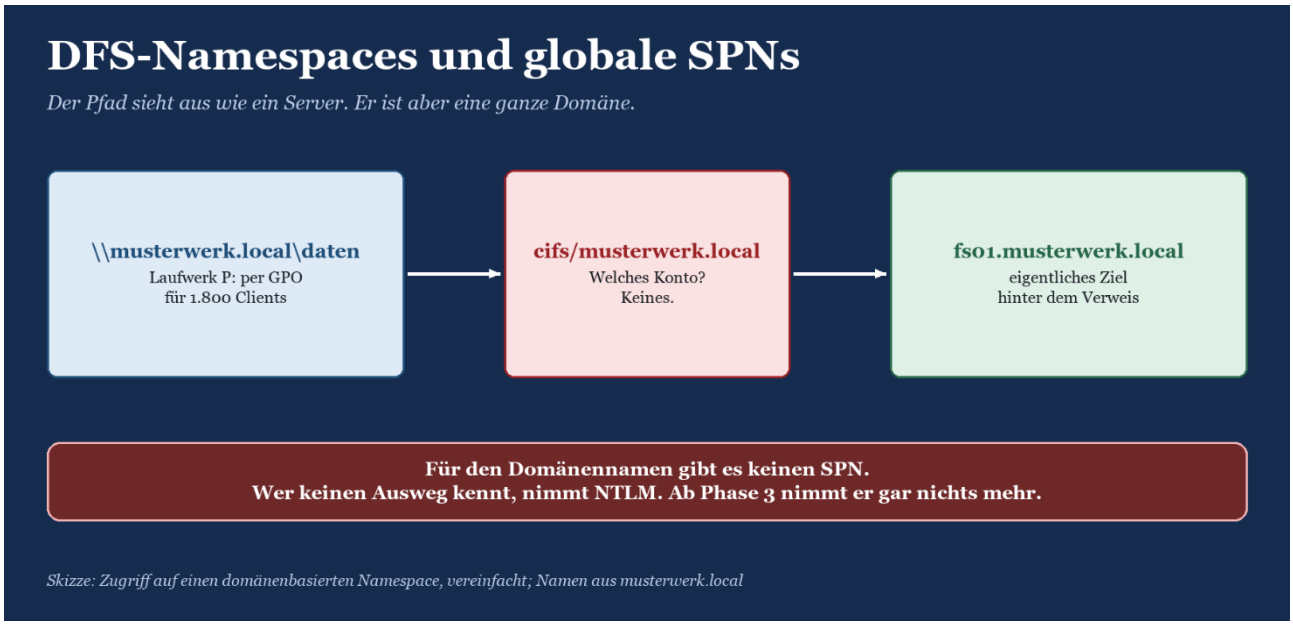
DFS-Namespaces und globale SPNs: wenn \\domäne\freigabe NTLM auslöst



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

BERATUNG
Namespaces, Dateiserver, Scan-Ziele? Wir sortieren mit dir die DFS-Zugriffe.
› Beratung zur NTLM-Ablösung

SCHULUNG
NTLM-Ereignisse lesen, SPNs prüfen, Abschaltung testen: praxisnah für dein Team.
› Schulung zum NTLM Diagnostiker

Es gibt Pfade, die jeder in der Firma auswendig kann. \\musterwerk.local\daten gehört dazu. Er steht in der Laufwerkszuordnung, im Anmeldeskript von 2011, auf dem Zettel am Monitor der Buchhaltung und in der Konfiguration des Kopierers im zweiten Stock. Domänenbasierte DFS-Namespaces waren ja genau dafür gedacht: ein Name, der bleibt, egal welcher Dateiserver gerade dahintersteckt. Dumm nur, dass dieser schöne Name für Kerberos ein Problem ist. Denn musterwerk.local ist kein Server, sondern eine ganze Domäne, und für die gibt es keinen Dienstprinzipalnamen.

In den erweiterten NTLM-Ereignissen taucht das als eigener Begründungstext auf: „The target name is a global SPN like cifs/contoso.com and could not be resolved …“, in der Praxis meist mit der Reason-ID 12. Dieser Beitrag dreht sich genau um diesen Fall: dfs ntlm kerberos, also warum der Zugriff über den Domänennamen NTLM auslöst, wer davon wirklich betroffen ist, was du heute schon belegt tun kannst und was du besser lässt. Die Grundlagen zu Reason-IDs, Auditing und Restrict-Richtlinien wiederholen wir hier nicht, dafür gibt es die verlinkten Beiträge der Serie.

Der Zeitdruck 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. Microsoft selbst nennt domänenbasierte DFS-Namespaces in seinen FAQ zur NTLM-Ablösung eine historisch verlässliche Quelle für NTLM-Rückfälle. Wenn sogar der Hersteller „verlässlich“ sagt, weißt du, dass es ernst ist.

FAKTEN · Das Wichtigste in Kürze

Ein domänenbasierter Namespace wird über \\<domäne>\<namespace> angesprochen. Der Client muss zuerst einen Domain Controller kontaktieren, um an den Namespace-Server verwiesen zu werden.

Für cifs/<domänenname> trägt kein Objekt im Active Directory einen SPN. Ein Dienstticket für diesen Namen kann der KDC also nicht ausstellen.

Windows-Clients in der Domäne weichen laut Microsoft auf ein Ticket für einen Domain Controller aus. Windows-Rechner ohne Domäne und Fremdgeräte kennen diesen Ausweg nicht und landen bei NTLM.

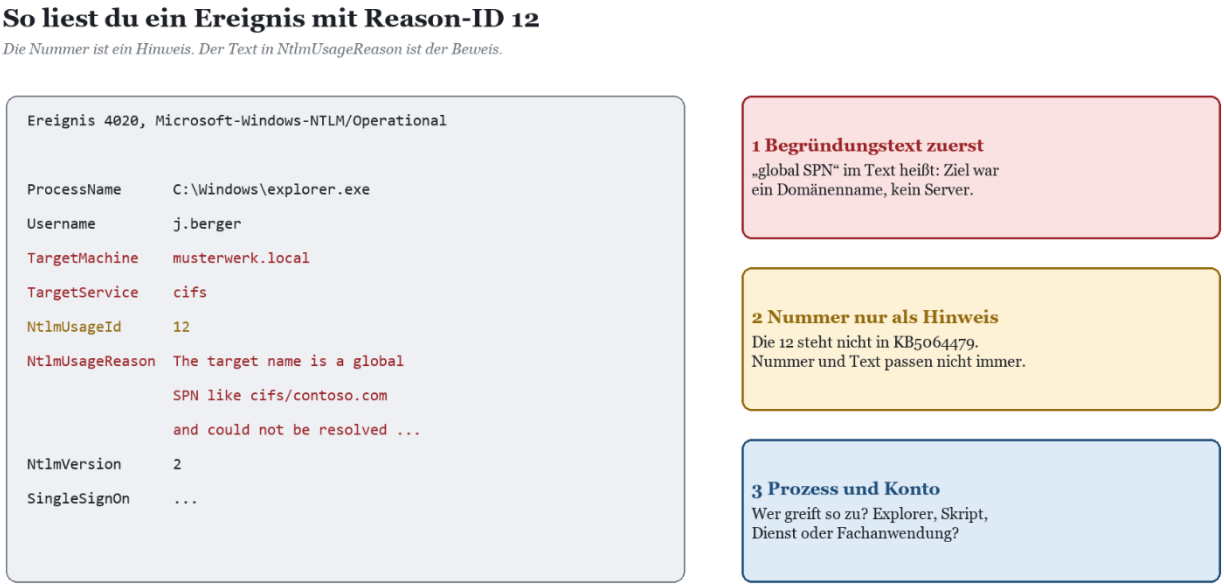
Microsoft hat angekündigt, DFS-Zugriffe mit dem Release, das NTLM standardmäßig abschaltet, durchgehend auf Kerberos zu bringen. Bis dahin ist das dein Thema.

Maßgeblich ist der Begründungstext im Feld NtlmUsageReason. Die Reason-ID 12 ist in KB5064479 nicht dokumentiert; die Nummer ist nur ein Hinweis.

Reason-ID 12: der Begründungstext, den keine Liste kennt

Microsoft dokumentiert in KB5064479 die Reason-IDs 0 bis 11 für die erweiterten NTLM-Ereignisse 4020 und 4021. Eine 12 kommt dort nicht vor. In echten Protokollen taucht sie trotzdem auf, und zwar mit dem Text „The target name is a global SPN like cifs/contoso.com and could not be resolved …“. Gleichzeitig gilt, was in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat ausführlich steht: Nummer und Text passen nicht immer zusammen. Es gibt Ereignisse mit der Nummer 10 und dem Text, der laut Liste zur 6 gehört. Wer also nach NtlmUsageId gleich 12 filtert, findet vielleicht nicht alles und vielleicht das Falsche.

Die Regel für die Auswertung ist deshalb einfach: Filtere auf den Begründungstext im Feld NtlmUsageReason, nicht auf die Nummer, und schon gar nicht auf den Meldungstext des Ereignisses. Über Windows Event Forwarding weitergeleitete Ereignisse kommen gern mit leerem Meldungstext an. Dann zählen nur noch die EventData-Felder. Wie du die zentrale Sammlung aufsetzt, steht in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding.



Skizze: Felder eines 4020-Ereignisses, Werte beispielhaft und gekürzt

Was „global SPN“ hier bedeutet

„Global“ meint in diesem Text keinen besonderen SPN-Typ im Active Directory, den du irgendwo anlegen könntest. Gemeint ist ein Zielname, der nicht auf einen einzelnen Rechner zeigt, sondern auf die Domäne selbst. Der Client baut aus dem Pfad \\musterwerk.local\daten brav den SPN cifs/musterwerk.local, fragt den KDC danach und bekommt eine Abfuhr. Ab da entscheidet der Client, ob er einen anderen Weg zu Kerberos kennt oder ob er NTLM aushandelt. Das Ereignis 4020 schreibt er nur im zweiten Fall.

Feld im Ereignis 4020/4021	Was du bei diesem Verursacher typischerweise siehst	Was es dir sagt
NtlmUsageReason	Text mit „global SPN like cifs/contoso.com“	Ziel war ein Domänenname. Das ist das entscheidende Merkmal.
NtlmUsageId	häufig 12, aber nicht verlässlich	Nur Hinweis, nie alleiniges Filterkriterium.
TargetMachine / TargetService	Domänenname statt Servername, Dienst cifs	Zugriff über \\domäne\..., nicht über den Dateiserver.
ProcessName	explorer.exe, svchost.exe, Skript-Host oder Fachanwendung	Wer den Pfad benutzt. Bestimmt die Lösung.
Username / DomainName	Benutzerkonto oder Dienstkonto	Mensch am Laufwerk oder Dienst im Hintergrund.
Hostname	anfragender Rechner	Domänenmitglied? Dann ist es ein Sonderfall, siehe unten.

WICHTIG · Server-Ereignisse helfen nur halb

Auf den Namespace-Servern und Domain Controllern siehst du die eingehenden NTLM-Anmeldungen als 4022/4023 beziehungsweise in der klassischen Überwachung als 8003 und 8004, mit dem anfragenden Client im Feld RemoteClientMachine oder Workstation. Den Grund für den Rückfall kennt aber nur der Client. Ein Begründungstext mit „global SPN“ steht ausschließlich in 4020/4021 auf der Clientseite.

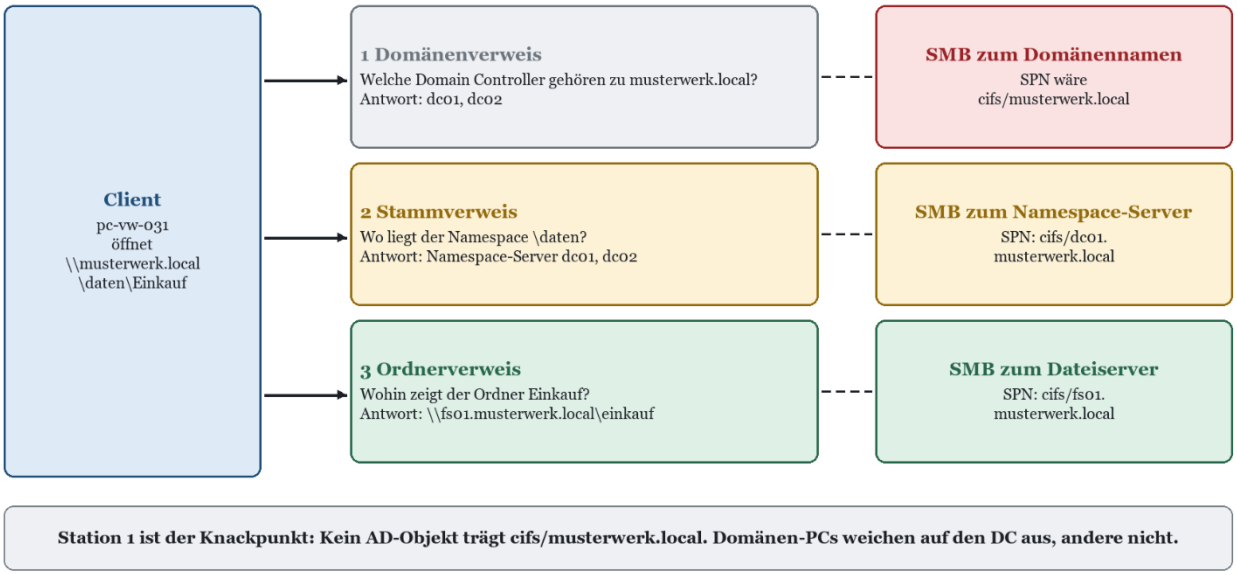
Für Geräte ohne Windows-Ereignisprotokoll, also Kopierer, NAS-Systeme oder Linux-Rechner, bleiben dir nur die Serverereignisse oder ein Netzwerkmitschnitt.

Warum für \\domäne\freigabe kein Server-SPN greift

Ein Zugriff auf einen domänenbasierten Namespace ist kein einzelner Verbindungsaufbau, sondern eine kleine Schnitzeljagd. Der DFS-Client fragt zuerst, welche Domain Controller für die Domäne zuständig sind (Domänenverweis), dann, welche Namespace-Server den Namespace hosten (Stammverweis), und schließlich, auf welchen Dateiserver ein Ordner zeigt (Ordnerverweis). Erst die letzte Station ist ein Rechner mit eigenem Computerkonto und sauberem SPN wie cifs/fs01.musterwerk.local.

Drei Stationen bis zur Datei

Der DFS-Client fragt sich durch. Nur die letzte Station hat einen echten Servernamen.



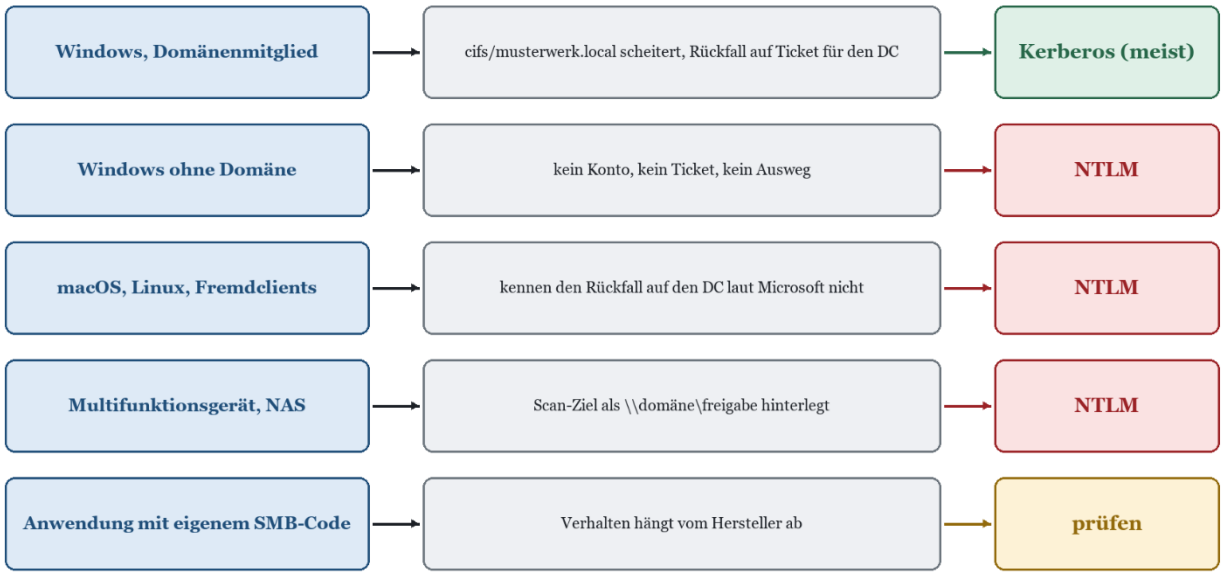
Skizze: DFS-Verweisablauf vereinfacht; Namen und Namespace aus musterwerk.local

Microsoft beschreibt das Problem in Teil 8 seiner Active-Directory-Hardening-Reihe auf techcommunity.microsoft.com ungewohnt offen: Bei einem domänenbasierten DFS-Pfad muss der Client zuerst einen Domain Controller kontaktieren. Da kein Objekt einen SPN für CIFS/CONTOSO.LOCAL trägt, lässt sich für diesen Pfad kein Dienstticket anfordern. Ein Windows-Client in der Domäne fragt zwar nach cifs/contoso.local, fällt aber sofort auf ein CIFS-Ticket für einen Domain Controller zurück, zum Beispiel cifs/contoso-dc1.contoso.local. Dadurch funktionieren DFS-Verweise auch dann noch, wenn die Domain Controller kein NTLM mehr akzeptieren.

Und dann kommt der Satz, der dich interessieren sollte: Windows-Rechner ohne Domänenmitgliedschaft und Fremdgeräte wissen nicht, wie sie zurückfallen sollen, wenn die Ticketanfrage scheitert. Schaltest du NTLM auf den Domain Controllern ab, verlieren sie nach Microsofts Einschätzung höchstwahrscheinlich den Zugriff auf domänenbasierte DFS-Freigaben. Das ist der Kopierer, der seine Scans nach \\musterwerk.local\scan schiebt. Das ist das MacBook der Marketingabteilung. Und das ist der Laborrechner, der seit Jahren in der Arbeitsgruppe steht, weil „der Hersteller das so wollte“.

Wer kommt per Kerberos durch den Namespace?

Der Pfad ist derselbe. Wer fragt, entscheidet über das Protokoll.



Skizze: Einordnung nach Microsofts AD-Hardening-Reihe, Teil 8; Gerätetypen beispielhaft

Und warum sehe ich dann Treffer von Domänen-PCs?

Gute Frage, und die ehrliche Antwort lautet: Der beschriebene Rückfall auf ein DC-Ticket ist das Verhalten des Windows-DFS-Clients. Nicht jeder Zugriff auf \\musterwerk.local läuft aber über diesen Weg. Anwendungen mit eigener SMB- oder Authentifizierungslogik, Dienste unter besonderen Konten, Zugriffe auf die Wurzel des Namespace oder ältere Clientstände können sich anders verhalten. Microsoft weist in einem Kommentar zur Hardening-Reihe darauf hin, dass beim Durchsuchen der Wurzel eines DFS-Namespace kein SPN existiert und damit kein Kerberos möglich ist, anders als beim eigentlichen Ordnerziel auf einem echten Server. Wenn ein Domänenrechner also Ereignisse mit „global SPN“ schreibt, ist der ProcessName die wichtigste Spur.

AUS DER PRAXIS · Typische Situation bei der Musterwerk GmbH

Die Auswertung zeigt rund 1.600 Ereignisse pro Tag mit „global SPN“ im Begründungstext. 1.540 davon stammen von einem einzigen Prozess: einem Inventaragenten, der jede Nacht \\musterwerk.local\software nach Paketen durchsucht und dabei die Wurzel des Namespace aufzählt. Der Rest verteilt sich auf zwei Multifunktionsgeräte und ein Skript auf einem Arbeitsgruppen-Rechner in der Qualitätssicherung.

Explorer-Zugriffe der Clients? Kaum. Die sind über den Rückfall auf den DC längst auf Kerberos. Hätte das Team nach Reason-ID gefiltert, wären 400 Treffer mit abweichender Nummer im Rauschen untergegangen.

WARNUNG · Finger weg vom SPN cifs/musterwerk.local

Die naheliegende Idee lautet: Dann trage ich cifs/musterwerk.local eben an einem Konto ein. Lass es. Microsoft nennt das nirgends als Lösung. Ein solcher SPN gehört zwangsläufig genau einem Konto, etwa einem einzigen Domain Controller. Tickets für den Domänennamen wären dann mit dessen Schlüssel verschlüsselt, der Namespace-Verweis kann den Client aber zu jedem anderen DC schicken. Dort scheitert die Anmeldung, und du hast aus einem NTLM-Rückfall einen Zugriffsfehler gemacht.

Microsoft schreibt in den FAQ zur NTLM-Ablösung außerdem ausdrücklich, dass fehlende, doppelte oder fehlerhafte SPNs in deinem Verzeichnis deine Aufgabe sind. Ein selbst gebauter Behelfs-SPN fällt genau in die Kategorie „fehlerhaft“.

Mit Bordmitteln eingrenzen

Bevor du irgendetwas umbaust, willst du wissen, wer in deiner Umgebung über den Domänennamen zugreift und mit welchem Prozess. Voraussetzung ist das erweiterte NTLM-Auditing auf den Clients, das ab Windows 11 24H2, Windows Server 2025 sowie Server 2022 und 2019 mit den Updates ab 13.10.2026 verfügbar ist. Wie du es per Gruppenrichtlinie einschaltest, erklärt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; wer es nicht von Hand klicken will, nimmt das NTLM-Audit-GPO-Skript.

Ereignisse über die Felder filtern

Das folgende PowerShell-Rezept liest die Ereignisse 4020 und 4021 aus dem Protokoll Microsoft-Windows-NTLM/Operational, zerlegt die EventData-Felder und behält nur Einträge, deren Begründungstext „global SPN“ enthält. Gruppiert wird nach Prozess, Ziel und Rechner, denn genau diese Kombination bestimmt später die Maßnahme. Weitere Rezepte findest du in NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

```
$ev = Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' `
        -FilterXPath '*[System[(EventID=4020 or EventID=4021)]]' -ErrorAction SilentlyContinue
$treffer = foreach ($e in $ev) {
    $f = @{}
    ([xml]$e.ToXml()).Event.EventData.Data | ForEach-Object { $f[$_.Name] = $_.'#text' }
    if ($f['NtlmUsageReason'] -match 'global SPN') {
        [pscustomobject]@{
            Rechner = $f['Hostname']; Prozess = $f['ProcessName']
            Ziel = $f['TargetMachine']; Dienst = $f['TargetService']
            Konto = $f['Username']; Id = $f['NtlmUsageId']
        }
    }
}
$treffer | Group-Object Prozess, Ziel | Sort-Object Count -Descending |
    Select-Object Count, Name -First 20
```

Auf einem einzelnen Client ist das in Sekunden erledigt. Für einen Schnelltest per wevtutil reicht auch eine Abfrage der letzten Ereignisse im Textformat; die Auswertung danach erledigst du aber besser über die Felder, nicht über den Meldungstext:

```
wevtutil qe Microsoft-Windows-NTLM/Operational /q:"*[System[(EventID=4020)]]" /c:50 /rd:true
/f:xml
```

Gegenprobe mit setspn und klist

Zwei kurze Prüfschritte bestätigen die Diagnose. Mit setspn suchst du gesamtstrukturweit nach dem SPN des Domänennamens. Erwartetes Ergebnis: Es gibt keinen. Findest du doch einen, hat ihn jemand irgendwann von Hand angelegt, und das ist ein eigener Befund, siehe Warnkasten oben.

```
setspn -Q cifs/musterwerk.local
setspn -Q cifs/musterwerk

klist purge
dir \\musterwerk.local\daten
klist
```

Nach dem Zugriff zeigt klist auf einem Domänen-PC typischerweise Tickets für cifs/<dc>.musterwerk.local und für den Dateiserver hinter dem Ordnerverweis. Steht dort ein Ticket für cifs/fs01.musterwerk.local, lief der eigentliche Dateizugriff per Kerberos. Fehlt es, liegt das Problem eher beim Ordnerziel als beim Namespace, etwa bei einem Alias ohne SPN. Wie du klist-Ausgaben sicher liest, steht in Mit klist prüfen, ob Kerberos wirklich greift.

Namespace-Konfiguration prüfen

Der Namespace selbst verrät dir, wohin er die Clients schickt. Mit den DFSN-Cmdlets Get-DfsnRoot, Get-DfsnRootTarget und Get-DfsnFolderTarget siehst du, ob Stamm- und Ordnerziele als NetBIOS-Name, als FQDN oder gar als IP-Adresse eingetragen sind. Get-DfsnServerConfiguration zeigt dir für jeden Namespace-Server, ob er FQDN-Verweise ausliefert (Eigenschaft UseFqdn).

```
Get-DfsnRoot -Domain musterwerk.local | Where-Object Type -NotMatch 'Standalone'
Get-DfsnRootTarget -Path \\musterwerk.local\daten
Get-DfsnFolder -Path '\\musterwerk.local\daten\*' |
    ForEach-Object { Get-DfsnFolderTarget -Path $_.Path } |
    Select-Object Path, TargetPath, State
Get-DfsnServerConfiguration -ComputerName dc01.musterwerk.local
```

Befund	Bedeutung für Kerberos	Nächster Schritt
Ordnerziel \\fs01\einkauf (NetBIOS)	Für Windows-Clients in der Domäne meist unkritisch, SPN cifs/fs01 existiert in der Regel.	Für Fremdclients und DNS-only-Umgebungen auf FQDN umstellen.
Ordnerziel \\daten.musterwerk.local\… (Alias)	Kerberos nur, wenn der Alias einen passenden SPN am Dateiserver hat.	SPN-Prüfung, siehe Beitrag zu CNAME und Aliasnamen.
Ordnerziel \\10.20.0.10\…	Kein SPN für die IP-Adresse, NTLM vorprogrammiert.	Auf den Servernamen umstellen.
UseFqdn = False	Verweise kommen als NetBIOS-Name.	Prüfen, ob Fremdclients den Namen auflösen; ggf. FQDN-Verweise einschalten.
SPN cifs/musterwerk.local vorhanden	Behelfs-SPN an einem einzelnen Konto.	Herkunft klären, Rücknahme planen und testen.

Wo es mühsam wird

So weit, so ordentlich, solange es um einen Rechner geht. In einer Umgebung mit 1.800 Clients, drei Namespaces und Ereignissen von hundert Maschinen sieht die Sache anders aus. Du sammelst Tausende Ereignisse pro Tag, von denen manche mit Nummer 12 und manche mit einer anderen Nummer kommen. Ein Teil der Clients liefert gar nichts, weil das Auditing dort nie angekommen ist, und die eigentlichen Problemkinder, Kopierer und NAS-Systeme, schreiben ohnehin kein Ereignisprotokoll. Am Ende sitzt du mit einer CSV-Datei in Excel und versuchst zu verstehen, ob der svchost.exe auf 340 Rechnern ein Problem ist oder nur Rauschen. Das ist der Punkt, an dem ein Werkzeug Zeit spart.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Verursacher erkennen statt Ereignisse zählen

Der NTLM Diagnostiker fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen und gleicht sie mit seiner Wissensbasis bekannter Verursacher ab. Zugriffe mit „global SPN“ im Begründungstext landen dabei als eigener Verursacher in der Liste, getrennt von fehlenden SPNs, Zugriffen per IP-Adresse oder Aliasnamen. Die Ursachen-Engine wertet dafür den Begründungstext

aus, nicht nur die Reason-ID, damit abweichende Nummern nicht durchrutschen.

In der Ansicht „Befunde“ unter „Bekannte Verursacher“ siehst du je Eintrag Kategorie, Prozess und Ziel, die Zahl der Quellen und der Anmeldungen. Rechts stehen die Erklärung, die typische Lösung und die betroffenen Konten. So erkennst du sofort, ob hinter dem DFS-Befund ein Inventaragent auf 340 Rechnern oder ein einzelner Kopierer steckt.

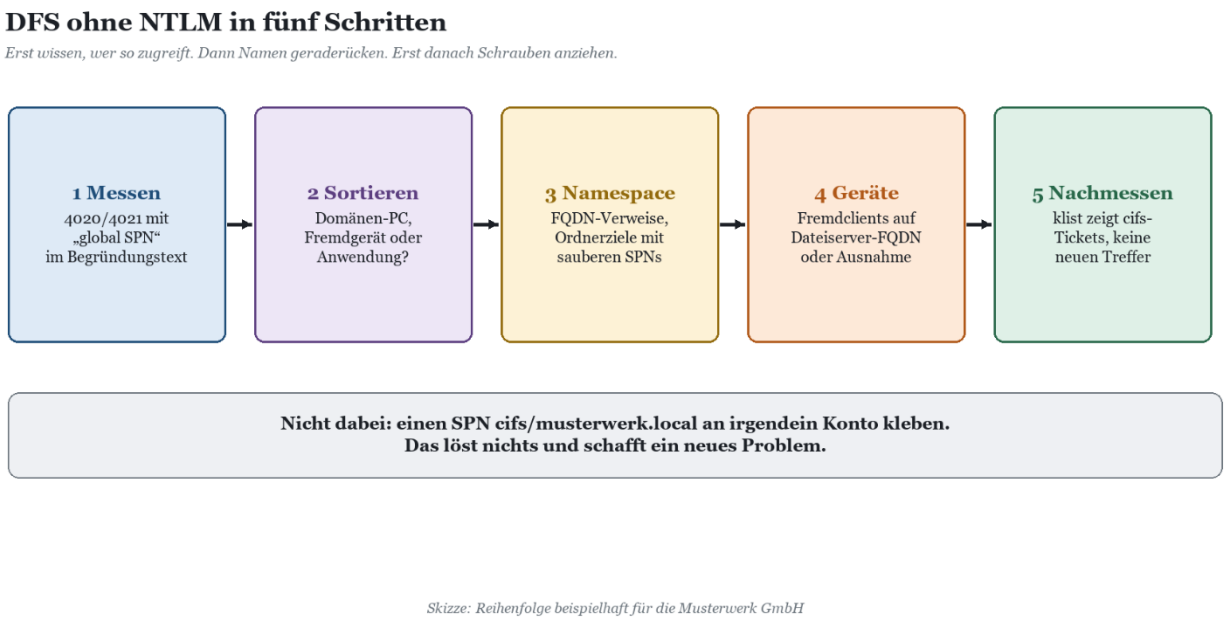
Die Abdeckungskarte zeigt dir dazu, welche Rechner überhaupt Ereignisse liefern und welche schweigen. Geräte ohne Ereignisprotokoll holst du über den Import eines Netzwerkmitschnitts (pcap oder pcapng) in die Auswertung.

Der Diagnostiker arbeitet ausschließlich lesend. Er ändert weder Namespaces noch SPNs; Befehle zeigt er dir an und bietet sie zum Kopieren an, ausführen musst du sie selbst.

Mehr über Funktionsumfang und Arbeitsweise erfährst du auf der Seite zum NTLM Diagnostiker. Die Express-Edition ist kostenlos und unbegrenzt nutzbar: Sie liefert dir in fünf Minuten direkt vom Domain Controller die Readiness-Ampel, die Abdeckungskarte, die Top-10-Verursacher mit Hinweisen aus der Wissensbasis und einen Kurzbefund als PDF. Für die Detailansichten, den Mitschnitt-Import und den Abschalt-Simulator gibt es einen Testzeitraum von sieben Tagen, einmal pro Domäne.

Konfiguration und Clients aufräumen

Gleich vorweg: Für den Domänenpfad selbst gibt es heute keinen Schalter, der Fremdgeräten Kerberos beibringt. Microsoft hat angekündigt, DFS-Zugriffe durchgehend auf Kerberos zu bringen, und zwar mit denselben Windows-Server- und Client-Versionen, die NTLM standardmäßig abschalten. Was du bis dahin tun kannst, ist dreierlei: dafür sorgen, dass alles hinter dem Domänenpfad sauber per Kerberos erreichbar ist, die Clients ohne Rückfallweg identifizieren und ihnen einen anderen Weg geben, und den Rest bewusst als Ausnahme führen. Den Gesamtfahrplan der Ablösung findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.



Skizze: Reihenfolge beispielhaft für die Musterwerk GmbH

Namespace: Verweise auf FQDN umstellen

Standardmäßig liefern Namespace-Server Stammverweise im NetBIOS-Format aus, also \\dc01\daten. Für Windows-Clients in der Domäne funktioniert das. Clients ohne NetBIOS-Namensauflösung, etwa Geräte ohne Windows, können den Namen aber unter Umständen nicht

auflösen. Microsoft beschreibt im Support-Artikel Configure DFS to use domain names (früher KB 244380), wie du Namespace-Server auf FQDN-Verweise umstellst. Kurz zusammengefasst:

- **Sichern:** Namespace-Metadaten mit dfsutil root export sichern.
- **Stammziel entfernen:** Den domänenbasierten Namespace vom Namespace-Server nehmen. Das geht ohne Ausfall nur, wenn mindestens ein weiterer Namespace-Server den Namespace hostet.
- **FQDN einschalten:** Set-DfsnServerConfiguration -ComputerName <server> -UseFqdn $true und den DFS-Namespace-Dienst neu starten.
- **Stammziel wieder hinzufügen:** New-DfsnRootTarget, danach gegebenenfalls die Sicherung importieren.
- **Ordnerziele anpassen:** Ordnerziele mit NetBIOS-Namen in der exportierten Datei auf FQDN ändern und mit dfsutil root import set zurückspielen.

TIPP · Was FQDN-Verweise leisten und was nicht

FQDN-Verweise sorgen dafür, dass Clients die Ziele hinter dem Namespace sauber per DNS auflösen und dafür passende SPNs wie cifs/fs01.musterwerk.local anfragen können. Am ersten Schritt, dem Zugriff auf den Domänennamen, ändern sie nichts. Für Fremdclients sind sie trotzdem eine Voraussetzung, damit nach dem Verweis überhaupt Kerberos möglich ist. Teste die Umstellung auf einem Namespace-Server in einem Wartungsfenster und miss danach nach.

Ordnerziele: echte Namen mit sauberen SPNs

Der beste DFS-Namespace nützt wenig, wenn der Ordnerverweis auf einen Alias ohne SPN oder auf eine IP-Adresse zeigt. Dann hast du das NTLM-Problem nur eine Station weitergeschoben, und im Ereignis steht nicht mehr „global SPN“, sondern ein anderer Begründungstext. Prüfe jedes Ordnerziel gegen die SPNs des Zielservers. Bei Aliasnamen hilft CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet, bei fehlenden SPNs Reason-ID 6: wenn der Zielname nicht auflösbar ist. Für Namespaces, die alte Servernamen nach einer Konsolidierung weiterleben lassen, nennt Microsoft in der Dokumentation zu DFS-N mit Azure Files den Weg über netdom computername /add, der den alten Namen als alternativen Computernamen samt HOST-SPN registriert, statt cifs-SPNs von Hand anzulegen. Ob das in deiner Umgebung passt, ist ein Prüfschritt, kein Automatismus.

Clients: wer keinen Rückfallweg kennt, braucht einen anderen Pfad

Bei den Clients entscheidet die Art des Geräts. Windows-Rechner in der Domäne, die per Explorer oder Laufwerkszuordnung zugreifen, sind laut Microsoft über den Rückfall auf das DC-Ticket bereits Kerberos-fähig. Hier musst du in der Regel nichts ändern, außer es taucht ein Prozess mit eigener Logik auf. Bei allen anderen sieht es so aus:

Client	Typischer Zugriff	Empfehlung bis zur Plattformlösung
Windows in der Domäne (Explorer, GPO-Laufwerk)	\\musterwerk.local\daten	Belassen; Treffer nur prüfen, wenn ein Prozess mit „global SPN“ auffällt.
Inventar-, Backup- oder Softwareverteilungsagent	Wurzel des Namespace aufzählen	Konfiguration auf den Ordnerpfad oder den Dateiserver-FQDN umstellen; beim Hersteller nachfragen.
Multifunktionsgerät, Scan-to-Folder	\\musterwerk.local\scan	Scan-Ziel direkt auf \\fs01.musterwerk.local\scan setzen, wenn das Gerät Kerberos kann; sonst als Ausnahme führen.
Windows ohne Domäne,	Pfad im Skript oder in der	Domänenbeitritt prüfen; sonst direkter

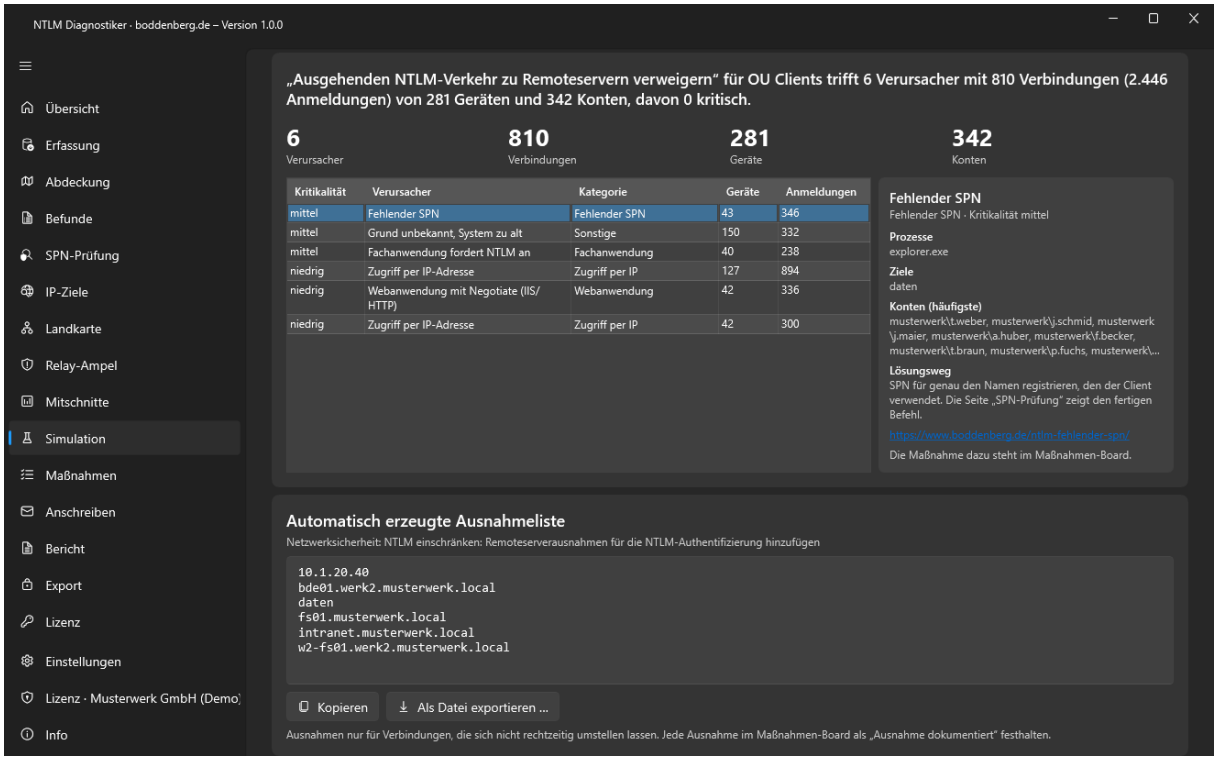
Laborrechner	Anwendung	Serverpfad und Ausnahme.
macOS, Linux	Mount des Domänenpfads	Direkt den Dateiserver ansprechen und Kerberos am Client prüfen.
Client aus vertrauter Domäne	\\musterwerk.local\… über Vertrauensstellung	Gesondert betrachten; Microsoft plant auch hier Verbesserungen.

Zu den einzelnen Gerätegruppen gibt es eigene Beiträge: Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden, Rechner ohne Domäne: Arbeitsgruppen, Laborgeräte und NTLM, Linux und Samba in der Domäne: Kerberos statt NTLM und NTLM über Vertrauensstellungen: Gesamtstrukturen, Domänen und Kerberos. Laufwerkszuordnungen und Skripte, in denen der Domänenpfad steckt, findest du mit den Methoden aus Laufwerkszuordnungen und Anmeldeskripte: NTLM-Fallen per GPO finden.

WARNUNG · Domain Controller zuerst? Lieber nicht.

NTLM auf den Domain Controllern einzuschränken ist ein großer Schritt. Microsoft sagt für diesen Fall selbst voraus, dass Fremdgeräte und Windows-Rechner ohne Domäne dann höchstwahrscheinlich keinen Zugriff mehr auf domänenbasierte DFS-Freigaben haben. Bevor du die Restrict-NTLM-Richtlinien von Überwachen auf Verweigern stellst, muss die Liste der betroffenen Geräte leer oder als Ausnahme dokumentiert sein. Wie Ausnahmelisten funktionieren, steht in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern.

Genau für diese Frage gibt es im NTLM Diagnostiker den Abschalt-Simulator: Er spielt eine Richtlinie gegen die erfassten Verbindungen durch, zeigt die getroffenen Verursacher mit Geräten und Konten und erzeugt daraus eine Ausnahmeliste. Der Vertrauenswert richtet sich nach der Abdeckung, denn ein Rechner, der keine Ereignisse liefert, taucht auch in keiner Simulation auf. Lieferanten von Agenten oder Fachanwendungen, die stur die Namespace-Wurzel abfragen, schickst du mit dem Hersteller-Anschreiben einen Beleg mit Prozess, Ziel und Häufigkeit.



So siehst du im Simulator, welche Verursacher eine Richtlinie zum ausgehenden NTLM-Verkehr treffen würde und welche Ausnahmen daraus entstehen (Demodaten der Musterwerk GmbH).

Wenn du die Umstellung nicht allein planen willst, etwa weil Namespaces, Scan-Ziele und Fachanwendungen in drei Händen liegen, hilft dir die Beratung zur NTLM-Ablösung. Und damit dein Team die Ereignisse künftig selbst sicher liest, gibt es die Schulung zum NTLM Diagnostiker.

FAQ zu DFS, globalen SPNs und NTLM

Was bedeutet Reason-ID 12 bei NTLM-Ereignissen?

In der Praxis steht die 12 meist mit dem Text „The target name is a global SPN like cifs/contoso.com and could not be resolved …“. Das Ziel war also ein Domänenname, zum Beispiel ein domänenbasierter DFS-Pfad. Die 12 ist in KB5064479 nicht dokumentiert. Maßgeblich ist der Begründungstext in NtlmUsageReason, die Nummer ist nur ein Hinweis.

Warum gibt es keinen SPN für cifs/musterwerk.local?

Weil der Domänenname kein einzelner Rechner ist. Laut Microsoft trägt kein Objekt einen solchen SPN, deshalb kann der KDC dafür kein Dienstticket ausstellen.

Fallen Windows-Clients in der Domäne bei DFS auf NTLM zurück?

In der Regel nicht. Microsoft beschreibt, dass sie nach der gescheiterten Ticketanfrage auf ein CIFS-Ticket für einen Domain Controller ausweichen. Treffer von Domänen-PCs stammen meist von Prozessen mit eigener Logik oder Zugriffen auf die Namespace-Wurzel.

Kann ich den SPN cifs/<domäne> einfach selbst registrieren?

Davon raten wir ab. Microsoft nennt das nicht als Lösung, und der SPN würde an genau einem Konto hängen, während der Namespace Clients an verschiedene Server verweist.

Hilft es, Namespace-Server auf FQDN-Verweise umzustellen?

Für die Ziele hinter dem Namespace ja, insbesondere für Clients ohne NetBIOS-Namensauflösung. Den ersten Zugriff auf den Domänennamen ändert es nicht.

Was passiert mit Kopierern und NAS-Systemen, wenn NTLM auf den DCs abgeschaltet wird?

Nach Microsofts Einschätzung verlieren sie höchstwahrscheinlich den Zugriff auf domänenbasierte DFS-Freigaben. Stelle sie vorher auf den direkten Serverpfad um oder führe sie als Ausnahme.

Löst Microsoft das Problem selbst?

Microsoft hat angekündigt, DFS-Zugriffe durchgehend auf Kerberos zu bringen, mit dem Release, das NTLM standardmäßig abschaltet. Saubere SPNs und die Umstellung von Fremdgeräten bleiben trotzdem deine Aufgabe.

Welche Ereignisse zeigen den Grund auf dem Server?

Keine. Der Begründungstext steht nur in 4020/4021 auf dem Client. Auf Server und Domain Controller siehst du 4022/4023, 4030 bis 4033 oder klassisch 8003 und 8004 mit dem anfragenden Client.

Gilt das auch für Standalone-Namespaces?

Nein, nicht in dieser Form. Ein Standalone-Namespace wird über den Namen eines Servers angesprochen, etwa \\fs01.musterwerk.local\daten, und dafür existiert ein normaler SPN am Computerkonto.

Fazit: Der Domänenpfad bleibt, der Rückfallweg nicht

\\musterwerk.local\daten ist ein guter Pfad, und du musst ihn nicht abschaffen. Für Windows-Clients in der Domäne hat Microsoft den fehlenden SPN längst umschifft, und eine Plattformlösung für den Rest ist angekündigt. Das Problem sind die Geräte und Prozesse, die den Ausweg über den Domain Controller nicht kennen: Kopierer, Arbeitsgruppen-Rechner, Fremdclients und Agenten, die die Namespace-Wurzel abgrasen. Die findest du nur, wenn du nach dem Begründungstext filterst und nicht nach einer Nummer, die in keiner offiziellen Liste steht.

Räum die Ordnerziele auf, gib Fremdgeräten einen direkten Serverpfad, und lass die Finger von selbst gebauten Domänen-SPNs. Dann ist der Tag, an dem NTLM auf den Domain Controllern fällt, für deinen Namespace ein ganz normaler Arbeitstag. Für den Kopierer im zweiten Stock vielleicht nicht, aber der hatte ohnehin noch nie einen guten Tag. Die vollständige Liste der Prüfpunkte vor dem Stichtag findest du in Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet
› Scan-to-Folder ohne NTLM: Multifunktionsgeräte richtig anbinden
› Rechner ohne Domäne: Arbeitsgruppen, Laborgeräte und NTLM
› Laufwerkszuordnungen und Anmeldeskripte: NTLM-Fallen per GPO finden
› Mit klist prüfen, ob Kerberos wirklich greift
› NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte
› Microsoft Kerberos
› Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben