6.7 Anmeldung an der Domäne geht nicht

Wenn sich ein Benutzer nicht an einer Active-Directory-Domäne anmelden kann, liegt die Ursache nicht automatisch an einem falschen Kennwort.

Eine Domänenanmeldung benötigt mehrere funktionierende Komponenten:

1. der Client besitzt eine gültige Netzwerkkonfiguration,
2. der Client verwendet die vorgesehenen internen DNS-Server,
3. die Active-Directory-Domäne kann über DNS gefunden werden,
4. ein geeigneter Domain Controller ist erreichbar,
5. Client und Domain Controller besitzen ausreichend übereinstimmende Systemzeiten,
6. das Benutzerkonto ist vorhanden und verwendbar,
7. das Computerkonto und der sichere Kanal zur Domäne funktionieren,
8. Kerberos oder gegebenenfalls NTLM kann die Anmeldung verarbeiten,
9. Gruppenrichtlinien und Benutzerprofile verhindern die Anmeldung nicht,
10. die Domain Controller replizieren die benötigten Informationen ordnungsgemäß.

Die sichtbare Meldung am Client beschreibt häufig nur das Ergebnis. Die eigentliche Ursache kann bei DNS, Uhrzeit, Netzwerk, Benutzerkonto, Computerkonto, Domain Controller, Replikation oder Richtlinien liegen.

---

1. Typische Fehlermeldungen

Mögliche Meldungen sind:

> Der Benutzername oder das Kennwort ist falsch.

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

> Die Sicherheitsdatenbank auf dem Server enthält kein Computerkonto für diese Arbeitsstationsvertrauensstellung.

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

> Die angegebene Domäne ist nicht vorhanden, oder es konnte keine Verbindung hergestellt werden.

Das referenzierte Konto ist momentan gesperrt und kann nicht für die Anmeldung verwendet werden.

Die Anmeldung ist aufgrund einer Kontoeinschränkung nicht möglich.

Die Anmeldemethode, die Sie verwenden möchten, ist nicht zulässig.

Ihr Konto wurde deaktiviert. Wenden Sie sich an den Systemadministrator.

Das Kennwort des Benutzers muss vor der Anmeldung geändert werden.

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

Der genaue deutsche Wortlaut kann sich je nach Windows-Version unterscheiden. Deshalb sollten zusätzlich Fehlercode, Ereignis-ID, Uhrzeit und die englische Originalmeldung dokumentiert werden, wenn sie in einem Protokoll vorhanden ist.

---

2. Auswirkungen

Mögliche Auswirkungen:

- ein einzelner Benutzer kann sich nicht anmelden,
- alle Benutzer eines Clients sind betroffen,
- mehrere Clients eines Standorts sind betroffen,
- neue Benutzer können sich nicht anmelden,
- bisher angemeldete Benutzer können sich nur mit zwischengespeicherten Anmeldedaten anmelden,
- Gruppenrichtlinien werden nicht verarbeitet,
- Netzlaufwerke und Drucker werden nicht verbunden,
- Kerberos-Authentifizierung funktioniert nicht,
- Dienste mit Domänenkonten starten nicht,
- ein Computer verliert seine Vertrauensstellung,
- Kennwortänderungen werden nicht überall erkannt,
- Anmeldungen funktionieren abhängig vom erreichten Domain Controller,
- Remoteanmeldungen funktionieren, lokale Konsolenanmeldungen jedoch nicht oder umgekehrt.

---

3. Sicherheits- und Betriebswarnung

Bei der Untersuchung dürfen Benutzerkonten, Computerkonten, Domain Controller und Vertrauensstellungen nicht unkontrolliert verändert werden.

Insbesondere sollten nicht vorschnell:

- Benutzerkennwörter zurückgesetzt,
- Konten entsperrt, ohne die Sperrquelle zu untersuchen,
- Computerkonten gelöscht,
- Clients aus der Domäne entfernt,
- Domain Controller neu gestartet,
- DNS-Einträge manuell gelöscht,
- Kerberos-Tickets produktiver Sitzungen entfernt,
- Gruppenrichtlinien deaktiviert,
- Sicherheitsrichtlinien abgeschwächt,
- Replikationen erzwungen,
- Zeiteinstellungen manuell verändert,
- lokale Administratorzugänge neu angelegt,
- Protokolle gelöscht werden.

Das Entfernen eines Computers aus der Domäne und das anschließende erneute Hinzufügen ist keine Ursachenanalyse. Dadurch können Beweise verloren gehen und zusätzliche Probleme mit Profilen, Zertifikaten, Gruppenrichtlinien, BitLocker, Softwareverteilung oder Verwaltungsdiensten entstehen.

Korrekturmaßnahmen sind nur mit entsprechender Berechtigung und nach Sicherung der Diagnosedaten durchzuführen.

---

4. Zuerst den Umfang bestimmen

Die wichtigste erste Frage lautet:

> „ Ist nur ein Benutzer, nur ein Client oder ein größerer Teil der Domäne betroffen?

Beobachtung	zuerst zu untersuchender Bereich
ein Benutzer kann sich an keinem Client anmelden	Benutzerkonto, Kennwort, Sperre, Ablauf, Anmelderechte
ein Benutzer kann sich nur an einem Client nicht anmelden	Client, lokales Profil, Anmeldeformat, Richtlinie, gespeicherte Daten
kein Domänenbenutzer kann sich an einem Client anmelden	DNS, Netzwerk, Uhrzeit, sicherer Kanal, Computerkonto
mehrere Clients eines Standorts sind betroffen	DNS, DHCP, VLAN, Standort-Uplink, Firewall, erreichbarer Domain Controller

Beobachtung	zuerst zu untersuchender Bereich
alle Benutzer der Domäne sind betroffen	Domain Controller, DNS, Replikation, Zeitdienst, zentrale Infrastruktur
Anmeldung funktioniert offline, aber nicht im Firmennetz	erreichter Domain Controller, Kontostatus, Kennwort, DNS oder sicherer Kanal
Anmeldung funktioniert im Firmennetz, aber nicht über VPN	VPN-Verbindungszeitpunkt, DNS, Routing, Firewall, Gerätezertifikat
alte Anmeldedaten funktionieren offline	zwischengespeicherte Domänenanmeldung
neues Kennwort funktioniert nur an manchen Clients	Replikation, erreichter Domain Controller, gespeicherte Anmeldedaten
lokale Anmeldung funktioniert, Domänenanmeldung nicht	Domänenpfad, Benutzerkonto, DNS, Domain Controller oder Vertrauensstellung
Anmeldung funktioniert mit einem anderen Domänenbenutzer	Benutzerkonto oder benutzerspezifische Richtlinie priorisieren
Anmeldung funktioniert nach Neustart gelegentlich wieder	Netzwerkstart, DNS, Dienstreihenfolge, sicherer Kanal oder erreichter DC

Ein einzelner erfolgreicher Anmeldeversuch mit einem anderen Benutzer beweist nicht, dass die gesamte Domäneninfrastruktur fehlerfrei ist. Der andere Benutzer könnte zwischengespeicherte Anmeldedaten verwenden oder einen anderen Authentifizierungspfad besitzen.

---

5. Mindestinformationen erfassen

Vor einer Änderung sollten mindestens dokumentiert werden:

```
Ticket:
Datum und genaue Uhrzeit:
Zeitzone:
Benutzerkonto:
Clientname:
Client-IP:
Standort:
Verbindung: Ethernet / WLAN / VPN
Domäne:
verwendetes Anmeldeformat:
genauer Meldungstext:
Fehlercode:
Anmeldung lokal oder remote:
erstmalige oder wiederkehrende Anmeldung:
anderer Benutzer am selben Client getestet:
```

```
derselbe Benutzer an anderem Client getestet:
lokale Anmeldung möglich:
Netzwerk vor der Anmeldung verfügbar:
zuletzt erfolgreiche Anmeldung:
kürzlich geändertes Kennwort:
zuletzt installierte Updates oder Änderungen:
```

Kennwörter dürfen nicht in das Ticket oder Diagnoseprotokoll geschrieben werden.

---

6. Lokales Konto und Domänenkonto unterscheiden

Die Eingabe auf dem Anmeldebildschirm kann unterschiedliche Kontotypen ansprechen.

Domänenkonto als UPN

```
benutzer@ad.example.test
```

Domänenkonto im älteren Format

```
EXAMPLE\benutzer
```

Lokales Konto

```
.\benutzer
```

oder:

```
CLIENT01\benutzer
```

`.\benutzer` bezeichnet ein lokales Konto des aktuellen Computers. Es ist keine Domänenanmeldung.

Eine Anmeldung kann fehlschlagen, weil:

- versehentlich das lokale Konto ausgewählt wurde,
- eine falsche Domäne vorangestellt wurde,
- der UPN-Suffix nicht zum Benutzerkonto passt,
- ein gleichnamiges lokales Konto existiert,
- der zuletzt verwendete Anmeldekontext übernommen wurde,
- die Tastaturbelegung auf dem Anmeldebildschirm abweicht.

Vor tieferer Diagnose sollte deshalb feststehen, welches Konto Windows tatsächlich authentifizieren soll.

---

7. Gesicherte Anmeldung und zwischengespeicherte Anmeldedaten

Windows kann erfolgreiche Domänenanmeldungen zwischenspeichern. Dadurch kann sich ein Benutzer möglicherweise an einem Notebook anmelden, obwohl momentan kein Domain Controller erreichbar ist.

Das bedeutet:

```
Anmeldung erfolgreich
≠
Domain Controller war erreichbar
```

Bei einer zwischengespeicherten Anmeldung können anschließend trotzdem ausfallen:

- Gruppenrichtlinien,
- Netzlaufwerke,
- Domänendrucker,
- Kerberos-Tickets,
- Zugriff auf interne Anwendungen,
- Kennwortänderungen,
- Anmeldung mit einem erstmals verwendeten Konto.

Typische Hinweise auf eine zwischengespeicherte Anmeldung:

- Anmeldung funktioniert ohne Netzwerk,
- ein bereits bekannter Benutzer kann sich anmelden,
- ein neuer Benutzer kann sich am selben Gerät nicht anmelden,
- das neue Kennwort funktioniert nicht, das vorherige jedoch schon,
- Domänenressourcen sind nach der Anmeldung nicht erreichbar,
- Gruppenrichtlinien werden nicht aktualisiert.

Die Anzahl zwischengespeicherter Anmeldungen wird durch Sicherheitsrichtlinien bestimmt. Diese Einstellung sollte nicht allein zur Fehlerbehebung verändert werden.

---

8. Netzwerkstatus vor der Anmeldung berücksichtigen

Eine Domänenanmeldung kann erfolgen, bevor WLAN, VPN oder 802.1X vollständig verfügbar ist.

Zu prüfen sind:

- ist das Netzwerkkabel angeschlossen,

- ist der Switchport aktiv,
- ist WLAN bereits am Anmeldebildschirm verbunden,
- benötigt das WLAN zuerst eine Benutzeranmeldung,
- verwendet der Client Maschinen- oder Benutzerzertifikate,
- ist ein Pre-Logon-VPN erforderlich,
- startet das VPN erst nach der Windows-Anmeldung,
- erhält der Client rechtzeitig eine DHCP-Adresse,
- wird ein falsches VLAN zugewiesen,
- blockiert Network Access Control den Client,
- benötigt der Netzwerkadapter nach dem Start ungewöhnlich lange,
- wird durch Fast Startup ein fehlerhafter Netzwerkzustand übernommen.

Nach der Anmeldung kann der aktuelle Zustand geprüft werden:

```
Get-NetAdapter
```

```
Get-NetIPConfiguration
```

```
ipconfig /all
```

Wichtige Angaben:

- IPv4-Adresse,
- IPv6-Adresse,
- Subnetzmaske oder Präfix,
- Standardgateway,
- DHCP-Server,
- DNS-Server,
- DNS-Suffix,
- Lease-Zeitpunkt,
- Adapterstatus,
- Name der Verbindung.

Eine Adresse aus `169.254.0.0/16` weist bei IPv4 typischerweise darauf hin, dass keine reguläre DHCP-Konfiguration bezogen wurde. Sie beweist jedoch noch nicht, ob DHCP-Server, Relay, VLAN, Port oder Client die Ursache ist.

---

9. Erreichbarkeit schrittweise prüfen

Nach einer lokalen oder zwischengespeicherten Anmeldung kann der Netzwerkpfad untersucht werden.

Eigene Netzwerkkonfiguration

```
ipconfig /all
```

Standardgateway

```
Test-Connection -TargetName <gateway> -Count 4
```

Interner DNS-Server

```
Test-Connection -TargetName <dns-server> -Count 4
```

Domain Controller

```
Test-Connection -TargetName <dc-fqdn> -Count 4
```

Relevante TCP-Verbindungen

```
Test-NetConnection -ComputerName <dc-fqdn> -Port 53
Test-NetConnection -ComputerName <dc-fqdn> -Port 88
Test-NetConnection -ComputerName <dc-fqdn> -Port 389
Test-NetConnection -ComputerName <dc-fqdn> -Port 445
```

Ein erfolgreicher Ping beweist nicht, dass DNS, Kerberos, LDAP, SMB, RPC oder die Anmeldung funktioniert. Umgekehrt kann Ping durch eine Firewall blockiert sein, obwohl die benötigten Dienste erreichbar sind.

Active Directory verwendet mehrere Protokolle und dynamische RPC-Ports. Vier erfolgreiche Porttests ersetzen deshalb keine vollständige Prüfung des Domänenpfades.

---

10. DNS-Konfiguration des Clients prüfen

Active Directory ist in hohem Maß von DNS abhängig. Ein Domänenclient muss die DNS-Server verwenden, welche die Active-Directory-DNS-Zone und die zugehörigen Dienstressourceneinträge auflösen können.

Prüfen:

```
Get-DnsClientServerAddress
```

```
Get-DnsClientGlobalSetting
```

```
Get-DnsClient
```

Alternativ:

```
ipconfig /all
```

Verdächtig sind insbesondere:

- ausschließlich ein öffentlicher DNS-Server,
- DNS-Server des Internetrouters statt des vorgesehenen AD-DNS,
- falsche DNS-Server durch statische Konfiguration,
- falsche DNS-Server durch VPN oder DHCP,
- unerwarteter DNS-Suffix,
- veraltete DNS-Adressen,
- nicht erreichbarer bevorzugter DNS-Server,
- Split-DNS mit fehlenden internen Einträgen,
- unterschiedliche Antworten verschiedener DNS-Server.

Öffentliche Resolver können Internetnamen auflösen, kennen aber normalerweise nicht die internen SRV-Einträge der Active-Directory-Domäne.

Eine funktionierende Auflösung von `www.example.com` beweist daher nicht, dass Active Directory über DNS gefunden werden kann.

---

11. DNS-Auflösung der Domäne prüfen

Domänenname auflösen

```
Resolve-DnsName -Name <ad-domain>
```

Domain-Controller-Dienst suchen

```
Resolve-DnsName `
  -Name "_ldap._tcp.dc._msdcs.<ad-domain>" `
  -Type SRV
```

Kerberos-Dienst suchen

```
Resolve-DnsName `
  -Name "_kerberos._tcp.<ad-domain>" `
  -Type SRV
```

Global Catalog suchen

```
Resolve-DnsName `
  -Name "_ldap._tcp.gc._msdcs.<forest-root-domain>" `
  -Type SRV
```

Mit `nslookup`:

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.<ad-domain>
```

```
nslookup -type=SRV _kerberos._tcp.<ad-domain>
```

Erwartet werden SRV-Antworten mit geeigneten Domain Controllern. Anschließend müssen auch deren Hostnamen auflösbar sein:

```
Resolve-DnsName -Name <dc-fqdn>
```

Eine vorhandene SRV-Antwort reicht nicht aus, wenn:

- der zurückgegebene Domain Controller nicht erreichbar ist,
- sein Hostname auf eine falsche IP-Adresse zeigt,
- ein veralteter Domain Controller eingetragen ist,
- Firewall oder Routing die benötigten Dienste blockieren,
- der Client einem falschen AD-Standort zugeordnet wird.

---

12. DNS-Cache kontrolliert untersuchen

Cache anzeigen:

```
ipconfig /displaydns
```

PowerShell:

```
Get-DnsClientCache
```

Der Cache kann Hinweise auf bereits verwendete Einträge liefern.

Erst nach Sicherung der relevanten Informationen kann für einen kontrollierten Vergleich der Clientcache geleert werden:

```
ipconfig /flushdns
```

Das Leeren des DNS-Caches ist eine Zustandsänderung. Wenn der Fehler nur sporadisch auftritt, kann dadurch ein wichtiger Hinweis auf einen falschen oder veralteten Eintrag verloren gehen.

Eine erfolgreiche Anmeldung nach dem Leeren beweist noch nicht, welcher DNS-Eintrag fehlerhaft war. Dafür müssen Antworten vor und nach der Änderung verglichen werden.

---

13. Domain Controller Locator prüfen

Windows verwendet den Domain Controller Locator, um einen geeigneten Domain Controller zu finden.

Domain Controller suchen

```
nltest /dsgetdc:<ad-domain>
```

Erzwungene erneute Suche

```
nltest /dsgetdc:<ad-domain> /force
```

Domain Controller eines AD-Standorts suchen

```
nltest /dsgetdc:<ad-domain> /site:<site-name>
```

Clientstandort anzeigen

```
nltest /dsgetsite
```

Liste der Domain Controller

```
nltest /dclist:<ad-domain>
```

Die Ausgabe von `nltest /dsgetdc` kann unter anderem zeigen:

- gefundenen Domain Controller,
- Adresse,
- Domänen-GUID,
- AD-Standort,
- Eigenschaften wie LDAP, KDC, DNS oder Global Catalog.

Fehler wie:

```
ERROR_NO_SUCH_DOMAIN
```

oder:

```
DsGetDcName failed: Status = 1355
```

weisen darauf hin, dass kein geeigneter Domain Controller gefunden wurde. Die Ursache kann unter anderem bei DNS, Netzwerk, Firewall, AD-Standort, Dienstregistrierung oder Domain Controller liegen.

---

14. Verwendeten Anmeldeserver feststellen

Nach einer erfolgreichen Domänenanmeldung:

```
echo %LOGONSERVER%
```

PowerShell:

```
$env:LOGONSERVER
```

Zusätzlich:

```
whoami
```

```
whoami /user
```

```
whoami /groups
```

Der Wert von `LOGONSERVER` ist hilfreich, darf aber nicht als vollständiger Nachweis für jeden späteren Authentifizierungsvorgang betrachtet werden. Unterschiedliche Dienste können andere Domain Controller oder Kerberos-Dienstpfade verwenden.

Wenn die Anmeldung nur bei einem bestimmten Domain Controller fehlschlägt, sind besonders zu prüfen:

- Replikation,
- DNS-Registrierung,
- Erreichbarkeit,
- Uhrzeit,
- SYSVOL und NETLOGON,
- Kerberos,
- Kontostand auf diesem DC,
- AD-Standortzuordnung.

---

15. Systemzeit und Zeitzone prüfen

Kerberos ist auf ausreichend übereinstimmende Zeit angewiesen. Eine zu große Zeitabweichung kann die Authentifizierung verhindern.

Clientstatus

```
w32tm /query /status
```

Konfiguration

```
w32tm /query /configuration
```

Zeitquelle

```
w32tm /query /source
```

Vergleich mit einem Domain Controller

```
w32tm /stripchart /computer:<dc-fqdn> /dataonly /samples:10
```

Windows-Time-Service

```
Get-Service -Name W32Time
```

Zusätzlich dokumentieren:

```
Get-Date
```

```
Get-TimeZone
```

Zu prüfen sind:

- Datum,
- Uhrzeit,
- Zeitzone,
- Zeitquelle,
- letzte erfolgreiche Synchronisierung,
- Erreichbarkeit der Zeitquelle,
- Zeithierarchie der Domäne,
- Zustand des Windows-Zeitdienstes,
- Zeit des Hypervisors bei virtuellen Maschinen.

Die Uhr darf während der Diagnose nicht unkontrolliert manuell verändert werden. Vor einer Korrektur sollten Status und Abweichung dokumentiert werden.

---

16. Benutzerkonto prüfen

Mit installiertem Active-Directory-PowerShell-Modul und ausreichender Berechtigung:

```
Get-ADUser -Identity <benutzer> `
  -Properties Enabled, LockedOut, PasswordExpired,
              PasswordLastSet, AccountExpirationDate,
              UserPrincipalName, SamAccountName,
              LastLogonDate, LogonWorkstations
```

Gezielt formatieren:

```
Get-ADUser -Identity <benutzer> `
  -Properties Enabled, LockedOut, PasswordExpired,
              PasswordLastSet, AccountExpirationDate,
              UserPrincipalName, LogonWorkstations |
```

```
    Select-Object SamAccountName,
                  UserPrincipalName,
                  Enabled,
                  LockedOut,
                  PasswordExpired,
                  PasswordLastSet,
                  AccountExpirationDate,
                  LogonWorkstations
```

Zu prüfen sind:

- Konto vorhanden,
- Konto aktiviert,
- Konto gesperrt,
- Konto abgelaufen,
- Kennwort abgelaufen,
- Kennwortänderung erforderlich,
- korrekter Benutzerprinzipalname,
- korrekter Anmeldename,
- erlaubte Arbeitsstationen,
- erlaubte Anmeldezeiten,
- Smartcard- oder Zertifikatsanforderungen,
- Mitgliedschaften in relevanten Gruppen,
- wirksame Richtlinien und Anmelderechte.

`LastLogonDate` ist nicht für jede sekundengenaue Untersuchung geeignet. Je nach benötigter Genauigkeit müssen die entsprechenden Attribute und Ereignisprotokolle auf den relevanten Domain Controllern ausgewertet werden.

---

17. Kontosperre untersuchen

Ein Konto kann durch wiederholte fehlerhafte Anmeldeversuche gesperrt werden.

Mögliche Quellen:

- Benutzer gibt mehrfach ein falsches Kennwort ein,
- Smartphone verwendet ein altes Kennwort,
- gespeicherte Anmeldeinformationen,
- getrennte RDP-Sitzung,
- Windows-Dienst mit Benutzerkonto,
- geplante Aufgabe,
- Netzlaufwerk,
- Drucker,
- VPN-Client,

- WLAN-Authentifizierung,
- Outlook oder andere Anwendung,
- Skript,
- Anwendungspool,
- zweiter Computer,
- Gerät außerhalb des Firmennetzes,
- Angriffsversuch.

Kontostatus:

```
Get-ADUser -Identity <benutzer> -Properties LockedOut |
    Select-Object SamAccountName, LockedOut
```

Sperrereignisse auf einem Domain Controller:

```
Get-WinEvent -FilterHashtable @{
    LogName = "Security"
    Id      = 4740
} |
    Select-Object TimeCreated, Id, Message
```

Ereignis-ID `4740` zeigt eine Kontosperre. Das Ereignis kann Informationen über den aufrufenden Computer enthalten.

Nur das Entsperren des Kontos behebt eine wiederkehrende Sperrquelle nicht. Vor dem Entsperren sollten Zeitpunkt, Domain Controller, aufrufender Computer und vorausgehende Authentifizierungsfehler dokumentiert werden.

---

18. Kennwortänderung und Replikation berücksichtigen

Nach einer Kennwortänderung können Probleme entstehen, wenn:

- ein Client noch das alte Kennwort verwendet,
- gespeicherte Anmeldedaten nicht aktualisiert wurden,
- ein Gerät dauerhaft alte Zugangsdaten sendet,
- Domain Controller nicht ordnungsgemäß replizieren,
- ein Standort nur einen fehlerhaften Domain Controller erreicht,
- ein Dienstkontokennwort geändert wurde, die Dienstkonfiguration jedoch nicht,
- das Benutzerkonto gesperrt wurde,
- der Benutzer offline arbeitet und zwischengespeicherte Anmeldedaten verwendet.

Zu erfassen:

```
Zeitpunkt der Kennwortänderung:
System, an dem das Kennwort geändert wurde:
vermutlich beteiligter Domain Controller:
erstes Auftreten des Fehlers:
funktioniert altes Kennwort offline:
funktioniert neues Kennwort online:
funktioniert Anmeldung an anderem Client:
funktioniert Anmeldung an anderem Standort:
```

Kennwörter dürfen nicht testweise an mehreren Stellen verteilt oder protokolliert werden.

---

19. Computerkonto prüfen

Ein Domänencomputer besitzt in Active Directory ein eigenes Computerkonto.

Mit dem Active-Directory-PowerShell-Modul:

```
Get-ADComputer -Identity <computername> `
  -Properties Enabled, PasswordLastSet, LastLogonDate,
              DistinguishedName, DNSHostName
```

Formatierte Ausgabe:

```
Get-ADComputer -Identity <computername> `
  -Properties Enabled, PasswordLastSet, LastLogonDate,
              DistinguishedName, DNSHostName |
    Select-Object Name,
                  DNSHostName,
                  Enabled,
                  PasswordLastSet,
                  LastLogonDate,
                  DistinguishedName
```

Zu prüfen sind:

- Computerkonto vorhanden,
- Computerkonto aktiviert,
- korrekter Name,
- keine unerwarteten doppelten oder alten Objekte,
- erwartete Organisationseinheit,

- plausibler Zeitpunkt des Maschinenkennworts,
- Client wurde nicht aus einem alten Snapshot wiederhergestellt,
- Client wurde nicht geklont, ohne korrekt vorbereitet zu werden,
- Computerkonto wurde nicht gelöscht und neu erstellt,
- Clientname wurde nicht unsachgemäß geändert.

`PasswordLastSet` allein beweist nicht, dass der sichere Kanal funktioniert. Es ist nur ein Hinweis innerhalb der Gesamtanalyse.

---

20. Sicheren Kanal prüfen

Der sichere Kanal verbindet einen Domänenmitgliedscomputer mit der Domäne.

PowerShell auf einem Mitgliedscomputer

```
Test-ComputerSecureChannel -Verbose
```

Mit ausdrücklich angegebener Domäne:

```
Test-ComputerSecureChannel `
  -Server <dc-fqdn> `
  -Verbose
```

NLTEST

```
nltest /sc_query:<ad-domain>
```

Zusätzliche Informationen:

```
nltest /sc_verify:<ad-domain>
```

Je nach Systemrolle und verwendetem Werkzeug unterscheiden sich Bedeutung und Verhalten einzelner Prüfungen. `Test-ComputerSecureChannel` ist für Domänenmitgliedscomputer vorgesehen und sollte nicht als allgemeiner Zustandstest eines Domain Controllers verwendet werden.

Ein fehlerhafter sicherer Kanal kann Meldungen verursachen wie:

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

Mögliche Ursachen:

- Maschinenkennwort stimmt zwischen Client und AD nicht überein,
- Client wurde auf einen alten Snapshot zurückgesetzt,
- Computerkonto wurde gelöscht oder neu angelegt,
- replizierte Kontodaten sind inkonsistent,
- Client wurde fehlerhaft geklont,
- lange getrenntes oder zurückgesetztes System,
- Wiederherstellung aus einem ungeeigneten Image,
- DNS oder Netzwerk verhindert die Kontaktaufnahme.

---

21. Sicheren Kanal nur kontrolliert reparieren

Die folgenden Befehle verändern den Zustand und gehören nicht zur rein lesenden Diagnose.

PowerShell

```
Test-ComputerSecureChannel `
  -Repair `
  -Credential (Get-Credential) `
  -Verbose
```

Alternative:

```
Reset-ComputerMachinePassword `
  -Server <dc-fqdn> `
  -Credential (Get-Credential)
```

Eine Reparatur sollte nur erfolgen, wenn:

1. DNS und Netzwerk geprüft wurden,
2. die Uhrzeit korrekt ist,
3. das richtige Computerkonto identifiziert wurde,
4. der Fehler des sicheren Kanals bestätigt wurde,
5. erforderliche Berechtigungen vorhanden sind,
6. Auswirkungen und Rückfallmöglichkeit bekannt sind,
7. Diagnoseinformationen vorher gesichert wurden.

Nach der Reparatur müssen mindestens geprüft werden:

- sicherer Kanal,
- Neustartanforderung,
- Domänenanmeldung,

- Gruppenrichtlinien,
- Kerberos-Tickets,
- Zugriff auf Domänenressourcen,
- Verwaltungs- und Sicherheitssoftware,
- Ereignisprotokolle.

Das Entfernen und erneute Hinzufügen zur Domäne sollte erst nach nachvollziehbarer Diagnose und gemäß dem betrieblichen Verfahren erfolgen.

---

22. Kerberos-Tickets prüfen

Aktuelle Tickets des angemeldeten Sicherheitskontexts:

```
klist
```

Kerberos-Ticket-Granting-Tickets anzeigen:

```
klist tgt
```

Weitere Sitzungsinformationen:

```
klist sessions
```

Verfügbarer Domain Controller:

```
klist query_bind
```

Je nach Windows-Version und Sicherheitskontext können die verfügbaren Unterbefehle und sichtbaren Tickets variieren. Die lokale Hilfe ist zu prüfen:

```
klist ?
```

Zu untersuchen sind:

- ist ein TGT vorhanden,
- welcher KDC wurde verwendet,
- stimmen Client- und Domänenname,
- sind Tickets abgelaufen,
- treten Kerberos-Fehler in den Ereignisprotokollen auf,
- funktioniert DNS für den KDC,

- stimmt die Uhrzeit,
- ist der verwendete Dienstprinzipalname korrekt,
- wird unerwartet NTLM statt Kerberos verwendet.

Tickets kontrolliert entfernen:

```
klist purge
```

`klist purge` verändert den Anmeldezustand der aktuellen Sitzung. Vorher sollten die vorhandenen Tickets dokumentiert werden. Eine erfolgreiche Funktion nach dem Purge beweist ohne Vergleich der vorherigen Tickets nicht automatisch die Ursache.

---

23. NTLM und Kerberos unterscheiden

Eine Windows-Domäne kann je nach Vorgang Kerberos oder NTLM verwenden.

Vereinfacht:

Bereich	typischer Hinweis
Kerberos-Vorauthentifizierung fehlgeschlagen	Ereignis 4771
Kerberos-TGT angefordert	Ereignis 4768
Kerberos-Dienstticket angefordert	Ereignis 4769
NTLM-Anmeldeinformationen geprüft	Ereignis 4776
Anmeldung auf Zielsystem fehlgeschlagen	Ereignis 4625
Konto gesperrt	Ereignis 4740

Ein Ereignis muss immer zusammen mit Zeitpunkt, Benutzer, Clientadresse, Anmeldetyp, Statuscode, Substatus und beteiligtem System bewertet werden.

---

24. Ereignis 4625 auswerten

Ereignis-ID `4625` bedeutet, dass eine Kontoanmeldung fehlgeschlagen ist. Es entsteht auf dem System, auf dem der Anmeldeversuch verarbeitet wurde.

Zeitlich begrenzte Abfrage:

```
$Start = Get-Date "2026-08-02 09:10:00"
$End = Get-Date "2026-08-02 09:20:00"

Get-WinEvent -FilterHashtable @{
```

```
    LogName   = "Security"
    Id        = 4625
    StartTime = $Start
    EndTime   = $End
} |
    Select-Object TimeCreated, Id, Message
```

Wichtige Felder können sein:

- Kontoname,
- Kontodomäne,
- Anmelde-ID,
- Anmeldetyp,
- Fehlergrund,
- Status,
- Substatus,
- Arbeitsstationsname,
- Quellnetzwerkadresse,
- Quellport,
- Authentifizierungspaket,
- beteiligter Prozess.

Häufige Anmeldetypen:

Anmeldetyp	Bedeutung
2	interaktive Anmeldung an der Konsole
3	Netzwerkanmeldung
4	Batch, beispielsweise geplante Aufgabe
5	Dienst
7	Entsperren
8	NetworkCleartext
9	NewCredentials
10	RemoteInteractive, beispielsweise RDP
11	CachedInteractive

Anmeldetyp `11` weist auf eine interaktive Anmeldung mit zwischengespeicherten Domäneninformationen hin. Er bedeutet nicht, dass während der Anmeldung ein Domain Controller erreicht wurde.

Status- und Substatuswerte müssen anhand der Microsoft-Dokumentation und des konkreten Ereignisses interpretiert werden.

25. Relevante Authentifizierungsereignisse

Auf Client, Mitgliedsserver und Domain Controllern können unter anderem relevant sein:

Ereignis-ID	allgemeine Bedeutung
4624	erfolgreiche Anmeldung
4625	fehlgeschlagene Anmeldung
4648	Anmeldung mit ausdrücklich angegebenen Anmeldeinformationen
4672	besondere Rechte wurden einer neuen Anmeldung zugewiesen
4722	Benutzerkonto aktiviert
4725	Benutzerkonto deaktiviert
4726	Benutzerkonto gelöscht
4738	Benutzerkonto geändert
4740	Benutzerkonto gesperrt
4767	Benutzerkonto entsperrt
4768	Kerberos-TGT angefordert
4769	Kerberos-Dienstticket angefordert
4770	Kerberos-Dienstticket erneuert
4771	Kerberos-Vorauthentifizierung fehlgeschlagen
4776	Anmeldeinformationen wurden über NTLM geprüft
5719	kein Domain Controller für eine sichere Sitzung verfügbar
5722	Authentifizierung der Sitzung beziehungsweise des Computerkontos fehlgeschlagen
5805	Sitzung eines Computers konnte nicht authentifiziert werden

Nicht jedes Ereignis ist standardmäßig aktiviert oder auf jedem System vorhanden. Ereignisse können auf unterschiedlichen beteiligten Computern entstehen.

26. Mehrere Ereignisse zeitlich abfragen

```
$Start = Get-Date "2026-08-02 09:10:00"
$End = Get-Date "2026-08-02 09:20:00"
$Ids = 4624, 4625, 4648, 4740, 4768, 4769, 4771, 4776
```

```
Get-WinEvent -FilterHashtable @{
    LogName   = "Security"
    Id        = $Ids
    StartTime = $Start
    EndTime   = $End
} |
    Select-Object TimeCreated, Id, ProviderName,
                  LevelDisplayName, Message |
    Sort-Object TimeCreated
```

Systemereignisse:

```
Get-WinEvent -FilterHashtable @{
    LogName   = "System"
    Id        = 5719, 5722, 5805
    StartTime = $Start
    EndTime   = $End
} |
    Select-Object TimeCreated, Id, ProviderName,
                  LevelDisplayName, Message |
    Sort-Object TimeCreated
```

Für große Protokolle sollte bereits serverseitig mit `FilterHashtable` nach Zeitraum und Ereignis-ID gefiltert werden.

---

27. Ereignisprotokolle auf dem Client prüfen

Relevante Protokolle können sein:

```
Windows-Protokolle → System
Windows-Protokolle → Sicherheit
Windows-Protokolle → Anwendung
Anwendungs- und Dienstprotokolle → Microsoft → Windows → GroupPolicy → Operational
Anwendungs- und Dienstprotokolle → Microsoft → Windows → User Profile Service → Operational
Anwendungs- und Dienstprotokolle → Microsoft → Windows → DNS Client Events
Anwendungs- und Dienstprotokolle → Microsoft → Windows → WLAN-AutoConfig → Operational
```

Vorhandene Protokolle auflisten:

```
Get-WinEvent -ListLog * |
    Where-Object {
        $_.LogName -match "GroupPolicy|User Profile|DNS|WLAN|Kerberos|Netlogon"
    } |
    Select-Object LogName, IsEnabled, RecordCount
```

Nicht jedes Protokoll ist auf jedem System aktiviert. Zusätzliche Protokollierung darf nur kontrolliert unter Berücksichtigung von Speicherbedarf, Datenschutz und Betriebsrichtlinien aktiviert werden.

---

28. Netlogon-Diagnose berücksichtigen

Der Netlogon-Dienst ist unter anderem an Domain-Controller-Ermittlung und sicherem Kanal beteiligt.

Dienststatus:

```
Get-Service -Name Netlogon
```

Ausführliche Dienstinformationen:

```
sc.exe query netlogon
```

Netlogon kann ein Diagnoseprotokoll unter folgendem Pfad verwenden:

```
%windir%\debug\netlogon.log
```

Erweiterte Netlogon-Protokollierung verändert den Diagnosezustand und kann umfangreiche oder sensible Informationen erzeugen. Sie sollte nur gezielt, zeitlich begrenzt und entsprechend der offiziellen Microsoft-Anleitung aktiviert werden.

Nach Abschluss muss eine zusätzlich aktivierte Diagnoseprotokollierung wieder auf den vorgesehenen Zustand zurückgesetzt werden.

---

29. Gruppenrichtlinien prüfen

Eine Anmeldung kann technisch erfolgreich sein, während Gruppenrichtlinien, Skripte oder Ressourcenverbindungen fehlschlagen.

Aktuelle Richtlinien aktualisieren:

```
gpupdate /force
```

Dieser Befehl ist eine aktive Zustandsänderung und sollte erst nach Sicherung der relevanten Ereignisse verwendet werden.

Resultierende Richtlinien anzeigen:

```
gpresult /r
```

Ausführlicher HTML-Bericht:

```
gpresult /h C:\Temp\gpresult.html
```

Relevante Fragen:

- erreicht der Client SYSVOL und NETLOGON,
- werden Benutzer- und Computerrichtlinien angewendet,
- blockiert ein Anmelderecht die interaktive Anmeldung,
- ist „Lokal anmelden zulassen“ passend konfiguriert,
- greift „Lokal anmelden verweigern“,
- greift „Anmelden über Remotedesktopdienste zulassen“,
- verhindert eine Software Restriction Policy oder AppLocker einen Bestandteil,
- hängt ein Anmelde- oder Startskript,
- ist ein Netzlaufwerk oder Druckerziel nicht erreichbar,
- wartet die Anmeldung auf das Netzwerk,
- wurden Richtlinien kürzlich geändert.

Ein lang laufendes Anmeldeskript kann wie eine fehlgeschlagene Anmeldung erscheinen, obwohl die Authentifizierung bereits abgeschlossen wurde.

---

30. SYSVOL und NETLOGON prüfen

Freigaben eines Domain Controllers anzeigen:

```
net view \\<dc-fqdn>
```

SYSVOL testen:

```
dir \\<dc-fqdn>\SYSVOL
```

NETLOGON testen:

```
dir \\<dc-fqdn>\NETLOGON
```

Wenn diese Pfade nicht erreichbar sind, sind unter anderem zu prüfen:

- DNS-Auflösung,
- SMB-Erreichbarkeit,
- Firewall,
- Domain-Controller-Dienstzustand,
- SYSVOL-Bereitstellung,
- DFS-Replikation,
- Netzwerkpfad,
- Berechtigungen,
- sicherer Kanal.

Ein erfolgreicher Verzeichniszugriff beweist nicht, dass alle Gruppenrichtlinien oder die AD-Replikation fehlerfrei sind.

---

31. Benutzerprofilfehler von Authentifizierungsfehlern trennen

Der Benutzer kann erfolgreich authentifiziert worden sein, obwohl Windows das Profil nicht laden kann.

Typische Hinweise:

```
Die Anmeldung des Dienstes "Benutzerprofildienst" ist fehlgeschlagen.
```

```
Das Benutzerprofil kann nicht geladen werden.
```

```
Sie wurden mit einem temporären Profil angemeldet.
```

Dann sind besonders zu prüfen:

- Ereignisse des User Profile Service,
- freier Speicherplatz,
- Erreichbarkeit eines servergespeicherten Profils,
- Berechtigungen,
- beschädigtes lokales Profil,
- Profilcontainer,
- FSLogix bei entsprechender Umgebung,

- Antiviren- oder Sicherheitssoftware,
- Datenträgerfehler,
- Registry-Profilzuordnung,
- gleichzeitige Sitzung oder gesperrte Profildatei.

Ein Profilproblem darf nicht automatisch als fehlerhaftes Benutzerkonto oder fehlerhafte Domänenauthentifizierung behandelt werden.

---

32. RDP-Anmeldung gesondert untersuchen

Wenn nur die Remotedesktopanmeldung fehlschlägt, zusätzlich prüfen:

- RDP-Dienst erreichbar,
- TCP-Port erreichbar,
- Network Level Authentication,
- Benutzer besitzt RDP-Anmelderecht,
- Benutzer ist nicht durch eine Richtlinie ausgeschlossen,
- Zielsystem kann den Domain Controller erreichen,
- Zielsystemzeit stimmt,
- Zertifikat oder TLS-Verbindung funktioniert,
- CredSSP- oder Sicherheitsrichtlinien sind kompatibel,
- keine bereits bestehende oder beschränkte Sitzung,
- Anmeldetyp `10` in Ereignis 4625,
- Quelladresse und Zielsystem im Ereignis.

Porttest:

```
Test-NetConnection -ComputerName <zielserver> -Port 3389
```

Ein erfolgreicher Porttest beweist nur, dass eine TCP-Verbindung hergestellt werden konnte. Er beweist nicht, dass NLA, Authentifizierung, Anmelderechte oder Profilladen funktionieren.

---

33. Anmeldung über VPN untersuchen

Bei entfernten Clients ist entscheidend, wann das VPN verfügbar wird.

Mögliche Fälle:

1. Benutzer meldet sich mit zwischengespeicherten Daten an und startet danach das VPN.
2. Ein gerätebasiertes VPN ist bereits vor der Anmeldung aktiv.
3. Ein Pre-Logon-VPN wird am Anmeldebildschirm gestartet.
4. Das VPN benötigt Benutzeranmeldedaten, die erst nach der Windows-Anmeldung verfügbar sind.
5. Das VPN verteilt falsche DNS-Server oder Routen.

6. Der VPN-Tunnel erreicht nicht alle benötigten Domain Controller.
7. MTU-, Firewall- oder Fragmentierungsprobleme stören einzelne Protokolle.
8. Gerätezertifikat oder Maschinenkonto ist fehlerhaft.

Nach Aufbau des VPN prüfen:

```
ipconfig /all
```

```
Get-DnsClientServerAddress
```

```
Get-NetRoute
```

```
nltest /dsgetdc:<ad-domain>
```

```
w32tm /query /status
```

Die erfolgreiche Anmeldung am Notebook vor dem VPN beweist nur, dass zwischengespeicherte Anmeldedaten verwendbar waren.

---

34. Domain Controller diagnostizieren

Auf einem Domain Controller und mit entsprechender Berechtigung:

```
dcdiag
```

Ausführliche Ausgabe in eine Datei:

```
dcdiag /v > C:\Temp\dcdiag.txt
```

DNS-Prüfung:

```
dcdiag /test:dns /v
```

Bestimmten Domain Controller testen:

```
dcdiag /s:<dc-name> /v
```

Unternehmensweite Prüfung:

```
dcdiag /e /v
```

Die unternehmensweite Prüfung kann umfangreich sein und sollte kontrolliert eingesetzt werden.

Zu untersuchen sind unter anderem:

- DNS,
- Erreichbarkeit,
- Netlogon,
- Advertising,
- Dienste,
- Replikation,
- SYSVOL,
- Rollen und Verzeichniszustand.

Nicht jede Warnung in `dcdiag` erklärt automatisch die konkrete Anmeldestörung. Der Zeitpunkt und der betroffene Authentifizierungspfad müssen weiterhin korreliert werden.

---

35. Active-Directory-Replikation prüfen

Zusammenfassung:

```
repadmin /replsummary
```

Eingehende Replikationspartner:

```
repadmin /showrepl
```

Alle Domain Controller detailliert:

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

Replikationswarteschlange:

```
repadmin /queue
```

Zu prüfen sind:

- fehlgeschlagene Replikationen,
- Zeitpunkt der letzten erfolgreichen Replikation,
- Fehlercode,
- betroffene Partition,
- nur ein Standort oder ein Domain Controller betroffen,
- DNS- oder RPC-Fehler,
- Zeitabweichung,
- Authentifizierungsfehler,
- Netzwerkunterbrechung.

Eine erzwungene Replikation ist eine aktive Änderung und sollte nicht als erster Diagnoseschritt verwendet werden.

Wenn ein Benutzer sein Kennwort geändert hat und die Anmeldung abhängig vom erreichten Domain Controller funktioniert, ist eine Replikationsstörung eine mögliche Hypothese. Sie muss durch Replikationsdaten und den tatsächlich verwendeten Domain Controller bestätigt werden.

---

36. AD-Standorte und Subnetze berücksichtigen

Der Domain Controller Locator berücksichtigt Active-Directory-Standorte.

Clientstandort:

```
nltest /dsgetsite
```

Gefundener Domain Controller:

```
nltest /dsgetdc:<ad-domain>
```

Mögliche Fehler:

- Clientsubnetz fehlt in Active Directory Sites and Services,
- Subnetz ist dem falschen Standort zugeordnet,
- lokaler Domain Controller ist nicht erreichbar,
- Client verwendet einen entfernten Domain Controller,
- DNS liefert veraltete oder ungeeignete Einträge,
- Standort-Uplink blockiert benötigte Protokolle,
- Anmeldung wird durch hohe Latenz oder Paketverlust verzögert,
- nur der Domain Controller eines Standorts besitzt veraltete Daten.

Ein entfernter Domain Controller ist nicht automatisch fehlerhaft. Die Standortzuordnung ist jedoch wichtig für Performance, Verfügbarkeit und Fehlereingrenzung.

---

37. Firewall und benötigte Dienste berücksichtigen

Active Directory verwendet mehrere Dienste, beispielsweise:

- DNS,
- Kerberos,
- LDAP,
- LDAPS bei entsprechender Konfiguration,
- SMB,
- RPC Endpoint Mapper,
- dynamische RPC-Ports,
- Global Catalog,
- Kerberos-Kennwortänderung,
- Zeitdienst.

Einzelne typische Ports:

Dienst	Protokoll/Port
DNS	TCP/UDP 53
Kerberos	TCP/UDP 88
RPC Endpoint Mapper	TCP 135
NetBIOS Name Service	UDP 137
NetBIOS Datagram	UDP 138
NetBIOS Session	TCP 139
LDAP	TCP/UDP 389
SMB	TCP 445
Kerberos-Kennwortänderung	TCP/UDP 464
LDAPS	TCP 636
Global Catalog	TCP 3268
Global Catalog über TLS	TCP 3269
Windows-Zeitdienst	UDP 123
dynamisches RPC	versionsabhängiger TCP-Portbereich

Diese Tabelle ist keine vollständige Firewallfreigabe. Die tatsächlich benötigten Verbindungen hängen von Windows-Version, Topologie, Richtung und Funktion ab.

Firewalls dürfen nicht pauschal deaktiviert werden. Stattdessen sind verworfene Verbindungen, Quell- und Zieladressen, Ports, Richtung und Zeitpunkt zu untersuchen.

---

38. Paketmitschnitt nur gezielt einsetzen

Wenn DNS, DC Locator, Kerberos oder LDAP weiterhin unklar bleiben, kann ein autorisierter Paketmitschnitt helfen.

Mögliche Protokolle:

```
dns
kerberos
ldap
tcp.port == 445
tcp.port == 135
```

Möglicher Wireshark-Anzeigefilter:

```
dns || kerberos || ldap || tcp.port == 445 || tcp.port == 135
```

Zu beobachten sind:

- DNS-SRV-Abfragen,
- zurückgegebene Domain Controller,
- fehlgeschlagene Namensauflösung,
- Kerberos-AS-REQ und AS-REP,
- Kerberos-Fehler,
- LDAP-Verbindungsaufbau,
- TCP-Retransmissions,
- Verbindungszurücksetzungen,
- ICMP-Fehler,
- stark verzögerte Antworten,
- angesprochener Domain Controller,
- wechselnde Domain Controller.

Paketmitschnitte können Kontonamen, interne Strukturen, Tickets und andere vertrauliche Daten enthalten. Sie dürfen nur autorisiert, begrenzt, geschützt und kontrolliert ausgewertet werden.

---

39. Praxisfall A: Nur ein Benutzer kann sich nicht anmelden

Symptom

- andere Benutzer können sich am selben Client anmelden,
- der Benutzer kann sich auch an einem zweiten Client nicht anmelden,
- Meldung weist auf gesperrtes Konto hin.

Prüfung

1. genaue Uhrzeit dokumentieren,
2. Benutzerkonto und Sperrstatus prüfen,
3. Ereignis `4740` auf den Domain Controllern suchen,
4. aufrufenden Computer ermitteln,
5. vorausgehende Ereignisse `4771`, `4776` oder `4625` korrelieren,
6. gespeicherte Anmeldedaten, Dienste, Aufgaben, VPN und Mobilgeräte prüfen,
7. erst danach Konto kontrolliert entsperren,
8. Ereignisse weiter überwachen.

Mögliche Ursache

Ein geplanter Task auf einem alten Client verwendet weiterhin das vorherige Benutzerkennwort und sperrt das Konto wiederholt.

Nachprüfung

- Aufgabe verwendet ein vorgesehenes Dienstkonto oder aktualisierte sichere Konfiguration,
- keine weiteren fehlerhaften Anmeldeversuche,
- keine neue Kontosperre,
- Benutzer kann sich anmelden,
- Sperrquelle und Maßnahme sind dokumentiert.

---

40. Praxisfall B: Kein Benutzer kann sich an einem Client anmelden

Symptom

- lokale Anmeldung funktioniert,
- Domänenanmeldungen schlagen fehl,
- andere Clients funktionieren,
- `nltest /dsgetdc:<ad-domain>` findet keinen Domain Controller.

Prüfung

1. IP-Konfiguration erfassen,
2. DNS-Server prüfen,
3. SRV-Einträge abfragen,
4. Domain Controller auflösen,
5. Netzwerkpfad prüfen,
6. Systemzeit kontrollieren,
7. sicheren Kanal erst nach Wiederherstellung des Netzwerkpfades testen.

Mögliche Ursache

Der Client verwendet durch eine statische Fehlkonfiguration einen öffentlichen DNS-Server und kann die internen Active-Directory-SRV-Einträge nicht auflösen.

Nachprüfung

- Client erhält die vorgesehenen DNS-Server,
- SRV-Abfragen funktionieren,
- Domain Controller Locator findet einen geeigneten DC,
- sicherer Kanal ist intakt,
- Domänenanmeldung und Gruppenrichtlinien funktionieren,
- Konfigurationsursache ist dokumentiert.

---

41. Praxisfall C: Vertrauensstellung ist fehlgeschlagen

Symptom

- lokale Anmeldung funktioniert,
- Domänenanmeldung meldet eine fehlerhafte Vertrauensstellung,
- DNS und Domain Controller sind erreichbar,
- der Client wurde kürzlich aus einem älteren Snapshot wiederhergestellt.

Prüfung

1. Client- und Computerkonto eindeutig identifizieren,
2. DNS und Uhrzeit prüfen,
3. Computerkonto untersuchen,
4. sicheren Kanal testen,
5. Snapshot-Zeitpunkt und Maschinenkennwort berücksichtigen,
6. Diagnoseereignisse sichern,
7. sicheren Kanal nach Freigabe kontrolliert reparieren.

Mögliche Ursache

Der Snapshot enthält ein älteres Maschinenkennwort als das Computerkonto in Active Directory.

Nachprüfung

- sicherer Kanal funktioniert,
- Domänenanmeldung ist möglich,
- Gruppenrichtlinien werden verarbeitet,
- Kerberos-Tickets werden ausgegeben,
- Clientverwaltung funktioniert,
- Wiederherstellungsverfahren für Domänencomputer wird angepasst.

---

42. Praxisfall D: Anmeldung funktioniert nur an einem Standort nicht

Symptom

- Benutzer können sich am Hauptstandort anmelden,
- an einer Außenstelle schlagen neue Anmeldungen fehl,
- bereits bekannte Benutzer kommen teilweise über zwischengespeicherte Daten hinein,
- ein lokaler Domain Controller wird über DNS gefunden.

Prüfung

1. betroffenen AD-Standort und Subnetz prüfen,
2. gefundenen Domain Controller dokumentieren,
3. DNS- und Dienstereichbarkeit testen,
4. `dcdiag` auf dem lokalen DC auswerten,
5. `repadmin /replsummary` und `/showrepl` prüfen,
6. Uhrzeit vergleichen,
7. Kontostand auf beteiligten Domain Controllern vergleichen,
8. Standort-Uplink und Firewall berücksichtigen.

Mögliche Ursache

Der lokale Domain Controller repliziert Benutzer- und Kennwortänderungen wegen einer gestörten Standortverbindung nicht ordnungsgemäß.

Nachprüfung

- Replikation ist fehlerfrei,
- Kennwortänderungen stehen an den vorgesehenen Domain Controllern zur Verfügung,
- neue Benutzer können sich anmelden,
- keine zwischengespeicherte Anmeldung wird fälschlich als Onlineanmeldung bewertet,
- Standortverbindung wird überwacht.

---

43. Praxisfall E: Anmeldung dauert mehrere Minuten

Symptom

- Anmeldeinformationen werden akzeptiert,
- der Bildschirm bleibt lange bei „Willkommen“ oder „Benutzereinstellungen werden angewendet“,
- Benutzerprofil wird schließlich geladen,
- andere Standorte sind schneller.

Prüfung

1. Authentifizierungszeit und Profil-Ladezeit trennen,
2. Ereignisse von GroupPolicy und User Profile Service prüfen,
3. `gpresult` auswerten,
4. SYSVOL und NETLOGON testen,
5. Anmelde- und Startskripte untersuchen,

6. Netzlaufwerke und Druckerverbindungen prüfen,
7. DNS und verwendeten Domain Controller erfassen,
8. Serverprofil oder Profilcontainer untersuchen,
9. Zeitlinie von Anmeldung, Richtlinien und Profilladen erstellen.

Mögliche Ursache

Ein Anmeldeskript wartet auf einen nicht erreichbaren Dateiserver, bis ein Timeout abläuft.

Nachprüfung

- Skriptziel ist erreichbar oder kontrolliert entfernt,
- Anmeldung erfolgt innerhalb des vorgesehenen Zeitraums,
- alle benötigten Richtlinien werden angewendet,
- Netzlaufwerke und andere Geschäftsprozesse funktionieren,
- Messwerte vor und nach der Änderung sind dokumentiert.

---

44. Ungeeignete Sofortmaßnahmen

Problematisch sind insbesondere:

- Benutzerkennwort sofort zurücksetzen,
- Konto nur entsperren und die Sperrquelle ignorieren,
- Computerkonto löschen,
- Client sofort aus der Domäne entfernen,
- Domain Controller neu starten,
- DNS-Cache leeren, bevor Einträge dokumentiert wurden,
- Kerberos-Tickets löschen, bevor sie geprüft wurden,
- Firewall vollständig deaktivieren,
- Gruppenrichtlinien pauschal abschalten,
- Systemzeit manuell verändern,
- mehrere Domain Controller gleichzeitig verändern,
- Replikation ungeprüft erzwingen,
- DNS-Einträge manuell neu anlegen, ohne die Registrierungsursache zu prüfen,
- Benutzerprofil löschen, obwohl die Authentifizierung fehlschlägt,
- lokale Administratorrechte unnötig vergeben,
- Kennwörter in Tickets oder Skripten speichern,
- nur Ping verwenden,
- nur den Client untersuchen,
- eine zwischengespeicherte Anmeldung als erfolgreiche DC-Anmeldung bewerten,
- einen erfolgreichen Test mit anderem Benutzer als Beweis für fehlerfreies AD ansehen.

---

45. Vollständige Prüfreihenfolge

1. genauen Meldungstext sichern.

2. Datum, Uhrzeit und Zeitzone erfassen.
3. Benutzer, Client und Standort bestimmen.
4. lokales Konto und Domänenkonto unterscheiden.
5. verwendetes Anmeldeformat dokumentieren.
6. prüfen, ob eine zwischengespeicherte Anmeldung möglich war.
7. feststellen, ob ein Benutzer, ein Client oder mehrere Systeme betroffen sind.
8. Vergleich mit anderem Benutzer am selben Client durchführen.
9. Vergleich mit demselben Benutzer an einem anderen Client durchführen.
10. Netzwerkstatus vor der Anmeldung berücksichtigen.
11. IP-Konfiguration erfassen.
12. Gateway und internen DNS-Server prüfen.
13. konfigurierte DNS-Server und Suffixe kontrollieren.
14. Active-Directory-SRV-Einträge auflösen.
15. Hostnamen der Domain Controller auflösen.
16. Domain Controller Locator prüfen.
17. AD-Standort des Clients bestimmen.
18. verwendeten Domain Controller dokumentieren.
19. Uhrzeit, Zeitzone und Zeitquelle prüfen.
20. Benutzerkonto auf Aktivierung, Sperre und Ablauf prüfen.
21. Anmeldezeiten und erlaubte Arbeitsstationen berücksichtigen.
22. Kennwortänderung und gespeicherte Anmeldedaten prüfen.
23. Ereignisse `4625`, `4740`, `4771` und `4776` korrelieren.
24. bei RDP den Anmeldetyp und das Zielsystem berücksichtigen.
25. Computerkonto prüfen.
26. sicheren Kanal diagnostizieren.
27. Kerberos-Tickets und KDC prüfen.
28. SYSVOL und NETLOGON testen.
29. Gruppenrichtlinien und Anmeldeskripte untersuchen.
30. Profilfehler von Authentifizierungsfehlern trennen.
31. bei VPN den Pre-Logon-Netzwerkzustand prüfen.
32. Domain Controller mit `dcdiag` untersuchen.
33. Replikation mit `repadmin` prüfen.
34. Firewall-, Routing- und Standortpfad berücksichtigen.
35. Daten aller beteiligten Systeme auf einer Zeitleiste zusammenführen.
36. konkrete Hypothese formulieren.
37. genau eine kontrollierbare Änderung durchführen.
38. dieselben Prüfungen erneut ausführen.
39. Domänenanmeldung testen.
40. Gruppenrichtlinien und Domänenressourcen prüfen.
41. Vergleichsbenutzer und Vergleichsclient testen.
42. Ereignisprotokolle auf neue Fehler prüfen.
43. temporäre Diagnosekonfiguration entfernen.
44. Ursache, Änderung und Nachweis dokumentieren.
45. Monitoring oder Präventionsmaßnahme festlegen.

---

46. Dokumentationsbeispiel

Ticket: INC-20831
Zeitraum: 02.08.2026, 08:14 bis 10:42 Uhr
Benutzer: test.user
Client: WS-BER-042
Domäne: ad.example.test
Standort: Berlin
Verbindung: Ethernet

Symptom:
Kein Domänenbenutzer kann sich an WS-BER-042 anmelden. Lokale Anmeldung ist möglich. Andere Clients desselben Standorts sind nicht betroffen.

Meldung:
„Es sind momentan keine Anmeldeserver zum Verarbeiten der Anmeldeanforderung verfügbar.“

Vergleich:
- anderer Domänenbenutzer am selben Client: fehlgeschlagen
- betroffener Benutzer an anderem Client: erfolgreich
- lokales Administratorkonto: erfolgreich

Messungen:
- Client besitzt gültige IPv4-Adresse und erreicht das Standardgateway
- interner DNS-Server ist erreichbar
- in der statischen Adapterkonfiguration ist jedoch ein öffentlicher DNS-Server eingetragen
- Abfrage von _ldap._tcp.dc._msdcs.ad.example.test schlägt fehl
- nltest /dsgetdc:ad.example.test liefert Fehler 1355
- Clientzeit ist korrekt
- Computerkonto ist vorhanden und aktiviert

Hypothese:
Der Client kann aufgrund der falschen DNS-Konfiguration keine Active-Directory-Domain-Controller finden.

Kontrollierte Änderung:
Die statische DNS-Konfiguration wurde entsprechend der freigegebenen

Netzwerkdokumentation auf die vorgesehenen internen DNS-Server korrigiert.

Andere Einstellungen blieben unverändert.

Nachprüfung:

- SRV-Abfrage liefert die vorgesehenen Domain Controller
- nltest findet einen Domain Controller des korrekten Standorts
- sicherer Kanal ist intakt
- Domänenanmeldung funktioniert
- Gruppenrichtlinien werden verarbeitet
- SYSVOL und NETLOGON sind erreichbar
- keine neuen Netlogon- oder Anmeldefehler
- Vergleichsbenutzer funktioniert ebenfalls

Ursache:

Falsch statisch eingetragener öffentlicher DNS-Server am Domänenclient.

Prävention:

- DNS-Konfiguration von Domänenclients zentral überwachen
- statische Clientkonfigurationen vermeiden, wenn DHCP vorgesehen ist
- Prüfung der AD-SRV-Auflösung in die Clientdiagnose aufnehmen

---

47. Checkliste „Anmeldung an der Domäne geht nicht“

- [ ] der genaue Meldungstext wurde gesichert.
- [ ] Fehlercode und Ereignis-ID wurden dokumentiert.
- [ ] Datum, Uhrzeit und Zeitzone sind bekannt.
- [ ] Benutzer, Client, Standort und Verbindungsart sind bekannt.
- [ ] lokales Konto und Domänenkonto wurden unterschieden.
- [ ] das verwendete Anmeldeformat wurde geprüft.
- [ ] Tastaturbelegung und versehentliche Eingabefehler wurden berücksichtigt.
- [ ] der Umfang der Störung wurde bestimmt.
- [ ] ein anderer Benutzer wurde am selben Client geprüft.
- [ ] derselbe Benutzer wurde an einem anderen Client geprüft.
- [ ] eine mögliche zwischengespeicherte Anmeldung wurde erkannt.
- [ ] der Netzwerkstatus vor der Anmeldung wurde berücksichtigt.
- [ ] IP-Adresse, Gateway, DHCP und DNS wurden dokumentiert.
- [ ] der Client verwendet die vorgesehenen internen DNS-Server.

- [ ] DNS-Suffixe wurden geprüft.
- [ ] die AD-Domäne ist auflösbar.
- [ ] LDAP-SRV-Einträge sind auflösbar.
- [ ] Kerberos-SRV-Einträge sind auflösbar.
- [ ] die zurückgegebenen Domain Controller sind auflösbar und erreichbar.
- [ ] Domain Controller Locator wurde geprüft.
- [ ] der AD-Standort des Clients wurde bestimmt.
- [ ] der tatsächlich verwendete Domain Controller wurde dokumentiert.
- [ ] Datum, Uhrzeit, Zeitzone und Zeitquelle wurden geprüft.
- [ ] Benutzerkonto ist vorhanden und aktiviert.
- [ ] Benutzerkonto ist nicht gesperrt.
- [ ] Konto und Kennwort sind nicht abgelaufen.
- [ ] erlaubte Anmeldezeiten und Arbeitsstationen wurden berücksichtigt.
- [ ] Ereignis `4740` wurde bei Kontosperren untersucht.
- [ ] alte gespeicherte Kennwörter wurden als mögliche Sperrquelle berücksichtigt.
- [ ] Kennwortänderung und AD-Replikation wurden berücksichtigt.
- [ ] Computerkonto ist vorhanden und aktiviert.
- [ ] sicherer Kanal wurde diagnostiziert.
- [ ] Snapshot-, Klon- oder Wiederherstellungsereignisse wurden berücksichtigt.
- [ ] Kerberos-Tickets wurden vor einer Veränderung geprüft.
- [ ] Ereignisse `4625`, `4768`, `4769`, `4771` und `4776` wurden passend untersucht.
- [ ] Anmeldetyp, Status und Substatus wurden ausgewertet.
- [ ] SYSVOL und NETLOGON wurden geprüft.
- [ ] Gruppenrichtlinien wurden berücksichtigt.
- [ ] Anmeldeskripte und Ressourcenzuordnungen wurden geprüft.
- [ ] Profilfehler wurden von Authentifizierungsfehlern getrennt.
- [ ] bei RDP wurden NLA und Anmelderechte geprüft.
- [ ] bei VPN wurde die Verfügbarkeit vor der Anmeldung berücksichtigt.
- [ ] Domain Controller wurden bei Bedarf mit `dcdiag` geprüft.
- [ ] Replikation wurde bei Bedarf mit `repadmin` geprüft.
- [ ] Firewall und benötigte AD-Dienste wurden berücksichtigt.
- [ ] Daten wurden auf einer gemeinsamen Zeitleiste korreliert.
- [ ] keine Kennwörter wurden protokolliert.
- [ ] nur eine kontrollierbare Änderung wurde durchgeführt.

- [ ] Domänenanmeldung wurde nach der Änderung erneut geprüft.
- [ ] Gruppenrichtlinien und Domänenressourcen funktionieren.
- [ ] Vergleichsbenutzer und Vergleichsclient funktionieren.
- [ ] temporäre Diagnosekonfiguration wurde entfernt.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.
- [ ] eine Präventions- oder Monitoringmaßnahme wurde festgelegt.

---

48. Schnellreferenz

Beobachtung	wahrscheinlicher Untersuchungsbereich
ein Benutzer überall betroffen	Konto, Kennwort, Sperre, Ablauf oder Anmelderechte
alle Benutzer an einem Client betroffen	DNS, Netzwerk, Uhrzeit, Computerkonto oder sicherer Kanal
mehrere Clients eines Standorts betroffen	Standort-DNS, VLAN, Uplink, Firewall oder lokaler DC
lokale Anmeldung funktioniert	lokales System grundsätzlich zugänglich; Domänenpfad weiter prüfen
alter Benutzer funktioniert offline	wahrscheinlich zwischengespeicherte Anmeldung
neuer Benutzer funktioniert offline nicht	keine zwischengespeicherten Anmeldedaten vorhanden
altes Kennwort funktioniert offline	Cache; keine Bestätigung des aktuellen Domänenkennworts
öffentliches DNS funktioniert, AD nicht	interne AD-DNS-Zone oder SRV-Auflösung
Fehler 1355 bei `nltest`	Domain Controller konnte nicht gefunden werden
Uhrzeit stark abweichend	Kerberos und Zeitdienst
Konto gesperrt	Sperrquelle über 4740 und vorausgehende Fehler suchen
Sperre kehrt sofort zurück	Gerät, Dienst, Aufgabe, VPN oder gespeicherte Daten
Vertrauensstellung fehlgeschlagen	Computerkonto oder sicherer Kanal
Fehler nach Snapshot-Rückkehr	Maschinenkennwort oder Computerzustand
Anmeldung abhängig vom DC	Replikation, DC-Zustand, DNS oder Standort
Anmeldung funktioniert, Profil lädt nicht	User Profile Service, Speicher oder Profilpfad
Anmeldung bleibt bei „Willkommen“ hängen	Gruppenrichtlinie, Skript, Profil oder Ressource
RDP allein betroffen	NLA, RDP-Rechte, Zielsystem oder Anmeldetyp 10
VPN allein betroffen	Pre-Logon-Verbindung, DNS, Routing, Zertifikat oder Tunnel
SYSVOL nicht erreichbar	DNS, SMB, DC, DFS-Replikation oder Firewall
`Test-ComputerSecureChannel` negativ	sicheren Kanal und Voraussetzungen gezielt untersuchen

Beobachtung	wahrscheinlicher Untersuchungsbereich
Ping erfolgreich, Anmeldung fehlschlägt	DNS, Kerberos, LDAP, SMB, RPC, Konto oder Richtlinie
anderes Konto funktioniert	benutzerspezifischen Bereich priorisieren
derselbe Benutzer funktioniert an anderem Client	Client oder clientspezifische Richtlinie priorisieren
keine Ereignisse gefunden	falsches System, falscher Zeitraum, Auditierung oder Rotation
Anmeldung nach DNS-Korrektur möglich	DNS-Ursache durch Vorher-Nachher-Daten bestätigen
Anmeldung nach Neustart möglich	Zustand geändert; Ursache noch nicht bewiesen

---

Merksatz

> Eine Domänenanmeldung ist kein einzelner Vorgang, sondern eine Kette aus Netzwerk, DNS, Domain Controller Locator, Zeit, Benutzerkonto, Computerkonto, sicherem Kanal und Authentifizierungsprotokoll. Die Diagnose beginnt deshalb mit dem genauen Umfang und dem originalen Fehlerzeitpunkt. Erst danach werden Client, DNS, Domain Controller und Ereignisprotokolle auf einer gemeinsamen Zeitleiste geprüft.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Troubleshoot domain controller location issues
- Microsoft Learn – Locating domain controllers in Windows and Windows Server
- Microsoft Learn – Domain controller is not functioning correctly
- Microsoft Learn – Active Directory domain join troubleshooting guidance
- Microsoft Learn – Event ID 5719, error 1311 or error 1355
- Microsoft Learn – Diagnose Active Directory replication failures
- Microsoft Learn – Best practices for DNS client settings
- Microsoft Learn – Advanced Audit Policy Configuration settings
- Microsoft Learn – Appendix L: Events to Monitor
- Microsoft Learn – Event 4740: A user account was locked out
- Microsoft Learn – nltest
- Microsoft Learn – Test-ComputerSecureChannel
- Microsoft Learn – Reset-ComputerMachinePassword
- Microsoft Learn – Get-ADUser
- Microsoft Learn – Get-ADComputer

- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – dcdiag
- Microsoft Learn – repadmin
- Microsoft Learn – klist
- Microsoft Learn – w32tm
- Microsoft Learn – gpresult
- Microsoft Learn – Get-WinEvent
