:     cifs/192.168.10.25
    Target IP:           192.168.10.25
NTLM Usage:
    Reason ID:           7
    Reason:              The target name contains an IP address.
```

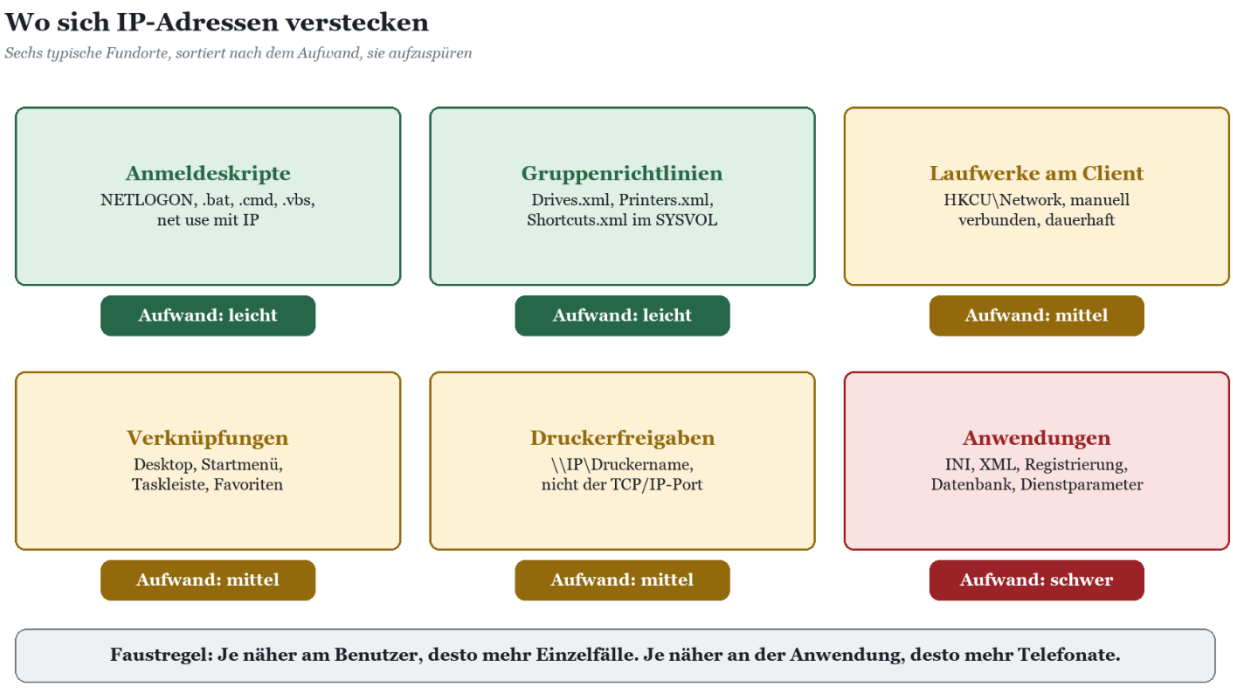
Drei Felder sind für dich wichtig. „Target Machine“ oder „Target IP“ liefert die Adresse, die du ersetzen musst. „Process Name“ verrät, wer die Adresse benutzt: explorer.exe deutet auf Laufwerke und Verknüpfungen, spoolsv.exe auf Drucker, alles andere meist auf eine Fachanwendung oder einen Dienst. Und „Username“ zeigt, ob es um einen Menschen oder ein Dienstkonto geht. Wie du die übrigen Felder liest, erklärt Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen, den Überblick über alle zwölf Gründe liefert NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

WARNUNG · Der Dateiserver weiß von nichts

Die Reason ID entsteht auf dem zugreifenden Rechner. Der Dateiserver protokolliert in 4022/4023 nur, dass NTLM ankommt, nicht warum. Wer ausschließlich Server- oder DC-Protokolle auswertet, sieht die Folgen von Reason ID 7, aber nie die Ursache. Was du auf der Serverseite siehst, beschreibt Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern.

Wo IP-Zugriffe in der Praxis stecken

IP-Adressen landen selten aus Bosheit in der Konfiguration, sondern aus Pragmatismus. DNS war kaputt, der Server hatte noch keinen Namen, der Dienstleister wollte schnell fertig werden. Das Provisorium hat dann, wie alle Provisorien, eine erstaunliche Lebenserwartung entwickelt.



Fundort	Typisches Beispiel	Prozess im Ereignis	So findest du es
Anmeldeskripte	net use S: \\192.168.10.25\daten	explorer.exe, svchost.exe	Volltextsuche in NETLOGON und SYSVOL
Gruppenrichtlinien-Einstellungen	Laufwerkszuordnung mit Pfad auf IP	explorer.exe	Drives.xml, Printers.xml, Shortcuts.xml im SYSVOL durchsuchen
Manuell verbundene Laufwerke	„Netzlaufwerk verbinden“ mit IP, dauerhaft	explorer.exe	HKCU\Network je Benutzer, Get-SmbMapping
Verknüpfungen	Desktop-Link auf \\10.20.1.8\scan	explorer.exe	.lnk-Dateien auslesen
Druckerfreigaben	\\192.168.10.30\Etage2	spoolsv.exe	Get-Printer, Printers.xml
Anwendungskonfigurationen	Ablagepfad, Datenbank oder Webdienst per IP	Fachanwendung, Dienst	INI, XML, Registrierung, Hersteller fragen
Geplante Aufgaben und Dienste	robocopy nach \\10.20.1.9\backup	robocopy.exe, Dienst	Get-ScheduledTask, Dienstparameter

Laufwerkszuordnungen und Anmeldeskripte

Der Klassiker und gleichzeitig der Hauptgewinn. Ein einziges Anmeldeskript, das bei jeder Anmeldung ein Laufwerk per IP verbindet, erzeugt bei 200 Benutzern jeden Morgen 200 NTLM-Anmeldungen, dazu jede Wiederverbindung nach Standby oder VPN. Typische Fundstellen sind Batch-Dateien in NETLOGON, VBScript-Relikte mit MapNetworkDrive, PowerShell mit New-PSDrive oder New-SmbMapping und Gruppenrichtlinien-Einstellungen unter „Laufwerkszuordnungen“. Bei Letzteren steckt der Pfad in der Datei Drives.xml im SYSVOL-Ordner der jeweiligen Richtlinie.

Dazu kommen Laufwerke, die Benutzer selbst verbunden haben. Windows merkt sich dauerhafte Verbindungen pro Benutzer unter HKCU\Network, jeweils mit dem Laufwerksbuchstaben als Schlüssel und dem Pfad im Wert RemotePath. Die tauchen in keinem Skript auf und überleben jede Bereinigung zentraler Richtlinien.

Verknüpfungen

Desktop-Verknüpfungen auf \\10.20.1.8\scan sind die Kakerlaken der IT: Du siehst eine, es gibt hundert. Sie liegen in Benutzerprofilen, im öffentlichen Desktop, im Startmenü, in angehefteten Taskleisten-Elementen und gern auch in den Schnellzugriff-Favoriten des Explorers. Manche verteilt eine Richtlinie (Shortcuts.xml), die meisten hat irgendwann jemand von Hand angelegt und per Profilkopie weitervererbt.

Anwendungskonfigurationen

Hier wird es zäh. Fachanwendungen speichern Ablagepfade, Exportverzeichnisse oder Datenbankverbindungen in INI- und XML-Dateien, in der Registrierung oder in ihrer eigenen Datenbank. Bei der Trendforge Digital GmbH stand der Pfad für Rechnungsexporte in einer Konfigurationstabelle der Warenwirtschaft, erreichbar nur über ein Admin-Menü, das niemand mehr kannte. Prozessname im Ereignis: die Anwendung selbst. Wenn sich der Pfad nicht ändern lässt oder die Anwendung zusätzlich NTLM fest eingebaut hat, hilft nur der Weg über den Hersteller; wie du ihn richtig fragst, steht in Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen.

Druckerfreigaben

Vorsicht mit vorschnellen Schlüssen: Ein Standard-TCP/IP-Port, der direkt auf die IP-Adresse eines Druckers zeigt, druckt ohne Windows-Anmeldung und erzeugt deshalb auch kein NTLM. Reason ID 7 entsteht, wenn ein Client eine Druckerfreigabe auf einem Druckserver über dessen Adresse verbindet, also \\192.168.10.30\Etage2 statt \\print01.musterwerk.local\Etage2. Im Ereignis steht dann meist spoolsv.exe als Prozess. Multifunktionsgeräte, die selbst per SMB auf Freigaben scannen, sind ein eigenes Kapitel, denn sie schreiben keine Ereignisse; mehr dazu in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

AUS DER PRAXIS · Sparfuchs & Partner: das Skript von 2014

Bei der Sparfuchs & Partner Steuerberatungs GmbH meldeten 64 Arbeitsplätze in einer Woche 23.800 Ereignisse mit Reason ID 7. Der Löwenanteil kam aus einem Anmeldeskript von 2014, das drei Laufwerke per IP verband, weil der Dateiserver damals bei einem Umzug kurzfristig keinen DNS-Eintrag hatte. Der Eintrag existiert seit neun Jahren. Das Skript auch. Zwei Zeilen geändert, am nächsten Morgen fehlten 19.000 Ereignisse.

IP-Zugriffe mit Bordmitteln finden

Du hast zwei Wege, die sich ergänzen: von den Ereignissen rückwärts zur Konfiguration, und von der Konfiguration vorwärts, ohne auf Ereignisse zu warten. Der erste findet, was tatsächlich passiert. Der zweite findet auch das, was nur einmal im Quartal passiert.

Schritt 1: Ereignisse mit Reason ID 7 auswerten

Das folgende Skript liest die Ereignisse 4020 und 4021 von einer Liste von Rechnern, filtert auf Reason ID 7, verdichtet nach Zieladresse und Prozess und versucht für jede Adresse eine DNS-Rückwärtsauflösung. Die Felder werden aus dem Meldungstext gezogen; auf deutschsprachigen Systemen prüfst du vorher an einem echten Ereignis, ob die Beschriftungen übersetzt sind.

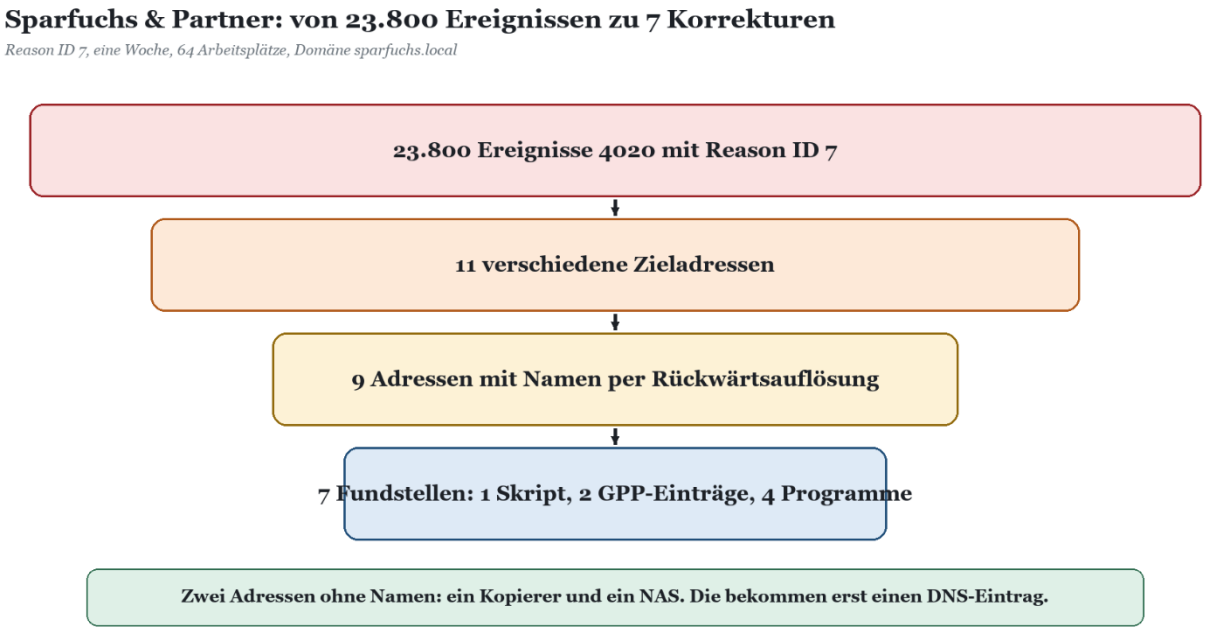
```
$felder = 'Process Name','Username','Target Machine','Target IP','Reason ID'
$ev = foreach ($c in Get-Content .\rechner.txt) {
```

```
  Get-WinEvent -ComputerName $c -ErrorAction SilentlyContinue -FilterHashtable @{
    LogName='Microsoft-Windows-NTLM/Operational'; Id=4020,4021
    StartTime=(Get-Date).AddDays(-7) } | ForEach-Object {
      $o = [ordered]@{ Rechner=$_.MachineName }
      foreach ($f in $felder) {
        if ($_.Message -match ('(?m)^\s*' + [regex]::Escape($f) + ':\s*([^\r\n]+)')) {
          $o[$f] = $Matches[1].Trim() } }
      [pscustomobject]$o }
}

# Nur Reason ID 7, verdichtet nach Ziel und Prozess
$ip7 = $ev | Where-Object { $_.'Reason ID' -eq '7' } |
  Group-Object 'Target Machine','Process Name' | Sort-Object Count -Descending

# Je Zieladresse einmal rückwärts auflösen
$ip7 | ForEach-Object {
  $ip  = ($_.Name -split ',')[0].Trim()
  $ptr = Resolve-DnsName $ip -Type PTR -ErrorAction SilentlyContinue | Select-Object -First 1
  [pscustomobject]@{ Anzahl=$_.Count; Ziel=$_.Name; Name=$ptr.NameHost;
                     Rechner=($_.Group.Rechner | Sort-Object -Unique).Count }
} | Format-Table -AutoSize
```

Damit hast du die Arbeitsliste: welche Adresse, welcher Prozess, wie viele Rechner, und im besten Fall gleich der Name. Für mehr als eine Handvoll Rechner holst du die Ereignisse nicht per Fernabfrage, sondern über einen Collector; wie das geht, steht in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.



Skizze: Zahlen eines fiktiven Beispiels

Schritt 2: Skripte und Gruppenrichtlinien durchsuchen

Der zweite Weg kommt ohne Ereignisse aus. Anmeldeskripte und Gruppenrichtlinien-Einstellungen liegen als Textdateien im SYSVOL, also lässt sich alles mit einem regulären Ausdruck nach UNC-Pfaden mit IPv4-Adresse durchsuchen. Das findet auch Laufwerke, die nur eine Abteilung einmal im Monat benutzt.

```
$muster = '\\\\(\d{1,3}\.){3}\d{1,3}'
$sysvol = '\\musterwerk.local\SYSVOL\musterwerk.local'

# Skripte, Batch-Dateien und GPP-XML (Drives, Printers, Shortcuts, ScheduledTasks)
Get-ChildItem $sysvol -Recurse -File -ErrorAction SilentlyContinue `
  -Include *.bat,*.cmd,*.vbs,*.ps1,*.kix,*.xml,*.ini |
```

```
  Select-String -Pattern $muster |
  Select-Object Path, LineNumber, Line | Export-Csv .\ip-fundstellen.csv -Delimiter ';' -
Encoding UTF8
```

Die Pfade in der Ergebnisliste enthalten die GUID der Richtlinie. Den Klarnamen holst du dir mit Get-GPO -Guid aus dem Modul GroupPolicy. Denk auch an Skripte, die nicht im SYSVOL liegen: auf Dateiservern, in Softwareverteilungspaketen, in der Aufgabenplanung einzelner Server.

Schritt 3: Clients durchsuchen

Manuell verbundene Laufwerke, Verknüpfungen und Drucker stehen auf den Clients. Das folgende Skript läuft im Kontext des angemeldeten Benutzers, etwa als einmaliges Anmeldeskript oder über deine Softwareverteilung, und schreibt die Treffer in eine zentrale Ablage.

```
$muster = '\\\\(\d{1,3}\.){3}\d{1,3}'
$treffer = @()

# Dauerhafte Laufwerke des Benutzers
Get-ChildItem HKCU:\Network -ErrorAction SilentlyContinue | ForEach-Object {
  $p = (Get-ItemProperty $_.PSPath).RemotePath
  if ($p -match $muster) { $treffer += [pscustomobject]@{ Art='Laufwerk'; Ort=$_.PSChildName;
Ziel=$p } } }

# Verknüpfungen auf Desktop, öffentlichem Desktop und im Startmenü
$sh = New-Object -ComObject WScript.Shell
$orte = [Environment]::GetFolderPath('Desktop'), "$env:PUBLIC\Desktop",
"$env:APPDATA\Microsoft\Windows\Start Menu"
Get-ChildItem $orte -Filter *.lnk -Recurse -ErrorAction SilentlyContinue | ForEach-Object {
  $l = $sh.CreateShortcut($_.FullName)
  if ("$($l.TargetPath) $($l.Arguments) $($l.WorkingDirectory)" -match $muster) {
    $treffer += [pscustomobject]@{ Art='Verknüpfung'; Ort=$_.FullName; Ziel=$l.TargetPath } } }

# Druckerverbindungen über Freigaben
Get-Printer | Where-Object { $_.Name -match $muster } | ForEach-Object {
  $treffer += [pscustomobject]@{ Art='Drucker'; Ort=$_.Name; Ziel=$_.Name } }

$treffer | Export-Csv \\fs01.musterwerk.local\inventar$\ip-$env:COMPUTERNAME-$env:USERNAME.csv
`
  -Delimiter ';' -Encoding UTF8 -NoTypeInformation
```

> **TIPP · Erst die Ereignisse, dann die Konfiguration**
>
> Beginne mit der Ereignisauswertung. Sie sagt dir, welche Adressen tatsächlich benutzt werden und wie oft. Die Konfigurationssuche ist dann die Gegenprobe: Sie findet die seltenen Fälle und zeigt dir die Stelle, an der du ändern musst. Wer nur in Skripten sucht, korrigiert womöglich tote Zeilen und übersieht die Fachanwendung.

Wo die Handarbeit kippt

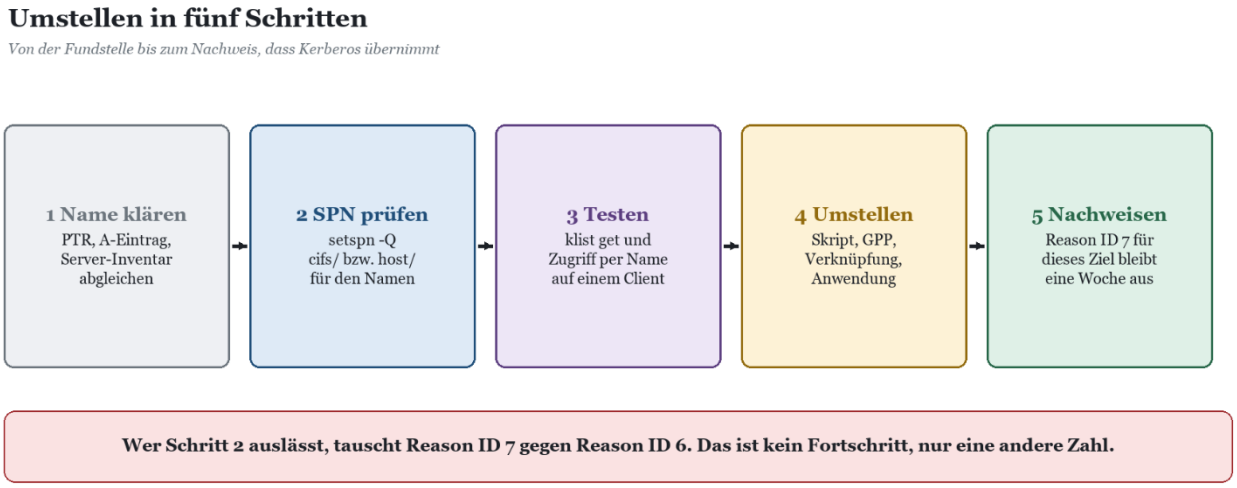
- **Masse.** Bei der Musterwerk GmbH lieferten 420 Clients in einer Woche knapp 24.000 Ereignisse mit Reason ID 7. Die Fernabfrage mit Meldungstext dauert, und Rechner, die gerade aus sind, fehlen still.
- **Lücken.** Ein Skript sagt dir, was es gefunden hat, nicht, welche Rechner nicht geantwortet haben oder gar nicht auditieren können, weil ihr Windows zu alt ist.
- **Rückwärtsauflösung.** PTR-Einträge fehlen in vielen Umgebungen, sind veraltet oder zeigen auf einen Namen, für den kein SPN existiert. Dann musst du jede Adresse einzeln nachrecherchieren.

- **Zuordnung.** Vom Ereignis zur Fundstelle ist es ein Sprung: Die Adresse kennst du, aber ob sie aus dem Skript, der GPP, einer Verknüpfung oder der Anwendung kommt, verrät erst der Prozess, und auch der nur ungefähr.
- **Nachweis.** Nach der Umstellung willst du sehen, dass die Ereignisse für dieses Ziel verschwinden. Also alles nochmal, nächste Woche.

Für eine Kanzlei mit 30 Rechnern reicht das Skript, und du lernst dabei viel über deine Umgebung. Bei ein paar Hundert Maschinen wird aus der Suche ein Dauerprojekt. Einen ehrlichen Vergleich, wann Bordmittel genügen, findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

Auf DNS-Namen umstellen, ohne dass etwas ausfällt

Das Umstellen selbst ist technisch banal. Die Kunst liegt darin, den richtigen Namen zu wählen und vorher zu prüfen, dass Kerberos mit diesem Namen auch wirklich funktioniert. Sonst tauschst du nur eine Reason-ID gegen die nächste.



Skizze: eigenes Vorgehensmodell

Den richtigen Namen finden

Die Rückwärtsauflösung ist ein guter Startpunkt, aber kein Beweis. Prüfe den gefundenen Namen in beide Richtungen: Löst er vorwärts wieder auf genau diese Adresse auf? Ist es der Name des Computerkontos oder ein Alias? Nimm bevorzugt den vollqualifizierten Namen, also fs01.musterwerk.local statt fs01. Kerberos funktioniert zwar auch mit dem Kurznamen, weil Windows beide SPN-Varianten am Computerkonto registriert, aber der FQDN ist eindeutig und unabhängig von DNS-Suffixlisten.

Willst du einen Alias wie daten.musterwerk.local verwenden, damit ein späterer Serverumzug nur den DNS-Eintrag betrifft, ist das eine gute Idee, mit einer Bedingung: Für den Alias muss ein SPN am richtigen Konto registriert sein. Fehlt er, wird aus Reason ID 7 eine Reason ID 6. Wie du das vermeidest, steht in Reason-ID 6: wenn der Zielname nicht auflösbar ist; und wenn derselbe SPN versehentlich an zwei Konten hängt, hilft Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten.

```
# Vorwärts und rückwärts prüfen
Resolve-DnsName 192.168.10.25 -Type PTR
Resolve-DnsName fs01.musterwerk.local

# Gibt es den SPN, und an welchem Konto?
setspn -Q cifs/fs01.musterwerk.local
```

```
setspn -Q host/fs01.musterwerk.local

# Probe auf einem Client: Ticket holen, dann Zugriff
klist get cifs/fs01.musterwerk.local
Test-Path \\fs01.musterwerk.local\daten
```

Bei Dateifreigaben genügt in der Regel der host-SPN am Computerkonto, weil der KDC cifs darauf abbildet. Liefert klist get ein Ticket, bist du auf der sicheren Seite. Mehr zu SPNs, Tickets und Delegierung findest du im Kompetenzbereich Microsoft Kerberos.

Vorher und nachher

Fundort	Vorher	Nachher	Worauf du achtest
Anmeldeskript	net use S: \\192.168.10.25\daten	net use S: \\fs01.musterwerk.local\daten	alte Verbindung vorher mit net use S: /delete trennen
GPP-Laufwerk	Pfad \\192.168.10.25\daten, Aktion Erstellen	Pfad \\fs01.musterwerk.local\daten, Aktion Ersetzen	„Ersetzen“ trennt das alte Laufwerk und verbindet neu
Verknüpfung	\\10.20.1.8\scan	\\scan01.musterwerk.local\scan	per GPP neu verteilen, alte Links aktiv löschen
Druckerfreigabe	\\192.168.10.30\Etage2	\\print01.musterwerk.local\Etage2	Drucker per GPP oder Skript neu verbinden, alten entfernen
Anwendung	Exportpfad 10.20.1.9	Exportpfad app01.musterwerk.local	Hersteller einbeziehen, Änderung testen
Geplante Aufgabe	robocopy D:\ \\10.20.1.9\backup	robocopy D:\ \\nas01.musterwerk.local\backup	Ziel muss Kerberos können, sonst Reason ID 6

Schrittweise umstellen und nachweisen

Stelle nicht alles an einem Freitagnachmittag um. Fang mit dem Fundort an, der die meisten Ereignisse erzeugt, teste ihn mit einer Pilotgruppe und rolle ihn dann aus. Danach schaust du eine Woche lang, ob Reason ID 7 für diese Adresse aus den Ereignissen verschwindet. Bleiben Reste, hast du eine Fundstelle übersehen: meist ein manuell verbundenes Laufwerk oder eine Verknüpfung, die jemand auf seinen neuen Rechner kopiert hat. Wie du aus vielen kleinen Korrekturen eine geordnete Abschaltung machst, beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

WARNUNG · Gerät ohne Domänenmitgliedschaft? Dann hilft der Name allein nicht

Ein NAS oder Multifunktionsgerät, das nicht Mitglied der Domäne ist, hat kein Computerkonto und damit keinen SPN. Ein DNS-Name ändert daran nichts: Aus Reason ID 7 wird Reason ID 6, und NTLM bleibt. Kläre vorher, ob das Gerät Kerberos überhaupt beherrscht. Wenn nicht, gehört es auf die Ausnahmeliste, bis es ersetzt ist; wie du die pflegst, steht in Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

Sonderfall: SPN mit IP-Adresse

Seit Windows 10 Version 1507 und Windows Server 2016 können Kerberos-Clients so konfiguriert werden, dass sie auch für IP-Adressen ein Ticket anfordern. Dafür setzt du auf jedem betroffenen Client den Registrierungswert TryIPSPN (DWORD, 1) unter HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters

und registrierst am Zielkonto einen SPN mit der Adresse, etwa setspn -s host/192.168.10.25 fs01. Microsoft beschreibt das in Configuring Kerberos for IP Address.

WICHTIG · Notausgang, kein Standardweg

Microsoft selbst empfiehlt IP-SPNs nur, wenn sich die Umstellung auf einen DNS-Namen nicht realisieren lässt, etwa bei einer Anwendung, die die Adresse fest einkompiliert hat. Du baust dir damit eine Abhängigkeit von einer festen Adresse ein: Wechselt sie, zeigt der SPN ins Leere oder auf das falsche Konto, und ein SPN kann nur an einem Konto hängen. Dazu kommt eine Registrierungseinstellung auf jedem Client, die jemand dokumentieren und pflegen muss. Nutze den Weg für einzelne, begründete Ausnahmen mit fester Adresse, nicht als Abkürzung für das Anmeldeskript.

Reason ID 7 im großen Maßstab: der NTLM Diagnostiker

Die Bordmittel-Strecke funktioniert, solange die Umgebung überschaubar ist. Bei Hunderten Rechnern, lückenhaften PTR-Einträgen und Geräten, die nie etwas protokollieren, wird sie zur Fleißarbeit. Dafür haben wir den NTLM Diagnostiker gebaut. Er findet die Zugriffe mit Reason ID 7, verdichtet sie nach Zieladresse und nennt per DNS-Rückwärtsauflösung gleich den Namen mit, auf den du umstellen solltest. Die SPN-Prüfung sagt dir dazu, ob Kerberos mit diesem Namen auch tatsächlich funktionieren wird, bevor du das Skript anfasst.

Wichtig für deinen Änderungsprozess: Der Diagnostiker arbeitet ausschließlich lesend. Er ändert kein Skript, keine Gruppenrichtlinie, keinen DNS-Eintrag und keinen SPN. Er liefert dir die Liste, die Umstellung bleibt in deiner Hand.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Von der IP-Adresse zum richtigen Namen

Ereignisquellen: direkt vom Domain Controller, von einem vorhandenen Windows Event Collector oder per Direktabfrage einzelner Rechner. Für Reason ID 7 brauchst du die Client-Ereignisse 4020 und 4021, also den Collector oder die Direktabfrage.

Ursachen-Engine mit SPN- und DNS-Prüfung: ordnet jedes Ereignis seiner Reason ID zu, fasst die IP-Zugriffe nach Zieladresse zusammen, löst die Adresse rückwärts auf und prüft, ob für den gefundenen Namen ein passender SPN existiert.

Kommunikationsmatrix und Konten-Sicht: zeigen, welche Rechner und Konten eine Adresse benutzen. So erkennst du, ob es um ein Anmeldeskript für alle oder um einen einzelnen Dienst geht.

Abdeckungsmonitor und OS-Landkarte: zeigen, welche Rechner Ereignisse liefern, welche schweigen und welche Windows-Versionen das erweiterte Auditing überhaupt beherrschen.

Stille Geräte: Für NAS, Scanner und Drucker ohne eigenes Protokoll importierst du einen Wireshark-Mitschnitt.

Einordnen und berichten: Readiness-Ampel für den Gesamtstand, Abschalt-Simulation für die Frage, welche Zugriffe am Stichtag ausfallen würden, Word-Bericht für die IT-Leitung, Excel- oder CSV-Export als Arbeitsliste für die Umstellung.

Editionen: Express ist kostenlos und liefert den Fünf-Minuten-Befund, die Vollversion testest du 7 Tage, lizenziert wird pro aktivem Computerkonto. Ein Skript-Generator und ein Verlauf zum Nachweis der Umstellung sind geplant, aber noch nicht enthalten.

› NTLM Diagnostiker

Wenn du die Fundstellen lieber gemeinsam mit jemandem durchgehst, der schon ein paar Hundert Anmeldeskripte entrümpelt hat, gibt es die Beratung zur NTLM-Ablösung. Betreust du als Systemhaus mehrere Kunden, lohnt ein Blick in NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen, und wenn dein Team die Auswertung künftig selbst fahren soll, ist die Schulung zum NTLM Diagnostiker der kürzere Weg.

FAQ: NTLM wegen IP-Adresse

Warum benutzt Windows bei einer IP-Adresse kein Kerberos?

Weil Kerberos-Tickets für Service Principal Names ausgestellt werden und Windows für Adressen standardmäßig keine SPNs registriert. Ohne SPN kein Ticket, also fällt der Client auf NTLM zurück und protokolliert Reason ID 7.

Funktioniert der Kurzname statt des FQDN?

Meistens ja, weil Windows am Computerkonto SPNs für beide Varianten registriert. Der FQDN ist trotzdem die bessere Wahl, weil er unabhängig von DNS-Suffixlisten eindeutig ist.

Was ist mit IPv6-Adressen?

Für sie gilt dasselbe: Eine Adresse ist kein Name. Die Suchmuster in diesem Beitrag erfassen nur IPv4; wenn bei dir IPv6-Literale in Pfaden vorkommen, erweitere den regulären Ausdruck entsprechend.

Erzeugt jeder Netzwerkdrucker mit IP-Port Reason ID 7?

Nein. Ein Standard-TCP/IP-Port auf die Druckeradresse druckt ohne Windows-Anmeldung. Relevant sind Druckerfreigaben, die über die Adresse eines Druckservers verbunden werden.

Ich habe umgestellt, jetzt sehe ich Reason ID 6. Was ist passiert?

Der neue Name löst auf, aber der KDC findet keinen passenden SPN. Typisch bei DNS-Aliasen ohne SPN oder bei Geräten, die nicht Mitglied der Domäne sind. Prüfe mit setspn -Q und klist get.

Soll ich einfach TryIPSPN überall setzen?

Nein. IP-SPNs sind laut Microsoft für Fälle gedacht, in denen sich ein DNS-Name nicht verwenden lässt. Als Pauschallösung schaffst du dir Abhängigkeiten von festen Adressen und eine Einstellung, die jemand dauerhaft pflegen muss.

Wo finde ich die offizielle Beschreibung der Reason-IDs?

In der Microsoft-Dokumentation Overview of NTLM auditing enhancements in Windows 11, version 24H2 and Windows Server 2025. Dort stehen auch die Ereignisse und Systemvoraussetzungen.

Braucht der NTLM Diagnostiker Schreibrechte?

Nein. Er arbeitet ausschließlich lesend und ändert weder Skripte noch Gruppenrichtlinien, DNS oder SPNs.

Fazit: Gib deinen Servern ihre Namen zurück

Reason ID 7 ist die Ursache, die du am ehesten loswirst. Kerberos verweigert IP-Adressen aus gutem Grund, und die Abhilfe ist fast immer dieselbe: Adresse raus, DNS-Name rein. Die Arbeit liegt im Finden, denn die Adressen verstecken sich in Anmeldeskripten, Gruppenrichtlinien, manuell verbundenen Laufwerken, Verknüpfungen, Druckerfreigaben und Fachanwendungen. Wer von den Ereignissen aus sucht und mit einer Durchsuchung von SYSVOL und Clients gegenprüft, findet die meisten Fälle.

Prüf vor jeder Umstellung, ob der neue Name einen SPN hat, sonst feierst du den Abschied von Reason ID 7 mit der Begrüßung von Reason ID 6. Für die wenigen Fälle mit fest verdrahteter Adresse gibt es IP-SPNs als Notausgang. Und für alles andere gilt: Das Skript von 2014 hat lange genug durchgehalten. Es darf jetzt in Rente, bevor die nächste Windows-Server-Version es mit Gewalt hineinschickt.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› Reason-ID 6: wenn der Zielname nicht auflösbar ist
› Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten
› Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM-Nutzung ermitteln: der komplette Leitfaden