7.10 Anmeldung an der Domäne funktioniert nicht

7.10.1 Ausgangssituation

Ein Benutzer kann sich an einem Windows-Computer nicht mit seinem Domänenkonto anmelden.

Mögliche Meldungen sind beispielsweise:

> Der Benutzername oder das Kennwort ist falsch.

> Es sind momentan keine Anmeldeserver zum Verarbeiten der Anmeldeanforderung verfügbar.

> Die Vertrauensstellung zwischen dieser Arbeitsstation und der primären Domäne konnte nicht hergestellt werden.

> Wir können Sie mit diesen Anmeldeinformationen nicht anmelden, weil Ihre Domäne nicht verfügbar ist.

> Der Sicherheitsdatenbank auf dem Server ist kein Computerkonto für diese Arbeitsstationsvertrauensstellung zugeordnet.

> Der Benutzerprofildienst konnte die Anmeldung nicht durchführen.

Diese Meldungen beschreiben unterschiedliche Fehlerbereiche. Eine fehlgeschlagene Domänenanmeldung darf deshalb nicht automatisch auf ein falsches Kennwort reduziert werden.

7.10.2 Ziel der Diagnose

Die Diagnose soll eindeutig bestimmen, ob der Fehler verursacht wird durch:

- eine falsche Anmeldeidentität;
- falsche oder veraltete Anmeldeinformationen;
- ein gesperrtes, deaktiviertes oder abgelaufenes Benutzerkonto;
- eine fehlende Netzwerk- oder VPN-Verbindung;
- eine fehlerhafte DNS-Konfiguration;
- eine fehlgeschlagene Domänencontroller-Ermittlung;

- einen nicht erreichbaren Domänencontroller;
- eine zu große Zeitabweichung;
- einen Kerberos- oder NTLM-Fehler;
- einen beschädigten sicheren Kanal des Computers;
- eine fehlerhafte Active-Directory-Replikation;
- eine Anmelde-, Sicherheits- oder Zugriffsrichtlinie;
- eine Smartcard-, Zertifikats- oder Windows-Hello-Abhängigkeit;
- den Benutzerprofildienst, eine Gruppenrichtlinie oder ein Anmeldeskript;
- eine RDP-, NLA- oder Remotedesktop-Besonderheit;
- eine standort-, RODC- oder vertrauensstellungsabhängige Konfiguration.

Erst nach dem Nachweis der Ursache wird eine kontrollierte Maßnahme durchgeführt.

7.10.3 Geltungsbereich und Abgrenzung

Diese Seite behandelt hauptsächlich die Anmeldung eines Domänenbenutzers an einem Computer, der Mitglied einer lokalen Active-Directory-Domäne mit Active Directory Domain Services ist.

Davon zu unterscheiden sind:

Konto- oder Geräteart	Kennzeichnung beziehungsweise Beispiel
lokales Konto	`.\MaxMustermann` oder `<Computername>\MaxMustermann`
Active-Directory-Domänenkonto	`<NETBIOS-Domäne>\MaxMustermann`
Active-Directory-UPN	`max.mustermann@<DNS-Domäne>`
Microsoft-Entra-Konto	häufig ebenfalls UPN-Format, aber cloudbasierte Identität
Microsoft-Konto	persönliche Microsoft-Identität
Smartcard-Anmeldung	zertifikatsbasierte Anmeldung
Windows Hello for Business	schlüssel- oder zertifikatsbasierte Anmeldung
Remotedesktop-Anmeldung	Anmeldung erfolgt am entfernten Zielsystem
Dienst- oder Aufgabenanmeldung	nicht interaktiver Anmeldetyp

Ein Benutzername im Format `benutzer@domäne` beweist allein nicht, ob ein lokales Active Directory, Microsoft Entra ID oder ein anderer Identitätsanbieter verwendet wird.

Microsoft-Entra-Anmeldefehler, MFA und Conditional Access benötigen teilweise andere Diagnoseverfahren. Sie dürfen nicht mit einer klassischen AD-Domänenanmeldung gleichgesetzt werden.

7.10.4 Technischer Anmeldeweg

Eine normale Online-Domänenanmeldung benötigt mehrere funktionierende Ebenen:

1. Der Benutzer wählt den richtigen Anmeldeanbieter.
2. Windows ordnet den eingegebenen Namen dem vorgesehenen Konto zu.
3. Der Computer besitzt eine geeignete Netzwerkverbindung.
4. Der Client verwendet die vorgesehenen DNS-Server.
5. DNS liefert die erforderlichen Domänen- und Dienstinformationen.
6. DC Locator ermittelt einen geeigneten Domänencontroller.
7. Die benötigten Netzwerkprotokolle erreichen den Domänencontroller.
8. Client und Domänencontroller besitzen ausreichend synchronisierte Uhrzeiten.
9. Der Computer besitzt eine gültige Vertrauensbeziehung zur Domäne.
10. Kerberos, NTLM oder das vorgesehene zertifikatsbasierte Verfahren beginnt.
11. Der Domänencontroller prüft das Benutzerkonto und die Anmeldeinformationen.
12. Kontorichtlinien und Anmelderechte werden ausgewertet.
13. Windows erzeugt die Anmeldesitzung und das Zugriffstoken.
14. Benutzerprofil, Gruppenrichtlinien und Anmeldeskripte werden verarbeitet.
15. Der Desktop beziehungsweise die vorgesehene Sitzung wird bereitgestellt.

Der sichtbare Fehler kann an jeder dieser Ebenen entstehen.

7.10.5 Zuerst die genaue Fehlerphase bestimmen

Fehlerphase	Typische Beobachtung	Wahrscheinlicher Bereich
vor Eingabe der Anmeldedaten	Netzwerk- oder Anmeldeoption fehlt	Client, Treiber, VPN oder Anmeldeanbieter
unmittelbar nach Eingabe	Kennwort- oder Kontofehler	Identität, Kennwort, Sperre oder Kontorichtlinie
längere Wartezeit vor Fehlermeldung	kein DC, DNS, Netzwerk oder Timeout	Infrastruktur und Erreichbarkeit
Meldung über Vertrauensstellung	Computerkonto oder sicherer Kanal	Computervertrauen
Anmeldung funktioniert offline, aber nicht online	Cache oder unterschiedlicher DC-Zustand	DNS, DC, Kennwort oder Replikation
Anmeldung wird akzeptiert, Desktop erscheint nicht	Profil, Richtlinie, Skript oder Ressource	Phase nach der Authentifizierung
temporäres Profil wird geladen	Benutzerprofilproblem	Profilpfad, Datenträger oder Profildienst
nur RDP schlägt fehl	RDP, NLA, Anmelderecht oder Zielsystem	entfernter Computer
PIN schlägt fehl, Kennwort funktioniert	Windows Hello oder PIN-Anbieter	Hello-Schlüssel, TPM oder Richtlinie
Smartcard schlägt fehl, Kennwort funktioniert	Zertifikat oder PKI	Smartcard, Zertifikatskette, KDC-Zertifikat oder Sperrprüfung

Eine erfolgreiche Kennwortprüfung bedeutet noch nicht, dass Benutzerprofil, Gruppenrichtlinien und Desktop erfolgreich geladen werden.

7.10.6 Beweise vor Änderungen sichern

Vor einem Neustart, einer Kennwortzurücksetzung, dem Entsperren eines Kontos oder einer Reparatur des sicheren Kanals sollten mindestens folgende Informationen gesichert werden:

- exakter Wortlaut der Fehlermeldung;
- Datum und Uhrzeit des Versuchs;
- betroffener Benutzer;
- betroffener Computer;
- Anmeldeart: lokal, Konsole, RDP, VPN, Smartcard, PIN oder Kennwort;
- eingegebenes Namensformat;
- aktueller Standort und Netzwerkweg;
- Verbindung mit oder ohne VPN;
- letzter erfolgreicher Anmeldezeitpunkt;
- Umfang des Fehlers;
- kürzlich erfolgte Kennwort-, Computer-, DNS-, VPN- oder Richtlinienänderungen;
- verwendeter oder erwarteter Domänencontroller;
- relevante Ereignisse auf Client und Domänencontroller.

Kennwörter, PINs, private Schlüssel, Wiederherstellungsschlüssel und vollständige Anmeldetoken dürfen nicht dokumentiert oder weitergegeben werden.

Wiederholte unkontrollierte Anmeldeversuche müssen vermieden werden, weil dadurch das Konto gesperrt werden kann.

7.10.7 Umfang des Fehlers bestimmen

Geeignete Kreuztests:

Vergleich	Erkenntnis
gleicher Benutzer an anderem Domänencomputer	benutzer- oder computerbezogenen Fehler unterscheiden
anderer Domänenbenutzer am gleichen Computer	Benutzerkonto und Computerzustand unterscheiden
gleiches Konto mit und ohne VPN	VPN-, DNS- oder Routingabhängigkeit erkennen
gleiches Konto an Konsole und per RDP	lokale und entfernte Anmeldung unterscheiden
Kennwort statt PIN	Windows-Hello-Fehler abgrenzen
Kennwort statt Smartcard	Zertifikats- oder Smartcardfehler abgrenzen
lokales Administratorkonto	Zugriff für die Clientdiagnose ermöglichen
Test gegen anderen Standort oder anderen DC	standort- oder DC-bezogenen Fehler erkennen

Auswertung:

Ergebnis	Wahrscheinlicher Bereich

nur ein Benutzer betroffen	Benutzerkonto, Kennwort, Sperre oder Benutzerprofil
alle Benutzer an einem Computer betroffen	Client, DNS, Netzwerk, Zeit oder sicherer Kanal
viele Computer betroffen	DNS, DC, Netzwerk, Zeitdienst, Replikation oder zentrale Richtlinie
nur ein Standort betroffen	Standortnetz, VPN, DNS, Firewall oder Standortzuordnung
nur ein Domänencontroller betroffen	DC-Dienst, DNS-Registrierung, Replikation oder Zeit
nur neue Kennwörter betroffen	Kennwortcache, Replikation oder gespeicherte alte Anmeldedaten
Authentifizierung funktioniert, Desktop nicht	Profil, Gruppenrichtlinie, Skript oder Ressource

Ein Testkonto darf nur nach den organisatorischen Sicherheitsvorgaben verwendet werden.

7.10.8 Richtige Identität und Anmeldeoption prüfen

Am Anmeldebildschirm muss geprüft werden:

- welcher Benutzer angezeigt wird;
- welche Domäne oder welcher Computername unter dem Benutzer steht;
- ob „Anderer Benutzer“ gewählt wurde;
- ob Kennwort, PIN, Smartcard oder ein anderer Anmeldeanbieter aktiv ist;
- ob das richtige Tastaturlayout verwendet wird;
- ob Feststelltaste oder Num-Taste den eingegebenen Wert verändert;
- ob ein alter Benutzername automatisch vorausgefüllt wurde;
- ob ein lokales Konto statt des Domänenkontos gewählt wurde;
- ob ein UPN oder der `DOMÄNE\Benutzer`-Name erforderlich ist.

Beispiele:

```
<NETBIOS-Domäne>\MaxMustermann
```

```
max.mustermann@<DNS-Domäne>
```

```
.\MaxMustermann
```

Bedeutung:

- `<NETBIOS-Domäne>\MaxMustermann` erzwingt die Zuordnung zur angegebenen AD-Domäne.
- `max.mustermann@<DNS-Domäne>` verwendet den Benutzerprinzipalnamen.
- `.\MaxMustermann` bezeichnet ein lokales Konto des Computers.

NETBIOS-Domänenname und DNS-Domänenname müssen nicht identisch sein.

Ein lokaler Anmeldeerfolg beweist weder eine funktionierende Domänenverbindung noch ein gültiges Domänenkonto.

7.10.9 Bestehende Sitzung und Identität prüfen

Wenn noch eine bestehende Sitzung verfügbar ist:

```
whoami
whoami /user
whoami /fqdn
whoami /groups
```

In PowerShell:

```
$env:USERDOMAIN
$env:USERDNSDOMAIN
$env:LOGONSERVER
```

Wichtige Einschränkungen:

- `whoami` beschreibt die bereits bestehende Sitzung.
- `$env:LOGONSERVER` zeigt den Anmeldeserver dieser Sitzung, nicht zwingend den DC, den ein neuer Versuch verwenden würde.
- Eine alte Sitzung kann weiter funktionieren, obwohl eine neue Anmeldung fehlschlägt.
- Eine Anmeldung aus dem lokalen Cache kann ohne aktuelle DC-Authentifizierung entstanden sein.
- Gruppenmitgliedschaften im bestehenden Zugriffstoken können veraltet sein.

7.10.10 Domänenmitgliedschaft des Computers prüfen

Mit einem autorisierten lokalen Konto oder einer noch verfügbaren Administrationssitzung:

```
Get-CimInstance Win32_ComputerSystem |
  Select-Object Name, PartOfDomain, Domain, Workgroup
```

Erwartet wird:

```
PartOfDomain : True
Domain       : <DNS-Domäne>
```

Zusätzlich:

```
systeminfo
```

Relevante Felder sind:

```
Domäne
Anmeldeserver
```

Zu prüfen sind:

- ist der Computer tatsächlich Domänenmitglied?
- gehört er zur erwarteten Domäne?
- wurde er versehentlich in eine Arbeitsgruppe verschoben?
- wurde ein altes Systemabbild oder ein VM-Snapshot wiederhergestellt?
- existiert ein anderer Computer mit demselben Namen?
- wurde das Computerkonto gelöscht, zurückgesetzt oder neu angelegt?
- wurde das Gerät geklont, ohne die Identität ordnungsgemäß vorzubereiten?

`PartOfDomain : True` beweist nur die lokale Mitgliedschaftskonfiguration. Es beweist nicht, dass der sichere Kanal aktuell funktioniert.

7.10.11 Online-Anmeldung und zwischengespeicherte Domänenanmeldung unterscheiden

Windows kann Informationen früherer Domänenanmeldungen lokal zwischenspeichern. Dadurch kann sich ein Benutzer unter bestimmten Voraussetzungen anmelden, obwohl kein Domänencontroller erreichbar ist.

Eine zwischengespeicherte Anmeldung beweist nicht:

- dass ein Domänencontroller erreichbar war;
- dass das Konto aktuell aktiviert ist;
- dass das Konto aktuell nicht gesperrt ist;
- dass das aktuelle Domänenkennwort verwendet wurde;
- dass Kerberos-Tickets ausgestellt wurden;
- dass Netzwerkressourcen erreichbar sind;
- dass Gruppenmitgliedschaften aktuell sind.

Wurde das Kennwort an einem anderen Computer geändert, kann ein offline verwendeter Client weiterhin den früher zwischengespeicherten Kennwortnachweis erwarten. Erst eine erfolgreiche Online-Anmeldung kann den lokalen Anmeldecache aktualisieren.

Die Anzahl zwischengespeicherter eindeutiger Benutzer wird durch die Sicherheitsrichtlinie bestimmt:

```
Computerkonfiguration
└── Windows-Einstellungen
    └── Sicherheitseinstellungen
        └── Lokale Richtlinien
            └── Sicherheitsoptionen
                └── Interaktive Anmeldung:
                    Anzahl zwischenzuspeichernder vorheriger Anmeldungen
```

Der genaue Wert ist eine Sicherheitsentscheidung der Organisation. Er darf nicht nur zur Fehlerumgehung verändert werden.

Typische Unterscheidung:

Verhalten	Einordnung
Anmeldung ohne Netzwerk funktioniert	Cache-Anmeldung möglich
Anmeldung mit Netzwerk schlägt fehl	Online-Authentifizierung oder anderer DC-Zustand fehlerhaft
altes Kennwort funktioniert offline	lokaler Cache kann noch den alten Nachweis enthalten
neues Kennwort funktioniert online	DC kennt das neue Kennwort
neues Kennwort funktioniert an einem Gerät, an anderem nicht	Cache, DC-Auswahl oder Replikation prüfen
noch nie auf diesem Computer angemeldeter Benutzer kann offline nicht anmelden	kein passender lokaler Anmeldecache vorhanden

---

7.10.12 Netzwerkzustand des Clients prüfen

```
Get-NetAdapter |
  Select-Object Name, Status, LinkSpeed, MacAddress
```

```
Get-NetIPConfiguration
```

```
ipconfig /all
```

Zu dokumentieren sind:

- aktive Schnittstelle;
- IPv4- und IPv6-Adresse;
- Präfix beziehungsweise Subnetzmaske;
- Standardgateway;
- DNS-Server;
- DHCP-Status;
- DNS-Suffix;
- VPN-Adapter;
- mehrere gleichzeitig aktive Verbindungen;
- APIPA-Adresse aus `169.254.0.0/16`;
- unerwartete öffentliche oder private DNS-Server.

Ein Ping zum Gateway oder zu einem DC ist nur ein Teilnachweis. Die Domänenanmeldung benötigt DNS, DC Locator und mehrere Anwendungsprotokolle.

Bei einer Anmeldung außerhalb des Unternehmensnetzes ist zu prüfen, ob eine Anmeldung vor dem Windows-Desktop überhaupt eine VPN-Verbindung herstellen kann. Ein VPN, das erst nach der Benutzeranmeldung startet, kann keine erstmalige Online-Domänenanmeldung ermöglichen.

7.10.13 DNS-Konfiguration prüfen

Active Directory ist auf DNS-basierte Diensterkennung angewiesen. Der Client sollte die für die AD-Domäne vorgesehenen DNS-Server verwenden.

DNS-Server anzeigen:

```
Get-DnsClientServerAddress |
  Select-Object InterfaceAlias, AddressFamily, ServerAddresses
```

Domänenname prüfen:

```
Resolve-DnsName -Name <DNS-Domäne> -Type A
```

Domänencontroller-Dienst prüfen:

```
Resolve-DnsName `
  -Name _ldap._tcp.dc._msdcs.<DNS-Domäne> `
```

```
  -Type SRV
```

Kerberos-Dienst prüfen:

```
Resolve-DnsName `
  -Name _kerberos._tcp.<DNS-Domäne> `
  -Type SRV
```

Einen bestimmten DNS-Server verwenden:

```
Resolve-DnsName `
  -Name _ldap._tcp.dc._msdcs.<DNS-Domäne> `
  -Type SRV `
  -Server <DNS-Server>
```

Zu prüfen sind:

- antwortet der vorgesehene interne DNS-Server?
- existieren die benötigten SRV-Einträge?
- verweisen die SRV-Einträge auf vorhandene Domänencontroller?
- lassen sich die zurückgegebenen DC-Namen in gültige Adressen auflösen?
- werden alte oder außer Betrieb genommene DCs geliefert?
- erhält der Client über VPN andere DNS-Server?
- verwendet eine zweite Netzwerkschnittstelle ungeeignete DNS-Server?
- stimmt das DNS-Suffix?
- sind IPv4- und IPv6-Antworten erreichbar?
- unterscheiden sich die Antworten verschiedener DNS-Server?

Öffentliche Resolver kennen die internen Active-Directory-Dienstinformationen normalerweise nicht. Ein zusätzlich eingetragener öffentlicher DNS-Server ist kein zuverlässiger Ersatz für den vorgesehenen AD-DNS-Server.

DNS-Caches sollten nicht sofort gelöscht werden. Zuerst müssen aktuelle Antworten, DNS-Server und die verwendete Zieladresse dokumentiert werden.

7.10.14 Domänencontroller-Ermittlung prüfen

Windows verwendet DC Locator und den Netlogon-Dienst, um über DNS-SRV-Einträge einen geeigneten Domänencontroller zu finden.

```
nltest /dsgetdc:<DNS-Domäne>
```

Erneute DNS-basierte Ermittlung ohne den bisherigen DC-Cache:

```
nltest /dsgetdc:<DNS-Domäne> /force
```

Nur einen beschreibbaren DC anfordern:

```
nltest /dsgetdc:<DNS-Domäne> /writable /force
```

Lokalen AD-Standort anzeigen:

```
nltest /dsgetsite
```

Bekannte Domänencontroller auflisten:

```
nltest /dclist:<DNS-Domäne>
```

In der Ausgabe von `nltest /dsgetdc` sind unter anderem wichtig:

```
DC
Address
Domain Name
Forest Name
Dc Site Name
Our Site Name
Flags
```

Auswertung:

Ergebnis	Bedeutung
geeigneter DC wird gefunden	DC Locator war für diesen Versuch erfolgreich
`ERROR_NO_SUCH_DOMAIN`	Domäne oder DC konnte nicht gefunden werden
falscher Standort	Subnetz- oder Standortzuordnung prüfen
alter DC wird geliefert	DNS-Registrierung und AD-Metadaten prüfen
nur ein entfernter DC wird gefunden	lokaler DC, Standort oder DNS möglicherweise fehlerhaft
DC wird gefunden, Anmeldung scheitert trotzdem	Erreichbarkeit, Zeit, Konto, sicherer Kanal und Protokoll prüfen

Ein erfolgreiches `nltest /dsgetdc` beweist nicht, dass alle für die Anmeldung benötigten Protokolle funktionieren.

7.10.15 Erreichbarkeit der benötigten Dienste prüfen

Grundlegende TCP-Tests:

```
Test-NetConnection -ComputerName <DC-FQDN> -Port 53
Test-NetConnection -ComputerName <DC-FQDN> -Port 88
Test-NetConnection -ComputerName <DC-FQDN> -Port 135
Test-NetConnection -ComputerName <DC-FQDN> -Port 389
Test-NetConnection -ComputerName <DC-FQDN> -Port 445
```

Je nach Funktion zusätzlich:

```
Test-NetConnection -ComputerName <DC-FQDN> -Port 464
Test-NetConnection -ComputerName <DC-FQDN> -Port 3268
Test-NetConnection -ComputerName <DC-FQDN> -Port 636
Test-NetConnection -ComputerName <DC-FQDN> -Port 3269
```

Wichtige AD-Protokolle:

Dienst	Protokoll und Port	Bedeutung
DNS	TCP/UDP 53	Namens- und Dienstauflösung
Kerberos	TCP/UDP 88	Kerberos-Authentifizierung
Windows-Zeit	UDP 123	Zeitsynchronisation
RPC Endpoint Mapper	TCP 135	RPC-Endpunktermittlung
LDAP	TCP 389	Verzeichniszugriff
DC Locator	UDP 389	DC-Ermittlung
SMB	TCP 445	Netlogon, SYSVOL und Gruppenrichtlinien
Kerberos-Kennwortdienst	TCP/UDP 464	Kennwortänderungen
Global Catalog	TCP 3268	gesamtstrukturweite Abfragen
LDAPS	TCP 636	LDAP über TLS, sofern verwendet
Global Catalog über TLS	TCP 3269	GC über TLS, sofern verwendet
dynamische RPC-Ports	üblicherweise TCP 49152–65535 bei modernen Windows-Versionen	ausgehandelte RPC-Verbindungen

Wichtige Einschränkungen:

- `Test-NetConnection` prüft hier nur TCP.
- Ein erfolgreicher Test auf TCP 53 beweist keine funktionierende DNS-Kommunikation über UDP.
- Ein erfolgreicher Test auf TCP 88 beweist keine vollständige Kerberos-Authentifizierung.
- Ein erfolgreicher Test auf TCP 135 beweist nicht, dass der anschließend ausgehandelte dynamische RPC-Port erreichbar ist.
- Nicht jede Umgebung benötigt bei jedem Anmeldevorgang alle aufgeführten optionalen Ports.
- Ein allgemeiner UDP-Porttest liefert keinen eindeutigen Funktionsnachweis.
- Die Freigabe einzelner Ports ohne Kenntnis des vollständigen AD-Verbindungswegs kann unvollständig sein.

Firewalls dürfen nicht pauschal deaktiviert werden. Die konkrete Regel muss anhand von Quelle, Ziel, Protokoll, Port, Richtung und Zeitstempel geprüft werden.

7.10.16 Zeit und Zeitsynchronisation prüfen

Kerberos benötigt ausreichend synchronisierte Uhrzeiten. Die standardmäßige maximale Kerberos-Zeitabweichung beträgt in vielen AD-Umgebungen fünf Minuten, kann aber durch Richtlinien verändert werden.

Clientstatus:

```
w32tm /query /status
w32tm /query /source
w32tm /query /configuration
```

Zeitabweichung zu einem DC beobachten:

```
w32tm /stripchart /computer:<DC-FQDN> /dataonly /samples:5
```

Zusätzlich zu prüfen:

```
Get-Service W32Time
```

Zu vergleichen sind:

- Datum;
- Uhrzeit;
- Zeitzone;

- Zeitquelle;
- letzter erfolgreicher Synchronisierungszeitpunkt;
- Zeitabweichung zum verwendeten DC;
- Zustand des Windows-Zeitdienstes;
- Hypervisor- oder VM-Zeitsynchronisation;
- Zeitquellen der Domänencontroller;
- PDC-Emulator und externe Zeitquelle.

Eine richtige Bildschirmanzeige allein beweist keine korrekte Zeitkonfiguration. Zeitzone, UTC-Zeit, Zeitquelle und tatsächliche Abweichung müssen getrennt betrachtet werden.

Eine Resynchronisation ist eine Änderung und sollte erst nach Dokumentation der bisherigen Quelle und Abweichung erfolgen:

```
w32tm /resync /rediscover
```

Danach müssen Quelle, Status und Abweichung erneut geprüft werden.

7.10.17 Benutzerkonto prüfen

Mit dem ActiveDirectory-PowerShell-Modul und ausreichender Leseberechtigung:

```
Get-ADUser `
  -Identity "<Benutzername>" `
  -Properties Enabled,
              LockedOut,
              PasswordExpired,
              AccountExpirationDate,
              PasswordLastSet,
              LastBadPasswordAttempt,
              BadLogonCount,
              LogonWorkstations |
  Select-Object SamAccountName,
                UserPrincipalName,
                Enabled,
                LockedOut,
                PasswordExpired,
                AccountExpirationDate,
                PasswordLastSet,
                LastBadPasswordAttempt,
                BadLogonCount,
```

```
LogonWorkstations
```

Ergebnisbezogene Kennwortrichtlinie prüfen:

```
Get-ADUserResultantPasswordPolicy `
 -Identity "<Benutzername>"
```

Gezielte Suchbefehle:

```
Search-ADAccount -LockedOut -UsersOnly
Search-ADAccount -AccountDisabled -UsersOnly
Search-ADAccount -AccountExpired -UsersOnly
Search-ADAccount -PasswordExpired -UsersOnly
```

Alternativ mit integrierten Werkzeugen:

```
net user <Benutzername> /domain
```

Zu prüfen sind:

- existiert das Konto?
- wird der richtige UPN verwendet?
- ist das Konto aktiviert?
- ist das Konto gesperrt?
- ist das Konto abgelaufen?
- ist das Kennwort abgelaufen?
- wurde das Kennwort kürzlich geändert oder zurückgesetzt?
- darf sich das Konto nur an bestimmten Arbeitsstationen anmelden?
- gelten eingeschränkte Anmeldezeiten?
- gilt eine fein abgestufte Kennwortrichtlinie?
- besitzt das Konto besondere Authentifizierungsanforderungen?
- stammt der angezeigte Zustand vom gleichen DC, der den Fehler verarbeitet hat?

`BadLogonCount`, `LastBadPasswordAttempt` und ähnliche Werte können DC-abhängig sein. Sie dürfen nicht ohne Berücksichtigung des abgefragten Domänencontrollers und der Replikation interpretiert werden.

Ein Konto sollte nicht vorsorglich entsperrt oder dessen Kennwort zurückgesetzt werden, bevor die Quelle fehlerhafter Anmeldeversuche untersucht wurde. Gespeicherte alte Kennwörter in Diensten, Aufgaben, Mobilgeräten oder Anwendungen können das Konto sofort erneut sperren.

7.10.18 Kennwortfehler systematisch abgrenzen

Mögliche Ursachen trotz scheinbar richtiger Eingabe:

- falscher Benutzer oder falsche Domäne;
- falsches Tastaturlayout;
- Feststelltaste oder Num-Taste;
- Kennwort wurde kürzlich geändert;
- alter zwischengespeicherter Anmeldenachweis;
- Kennwortänderung wurde noch nicht vollständig repliziert;
- gespeicherte alte Anmeldeinformationen;
- Konto wurde gesperrt;
- Kennwort ist abgelaufen;
- Benutzer muss das Kennwort bei der nächsten Anmeldung ändern;
- Kennwortänderungsdienst oder DC ist nicht erreichbar;
- Smartcard- oder Windows-Hello-Anbieter wurde statt Kennwort gewählt.

Ein administratives Zurücksetzen des Kennworts kann Auswirkungen auf verschlüsselte benutzerbezogene Daten, gespeicherte Anmeldeinformationen und Zertifikatsschlüssel besitzen. Es muss nach dem vorgesehenen Identitäts- und Wiederherstellungsverfahren erfolgen.

7.10.19 Sicheren Kanal des Computers prüfen

Domänencomputer und Domäne besitzen eine Vertrauensbeziehung auf Grundlage des Computerkontos und eines Computerkennworts. Stimmen der lokale und der in Active Directory gespeicherte Zustand nicht mehr überein, kann der sichere Kanal fehlschlagen.

Typische Meldung:

```
Die Vertrauensstellung zwischen dieser Arbeitsstation und der primären Domäne konnte nicht hergestellt werden.
```

Nur prüfen:

powershell

```
Test-ComputerSecureChannel -Verbose
```

Erwartetes Ergebnis:

```text
True
```

Ein bestimmter DC kann für den Test angegeben werden:

```
Test-ComputerSecureChannel `
  -Server "<DC-FQDN>" `
  -Verbose
```

Status des zuletzt verwendeten Netlogon-Kanals anzeigen:

```
nltest /sc_query:<DNS-Domäne>
```

Wichtige Einschränkungen:

- `Test-ComputerSecureChannel` ist für Domänenmitgliedscomputer geeignet.
- Auf Domänencontrollern kann das Cmdlet falsch-negative Ergebnisse liefern.
- `nltest /sc_query` meldet den Zustand der letzten Verwendung und ist kein vollständiger neuer Funktionstest.
- `nltest /sc_verify` ist kein rein lesender Test: Wenn der Kanal nicht funktioniert, kann der Befehl den Kanal entfernen und neu aufbauen.
- `nltest /sc_reset`, `nltest /sc_change_pwd`, `Reset-ComputerMachinePassword` und `Test-ComputerSecureChannel -Repair` verändern den Zustand.
- Eine Reparatur darf erst nach Prüfung von DNS, Netzwerk, Zeit, DC-Zustand und Computerkonto erfolgen.

Mögliche Ursachen eines defekten sicheren Kanals:

- Wiederherstellung eines alten VM-Snapshots;
- Zurückspielen eines veralteten Systemabbilds;
- doppelter Computername;
- gelöschtes oder zurückgesetztes Computerkonto;
- Neuinstallation mit wiederverwendetem Computernamen;
- nicht ordnungsgemäß geklonter Rechner;
- nicht übereinstimmendes Computerkennwort;
- AD-Replikationsfehler;
- längere Netzwerk- oder DC-Probleme;
- fehlerhafte Automatisierung bei der Gerätebereitstellung.

Ein defekter sicherer Kanal ist ein konkreter Befund. Der Computer sollte nicht vorsorglich aus der Domäne entfernt werden.

7.10.20 Kerberos und NTLM unterscheiden

Windows verwendet häufig das Aushandlungspaket `Negotiate`. Dieses wählt nach Möglichkeit Kerberos und kann unter bestimmten Bedingungen NTLM verwenden.

Kerberos benötigt unter anderem:

- funktionierende DNS-Auflösung;
- erreichbaren KDC auf dem Domänencontroller;
- ausreichend synchronisierte Zeit;
- ein gültiges Benutzerkonto;
- passende kryptografische Schlüssel;
- bei Dienstzugriffen einen korrekten Service Principal Name;
- bei Smartcard-Anmeldung geeignete Zertifikate und Vertrauensketten.

NTLM benötigt ebenfalls einen erreichbaren zuständigen Authentifizierungsserver und darf nicht als automatische oder dauerhafte Lösung für Kerberos-Probleme betrachtet werden.

Ein erfolgreicher NTLM-Versuch beweist nicht, dass Kerberos funktioniert. Ein Fehlschlag bei Kerberos darf nicht ungeprüft durch Lockerung der Sicherheitsrichtlinien oder dauerhafte Aktivierung veralteter Verfahren umgangen werden.

7.10.21 Kerberos-Tickets prüfen

In einer bestehenden Domänensitzung:

```
klist
```

TGT anzeigen:

```
klist tgt
```

Alle Tickets der aktuellen Sitzung anzeigen:

```
klist tickets
```

Zu prüfen sind:

- ist ein Ticket Granting Ticket vorhanden?
- für welche Kerberos-Realm wurde es ausgestellt?
- welcher KDC hat das Ticket ausgestellt?
- sind Start- und Ablaufzeit plausibel?
- sind Diensttickets für die erwarteten Dienste vorhanden?
- wird statt Kerberos möglicherweise NTLM verwendet?
- stimmt der Servername mit dem erwarteten Dienstnamen überein?

`klist purge` löscht Kerberos-Tickets der angegebenen Anmeldesitzung und ist daher keine rein lesende Diagnose:

```
klist purge
```

Mögliche Auswirkungen:

- bestehende Zugriffe müssen neu authentifiziert werden;
- Netzlaufwerke oder Anwendungen können vorübergehend Verbindungen verlieren;
- die eigentliche Ursache kann durch das Löschen alter Nachweise verdeckt werden;
- der Befehl betrifft nur die ausgewählte Anmeldesitzung.

Tickets sollten deshalb zuerst dokumentiert und nur im Rahmen eines kontrollierten Tests gelöscht werden.

Eine fehlgeschlagene interaktive Anmeldung besitzt möglicherweise noch keine normale Benutzersitzung, in der `klist` ausgeführt werden kann. In diesem Fall sind die Ereignisse auf dem Domänencontroller besonders wichtig.

7.10.22 Relevante Ereignisprotokolle

Ereignisse müssen anhand des gleichen Benutzer-, Computer- und Fehlerzeitpunkts korreliert werden.

Auf dem betroffenen Client:

- **Windows-Protokolle → System**
- **Windows-Protokolle → Sicherheit**
- **Anwendungs- und Dienstprotokolle → Microsoft → Windows → GroupPolicy → Operational**
- **Anwendungs- und Dienstprotokolle → Microsoft → Windows → User Profile Service → Operational**
- Netlogon-, DNS-Client-, LSA-, Kerberos-, W32Time- und Gruppenrichtlinienereignisse

Auf dem beteiligten Domänencontroller:

- **Windows-Protokolle → Sicherheit**
- **Windows-Protokolle → System**
- **Verzeichnisdienst**
- **DNS-Server**
- **DFS-Replikation**
- Kerberos-, Netlogon-, KDC-, LSA- und Replikationsereignisse

Beispiel für Clientereignisse der letzten zwei Stunden:

```
Get-WinEvent -FilterHashtable @{
  LogName   = 'System'
```

```
  StartTime = (Get-Date).AddHours(-2)
} |
  Where-Object {
    $_.ProviderName -match 'NETLOGON|W32Time|DNS|Lsa'
  } |
  Select-Object TimeCreated, ProviderName, Id, LevelDisplayName, Message
```

Fehlgeschlagene Anmeldungen auf einem System:

```
Get-WinEvent -FilterHashtable @{
  LogName   = 'Security'
  Id        = 4625
  StartTime = (Get-Date).AddHours(-2)
} |
  Select-Object TimeCreated, Id, Message
```

Relevante Ereignisse:

Ereignis-ID	Typische Bedeutung	Typischer Ort
`4624`	erfolgreiche Anmeldung	System, auf dem die Anmeldung erfolgte
`4625`	fehlgeschlagene Anmeldung	System, auf dem die Anmeldung versucht wurde
`4740`	Benutzerkonto wurde gesperrt	zuständiges System beziehungsweise DC
`4767`	Benutzerkonto wurde entsperrt	Domänencontroller
`4768`	Kerberos-TGT wurde angefordert	Domänencontroller
`4769`	Kerberos-Dienstticket wurde angefordert	Domänencontroller
`4771`	Kerberos-Vorauthentifizierung fehlgeschlagen	Domänencontroller
`4776`	NTLM-Anmeldeinformationen wurden geprüft	für Domänenkonten auf dem zuständigen DC
`3210`	Netlogon konnte Computer nicht beim DC authentifizieren	Mitgliedscomputer
`5719`	kein Domänencontroller für sichere Sitzung verfügbar	Mitgliedscomputer
`1053` oder `1055`	Gruppenrichtlinienverarbeitung mit Domänen- oder DC-Problem	Mitgliedscomputer

Die Ereignisse erscheinen nur, wenn die entsprechenden Überwachungsrichtlinien und Protokollkanäle aktiviert sind. Das Fehlen eines Ereignisses beweist deshalb nicht, dass kein Versuch stattgefunden hat.

7.10.23 Ereignis 4625 auswerten

Bei Ereignis `4625` sind besonders wichtig:

```
Account Name
Account Domain
Failure Reason
Status
Sub Status
Logon Type
Logon Process
Authentication Package
Workstation Name
Source Network Address
Caller Process Name
```

Wichtige Anmeldetypen:

Logon Type	Bedeutung
2	interaktive lokale Anmeldung
3	Netzwerkanmeldung
4	Batch beziehungsweise geplante Aufgabe
5	Dienstanmeldung
7	Entsperren
10	Remotedesktop beziehungsweise RemoteInteractive
11	zwischengespeicherte interaktive Anmeldung

Häufige Status- oder Substatuswerte:

Code	Bedeutung	Nächster Nachweis
0xC000005E	keine Anmeldeserver verfügbar	DNS, DC Locator, Netzwerk und DC-Zustand prüfen
0xC0000064	Benutzerkonto nicht gefunden	Benutzername, Domäne und Kontobestand prüfen

Code	Bedeutung	Nächster Nachweis
`0xC000006A`	falsches Kennwort	Eingabe, Kennwortänderung und gespeicherte Kennwörter prüfen
`0xC000006D`	allgemeiner Fehler bei Benutzername oder Authentifizierungsdaten	Status, Substatus und Authentifizierungspaket korrelieren
`0xC000006F`	Anmeldung außerhalb erlaubter Zeiten	Anmeldezeiten prüfen
`0xC0000070`	Anmeldung von nicht erlaubter Arbeitsstation	Arbeitsstationsbeschränkung prüfen
`0xC0000071`	Kennwort abgelaufen	Kennwortstatus und Änderungsweg prüfen
`0xC0000072`	Konto deaktiviert	Kontostatus und Änderungshistorie prüfen
`0xC000015B`	erforderlicher Anmeldetyp nicht gewährt	Benutzerrechte und Richtlinien prüfen
`0xC0000192`	Netlogon-Dienst ist nicht gestartet	Dienstzustand und Systemereignisse prüfen
`0xC0000193`	Konto abgelaufen	Ablaufdatum des Kontos prüfen
`0xC0000234`	Konto gesperrt	Ereignis 4740 und Quelle der Fehlversuche untersuchen
`0xC0000413`	Authentifizierungsfirewall verhindert Anmeldung	Authentifizierungsrichtlinie und zulässige Systeme prüfen

Status und Substatus müssen gemeinsam ausgewertet werden. Der sichtbare Meldungstext am Anmeldebildschirm kann absichtlich weniger genau sein als das Sicherheitsereignis.

7.10.24 Kerberos-Ereignisse auswerten

Ereignis `4768` zeigt die Anforderung eines Kerberos-TGT. Ereignis `4771` zeigt eine fehlgeschlagene Kerberos-Vorauthentifizierung.

Häufige Kerberos-Fehlercodes:

Code	Kerberos-Bezeichnung	Einordnung
`0x6`	`KDC_ERR_C_PRINCIPAL_UNKNOWN`	Benutzerprinzipal nicht in Kerberos-Datenbank gefunden
`0x7`	`KDC_ERR_S_PRINCIPAL_UNKNOWN`	angeforderter Dienstprinzipal nicht gefunden
`0x8`	`KDC_ERR_PRINCIPAL_NOT_UNIQUE`	Prinzipal nicht eindeutig
`0xC`	`KDC_ERR_POLICY`	KDC-Richtlinie lehnt Anfrage ab

Code	Kerberos-Bezeichnung	Einordnung
`0xE`	`KDC_ERR_ETYPE_NOSUPP`	keine gemeinsame unterstützte Verschlüsselungsart
`0x10`	`KDC_ERR_PADATA_TYPE_NOSUPP`	Vorauthentifizierungstyp nicht unterstützt; bei Smartcard auch Zertifikatsproblem möglich
`0x12`	`KDC_ERR_CLIENT_REVOKED`	Anmeldeinformationen des Clients wurden widerrufen
`0x17`	`KDC_ERR_KEY_EXPIRED`	Kennwort abgelaufen
`0x18`	`KDC_ERR_PREAUTH_FAILED`	Vorauthentifizierung ungültig; häufig falsches Kennwort
`0x19`	`KDC_ERR_PREAUTH_REQUIRED`	zusätzliche Vorauthentifizierung erforderlich; nicht automatisch ein Fehler
`0x1D`	`KDC_ERR_SVC_UNAVAILABLE`	Kerberos-Dienst nicht verfügbar
`0x20`	`KRB_AP_ERR_TKT_EXPIRED`	Ticket abgelaufen
`0x25`	`KRB_AP_ERR_SKEW`	Zeitabweichung zu groß
`0x34`	`KRB_ERR_RESPONSE_TOO_BIG`	Antwort zu groß für UDP; erneuter Versuch über TCP erforderlich

Ein einzelner Kerberos-Fehlercode muss mit Benutzer, Clientadresse, DC, Zeitstempel und nachfolgendem Erfolg oder Fehlschlag korreliert werden.

Der Code `0x19` kann Teil eines normalen Kerberos-Ablaufs sein und darf nicht allein als Störung gewertet werden.

7.10.25 Kontosperren bis zur Quelle verfolgen

Bei einer Sperre muss nicht nur das Konto entsperrt, sondern die Quelle der wiederholten falschen Kennwörter bestimmt werden.

Zu untersuchen sind:

- Ereignis `4740`;
- aufrufender Computer;
- Ereignisse `4771` bei Kerberos;
- Ereignisse `4776` bei NTLM;
- Ereignisse `4625` auf Quell- und Zielsystemen;
- gespeicherte Windows-Anmeldeinformationen;
- verbundene Netzlaufwerke;
- geplante Aufgaben;
- Windows-Dienste;
- Anwendungen mit gespeichertem Kennwort;

- Mobilgeräte und Mailprogramme;
- VPN-Clients;
- alte RDP-Sitzungen;
- Skripte;
- weitere Computer des Benutzers.

Eine Kontosperre kann durch einen Hintergrundprozess entstehen, obwohl der Benutzer sein aktuelles Kennwort am Anmeldebildschirm richtig eingibt.

7.10.26 Active-Directory-Replikation prüfen

Wenn Anmeldungen abhängig vom verwendeten Domänencontroller unterschiedlich reagieren, müssen Replikation und DC-Zustand geprüft werden.

Auf einem autorisierten Administrationssystem oder Domänencontroller:

```
repadmin /replsummary
```

```
repadmin /showrepl
```

Gesamtstrukturweite Übersicht:

```
repadmin /showrepl * /csv
```

Grundlegender DC-Test:

```
dcdiag /v
```

DNS-Test für einen bestimmten DC:

```
dcdiag /test:DNS /v /s:<DC-Name>
```

Zu prüfen sind:

- letzte erfolgreiche Replikation;
- Anzahl und Dauer der Fehler;
- betroffene Verzeichnispartition;
- Quell- und Ziel-DC;
- DNS-Fehler;
- RPC-Fehler;

- Zugriffs- oder Vertrauensfehler;
- Zeitabweichung;
- Replikation von Benutzer- und Computerkontoänderungen;
- Erreichbarkeit des PDC-Emulators;
- SYSVOL- und DFSR-Zustand.

Mögliche Symptome eines Replikationsfehlers:

- neues Kennwort funktioniert nur über bestimmte DCs;
- Konto erscheint auf einem DC gesperrt und auf einem anderen nicht;
- neues Benutzer- oder Computerkonto ist nicht überall vorhanden;
- reparierter sicherer Kanal schlägt über einen anderen DC erneut fehl;
- Gruppenmitgliedschaften unterscheiden sich;
- Anmeldung funktioniert standortabhängig.

Eine erzwungene Replikation ist keine erste Diagnosemaßnahme. Zuerst müssen Richtung, Fehlercode, Ursache und Replikationspartner bestimmt werden.

7.10.27 Standort, VPN und RODC berücksichtigen

AD-Standorte beeinflussen die Auswahl eines Domänencontrollers.

Clientstandort anzeigen:

```
nltest /dsgetsite
```

Zu prüfen sind:

- ist das Clientsubnetz in Active Directory Sites and Services eingetragen?
- ist es dem richtigen Standort zugeordnet?
- besitzt dieser Standort einen erreichbaren DC?
- antwortet ein entfernter DC schneller als der lokale DC?
- verteilt das VPN das richtige AD-Subnetz und die richtigen DNS-Server?
- sind die notwendigen Netze über den Tunnel erreichbar?
- existieren unterschiedliche Regeln vor und nach der Benutzeranmeldung?
- verwendet der Standort einen Read-Only Domain Controller?
- darf der RODC die Anmeldeinformationen dieses Benutzers zwischenspeichern?
- ist ein beschreibbarer DC erreichbar, wenn Kennwortänderung oder Kontosperrenbehandlung erforderlich ist?

Ein RODC kann nur solche Anmeldungen lokal verarbeiten, für die die erforderlichen Anmeldeinformationen entsprechend der Kennwortreplikationsrichtlinie verfügbar sind oder ein beschreibbarer DC erreicht werden kann.

7.10.28 RDP- und NLA-Anmeldungen abgrenzen

Bei Remotedesktop erfolgt die Anmeldung am entfernten Computer. Entscheidend sind daher DNS, Netzwerk, Zeit, Domänenverbindung, sicherer Kanal und Anmelderechte des Zielsystems.

Zu prüfen sind:

- wird der richtige Zielcomputer angesprochen?
- verwendet der RDP-Client gespeicherte alte Anmeldeinformationen?
- ist das richtige Namensformat angegeben?
- ist Network Level Authentication aktiv?
- kann das Zielsystem einen DC erreichen?
- ist der sichere Kanal des Zielsystems gültig?
- besitzt der Benutzer das Recht zur Anmeldung über Remotedesktopdienste?
- wird dieses Recht durch eine Verweigerungsrichtlinie überschrieben?
- ist der Benutzer Mitglied der vorgesehenen lokalen oder domänenweiten Gruppe?
- existiert bereits eine eingeschränkte oder getrennte Sitzung?
- liegt Ereignis `4625` mit Logon Type `10` vor?

Ein erfolgreicher Domänenlogin am lokalen Notebook beweist nicht, dass der entfernte Server die Domäne erreichen oder den Benutzer anmelden kann.

NLA sollte nicht dauerhaft deaktiviert werden, nur um einen Authentifizierungsfehler zu umgehen.

7.10.29 Smartcard und Windows Hello for Business abgrenzen

Wenn Kennwortanmeldung funktioniert, aber Smartcard oder Windows Hello fehlschlägt, ist die normale Kennwortprüfung wahrscheinlich nicht die Hauptursache.

Bei Smartcard-Anmeldung zu prüfen:

- Smartcard und Lesegerät;
- Benutzerzertifikat;
- Gültigkeitszeitraum;
- UPN beziehungsweise Identitätszuordnung;
- Zertifikatskette;
- Sperrstatus und Erreichbarkeit der CRL- oder OCSP-Dienste;
- KDC-Zertifikat des Domänencontrollers;
- geeignete Zertifikatvorlage;
- unterstützte Kryptografie;
- Zeit;
- Ereignis `4771` und PKINIT-Fehlercodes.

Bei Windows Hello for Business zu prüfen:

- wurde PIN oder Kennwort gewählt?

- ist das Gerät ordnungsgemäß registriert?
- ist der Hello-Schlüssel vorhanden?
- ist das TPM verfügbar?
- stimmt der Vertrauensmodus der Organisation?
- wurden Richtlinien oder Zertifikate verändert?
- ist eine Onlineverbindung für den jeweiligen Vorgang erforderlich?

Eine PIN ist nicht das Domänenkennwort. Ein PIN-Fehler beweist deshalb nicht, dass das AD-Kennwort falsch ist.

7.10.30 Authentifizierung, Sitzung und Benutzerprofil unterscheiden

Nach erfolgreicher Authentifizierung können weitere Fehler auftreten:

- Benutzerprofildienst kann das Profil nicht laden;
- Profilpfad ist nicht erreichbar;
- servergespeichertes Profil ist beschädigt;
- lokaler Profildatenträger ist voll;
- Berechtigungen des Profilordners sind fehlerhaft;
- Gruppenrichtlinienverarbeitung hängt;
- Anmeldeskript wartet auf eine nicht erreichbare Ressource;
- Ordnerumleitung schlägt fehl;
- Netzlaufwerk oder Druckerzuordnung hat ein Timeout;
- Sicherheitssoftware blockiert den Sitzungsaufbau;
- Windows lädt ein temporäres Profil.

Typische Unterscheidung:

Beobachtung	Einordnung
Ereignis 4624 vorhanden, danach Profilfehler	Authentifizierung war wahrscheinlich erfolgreich
Desktop erscheint nach langer Wartezeit	Gruppenrichtlinie, Skript oder Ressource prüfen
temporäres Profil	Benutzerprofil und Datenträger prüfen
nur ein Benutzerprofil betroffen	lokales oder servergespeichertes Profil möglich
Anmeldung anderer Benutzer funktioniert	allgemeine DC-Erreichbarkeit wahrscheinlich vorhanden
Anmeldung im abgesicherten Diagnosekontext funktioniert	nachgelagerte Erweiterung, Richtlinie oder Dienst möglich

Gruppenrichtlinienstatus in einer bestehenden Sitzung:

```
gpresult /r
```

Computerrichtlinien:

```
gpresult /r /scope computer
```

Benutzerrichtlinien:

```
gpresult /r /scope user
```

`gpupdate /force` ist keine reine Diagnose. Der Befehl kann neue Richtlinien anwenden und den Ausgangszustand verändern.

7.10.31 Systematischer Diagnoseablauf

1. **Fehlermeldung aufnehmen**
   Exakten Wortlaut, Benutzer, Computer, Uhrzeit und Anmeldeart dokumentieren.
2. **Anmeldephase bestimmen**
   Identität, Authentifizierung, Sitzung oder Profil unterscheiden.
3. **Umfang bestimmen**
   Einen Benutzer, einen Computer, einen Standort oder die gesamte Domäne unterscheiden.
4. **Anmeldeanbieter kontrollieren**
   Kennwort, PIN, Smartcard, lokales Konto und Domänenkonto unterscheiden.
5. **Namensformat prüfen**
   UPN und `DOMÄNE\Benutzer` kontrolliert vergleichen.
6. **Domänenmitgliedschaft prüfen**
   Lokale Mitgliedschaft und erwartete Domäne bestätigen.
7. **Online- und Cache-Anmeldung unterscheiden**
   Feststellen, ob ein DC tatsächlich beteiligt war.
8. **Netzwerkzustand prüfen**
   Schnittstelle, Adresse, Gateway, VPN und DNS-Server dokumentieren.
9. **DNS-SRV-Einträge prüfen**
   LDAP- und Kerberos-Diensteinträge auflösen.
10. **Domänencontroller ermitteln**
    `nltest /dsgetdc` und Standortinformationen auswerten.
11. **DC-Erreichbarkeit prüfen**
    DNS, Kerberos, LDAP, SMB, RPC und benötigte Zusatzdienste untersuchen.
12. **Zeit prüfen**
    Zeitquelle, Status und Abweichung zum DC bestimmen.
13. **Benutzerkonto prüfen**
    Existenz, UPN, Aktivierung, Sperre, Ablauf und Kennwortstatus auswerten.
14. **Sicheren Kanal prüfen**
    Ausschließlich mit lesenden Tests beginnen.
15. **Authentifizierungsverfahren bestimmen**
    Kerberos, NTLM, Smartcard oder Windows Hello unterscheiden.

16. **Ereignisse korrelieren**
    Client- und DC-Ereignisse auf denselben Versuch begrenzen.
17. **Fehlercode auswerten**
    Status, Substatus, Kerberos-Code und Anmeldetyp bestimmen.
18. **Replikation prüfen**
    Besonders bei DC- oder Standortabhängigkeit.
19. **Nachgelagerte Anmeldung prüfen**
    Profil, Gruppenrichtlinie, Skript und Ressourcen untersuchen.
20. **Hypothese formulieren**
    Erwarteten Befund und möglichen Gegenbeweis festlegen.
21. **Eine kontrollierte Maßnahme durchführen**
    Risiko, Berechtigung, Rückweg und Erfolgskriterium dokumentieren.
22. **Online-Domänenanmeldung verifizieren**
    Nicht nur Cache- oder lokale Anmeldung testen.
23. **Vollständige Benutzerfunktion prüfen**
    Desktop, Gruppenrichtlinien und benötigte Ressourcen kontrollieren.
24. **Nachkontrolle durchführen**
    Ereignisse, Replikation und weitere Benutzer beziehungsweise Systeme prüfen.

7.10.32 Befundmatrix

Befund	Mögliche Erklärung	Nächster Nachweis
lokales Konto funktioniert, Domänenkonto nicht	Domänenweg oder Domänenkonto fehlerhaft	DNS, DC Locator, Konto und sicheren Kanal prüfen
anderer Benutzer funktioniert am gleichen Computer	benutzerbezogener Fehler	Kontostatus, Kennwort und Profil prüfen
gleicher Benutzer funktioniert an anderem Computer	clientbezogener Fehler	DNS, Zeit, sicherer Kanal und Profil prüfen
Anmeldung funktioniert nur offline	Cache-Anmeldung	Onlineweg zum DC prüfen
altes Kennwort funktioniert offline	alter lokaler Anmeldecache	Onlineanmeldung mit aktuellem Kennwort prüfen
`nltest /dsgetdc` findet keinen DC	DNS, Netzwerk oder Netlogon	SRV-Einträge, DNS-Server und Dienst prüfen
DC wird gefunden, Ports schlagen fehl	Firewall, Routing oder DC-Dienst	Regeln und beidseitige Protokolle prüfen
Ereignis `0xC000005E`	keine Anmeldeserver verfügbar	DNS, DC Locator und Netzwerk prüfen
Ereignis `0xC0000064`	Benutzer nicht gefunden	Identität und Kontobestand prüfen
Ereignis `0xC000006A`	falsches Kennwort	Kennwort, Cache und gespeicherte Daten prüfen
Ereignis `0xC0000234`	Konto gesperrt	Ereignis 4740 und Sperrquelle prüfen
Kerberos `0x18`	Vorauthentifizierung fehlgeschlagen	Kennwort und zugehörigen Versuch prüfen

Befund	Mögliche Erklärung	Nächster Nachweis
Kerberos `0x25`	Zeitabweichung zu groß	Zeitquelle und Abweichung prüfen
sicherer Kanal liefert `False`	Computervertrauen fehlerhaft	DNS, Zeit, Computerkonto und Replikation prüfen
Vertrauensfehler nur bei einem Computer	Computerkennwort oder Computerkonto	sicheren Kanal kontrolliert reparieren
Anmeldung funktioniert abhängig vom DC	Replikations- oder DC-Fehler	DC-Ereignisse und `repadmin` auswerten
Kennwort funktioniert, PIN nicht	Windows-Hello-Problem	Hello-, TPM- und Richtlinienzustand prüfen
Kennwort funktioniert, Smartcard nicht	PKI- oder Zertifikatsproblem	Zertifikate, KDC und Sperrprüfung untersuchen
Ereignis 4624 vorhanden, Desktop fehlt	Authentifizierung erfolgreich, Folgephase fehlerhaft	Profil, GPO und Skripte prüfen
nur RDP schlägt fehl	RDP-Recht, NLA oder Zielsystem	Logon Type 10 und Zielsystem prüfen
Konto wird sofort erneut gesperrt	gespeichertes altes Kennwort	Quellcomputer und Hintergrundprozesse ermitteln

---

7.10.33 Ursachen und erforderliche Nachweise

Mögliche Ursache	Erforderlicher Nachweis
falsches Namensformat	Anmeldung richtet sich nachweislich an falsche Domäne oder lokales Konto
falsches Kennwort	Ereigniscode und kontrollierter Identitätsabgleich bestätigen die Ursache
Konto gesperrt	AD-Kontostatus und Ereignis gesper `4740` bestätigen die Sperre
Konto deaktiviert	`Enabled : False` oder entsprechendes Änderungsereignis
Konto abgelaufen	Ablaufdatum liegt in der Vergangenheit
Kennwort abgelaufen	`PasswordExpired` oder Kerberos-Code `0x17`
falscher DNS-Server	Client verwendet nicht den vorgesehenen AD-DNS-Server
fehlender SRV-Eintrag	autorisierte DNS-Abfrage liefert den benötigten Eintrag nicht
falscher DC-Eintrag	SRV- oder A/AAAA-Eintrag verweist auf falschen oder alten DC
DC nicht erreichbar	protokollspezifischer Test und Netzwerkprotokoll bestätigen Unterbrechung
falscher AD-Standort	`nltest /dsgetsite` und Subnetzkonfiguration stimmen nicht überein

Mögliche Ursache	Erforderlicher Nachweis
VPN vor Anmeldung fehlt	Onlineweg zum DC ist am Anmeldebildschirm nicht vorhanden
Zeitabweichung	`w32tm` oder Kerberos-Code `0x25` bestätigt die Abweichung
defekter sicherer Kanal	`Test-ComputerSecureChannel` meldet reproduzierbar `False`
Computerkonto fehlt	AD-Abfrage bestätigt fehlendes oder falsches Computerkonto
doppelter Computername	zwei Systeme verwenden nachweislich dieselbe Computeridentität
AD-Replikationsfehler	`repadmin` oder DC-Protokolle zeigen fehlgeschlagene Replikation
Kerberos-Verschlüsselungsproblem	Kerberos-Code und Kontokonfiguration bestätigen fehlende gemeinsame Verschlüsselungsart
Smartcard-Zertifikatsproblem	Zertifikatsprüfung oder PKINIT-Ereignis bestätigt Ursache
fehlendes Anmelderecht	Ereignis `0xC000015B` und wirksame Richtlinie stimmen überein
Profilfehler	erfolgreiche Authentifizierung und Profildienstereignis liegen nacheinander vor
Gruppenrichtlinienfehler	GroupPolicy-Protokoll zeigt konkrete fehlgeschlagene Richtlinienverarbeitung
gespeichertes altes Kennwort	Ereignisse zeigen wiederholte Fehlversuche von bestimmtem Gerät oder Prozess

---

7.10.34 Kontrollierte Maßnahmen, Risiko und Rückweg

Maßnahme	Risiko	Rückweg beziehungsweise Kontrolle
richtigen Benutzer oder richtige Domäne auswählen	gering	ursprüngliche Eingabe dokumentieren
Tastaturlayout korrigieren	Fehleingabe bleibt möglich	kontrollierte Testeingabe ohne Kennwortprotokollierung
Netzwerk oder Voranmelde-VPN wiederherstellen	anderer Netzwerkweg wird aktiv	vorherigen Netzwerkzustand dokumentieren
DNS-Konfiguration korrigieren	andere Namensauflösung kann beeinflusst werden	bisherige DNS-Werte sichern
falschen SRV- oder Hosteintrag korrigieren	viele Clients können betroffen sein	bisherigen Wert und TTL dokumentieren
Windows-Zeit kontrolliert synchronisieren	Zeitsprung kann Dienste beeinflussen	alte Quelle und Abweichung sichern

Maßnahme	Risiko	Rückweg beziehungsweise Kontrolle
Konto nach Ursachenprüfung entsperren	erneute sofortige Sperre möglich	Sperrquelle vorher ermitteln
Kennwort nach Identitätsprüfung zurücksetzen	gespeicherte Daten oder Schlüssel können betroffen sein	vorgesehenes Identitätsverfahren verwenden
sicheren Kanal reparieren	Computervertrauen wird verändert	verwendeten DC und Ausgangsbefund dokumentieren
Computerkennwort zurücksetzen	Vertrauensbeziehung kann bei Fehler weiter ausfallen	lokale Administrationsmöglichkeit sicherstellen
Computer neu in Domäne aufnehmen	Neustarts, Profilzuordnung und Verwaltungszustand können betroffen sein	nur als letzte Maßnahme mit Wiederaufnahmeplan
AD-Replikationsfehler beheben	domänenweite Auswirkungen möglich	DC-spezifischen Änderungsplan verwenden
GPO korrigieren	viele Benutzer oder Computer betroffen	Version, Sicherung und Zielbereich dokumentieren
beschädigtes Profil reparieren	Benutzerdaten können verloren gehen	Profil und Daten nach Vorgabe sichern
gespeicherte alte Anmeldeinformation aktualisieren	Anwendung oder Dienst kann ausfallen	betroffene Abhängigkeit vorher bestimmen

Pro Diagnoseversuch sollte möglichst nur eine relevante Variable verändert werden.

7.10.35 Sicheren Kanal kontrolliert reparieren

Eine Reparatur ist nur gerechtfertigt, wenn:

- die Domänenmitgliedschaft bestätigt ist;
- DNS korrekt funktioniert;
- ein geeigneter DC erreichbar ist;
- die Zeit ausreichend synchronisiert ist;
- das Computerkonto vorhanden ist;
- Replikationsprobleme berücksichtigt wurden;
- ein autorisiertes lokales Administratorkonto verfügbar ist;
- Risiko und Rückweg dokumentiert wurden.

Reparatur mit PowerShell:

```
$Credential = Get-Credential "<NETBIOS-Domäne>\<Administrationskonto>"

Test-ComputerSecureChannel `
  -Repair `
```

```
  -Server "<DC-FQDN>" `
  -Credential $Credential `
  -Verbose
```

Alternativ kann das lokale Computerkennwort kontrolliert zurückgesetzt werden:

```
$Credential = Get-Credential "<NETBIOS-Domäne>\<Administrationskonto>"

Reset-ComputerMachinePassword `
  -Server "<DC-FQDN>" `
  -Credential $Credential
```

Danach:

```
Test-ComputerSecureChannel `
  -Server "<DC-FQDN>" `
  -Verbose
```

Anschließend sind je nach Verfahren ein Neustart und eine erneute Online-Domänenanmeldung erforderlich.

Wichtig:

- Zugangsdaten dürfen nicht direkt in Klartext in einen Befehl geschrieben werden.
- `nltest /sc_verify`, `nltest /sc_reset` und `nltest /sc_change_pwd` können den Vertrauenszustand verändern.
- Auf Domänencontrollern gelten andere Reparaturverfahren.
- Das Entfernen und erneute Hinzufügen zur Domäne ist eine letzte Maßnahme.
- Eine Domänenneuanmeldung ohne Ursachenanalyse kann das Symptom nur vorübergehend beseitigen.
- Bei wiederkehrenden Vertrauensfehlern müssen Snapshot-Verfahren, Klonprozesse, doppelte Computernamen, Replikation und Computerkennwortänderungen untersucht werden.

7.10.36 Verifikation

Nach einer Maßnahme müssen mindestens folgende Punkte geprüft werden:

- Computer ist weiterhin Mitglied der richtigen Domäne;
- Client verwendet die vorgesehenen DNS-Server;
- LDAP- und Kerberos-SRV-Einträge werden korrekt aufgelöst;
- DC Locator findet einen geeigneten Domänencontroller;

- Client ist dem richtigen AD-Standort zugeordnet;
- erforderliche AD-Dienste sind erreichbar;
- Zeitquelle und Zeitabweichung sind plausibel;
- sicherer Kanal liefert ein erfolgreiches Ergebnis;
- Benutzerkonto ist aktiviert und nicht gesperrt;
- Anmeldung verwendet den richtigen Benutzer und die richtige Domäne;
- Anmeldung erfolgt online gegen einen Domänencontroller;
- ein Kerberos-TGT kann ausgestellt werden, sofern Kerberos vorgesehen ist;
- keine neuen Fehler `4625`, `4771`, `4776`, `3210` oder `5719` entstehen;
- Benutzerprofil wird vollständig geladen;
- Gruppenrichtlinien werden verarbeitet;
- Anmeldeskripte werden abgeschlossen;
- benötigte Netzressourcen funktionieren;
- RDP funktioniert, wenn es zum ursprünglichen Fehler gehörte;
- mehrere repräsentative Benutzer oder Clients funktionieren, wenn der Fehler größeren Umfang hatte;
- temporäre Diagnoseänderungen wurden zurückgenommen;
- Sicherheitsfunktionen wie NLA, Firewall und Zertifikatsprüfung bleiben aktiv;
- Ursache, Maßnahme und Prävention wurden dokumentiert.

Eine erfolgreiche lokale oder zwischengespeicherte Anmeldung ist keine ausreichende Verifikation einer reparierten Domänenanmeldung.

7.10.37 Präventionsmaßnahmen

- redundante und überwachte Domänencontroller bereitstellen;
- DNS-Dienste und AD-SRV-Einträge überwachen;
- Clients ausschließlich mit vorgesehenen AD-DNS-Servern konfigurieren;
- AD-Standorte und Subnetze vollständig dokumentieren;
- VPN mit geeigneter DNS- und Routingkonfiguration bereitstellen;
- bei Bedarf einen sicheren Voranmelde-VPN-Weg vorsehen;
- Windows-Zeithierarchie überwachen;
- PDC-Emulator und externe Zeitquelle dokumentieren;
- AD-Replikation kontinuierlich überwachen;
- Domänencontrollerereignisse zentral sammeln;
- Kontosperren mit Quellcomputer auswerten;
- Kennwortänderungen und gespeicherte Anmeldeinformationen berücksichtigen;
- Computerobjekte nicht unkontrolliert löschen oder zurücksetzen;
- VM-Snapshot- und Wiederherstellungsverfahren mit AD-Vertrauensbeziehungen abstimmen;
- Computer nur über standardisierte Verfahren klonen;
- doppelte Computernamen verhindern;
- sicheren Kanal überwachen, ohne automatische unkontrollierte Reparaturen auszuführen;
- lokale Notfalladministration nach Sicherheitsvorgabe gewährleisten;
- Gruppenrichtlinien vor breiter Verteilung testen;

- Profil-, SYSVOL- und DFSR-Zustand überwachen;
- Zertifikatsablauf und Sperrprüfungsdienste bei Smartcard-Anmeldung überwachen;
- Windows-Hello-Bereitstellung und Vertrauensmodell dokumentieren;
- Sicherheitsprotokolle ausreichend groß dimensionieren;
- Uhrzeiten aller Systeme zentral korrelierbar halten;
- Runbooks für DNS-, DC-, Replikations- und Vertrauensfehler testen.

7.10.38 Typische Fehler bei der Diagnose

- Die Meldung sofort als falsches Kennwort interpretieren.
- Lokales Konto und Domänenkonto verwechseln.
- UPN, DNS-Domäne und NETBIOS-Domäne gleichsetzen.
- PIN und Domänenkennwort gleichsetzen.
- Eine Cache-Anmeldung als erfolgreiche Online-Domänenanmeldung werten.
- Nur den Domänennamen anpingen.
- Einen erfolgreichen Ping als Nachweis der AD-Anmeldung betrachten.
- Öffentliche DNS-Server auf einem Domänenclient eintragen.
- DNS-Caches löschen, bevor die falsche Antwort dokumentiert wurde.
- Nur TCP 389 prüfen und die übrigen AD-Abhängigkeiten ignorieren.
- Einen erfolgreichen Test auf TCP 135 als vollständigen RPC-Nachweis betrachten.
- UDP mit einem allgemeinen Porttest als sicher funktionsfähig einstufen.
- Zeit nur optisch ablesen und die tatsächliche Abweichung nicht messen.
- Ein Konto wiederholt testen und dadurch sperren.
- Ein gesperrtes Konto entsperren, ohne die Sperrquelle zu ermitteln.
- Das Kennwort vorsorglich zurücksetzen.
- Gespeicherte alte Kennwörter in Diensten oder Aufgaben ignorieren.
- `nltest /sc_verify` als rein lesenden Test verwenden.
- Den sicheren Kanal reparieren, bevor DNS und Netzwerk funktionieren.
- `Test-ComputerSecureChannel` auf einem DC wie auf einem Mitgliedscomputer interpretieren.
- Den Computer sofort aus der Domäne entfernen.
- AD-Replikation durch eine erzwungene Synchronisation „reparieren“, ohne den Fehler auszuwerten.
- Nur einen Domänencontroller untersuchen.
- Den verwendeten DC und Standort nicht dokumentieren.
- Ereignis `4625` ohne Status, Substatus und Logon Type interpretieren.
- Kerberos-Code `0x19` automatisch als Störung einstufen.
- Kerberos-Tickets löschen, bevor sie dokumentiert wurden.
- RDP-Fehler nur auf dem lokalen Client untersuchen.
- NLA, Firewall oder Zertifikatsprüfung dauerhaft deaktivieren.
- Profilfehler mit fehlgeschlagener Kennwortprüfung verwechseln.
- Vor der Protokollsicherung neu starten.
- Kennwörter oder vollständige Sicherheitsprotokolle ungeschützt weitergeben.
- Nach der Maßnahme nur eine lokale oder zwischengespeicherte Anmeldung testen.

7.10.39 Typische Prüfungsfragen

Warum kann eine Domänenanmeldung trotz richtiger Anmeldedaten fehlschlagen?

Die Anmeldung benötigt neben gültigen Anmeldedaten unter anderem Netzwerk, DNS, einen erreichbaren Domänencontroller, ausreichende Zeitsynchronisation, ein gültiges Benutzerkonto und eine funktionierende Computervertrauensstellung.

Warum ist DNS für eine Active-Directory-Anmeldung erforderlich?

Der Client ermittelt Domänencontroller und Kerberos-Dienste über DNS-SRV-Einträge. Eine einfache Auflösung des Domänennamens reicht dafür nicht aus.

Was bedeutet die Meldung, dass keine Anmeldeserver verfügbar sind?

Der Client konnte keinen geeigneten Domänencontroller für die Anmeldeanforderung verwenden. Danach müssen DNS, DC Locator, Netzwerk, benötigte Dienste und der Zustand der Domänencontroller geprüft werden.

Was ist eine zwischengespeicherte Domänenanmeldung?

Windows verwendet lokal gespeicherte Informationen einer früheren erfolgreichen Domänenanmeldung, wenn kein Domänencontroller erreichbar ist. Dabei findet keine vollständige aktuelle Onlineprüfung des Domänenkontos statt.

Was beweist eine erfolgreiche Cache-Anmeldung nicht?

Sie beweist weder die Erreichbarkeit eines Domänencontrollers noch den aktuellen Konto-, Kennwort-, Gruppen- oder Sperrstatus.

Warum kann nach einer Kennwortänderung offline noch das alte Kennwort funktionieren?

Der lokale Computer kann noch den Nachweis der früheren erfolgreichen Domänenanmeldung gespeichert haben. Der Cache wird erst durch eine geeignete erfolgreiche Online-Anmeldung aktualisiert.

Welche Bedeutung besitzt die Uhrzeit bei Kerberos?

Kerberos verwendet Zeitstempel zum Schutz gegen Wiederholungsangriffe. Eine zu große Zeitabweichung zwischen Client und Domänencontroller kann die Authentifizierung verhindern.

Was bedeutet ein Kerberos-Fehler `0x18`?

Die Kerberos-Vorauthentifizierungsinformationen waren ungültig. Häufig wurde ein falsches Kennwort verwendet. Der konkrete Versuch muss mit Benutzer, Client und Zeitpunkt korreliert werden.

Was bedeutet Ereignis `4625`?

Auf dem protokollierenden System ist eine Anmeldung fehlgeschlagen. Status, Substatus, Anmeldetyp, Konto, Quelladresse und Authentifizierungspaket müssen gemeinsam ausgewertet werden.

Was bedeutet Ereignis `4740`?

Ein Benutzerkonto wurde gesperrt. Das Ereignis sollte verwendet werden, um Zeitpunkt und auslösenden Computer beziehungsweise Anmeldeweg zu bestimmen.

Was ist der sichere Kanal eines Domänencomputers?

Es ist die durch das Computerkonto und sein Kennwort abgesicherte Vertrauensbeziehung zwischen Domänenmitglied und Domäne.

Wie wird der sichere Kanal zunächst geprüft?

Auf einem Mitgliedscomputer mit:

```
Test-ComputerSecureChannel -Verbose
```

Der Test sollte zuerst ohne `-Repair` ausgeführt werden.

Warum ist `nltest /sc_verify` kein rein lesender Test?

Wenn der sichere Kanal nicht funktioniert, kann der Befehl den bestehenden Kanal entfernen und neu aufbauen.

Warum sollte ein Computer nicht sofort aus der Domäne entfernt werden?

DNS-, Netzwerk-, Zeit- oder Replikationsfehler können die eigentliche Ursache sein. Eine erneute Domänenaufnahme verändert den Systemzustand, benötigt Neustarts und kann weitere Verwaltungs- oder Profilprobleme verursachen.

Warum kann die Anmeldung über einen DC funktionieren und über einen anderen fehlschlagen?

Benutzer-, Kennwort- oder Computerkontoänderungen können wegen eines Replikationsfehlers nicht auf allen Domänencontrollern den gleichen Stand besitzen.

Warum kann die Kennwortanmeldung funktionieren, während die PIN fehlschlägt?

Die Windows-Hello-PIN verwendet einen gerätegebundenen Schlüssel und ist nicht identisch mit dem Domänenkennwort.

Warum kann Ereignis `4624` vorhanden sein, obwohl der Benutzer keinen Desktop erhält?

Die Authentifizierung und Sitzungserstellung können erfolgreich gewesen sein, während Benutzerprofil, Gruppenrichtlinie, Anmeldeskript oder eine benötigte Ressource anschließend fehlschlagen.

7.10.40 Checkliste

- [ ] exakte Fehlermeldung dokumentiert
- [ ] Benutzer, Computer und Fehlerzeitpunkt erfasst
- [ ] lokale, RDP-, VPN-, Smartcard-, PIN- oder Kennwortanmeldung bestimmt
- [ ] Fehlerphase bestimmt
- [ ] Umfang des Fehlers bestimmt
- [ ] richtiger Anmeldeanbieter gewählt
- [ ] lokales Konto und Domänenkonto unterschieden
- [ ] UPN und `DOMÄNE\Benutzer` geprüft
- [ ] Tastaturlayout kontrolliert
- [ ] Domänenmitgliedschaft bestätigt
- [ ] Online- und Cache-Anmeldung unterschieden
- [ ] aktive Netzwerkschnittstelle geprüft
- [ ] IP-Adresse, Gateway und VPN geprüft
- [ ] verwendete DNS-Server dokumentiert
- [ ] LDAP-SRV-Eintrag geprüft
- [ ] Kerberos-SRV-Eintrag geprüft
- [ ] zurückgegebene DC-Namen aufgelöst
- [ ] DC Locator ausgeführt
- [ ] AD-Standort geprüft
- [ ] geeigneter beschreibbarer DC bei Bedarf ermittelt
- [ ] DNS-Funktion gegen vorgesehenen Server geprüft
- [ ] Kerberos-Erreichbarkeit geprüft
- [ ] LDAP-Erreichbarkeit geprüft
- [ ] SMB-Erreichbarkeit geprüft
- [ ] RPC und dynamische Ports berücksichtigt
- [ ] UDP-Dienste nicht nur durch allgemeinen Porttest bewertet
- [ ] Windows-Zeitstatus geprüft

- [ ] Zeitquelle geprüft
- [ ] Abweichung zum DC gemessen
- [ ] Benutzerkonto gefunden
- [ ] UPN kontrolliert
- [ ] Kontoaktivierung geprüft
- [ ] Kontosperre geprüft
- [ ] Kontoablauf geprüft
- [ ] Kennwortablauf geprüft
- [ ] Anmeldezeiten und Arbeitsstationsbeschränkungen berücksichtigt
- [ ] Sperrquelle vor Entsperrung untersucht
- [ ] Computerkonto geprüft
- [ ] sicheren Kanal zunächst nur lesend geprüft
- [ ] Kerberos und NTLM unterschieden
- [ ] Kerberos-Tickets vor Änderungen dokumentiert
- [ ] Clientereignisse ausgewertet
- [ ] DC-Ereignisse ausgewertet
- [ ] Ereignis `4625` mit Status und Substatus geprüft
- [ ] Logon Type ausgewertet
- [ ] Kerberos-Ereignisse geprüft
- [ ] Ereignis `4740` bei Sperre geprüft
- [ ] AD-Replikation bei DC-Abhängigkeit geprüft
- [ ] RODC und Kennwortreplikationsrichtlinie berücksichtigt
- [ ] RDP und NLA bei Remoteanmeldung berücksichtigt
- [ ] Smartcard oder Windows Hello abgegrenzt
- [ ] Profil, Gruppenrichtlinie und Anmeldeskript geprüft
- [ ] Hypothese und Gegenbeweis formuliert
- [ ] Risiko und Rückweg dokumentiert
- [ ] nur eine kontrollierte Maßnahme durchgeführt
- [ ] Online-Domänenanmeldung verifiziert
- [ ] vollständiges Benutzerprofil geladen
- [ ] benötigte Netzwerkressourcen geprüft
- [ ] keine neuen relevanten Ereignisfehler vorhanden
- [ ] temporäre Diagnoseänderungen zurückgenommen
- [ ] Ursache und Präventionsmaßnahme dokumentiert

7.10.41 Schnellreferenz

Aufgabe	Befehl
aktuelle Identität	`whoami`
Benutzer-SID	`whoami /user`
vollständige Domänenidentität	`whoami /fqdn`
Gruppen der Sitzung	`whoami /groups`
Domänenmitgliedschaft	`Get-CimInstance Win32_ComputerSystem`
Netzwerkkonfiguration	`ipconfig /all`
DNS-Server	`Get-DnsClientServerAddress`
LDAP-SRV-Eintrag	`Resolve-DnsName _ldap._tcp.dc._msdcs.<Domäne> -Type SRV`
Kerberos-SRV-Eintrag	`Resolve-DnsName _kerberos._tcp.<Domäne> -Type SRV`
DC ermitteln	`nltest /dsgetdc:<Domäne>`
DC neu ermitteln	`nltest /dsgetdc:<Domäne> /force`
AD-Standort	`nltest /dsgetsite`
DC-Liste	`nltest /dclist:<Domäne>`
DNS-TCP-Test	`Test-NetConnection <DC> -Port 53`
Kerberos-TCP-Test	`Test-NetConnection <DC> -Port 88`
LDAP-TCP-Test	`Test-NetConnection <DC> -Port 389`
SMB-TCP-Test	`Test-NetConnection <DC> -Port 445`
RPC Endpoint Mapper	`Test-NetConnection <DC> -Port 135`
Zeitstatus	`w32tm /query /status`
Zeitquelle	`w32tm /query /source`
Zeitvergleich	`w32tm /stripchart /computer:<DC> /dataonly /samples:5`
Benutzerkonto	`Get-ADUser <Benutzer> -Properties *`
gesperrte Konten	`Search-ADAccount -LockedOut -UsersOnly`
sicherer Kanal, nur Test	`Test-ComputerSecureChannel -Verbose`
letzter Netlogon-Kanalstatus	`nltest /sc_query:<Domäne>`
Kerberos-Tickets	`klist tickets`
Kerberos-TGT	`klist tgt`
Anmeldefehler	`Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625}`
DC-Gesundheit	`dcdiag /v`
DC-DNS-Test	`dcdiag /test:DNS /v`

Aufgabe	Befehl
Replikationsübersicht	`repadmin /replsummary`
Replikationsdetails	`repadmin /showrepl`
Gruppenrichtlinienergebnis	`gpresult /r`

Ändernde Befehle, die nicht als erste Diagnose verwendet werden dürfen:

```
Test-ComputerSecureChannel -Repair
Reset-ComputerMachinePassword
nltest /sc_verify
nltest /sc_reset
nltest /sc_change_pwd
klist purge
w32tm /resync
gpupdate /force
```

7.10.42 Quellen

Offizielle Microsoft-Dokumentation

- Microsoft Learn – Locating Active Directory domain controllers in Windows and Windows Server
- Microsoft Learn – Troubleshoot domain controller location issues
- Microsoft Learn – Service overview and network port requirements for Windows
- Microsoft Learn – Configure a firewall for Active Directory domains and trusts
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Nltest
- Microsoft Learn – Test-ComputerSecureChannel
- Microsoft Learn – Reset-ComputerMachinePassword
- Microsoft Learn – Broken trust relationship between a domain-joined device and its domain
- Microsoft Learn – Data collection for troubleshooting secure channel issues
- Microsoft Learn – Secure Channel Problems Detected
- Microsoft Learn – How the Windows Time Service works
- Microsoft Learn – Maximum tolerance for computer clock synchronization

- Microsoft Learn – Interactive logon: Number of previous logons to cache
- Microsoft Learn – Cached and Stored Credentials Technical Overview
- Microsoft Learn – Klist
- Microsoft Learn – Kerberos authentication troubleshooting guidance
- Microsoft Learn – Get-ADUser
- Microsoft Learn – Search-ADAccount
- Microsoft Learn – Get-WinEvent
- Microsoft Learn – Ereignis 4625: An account failed to log on
- Microsoft Learn – Ereignis 4740: A user account was locked out
- Microsoft Learn – Ereignis 4768: A Kerberos authentication ticket was requested
- Microsoft Learn – Ereignis 4769: A Kerberos service ticket was requested
- Microsoft Learn – Ereignis 4771: Kerberos pre-authentication failed
- Microsoft Learn – Ereignis 4776: The computer attempted to validate the credentials for an account
- Microsoft Learn – Dcdiag
- Microsoft Learn – Diagnose Active Directory replication failures
- Microsoft Learn – Verify DNS functionality to support directory replication
- Microsoft Learn – Advanced audit policy configuration settings

Standards

- RFC 4120 – The Kerberos Network Authentication Service
- RFC 2782 – A DNS RR for specifying the location of services

Für diese Seite wurden keine Community-Berichte, Hersteller-Social-Media-Aussagen oder eigenen Laborergebnisse als Nachweis verwendet.
