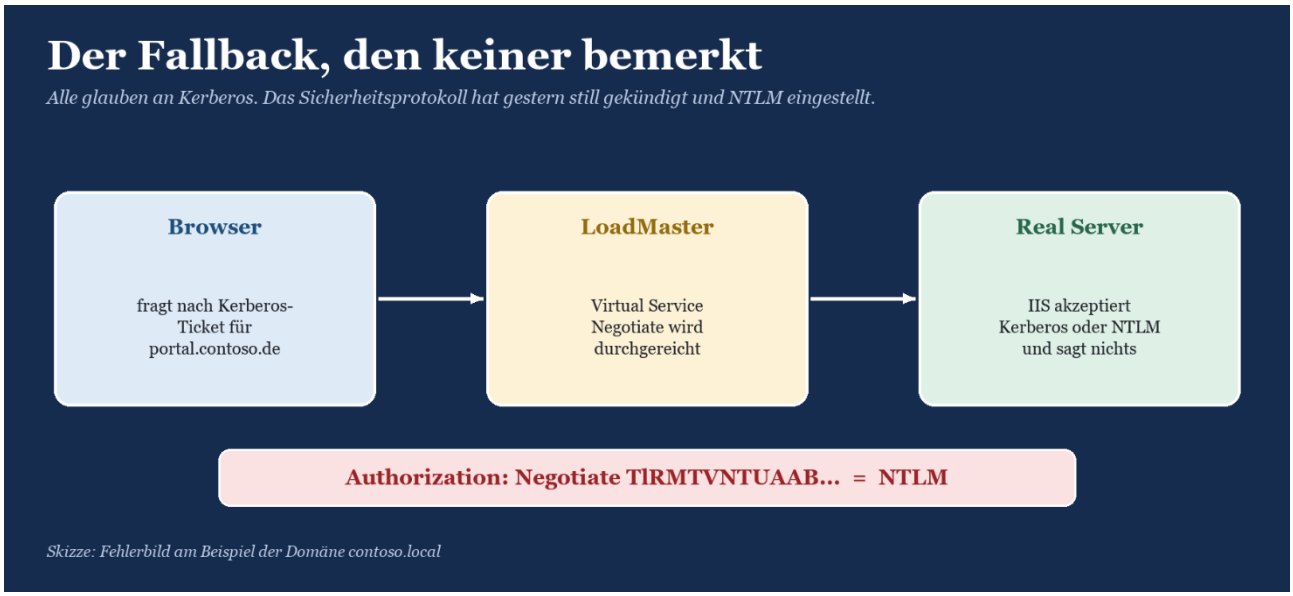
NTLM, NTLM-Proxy und der Kerberos-Fallback, den keiner bemerkt



WISSEN
Alles zum Kemp LoadMaster mit Microsoft-Brille: Exchange, SharePoint, ADFS, RDS und Kerberos an einem Ort.
› **Kemp LoadMaster**

BERATUNG
Du willst wissen, ob hinter deinem LoadMaster Kerberos oder heimlich NTLM läuft? Wir messen nach, bevor Microsoft abschaltet.
› **Beratung zum Kemp LoadMaster**

SCHULUNG
NTLM-Proxy, KCD und Negotiate im Labor aufbauen, kaputt machen und den Fallback mit eigenen Augen sehen.
› **Kemp-LoadMaster-Schulung**

Es gibt in der Windows-Welt eine Sorte Fehler, die besonders hinterhältig ist: die, die keine sind. Der Benutzer öffnet das Intranetportal, wird ohne Rückfrage angemeldet, alle sind zufrieden. Im Betriebshandbuch steht seit Jahren „Single Sign-on per Kerberos“. Nur hat Kerberos irgendwann zwischen zwei Firmware-Updates, einem neuen Pool-Konto und einer DNS-Umstellung leise gekündigt, und NTLM hat den Dienst übernommen. Ohne Übergabeprotokoll, ohne Fehlermeldung, ohne dass es jemand bemerkt hätte. Bis Microsoft NTLM abschaltet. Dann bemerken es alle, und zwar gleichzeitig.

Dieser Beitrag dreht sich um kemp ntlm in all seinen Spielarten: den NTLM-Modus und den NTLM-Proxy-Modus des Edge Security Packs, das schlichte Durchreichen von Negotiate über einen Virtual Service und die Kerberos Constrained Delegation als saubere, aber anspruchsvollere Alternative. Du erfährst, wann der NTLM-Proxy die pragmatische Wahl ist, weil er ohne SPN und ohne Delegation auskommt, welchen Preis du dafür bei Sicherheit, Zukunftsfähigkeit und Auditing zahlst und vor allem, wie du herausfindest, ob hinter deinem LoadMaster gerade still NTLM statt Kerberos läuft.

Die Übersicht über alle LoadMaster-Themen mit Microsoft-Bezug findest du auf der Seite Kemp LoadMaster. Die Kerberos-Grundlagen, von Tickets über SPNs bis zu Verschlüsselungstypen, stehen im Bereich Microsoft Kerberos.

FAKTEN · kemp ntlm in fünf Sätzen

Das Edge Security Pack kann Clients per NTLM anmelden. Im älteren Modus prüft der LoadMaster

die Anmeldedaten gegen einen LDAP-Endpunkt, im NTLM-Proxy-Modus reicht er den NTLM-Handshake an den Real Server weiter und lässt ihn dort bestätigen.

Der NTLM-Proxy-Modus kam mit LoadMaster-Firmware 7.2.48.4 (LTS) und 7.2.53. Neue Installationen haben ihn ab Werk aktiv, aktualisierte Systeme nicht.

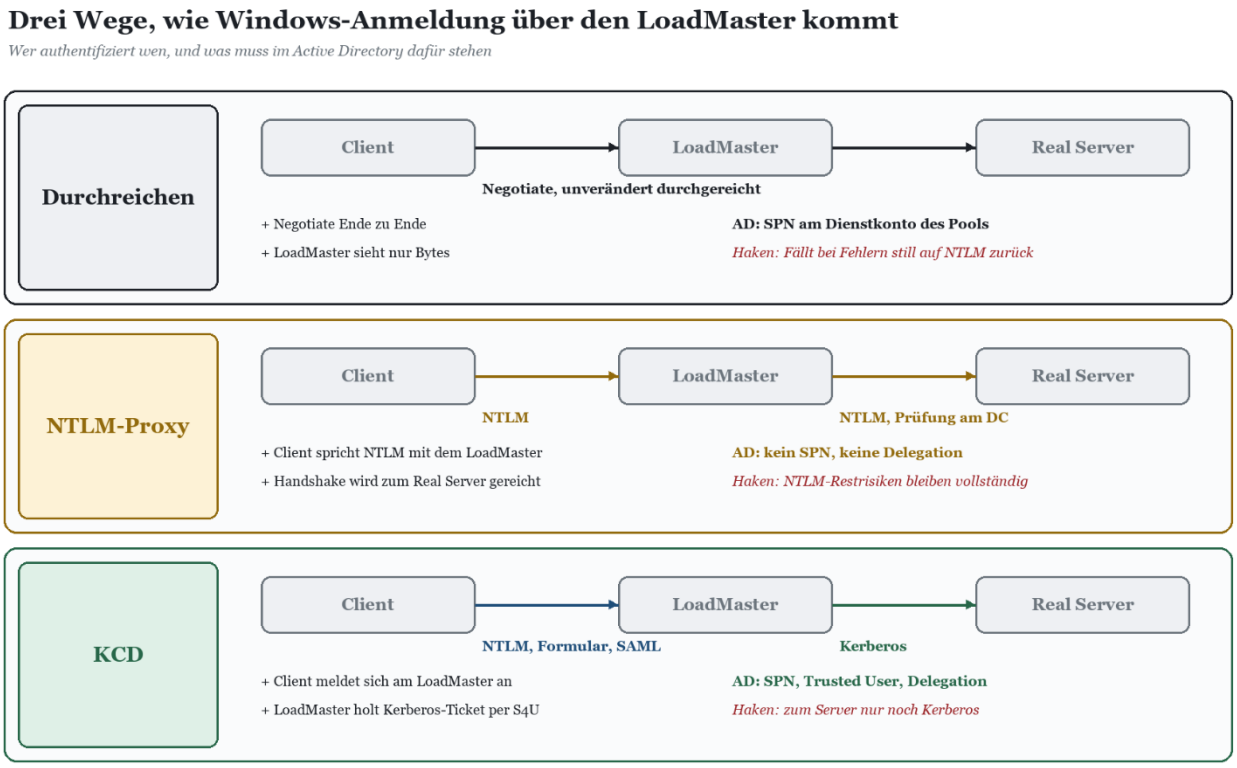
Der Schalter sitzt global unter System Configuration > Miscellaneous Options > L7 Configuration und benennt den Client-Authentifizierungsmodus in allen Virtual Services von NTLM in NTLM-Proxy um.

Microsoft hat NTLM im Juni 2024 abgekündigt, NTLMv1 ist seit Windows Server 2025 und Windows 11 24H2 entfernt, und im nächsten großen Windows-Server-Release soll Netzwerk-NTLM standardmäßig deaktiviert sein.

Negotiate fällt bei jedem Kerberos-Problem ohne Rückmeldung auf NTLM zurück. Sichtbar wird das nur in Protokollen, die kaum jemand liest.

Drei Wege durch den LoadMaster: Durchreichen, NTLM-Proxy, KCD

Bevor wir über Vor- und Nachteile streiten, lohnt sich ein genauer Blick darauf, wer bei welcher Variante eigentlich mit wem spricht. Denn die meisten Missverständnisse rund um NTLM am LoadMaster entstehen, weil drei grundverschiedene Architekturen im Gespräch alle „Windows-Anmeldung über den Kemp“ heißen.



Skizze: vereinfachte Gegenüberstellung, Beispielnamen aus contoso.local

Durchreichen: der LoadMaster als stummer Zeuge

Im einfachsten Fall ist der LoadMaster an der Anmeldung gar nicht beteiligt. Der Virtual Service terminiert vielleicht TLS, verteilt Verbindungen und prüft Health Checks, aber der Authorization-Header mit Negotiate wandert unverändert vom Browser zum Real Server. Ob dort Kerberos oder NTLM ankommt, entscheiden ausschließlich Client, Domänencontroller und IIS. Der LoadMaster ist ein stummer Zeuge, und genau deshalb bemerkt er auch nichts, wenn Kerberos ausfällt.

Damit Kerberos in dieser Variante funktioniert, muss der Client für den veröffentlichten Namen, etwa portal.contoso.de, ein Ticket bekommen. Das setzt voraus, dass genau ein Konto den SPN HTTP/portal.contoso.de trägt und alle Real Server den Schlüssel dieses Kontos kennen. Praktisch heißt das: ein gemeinsames Dienstkonto als Identität der Anwendungspools oder ein Alternate Service Account wie bei Exchange. Wie das sauber aussieht und warum ein SPN auf einem einzelnen Computerkonto in einer Farm zuverlässig schiefgeht, beschreibt SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server.

Eine Eigenheit, die beim Durchreichen gern übersehen wird: NTLM ist verbindungsgebunden. Die drei Nachrichten des Handshakes und alle folgenden Anfragen müssen über dieselbe TCP-Verbindung zum selben Real Server laufen. Kerberos ist da entspannter, NTLM nicht. Sobald der LoadMaster serverseitige Verbindungen zusammenlegt oder zwischen Anfragen auf einen anderen Server wechselt, sieht der Real Server eine Type-3-Nachricht ohne vorherige Challenge und quittiert mit 401. Das Ergebnis sind Anmeldefenster im Minutentakt, die aussehen wie ein Kennwortproblem und keines sind. Mehr zur Bindung von Clients an Server steht in Persistence und Scheduling: wer hängt an welchem Server und warum.

NTLM und NTLM-Proxy im Edge Security Pack

Sobald du am Virtual Service das Edge Security Pack aktivierst, wird der LoadMaster vom Zeugen zum Türsteher. In den ESP-Optionen wählst du den Client Authentication Mode, also wie sich der Benutzer am LoadMaster anmeldet, und getrennt davon den Server Authentication Mode, also wie der LoadMaster den Benutzer gegenüber dem Real Server vertritt. Einer der Client-Modi ist NTLM: Der Browser meldet sich ohne Formular mit seinen Windows-Anmeldedaten an, sofern er den Namen als Intranet einstuft.

Hier kommt die Unterscheidung ins Spiel, die vielen Installationen bis heute fehlt. Im älteren NTLM-Modus hat der LoadMaster die Anmeldedaten selbst gegen einen LDAP-Endpunkt aus der clientseitigen SSO-Domäne geprüft. Im NTLM-Proxy-Modus verwendet er den Real Server als Prüfinstanz: Er reicht den NTLM-Handshake an den Real Server weiter, und erst wenn dieser erfolgreich war, gilt der Benutzer als angemeldet. Der Real Server wiederum fragt per Netlogon beim Domänencontroller nach. Progress empfiehlt ausdrücklich, den Proxy-Modus aktiv zu lassen, und hat ihn als Sicherheitsverbesserung eingeführt.

Der entscheidende Punkt für diesen Beitrag: Wenn der Real Server den Benutzer ohnehin selbst per NTLM authentifiziert, braucht es auf der Serverseite weder einen SPN noch eine Delegation. Kein Trusted User, keine Keytab, keine Diskussion mit dem AD-Team über die Registerkarte Delegierung. Das ist der pragmatische Charme des NTLM-Proxys. Willst du zusätzlich Gruppenprüfungen am LoadMaster, also Permitted Groups oder Steering Groups, braucht die clientseitige SSO-Domäne trotzdem einen LDAP-Endpunkt.

WICHTIG · Nach dem Firmware-Update selbst einschalten

Wer seinen LoadMaster von einer Firmware vor 7.2.48.4 beziehungsweise 7.2.53 aktualisiert hat, läuft weiter im alten LDAP-basierten NTLM-Modus. Der Proxy-Modus wird bei Updates nicht automatisch aktiviert. Prüfe unter System Configuration > Miscellaneous Options > L7 Configuration, ob NTLM Proxy Mode gesetzt ist. Erkennbar ist das auch am Virtual Service: Steht dort als Client-Modus nur „NTLM“, ist der Schalter aus.

Vor dem Umschalten muss jeder betroffene Real Server NTLM als Teil der integrierten Windows-Authentifizierung anbieten. Ein IIS, der nur noch Negotiate:Kerberos akzeptiert, lässt den Proxy-Handshake scheitern.

KCD: der LoadMaster als Bevollmächtigter

Bei der Kerberos Constrained Delegation meldet sich der Benutzer am LoadMaster an, per Formular, per NTLM, per Zertifikat oder über SAML, und der LoadMaster besorgt sich anschließend per Protocol Transition ein Kerberos-Ticket im Namen des Benutzers für den Real Server. Zum Backend fließt ausschließlich Kerberos. Dafür brauchst du einen Trusted User mit SPN, eine Delegationsfreigabe auf die Ziel-SPNs oder eine ressourcenbasierte Delegation am Zielkonto und Verschlüsselungstypen, die zur Domäne passen. Wie das geht, steht ausführlich in Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten, und warum die Verschlüsselung dabei gern zur Stolperfalle wird, in Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne.

Interessant ist die Kombination: NTLM auf der Clientseite, KCD auf der Serverseite. Der Benutzer im internen Netz bekommt seine nahtlose Anmeldung ohne Formular, das Backend sieht trotzdem nur Kerberos. Progress empfiehlt auch hier den NTLM-Proxy-Modus, weil der LoadMaster damit zuerst einen erfolgreichen NTLM-Handshake mit dem Real Server verlangt, bevor er die KCD-Schritte ausführt. Das hat eine unbequeme Konsequenz, die man im Hinterkopf behalten sollte: Auch eine „Kerberos-only"-Kette nach hinten enthält dann vorn ein Stück NTLM.

Wann der NTLM-Proxy die pragmatische Wahl ist und was er kostet

Pragmatisch ist im Betrieb ein schönes Wort. Es bedeutet meist: funktioniert heute, rächt sich später. Beim NTLM-Proxy ist das nicht anders, aber es gibt Situationen, in denen er die vernünftigste Antwort ist.

Die guten Gründe

- **Keine Hoheit über das Active Directory.** Du betreibst den LoadMaster, aber das AD-Team gibt weder SPNs noch Delegationsrechte frei, oder der Änderungsprozess dafür dauert länger als das Projekt. Der NTLM-Proxy kommt ohne Änderungen am Verzeichnis aus.
- **Eigenentwicklungen ohne Kerberos-Verständnis.** Manche interne Anwendung läuft unter einer lokalen Identität, auf wechselnden Hosts oder in einem Container, dem niemand einen stabilen SPN zuordnen kann. NTLM ist dort oft das Einzige, was zuverlässig funktioniert.
- **Übergang und Migration.** Während du eine KCD-Konfiguration vorbereitest oder einen alten Reverse Proxy ablöst, hält der NTLM-Proxy den Betrieb aufrecht, und zwar sicherer als der LDAP-basierte Altmodus.
- **Interne Benutzer ohne Formular.** Für Clients im Firmennetz ist die NTLM-Anmeldung am ESP der einfachste Weg zu nahtlosem SSO, selbst wenn die Serverseite per KCD arbeitet.

Der Preis: Sicherheit

NTLM ist ein Challenge-Response-Verfahren aus einer Zeit, in der „Netzwerk" noch „vertrauenswürdiges LAN" hieß. Es kennt keine gegenseitige Authentifizierung: Der Client weiß nicht, ob er mit dem echten Server spricht. Genau das macht NTLM-Relay möglich, also das Weiterreichen eines Handshakes an einen anderen Dienst. Mit Pass-the-Hash genügt Angreifern der Kennwort-Hash, und abgefangene NTLMv2-Antworten lassen sich offline gegen schwache Kennwörter durchprobieren. Kerberos hat eigene Schwächen, aber diese drei gehören nicht dazu.

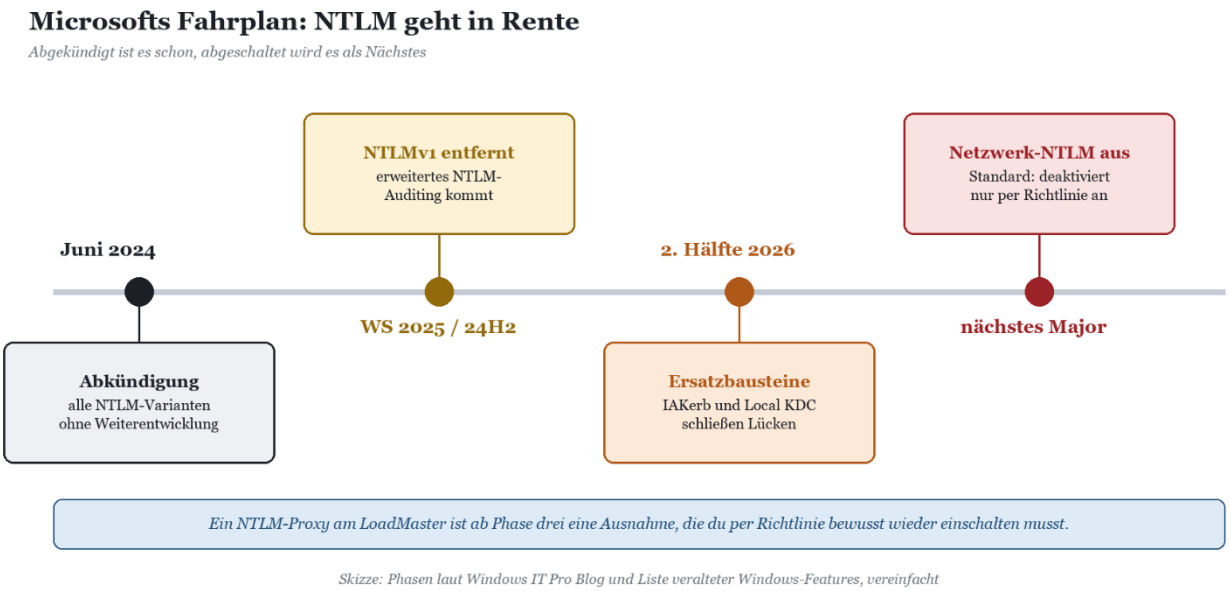
Der NTLM-Proxy ist architektonisch ein Mittelsmann, der einen NTLM-Handshake weiterreicht. Das ist erlaubt und gewollt, aber es ist eben dieselbe Mechanik, die Schutzmaßnahmen wie Extended Protection for Authentication verhindern sollen. Erzwingt ein Backend Channel Binding, muss die TLS-Kette dazu passen. Bei Exchange Server, wo Extended Protection seit Exchange 2019 CU14 standardmäßig aktiv ist, ist reines TLS-Offloading deshalb nicht unterstützt, Re-Encryption mit demselben Zertifikat schon. Mehr zu Exchange hinter dem LoadMaster liefert Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks.

WARNUNG · Protected Users und NTLM vertragen sich nicht

Konten in der Gruppe Protected Users dürfen sich nicht per NTLM anmelden. Wer seine Administratorinnen und Administratoren vorbildlich in diese Gruppe aufnimmt, sperrt sie damit hinter jedem NTLM-Proxy aus, und zwar mit einer Fehlermeldung, die nach falschem Kennwort aussieht. Dasselbe gilt für Konten, für die Richtlinien unter „Netzwerksicherheit: NTLM einschränken“ greifen.

Der Preis: Microsofts Fahrplan

Im Juni 2024 hat Microsoft alle NTLM-Varianten einschließlich NTLMv2 auf die Liste der veralteten Windows-Features gesetzt. Es gibt keine Weiterentwicklung mehr. NTLMv1 ist ab Windows Server 2025 und Windows 11 24H2 entfernt. Anfang 2026 hat Microsoft den weiteren Weg im Windows IT Pro Blog konkretisiert: zuerst erweitertes Auditing, dann in der zweiten Jahreshälfte 2026 Bausteine wie IAKerb und ein lokaler KDC für Windows Server 2025 und Windows 11 24H2, die die häufigsten Gründe für NTLM beseitigen sollen, und schließlich im nächsten großen Windows-Server-Release ein standardmäßig deaktiviertes Netzwerk-NTLM. Wer es dann noch braucht, muss es per Richtlinie ausdrücklich wieder einschalten. Ein festes Datum für diesen letzten Schritt hat Microsoft bisher nicht genannt.



Skizze: Phasen laut Windows IT Pro Blog und Liste veralteter Windows-Features, vereinfacht

Für dich bedeutet das: Ein NTLM-Proxy, den du heute einrichtest, ist eine Konfiguration mit Ablaufdatum. Er wird nicht morgen brechen, aber er wird zur dokumentierten Ausnahme, die bei jeder Härtung, jedem Audit und jedem neuen Domänencontroller begründet werden muss. IAKerb ist dabei besonders spannend: Es soll Kerberos auch dann ermöglichen, wenn der Client keinen Domänencontroller direkt erreicht, also genau in dem Fall, in dem heute externe Clients auf NTLM ausweichen.

Der Preis: Auditing

Kerberos hinterlässt eine saubere Spur: Der Domänencontroller protokolliert, wer für welchen SPN ein Ticket bekommen hat, und bei KCD sogar, welches Konto im Namen wessen delegiert hat. NTLM liefert deutlich weniger. Am Domänencontroller steht eine Kennwortprüfung mit dem Workstation-Namen, den der Client selbst angibt, am Real Server eine Anmeldung, deren Quell-IP wegen SNAT der LoadMaster ist. Wer im Sicherheitsvorfall nachvollziehen will, wer wann von wo

zugegriffen hat, muss dann Protokolle von LoadMaster, Real Server und Domänencontroller zusammenführen.

Kriterium	NTLM (Legacy-Modus)	NTLM-Proxy	KCD
Prüfung der Anmeldedaten	LoadMaster gegen LDAP	Real Server per Netlogon am DC	LoadMaster per Kerberos am KDC
Gegenseitige Authentifizierung	nein	nein	ja, zum Backend
Relay- und Hash-Risiken	voll	voll, aber ohne LDAP-Umweg	zum Backend nicht
Protected Users	scheitert	scheitert	nur mit passender Clientanmeldung
Spur am DC	LDAP-Bind	Ereignis 4776	Ereignisse 4768 und 4769 mit Delegation
Zukunft bei Microsoft	abgekündigt	abgekündigt	strategischer Weg

Entscheidungstabelle: KCD, NTLM-Proxy oder Durchreichen

Die folgende Tabelle ist kein Ersatz für ein Architekturgespräch, aber sie verhindert die häufigsten Fehlentscheidungen. Lies sie spaltenweise: Wo deine Rahmenbedingungen in einer Spalte mehrfach auf „nein“ stoßen, ist diese Variante nicht dein Freund.

Frage	Durchreichen	NTLM-Proxy	KCD
SPN im AD nötig?	ja, für den veröffentlichten Namen	nein	ja, für Trusted User und Ziele
Delegation nötig?	nein	nein	ja, klassisch oder RBCD
Vorauthentifizierung am LoadMaster?	nein	ja	ja
Externe Clients ohne DC-Sicht?	nur NTLM	ja, per NTLM	ja, Formular, SAML, MFA
MFA vorschaltbar?	nein	nicht sinnvoll	ja
Zum Backend garantiert Kerberos?	nein, stiller Fallback	nein	ja
Verhalten bei NTLM-Abschaltung	intern ok, wenn Kerberos sauber	bricht	Backend ok, Clientseite prüfen
Aufwand Ersteinrichtung	gering	gering	mittel bis hoch
Typischer Einsatz	interne Farmen mit sauberem SPN	Übergang, Eigenentwicklungen, kein AD-Zugriff	Exchange, SharePoint, Portale mit Außenzugriff

TIPP · Faustregel für den Mittelstand

Intern mit sauberem SPN: durchreichen und Kerberos messen. Extern mit Vorauthentifizierung: KCD, gern kombiniert mit Formular oder SAML am ESP. NTLM-Proxy nur als befristete, dokumentierte Ausnahme mit Enddatum im Ticket, nicht als Dauerlösung.

Die Grundlagen der Vorauthentifizierung und der SSO-Domänen erklärt Edge Security Pack:

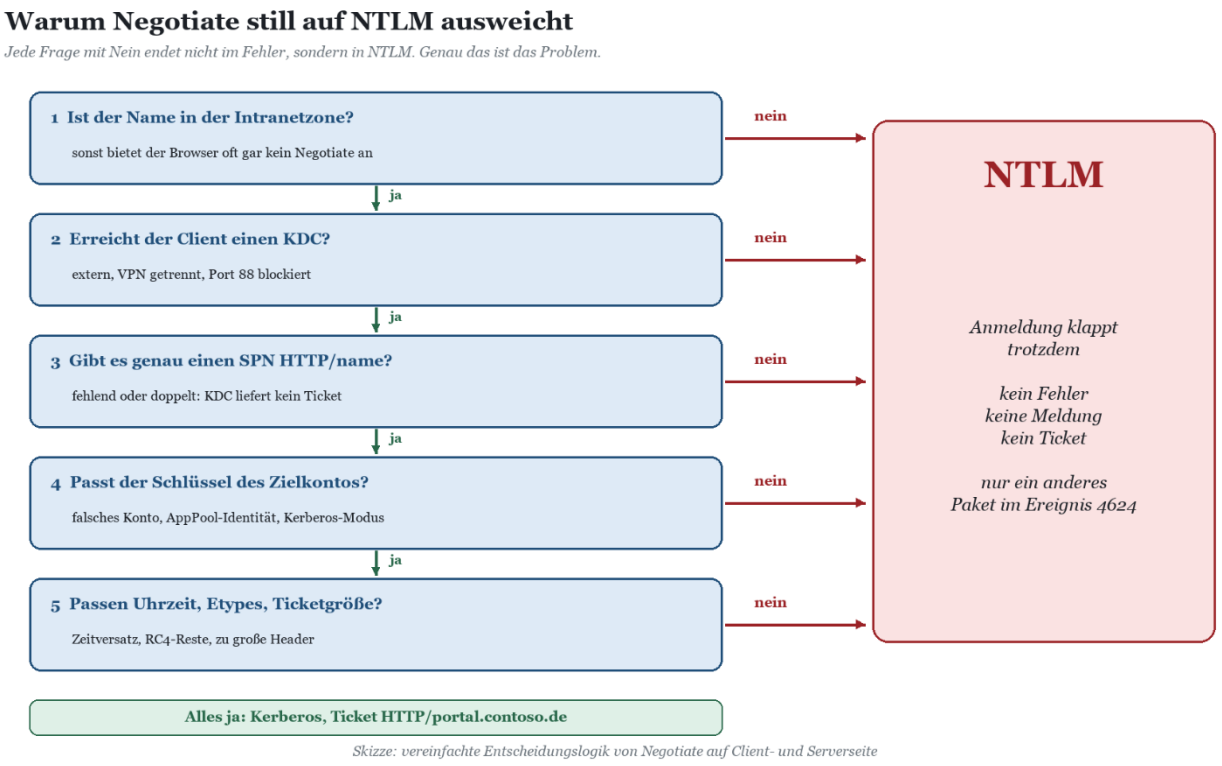
Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz.

AUS DER PRAXIS · Das Intranet, das seit drei Jahren NTLM spricht

Eine Kreisverwaltung veröffentlicht ihr SharePoint-Intranet über einen LoadMaster mit TLS-Offload und Durchreichen. Im Betriebshandbuch steht Kerberos. Bei der Vorbereitung auf Windows Server 2025 schaltet das Team das NTLM-Auditing an und staunt: Über 95 Prozent der Anmeldungen am Webfrontend laufen per NTLM V2. Ursache war ein Umzug der Anwendungspools auf ein neues Dienstkonto, bei dem der SPN HTTP/intranet.contoso.local am alten Konto hängen geblieben war. Der KDC stellte brav Tickets mit dem falschen Schlüssel aus, IIS konnte sie nicht entschlüsseln, der Browser wich auf NTLM aus. Drei Jahre lang. Die Korrektur dauerte zehn Minuten, die Suche zwei Tage.

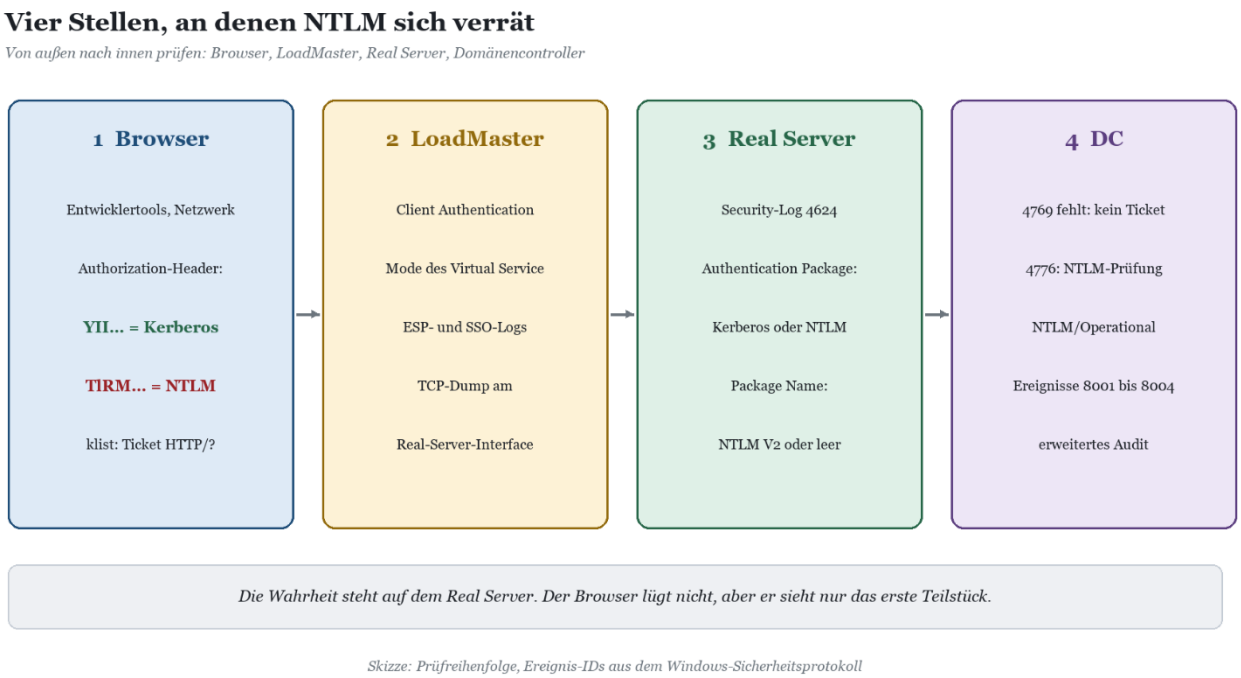
So prüfst du, ob hinter dem LoadMaster still NTLM läuft

Der Kerberos-Fallback ist deshalb so tückisch, weil Negotiate genau so gebaut ist: Der Client versucht Kerberos, und wenn irgendetwas nicht passt, nimmt er NTLM. Der Benutzer merkt nichts, der Server ist zufrieden, und der Helpdesk bekommt keinen Anruf. Die Skizze zeigt die üblichen Verdächtigen.



Skizze: vereinfachte Entscheidungslogik von Negotiate auf Client- und Serverseite

Prüfen musst du deshalb nicht, ob die Anmeldung klappt, sondern womit. Und zwar getrennt für jedes Teilstück: Client zum LoadMaster und LoadMaster zum Real Server. Beim Durchreichen ist das ein und dasselbe Gespräch, bei ESP sind es zwei.



Skizze: Prüfreihenfolge, Ereignis-IDs aus dem Windows-Sicherheitsprotokoll

Schritt 1: der Authorization-Header im Browser

Öffne die Entwicklertools des Browsers, Registerkarte Netzwerk, und lade die Seite neu. In der ersten Anfrage, die mit 401 beantwortet wird, steht im Antwortheader WWW-Authenticate: Negotiate. Interessant ist die nächste Anfrage des Browsers. Beginnt der Wert hinter Authorization: Negotiate mit YII, handelt es sich um ein SPNEGO-verpacktes Kerberos-Ticket. Beginnt er mit TlRMTVNTUAAB, ist das die Base64-Form von NTLMSSP, also eine NTLM-Type-1-Nachricht. Mehr Diagnose in zehn Sekunden bekommst du nirgends.

Ergänzend zeigt klist in einer Eingabeaufforderung des Clients, ob ein Ticket für HTTP/portal.contoso.de im Cache liegt. Fehlt es nach dem Seitenaufruf, hat der Client gar nicht erst Kerberos verwendet. Mit klist purge leerst du den Cache, um den Test zu wiederholen.

```
klist purge
REM Seite im Browser neu laden, dann:
klist | findstr /i "HTTP/portal.contoso.de"
```

WICHTIG · Der Browser sieht nur das erste Teilstück

Bei ESP mit NTLM oder NTLM-Proxy sagt der Header im Browser nur etwas über die Strecke zum LoadMaster. Ob der LoadMaster nach hinten Kerberos über KCD oder den durchgereichten NTLM-Handshake verwendet, siehst du nur auf dem Real Server oder in einem Mitschnitt auf der Serverseite des LoadMasters. Wie du L7-Debug und TCP-Dump dafür einsetzt, beschreibt Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump.

Schritt 2: das Sicherheitsprotokoll des Real Servers

Die verlässlichste Quelle ist das Ereignis 4624, eine erfolgreiche Anmeldung, im Sicherheitsprotokoll jedes Real Servers. Das Feld Authentication Package nennt Kerberos oder NTLM, das Feld Package Name bei NTLM zusätzlich die Version, im Idealfall NTLM V2 und niemals NTLM V1. Bei Webanmeldungen über IIS ist der Logon Type üblicherweise 3, also Netzwerk. Das folgende PowerShell-Fragment zählt die Netzwerkanmeldungen der letzten Stunden nach Paket:

```
$seit = (Get-Date).AddHours(-8)
```

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624; StartTime=$seit} |
  ForEach-Object {
    $x = [xml]$_.ToXml()
    $d = @{}; $x.Event.EventData.Data | ForEach-Object { $d[$_.Name] = $_.'#text' }
    if ($d.LogonType -eq '3') {
      [pscustomobject]@{ Paket = $d.AuthenticationPackageName; Version = $d.LmPackageName
}
    }
  } | Group-Object Paket, Version | Sort-Object Count -Descending |
  Select-Object Count, Name
```

Taucht dort NTLM in nennenswerter Menge auf, obwohl du Kerberos erwartest, weißt du Bescheid. Achte darauf, dass auch Health Checks des LoadMasters, Monitoring und Backup-Agenten Anmeldungen erzeugen. Filtere bei Bedarf nach Benutzerkonto, damit das technische Grundrauschen nicht die Statistik verfälscht.

Schritt 3: Domänencontroller und NTLM-Auditing

Am Domänencontroller ist die Abwesenheit das Signal. Fordert ein Client ein Service-Ticket für HTTP/portal.contoso.de an, entsteht ein Ereignis 4769. Fehlt es, während gleichzeitig Ereignisse 4776 zur Prüfung von Anmeldedaten für dieselben Benutzer auftauchen, läuft NTLM. Gezielter wird es mit den NTLM-Überwachungsrichtlinien unter „Netzwerksicherheit: NTLM einschränken“. Im Überwachungsmodus blockieren sie nichts, schreiben aber in das Protokoll Microsoft-Windows-NTLM/Operational, welcher Client sich bei welchem Server per NTLM angemeldet hat, am Domänencontroller etwa als Ereignis 8004. Windows Server 2025 und Windows 11 24H2 bringen zusätzlich ein erweitertes NTLM-Auditing mit, das Microsoft als ersten Schritt der Abschaltung versteht.

Ort	Ereignis oder Werkzeug	Was es dir sagt
Browser	Authorization-Header	YII: Kerberos, TlRM: NTLM auf der Strecke zum ersten Hop
Client	klist	Ticket für HTTP/name vorhanden oder nicht
Real Server	Sicherheit 4624	Authentication Package und NTLM-Version je Anmeldung
Real Server	NTLM/Operational 8002	eingehende NTLM-Anmeldungen bei aktivem Audit
Domänencontroller	Sicherheit 4769	Service-Ticket ausgestellt, also Kerberos
Domänencontroller	Sicherheit 4776	Prüfung von Anmeldedaten, typisch für NTLM
Domänencontroller	NTLM/Operational 8004	NTLM-Anmeldung über diesen DC bei aktivem Audit
LoadMaster	ESP-Logs, TCP-Dump	was zwischen LoadMaster und Real Server wirklich passiert

TIPP · Erst messen, dann härten

Schalte die NTLM-Überwachung auf Domänencontrollern und Real Servern mehrere Wochen im reinen Auditmodus ein, bevor irgendjemand NTLM einschränkt. Monatsabschluss, Quartalsberichte und der eine Scanner im Keller melden sich gern erst spät. Erst wenn die Liste stabil ist, weißt du, welche Virtual Services wirklich betroffen sind.

Wenn du den Fallback gefunden hast

Die Ursachen sind meist banal und liegen fast nie am LoadMaster selbst. Ein fehlender oder doppelter SPN, ein Anwendungspool unter einer anderen Identität als gedacht, ein Name, der per

CNAME auf einen Server zeigt, dessen Computerkonto den SPN nicht trägt, oder eine Browserzone, die den Namen als Internet einstuft. Prüfe mit setspn -Q HTTP/portal.contoso.de, wer den SPN hält, und mit setspn -X, ob er doppelt vergeben ist. Danach kläre, ob die Identität der Anwendung auf allen Real Servern dieselbe ist.

```
setspn -Q HTTP/portal.contoso.de
setspn -X -F
```

WARNUNG · Nicht einfach Kerberos erzwingen

Der Reflex, auf dem IIS NTLM aus der Providerliste zu streichen, um Kerberos zu erzwingen, ist verständlich und gefährlich. Ein Teil der Clients sieht dann keinen Fallback mehr, sondern eine Fehlermeldung, und ein NTLM-Proxy am LoadMaster für denselben Server hört sofort auf zu funktionieren. Erst die Ursache beheben, dann mit Auditing bestätigen, dann einschränken.

FAQ: NTLM, NTLM-Proxy und Kerberos am LoadMaster

Ist NTLM-Proxy dasselbe wie das Durchreichen von NTLM?

Nein. Beim Durchreichen ist der LoadMaster an der Anmeldung nicht beteiligt. Im NTLM-Proxy-Modus des Edge Security Packs authentifiziert der LoadMaster den Benutzer aktiv und lässt den Handshake vom Real Server bestätigen. Er kennt danach die Identität und kann sie für Gruppenprüfungen oder serverseitige KCD verwenden.

Brauche ich für den NTLM-Proxy einen SPN oder eine Delegation?

Nein, solange der Real Server den Benutzer selbst per NTLM authentifiziert. Genau das macht den Modus attraktiv. Kombinierst du ihn serverseitig mit KCD, gelten für diesen Teil natürlich die üblichen KCD-Voraussetzungen.

Woran erkenne ich, ob mein LoadMaster noch im alten NTLM-Modus arbeitet?

Am globalen Schalter NTLM Proxy Mode unter System Configuration > Miscellaneous Options > L7 Configuration und an der Bezeichnung des Client-Modus im Virtual Service. Steht dort NTLM statt NTLM-Proxy, ist der alte LDAP-basierte Modus aktiv.

Hört der NTLM-Proxy auf zu funktionieren, wenn Microsoft NTLM abschaltet?

Wenn Netzwerk-NTLM auf deinen Real Servern oder Domänencontrollern deaktiviert ist, ja. Laut Microsoft wird das im nächsten großen Windows-Server-Release der Standard sein, mit der Möglichkeit, NTLM per Richtlinie wieder einzuschalten. Plane deshalb jetzt die Ablösung durch KCD oder sauberes Kerberos.

Warum sieht mein Browser Kerberos, der Real Server aber NTLM?

Weil du zwei Teilstücke hast. Bei ESP endet das Kerberos des Browsers am LoadMaster, sofern der Client-Modus das überhaupt nutzt. Was der LoadMaster nach hinten spricht, bestimmt der Server-Modus. Prüfe deshalb immer auch das Ereignis 4624 auf dem Real Server.

Kann ich mit dem NTLM-Proxy MFA vor die Anwendung setzen?

Nicht sinnvoll. NTLM ist eine stille Anmeldung ohne Interaktion. Wer MFA am LoadMaster will, nimmt eine formularbasierte oder SAML-basierte Clientanmeldung und KCD auf der Serverseite.

Fazit: Pragmatismus mit Ablaufdatum

Der NTLM-Proxy des LoadMasters ist ein ehrliches Werkzeug. Er löst ein reales Problem, nämlich nahtlose Windows-Anmeldung ohne SPN-Pflege und ohne Delegationsrechte, und er ist deutlich besser als der alte LDAP-basierte NTLM-Modus. Wer nach einem Firmware-Update noch im

Altmodus läuft, sollte das als Erstes ändern. Gleichzeitig steht NTLM bei Microsoft auf der Abschussliste, bringt bekannte Sicherheitsschwächen mit und liefert ein dünneres Audit. Als Brücke ist der NTLM-Proxy gut, als Fundament nicht.

Der größere Feind ist ohnehin nicht der NTLM, den du bewusst eingerichtet hast, sondern der, von dem du nichts weißt. Nimm dir eine Stunde, schau in die Authorization-Header, zähle die Ereignisse 4624 auf deinen Real Servern und schalte das NTLM-Auditing ein. Schwarzhumorig formuliert: Lieber findest du den stillen Fallback heute selbst, als dass Microsoft ihn dir an einem Patchday zeigt.

TIPP · Unterstützung bei Bestandsaufnahme und Umstellung

Wenn du wissen willst, welche Virtual Services heimlich NTLM sprechen, und den Weg zu KCD oder sauberem Kerberos planen möchtest, hilft dir die Beratung zum Kemp LoadMaster. Wer Negotiate, NTLM-Proxy und KCD mit dem eigenen Team im Labor durchspielen will, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server
› Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten
› Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz
› Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump
› Microsoft Kerberos