Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung



Wissen

Der Überblick zur ganzen Serie: Recht, Technik und Organisation von Microsoft 365 in der Klinik.

› Microsoft 365 im Krankenhaus

Beratung

Bestandsaufnahme der Vertrauensstellungen, Zielbild für Ihren Verbund und Begleitung der Umstellung je Standort.

› Microsoft-365-Beratung für Krankenhäuser

Schulung

Administratoren fit machen für Kerberos, Vertrauensstellungen, Netzwerkmitschnitt und Fehlersuche.

› Microsoft-365-Schulung für Krankenhäuser

Jeder Klinikverbund hat eine Fusionsgeschichte, und jede Fusionsgeschichte hat ein Active Directory, das sie konserviert. Das Haus, das vor Jahren übernommen wurde, hat seine Domäne behalten. Das zweite auch. Dazwischen hängen externe Vertrauensstellungen, die irgendwann an einem Freitagnachmittag eingerichtet wurden, damit die Geschäftsführung am Montag auf die Freigaben der Personalabteilung zugreifen konnte. Das war als Übergang gedacht. Übergänge sind in der Krankenhaus-IT bekanntlich die langlebigste Bauform, gleich nach dem Provisorium und kurz vor dem Faxgerät.

Solange alles läuft, fällt das niemandem auf. Spätestens wenn Sie NTLM einschränken wollen, ein Audit nach dem Stand der Technik fragt oder die Synchronisierung in einen gemeinsamen Microsoft-Entra-Mandanten ansteht, wird aus der historischen Kuriosität ein Projekt. Dieser Beitrag erklärt, warum externe Vertrauensstellungen Kerberos ausbremsen und NTLM praktisch erzwingen, was eine Gesamtstruktur-Vertrauensstellung anders macht, welche Rolle SID-Filterung, Quarantäne und Namenssuffix-Routing spielen und wie Sie die Umstellung Standort für Standort mit Netzwerkmitschnitt absichern. Und er sagt offen, was am Ende realistisch ist: Selten die große Vollmigration, häufig eine saubere Koexistenz.

Der Artikel gehört zur Serie Microsoft 365 im Krankenhaus und ist der technische Kern des Blocks zu Identität und Infrastruktur. Er richtet sich an IT-Leitungen und Administratoren, gibt aber auch Geschäftsführung, Informationssicherheitsbeauftragten und Vertretungen der Belegschaft genug

Kontext, um die Entscheidungen mitzutragen. Arztpraxen, Pflegeheime und Krankenkassen haben meist andere Sorgen; hier geht es um Akutkrankenhäuser, Fach- und Rehakliniken, Universitätsklinika und Verbünde mit mehreren Standorten.

Die Ausgangslage: Zentraldomäne, Altdomänen und das Erbe der Fusionsphase

Das typische Bild sieht so aus: Der Träger betreibt eine Zentraldomäne, meist am Hauptstandort, in der Verwaltung, IT und oft schon die Geschäftsführung leben. Daneben existieren mehrere Altdomänen der übernommenen Häuser, jede eine eigene Gesamtstruktur mit eigenem Schema, eigenen Domänencontrollern, eigenen Gruppenrichtlinien und eigener Vorstellung davon, was ein sicheres Kennwort ist. Verbunden sind sie über externe Vertrauensstellungen, gelegentlich zusätzlich quer zwischen zwei Häusern, weil das Labor von Haus B einmal für Haus C mitarbeiten sollte.

In den Altdomänen hängt der eigentliche Krankenhausbetrieb: Stationsrechner, Funktionsbereiche, das KIS mit seinen Subsystemen wie LIS, RIS und PACS, die Medizintechnik mit ihren Servern und Modalitäten, dazu Fachanwendungen, deren Hersteller bei der Frage nach einer Domänenänderung höflich, aber bestimmt auf den Wartungsvertrag verweisen. Das erklärt, warum diese Domänen so zäh überleben: Sie sind nicht nur Verzeichnis, sondern Betriebsgrundlage.

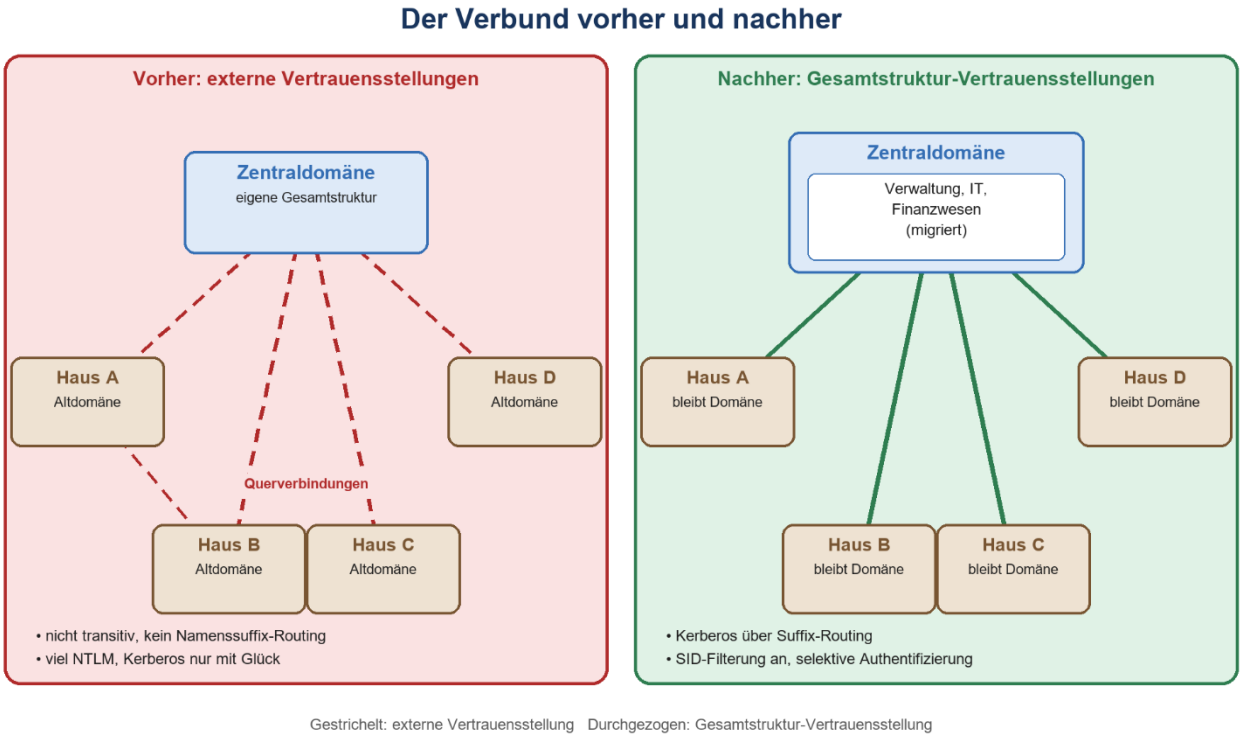

Abbildung 1: Links der gewachsene Zustand mit externen Vertrauensstellungen, rechts das Zielbild mit Gesamtstruktur-Vertrauensstellungen und teilweiser Konsolidierung.

Woran Sie merken, dass die Vertrauensstellungen ein Problem sind

- Anmeldungen über die Domänengrenze landen im Ereignisprotokoll mit dem Authentifizierungspaket NTLM, obwohl alle Beteiligten Kerberos könnten.
- Ein Dienst funktioniert nur, wenn man ihn per NetBIOS-Kurzname oder IP-Adresse anspricht, mit vollqualifiziertem Namen aber nicht, oder umgekehrt.
- Delegierungsszenarien, etwa ein Webportal, das im Namen der Benutzer auf eine Datenbank zugreift, scheitern über die Domänengrenze.

- Niemand kann sagen, ob auf den Vertrauensstellungen SID-Filterung aktiv ist, und die Dokumentation stammt aus der Zeit vor der letzten Umbenennung der IT-Abteilung.
- Die NTLM-Überwachung zeigt Ihnen eine Liste, deren Länge Ihre Rufbereitschaft schlecht schlafen lässt.

Fakten: Begriffe in einem Satz

• **Gesamtstruktur (Forest):** Sicherheitsgrenze im Active Directory mit gemeinsamem Schema, Konfiguration und globalem Katalog.

• **Externe Vertrauensstellung:** nicht transitive Vertrauensstellung zwischen zwei einzelnen Domänen unterschiedlicher Gesamtstrukturen.

• **Gesamtstruktur-Vertrauensstellung:** transitive Vertrauensstellung zwischen den Stammdomänen zweier Gesamtstrukturen, einseitig oder beidseitig, nicht auf eine dritte Gesamtstruktur erweiterbar.

• **TDO (Trusted Domain Object):** das Objekt im Container System, das jede Vertrauensstellung beschreibt; bei Gesamtstruktur-Vertrauensstellungen enthält es zusätzlich die Namensräume des Partners.

• **Namenssuffix-Routing:** Regeln, welche DNS-, UPN- und SPN-Suffixe über eine Gesamtstruktur-Vertrauensstellung an den Partner verwiesen werden.

Warum externe Vertrauensstellungen Kerberos ausbremsen

Die Antwort liegt darin, wie ein Domänencontroller entscheidet, wohin er einen Client schickt. Will ein Client in Haus A auf einen Dateiserver der Zentrale zugreifen, fragt er seinen eigenen Domänencontroller nach einem Dienstticket für den Dienstprinzipalnamen (SPN) des Servers. Der Domänencontroller sucht diesen SPN in der eigenen Domäne und im globalen Katalog seiner Gesamtstruktur. Dort findet er ihn nicht, denn der Server gehört zu einer anderen Gesamtstruktur.

Jetzt kommt der Unterschied. Bei einer Gesamtstruktur-Vertrauensstellung hat das TDO beim Einrichten die Namensräume der Partnergesamtstruktur gesammelt: Domänenbaumnamen, UPN-Suffixe, SPN-Suffixe und SID-Namensräume. Microsoft beschreibt in der Dokumentation zu Vertrauensstellungen auf Microsoft Learn genau diesen Mechanismus: Der globale Katalog vergleicht das Suffix des gesuchten SPN mit den im TDO hinterlegten Namensräumen, liefert bei einem Treffer einen Routinghinweis, und der Client folgt der Verweiskette bis zum Domänencontroller, der das Ticket ausstellen kann.

Eine externe Vertrauensstellung kennt diese Namensräume nicht. Sie bildet nur den exakten Domänennamen des Partners ab, eine Suffixzuordnung, wie Kerberos sie für Verweise braucht, gibt es nicht. Der Domänencontroller antwortet dem Client also sinngemäß, dass er den Dienstprinzipal nicht kennt. Der Client zuckt mit den Schultern und versucht es über Negotiate mit NTLM. Das funktioniert, weil NTLM über die Vertrauensstellung per Pass-Through-Authentifizierung beim Domänencontroller des Benutzers nachfragt. Für den Benutzer sieht alles gut aus. Für Ihre Sicherheitsarchitektur nicht.

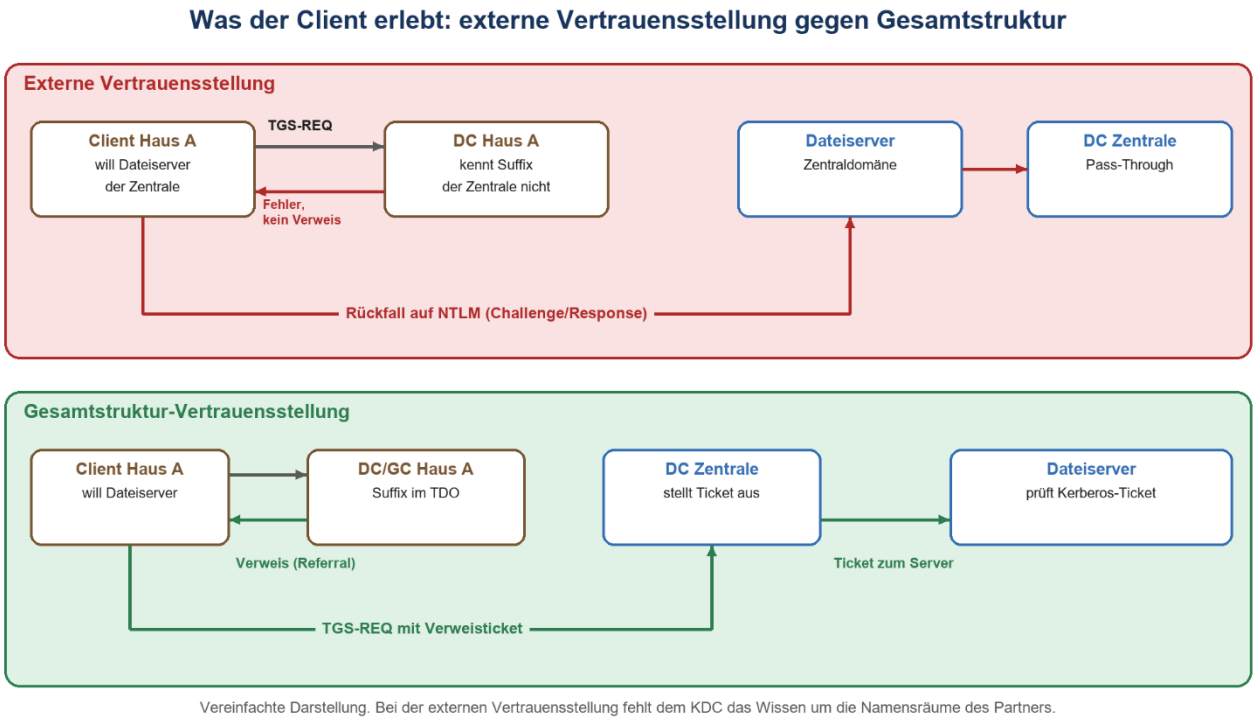

Abbildung 2: Bei der externen Vertrauensstellung endet der Kerberos-Versuch beim eigenen Domänencontroller, der Client fällt auf NTLM zurück. Die Gesamtstruktur-Vertrauensstellung liefert einen Verweis.

Wichtig: Kerberos über externe Vertrauensstellungen ist nicht unmöglich, nur unzuverlässig

Es gibt Konstellationen, in denen Kerberos auch über eine externe Vertrauensstellung klappt, etwa wenn auf dem Client eine explizite Zuordnung von Host zu Bereich hinterlegt ist (ksetup) oder die Anwendung den Zielbereich selbst mitgibt. Darauf eine Verbundarchitektur zu bauen, ist ungefähr so belastbar wie ein Dienstplan, der auf „Das macht schon jemand“ beruht. Wurde die Vertrauensstellung zudem nur mit NetBIOS-Namen angelegt, bleibt ohnehin nur NTLM.

Warum NTLM über Vertrauensstellungen ein Sicherheitsthema ist

NTLM ist ein Challenge-Response-Verfahren ohne gegenseitige Authentifizierung des Servers, anfällig für Relay-Angriffe und für das Weiterreichen erbeuteter Hashes. Genau diese Techniken tauchen in den Ransomware-Fällen auf, die Krankenhäuser in den vergangenen Jahren getroffen haben: Ein kompromittiertes Konto in einem Haus, eine Vertrauensstellung ohne Einschränkungen, und der Angreifer spaziert in die Zentrale. Microsoft hat Anfang 2026 einen Fahrplan veröffentlicht, nach dem Netzwerk-NTLM in einer künftigen Windows-Server-Version standardmäßig deaktiviert sein soll; die erweiterte NTLM-Überwachung steht mit Windows Server 2025 und Windows 11 24H2 bereits zur Verfügung. Abgeschafft wird NTLM damit nicht, aber wer heute noch auf NTLM über Vertrauensstellungen angewiesen ist, steht absehbar vor einer Ausnahmeregel, die er begründen muss.

Hinzu kommt die Verschlüsselung: Microsoft drängt RC4 als Verschlüsselungstyp für Kerberos seit 2026 schrittweise zurück, die Domänencontroller verwenden für Konten ohne explizite Einstellung AES. Vertrauensstellungen, die vor langer Zeit angelegt wurden, sollten Sie deshalb auch auf ihre unterstützten Verschlüsselungstypen prüfen. Es wäre ärgerlich, NTLM sauber verdrängt zu haben, nur um dann an einer RC4-Vertrauensstellung hängen zu bleiben. Mehr zu den Grundlagen finden Sie im Kompetenzbereich Kerberos.

SID-Filterung, Quarantäne und selektive Authentifizierung

Die zweite Baustelle ist die Frage, welche Sicherheitskennungen über die Vertrauensstellung akzeptiert werden. Ein Konto kann im Attribut sIDHistory frühere SIDs mitbringen, etwa aus einer Migration. Ohne Filterung könnte ein Administrator der vertrauten Domäne einem Konto beliebige SIDs unterschieben, auch die der Domänen-Admins der vertrauenden Seite. Die SID-Filterung verhindert das, indem sie nur SIDs aus der vertrauten Domäne bzw. Gesamtstruktur durchlässt.

- **Externe Vertrauensstellungen:** Hier heißt die SID-Filterung Quarantäne. Auf Vertrauensstellungen, die mit aktuellen Domänencontrollern angelegt wurden, ist sie standardmäßig aktiv. Alte Vertrauensstellungen oder solche, bei denen jemand während einer Migration die Quarantäne mit netdom abgeschaltet und nie wieder eingeschaltet hat, sind die klassische Fundstelle.
- **Gesamtstruktur-Vertrauensstellungen:** SID-Filterung ist standardmäßig aktiv, SIDs aus sIDHistory werden verworfen. Für eine Migration mit SID-Verlauf lässt sich das gezielt öffnen; das ist dann ein befristeter, dokumentierter Ausnahmezustand und kein Dauerzustand.
- **Selektive Authentifizierung:** Statt jedem Konto der vertrauten Seite die Anmeldung an allen Rechnern der vertrauenden Seite zu erlauben, braucht es dann das Recht „Authentifizierung zulassen“ am jeweiligen Computerobjekt. Für einen Verbund, in dem die Häuser nur auf ausgewählte zentrale Server zugreifen sollen, ist das das Mittel der Wahl.

```
# Vertrauensstellungen und ihre Eigenschaften anzeigen (Beispiel)
Get-ADTrust -Filter * | Select-Object Name, Direction, ForestTransitive,
SIDFilteringQuarantined,
    SIDFilteringForestAware, SelectiveAuthentication, TrustAttributes

# Quarantäne einer externen Vertrauensstellung prüfen (auf der vertrauenden Seite)
netdom trust haus-a.example /domain:zentrale.example /quarantine

# Vertraute Domänen und Status des sicheren Kanals
nltest /domain_trusts /all_trusts /v
```

Namenssuffix-Routing: der Teil, der bei Fusionen gern kollidiert

Bei einer Gesamtstruktur-Vertrauensstellung entscheidet das Namenssuffix-Routing, welche Suffixe an den Partner verwiesen werden. Neue Suffixe, die nach dem Anlegen hinzukommen, müssen Sie aktiv freigeben, sonst landen Anmeldungen mit dem neuen UPN-Suffix im Nirgendwo. Kritischer sind Überschneidungen: Haben zwei Gesamtstrukturen denselben UPN-Suffix, etwa weil alle Häuser nach der Fusion die neue Verbund-Maildomäne als UPN-Suffix eingetragen haben, erkennt Windows den Konflikt und deaktiviert das Routing für den betroffenen Namen. Das ist kein Fehler, sondern Absicht: Ein Name darf nur in eine Richtung zeigen.

Genau hier treffen sich lokales Active Directory und Cloud-Identität. Für die Synchronisierung in einen gemeinsamen Entra-Mandanten wollen Sie eindeutige UPN-Suffixe je Gesamtstruktur oder eine bewusste Entscheidung, welche Gesamtstruktur welchen Suffix führt. Wie man das planerisch auflöst, beschreibt der Beitrag Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen.

Vertrauensstellungstypen im Vergleich

Vertrauensstellungstyp	Kerberos	Risiko	Einsatz im Klinikverbund
Übergeordnet/untergeordnet (innerhalb einer	Ja, transitiv,	Gering bis mittel: Die Gesamtstruktur ist die	Nur sinnvoll, wenn die Häuser einer

Vertrauensstellungstyp	Kerberos	Risiko	Einsatz im Klinikverbund
Gesamtstruktur)	automatisch	Sicherheitsgrenze, nicht die Domäne	gemeinsamen Gesamtstruktur angehören sollen; kaum nachträglich herstellbar
Verknüpfung (Shortcut)	Ja, verkürzt Verweisketten	Gering	Große Gesamtstruktur mit tiefen Domänenbäumen; im Verbund selten
Extern	Nur in Sonderfällen, sonst Rückfall auf NTLM	Hoch, wenn Quarantäne fehlt; NTLM-Relay und Pass-the-Hash über die Grenze	Übergangslösung aus der Fusionsphase; Zugriff auf eine einzelne Domäne einer fremden Gesamtstruktur
Extern, nur NetBIOS-Name	Nein	Hoch	Altlast, zeitnah ersetzen
Gesamtstruktur	Ja, über Namenssuffix-Routing	Mittel; mit SID-Filterung und selektiver Authentifizierung gut beherrschbar	Regelfall für die dauerhafte Koexistenz von Zentraldomäne und Hausdomänen
Bereich (Realm)	Ja, mit MIT-kompatiblen Bereichen	Abhängig vom Partner	Anbindung von Unix- oder Linux-Kerberos, etwa in Forschungsnetzen von Universitätsklinika

Die Umstellung je Standort: von extern zu Gesamtstruktur

Eine externe Vertrauensstellung lässt sich nicht in eine Gesamtstruktur-Vertrauensstellung umwandeln. Zwischen zwei Domänen gibt es genau ein TDO, also genau eine Vertrauensstellung. Der Weg führt über Löschen und Neuanlegen, und zwischen beidem gibt es einen Moment, in dem keine Vertrauensstellung existiert. Bei einer Verwaltungsdomäne ist das lästig. Bei einer Domäne, in der Stationsrechner, Medizintechnik und KIS-Schnittstellen hängen, ist das ein Change mit Rufbereitschaft, Rückweg und Abstimmung mit der Pflegedirektion, damit niemand im Nachtdienst plötzlich ohne Laborbefunde dasteht.



Abbildung 3: Die Umstellung je Standort in sieben Schritten. Die ersten vier Schritte sind risikoarme Vorarbeit.

Vorbereitung: Inventur und Voraussetzungen

Bevor Sie irgendetwas löschen, brauchen Sie ein vollständiges Bild. Welche Vertrauensstellungen gibt es, in welche Richtung, mit welchen Attributen? Welche Gruppen der einen Seite stehen in Berechtigungen der anderen? Welche Dienstkonten aus einem Haus laufen auf Servern der Zentrale? Und vor allem: Wer nutzt die Vertrauensstellung tatsächlich? Die Antwort auf die letzte Frage liefert nicht die Dokumentation, sondern die Überwachung.

Prüfpunkt	Werkzeug	Was Sie erwarten wollen
Beide Domänen sind Stammdomänen ihrer Gesamtstruktur	Active Directory-Domänen und -Vertrauensstellungen, Get-ADForest	Gesamtstruktur-Vertrauensstellungen gibt es nur zwischen Stammdomänen
Funktionsebene der Gesamtstruktur	Get-ADForest	Mindestens Windows Server 2003; realistisch deutlich höher, sonst haben Sie andere Probleme
DNS-Auflösung in beide Richtungen	Bedingte Weiterleitungen oder sekundäre Zonen, Resolve-DnsName	Jede Seite löst die Namensräume der anderen auf, auch die SRV-Einträge
UPN- und SPN-Suffixe ohne Überschneidung	Get-ADForest (UPNSuffixes), setspn -X	Keine doppelten Suffixe, keine doppelten SPN
NTLM-Nutzung über die Grenze	NTLM-Überwachung auf den Domänencontrollern, Ereignisse 8004 und 4624	Liste der Quellen, Ziele und Konten, die noch NTLM verwenden
Firewall zwischen den Standorten	Portprüfung gemäß Microsoft-Dokumentation zu Vertrauensstellungen	Kerberos, LDAP, RPC und SMB zwischen den Domänencontrollern frei
Verschlüsselungstypen	Eigenschaften des TDO, msDS-SupportedEncryptionTypes	AES aktiv, RC4 nur bewusst und befristet

Tipp: Erst messen, dann reden

Schalten Sie die NTLM-Überwachung auf allen Domänencontrollern Wochen vor der Umstellung ein und lassen Sie sie über mindestens einen vollständigen Monatszyklus laufen.

Monatsabschluss im Finanzwesen, Quartalsberichte, die nächtliche Datensicherung, der Dienstplanexport für die Personalabteilung: Manche NTLM-Verbindung meldet sich nur einmal im Monat, dann aber garantiert während Ihres Wartungsfensters.

Testen mit Netzwerkmitschnitt

Ereignisprotokolle sagen Ihnen, dass NTLM verwendet wurde. Der Netzwerkmitschnitt sagt Ihnen, warum. Für jede kritische Verbindung über die Domänengrenze lohnt sich ein Mitschnitt direkt auf dem Client oder unmittelbar davor, mit einem Filter auf Kerberos und NTLMSSP. Vor der Umstellung dokumentieren Sie damit den Ist-Zustand, danach liefern Sie den Nachweis, dass tatsächlich Kerberos spricht. Das ist nicht nur technisch hilfreich, sondern auch für das Änderungsprotokoll und die Gespräche mit Herstellern von Fachanwendungen Gold wert.

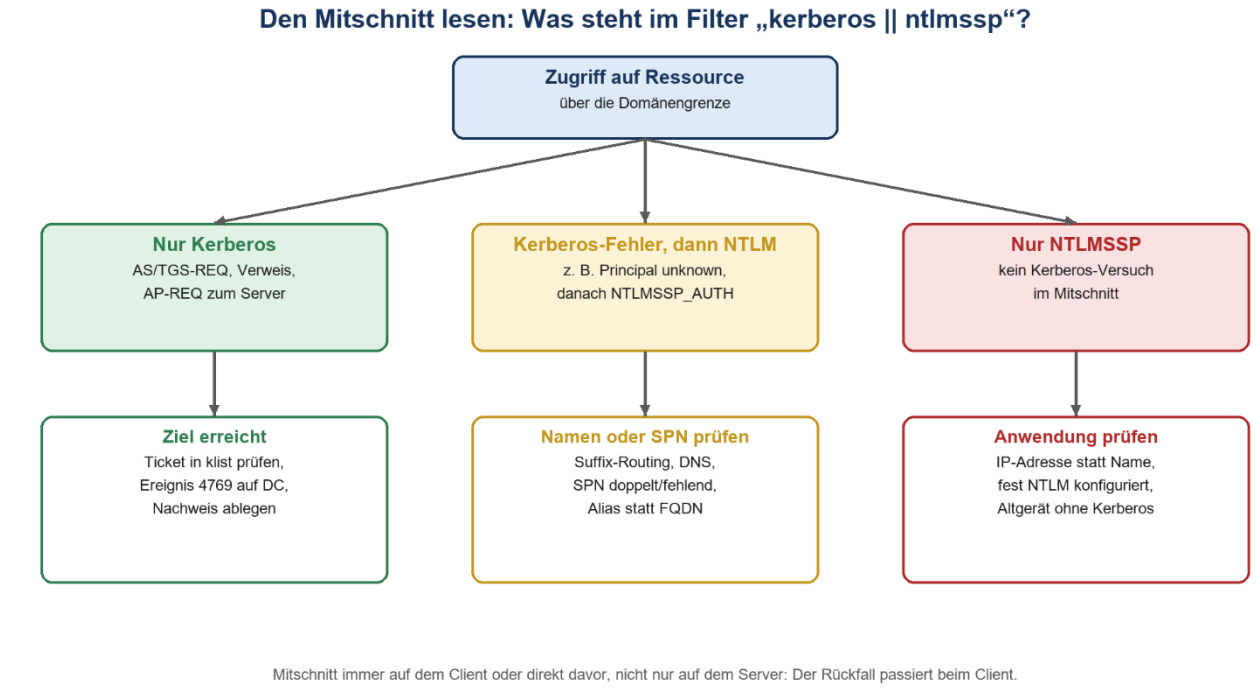

Abbildung 4: Drei typische Befunde im Mitschnitt und was daraus folgt.

Befund im Mitschnitt	Bedeutung	Nächster Schritt
TGS-REQ, Antwort mit Fehler Principal unknown, danach NTLMSSP	Kein Verweis möglich, typischer Fall der externen Vertrauensstellung oder fehlendes Suffix-Routing	Suffix-Routing und DNS prüfen; nach Umstellung erneut messen
TGS-REQ, Verweisticket, AP-REQ an den Server	Kerberos über die Vertrauensstellung funktioniert	Nachweis ablegen, klist und Ereignis 4769 als Beleg
Nur NTLMSSP, kein Kerberos-Versuch	Client spricht Ziel per IP-Adresse an oder Anwendung ist fest auf NTLM konfiguriert	Namen statt IP-Adressen, Konfiguration der Anwendung prüfen, Hersteller einbinden
Kerberos-Fehler wegen doppeltem oder fehlendem SPN	SPN-Registrierung fehlerhaft	setspn -X, SPN am richtigen Konto registrieren
Kerberos-Fehler zu Verschlüsselungstyp	Konto oder Vertrauensstellung ohne passenden AES-Schlüssel	Kennwort neu setzen, Verschlüsselungstypen anpassen

```
# Beispielfilter für Wireshark auf dem Client
kerberos || ntlmssp

# Kerberos-Tickets des angemeldeten Benutzers anzeigen und Cache leeren
klist
klist purge
```

Das Wartungsfenster und danach

Im Wartungsfenster löschen Sie die externe Vertrauensstellung auf beiden Seiten, legen die Gesamtstruktur-Vertrauensstellung mit den vorab festgelegten Parametern an, prüfen das Namenssuffix-Routing, aktivieren die selektive Authentifizierung und vergeben die Berechtigung „Authentifizierung zulassen“ an den Servern, die aus dem jeweiligen Haus erreichbar sein müssen. Dann folgen die Tests mit der vorbereiteten Liste kritischer Verbindungen, erneut mit Mitschnitt. Erst wenn diese grün sind, endet das Fenster.

Die Härtung kommt in Etappen: NTLM für die Domänengrenze zunächst überwachen, dann für bekannte Ziele einschränken, Ausnahmen mit Begründung und Ablaufdatum dokumentieren. Die vollständige NTLM-Abschaltung ist ein eigenes Projekt mit eigener Dramaturgie, vor allem dort, wo Medizintechnik und Altanwendungen im Spiel sind. Eine funktionierende PKI hilft dabei an vielen Stellen, von Domänencontrollerzertifikaten bis zur zertifikatsbasierten Anmeldung; Grundlagen dazu finden Sie im Kompetenzbereich PKI mit ADCS.

Warnung: Nie alle Häuser in einem Fenster

Die Versuchung ist groß, alle Vertrauensstellungen in einer Nacht umzubauen, weil die Vorbereitung ja ohnehin gemacht ist. Tun Sie es nicht. Jedes Haus hat seine eigenen Fachanwendungen, seine eigenen Ausnahmen und seine eigene Station, die um drei Uhr morgens anruft. Ein Standort pro Fenster, mit Puffer bis zum nächsten, ist langsamer und erheblich weniger aufregend. In der Krankenhaus-IT ist „weniger aufregend“ ein Qualitätsmerkmal.

Aus der Praxis: Begleitung eines Krankenhausverbunds mit mehreren Standorten

In der langjährigen Begleitung eines Krankenhausverbunds hingen die übernommenen Häuser über externe Vertrauensstellungen aus der Fusionsphase an der Zentraldomäne. Sichtbar wurde das Problem, als NTLM eingeschränkt werden sollte: Die Überwachung zeigte, dass ein großer Teil des Verkehrs über die Domänengrenzen gar nicht wegen alter Anwendungen auf NTLM lief, sondern schlicht deshalb, weil die Vertrauensstellungen Kerberos keine Chance ließen.

Der Umbau auf Gesamtstruktur-Vertrauensstellungen erfolgte Standort für Standort, jeweils mit Netzwerkmitschnitt vorher und nachher. Parallel entstanden eine gehärtete PKI und eine saubere Kerberos-Konfiguration, die Exchange-Hybrid-Umgebung profitierte von den bereinigten Identitäten. Die wichtigste Erkenntnis: Erst nach dem Umbau ließ sich überhaupt ehrlich unterscheiden, welche NTLM-Fälle echte Altlasten waren und welche nur Symptome der Architektur.

Konsolidierung realistisch: saubere Koexistenz statt Vollmigration

Auf Folien sieht die Konsolidierung immer gleich aus: Alle Altdomänen werden in die Zentraldomäne migriert, die alten Domänencontroller abgeschaltet, Ende. In der Wirklichkeit

eines Klinikverbunds endet diese Folie häufig an der ersten Fachanwendung, die ihre Benutzer per SID, Domänenname oder Dienstkonto fest verdrahtet hat, an einem Medizintechnik-Server, den nur der Hersteller anfassen darf, oder an der schlichten Rechnung, wie viele Stationsrechner im laufenden Schichtdienst umgezogen werden müssten.

Deshalb sieht das realistische Ergebnis meist anders aus: Verwaltung, IT und Finanzwesen ziehen in die Zentraldomäne, weil sie ohnehin standortübergreifend arbeiten, die gleichen Anwendungen nutzen und von einer gemeinsamen Verwaltung am meisten profitieren. Die Häuser selbst, mit Stationen, Funktionsbereichen, Medizintechnik und lokalen Subsystemen, bleiben dauerhaft in ihren Domänen. Das Ziel ist dann saubere Koexistenz: Gesamtstruktur-Vertrauensstellungen, gemeinsame Sicherheitsstandards, zentrale Überwachung und ein gemeinsamer Entra-Mandant.

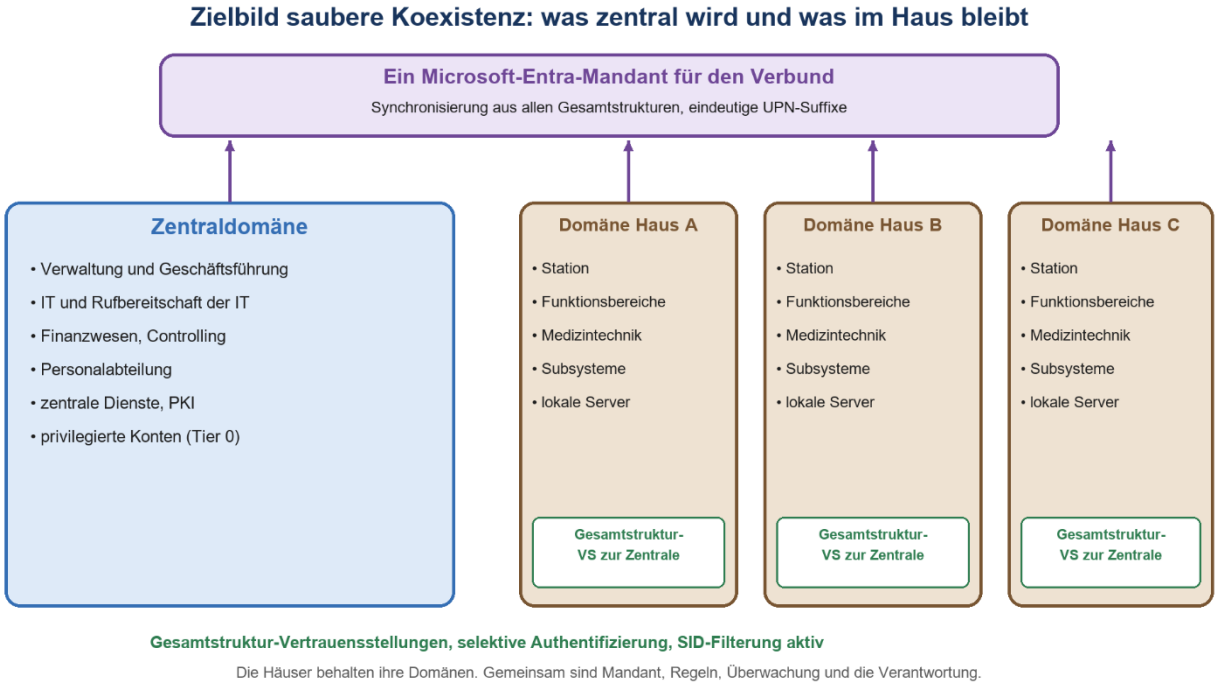

Abbildung 5: Zielbild saubere Koexistenz. Die Hausdomänen bleiben, gemeinsam sind Mandant, Regeln und Überwachung.

Option	Aufwand	Risiko für den Betrieb	Wann sinnvoll
Vollmigration aller Häuser in die Zentraldomäne	Sehr hoch, über Jahre	Hoch, berührt KIS, Subsysteme, Medizintechnik	Wenige, homogene Häuser; Neuaufbau ohnehin geplant; Hersteller sind mit im Boot
Teilmigration (Verwaltung, IT, Finanzwesen) plus Koexistenz	Mittel	Gering bis mittel, betrifft vor allem Büroarbeitsplätze	Regelfall im gewachsenen Verbund
Koexistenz ohne Migration	Gering	Gering	Häuser sind organisatorisch eigenständig oder ein Verkauf ist nicht ausgeschlossen
Alles lassen, wie es ist	Scheinbar keiner	Steigt jedes Jahr	Nie; spätestens die NTLM-Abkündigung und das nächste Audit holen Sie ein

Was saubere Koexistenz konkret bedeutet

- **Gemeinsame Mindeststandards:** Kennwortrichtlinien, Tiering für privilegierte Konten, LAPS, Härtung der Domänencontroller und einheitliche Überwachung in allen Gesamtstrukturen, nicht nur in der Zentrale.
- **Klare Administrationsgrenzen:** Wer administriert welche Gesamtstruktur? Domänen-Admins der Zentrale sind nicht automatisch Admins in den Häusern, und umgekehrt schon gar nicht.
- **Eindeutige Identitäten:** Jede Person hat genau ein führendes Konto. Doppelte Konten in Zentrale und Haus sind die Brutstätte für verwaiste Berechtigungen und für Lizenzchaos im Mandanten.
- **Ein Mandant, mehrere Quellen:** Microsoft Entra Connect und Entra Cloud Sync können mehrere Gesamtstrukturen in einen Mandanten synchronisieren. Welches Werkzeug in Ihrer Konstellation passt, hängt von Topologie und Anforderungen ab; das klären Sie im Kompetenzbereich Microsoft Entra ID.
- **Gemeinsame Notfallplanung:** Wiederherstellung einer Gesamtstruktur, Ausfall einer Vertrauensstellung, Notbetrieb eines Hauses ohne Verbindung zur Zentrale: Das gehört in die Notfallhandbücher, und zwar je Gesamtstruktur.

Migration der Verwaltung: was dabei zu beachten ist

Für die Teilmigration gelten die bekannten Regeln: Konten mit SID-Verlauf migrieren, damit Berechtigungen auf alten Ressourcen während der Übergangszeit greifen, Gruppen vor Benutzern, Rechner nach Benutzern, Profile mit Bedacht. Der SID-Verlauf setzt voraus, dass die SID-Filterung auf der betroffenen Vertrauensstellung für die Dauer der Migration entsprechend gelockert ist. Planen Sie das Zurückdrehen und das spätere Bereinigen von sIDHistory gleich mit, sonst wird aus der Übergangsregel die nächste Altlast. Ob und mit welchem Werkzeug Sie migrieren, prüfen Sie vorher gegen den aktuellen Supportstand bei Microsoft und gegen die Angebote spezialisierter Hersteller.

Und dann ist da die Datenebene. Mit den Konten ziehen Dateifreigaben um, und auf Dateifreigaben der Verwaltung finden sich erfahrungsgemäß Dinge, die dort nicht hingehören, darunter die berühmte Excel-Liste mit Patientennamen, die jemand vor Jahren für eine Auswertung angelegt hat. Das ist nicht der Normalfall, aber es kommt vor. Patientendaten gehören ins KIS und seine Subsysteme; eine Migration ist ein guter Anlass, solche Funde zu bereinigen, statt sie ordentlich in die neue Struktur zu übertragen. Die Abgrenzung beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt.

Wichtig: Recht, Nachweise und Mitbestimmung (keine Rechtsberatung)

Vertrauensstellungen und Authentifizierungsverfahren sind keine reine Geschmacksfrage der IT. Für Krankenhäuser regelt § 391 SGB V die IT-Sicherheit, seit dem NIS2-Umsetzungsgesetz in neuer Fassung; für Betreiber kritischer Anlagen gelten stattdessen die Pflichten des BSIG. Der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ der DKG liegt in Version 1.3.1 vor. Welche konkreten Anforderungen daraus für Ihre Verzeichnisdienste folgen, klären Sie mit Ihrer Informationssicherheit und gegebenenfalls juristisch. Den Überblick gibt der Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

Kontenmigrationen, neue Überwachung und geänderte Protokollierung berühren außerdem die Mitbestimmung. Ob Betriebsrat, Personalrat oder Mitarbeitervertretung zuständig ist und welche Beteiligungsrechte bestehen, hängt von Trägerschaft und Bundesland ab: Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

FAQ: Häufige Fragen zu Active Directory im Klinikverbund

Kann ich eine externe Vertrauensstellung einfach in eine Gesamtstruktur-Vertrauensstellung umwandeln?

Nein. Zwischen zwei Domänen existiert nur eine Vertrauensstellung. Sie löschen die externe und legen die Gesamtstruktur-Vertrauensstellung neu an. Deshalb gehört der Schritt in ein Wartungsfenster mit Rückweg.

Was ist, wenn die Altdomäne keine Stammdomäne ist?

Gesamtstruktur-Vertrauensstellungen gibt es nur zwischen Stammdomänen. Ist die Domäne des Hauses eine untergeordnete Domäne einer fremden Gesamtstruktur, wird die Vertrauensstellung mit deren Stammdomäne eingerichtet, oder Sie bleiben bei einer externen Vertrauensstellung mit Quarantäne und planen die Ablösung. Übernommene Häuser haben in der Praxis aber meist eine eigene Gesamtstruktur mit nur einer Domäne.

Ist eine Gesamtstruktur-Vertrauensstellung nicht unsicherer, weil sie transitiv ist?

Transitiv heißt hier: innerhalb der beiden Gesamtstrukturen, nicht weiter zu einer dritten. Mit SID-Filterung und selektiver Authentifizierung können Sie genauer steuern, wer sich wo anmeldet, als mit einer externen Vertrauensstellung ohne Einschränkungen. Der Sicherheitsgewinn durch Kerberos statt NTLM kommt hinzu.

Woran erkenne ich, ob auf einer Vertrauensstellung SID-Filterung aktiv ist?

Mit Get-ADTrust (Eigenschaften SIDFilteringQuarantined und SIDFilteringForestAware) oder mit netdom trust und dem Schalter /quarantine bzw. /enablesidhistory auf der vertrauenden Seite. Dokumentieren Sie den Befund je Vertrauensstellung.

Müssen die Häuser für einen gemeinsamen Microsoft-365-Mandanten in die Zentraldomäne?

Nein. Mehrere Gesamtstrukturen lassen sich in einen Entra-Mandanten synchronisieren. Wichtig sind eindeutige Identitäten und UPN-Suffixe. Die Vertrauensstellungen zwischen den Gesamtstrukturen sind dafür keine Voraussetzung, für den Zugriff auf lokale Ressourcen über Standortgrenzen aber weiterhin relevant.

Wie lange dauert die Umstellung je Standort?

Die Vorarbeit mit NTLM-Überwachung braucht Wochen, weil Sie mindestens einen Monatszyklus beobachten sollten. Das eigentliche Wartungsfenster ist überschaubar. Die meiste Zeit kostet die Klärung der Fundstellen mit Herstellern von Fachanwendungen und der Medizintechnik.

Was passiert mit Medizingeräten, die nur NTLM können?

Die bleiben zunächst, wo sie sind, und bekommen eine dokumentierte Ausnahme mit Begründung, Verantwortlichem und Prüftermin. Wichtig ist, dass solche Geräte nicht über die Domänengrenze authentifizieren müssen. Die Abstimmung läuft über die Medizintechnik und den Hersteller, nicht über einen beherzten Gruppenrichtlinien-Klick.

Fazit: Koexistenz ist kein Scheitern, sondern ein Architekturziel

Externe Vertrauensstellungen aus der Fusionsphase sind die Klebestreifen des Klinikverbunds: schnell angebracht, überraschend haltbar und irgendwann vergilbt. Sie bremsen Kerberos aus, weil

ihnen das Namenssuffix-Routing fehlt, und schieben damit Verkehr auf NTLM, das Microsoft absehbar standardmäßig abschaltet. Der Umbau auf Gesamtstruktur-Vertrauensstellungen mit SID-Filterung und selektiver Authentifizierung ist technisch gut beherrschbar, wenn Sie ihn Standort für Standort angehen und mit Netzwerkmitschnitt belegen.

Die große Vollmigration aller Häuser ist dagegen selten das richtige Ziel. Verwaltung, IT und Finanzwesen in die Zentraldomäne, die Häuser in sauber verbundenen eigenen Domänen, ein gemeinsamer Mandant und gemeinsame Sicherheitsstandards: Das ist kein fauler Kompromiss, sondern eine Architektur, die den Krankenhausbetrieb nicht gefährdet. Wenn Sie den Zustand Ihrer Vertrauensstellungen bewerten oder die Umstellung planen wollen, unterstützt Sie die Microsoft-365-Beratung für Krankenhäuser; Ihr Team bringt die Microsoft-365-Schulung für Krankenhäuser auf den Stand für Kerberos und Fehlersuche. Warum all das in der Klinik anders läuft als im Mittelstand, erklärt der Beitrag Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand.

Weiter: Passende Beiträge und Kompetenzbereiche

› Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen

› Kompetenzbereich Kerberos

› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten

› PKI mit ADCS

› Microsoft Entra ID

› NIS2 technisch umsetzen mit Microsoft 365

› Microsoft 365 Security