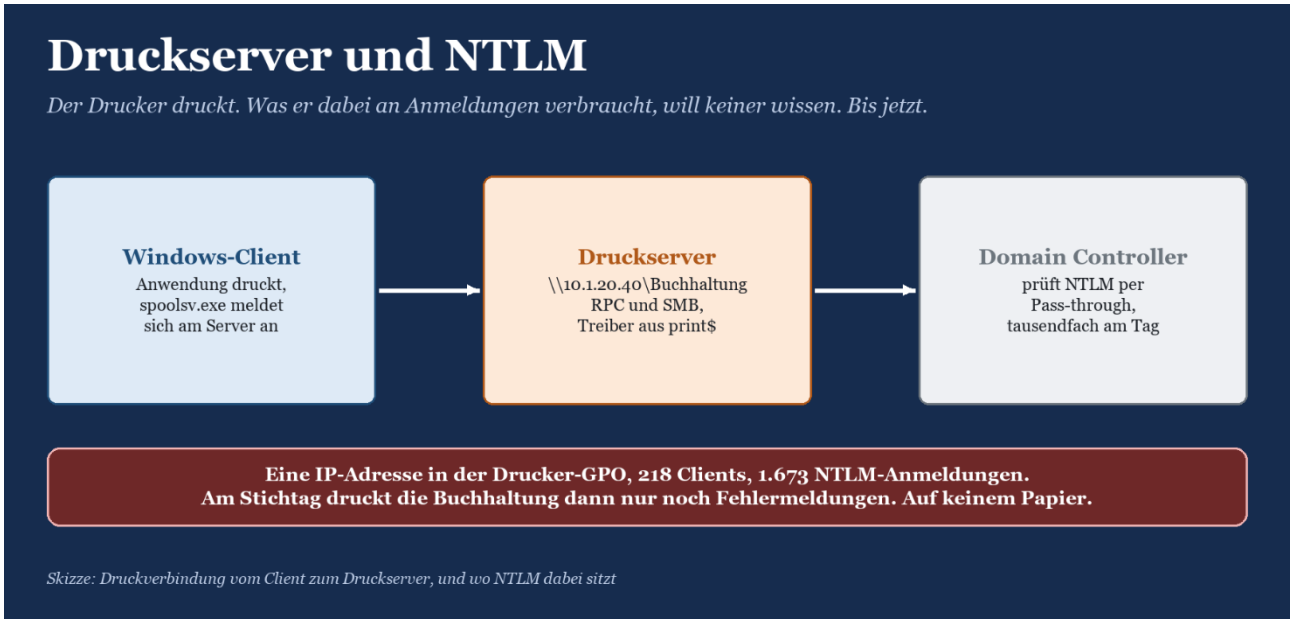
Druckserver und Point-and-Print: NTLM beim Drucken



WISSEN

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

› **NTLM Diagnostiker**

BERATUNG

Druckserver, Drucker-GPOs und Warteschlangen gemeinsam NTLM-frei machen: Wir planen das mit dir.

› **Beratung zur NTLM-Ablösung**

SCHULUNG

Ereignisse lesen, Verursacher wie spoolsv.exe einordnen, Ausnahmen begründen: praxisnah für dein Team.

› **Schulung zum NTLM Diagnostiker**

Drucken ist die Disziplin, in der die IT seit vierzig Jahren verlässlich verliert. Toner, Papierstau, Treiber, PrintNightmare: Wer einen Druckserver betreut, hat gelernt, nichts anzufassen, was gerade läuft. Genau deshalb steht in vielen Drucker-GPOs noch eine IP-Adresse aus dem Jahr 2015, der Druckserver heißt seit zwei Migrationen per CNAME „druck“, und auf einigen Arbeitsplätzen hängt ein freigegebener Etikettendrucker, den die halbe Versandabteilung mitbenutzt. Das alles funktioniert. Es funktioniert nur leider fast vollständig über NTLM.

In diesem Beitrag zum Thema druckserver ntlm geht es darum, warum im NTLM-Protokoll so oft spoolsv.exe als Verursacher auftaucht, welche Konstellationen in Druckumgebungen NTLM auslösen, wie die Point-and-Print-Härtung seit PrintNightmare dazu passt (und wie wenig), wie du die Druck-NTLM mit Bordmitteln findest und wie du sie loswirst: mit Namen statt IP-Adressen, sauberen SPNs, Kerberos für den Druck-RPC und, wo es passt, Universal Print. Wie du NTLM-Nutzung grundsätzlich erfasst, steht in NTLM-Nutzung ermitteln: der komplette Leitfaden; hier bleiben wir beim Drucken.

FAKTEN · Das Wichtigste in Kürze

Am Druckserver meldet sich nicht die Anwendung an, sondern der lokale Druckspooler des Clients. In den ausgehenden NTLM-Ereignissen 4020/4021 und 8001 steht deshalb als Prozess spoolsv.exe.

Die häufigsten Ursachen: Druckerfreigaben per IP-Adresse, Aliasnamen ohne passenden SPN, alte Verbindungen, die nach einer Migration auf den Clients liegen bleiben, und freigegebene Drucker auf Arbeitsplätzen.

Die Point-and-Print-Härtung seit August 2021 regelt, wer Druckertreiber installieren darf. An der

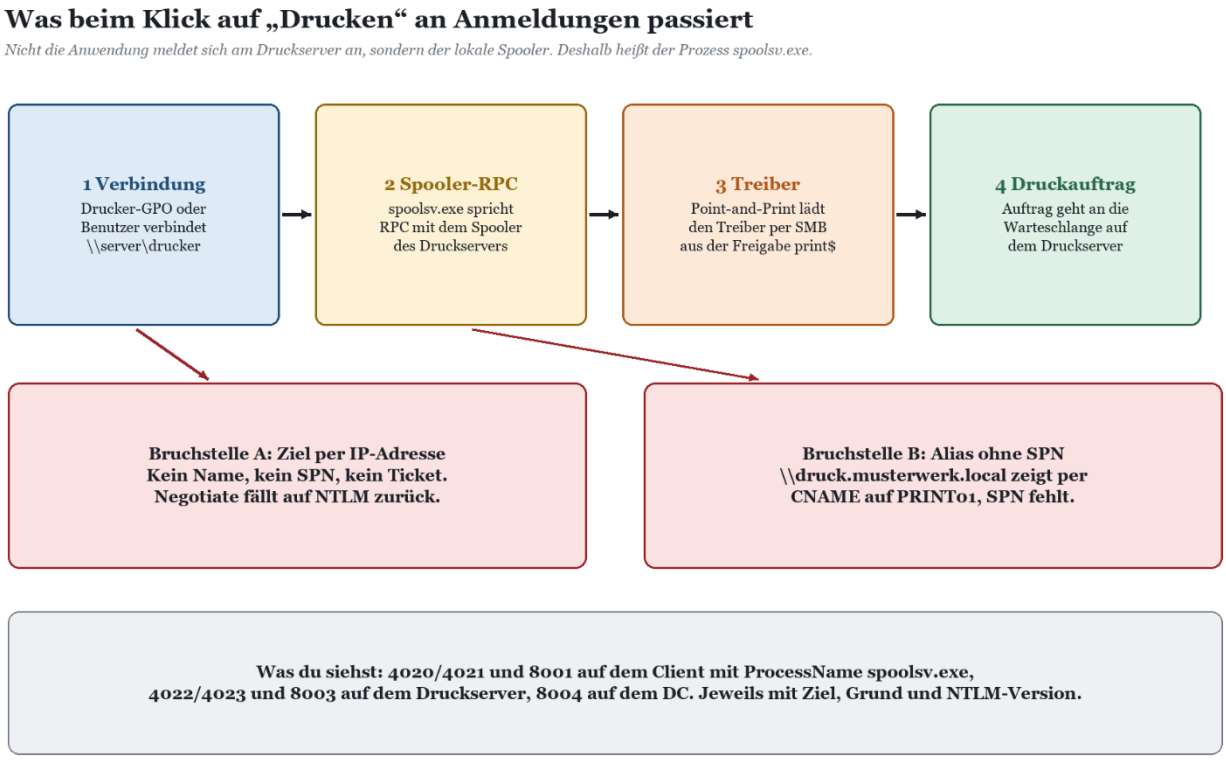
Frage NTLM oder Kerberos ändert sie nichts.

Ab Windows 11 22H2 läuft der Druck-RPC standardmäßig über TCP. Auf dem Druckserver lässt sich per Richtlinie festlegen, dass eingehende Druck-RPC-Verbindungen Kerberos verwenden müssen.

Universal Print kommt ganz ohne Druckserver im eigenen Netz aus. Auf diesem Weg gibt es keine Spooler-Verbindung zum Server und damit auch kein NTLM.

Warum der Druckserver NTLM spricht: spoolsv.exe, RPC und SMB

Eine Druckerverbindung zu \\print01\Buchhaltung besteht aus mehr als einer Anmeldung. Der Spooler des Clients spricht per RPC mit dem Spooler des Druckservers, fragt die Warteschlange und die Treiberinformationen ab und lädt bei Bedarf den Treiber über SMB aus der Freigabe print$. Jede dieser Verbindungen authentifiziert sich per Negotiate. Kerberos gewinnt dabei nur, wenn der Client zum Zielnamen einen passenden SPN findet. Findet er keinen, nimmt Negotiate NTLM, und zwar ohne dass irgendjemand eine Fehlermeldung zu sehen bekommt. Gedruckt wird ja trotzdem.



Skizze: Verbindung zu einem freigegebenen Drucker, vereinfacht; Beispielnamen der Musterwerk GmbH

Wer da eigentlich anmeldet

Wenn du auf einem Client die ausgehenden NTLM-Ereignisse auswertest, wirst du explorer.exe für Dateifreigaben finden, msedge.exe für Intranetseiten und eben spoolsv.exe für alles, was mit Druckern zu tun hat. Das liegt daran, dass die Druckerverbindung im Kontext des Spoolers aufgebaut wird, auch wenn der Benutzer sie ausgelöst hat. Im Feld Username steht dabei meist trotzdem der angemeldete Benutzer, im Feld TargetMachine der Druckserver, wie der Client ihn aufgerufen hat. Und genau dieses Feld ist der Schlüssel: Steht dort eine IP-Adresse oder ein Aliasname, hast du die Ursache in aller Regel schon gefunden.

Die Gründe, warum Windows nicht Kerberos benutzt hat, stehen im Feld NtlmUsageReason. Maßgeblich ist der Begründungstext, nicht die Nummer in NtlmUsageId: Nummer und Text

passen in der Praxis nicht immer zur Liste von Microsoft. Mehr dazu in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

Die üblichen Verdächtigen in der Druckumgebung

Konstellation	Was passiert	Typischer Befund
Drucker-GPO mit IP-Adresse	\\10.1.20.40\Buchhaltung, kein SPN zur IP	spoolsv.exe, TargetMachine = IP, auf jedem Client der OU
Aliasname ohne SPN	\\druck.musterwerk.local per CNAME auf PRINT01	Begründungstext: Ziel nicht auflösbar oder SPN nicht gefunden
Alte Verbindung nach Migration	Client hält die Verbindung zum alten Server oder zur IP	NTLM zu einem Ziel, das offiziell längst stillgelegt ist
Freigegebener Drucker am Arbeitsplatz	Client wird selbst zum Druckserver	4022/4023 oder 8003 auf einem Client statt auf einem Server
Clients außerhalb der Domäne	Laptops ohne Domäne, Laborrechner, Gäste	Lokales Konto, Kerberos grundsätzlich nicht möglich
Druckserver in anderer Gesamtstruktur	Verbindung über eine Vertrauensstellung	Kerberos nur mit sauberer Namensauflösung über die Grenze

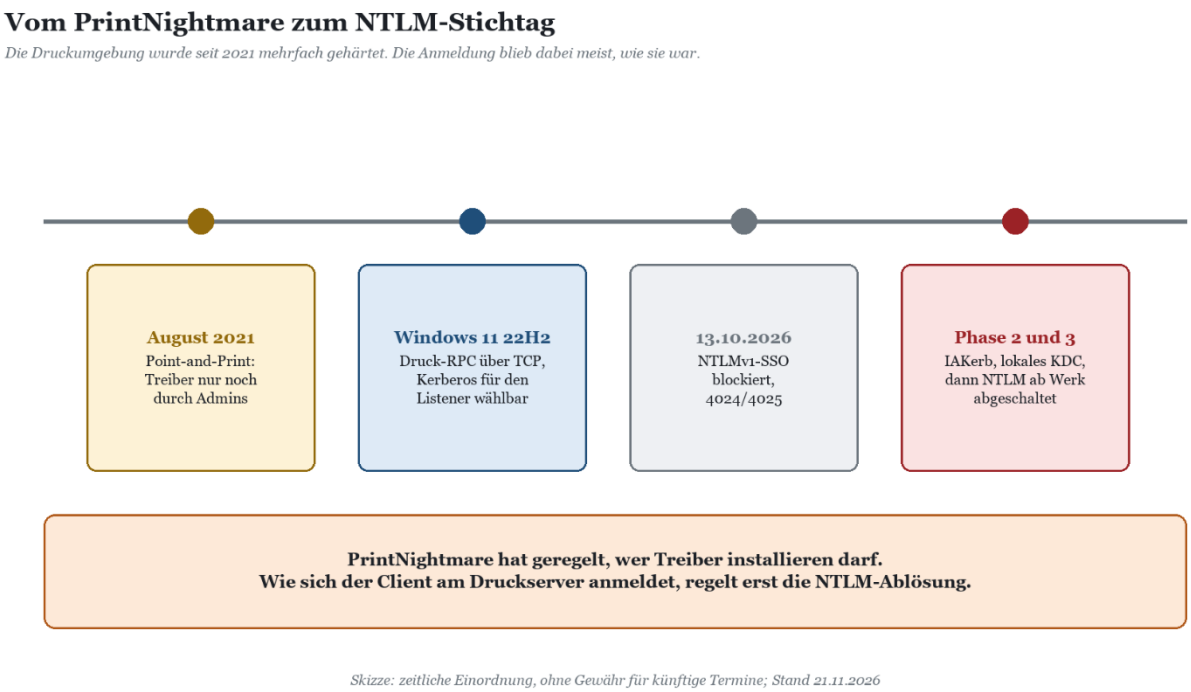
Netzwerkdrucker, die selbst per SMB irgendwo hinschreiben, gehören nicht in diese Liste. Das ist die Gegenrichtung, und die steht in Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden beziehungsweise für Geräte ohne Windows allgemein in NAS, Drucker und Scanner: NTLM bei Geräten ohne Windows. Hier geht es um den Weg vom Windows-Client zum Windows-Druckserver.

> **WICHTIG · Der Aliasname ist kein Kavaliersdelikt**
>
> Ein CNAME wie druck.musterwerk.local ist bequem, weil er Servertausch ohne GPO-Änderung erlaubt. Für Kerberos braucht er aber einen SPN am Computerkonto des Druckservers, sonst fällt jede Verbindung auf NTLM zurück. Warum das so ist und wie du Aliasnamen sauber einträgst, steht in CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet.

Point-and-Print seit PrintNightmare: kurz eingeordnet

Kein Artikel über Druckserver kommt ohne PrintNightmare aus, also kurz und schmerzlos: Seit den Updates vom August 2021 dürfen standardmäßig nur noch Administratoren Druckertreiber über Point-and-Print installieren. Gesteuert wird das über den Registrierungswert RestrictDriverInstallationToAdministrators unter HKLM\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint; fehlt der Wert, gilt er als 1. Microsoft beschreibt das in KB5005652: Neues Standardverhalten bei der Point-and-Print-Treiberinstallation. Seit den Updates vom Oktober 2021 gibt es dafür auch die Gruppenrichtlinie „Limits print driver installation to Administrators“.

Für die NTLM-Ablösung heißt das: Point-and-Print entscheidet, ob ein Treiber installiert werden darf, nicht, wie sich der Client dabei anmeldet. Indirekt hat PrintNightmare die Lage trotzdem verschlechtert. Viele Umgebungen haben damals in der Not Druckerverbindungen umgebaut, Treiber vorab verteilt und dabei hier und da IP-Adressen statt Servernamen eingetragen, weil es schnell gehen musste. Diese Provisorien sind heute die Top-Verursacher in der NTLM-Statistik.



Einstellung	Wirkung	Bezug zu NTLM
RestrictDriverInstallationToAdministrators	Treiberinstallation per Point-and-Print nur für Admins	Keiner; regelt Rechte, nicht die Anmeldung
Point-and-Print-Einschränkungen (GPO)	Erlaubte Druckserver und Warnverhalten	Indirekt: Liste der Server nach Namen pflegen, nicht nach IP
Configure RPC connection settings (Client)	Protokoll für ausgehenden Druck-RPC, Standard TCP	Gering; die Anmeldung bleibt Negotiate
Configure RPC listener settings (Server)	Protokolle und Authentifizierung für eingehenden Druck-RPC	Direkt: Authentifizierung auf Kerberos festlegbar
Allow Print Spooler to accept client connections	Darf der Spooler Verbindungen von außen annehmen	Direkt: schließt Arbeitsplätze als Druckserver und als Ziel für NTLM aus

WARNUNG · Die Härtung nicht für den Drucker zurückdrehen

RestrictDriverInstallationToAdministrators auf 0 zu setzen, damit Benutzer wieder selbst Treiber ziehen, öffnet genau die Lücke, die 2021 geschlossen wurde. Microsoft beschreibt den Wert 0 nur als Übergangslösung. Verteil die Treiber stattdessen vorab mit deiner Softwareverteilung und lass Point-and-Print nur noch die Verbindung herstellen.

Druck-RPC über TCP und Kerberos am Listener

Interessanter für die NTLM-Ablösung ist eine Änderung, die mit Windows 11 22H2 kam: Der Druck-RPC zwischen Client und Server läuft seitdem standardmäßig über RPC über TCP statt über Named Pipes. Unter Computerkonfiguration, Administrative Vorlagen, Drucker gibt es dafür zwei Richtlinien: „Configure RPC connection settings“ für die Clients und „Configure RPC listener settings“ für den Druckserver. In der Listener-Richtlinie legst du neben den erlaubten Protokollen auch die Authentifizierung für eingehende Verbindungen fest, und dort lässt sich Kerberos

erzwingen. Details stehen bei Microsoft unter RPC-Verbindungsupdates für den Druck unter Windows 11.

Das ist ein scharfes Werkzeug: Sobald der Listener nur noch Kerberos annimmt, kommen Clients, die den Server per IP-Adresse oder per Alias ohne SPN ansprechen, mit ihrem Druck-RPC nicht mehr durch. Deshalb steht es in der Reihenfolge ganz hinten, nach dem Messen und Umbauen. Beachte außerdem: Die Richtlinie betrifft den Druck-RPC. Der Treiberdownload aus print$ läuft über SMB und unterliegt den allgemeinen Regeln aus Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern.

TIPP · Port 135 und der dynamische Bereich

Wer nach einem Clientwechsel auf Windows 11 Fehler wie 0x00000709 beim Verbinden mit älteren Druckservern sieht, schaltet gern auf Named Pipes zurück. Prüf vorher die Firewall: RPC über TCP braucht Port 135 und den dynamischen Portbereich am Druckserver. Microsoft empfiehlt, bei TCP zu bleiben und Named Pipes nur zu nutzen, wenn TCP nicht geht.

Druck-NTLM finden: mit Bordmitteln und darüber hinaus

Voraussetzung ist, dass die NTLM-Überwachung auf Clients, Druckservern und Domain Controllern aktiv ist. Wie das geht, steht in NTLM-Auditing aktivieren: Schritt für Schritt; die passende Gruppenrichtlinie erzeugt dir das Audit-GPO-Skript für die NTLM-Überwachung. Mit dem erweiterten Auditing (Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit den Updates ab 13.10.2026) bekommst du auf dem Client die Ereignisse 4020 und 4021, auf dem Druckserver 4022 und 4023. Ältere Systeme liefern die klassischen Ereignisse 8001 (ausgehend) und 8003 (eingehende Anmeldung am Server, mit dem Feld „Workstation“ als anfragendem Client).

Auf dem Client: spoolsv.exe herausfiltern

Auf einem Client genügt ein Einzeiler, um die Druckverbindungen von allem anderen zu trennen. Er wertet die EventData-Felder aus und nicht den Meldungstext, denn bei weitergeleiteten Ereignissen kann der Meldungstext leer sein:

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-NTLM/Operational'; Id=4020,4021} |
  ForEach-Object {
    $x = [xml]$_.ToXml(); $f = @{}
    $x.Event.EventData.Data | ForEach-Object { $f[$_.Name] = $_.'#text' }
    [pscustomobject]@{ Prozess=$f.ProcessName; Ziel=$f.TargetMachine; Grund=$f.NtlmUsageReason
}
  } | Where-Object Prozess -like '*spoolsv.exe' |
  Group-Object Ziel, Grund | Sort-Object Count -Descending | Select-Object Count, Name
```

Auf dem Druckserver drehst du die Frage um: In 4022/4023 stehen RemoteClientMachine und ClientIP des anfragenden Clients, dazu NtlmVersion und „Mic Status“. Leere Felder stehen dort als „Null“ oder „(NULL)“. Weitere Rezepte, auch für das Zusammenführen vieler Rechner, findest du in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

In den Gruppenrichtlinien: IP-Adressen und Aliasnamen

Die Ereignisse sagen dir, welche Ziele auffallen. Woher sie kommen, steht meistens in den Gruppenrichtlinien. Druckerverbindungen aus den Gruppenrichtlinien-Einstellungen liegen als Printers.xml im SYSVOL, getrennt für Computer- und Benutzerkonfiguration. Eine einfache Suche nach UNC-Pfaden mit IP-Adresse:

```
$sysvol = '\\musterwerk.local\SYSVOL\musterwerk.local\Policies'
Get-ChildItem $sysvol -Recurse -Filter Printers.xml |
```

```
  Select-String -Pattern 'path="\\\\\d{1,3}(\.\d{1,3}){3}\\' |
  Select-Object Path, LineNumber
```

Dazu kommen Drucker, die über die Druckverwaltung als „bereitgestellte Drucker“ per GPO verteilt werden, und Anmeldeskripte, die mit rundll32 printui.dll oder Add-Printer arbeiten. Für die Skripte im NETLOGON-Verzeichnis gilt dieselbe Suche wie bei Laufwerkszuordnungen, siehe Laufwerkszuordnungen und Anmeldeskripte: NTLM-Fallen per GPO finden. Auf einzelnen Clients zeigt dir Get-Printer, welche Verbindungen tatsächlich eingerichtet sind; die Spalten ComputerName und ShareName verraten, ob noch der alte Server oder eine IP-Adresse drinsteckt.

AUS DER PRAXIS · Sparfuchs & Partner und der Drucker, den es nicht mehr gab

Bei der Sparfuchs & Partner Steuerberatungs GmbH zeigte die NTLM-Auswertung auf jedem Client spoolsv.exe mit Ziel 10.1.20.15, alle paar Minuten. Unter dieser Adresse stand seit dem Serverumzug vor zwei Jahren nichts mehr. Die Drucker-GPO war längst umgestellt, nur hatte die alte GPP-Aktion „Aktualisieren“ die alte Verbindung nie entfernt. Jeder Client versuchte also tapfer, eine Warteschlange auf einem Server zu erreichen, der inzwischen als Blumenständer im Archiv diente. Gedruckt hat dort niemand. Angemeldet haben sich alle.

Wo es mit Bordmitteln mühsam wird

Für einen Druckserver und eine Handvoll Clients ist das alles gut machbar. In einer Klinik mit 800 Arbeitsplätzen, drei Druckservern, Etikettendruckern auf Stationsrechnern und einer Gruppenrichtlinienlandschaft aus fünfzehn Jahren sieht das anders aus: Die Ereignisse liegen verteilt auf Hunderten Clients, spoolsv.exe erzeugt Tausende Einträge am Tag, und dieselbe Ursache taucht in jeder OU unter anderem Namen auf. Du brauchst dann eine Sicht, die gleichartige Verbindungen zusammenfasst und sagt, woher die IP-Adresse kommt. Genau dafür gibt es den NTLM Diagnostiker.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · spoolsv.exe in den Top-10-Verursachern

Die Übersicht des NTLM Diagnostikers fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen. In den Demodaten der Musterwerk GmbH steht spoolsv.exe mit dem Ziel 10.1.20.40 auf Platz zwei der Top-10-Verursacher: Ursache „Zugriff per IP-Adresse“, 218 Quellen, 1.673 Anmeldungen. Eine einzige Zeile statt 1.673 Ereignissen, verteilt auf 218 Rechner.

Klickst du dich zum Befund durch, erklärt die Wissensbasis das Muster und nennt den Lösungsweg. Die Ansicht IP-Ziele löst 10.1.20.40 rückwärts auf und zeigt die Fundstellen in Gruppenrichtlinien und Anmeldeskripten aus SYSVOL und NETLOGON, also genau die Printers.xml, die du sonst von Hand durchsuchst. Steckt ein Aliasname dahinter, meldet die SPN-Prüfung den fehlenden SPN.

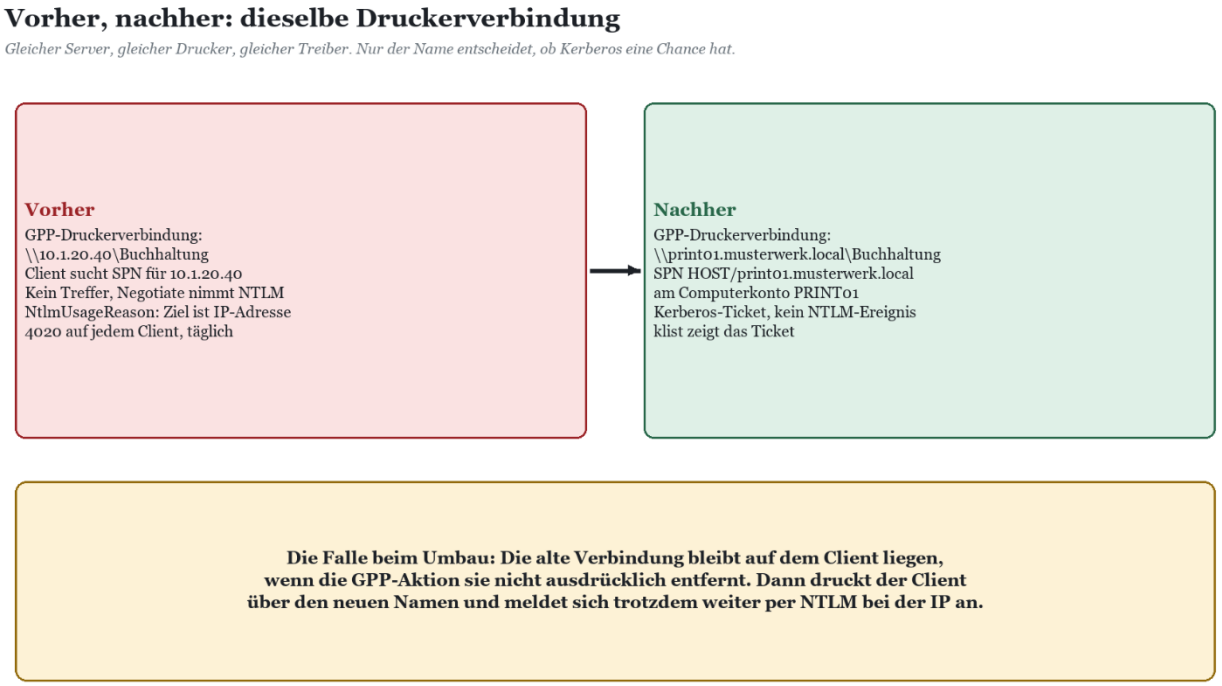
Der Diagnostiker arbeitet ausschließlich lesend. Er ändert weder GPOs noch SPNs; den passenden setspn-Befehl zeigt er an und bietet ihn zum Kopieren an, ausführen musst du ihn selbst. Die Top-10-Verursacher und die Hinweise aus der Wissensbasis liefert schon die kostenlose Edition Express, direkt vom DC.

Umbauen: Namen, SPNs, Kerberos für den Druck-RPC und Universal Print

Die gute Nachricht vorweg: Druckumgebungen gehören zu den dankbaren Baustellen der NTLM-Ablösung. Der Druckserver ist ein Windows-Server in der Domäne, Kerberos kann er von Haus aus. Es fehlt meist nur an einem Namen, den Kerberos auflösen kann.

Freigaben per Namen statt IP-Adresse

Stell jede Druckerverbindung auf den vollqualifizierten Namen des Druckservers um, also \\print01.musterwerk.local\Buchhaltung statt \\10.1.20.40\Buchhaltung. In den Gruppenrichtlinien-Einstellungen heißt das: neue Verbindung mit dem Servernamen anlegen und die alte mit der Aktion „Löschen“ ausdrücklich entfernen. Die Aktion „Aktualisieren“ für die neue Verbindung allein lässt die alte auf dem Client liegen, und der Spooler meldet sich weiter bei der IP an.



Skizze: Umstellung einer Druckerverbindung von IP-Adresse auf DNS-Namen; Musterwerk GmbH

Aliasnamen mit SPN

Soll der Alias bleiben, braucht das Computerkonto des Druckservers die passenden SPNs. Vorher prüfen, ob der Name schon an einem anderen Konto hängt, denn ein doppelter SPN bricht Kerberos ebenso zuverlässig wie ein fehlender:

```
setspn -Q HOST/druck.musterwerk.local
setspn -S HOST/druck.musterwerk.local PRINT01
setspn -S HOST/druck PRINT01
```

setspn -S prüft vor dem Eintragen auf Duplikate. Die Grundlagen zum fehlenden SPN stehen in Fehlender SPN: wenn Kerberos den Dienst nicht findet. Ob danach wirklich Kerberos greift, prüfst du auf dem Client nach dem nächsten Druck mit klist: Ein Ticket für den Druckserver muss in der Liste stehen, siehe Mit klist prüfen, ob Kerberos wirklich greift.

Kerberos am Druckserver erzwingen

Erst wenn auf dem Druckserver über mindestens zwei Wochen keine eingehenden NTLM-Anmeldungen mehr von Domänenclients auftauchen, ist es Zeit für die Listener-Richtlinie mit Kerberos. Setz sie zunächst auf einem Druckserver mit wenigen Warteschlangen, teste jeden Druckertyp einmal und miss einen Tag nach. Für Clients außerhalb der Domäne, etwa Laborrechner oder Gästegeräte, ist das das Ende des Druckens über diesen Server. Dafür brauchst du einen anderen Weg, zum Beispiel Universal Print, oder eine dokumentierte Ausnahme mit Enddatum.

Druckerwarteschlangen auf Clients schließen

Ein Arbeitsplatz mit freigegebenem Drucker ist ein kleiner Druckserver ohne SPN-Pflege, ohne Überwachung und meist ohne Wissen der IT. Die Richtlinie „Allow Print Spooler to accept client connections“ auf „Deaktiviert“ verhindert, dass der Spooler eines Clients Verbindungen von außen annimmt. Den freigegebenen Etikettendrucker verlagerst du auf den Druckserver. Nebenbei schließt du damit eine bekannte Angriffsfläche: Der Spooler-RPC lässt sich missbrauchen, um einen Rechner zu einer Anmeldung bei einem fremden Ziel zu bewegen, die dann weitergereicht wird. Auf Domain Controllern sollte der Druckspooler aus genau diesem Grund ohnehin nicht laufen. Mehr dazu in NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

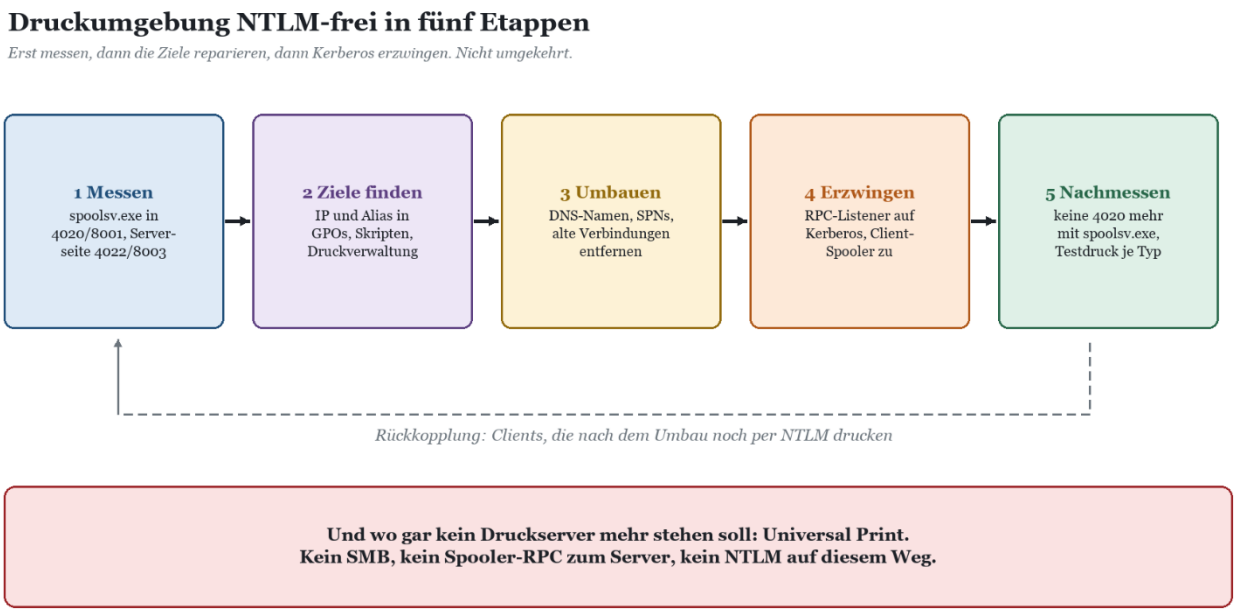
WARNUNG · Terminalserver und virtuelle Desktops nicht vergessen

Auf Terminalservern und in VDI-Umgebungen kommen die Druckerverbindungen oft aus mehreren Quellen gleichzeitig: GPO, Profilverwaltung und die Druckerumleitung des Clients. Eine alte IP-Verbindung im Profil überlebt dort jeden GPO-Umbau. Die Besonderheiten stehen in Citrix und virtuelle Desktops: NTLM in VDI- und Terminalserver-Umgebungen.

Universal Print als Alternative

Wo du ohnehin über den Abbau lokaler Infrastruktur nachdenkst, ist Universal Print eine ernst zu nehmende Alternative. Die Clients drucken an einen Clouddienst in Microsoft 365, angemeldet über Microsoft Entra ID. Drucker mit eingebauter Universal-Print-Unterstützung melden sich direkt dort an, ältere Geräte über einen Connector im lokalen Netz. Zwischen Client und Druckserver gibt es dann keine SMB-Freigabe und keinen Spooler-RPC mehr, also auch kein NTLM. Der Preis: Lizenzen, eine Internetabhängigkeit fürs Drucken und eine Umstellung, die sich bei Etikettendruckern mit Spezialtreibern nicht immer lohnt. Prüf das je Druckertyp, nicht pauschal.

Weg	NTLM danach	Aufwand	Passt, wenn
Namen statt IP in GPOs	keins	gering	Druckserver in der Domäne, DNS sauber
Alias mit SPN	keins	gering	Alias soll für Servertausch bleiben
Listener auf Kerberos	keins, auch kein Rückfall	gering, aber erst zum Schluss	alle Clients sprechen Kerberos
Client-Spooler schließen	keins auf Arbeitsplätzen	mittel	Arbeitsplatzdrucker umziehbar
Universal Print	keins auf dem Druckweg	mittel bis hoch	Microsoft 365 vorhanden, Druckertypen unterstützt
Ausnahme in Restrict-NTLM	ja, dokumentiert	gering	nur befristet, mit Enddatum



Skizze: Vorgehen für die Druckumgebung, je Druckserver oder je Standort

Wie der Druckumbau in den Gesamtplan passt, beschreiben NTLM schrittweise abschalten, ohne dass etwas ausfällt und der große Zeitrahmen in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Wenn du für eine größere Druckumgebung mit mehreren Standorten Unterstützung bei Inventur und Umbau willst, sprich mit uns über die Beratung zur NTLM-Ablösung.

AUS DER PRAXIS · Musterwerk GmbH: 1.673 Anmeldungen, eine GPO

Bei der Musterwerk GmbH ging der zweitgrößte NTLM-Verursacher auf eine einzige Gruppenrichtlinie zurück: Druckerverbindungen für die Verwaltung, eingetragen per IP-Adresse. Neue Verbindung mit print01.musterwerk.local, alte mit „Löschen“ entfernt, zwei Tage gewartet, bis alle Clients die Richtlinie gezogen hatten. Danach tauchte spoolsv.exe in der Liste nicht mehr auf. Aufwand: eine Stunde, davon fünfzig Minuten für die Frage, wer die GPO damals angelegt hatte.

FAQ: Druckserver und NTLM

Warum steht spoolsv.exe so weit oben in meiner NTLM-Auswertung?

Weil der Spooler des Clients die Verbindung zum Druckserver aufbaut, nicht die Anwendung. Jede Druckerverbindung per IP-Adresse oder Alias ohne SPN erzeugt deshalb NTLM-Ereignisse mit spoolsv.exe als Prozess, und zwar auf jedem Client, der die Verbindung hat.

Hat die Point-and-Print-Härtung nach PrintNightmare etwas mit NTLM zu tun?

Direkt nicht. Sie regelt, dass nur Administratoren Druckertreiber per Point-and-Print installieren dürfen. Wie sich der Client am Druckserver anmeldet, ändert sie nicht.

Trifft die NTLMv1-Blockierung vom Oktober 2026 meine Drucker?

In aller Regel nicht. Die Blockierung über BlockNtlmv1SSO betrifft das Erzeugen von NTLMv1-Anmeldedaten für Single Sign-on, sichtbar in den Ereignissen 4024 und 4025. Druckverbindungen zwischen aktuellen Windows-Systemen laufen mit NTLMv2. Ausfälle drohen mit Restrict-NTLM-Richtlinien und Phase 3, in der NTLM ab Werk abgeschaltet ist.

Reicht es, im GPO die IP-Adresse durch den Servernamen zu ersetzen?

Fast. Die alte Verbindung muss zusätzlich mit der Aktion „Löschen“ entfernt werden, sonst bleibt sie auf den Clients liegen und erzeugt weiter NTLM.

Welchen SPN braucht ein Druckserver-Alias?

HOST/alias und HOST/alias.domäne am Computerkonto des Druckservers, eingetragen mit setspn -S. Vorher mit setspn -Q prüfen, ob der Name schon an einem anderen Konto hängt.

Kann ich Kerberos für den Druck erzwingen?

Für den Druck-RPC ja, über die Richtlinie „Configure RPC listener settings“ auf dem Druckserver. Tu das erst, wenn die Messung zeigt, dass keine Clients mehr per IP oder Alias ohne SPN kommen.

Sollte der Druckspooler auf Clients überhaupt laufen?

Lokal ja, sonst druckt der Client nicht. Eingehende Verbindungen sollte er aber nicht annehmen: „Allow Print Spooler to accept client connections“ auf Clients deaktivieren und freigegebene Arbeitsplatzdrucker auf den Druckserver umziehen.

Ist Universal Print die Lösung für alles?

Nein, aber für viele Standarddrucker eine gute. Für Spezialdrucker mit eigenen Treibern und für Bereiche, die ohne Internetverbindung drucken müssen, bleibt der Druckserver mit Kerberos meist die bessere Wahl.

Fazit: Der Druckserver ist die dankbarste Baustelle

Druck-NTLM ist laut, weil sie auf jedem Client entsteht, aber selten schwierig. Hinter spoolsv.exe in der Verursacherliste stecken fast immer dieselben Ursachen: IP-Adressen in Drucker-GPOs, Aliasnamen ohne SPN, liegen gebliebene Verbindungen und Arbeitsplätze, die heimlich Druckserver spielen. PrintNightmare hat die Treiberinstallation gehärtet, nicht die Anmeldung; die musst du selbst in Ordnung bringen. Mit Namen statt IP-Adressen, sauberen SPNs und zum Schluss Kerberos am Druck-Listener ist der Druckserver einer der ersten Kandidaten, die du in deiner Statistik abhaken kannst. Wo kein Druckserver mehr stehen soll, nimmt Universal Print das Thema ganz vom Tisch.

Damit das so bleibt, wenn der nächste Kollege eine Druckerverbindung schnell mal per IP einträgt, lies Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben. Und wenn dein Team diese Auswertung künftig selbst sicher fahren will, schau in die Schulung zum NTLM Diagnostiker. Zum Kerberos-Unterbau insgesamt lohnt der Blick in Microsoft Kerberos.

WEITERLESEN · Weiter in dieser Serie

› CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet
› Fehlender SPN: wenn Kerberos den Dienst nicht findet
› Laufwerkszuordnungen und Anmeldeskripte: NTLM-Fallen per GPO finden
› Mit klist prüfen, ob Kerberos wirklich greift
› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz
› Citrix und virtuelle Desktops: NTLM in VDI- und Terminalserver-Umgebungen
› Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden
› Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte