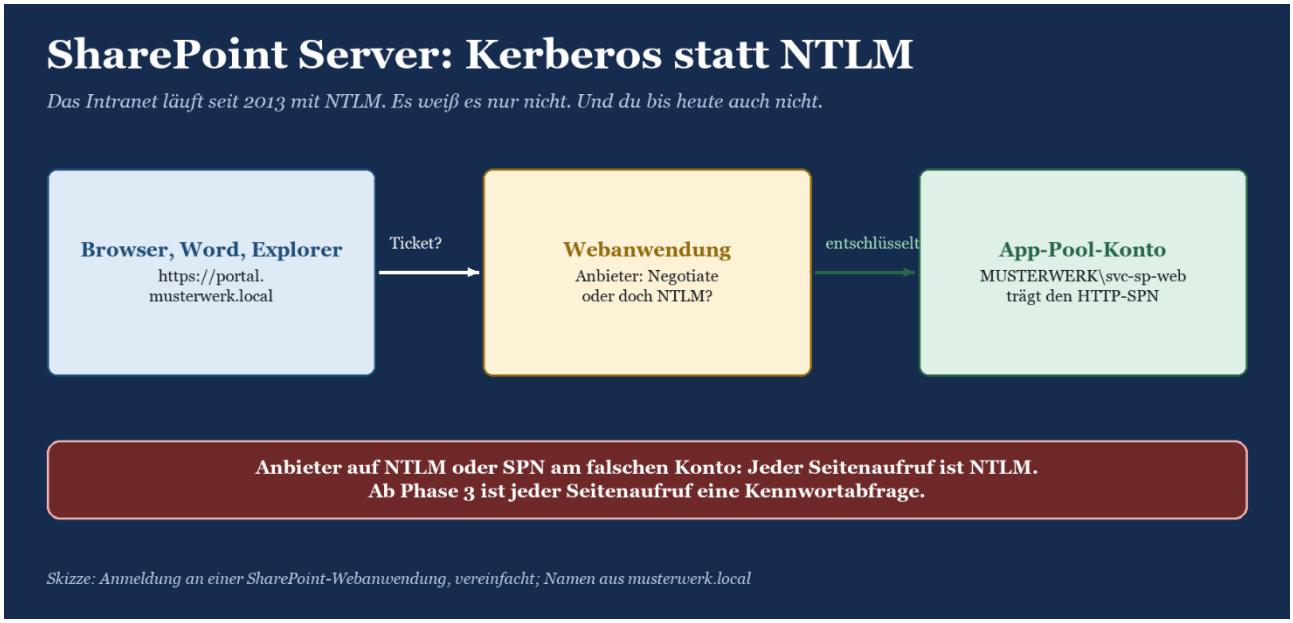
SharePoint Server: Kerberos statt NTLM für Webanwendungen



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

BERATUNG
SharePoint-Farm mit Zonen, Load Balancer und Suche? Wir sortieren mit.
› **Beratung zur NTLM-Ablösung**

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

SharePoint Server ist das Intranet, das niemand mehr anfasst, weil es ja läuft. Die Farm wurde irgendwann zwischen 2013 und 2019 aufgesetzt, später auf die Subscription Edition (SE) migriert, und bei der Frage „NTLM oder Negotiate (Kerberos)?“ im Assistenten für neue Webanwendungen hat jemand das Häkchen dort gelassen, wo es stand: bei NTLM. Seitdem meldet sich jeder Seitenaufruf, jedes in Word geöffnete Dokument und jeder Crawl-Durchlauf der Suche per NTLM an. Tausendfach am Tag, völlig geräuschlos.

Geräuschlos bleibt das nicht. NTLMv1 ist für Single Sign-on seit dem Update vom 13.10.2026 auf Windows 11 ab 24H2 und Windows Server 2025 standardmäßig blockiert, und mit der nächsten Windows-Server-Version ist NTLM insgesamt standardmäßig abgeschaltet. Dann wird aus dem Intranet eine Kennwortabfrage mit angeschlossenem Helpdesk-Ticket. Wer nach sharepoint server kerberos ntlm sucht, will genau das vermeiden. In diesem Beitrag stellst du die Webanwendungen deiner Farm auf Negotiate um, setzt die HTTP-SPNs für Hostnamen und Load-Balancer-Namen an die richtigen Anwendungspool-Konten, nimmst die Suche und das Crawl-Konto mit und prüfst, was Word, Excel und der Explorer dazu sagen.

Wie Negotiate im IIS grundsätzlich funktioniert, warum Kernelmodus-Authentifizierung und Anwendungspool-Identität zusammenpassen müssen und wie du Anbieterlisten liest, steht bereits in NTLM in IIS und Webanwendungen: Negotiate statt NTLM. Den Zeitplan der Ablösung erklärt NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Hier geht es nur um das, was SharePoint anders macht.

FAKTEN · SharePoint und Kerberos in 30 Sekunden

Jede Zone einer Webanwendung hat einen eigenen Authentifizierungsanbieter. Bei Windows-Anmeldung wählst du zwischen NTLM und Negotiate (Kerberos). Steht die Zone auf NTLM, hilft der schönste SPN nichts.

Der HTTP-SPN gehört an das Domänenkonto, unter dem der Anwendungspool der Webanwendung läuft, nicht an die Computerkonten der Frontend-Server. Laufen alle Frontends mit demselben Konto, deckt ein SPN für den Load-Balancer-Namen die ganze Farm ab.

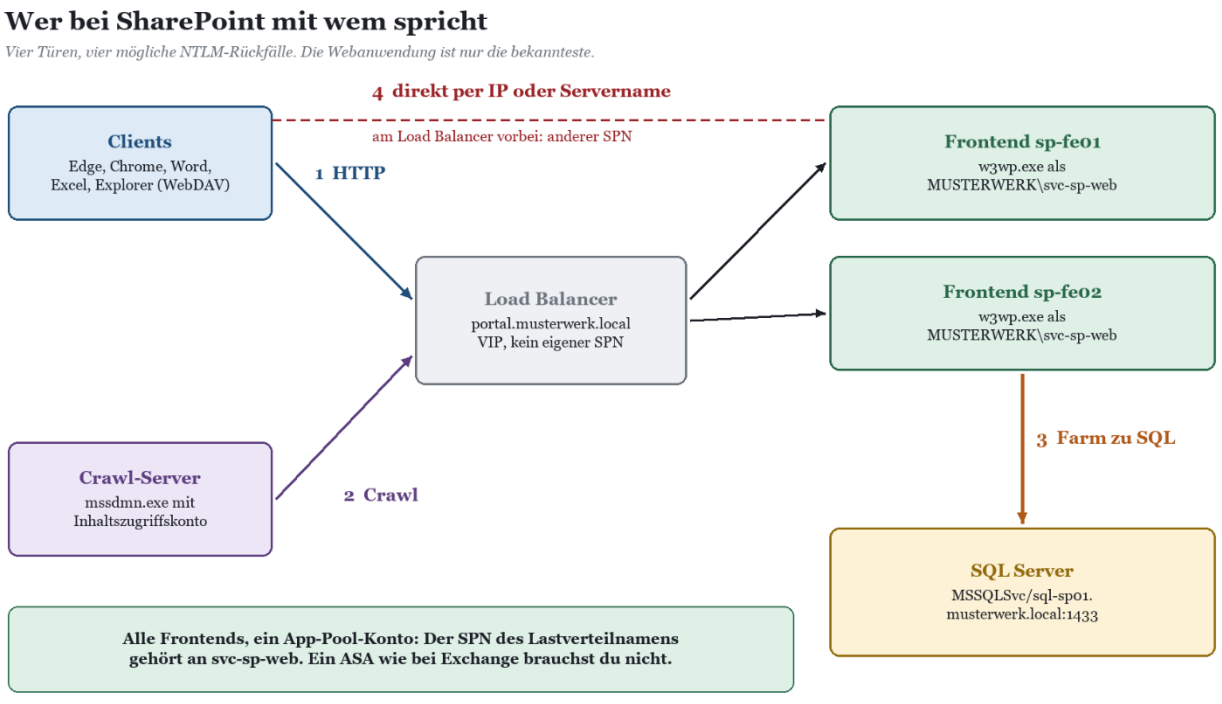
Ein SPN mit der Dienstklasse HTTP gilt für http und https gleichermaßen. Ein eigener HTTPS-SPN existiert nicht.

Microsoft weist darauf hin: Läuft eine Webanwendung im Windows-Claims-Modus ausschließlich mit Kerberos ohne NTLM-Rückfall, funktioniert die App-Authentifizierung (Add-ins) nicht. Prüfe vor der NTLM-Abschaltung, ob du solche Add-ins betreibst.

SharePoint Server 2016 und 2019 sind seit dem 14.07.2026 aus dem Support. Alles Folgende gilt für SharePoint Server SE, funktioniert technisch aber genauso in den Vorgängern.

Wo SharePoint Server NTLM nutzt

SharePoint ist mehr als eine Website im IIS. Eine Farm besteht aus mehreren Webanwendungen mit je bis zu fünf Zonen, einer Zentraladministration, Dienstanwendungen, der Suche und einer Datenbankverbindung. NTLM kann an vier Stellen auftauchen, und nur eine davon sieht man im Browser.



Skizze: SharePoint-Farm der Musterwerk GmbH, vereinfacht

Weg	Wer meldet sich an	SPN, den der Client sucht	Typischer NTLM-Grund
Seitenaufruf im Browser	Edge, Chrome, Firefox	HTTP/portal.musterwerk.local	Zone steht auf NTLM oder SPN fehlt
Dokument in Word oder Excel öffnen	WINWORD.EXE, EXCEL.EXE	HTTP/portal.musterwerk.local	Seite nicht in der Intranetzone, Aufruf per Servername
Explorer-Ansicht,	svchost.exe	HTTP/portal.musterwerk.local	Laufwerk per IP oder

WebDAV-Laufwerk	(WebClient-Dienst)		Kurzname verbunden
Suche crawlt Inhalte	mssdmn.exe mit Crawl-Konto	HTTP/<Name der Standardzone>	Startadresse mit Servername, SPN fehlt
Farm zur Datenbank	w3wp.exe, OWSTIMER.EXE	MSSQLSvc/sql-sp01.musterwerk.local:1433	SQL-SPN fehlt, Alias per IP

Die Datenbankseite behandelt SQL Server und NTLM: Windows-Anmeldung auf Kerberos umstellen ausführlich; dort steht auch, wie du einen SQL-Alias der Farm auf einen Namen mit passendem MSSQLSvc-SPN umstellst. In diesem Beitrag bleiben wir bei HTTP.

So sieht SharePoint in den Ereignissen aus

Auf den Clients erscheinen ausgehende NTLM-Anmeldungen als Ereignis 4020 (erweitertes Auditing) beziehungsweise 8001 (klassische Überwachung). Auf den Frontend-Servern landen die eingehenden Anmeldungen als 4022 und als 8003. Wichtig: 8003 kommt auf jedem Mitgliedsserver vor, nicht nur auf Domain Controllern, und das Feld „Workstation“ nennt dir den anfragenden Client. Wie du das Auditing einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; die passende Gruppenrichtlinie legt dir das NTLM-Audit-GPO-Skript an.

Feld	Typischer Wert bei SharePoint	Was es dir sagt
ProcessName	msedge.exe, WINWORD.EXE, svchost.exe, mssdmn.exe	Browser, Office, WebDAV oder Suche
TargetService	HTTP/portal.musterwerk.local	Name, für den kein Ticket kam
TargetMachine / TargetIP	portal.musterwerk.local oder 10.20.0.80	IP statt Name heißt fast immer: Zugriff per IP
NtlmUsageReason	Begründungstext	maßgeblich ist der Text, nicht die Nummer
Username	MUSTERWERK\svc-sp-crawl	Dienstkonto statt Mensch: Suche oder Timer
RemoteClientMachine (4022)	Clientname	auf dem Frontend: wer kommt per NTLM

Die Reason-ID ist nur ein Hinweis. In der Praxis passen Nummer und Begründungstext nicht immer zusammen, beobachtet etwa Reason-ID 10 mit dem Text „The target name could not be resolved by Kerberos or other protocols.“ Maßgeblich ist deshalb das Feld NtlmUsageReason. Mehr dazu in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Und weil über Windows Event Forwarding weitergeleitete Ereignisse einen leeren Meldungstext haben können, wertest du immer die EventData-Felder aus:

```
# Ausgehende NTLM-Anmeldungen gegen HTTP-Ziele auf einem Client
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -FilterXPath
'*[System[EventID=4020]]' |
  ForEach-Object {
    $x = [xml]$_.ToXml(); $f = @{}
    $x.Event.EventData.Data | ForEach-Object { $f[$_.Name] = $_.'#text' }
    [pscustomobject]@{ Zeit=$_.TimeCreated; Prozess=$f.ProcessName;
      Ziel=$f.TargetService; Grund=$f.NtlmUsageReason }
  } | Where-Object Ziel -like 'HTTP/*' | Group-Object Prozess, Ziel | Sort-Object Count -Desc
```

Weitere Rezepte für Get-WinEvent sammelt NTLM-Ereignisse mit PowerShell auswerten: Get-WinEvent-Rezepte.

Die Webanwendung auf Negotiate umstellen

Die eigentliche Umstellung ist in SharePoint unspektakulär. Spektakulär wird sie nur, wenn du sie vor den SPNs machst. Dann funktioniert es zwar weiter, weil Negotiate still auf NTLM zurückfällt, aber du glaubst, fertig zu sein. Die schlimmere Variante: Du setzt den SPN an das falsche Konto, Kerberos klappt mit einem Fehler beim Entschlüsseln, und der Browser zeigt eine Kennwortabfrage, die niemand bestehen kann.

Was der Authentifizierungsanbieter einer Zone wirklich bewirkt

Die Einstellung in der Zentraladministration landet als Anbieterliste im IIS

Einstellung der Zone	IIS-Anbieter	Ergebnis ohne SPN	Ergebnis mit SPN
Integrierte Windows-Auth.: NTLM	NTLM	NTLM	NTLM, SPN wirkungslos
Integrierte Windows-Auth.: Negotiate (Kerberos)	Negotiate, NTLM	Negotiate fällt still auf NTLM zurück	Kerberos
Standardauthentifizierung	Basic	Kennwort bei jeder Anfrage, nur TLS schützt	kein Kerberos
Trusted Identity Provider (SAML)	keine Windows-Auth.	kein NTLM im Spiel	kein NTLM im Spiel

Skizze: gilt je Zone einer Webanwendung; jede erweiterte Zone hat ihren eigenen Anbieter

Inventar: Zonen, Hostnamen und Anwendungspool-Konten

Bevor du irgendetwas änderst, schreibst du auf, welche Webanwendung unter welchem Namen erreichbar ist und unter welchem Konto ihr Anwendungspool läuft. Die Verwaltungsshell liefert beides:

```
# Alle Webanwendungen mit Zonen, URL, Anbieter und Anwendungspool-Konto
Get-SPWebApplication | ForEach-Object {
  $wa = $_
  foreach ($z in $wa.IisSettings.Keys) {
    $ap = Get-SPAuthenticationProvider -WebApplication $wa -Zone $z |
          Where-Object { $_.DisplayName -eq 'Windows Authentication' }
    [pscustomobject]@{
      Webanwendung = $wa.DisplayName
      Zone         = $z
      Url          = ($wa.AlternateUrls | Where-Object Zone -eq $z | Select-Object -First
1).IncomingUrl
      Kerberos     = if ($ap) { -not $ap.DisableKerberos } else { 'keine Windows-Auth.' }
      PoolKonto    = $wa.ApplicationPool.Username
    }
  }
} | Format-Table -AutoSize
```

Typisch für eine gewachsene Farm sieht das Ergebnis so aus: Portal und Teamsites laufen unter einem gemeinsamen Webkonto, die Meine-Websites-Hostwebanwendung unter einem zweiten, die Zentraladministration unter dem Farmkonto. Mehrere Webanwendungen mit demselben Konto sind für Kerberos ausdrücklich bequem: alle SPNs an ein Konto, fertig. Welche Konten wo laufen und wie du sie generell auf Kerberos trimmst, beschreibt Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen.

HTTP-SPNs für Hostnamen und Load-Balancer-Namen

Der Client bildet den SPN aus dem Namen, den er in der Adresszeile hat. Steht dort portal.musterwerk.local, sucht er HTTP/portal.musterwerk.local. Hinter einem Load Balancer ist das der Name der virtuellen IP, nicht der Name eines Frontends. Weil alle Frontends den Anwendungspool mit demselben Domänenkonto betreiben, kann jedes von ihnen das Ticket entschlüsseln, egal wohin der Load Balancer die Verbindung schickt. Genau hier ist SharePoint angenehmer als Exchange, wo dafür ein eigenes alternatives Dienstkonto nötig ist (siehe Exchange Server und Outlook: NTLM bei MAPI over HTTP und EWS).

```
# 1. Gibt es den SPN schon, und wenn ja, wo?
setspn -Q HTTP/portal.musterwerk.local
setspn -Q HTTP/portal

# 2. An das Anwendungspool-Konto hängen (-S prüft vorher auf Duplikate)
setspn -S HTTP/portal.musterwerk.local MUSTERWERK\svc-sp-web
setspn -S HTTP/portal MUSTERWERK\svc-sp-web

# 3. Gegenprobe: alle SPNs des Kontos, Duplikate in der Gesamtstruktur
setspn -L MUSTERWERK\svc-sp-web
setspn -F -X
```

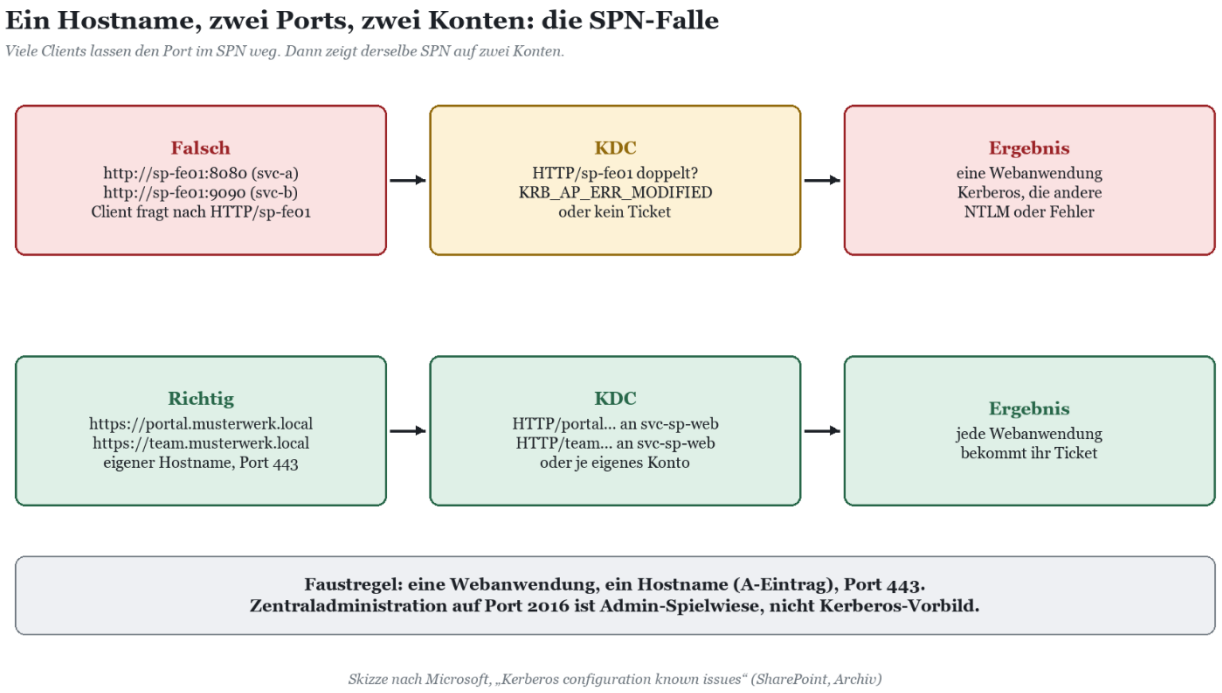
Den Kurznamen brauchst du nur, wenn Anwenderinnen und Anwender ihn tatsächlich eintippen oder alte Verknüpfungen ihn enthalten. Besser ist es, Kurznamen per Umleitung auf den vollqualifizierten Namen zu schicken und den SPN gar nicht erst zu brauchen. Hängt ein HTTP-SPN für denselben Namen noch am Computerkonto eines Frontends oder an einem alten Konto aus der Migration, ist das ein doppelter SPN. Der KDC stellt dann irgendein Ticket aus, und das falsche Konto bekommt es nicht auf.

Situation	SPNs	Worauf du achtest
Ein Frontend, Zugriff per Servername	HTTP/sp-fe01.musterwerk.local am Pool-Konto	Kollision mit dem HOST-SPN des Computerkontos ist kein Problem, aber kein zweites Konto mit HTTP/sp-fe01
Mehrere Frontends hinter Load Balancer	HTTP/portal.musterwerk.local am Pool-Konto	kein SPN für den VIP-Namen an einem Computerkonto
Mehrere Webanwendungen, ein Konto	je Hostname ein SPN am selben Konto	einfachster Fall
Mehrere Webanwendungen, mehrere Konten	je Hostname ein SPN am jeweiligen Konto	nie zwei Webanwendungen mit verschiedenen Konten auf demselben Hostnamen
Hostname als CNAME	SPN für den Namen, den der Client nach Auflösung verwendet	Verhalten unterscheidet sich je nach Client, A-Eintrag ist sicherer
Hostbenannte Websitesammlungen	je Hostname ein SPN am Pool-Konto	neue Hostnamen kommen bei jedem neuen Projekt dazu

WARNUNG · Der CNAME, den alle lieben

Viele Intranets heißen intranet.musterwerk.local und sind ein CNAME auf sp-fe01 oder auf den Load-Balancer-Namen. Manche Clients bauen den SPN aus dem Alias, manche aus dem kanonischen Namen hinter dem CNAME. Microsoft hat dieses Verhalten für SharePoint bereits früh als bekanntes Problem dokumentiert und empfiehlt für Kerberos-Webanwendungen A-Einträge. Wenn du den CNAME behalten musst, prüfst du mit klist auf zwei Clients unterschiedlicher Bauart, nach welchem SPN tatsächlich gefragt wird.

Wie Windows, Edge und Chrome Aliasnamen auflösen und warum die hosts-Datei dabei mitspielt, erklärt CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet im Detail.



Skizze nach Microsoft, „Kerberos configuration known issues" (SharePoint, Archiv)

Die zweite Falle sind Ports. Viele Clients lassen bei Ports außer 80 und 443 die Portnummer im SPN weg. Laufen zwei Webanwendungen auf demselben Hostnamen mit unterschiedlichen Ports und unterschiedlichen Anwendungspool-Konten, brauchen beide denselben SPN, und das geht nicht. Microsoft nennt für diesen Fall genau zwei Auswege: ein gemeinsames Konto für alle betroffenen Webanwendungen oder je ein eigener Hostname. Der eigene Hostname auf Port 443 ist die saubere Lösung.

Den Anbieter umschalten

In der Zentraladministration findest du die Einstellung unter Anwendungsverwaltung, Webanwendungen verwalten, Webanwendung markieren, Authentifizierungsanbieter, Zone wählen. Im Abschnitt „Integrierte Windows-Authentifizierung" stellst du von NTLM auf „Negotiate (Kerberos)". Per PowerShell geht es zonengenau und nachvollziehbar:

```
$wa = Get-SPWebApplication https://portal.musterwerk.local
$ap = New-SPAuthenticationProvider -UseWindowsIntegratedAuthentication -DisableKerberos:$false
Set-SPWebApplication -Identity $wa -Zone Default -AuthenticationProvider $ap

# Kontrolle
Get-SPAuthenticationProvider -WebApplication $wa -Zone Default |
  Select-Object DisplayName, DisableKerberos, UseWindowsIntegratedAuthentication

# Rücknahme: -DisableKerberos:$true stellt die Zone wieder auf NTLM
```

SharePoint schreibt die Änderung auf allen Frontends in die IIS-Konfiguration der jeweiligen Website: Die Anbieterliste lautet danach Negotiate, NTLM. Prüfe auf einem Frontend, dass die Website weiterhin ohne Kernelmodus-Authentifizierung läuft; wurde die irgendwann von Hand eingeschaltet, versucht HTTP.sys das Ticket mit dem Schlüssel des Computerkontos zu öffnen, und dein SPN am Pool-Konto läuft ins Leere. Warum das so ist, steht im IIS-Beitrag.

TIPP · Pilot mit einer erweiterten Zone

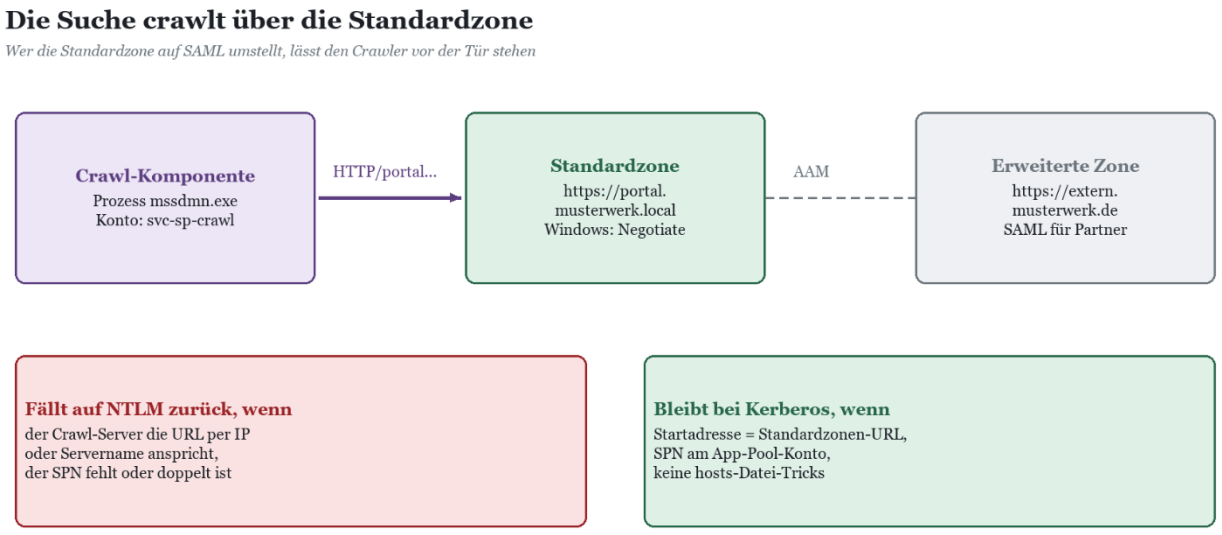
Du willst nicht das ganze Intranet auf einmal umstellen? Erweitere die Webanwendung um eine Zone mit eigenem Hostnamen, etwa portal-test.musterwerk.local, setze dort Negotiate und den passenden SPN und lass die IT-Abteilung eine Woche lang darüber arbeiten. Danach weißt du, ob Office, Explorer-Ansicht und Add-ins mitspielen, ohne dass die Buchhaltung etwas davon merkt. Zone anschließend wieder entfernen, SPN löschen.

WICHTIG · Große Tickets, kurze Köpfe

Kerberos-Tickets von Konten mit sehr vielen Gruppenmitgliedschaften werden groß. Sie wandern Base64-kodiert im Authorization-Header, und HTTP.sys hat Grenzen für die Kopfzeilenlänge. Das Symptom ist ein HTTP-Fehler 400 bei genau den Leuten, die überall Mitglied sind: Geschäftsführung und IT. Teste vor dem Rollout mit einem solchen Konto und prüfe die Microsoft-Empfehlungen zu den HTTP.sys-Grenzwerten, bevor du an SharePoint zweifelst.

Suche, Crawl-Konto und Office-Clients

Nach der Umstellung des Browsers bleiben zwei Gruppen übrig, die in den Ereignissen gerne weiter NTLM produzieren: die Suche, die mit ihrem eigenen Konto durch alle Websites läuft, und die Office-Clients, die Dokumente über ihren eigenen HTTP-Stapel öffnen.



Skizze: Inhaltsquelle „Lokale SharePoint-Websites“, vereinfacht

Suche und Crawl-Konto

Die Crawl-Komponente meldet sich mit dem Standardkonto für den Inhaltszugriff an, den der Prozess mssdmn.exe auf dem Crawl-Server verwendet. Sie crawlt SharePoint-Inhalte über die Standardzone der Webanwendung. Für die NTLM-Ablösung bedeutet das: Die Standardzone muss Windows-Authentifizierung mit Negotiate anbieten, die Startadressen der Inhaltsquelle „Lokale SharePoint-Websites“ müssen den Hostnamen der Standardzone verwenden, und der SPN dieses Namens muss am Pool-Konto hängen. Startadressen mit Servernamen oder IP-Adressen aus der Einrichtungszeit sind ein Klassiker, ebenso hosts-Einträge auf dem Crawl-Server, die den Load Balancer umgehen.

Prüfpunkt	Wo	Erwartung

Startadressen der Inhaltsquellen	Suchdienstanwendung, Inhaltsquellen	nur Hostnamen der Standardzone, keine IP, kein Servername
Anbieter der Standardzone	Get-SPAuthenticationProvider -Zone Default	Windows-Authentifizierung, DisableKerberos = False
hosts-Datei des Crawl-Servers	C:\Windows\System32\drivers\etc\hosts	Einträge bewusst und dokumentiert, Name unverändert
Personensuche	Startadresse sps3s:// der Meine-Websites-Hostanwendung	SPN für deren Hostnamen am zugehörigen Pool-Konto
Crawl-Ergebnis	Crawlprotokoll	keine Zugriffsfehler nach der Umstellung
NTLM-Ereignisse	4020 auf dem Crawl-Server, Username = Crawl-Konto	keine neuen Einträge mit HTTP-Zielen

WARNUNG · SAML in der Standardzone

Wer die Standardzone auf einen vertrauenswürdigen Identitätsanbieter (SAML) umstellt und Windows dort abschaltet, nimmt dem Crawler die Anmeldemöglichkeit. Die Standardzone bleibt die Zone mit Windows-Authentifizierung. Externe Anmeldungen gehören in eine erweiterte Zone.

Word, Excel, Explorer und WebDAV

Office meldet sich beim Öffnen eines Dokuments mit seiner Windows-Anmeldung automatisch an, wenn die Adresse in der Intranetzone liegt. Liegt sie nicht dort, gibt es eine Kennwortabfrage oder, schlimmer, eine gespeicherte Anmeldung in der Anmeldeinformationsverwaltung, die munter NTLM spricht. Die Zonenzuordnung verteilst du per Gruppenrichtlinie über die Liste der Sites zu Zonen; wie das für Edge, Chrome und Firefox zusammenspielt, steht in Edge, Chrome und Firefox: Browser für Kerberos im Intranet einstellen.

- **WINWORD.EXE und EXCEL.EXE in 4020:** Meist ist der Name korrekt, aber die Zone fehlt, oder das Dokument wurde über einen alten Link mit Servernamen geöffnet.
- **svchost.exe mit HTTP-Ziel:** Das ist der WebClient-Dienst, also die Explorer-Ansicht oder ein als Laufwerk verbundener Dokumentbibliothekspfad. Gern per Anmeldeskript mit \\10.20.0.80@SSL\ verbunden. IP heißt NTLM, immer.
- **Gespeicherte Anmeldeinformationen:** Einträge für portal.musterwerk.local in der Anmeldeinformationsverwaltung erzwingen eine explizite Anmeldung. Entfernen und testen.
- **Fachanwendungen mit SharePoint-Zugriff:** Workflow-Werkzeuge, Dokumentenimporte und Skripte, die per CSOM oder REST mit fest eingestellter NTLM-Anmeldung arbeiten. Hier hilft nur der Blick in die Konfiguration oder die Frage an den Hersteller.

AUS DER PRAXIS · Sparfuchs & Partner und das Q-Laufwerk

Bei der Sparfuchs & Partner Steuerberatungs GmbH lief das Portal nach der Umstellung sauber mit Kerberos, der Browser zeigte Tickets für HTTP/portal.sparfuchs.local. Trotzdem blieben täglich einige Hundert NTLM-Anmeldungen am Frontend übrig, alle von svchost.exe. Die Ursache: Ein Anmeldeskript aus dem Jahr 2016 verband die Mandantenbibliothek als Laufwerk Q: über die IP-Adresse des damaligen Einzelservers, inzwischen die virtuelle IP des Load Balancers. Das Laufwerk funktionierte, also hat es nie jemand angefasst. Eine Zeile im Skript später waren auch diese Anmeldungen Kerberos.

Solche Fundstellen in Gruppenrichtlinien und Anmeldeskripten systematisch aufzuspüren, ist Thema von Laufwerkszuordnungen und Anmeldeskripte: NTLM-Fallen per GPO finden.

Von einer Farm zu zwanzig Hostnamen: SPNs im Griff behalten

Für eine Webanwendung mit einem Hostnamen ist das alles in einer Stunde erledigt. In einer Klinik oder Kreisverwaltung sieht die Farm anders aus: Portal, Teamsites, Projektwebsites, Meine Websites, ein Dutzend hostbenannter Websitesammlungen für Abteilungen und Fachverfahren, dazu Aliasnamen aus drei Umbenennungen und ein Load Balancer, auf den jedes Jahr ein neuer Name kommt. Jeder dieser Namen braucht genau einen SPN am richtigen Konto. Mit setspn prüfst du einen Namen nach dem anderen, und für jeden Alias musst du erst herausfinden, worauf er zeigt und nach welchem SPN die Clients eigentlich fragen.

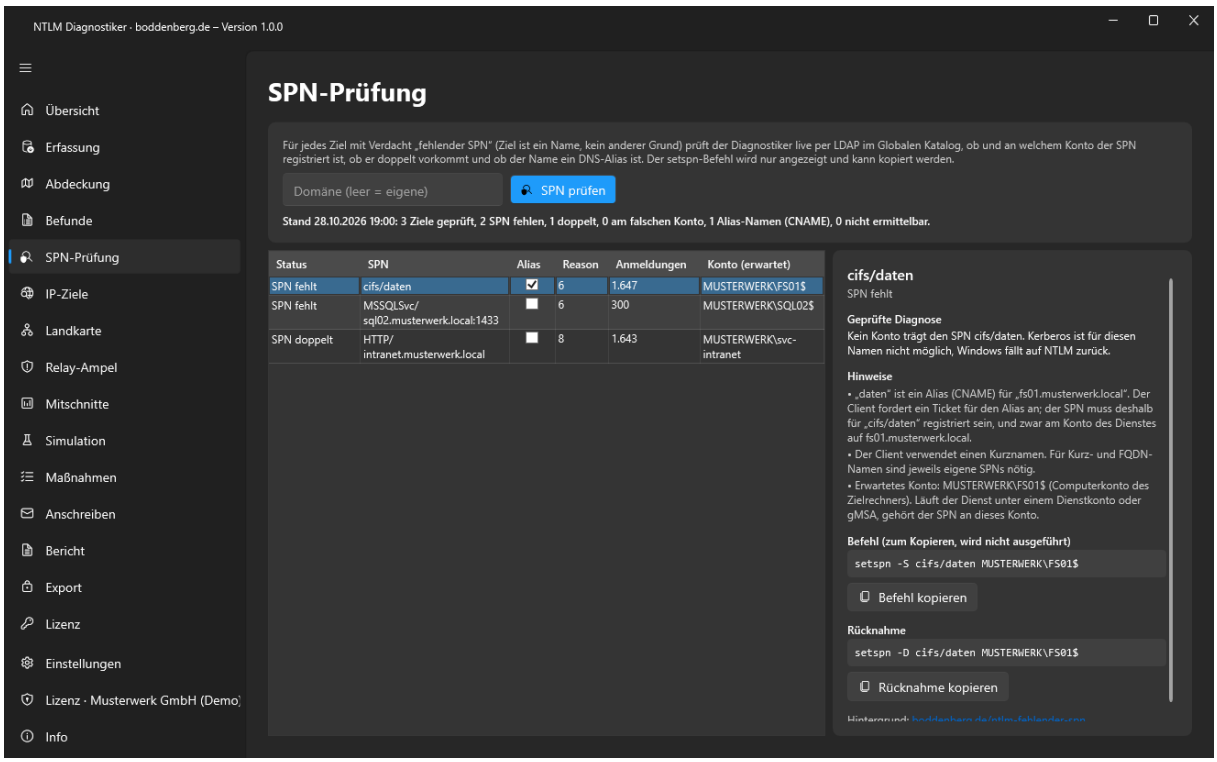
Mit Bordmitteln heißt das: NTLM-Ereignisse von Clients und Frontends einsammeln, die HTTP-Ziele über die EventData-Felder herausziehen, jeden Namen per DNS auflösen, gegen das Active Directory halten und eine Liste mit fehlenden und doppelten SPNs pflegen. Diese Fleißarbeit nimmt dir der NTLM Diagnostiker ab. Er arbeitet ausschließlich lesend, sammelt die Ereignisse direkt vom Domain Controller, über einen Windows Event Collector, per Direktabfrage oder aus importierten Dateien und fasst gleichartige Verbindungen nach Ursache, Prozess und Ziel zusammen.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · SPN-Prüfung mit Aliasnamen für SharePoint-Hostnamen

Die SPN-Prüfung nimmt jedes Ziel aus den NTLM-Ereignissen, also auch jeden SharePoint-Hostnamen, und hält es gegen das Active Directory. Sie meldet fehlende SPNs, doppelte SPNs und Aliasnamen. Steckt hinter einem Namen ein CNAME, kennzeichnet sie das Ziel als Alias und zeigt dir, welches Konto den SPN erwartungsgemäß tragen müsste.

Rechts im Detailbereich stehen die geprüfte Diagnose, Hinweise zum Alias und der passende Befehl setspn -S zum Kopieren, dazu die Rücknahme mit setspn -D. Ausführen tust du den Befehl selbst, der Diagnostiker ändert nichts an deinem Active Directory. Bei SharePoint prüfst du vor dem Kopieren, ob als Konto das Anwendungspool-Konto der Webanwendung eingetragen ist; das Inventar aus der Verwaltungsshell oben liefert dir die Zuordnung.

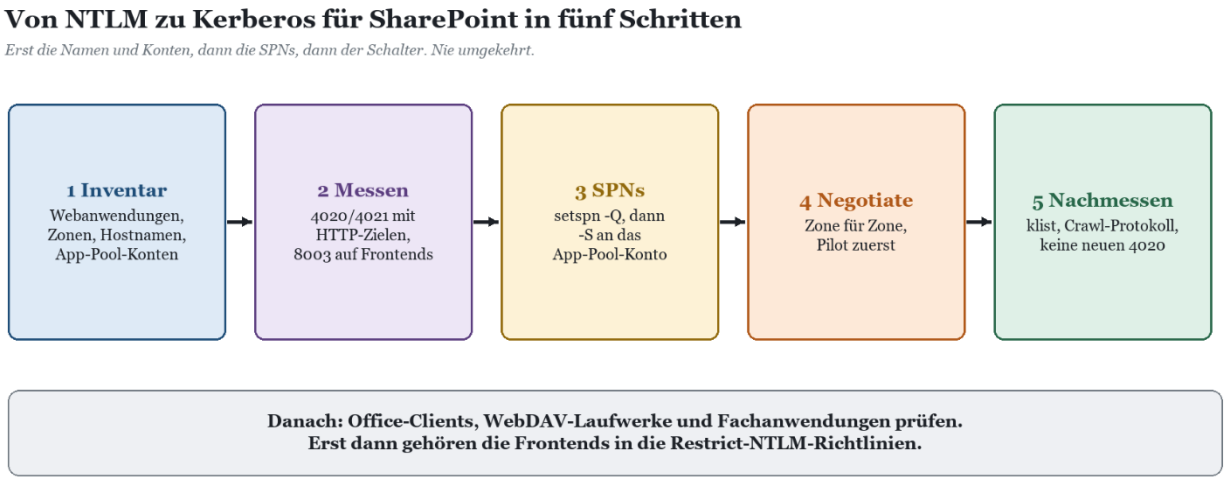
Die Ursachen-Engine wertet dafür den Begründungstext in NtlmUsageReason aus, nicht nur die Nummer. Du siehst also, ob der Name keinen SPN hat oder ob ein Client gar nicht erst nach einem Namen gefragt hat, weil er per IP kam.



So erkennst du in der SPN-Prüfung, dass ein Alias-Name einen eigenen SPN braucht, und kopierst den passenden setspn-Befehl samt Rücknahme. Das Beispiel zeigt einen Dateiserver-Alias (Demodaten).

Readiness-Ampel, Abdeckungskarte, Top-10-Verursacher und Hinweise aus der Wissensbasis bekommst du in der kostenlosen Express-Edition als Fünf-Minuten-Befund direkt vom Domain Controller. Die SPN-Prüfung testest du im siebentägigen Testzeitraum, einmal pro Domäne. Wenn du Zonen, Load Balancer und Suche lieber gemeinsam planst, ist die Beratung zur NTLM-Ablösung der richtige Ansprechpartner.

Umstellen ohne Kennwortabfrage-Festival: Reihenfolge und Erfolgskontrolle

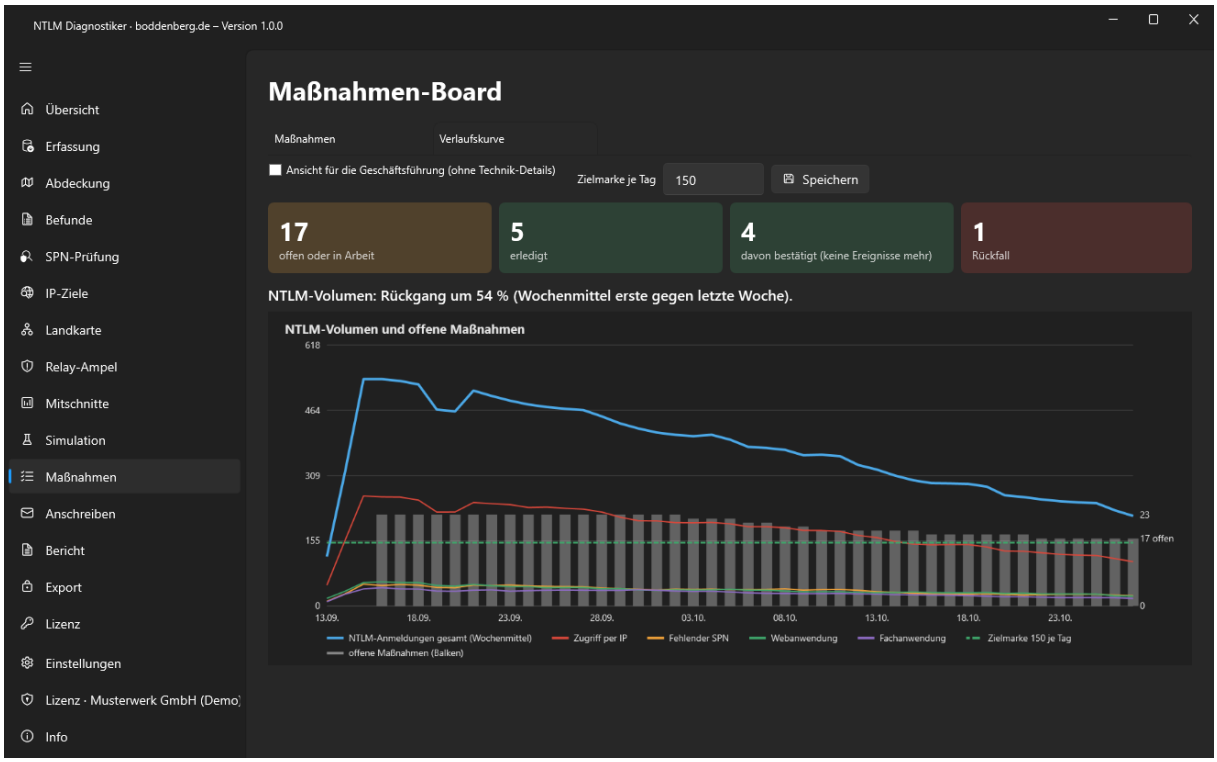


Skizze: Reihenfolge beispielhaft für die Musterwerk GmbH

Bei SharePoint ist die Reihenfolge entscheidend, weil ein Fehler nicht einen Server betrifft, sondern das Intranet aller Anwenderinnen und Anwender. Deshalb gilt: Inventar, Messen, SPNs prüfen und setzen, erst dann den Anbieter umschalten, Zone für Zone, Pilot zuerst.

Schritt	Werkzeug	Erfolgskriterium
Webanwendungen, Zonen, Konten erfassen	Get-SPWebApplication, Get-SPAuthenticationProvider	Tabelle aus Hostname, Zone, Anbieter, Pool-Konto
NTLM gegen SharePoint-Namen messen	4020/4021 auf Clients, 4022/8003 auf Frontends	Liste aus Prozess, Ziel, Begründung, Anzahl
SPNs prüfen und setzen	setspn -Q, setspn -S, setspn -F -X	jeder Hostname genau einmal, am Pool-Konto
Anbieter umschalten	Set-SPWebApplication -AuthenticationProvider	DisableKerberos = False in jeder Windows-Zone
Große Tickets testen	Testkonto mit vielen Gruppen	kein HTTP 400
Suche prüfen	Inhaltsquellen, Crawlprotokoll	voller Crawl ohne Zugriffsfehler
Office und WebDAV nachziehen	Sites-zu-Zonen-Liste, Anmeldeskripte	keine 4020 von WINWORD.EXE oder svchost.exe mit HTTP-Zielen
Nachmessen	klist, NTLM-Ereignisse	Tickets für HTTP/<Hostname>, keine neuen 4020

Ob Kerberos wirklich greift, siehst du auf dem Client an einem Ticket für HTTP/portal.musterwerk.local; wie du klist dafür liest, erklärt Mit klist prüfen, ob Kerberos wirklich greift. Erst wenn keine NTLM-Anmeldungen gegen die SharePoint-Namen mehr auftauchen, nimmst du die Frontends in die Restrict-NTLM-Richtlinien auf, wie in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern beschrieben. Dass danach nichts zurückfällt, überwachst du wie in Nach der Abschaltung: Rückfälle erkennen und NTLM-frei bleiben.



So verfolgst du in der Verlaufskurve, wie die NTLM-Anmeldungen nach Quelle, etwa Webanwendung oder fehlender SPN, über die Wochen sinken (Demodaten).

WARNUNG · Die Rücknahme gehört in den Änderungsantrag

Der Rückweg ist kurz: Zone wieder auf NTLM stellen (DisableKerberos:$true). SPNs musst du dafür nicht löschen, ein vorhandener SPN schadet einer NTLM-Zone nicht. Schreib das in den Änderungsantrag, bevor du anfängst. Nach der NTLM-Abschaltung gibt es diesen Rückweg allerdings nicht mehr. Bis dahin muss alles sauber sein.

FAQ zu SharePoint Server, NTLM und Kerberos

Nutzt SharePoint Server standardmäßig NTLM oder Kerberos?

Das hängt davon ab, was beim Anlegen der Webanwendung gewählt wurde. In sehr vielen Farmen steht die Windows-Authentifizierung der Zonen auf NTLM. Prüfe es je Zone mit Get-SPAuthenticationProvider und dem Wert DisableKerberos.

An welches Konto gehört der HTTP-SPN einer SharePoint-Webanwendung?

An das Domänenkonto, unter dem der IIS-Anwendungspool der Webanwendung läuft. Nicht an die Computerkonten der Frontends und nicht an das Farmkonto, sofern das nicht zufällig der Pool ist.

Brauche ich für den Load Balancer ein zusätzliches Konto wie bei Exchange?

Nein. Weil alle Frontends den Anwendungspool mit demselben Domänenkonto betreiben, reicht ein SPN für den Load-Balancer-Namen an diesem Konto.

Brauche ich einen eigenen SPN für HTTPS?

Nein. Die Dienstklasse HTTP gilt für http und https. Für eine Webanwendung auf https://portal.musterwerk.local setzt du HTTP/portal.musterwerk.local.

Kann die Suche nach der Umstellung noch crawlen?

Ja, wenn die Standardzone Windows-Authentifizierung mit Negotiate anbietet, die Startadressen den Hostnamen der Standardzone verwenden und der SPN dafür am Pool-Konto hängt. Ein voller Crawl nach der Umstellung zeigt dir im Crawlprotokoll, ob es klappt.

Warum öffnet Word Dokumente aus SharePoint weiterhin per NTLM?

Meist liegt die Adresse nicht in der Intranetzone, das Dokument wurde über einen Link mit Servernamen oder IP geöffnet, oder es gibt gespeicherte Anmeldeinformationen für den Namen. Prüfe das Ereignis 4020 mit ProcessName WINWORD.EXE und dem TargetService.

Was passiert mit SharePoint-Add-ins, wenn NTLM wegfällt?

Microsoft dokumentiert, dass die App-Authentifizierung in einer Webanwendung im Windows-Claims-Modus nicht funktioniert, wenn ausschließlich Kerberos ohne NTLM-Rückfall konfiguriert ist. Inventarisiere deine Add-ins deshalb früh und kläre den Weg mit dem jeweiligen Hersteller.

Funktioniert Kerberos auch mit Aliasnamen (CNAME)?

Es kann, aber das Verhalten unterscheidet sich je nach Client. Manche bilden den SPN aus dem Alias, manche aus dem kanonischen Namen. Für SharePoint-Webanwendungen sind A-Einträge der sichere Weg. Musst du den Alias behalten, prüfe mit klist, welcher SPN wirklich angefragt wird.

Fazit: Ein Häkchen, ein SPN, ein ruhiges Intranet

SharePoint ist kein schwieriger Kerberos-Kandidat. Ein gemeinsames Anwendungspool-Konto für alle Frontends, ein SPN je Hostname an genau diesem Konto, Negotiate statt NTLM in jeder Windows-Zone und eine Standardzone, über die die Suche sauber crawlen kann: Mehr braucht die Webanwendung nicht. Die eigentliche Arbeit steckt in den Rändern, also in Aliasnamen, Ports,

alten Startadressen, WebDAV-Laufwerken per IP und Add-ins, die nur NTLM können. Microsoft beschreibt die Grundlagen in Plan for Kerberos authentication in SharePoint Server; die Kerberos-Seite insgesamt vertieft Microsoft Kerberos.

Und wenn die nächste Windows-Server-Version NTLM standardmäßig abdreht, öffnet die Belegschaft am Montag das Intranet wie immer, sieht den Kantinenplan und ärgert sich über das Mittagessen. Nicht über eine Kennwortabfrage. Mehr Aufmerksamkeit hat ein Intranet nie verdient.

WEITERLESEN · Weiter in dieser Serie

› NTLM in IIS und Webanwendungen: Negotiate statt NTLM
› CNAME, Aliasnamen und hosts-Datei: warum Kerberos den Namen nicht findet
› Edge, Chrome und Firefox: Browser für Kerberos im Intranet einstellen
› Mit klist prüfen, ob Kerberos wirklich greift
› SQL Server und NTLM: Windows-Anmeldung auf Kerberos umstellen
› Exchange Server und Outlook: NTLM bei MAPI over HTTP und EWS
› Reason-ID 6: wenn der Zielname nicht auflösbar ist
› Checkliste vor dem NTLM-Stichtag: 25 Prüfpunkte