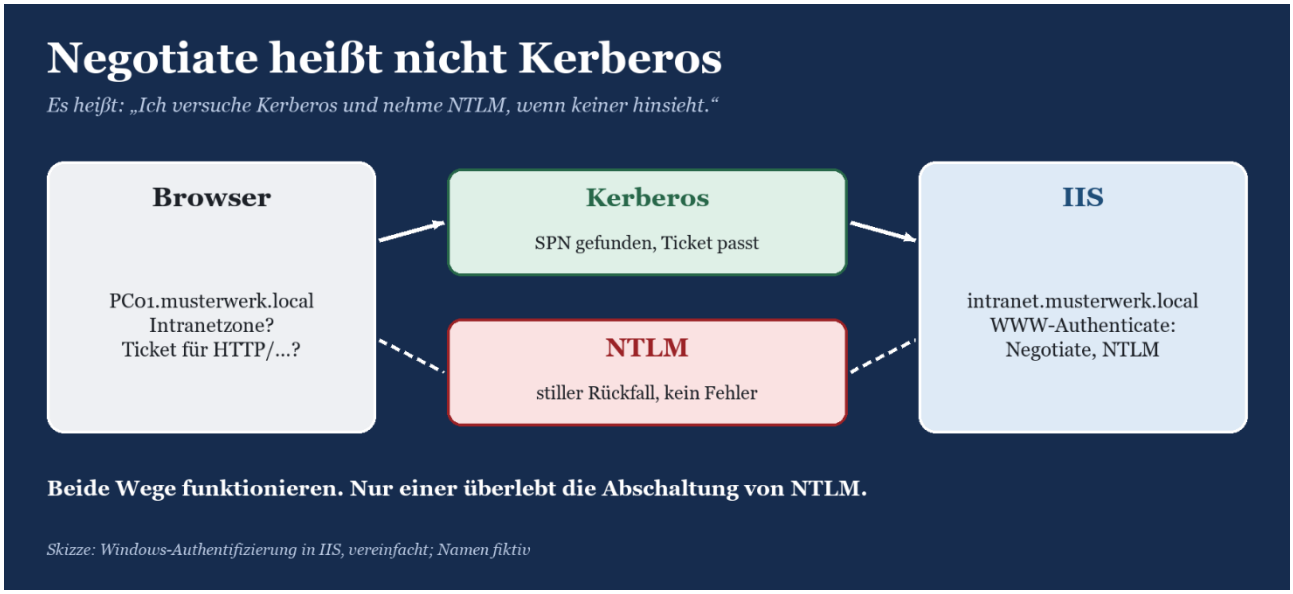
NTLM in IIS und Webanwendungen: Negotiate statt NTLM



WISSEN
Wie der NTLM Diagnostiker zeigt, welche Webserver per NTLM angesprochen werden und von welchen Clients.
› **NTLM Diagnostiker**

BERATUNG
SPNs, Anwendungspools und Load Balancer prüfen und Webanwendungen geordnet auf Kerberos bringen.
› **Beratung zur NTLM-Ablösung**

SCHULUNG
Negotiate, Kerberos und NTLM in IIS verstehen, statt bei jedem Kennwortdialog zu raten.
› **Schulung zum NTLM Diagnostiker**

Es gibt einen Satz, der in IT-Abteilungen mehr Schaden angerichtet hat als jede Kaffeepfütze im Serverraum: „Die Windows-Authentifizierung ist an, also läuft das mit Kerberos." Das stimmt ungefähr so oft, wie der Drucker beim ersten Versuch druckt. In IIS steht unter „Windows-Authentifizierung" standardmäßig die Anbieterliste Negotiate und NTLM. Negotiate versucht Kerberos und fällt still auf NTLM zurück, wenn irgendetwas nicht passt. Und irgendetwas passt fast immer nicht: ein fehlender SPN, ein Dienstkonto am Anwendungspool, ein Load Balancer mit virtuellem Namen oder ein Browser, der die Seite für Internet hält.

Solange NTLM erlaubt ist, merkt das niemand. Das Intranet öffnet sich, das Ticketsystem begrüßt dich mit Namen, das Reporting lädt. Der Unterschied zwischen iis ntlm kerberos ist für die Anwender unsichtbar. Er wird erst sichtbar, wenn NTLM wegfällt, und dann gleich für alle auf einmal. Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Den gesamten Zeitplan findest du in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet.

Dieser Beitrag nimmt sich die Webseite vor: Anbieterreihenfolge, Kernelmodus und Anwendungspool-Identität, HTTP-SPNs, Load Balancer und die Browser-Einstellungen. Am Ende weißt du, warum deine Webanwendung NTLM spricht, wie du es mit Bordmitteln nachweist und wie du sie auf Kerberos bringst, ohne dass am Montagmorgen die Hotline explodiert.

FAKTEN · IIS und NTLM auf einen Blick

Die Windows-Authentifizierung in IIS kennt die Anbieter Negotiate und NTLM. Standard ist die Reihenfolge Negotiate vor NTLM. Negotiate wählt Kerberos, wenn ein Ticket zu bekommen ist, sonst NTLM.

Die Kernelmodus-Authentifizierung (useKernelMode) ist standardmäßig aktiv. Dann prüft IIS Kerberos-Tickets mit dem Schlüssel des Computerkontos, solange useAppPoolCredentials nicht auf true steht.

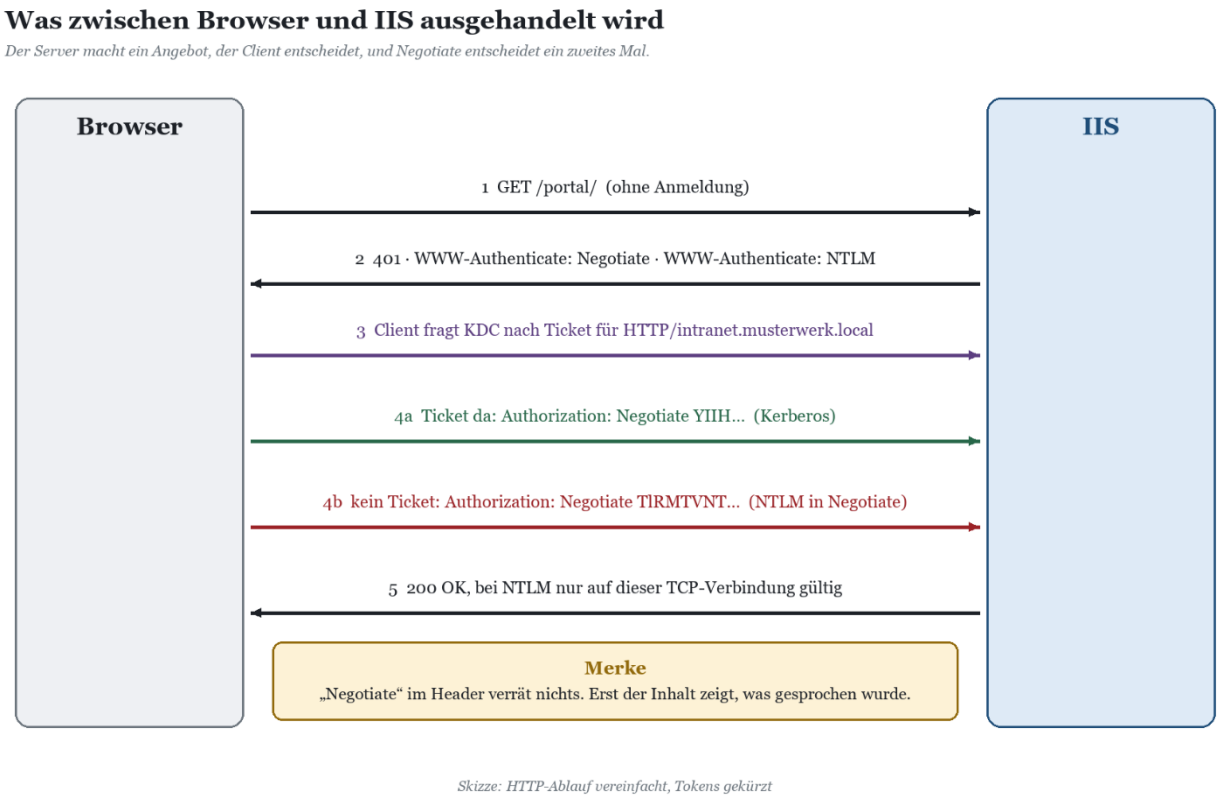
Der Browser fragt ein Ticket für HTTP/<Hostname> an. Dieser SPN muss genau einmal in der Gesamtstruktur existieren, und zwar an dem Konto, das das Ticket entschlüsselt.

Automatische Anmeldung gibt es in Edge und Chrome unter Windows standardmäßig nur für Seiten der lokalen Intranetzone.

Eingehende NTLM-Anmeldungen am Webserver protokollieren die Ereignisse 4022 und 4023 (erweitertes Auditing) beziehungsweise die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004.

Windows-Authentifizierung in IIS: Anbieter, Reihenfolge, Rückfall

Wenn du in IIS-Manager eine Website auswählst, auf „Authentifizierung“ gehst, die Windows-Authentifizierung markierst und rechts „Anbieter“ anklickst, siehst du eine kurze Liste. Im Auslieferungszustand stehen dort Negotiate und NTLM, in genau dieser Reihenfolge. IIS schickt beide als WWW-Authenticate-Kopfzeilen an den Client. Was der Client daraus macht, hängt vom Client ab: Browser bevorzugen Negotiate, manche Fachanwendungen, Java-Bibliotheken und alte .NET-Programme nehmen das, was sie zuerst verstehen.



Skizze: HTTP-Ablauf vereinfacht, Tokens gekürzt

Die drei Konfigurationen, die du in der Praxis siehst

Anbieterliste	Was passiert	Bewertung
Negotiate, NTLM	Kerberos, wenn möglich; sonst NTLM in Negotiate oder direkt NTLM	Standard, gut für die Übergangszeit
NTLM, Negotiate	Clients, die das erste Angebot nehmen, sprechen	Altlast, umdrehen

	NTLM, obwohl Kerberos ginge	
nur NTLM	immer NTLM, Kerberos ist ausgeschlossen	dringend ändern, fällt bei Phase 3 aus
Negotiate:Kerberos	nur Kerberos, kein Rückfall auf NTLM	Zielbild, vorher gründlich testen
nur Negotiate	Kerberos oder NTLM innerhalb von Negotiate	wie Standard, nur ohne direktes NTLM

Der Anbieter „Negotiate:Kerberos“ ist das Werkzeug für die Ehrlichkeitsprobe. Damit lehnt IIS jeden NTLM-Versuch ab. Auf einer Testinstanz zeigt dir das in Minuten, ob deine Kerberos-Konfiguration wirklich trägt oder nur geduldet wird. In Produktion schaltest du ihn erst, wenn das Auditing über Wochen keine NTLM-Anmeldungen mehr zeigt.

Die Konfiguration mit Bordmitteln auslesen

Bei zwei Websites klickst du dich durch. Bei zwanzig Websites auf fünf Servern nimmst du PowerShell. Das Modul WebAdministration bringt alles mit, was du brauchst:

```
# Auf WEB01.musterwerk.local: Anbieter und Kernelmodus je Website
Import-Module WebAdministration
$f = 'system.webServer/security/authentication/windowsAuthentication'
Get-Website | ForEach-Object {
  $s = $_.Name
  [pscustomobject]@{
    Site      = $s
    Enabled   = (Get-WebConfigurationProperty -PSPath 'IIS:\' -Location $s -Filter $f -Name
enabled).Value
    Kernel    = (Get-WebConfigurationProperty -PSPath 'IIS:\' -Location $s -Filter $f -Name
useKernelMode).Value
    AppPoolCr = (Get-WebConfigurationProperty -PSPath 'IIS:\' -Location $s -Filter $f -Name
useAppPoolCredentials).Value
    Providers = ((Get-WebConfigurationProperty -PSPath 'IIS:\' -Location $s -Filter
"$f/providers" -Name Collection).value -join ', ')
  }
} | Format-Table -AutoSize
```

Die Reihenfolge korrigierst du am saubersten mit appcmd, weil das auch auf Server-Core-Installationen und in Skripten funktioniert. Der Trick: NTLM entfernen und wieder anhängen, dann steht es hinten.

```
%windir%\system32\inetsrv\appcmd.exe set config "Intranet" ^
  -section:system.webServer/security/authentication/windowsAuthentication ^
  /-providers.[value='NTLM'] /commit:apphost
%windir%\system32\inetsrv\appcmd.exe set config "Intranet" ^
  -section:system.webServer/security/authentication/windowsAuthentication ^
  /+providers.[value='NTLM'] /commit:apphost
```

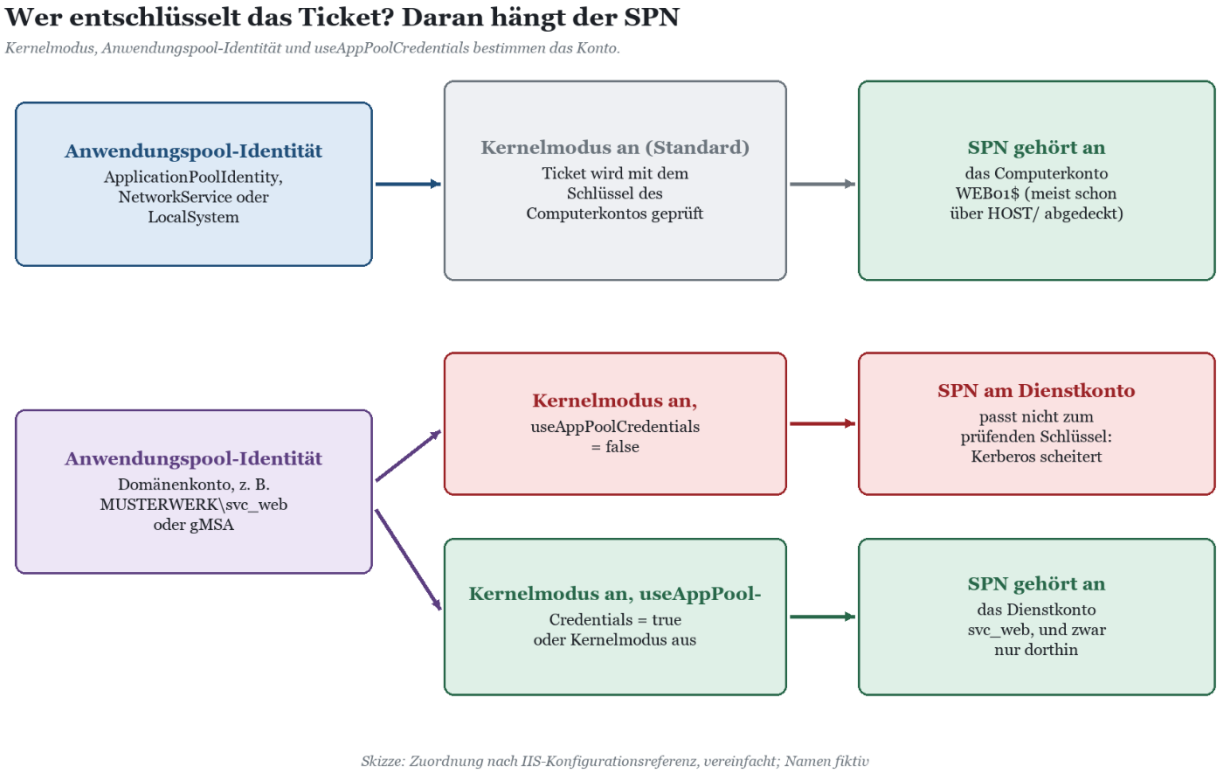
WARNUNG · Die web.config hat auch eine Meinung

Die Anbieterliste lässt sich auf Server-, Website- und Anwendungsebene setzen, und manche Hersteller liefern ihre eigene web.config mit. Prüfe deshalb die effektive Konfiguration an der Anwendung, nicht nur die der Website. Und merke dir, wer beim nächsten Update des Herstellers die Datei überschreibt.

Kernelmodus, Anwendungspool-Identität und HTTP-SPNs

Jetzt kommt der Teil, an dem die meisten Kerberos-Versuche sterben, und zwar leise. Ein Kerberos-Ticket ist mit dem Schlüssel des Kontos verschlüsselt, an dem der angefragte SPN hängt.

Der Webserver muss es mit genau diesem Schlüssel öffnen können. Welcher Schlüssel das ist, entscheiden zwei Schalter und die Identität des Anwendungspools.



Skizze: Zuordnung nach IIS-Konfigurationsreferenz, vereinfacht; Namen fiktiv

Kernelmodus und useAppPoolCredentials

Mit aktivem Kernelmodus, dem Standard seit IIS 7, erledigt der HTTP-Treiber http.sys die Anmeldung. Er prüft Tickets mit dem Schlüssel des Computerkontos, also WEB01$. Läuft der Anwendungspool als ApplicationPoolIdentity oder NetworkService, ist das genau richtig: Der Browser fragt nach HTTP/web01.musterwerk.local, und dieser Name ist über den HOST-SPN des Computerkontos bereits abgedeckt. Kerberos funktioniert ohne zusätzlichen SPN.

Anders bei einem Domänenkonto als Pool-Identität und einem eigenen Namen wie intranet.musterwerk.local. Dann registriert jemand pflichtbewusst HTTP/intranet.musterwerk.local am Dienstkonto svc_web, der Browser bekommt ein Ticket für svc_web, und http.sys versucht es mit dem Schlüssel von WEB01$ zu öffnen. Das klappt nicht. Negotiate zuckt mit den Schultern und nimmt NTLM. Die Lösung ist das Attribut useAppPoolCredentials. Steht es auf true, prüft auch der Kernelmodus mit dem Schlüssel der Pool-Identität. Microsoft rät ausdrücklich, den Kernelmodus bei Kerberos mit eigener Pool-Identität nicht abzuschalten; useAppPoolCredentials ist der elegantere Weg.

```
%windir%\system32\inetsrv\appcmd.exe set config "Intranet" ^
  -section:system.webServer/security/authentication/windowsAuthentication ^
  /useKernelMode:true /useAppPoolCredentials:true /commit:apphost
```

HTTP-SPNs prüfen und richtig setzen

Für Webanwendungen gilt eine einfache Regel: Der SPN heißt HTTP/ plus der Name, den der Anwender in die Adresszeile tippt. Auch bei HTTPS heißt er HTTP/, nicht HTTPS/. Ein HTTPS-SPN ist ein Klassiker unter den gut gemeinten Fehlern. Registriere sowohl den voll qualifizierten Namen als auch den Kurznamen, falls Anwender ihn benutzen, und prüfe vorher, ob es den SPN schon gibt.

```
# Wer hat den SPN schon?
```

```
setspn -Q HTTP/intranet.musterwerk.local
setspn -Q HTTP/intranet

# Am Konto der Pool-Identität registrieren (-S prüft auf Doppelte)
setspn -S HTTP/intranet.musterwerk.local MUSTERWERK\svc_web
setspn -S HTTP/intranet MUSTERWERK\svc_web

# Doppelte SPNs in der Gesamtstruktur suchen
setspn -X -F

# Auf dem Client: Hat der Browser ein Ticket bekommen?
klist get HTTP/intranet.musterwerk.local
```

Pool-Identität	Kernelmodus / useAppPoolCredentials	SPN gehört an
ApplicationPoolIdentity, NetworkService	an / false (Standard)	Computerkonto; für den Servernamen meist schon da, für Aliasse ergänzen
Domänenkonto oder gMSA	an / true	Dienstkonto, nicht ans Computerkonto
Domänenkonto oder gMSA	aus / egal	Dienstkonto (funktioniert, aber nicht empfohlen)
Domänenkonto oder gMSA	an / false	Konflikt: SPN am Dienstkonto, Prüfung mit Computerkonto

TIPP · Alias nur als A-Eintrag

Zeigt intranet.musterwerk.local als CNAME auf web01.musterwerk.local, bilden Windows-Browser den SPN je nach Einstellung aus dem kanonischen Namen. Dann fragt der Client nach HTTP/web01… statt nach HTTP/intranet…, und dein sorgfältig gesetzter SPN läuft ins Leere. Ein A-Eintrag für den Alias vermeidet die Diskussion. Ähnlich heimtückisch sind nicht standardmäßige Ports: Browser hängen den Port standardmäßig nicht an den SPN an.

Fehlende und doppelte SPNs sind die häufigsten Ursachen, die du im Auditing als Reason-ID wiederfindest. Was hinter den einzelnen Werten steckt, erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Für die zwei Dauerbrenner gibt es eigene Beiträge: Reason-ID 6: wenn der Zielname nicht auflösbar ist und Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten. Wer gerade Pool-Identitäten aufräumt und sie auf gMSA umstellen will, findet das Vorgehen in Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen. Den Kerberos-Hintergrund mit Tickets, Schlüsseln und Delegierung behandelt Microsoft Kerberos.

AUS DER PRAXIS · Sparfuchs & Partner: das Portal, das immer funktioniert hat

Bei der fiktiven Sparfuchs & Partner Steuerberatungs GmbH lief das Mandantenportal seit Jahren unter portal.sparfuchs.local, Pool-Identität SPARFUCHS\svc_portal, SPN sauber am Dienstkonto. Alles richtig, dachte man. Im NTLM-Audit stand der Webserver trotzdem mit jedem einzelnen Arbeitsplatz. Die Ursache: Kernelmodus an, useAppPoolCredentials aus. Der Browser bekam brav ein Ticket für svc_portal, http.sys wollte es mit dem Schlüssel des Computerkontos öffnen, Negotiate fiel auf NTLM zurück. Ein Attribut später sprach das Portal Kerberos. Gemerkt hatte es in sieben Jahren niemand, weil es eben immer funktioniert hat.

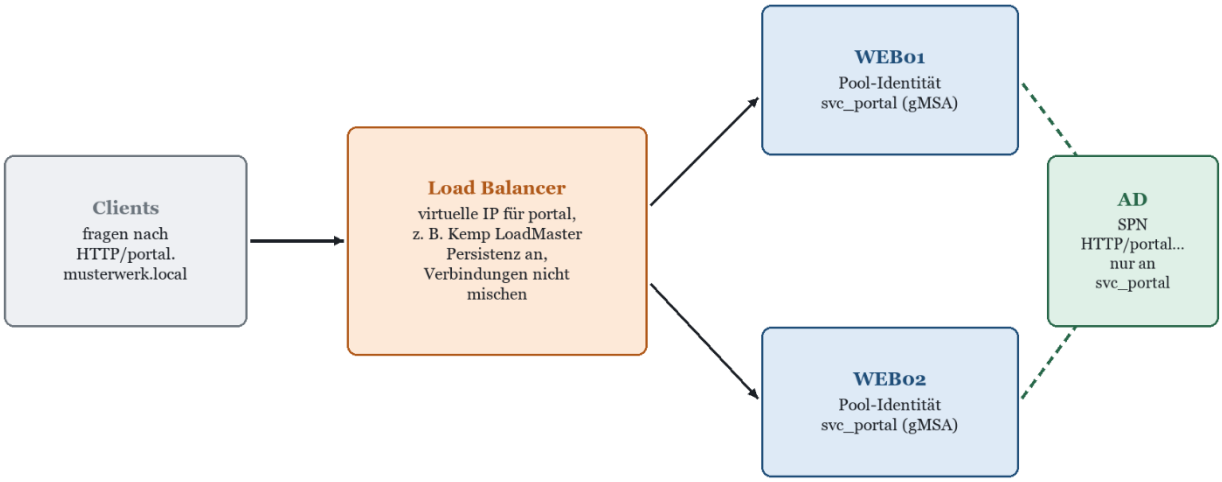
Load Balancer und Browser: die zwei Stellen außerhalb von IIS

Wenn IIS sauber konfiguriert ist und trotzdem NTLM gesprochen wird, liegt die Ursache meistens vor dem Webserver. Entweder steht ein Load Balancer dazwischen, der den Namen ändert und Verbindungen umsortiert, oder der Browser entscheidet sich gegen die automatische Anmeldung.

Load Balancer: virtueller Name, gemeinsames Konto

Load Balancer davor: ein Name, mehrere Server, ein Konto

Der Client bittet um ein Ticket für den virtuellen Namen, nicht für WEB01 oder WEB02.



SPN am Computerkonto WEB01$ für den virtuellen Namen: Kerberos klappt nur, wenn der Zufall auf WEB01 fällt.

Mit gemeinsamem Konto und useAppPoolCredentials passt jedes Ticket auf jeden Knoten.

Skizze: Beispiel Musterwerk GmbH, Namen fiktiv

Hinter einem Load Balancer tippt der Anwender portal.musterwerk.local, der Load Balancer verteilt auf WEB01 und WEB02. Der Client fragt das KDC nach einem Ticket für HTTP/portal.musterwerk.local, und dieses Ticket muss auf jedem Knoten passen. Das geht nur, wenn alle Knoten den Anwendungspool mit demselben Domänenkonto betreiben, am besten einem gMSA, der SPN genau an diesem Konto hängt und useAppPoolCredentials auf true steht. Wer den SPN stattdessen ans Computerkonto von WEB01 hängt, baut ein Glücksspiel: Kerberos klappt nur auf einem Knoten, auf dem anderen fällt Negotiate auf NTLM zurück.

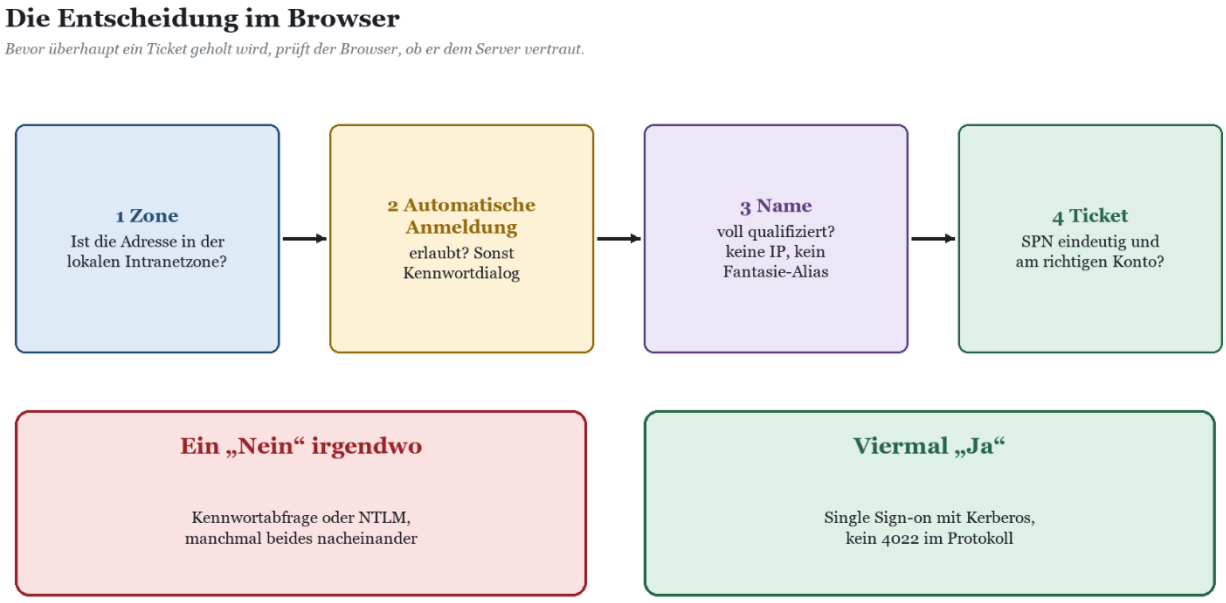
Der zweite Punkt betrifft NTLM selbst. NTLM authentifiziert eine TCP-Verbindung, nicht eine Anfrage. Fasst ein Load Balancer im Layer-7-Betrieb Verbindungen mehrerer Clients zu einer Backend-Verbindung zusammen, bekommst du im besten Fall ständige Kennwortabfragen und im schlechtesten Fall eine Sitzung mit der falschen Identität. Kerberos ist hier gutmütiger, weil das Ticket in jeder Anfrage mitkommen kann. Bei einem Kemp LoadMaster etwa entscheidet die Konfiguration des virtuellen Dienstes, ob Verbindungen wiederverwendet werden und ob TLS am Load Balancer endet. Für die NTLM-Ablösung heißt das: Persistenz an, keine Verbindungsbündelung für Seiten mit Windows-Authentifizierung und einen Blick auf den erweiterten Schutz.

WICHTIG · Erweiterter Schutz und TLS-Auslagerung

Endet TLS am Load Balancer, sieht IIS ein anderes Zertifikat als der Client. Erweiterter Schutz mit Kanalbindung (extendedProtection mit tokenChecking „Require“) schlägt dann fehl. Für die Webseite heißt das entweder TLS bis zum Webserver durchreichen oder auf Kerberos setzen und den erweiterten Schutz passend planen. Die Hintergründe zu Kanalbindung und Relay stehen in NTLM-

Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

Browser-Einstellungen: die Intranetzone entscheidet



Skizze: Edge und Chrome unter Windows; Firefox verwaltet die Liste getrennt

Edge und Chrome greifen unter Windows auf die Zoneneinstellungen der Internetoptionen zurück. Automatisch angemeldet wird standardmäßig nur in der lokalen Intranetzone. Adressen ohne Punkt landen dort meist automatisch, voll qualifizierte Namen wie intranet.musterwerk.local häufig nicht. Dann behandelt der Browser deine Seite wie ein Angebot aus dem Internet und zeigt einen Kennwortdialog. Anwender tippen brav Name und Kennwort ein, und je nach Ablauf landet das Ganze als NTLM beim Server. Herzlichen Glückwunsch: Du hast Single Sign-on durch Single Sign-in ersetzt.

Die saubere Lösung ist eine Gruppenrichtlinie. Unter Computerkonfiguration, Administrative Vorlagen, Windows-Komponenten, Internet Explorer, Internetsystemsteuerung, Sicherheitsseite liegt die „Liste der Site zu Zonenzuweisungen“. Trage dort *.musterwerk.local mit dem Wert 1 für die Intranetzone ein. Für Edge gibt es zusätzlich die Richtlinie AuthServerAllowlist, mit der du die Server für integrierte Authentifizierung ausdrücklich festlegst. Firefox pflegt seine eigene Liste in network.negotiate-auth.trusted-uris und lässt sich ebenfalls zentral über Richtlinien steuern.

Symptom im Browser	Wahrscheinliche Ursache	Prüfung
Kennwortdialog im Intranet	Seite nicht in der Intranetzone	Zone in den Internetoptionen, GPO-Zonenliste
kein Dialog, aber NTLM im Audit	kein oder falscher SPN, useAppPoolCredentials	klist get HTTP/..., setspn -Q
Kerberos auf WEB01, NTLM auf WEB02	SPN am Computerkonto statt am gemeinsamen Konto	setspn -Q, Pool-Identität beider Knoten
Aufruf per IP-Adresse	für IP-Adressen gibt es standardmäßig kein Ticket	DNS-Namen verwenden
sporadische Kennwortabfragen	Load Balancer bündelt Verbindungen	Konfiguration des virtuellen Dienstes
nur NTLM, egal was du	Anbieterliste nur NTLM oder NTLM	Anbieter in IIS, web.config

tust	zuerst	

Der Aufruf per IP-Adresse verdient eine Extrazeile, weil er nicht nur bei Dateifreigaben vorkommt. Lesezeichen auf die nackte IP-Adresse 10.20.1.30 sind in Fachabteilungen erstaunlich langlebig. Wie du solche Adressen findest und umstellst, beschreibt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen.

Nachweisen, welche Webserver NTLM sprechen

Konfiguration lesen ist gut, Nachweis ist besser. Auf dem Webserver selbst melden die erweiterten NTLM-Ereignisse 4022 und 4023, wer sich eingehend per NTLM angemeldet hat. Sie gibt es ab Windows Server 2025 sowie auf Server 2022 und 2019 mit den Updates ab dem 13.10.2026; auf älteren Systemen bleiben die klassischen Restrict-NTLM-Ereignisse 8001 bis 8004 im Überwachungsmodus. Auf der Client-Seite zeigen 4020 und 4021 die ausgehende Sicht, einschließlich „Target Machine“ und „Reason ID“. Wie du das Auditing einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; die passenden Richtlinien legt das NTLM-Audit-GPO-Skript in einem Durchgang an.

```
# Auf WEB01: eingehende NTLM-Anmeldungen der letzten 24 Stunden
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -FilterXPath `
  "*[System[(EventID=4022 or EventID=4023) and TimeCreated[timediff(@SystemTime) <=
86400000]]]" |
  Select-Object TimeCreated, Id, @{n='Text';e={($_.Message -split "`n")[0..12] -join ' '}} |
  Format-List

# Export für die Auswertung an anderer Stelle
wevtutil epl Microsoft-Windows-NTLM/Operational C:\Temp\web01-ntlm.evtx
```

Die Einzelheiten zu den Feldern und ihrer Deutung findest du in Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern und Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen. Bei Webanwendungen ohne TLS lohnt zusätzlich ein Mitschnitt: Beginnt der Authorization-Header nach „Negotiate“ mit TlRMTVNT, ist es NTLM im Negotiate-Gewand. Mehr dazu in NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen.

Wo es mit Bordmitteln mühsam wird

Für einen Webserver reicht das. Bei der Musterwerk GmbH sind es aber elf IIS-Server, drei davon hinter einem Load Balancer, dazu ein Dokumentenmanagement, ein Zeiterfassungsterminal mit Weboberfläche und zwei SharePoint-Altlasten. Jeder Webserver schreibt pro Arbeitstag Tausende Ereignisse, weil NTLM pro Verbindung neu authentifiziert. Willst du wissen, welche Clients mit welchem Webserver NTLM sprechen und warum, sammelst du Ereignisse von allen Servern, legst Client- und Serversicht nebeneinander, ordnest IP-Adressen Rechnern zu, prüfst für jeden Zielnamen SPN und DNS und entfernst am Ende die Dubletten. Das ist kein Nachmittag mehr, das ist ein Projekt mit eigenem Excel-Dialekt.

Genau diese Fleißarbeit übernimmt der NTLM Diagnostiker. Er zeigt in der Kommunikationsmatrix, welche Webserver per NTLM angesprochen werden und von welchen Clients, und liefert die Ursache gleich mit, statt dich mit der Reason-ID allein zu lassen.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Webserver mit NTLM finden, Ursache gleich dazu

Ereignisse holt der NTLM Diagnostiker direkt vom DC, über einen vorhandenen Windows Event Collector oder per Direktabfrage von den Webservern. Er arbeitet dabei ausschließlich lesend: keine Änderung an IIS, an SPNs, an Gruppenrichtlinien oder an Konten.

Die Kommunikationsmatrix zeigt jede Kombination aus Client und Webserver mit NTLM, die

Konten-Sicht ergänzt, welche Benutzer- und Dienstkonten beteiligt sind. So siehst du auf einen Blick, ob ein Webserver mit der ganzen Belegschaft NTLM spricht (Konfigurationsproblem am Server) oder nur mit einzelnen Clients (Browser, Zone, Lesezeichen).

Die Ursachen-Engine mit SPN- und DNS-Prüfung erkennt fehlende und doppelte HTTP-SPNs und Zielnamen, die nicht sauber auflösen, etwa CNAME-Aliasse oder Aufrufe per IP-Adresse.

Die Abschalt-Simulation zeigt dir vorab, welche Webanwendungen und Clients betroffen wären, wenn NTLM am Server verweigert würde. Die NTLMv1-Hitliste, die Sicherheitsflaggen, die Readiness-Ampel sowie Abdeckungsmonitor und OS-Landkarte ordnen das Ergebnis ein; Word-Bericht und Excel/CSV-Export gehen an Webentwicklung, Hersteller und IT-Leitung.

Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund, der volle Umfang lässt sich sieben Tage testen. Lizenziert wird pro aktivem Computerkonto. Ein Kerberos-Gegencheck ist für eine spätere Ausbaustufe geplant.

Bei der Trendforge Digital GmbH ergab der erste Lauf ein klares Bild: Vier Webserver sprachen mit nahezu allen Clients NTLM, zwei weitere nur mit einer Handvoll Rechner. Bei den vier lagen fehlende SPNs und einmal useAppPoolCredentials zugrunde, bei den zwei anderen Lesezeichen mit IP-Adresse in einer einzigen Abteilung. Wo eine Anwendung NTLM fest eingebaut hat, hilft das Gespräch mit dem Hersteller, vorbereitet nach Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen. Was bis zur Abschaltung nicht fertig wird, gehört in eine gepflegte Ausnahme statt in ein dauerhaftes Loch; dazu passt Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

Wenn du die Webanwendungen nicht alle selbst auseinandernehmen möchtest, unterstützt dich die Beratung zur NTLM-Ablösung bei der Prüfung von SPNs, Pool-Identitäten und Load-Balancer-Konfiguration. Für das Team, das künftig selbst Ursachen lesen will, gibt es die Schulung zum NTLM Diagnostiker.

FAQ: IIS, NTLM und Kerberos

Ist Negotiate dasselbe wie Kerberos?

Nein. Negotiate ist ein Verhandlungsverfahren, das Kerberos bevorzugt und auf NTLM zurückfällt. Ob Kerberos tatsächlich verwendet wurde, siehst du mit klist auf dem Client oder an den NTLM-Ereignissen auf dem Server.

Soll ich NTLM aus der Anbieterliste einfach löschen?

Nicht sofort. Zuerst Auditing einschalten und nachweisen, dass Kerberos für alle Clients klappt. Danach kannst du NTLM entfernen oder auf Negotiate:Kerberos umstellen. Vorher löschen ist der schnellste Weg zu einem vollen Ticketsystem. Das Vorgehen beschreibt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

Brauche ich bei ApplicationPoolIdentity einen eigenen SPN?

Für den Servernamen meist nicht, weil das Computerkonto mit seinem HOST-SPN schon abgedeckt ist. Für einen eigenen Alias wie intranet.musterwerk.local brauchst du HTTP/intranet.musterwerk.local am Computerkonto des Webservers.

Was macht useAppPoolCredentials genau?

Es sorgt dafür, dass die Kernelmodus-Authentifizierung Kerberos-Tickets mit dem Schlüssel der Anwendungspool-Identität prüft statt mit dem des Computerkontos. Das brauchst du, sobald ein Domänenkonto oder gMSA den Pool betreibt und der SPN an diesem Konto hängt.

Heißt der SPN bei HTTPS-Seiten HTTPS/?

Nein. Auch für HTTPS lautet der Dienstteil HTTP/. Ein SPN mit HTTPS/ wird von Browsern nicht angefragt und bewirkt nichts außer Verwirrung.

Warum klappt Kerberos auf dem Server selbst, aber nicht vom Client?

Wer die Seite direkt auf dem Webserver aufruft, testet einen Sonderfall mit lokaler Anmeldung. Teste immer von einem normalen Arbeitsplatz aus, mit dem Namen, den die Anwender verwenden.

Was ändert sich bei einem Load Balancer?

Der SPN gehört zum virtuellen Namen und an ein gemeinsames Konto aller Knoten, idealerweise ein gMSA, mit useAppPoolCredentials auf true. Außerdem darf der Load Balancer bei Windows-Authentifizierung keine Verbindungen mehrerer Clients bündeln.

Ändert der NTLM Diagnostiker etwas an meinen Webservern?

Nein. Er arbeitet ausschließlich lesend, wertet Ereignisse aus und prüft SPNs und DNS. Die Änderungen an IIS, SPNs und Browser-Richtlinien nimmst du selbst vor, mit den Befunden als Grundlage.

Fazit: Kerberos ist kein Zufall, sondern Konfiguration

Webanwendungen mit Windows-Authentifizierung sind die stillsten NTLM-Quellen im Netz. Sie funktionieren, sie beschweren sich nicht, und genau deshalb fallen sie erst auf, wenn NTLM weg ist. Die Ursachen sind dabei überschaubar: Anbieterreihenfolge, Kernelmodus mit falschem Schlüssel, fehlende oder doppelte HTTP-SPNs, Load Balancer mit virtuellem Namen und Browser, die deine Seite für Internet halten. Jede davon lässt sich mit Bordmitteln prüfen und beheben.

Mühsam wird es durch die Menge: viele Webserver, viele Clients, viele Ereignisse. Dann lohnt es sich, die Zuordnung nicht von Hand zu machen. Wenn am Ende jeder Webserver Kerberos spricht und „Negotiate:Kerberos“ in der Anbieterliste steht, ohne dass jemand anruft, hast du alles richtig gemacht. Und falls doch jemand anruft, hat er vermutlich ein Lesezeichen mit IP-Adresse.

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 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen
› NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› NTLM schrittweise abschalten, ohne dass etwas ausfällt