5.3 Windows Server, Active Directory und Gruppenrichtlinien

Windows-Server-Infrastrukturen bestehen häufig aus mehreren voneinander abhängigen Diensten. Eine Störung bei Anmeldung, Gruppenrichtlinien, Namensauflösung oder Dateizugriff kann deshalb ihre eigentliche Ursache in einem anderen Teilbereich haben.

Typische Abhängigkeiten sind:

- Active Directory Domain Services
- DNS
- Kerberos
- Netlogon
- Zeitsynchronisation
- AD-Replikation
- SYSVOL-Replikation
- Gruppenrichtlinien
- DHCP
- DFS und DFS-Replikation
- Zertifikatsdienste
- Netzwerkverbindungen und Firewalls
- Failovercluster
- Serverrollen und deren Datenbanken

Ein erfolgreicher Ping beweist weder eine funktionierende Domänenanmeldung noch eine fehlerfreie AD-Replikation. Ebenso beweist eine erfolgreiche Anmeldung nicht, dass alle Gruppenrichtlinien, DNS-Zonen oder Verzeichnisänderungen korrekt repliziert wurden.

Kennzeichnung der Befehle

Kennzeichnung	Bedeutung
`[RO]`	grundsätzlich nur lesende Diagnose
`[TEST]`	erzeugt Testzugriffe oder zusätzliche Protokolle
`[CHANGE]`	verändert Konfiguration, Cache oder Systemzustand
`[PRIV]`	erhöhte oder administrative Rechte erforderlich beziehungsweise sinnvoll
`[REMOTE]`	greift auf einen anderen Computer oder Dienst zu
`[SENS]`	Ausgabe kann interne oder personenbezogene Informationen enthalten
`[LOG]`	kann umfangreiche zusätzliche Protokolldaten erzeugen

Kennzeichnung	Bedeutung
[DANGER]	fehlerhafte Verwendung kann größere Störungen verursachen
[RESTART]	kann einen Neustart oder eine Dienstunterbrechung erfordern

Die Kennzeichnungen sind Sicherheitshinweise dieser Dokumentation und nicht Bestandteil der eigentlichen Befehle.

---

1. Abhängigkeiten einer Windows-Domäne verstehen

Eine typische Domänenanmeldung umfasst mehrere Schritte:

1. Der Client ermittelt über DNS einen geeigneten Domain Controller.
2. Der DC-Locator berücksichtigt Domäne, Standort und verfügbare Dienste.
3. Client und Domain Controller prüfen ihre Vertrauensbeziehung.
4. Kerberos oder NTLM authentifiziert den Benutzer.
5. Active Directory liefert Benutzer-, Computer- und Gruppeninformationen.
6. SYSVOL stellt Gruppenrichtliniendateien und Anmeldeskripte bereit.
7. Der Gruppenrichtliniendienst ermittelt und verarbeitet passende GPOs.
8. Weitere Dienste stellen Profile, Laufwerke, Drucker oder Anwendungen bereit.

Daraus ergibt sich eine wichtige Diagnose-Reihenfolge:

1. lokaler Netzwerkzustand
2. IP-Konfiguration
3. DNS-Clientkonfiguration
4. DNS-Auflösung der Domänendienste
5. Erreichbarkeit eines geeigneten Domain Controllers
6. Uhrzeit und Zeitzone
7. Secure Channel
8. Kerberos-Tickets und SPNs
9. AD-Replikation
10. SYSVOL und DFS-Replikation
11. Gruppenrichtlinienverarbeitung
12. abhängige Serverrollen

> In Active Directory ist DNS Bestandteil der Dienstermittlung. Ein Client, der ausschließlich einen öffentlichen DNS-Server verwendet, kann zwar Internetnamen auflösen, aber normalerweise die internen Domänendienste nicht korrekt ermitteln.

2. Diagnosekontext und Ausgangslage dokumentieren

Vor der ersten Änderung müssen mindestens folgende Angaben erfasst werden:

- betroffener Benutzer
- betroffener Computer
- Domänenname
- Active-Directory-Standort
- verwendeter Domain Controller
- Zeitpunkt des Fehlers
- originale Fehlermeldung
- betroffene Anwendung oder Ressource
- einmalige oder wiederkehrende Störung
- Anzahl betroffener Systeme
- letzte bekannte funktionierende Nutzung
- letzte administrative Änderung
- kürzlich installierte Updates
- Netzwerksegment und VPN-Zustand
- Anmeldung lokal, zwischengespeichert oder gegen einen Domain Controller
- administrative oder normale Benutzersitzung

Grundinformationen auf einem Client

```
[RO][SENS] hostname
[RO][SENS] whoami
[RO][SENS] whoami /upn
[RO][SENS] whoami /user
[RO][SENS] whoami /groups
[RO][SENS] systeminfo
[RO][SENS] ipconfig /all
```

Domäneninformationen mit PowerShell

```
[RO][SENS] Get-CimInstance Win32_ComputerSystem |
    Select-Object Name, Domain, PartOfDomain
```

Anmelde- und Logonserver-Variablen

```
[RO][SENS] set LOGONSERVER
[RO][SENS] set USERDNSDOMAIN
```

```
[RO][SENS] set USERDOMAIN
```

> Die Variable `LOGONSERVER` ist ein nützlicher Hinweis, aber keine vollständige Aussage darüber, welcher Domain Controller bei allen späteren LDAP-, Kerberos-, DNS- oder GPO-Vorgängen verwendet wird.

3. Ereignisprotokolle gezielt untersuchen

Wichtige Protokolle befinden sich in der Ereignisanzeige unter:

```
Ereignisanzeige
├── Windows-Protokolle
│   ├── Anwendung
│   ├── Sicherheit
│   └── System
└── Anwendungs- und Dienstprotokolle
    └── Microsoft
        └── Windows
```

Relevante Protokollbereiche können sein:

- ActiveDirectory_DomainService
- DNS-Server
- Directory Service
- DFS Replication
- GroupPolicy
- Kerberos
- KDC
- Netlogon
- Time-Service
- DHCP-Server
- FailoverClustering
- ServerManager
- CertificateServicesClient
- TerminalServices
- SMBClient und SMBServer

GroupPolicy-Betriebsprotokoll

```
Anwendungs- und Dienstprotokolle
└── Microsoft
    └── Windows
        └── GroupPolicy
            └── Operational
```

Ereignisse per PowerShell abrufen

```
[RO][PRIV][SENS] Get-WinEvent -LogName System -MaxEvents 100
```

```
[RO][PRIV][SENS] Get-WinEvent -LogName "Microsoft-Windows-GroupPolicy/Operational" -MaxEvents 100
```

Nach Zeitraum und Ebene filtern

```
[RO][PRIV][SENS] Get-WinEvent -FilterHashtable @{
    LogName   = "System"
    StartTime = (Get-Date).AddHours(-2)
    Level     = 2,3
}
```

Verfügbare Protokolle suchen

```
[RO][SENS] Get-WinEvent -ListLog * |
    Where-Object LogName -match "GroupPolicy|DNS|DFS|Kerberos|Netlogon|Failover"
```

> Ereignis-IDs dürfen nicht isoliert interpretiert werden. Quelle, Windows-Version, Ereignistext, Fehlercode, Zeitpunkt und begleitende Ereignisse müssen gemeinsam ausgewertet werden.

4. Domain Controller mit DCDiag prüfen

`dcdiag` führt verschiedene Tests für Domain Controller aus. Abhängig von den Parametern werden unter anderem Erreichbarkeit, DNS, Replikation, Dienste, Rolleninhaber und Verzeichnispartitionen geprüft.

Grundprüfung des lokalen Domain Controllers

```
[TEST][PRIV][SENS] dcdiag
```

Ausführliche Ausgabe

```
[TEST][PRIV][SENS] dcdiag /v
```

Bestimmten Domain Controller prüfen

```
[TEST][PRIV][REMOTE][SENS] dcdiag /s:<DC-NAME>
```

Alle Domain Controller des Unternehmensbereichs prüfen

```
[TEST][PRIV][REMOTE][SENS] dcdiag /e
```

DNS-Tests ausführen

```
[TEST][PRIV][REMOTE][SENS] dcdiag /test:DNS /e /v
```

Bestimmten Test ausführen

```
[TEST][PRIV][SENS] dcdiag /test:<TESTNAME>
```

Ausgabe in Dateien schreiben

```
[TEST][PRIV][SENS] dcdiag /v /f:"<AUSGABEDATEI>"
```

Wichtige Bewertungsfragen

- Welcher konkrete Test ist fehlgeschlagen?
- Welcher Domain Controller wurde geprüft?
- Welcher Partner oder Dienst war beteiligt?
- Handelt es sich um einen aktuellen oder historischen Fehler?
- Ist DNS korrekt konfiguriert?
- Sind notwendige Dienste gestartet?
- Funktioniert die Replikation aller Verzeichnispartitionen?

- Sind die FSMO-Rolleninhaber erreichbar?
- Ist SYSVOL freigegeben?
- Tritt der Fehler auf allen DCs oder nur auf einem DC auf?

> `dcdiag` liefert mehrere unabhängige Testergebnisse. Eine einzelne Warnung beweist nicht automatisch einen Gesamtausfall des Domain Controllers.

5. AD-Replikation mit Repadmin untersuchen

Active Directory ist ein Multi-Master-Verzeichnis. Änderungen werden zwischen Domain Controllern repliziert. Fehler können dazu führen, dass Benutzer, Gruppen, Kennwörter, Computerobjekte oder DNS-Daten auf verschiedenen DCs unterschiedliche Stände besitzen.

Gesamtübersicht

```
[RO][PRIV][REMOTE][SENS] repadmin /replsummary
```

Die Ausgabe zeigt unter anderem:

- Quell- und Ziel-DCs
- Anzahl fehlgeschlagener Replikationen
- Fehlerquote
- größte Replikationsverzögerung
- Fehlercode

Eingehende Replikationspartner anzeigen

```
[RO][PRIV][REMOTE][SENS] repadmin /showrepl
```

Bestimmten Domain Controller untersuchen

```
[RO][PRIV][REMOTE][SENS] repadmin /showrepl <DC-NAME>
```

Alle Domain Controller ausführlich untersuchen

```
[RO][PRIV][REMOTE][SENS] repadmin /showrepl * /csv
```

Replikationswarteschlange anzeigen

```
[RO][PRIV][SENS] repadmin /queue
```

Replikationsmetadaten eines Objekts untersuchen

```
[RO][PRIV][REMOTE][SENS] repadmin /showobjmeta <DC-NAME> "<DISTINGUISHED-NAME>"
```

Replikation anstoßen

```
[CHANGE][PRIV][REMOTE] repadmin /syncall <DC-NAME> /AdeP
```

Dieser Befehl darf nicht als erster Diagnoseschritt verwendet werden. Er verändert zwar keine AD-Objektinhalte direkt, löst aber Replikationsvorgänge aus und kann Netzwerk- sowie Systemlast erzeugen.

Typische Fehlerbereiche

Fehler oder Beobachtung	Möglicher Prüfbereich
RPC-Server nicht verfügbar	DNS, Firewall, RPC, Routing, Dienste
Zugriff verweigert	Secure Channel, Kerberos, Berechtigungen, Zeit
Zielprinzipalname falsch	SPN, Computerkontokennwort, DNS, Kerberos
DNS-Nachschlagefehler	DNS-Client, Zonen, SRV-Records, Registrierung
große Replikationsverzögerung	Standortverbindungen, Zeitplan, Erreichbarkeit
nur eine Partition betroffen	Namenskontext und zuständiger Replikationspfad
nur ein DC betroffen	lokaler Dienst, DNS, Datenbank oder Netzwerkpfad

> Eine manuell erfolgreich ausgelöste Replikation beweist nicht, dass Topologie, Zeitplan und automatische Replikation dauerhaft funktionieren.

6. Domain Controller über den DC-Locator ermitteln

Der DC-Locator ermittelt anhand von DNS-Daten, Domäne, Standort und Anforderungen einen geeigneten Domain Controller.

Domain Controller ermitteln

```
[TEST][SENS] nltest /dsgetdc:<DOMÄNE>
```

Beispiel:

```
[TEST][SENS] nltest /dsgetdc:example.internal
```

Ermittlung neu durchführen

```
[CHANGE][SENS] nltest /dsgetdc:<DOMÄNE> /force
```

Domain Controller auflisten

```
[RO][SENS] nltest /dclist:<DOMÄNE>
```

Standort des Computers anzeigen

```
[RO][SENS] nltest /dsgetsite
```

Standortabdeckung eines DCs untersuchen

```
[RO][SENS] nltest /dsgetsite
```

DNS-SRV-Einträge prüfen

```
[TEST][SENS] nslookup -type=SRV _ldap._tcp.dc._msdcs.<DOMÄNE>
```

```
[TEST][SENS] nslookup -type=SRV _kerberos._tcp.<DOMÄNE>
```

Zu prüfen sind:

- werden mehrere erwartete Domain Controller geliefert?
- stimmen Namen und IP-Adressen?
- wird ein DC des erwarteten Standorts bevorzugt?
- existieren veraltete Einträge?

- sind LDAP- und Kerberos-SRV-Records vorhanden?
- verwendet der Client ausschließlich interne DNS-Server?
- erreicht der Client die ausgegebenen Server?

> Das direkte Eintragen eines Domain Controllers in die Hosts-Datei ersetzt die DNS-basierte Dienstermittlung nicht und kann die eigentliche Ursache verdecken.

7. Secure Channel prüfen

Domänenmitglieder besitzen ein Computerkonto mit einem Kennwort. Der Secure Channel verwendet diese Vertrauensbeziehung für die Kommunikation mit der Domäne.

Secure Channel mit NLTest prüfen

```
[TEST][PRIV][REMOTE][SENS] nltest /sc_verify:<DOMÄNE>
```

Vertraute Domäne abfragen

```
[RO][PRIV][SENS] nltest /sc_query:<DOMÄNE>
```

PowerShell-Prüfung auf einem Domänenmitglied

```
[TEST][PRIV][REMOTE] Test-ComputerSecureChannel -Verbose
```

`Test-ComputerSecureChannel` ist für Domänenmitglieder vorgesehen. Die Interpretation auf Domain Controllern unterscheidet sich, weil DCs eigene Replikations- und Vertrauensmechanismen verwenden.

Reparatur mit PowerShell

```
[CHANGE][PRIV][REMOTE][DANGER] Test-ComputerSecureChannel -Repair -Credential
"<DOMÄNE>\<ADMIN-KONTO>"
```

Vor einer Reparatur müssen geprüft werden:

- DNS-Konfiguration

- Erreichbarkeit eines Domain Controllers
- Uhrzeit
- Computerkonto im Active Directory
- mögliche doppelte Computernamen
- Wiederherstellung eines alten VM-Snapshots
- kürzlich erfolgte Domänenwiederaufnahme
- verwendete administrative Anmeldeinformationen
- Auswirkungen auf Dienste und geplante Aufgaben

> Ein Computer sollte nicht vorschnell aus der Domäne entfernt und wieder aufgenommen werden. Dadurch können Computerkonto, Zertifikate, lokale Profile, verschlüsselte Daten, Dienstkonten und Verwaltungszuordnungen beeinflusst werden.

8. DNS-Clientkonfiguration der Domänenmitglieder prüfen

Vollständige IP-Konfiguration

```
[RO][SENS] ipconfig /all
```

PowerShell-Übersicht

```
[RO][SENS] Get-DnsClientServerAddress
```

```
[RO][SENS] Get-NetIPConfiguration
```

Zu prüfen sind:

- verwendete DNS-Server
- Reihenfolge der DNS-Server
- DNS-Suffix
- verbindungsspezifisches DNS-Suffix
- Registrierung der Adresse
- mehrere aktive Netzwerkadapter
- VPN-Adapter
- virtuelle Adapter
- fehlerhafte statische Einstellungen
- DHCP-Optionen

- Erreichbarkeit der eingetragenen DNS-Server

DNS-Clientcache anzeigen

```
[RO][SENS] ipconfig /displaydns
```

DNS-Clientcache leeren

```
[CHANGE] ipconfig /flushdns
```

Das Leeren des Caches kann einen neuen Auflösungsversuch erzwingen, beseitigt aber keine fehlerhafte Zone, falsche Delegierung oder falsche DNS-Clientkonfiguration.

DNS-Namen prüfen

```
[TEST][SENS] Resolve-DnsName "<HOSTNAME>"
```

```
[TEST][SENS] Resolve-DnsName "<FQDN>" -Type A
```

```
[TEST][SENS] Resolve-DnsName "_ldap._tcp.dc._msdcs.<DOMÄNE>" -Type SRV
```

> Ein Domänenclient sollte nicht ohne geplante interne DNS-Weiterleitung öffentliche DNS-Resolver zusätzlich zu internen AD-DNS-Servern verwenden. Windows behandelt mehrere eingetragene DNS-Server nicht als einfache interne-und-externe Suchreihenfolge.

9. DNS-Server und AD-integrierte Zonen untersuchen

Wichtige Prüfbereiche im DNS-Manager:

- Forward-Lookupzonen
- Reverse-Lookupzonen
- AD-integrierte Zonen
- Replikationsbereich der Zone
- dynamische Updates
- sichere dynamische Updates

- Weiterleitungen
- bedingte Weiterleitungen
- Stammhinweise
- veraltete Hosteinträge
- SRV-Einträge
- Delegierungen
- Alterung und Aufräumvorgänge
- DNSSEC, falls verwendet

DNS-Serverzonen mit PowerShell anzeigen

```
[RO][PRIV][SENS] Get-DnsServerZone
```

Ressourceneinträge einer Zone anzeigen

```
[RO][PRIV][SENS] Get-DnsServerResourceRecord -ZoneName "<ZONE>"
```

DNS-Servereinstellungen anzeigen

```
[RO][PRIV][SENS] Get-DnsServer
```

Weiterleitungen anzeigen

```
[RO][PRIV][SENS] Get-DnsServerForwarder
```

DNS-Diagnose mit DCDiag

```
[TEST][PRIV][SENS] dcdiag /test:DNS /v
```

DNS-Registrierung eines Domänenmitglieds anfordern

```
[CHANGE] ipconfig /registerdns
```

Auf einem Domain Controller kann außerdem eine erneute Registrierung domänenbezogener Einträge erforderlich sein. Dienstneustarts dürfen jedoch erst nach Prüfung der Auswirkungen erfolgen.

DNS-Debugprotokollierung

Die DNS-Debugprotokollierung kann sehr viele Daten und interne Abfragen erfassen. Sie sollte:

1. nur mit einem konkreten Fehlerbild aktiviert werden,
2. nach Client, Protokoll oder Pakettyp begrenzt werden,
3. nur so lange wie erforderlich laufen,
4. hinsichtlich Speicherplatz überwacht werden,
5. anschließend wieder deaktiviert werden.

```
[CHANGE][PRIV][LOG][SENS]
```

> DNS-Debuglogs können interne Hostnamen, abgefragte Dienste, Clientadressen und Benutzeraktivitäten offenlegen.

10. Netlogon-Protokollierung kontrolliert verwenden

Netlogon ist unter anderem an Domänenanmeldung, DC-Locator und Secure-Channel-Vorgängen beteiligt.

Eine erweiterte Netlogon-Protokollierung darf nur zeitlich begrenzt aktiviert werden.

Aktuellen Netlogon-Zustand prüfen

```
[RO][PRIV] sc query netlogon
```

Netlogon-Diagnoseprotokollierung aktivieren

```
[CHANGE][PRIV][LOG][SENS] nltest /dbflag:0x2080ffff
```

Protokollierung wieder auf den Standardzustand zurücksetzen

```
[CHANGE][PRIV] nltest /dbflag:0x0
```

Das Protokoll befindet sich typischerweise unter:

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

Vor und während der Aufzeichnung müssen geprüft werden:

- freier Speicherplatz
- Aufzeichnungsdauer
- konkreter Fehlerzeitpunkt
- betroffener Benutzer und Computer
- Schutz der Protokolldatei
- anschließende Deaktivierung

> Der Debug-Schalter darf nicht unkontrolliert dauerhaft aktiviert bleiben. Die Datei kann umfangreich werden und interne Domäneninformationen enthalten.

11. Kerberos-Tickets mit Klist untersuchen

Kerberos verwendet Tickets zur Authentifizierung. Dabei sind unter anderem Client, Key Distribution Center, Zielservice, SPN, Uhrzeit und DNS beteiligt.

Tickets des aktuellen Anmeldekontexts anzeigen

```
[RO][SENS] klist
```

Ticket Granting Tickets anzeigen

```
[RO][SENS] klist tgt
```

Kerberos-Sitzungen anzeigen

```
[RO][SENS] klist sessions
```

Tickets löschen

```
[CHANGE][SENS] klist purge
```

Das Löschen der Tickets beeinflusst den aktuellen Authentifizierungskontext. Anwendungen müssen danach möglicherweise neue Tickets anfordern.

Ticket für einen Dienst anfordern

```
[TEST][REMOTE][SENS] klist get <SPN>
```

Typische Prüfungen

- wurde ein TGT ausgestellt?
- welcher KDC hat das Ticket ausgestellt?
- für welchen SPN wurde ein Serviceticket ausgestellt?
- ist das Ticket abgelaufen?
- stimmen Client- und Servernamen?
- wurde auf NTLM zurückgefallen?
- tritt der Fehler nur mit Aliasnamen auf?
- funktioniert der Zugriff mit FQDN, aber nicht mit Kurzname?
- befindet sich ein altes Ticket im Cache?
- stimmt die Uhrzeit?

> `klist purge` ist keine Ursachenbehebung. Wenn DNS, SPN, Zeit oder Kontokonfiguration fehlerhaft sind, tritt das Problem nach Ausstellung neuer Tickets erneut auf.

12. Service Principal Names mit SetSPN prüfen

Ein SPN identifiziert eine Dienstinstanz für Kerberos. Er muss dem richtigen AD-Konto eindeutig zugeordnet sein.

SPNs eines Kontos anzeigen

```
[RO][PRIV][SENS] setspn -L "<KONTO>"
```

Bestimmten SPN suchen

```
[RO][PRIV][SENS] setspn -Q "<SPN>"
```

Forestweit nach doppelten SPNs suchen

```
[RO][PRIV][REMOTE][SENS] setspn -X
```

SPN mit Duplikatprüfung registrieren

```
[CHANGE][PRIV][DANGER] setspn -S "<SPN>" "<KONTO>"
```

SPN entfernen

```
[CHANGE][PRIV][DANGER] setspn -D "<SPN>" "<KONTO>"
```

Vor jeder Änderung müssen geprüft werden:

- vollständiger SPN
- Dienstklasse
- Hostname und FQDN
- Port, falls Teil des SPN
- tatsächlich verwendetes Dienstkonto
- bestehende Zuordnung
- Cluster-, Alias- oder Load-Balancer-Namen
- Auswirkungen auf andere Dienstinstanzen
- Replikationsstatus

Typische Kerberos-Probleme entstehen durch:

- fehlenden SPN
- doppelten SPN
- SPN auf falschem Konto
- Dienst läuft unter anderem Konto als erwartet
- DNS-Alias ohne passende SPN-Konfiguration
- altes Computerkonto
- nicht replizierte SPN-Änderung
- falschen Zielnamen der Anwendung

> SPNs dürfen nicht durch Ausprobieren auf verschiedene Konten geschrieben werden. Eine falsche Zuordnung kann die Kerberos-Authentifizierung mehrerer Systeme beeinträchtigen.

13. Zeitsynchronisation mit W32Time prüfen

Kerberos benötigt ausreichend übereinstimmende Zeitangaben. In einer AD-Domäne folgt die Zeithierarchie grundsätzlich der Domänenhierarchie. Der PDC-Emulator der Gesamtstruktur-

Stammdomäne besitzt dabei eine besondere Rolle.

Status anzeigen

```
[RO][SENS] w32tm /query /status
```

Zeitquelle anzeigen

```
[RO][SENS] w32tm /query /source
```

Konfiguration anzeigen

```
[RO][SENS] w32tm /query /configuration
```

Peers anzeigen

```
[RO][SENS] w32tm /query /peers
```

Domänenhierarchie überwachen

```
[TEST][REMOTE][SENS] w32tm /monitor
```

Abweichung zu einem Computer messen

```
[TEST][REMOTE][SENS] w32tm /stripchart /computer:<COMPUTER> /dataonly /samples:10
```

Neue Synchronisation anfordern

```
[CHANGE][PRIV][REMOTE] w32tm /resync
```

Zu prüfen sind:

- verwendete Zeitquelle
- letzte erfolgreiche Synchronisation
- aktuelle Zeitabweichung
- Zeitzone
- PDC-Emulator
- Virtualisierung und Hypervisor-Zeitquelle

- NTP-Erreichbarkeit
- Firewall
- kürzlich wiederhergestellte VM
- manuelle Zeitkonfiguration
- Dienstzustand

FSMO-Rollen anzeigen

```
[RO][PRIV][SENS] netdom query fsmo
```

> Die manuelle Konfiguration externer Zeitserver auf allen Domänenmitgliedern kann die vorgesehene AD-Zeithierarchie umgehen. Änderungen müssen passend zur Rolle des Systems geplant werden.

14. Gruppenrichtlinienergebnis mit GPResult untersuchen

`gpresult` zeigt die Resultant Set of Policy, also die ermittelten Gruppenrichtlinienergebnisse für Computer und Benutzer.

Zusammenfassung

```
[RO][SENS] gpresult /r
```

Ausführliche Ausgabe

```
[RO][SENS] gpresult /v
```

Maximal ausführliche Textausgabe

```
[RO][SENS] gpresult /z
```

HTML-Bericht erzeugen

```
[RO][SENS] gpresult /h "<BERICHT>.html"
```

Nur Computerrichtlinien anzeigen

```
[RO][PRIV][SENS] gpresult /scope computer /r
```

Nur Benutzerrichtlinien anzeigen

```
[RO][SENS] gpresult /scope user /r
```

Bericht für einen anderen Benutzer

```
[RO][PRIV][SENS] gpresult /user "<DOMÄNE>\<BENUTZER>" /h "<BERICHT>.html"
```

Wichtige Auswertungsbereiche:

- angewendete GPOs
- abgelehnte GPOs
- Ablehnungsgrund
- Sicherheitsgruppen
- Benutzer- und Computer-OU
- langsame oder schnelle Netzwerkverbindung
- WMI-Filter
- Vererbungsinformationen
- Loopback-Verarbeitung
- Richtlinienrevision
- letzter Verarbeitungszeitpunkt
- verwendeter Domain Controller

> Eine GPO kann in der Gruppenrichtlinienverwaltung vorhanden und mit einer OU verknüpft sein, ohne auf das untersuchte Objekt angewendet zu werden.

15. Gruppenrichtlinienabruf mit GPUpdate testen

Normale Aktualisierung

```
[CHANGE][REMOTE] gpupdate
```

Alle Richtlinieneinstellungen erneut verarbeiten

```
[CHANGE][REMOTE] gpupdate /force
```

Zeitlimit festlegen

```
[CHANGE][REMOTE] gpupdate /wait:<SEKUNDEN>
```

Abmeldung zulassen, falls erforderlich

```
[CHANGE][REMOTE] gpupdate /logoff
```

Neustart zulassen, falls erforderlich

```
[CHANGE][REMOTE][RESTART] gpupdate /boot
```

`gpupdate /force` sollte nicht reflexartig auf vielen Systemen gleichzeitig ausgeführt werden. Es kann:

- zusätzliche DC- und Netzwerkbelastung erzeugen
- Skripte erneut ausführen
- Softwareinstallation anstoßen
- Abmeldung oder Neustart erforderlich machen
- bestehende Sitzungen beeinflussen
- Drucker- und Laufwerkszuordnungen erneut verarbeiten

Empfohlener Testablauf

1. `gpresult` vor der Aktualisierung speichern.
2. Fehlerzeitpunkt dokumentieren.
3. Ereignisprotokoll prüfen.
4. `gpupdate` auf einem kontrollierten Testsystem ausführen.
5. Meldungen vollständig dokumentieren.
6. erforderliche Abmeldung oder Neustart berücksichtigen.
7. `gpresult` erneut erzeugen.
8. vorherigen und nachfolgenden Zustand vergleichen.

16. Warum eine GPO nicht angewendet wird

Mögliche Ursachen:

- Benutzer oder Computer befindet sich in der falschen OU.
- GPO ist mit einer anderen OU verknüpft.
- Verknüpfung ist deaktiviert.
- Benutzer- oder Computerteil der GPO ist deaktiviert.
- Sicherheitsfilter schließt das Objekt aus.
- notwendige Rechte `Lesen` oder `Gruppenrichtlinie übernehmen` fehlen.
- WMI-Filter liefert `False` oder kann nicht ausgewertet werden.
- Vererbung wurde blockiert.
- eine erzwungene GPO beeinflusst die Vererbungsreihenfolge.
- eine Richtlinie mit höherer Priorität überschreibt die Einstellung.
- Loopback-Verarbeitung verändert die Benutzerrichtlinien.
- Client erreicht keinen Domain Controller.
- DNS oder Secure Channel ist fehlerhaft.
- SYSVOL ist nicht erreichbar.
- AD- und SYSVOL-Replikation besitzen unterschiedliche Stände.
- Client Side Extension benötigt synchrone Verarbeitung.
- Richtlinie wird erst nach Abmeldung oder Neustart wirksam.
- Fast Startup beeinflusst den erwarteten Startvorgang.
- Anwendung liest die Einstellung nur beim Start.
- Einstellung gilt nicht für die verwendete Windows-Version oder Edition.
- ADMX-Vorlage und tatsächlich unterstützte Einstellung passen nicht zusammen.

Prüfreihenfolge

1. Objekt und OU bestätigen.
2. GPO-Verknüpfung bestätigen.
3. GPO-Status prüfen.
4. Sicherheitsfilter prüfen.
5. Delegierung prüfen.
6. WMI-Filter prüfen.
7. Vererbung und Reihenfolge prüfen.
8. `gpresult` auswerten.
9. GroupPolicy-Betriebsprotokoll auswerten.
10. DNS, DC-Locator und SYSVOL testen.
11. AD- und DFS-R-Replikation prüfen.
12. erforderliche Abmeldung oder Neustart testen.

17. GPO-Verarbeitung fachgerecht dokumentieren

Für jede untersuchte Gruppenrichtlinie sollten folgende Angaben erfasst werden:

Aufgabe:

Betroffener Benutzer:

Betroffener Computer:

Domäne:

Standort:

Verwendeter Domain Controller:

Name der GPO:

GPO-ID:

GPO-Status:

Benutzer- oder Computerkonfiguration:

Verknüpfte OU:

Verknüpfungsreihenfolge:

Verknüpfung aktiviert:

Erzwungen:

Vererbung blockiert:

Sicherheitsfilter:

Delegierung:

WMI-Filter:

Loopback-Modus:

Pfad der Richtlinieneinstellung:

Konfigurierte Einstellung:

Erwarteter Wert:

Tatsächlicher Wert:

GPResult vor dem Test:

GPUpdate-Ergebnis:

Abmeldung erforderlich:

Neustart erforderlich:

GPResult nach dem Test:

GroupPolicy-Ereignisse:

SYSVOL erreichbar:

AD-Replikation geprüft:

DFS-R-Replikation geprüft:

Ursache:

Änderung:

Rückfallplan:

Testergebnis:

18. SYSVOL und NETLOGON prüfen

SYSVOL enthält unter anderem Gruppenrichtliniendateien und Skripte. Active Directory speichert den Verzeichnisanteil einer GPO, während SYSVOL den Dateianteil enthält. Beide Teile müssen konsistent und repliziert sein.

Freigaben eines Domain Controllers anzeigen

```
[RO][REMOTE][SENS] net view \\<DC-NAME>
```

Erwartete Domänencontroller-Freigaben sind normalerweise:

- `SYSVOL`
- `NETLOGON`

SYSVOL öffnen

```
[TEST][REMOTE][SENS] dir \\<DC-NAME>\SYSVOL
```

NETLOGON öffnen

```
[TEST][REMOTE][SENS] dir \\<DC-NAME>\NETLOGON
```

Bestimmte Richtlinie prüfen

```
[RO][REMOTE][SENS] dir "\\<DC-NAME>\SYSVOL\<DOMÄNE>\Policies\{<GPO-GUID>}"
```

Zu vergleichen sind:

- Existenz des GPO-Verzeichnisses
- GPO-GUID
- Inhalt auf mehreren Domain Controllern
- Zeitstempel
- `GPT.INI`
- Skripte
- Registry-Policy-Dateien

- Zugriffsrechte
- DFS-R-Ereignisse

> Dateien in SYSVOL dürfen nicht als normale Konfigurationsmethode manuell auf mehreren Domain Controllern bearbeitet oder kopiert werden. Dadurch können AD- und Dateianteil einer GPO inkonsistent werden.

19. DFS-Replikation von SYSVOL untersuchen

Moderne Windows-Domänen verwenden DFS Replication für SYSVOL. Wichtige Datenquellen sind:

- Ereignisprotokoll `DFS Replication`
- DFS-Verwaltung
- `dfsrdiag`
- PowerShell
- AD-Replikationszustand
- Zustand der SYSVOL- und NETLOGON-Freigaben

DFS-R-Zustand abfragen

```
[RO][PRIV][SENS] dfsrdiag ReplicationState
```

Konfiguration neu aus Active Directory einlesen

```
[CHANGE][PRIV] dfsrdiag PollAD
```

DFS-R-Ereignisse abrufen

```
[RO][PRIV][SENS] Get-WinEvent -LogName "DFS Replication" -MaxEvents 200
```

Typische Prüfbereiche:

- Replikationsgruppe
- replizierter Ordner
- eingehender und ausgehender Partner
- Rückstand
- pausierte Replikation

- Datenbankzustand
- nicht ordnungsgemäß heruntergefahrener Server
- Kommunikationsfehler
- AD-Konfiguration noch nicht eingelesen
- Speicherplatz
- USN- oder Datenbankprobleme

> Eine DFS-R-Wiederherstellung oder autoritative SYSVOL-Synchronisierung ist eine eingriffsintensive Maßnahme. Sie darf erst nach gesicherter Diagnose, aktueller Sicherung und dokumentiertem Wiederherstellungsplan durchgeführt werden.

20. DHCP-Server untersuchen

DHCP-Probleme können dazu führen, dass Clients:

- keine Adresse erhalten
- eine APIPA-Adresse verwenden
- falsches Gateway erhalten
- falsche DNS-Server verwenden
- falsches DNS-Suffix erhalten
- ihre Lease nicht verlängern können
- aus einem falschen Bereich versorgt werden
- aufgrund ausgeschöpfter Bereiche keine Adresse erhalten

DHCP-Konfiguration auf dem Client

```
[RO][SENS] ipconfig /all
```

Lease freigeben

```
[CHANGE] ipconfig /release
```

Lease erneuern

```
[CHANGE][REMOTE] ipconfig /renew
```

Diese Befehle unterbrechen die aktuelle IP-Konnektivität und sollten nicht unüberlegt über eine entfernte Verwaltungssitzung ausgeführt werden.

DHCP-Server anzeigen

```
[RO][PRIV][SENS] Get-DhcpServerInDC
```

IPv4-Bereiche anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-DhcpServerv4Scope -ComputerName "<DHCP-SERVER>"
```

Leases anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-DhcpServerv4Lease -ComputerName "<DHCP-SERVER>" -ScopeId "<NETZ-ID>"
```

Bereichsstatistik anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-DhcpServerv4ScopeStatistics -ComputerName "<DHCP-SERVER>"
```

Serveroptionen anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-DhcpServerv4OptionValue -ComputerName "<DHCP-SERVER>"
```

Zu prüfen sind:

- DHCP-Autorisierung in Active Directory
- Dienstzustand
- Bereich aktiviert
- verfügbarer Adressvorrat
- Ausschlussbereiche
- Reservierungen
- Lease-Dauer
- Option 003 – Router
- Option 006 – DNS-Server
- Option 015 – DNS-Domänenname
- Relay-Agent oder IP Helper
- DHCP-Failover
- Konflikterkennung

- mehrere unerwartete DHCP-Server
- Auditprotokolle

> DHCP-Debug- und Auditlogs können MAC-Adressen, Hostnamen, IP-Adressen und zeitliche Gerätenutzung enthalten und müssen entsprechend geschützt werden.

21. DFS-Namespace und DFS-Replikation unterscheiden

DFS besteht aus unterschiedlichen Funktionen:

Komponente	Aufgabe
DFS Namespace	stellt einen einheitlichen logischen Pfad bereit
DFS Replication	repliziert Ordnerinhalte zwischen Servern

Ein erreichbarer Namespace beweist nicht, dass alle Replikationspartner denselben Datenstand besitzen. Umgekehrt beweist ein gesunder DFS-R-Status nicht, dass Namespace-Ziele, Berechtigungen und Verweise korrekt funktionieren.

Namespacepfad testen

```
[TEST][REMOTE][SENS] dir "\\<DOMÄNE>\<NAMESPACE>"
```

DFS-Ziele und Verweise untersuchen

```
[RO][SENS] dfsutil /pktinfo
```

Zwischengespeicherte Verweise leeren

```
[CHANGE] dfsutil /pktflush
```

Typische Prüfbereiche

- DNS-Auflösung
- Namespace-Server
- Ordnerziele
- Zielstatus

- Standortkosten
- Referral-Reihenfolge
- SMB-Erreichbarkeit
- Freigabeberechtigungen
- NTFS-Berechtigungen
- DFS-R-Rückstand
- Dateisperren
- Konflikt- und gelöschte Ordner
- Staging-Speicher

22. Failovercluster untersuchen

Ein Failovercluster besteht aus mehreren voneinander abhängigen Komponenten:

- Clusterknoten
- Clusterdienst
- Quorum
- Witness
- Cluster-Netzwerke
- Speicher
- Cluster Shared Volumes
- Ressourcen
- Rollen
- Abhängigkeiten
- DNS
- Active-Directory-Computerobjekte
- Anwendungen

Cluster anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-Cluster
```

Knoten anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-ClusterNode
```

Clustergruppen anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-ClusterGroup
```

Ressourcen anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-ClusterResource
```

Quorum anzeigen

```
[RO][PRIV][REMOTE][SENS] Get-ClusterQuorum
```

Clusterprotokoll erzeugen

```
[TEST][PRIV][REMOTE][LOG][SENS] Get-ClusterLog -UseLocalTime -Destination "<VERZEICHNIS>"
```

Cluster validieren

```
[TEST][PRIV][REMOTE][LOG][SENS] Test-Cluster
```

Die vollständige Validierung kann Netzwerk-, Speicher- und Systemtests durchführen. Umfang und Auswirkungen müssen vor dem Start geprüft werden.

Typische Diagnosefragen

- Welche Ressource ist zuerst ausgefallen?
- Welche abhängigen Ressourcen folgten?
- Welcher Knoten war Besitzer?
- War Quorum vorhanden?
- War der Witness erreichbar?
- trat ein Netzwerk- oder Speicherfehler auf?
- konnte das Clustercomputerobjekt DNS-Daten aktualisieren?
- stimmen Ereigniszeit und Clusterlog überein?
- war der Failover geplant oder ungeplant?
- funktioniert die Anwendung nach dem Ressourcenstart tatsächlich?

> Das manuelle Verschieben oder Neustarten einer Clusterrolle ist eine Änderung am produktiven Dienst und keine rein lesende Diagnose.

23. Server Manager und Windows Admin Center richtig einordnen

Server Manager

Server Manager kann unter anderem anzeigen:

- Serverrollen
- Features
- verwaltete Server
- Dienstzustände
- Ereignisse
- Leistungswarnungen
- Best-Practices-Ergebnisse
- Rolleninstallationen

Windows Admin Center

Windows Admin Center kann abhängig von Version und Erweiterungen unter anderem verwalten:

- Server
- Cluster
- virtuelle Maschinen
- Zertifikate
- Ereignisse
- Dienste
- Speicher
- Netzwerke
- Updates
- Firewall
- Registry
- PowerShell

Grenzen

- eine grüne Übersicht ersetzt keine Detailprüfung
- Daten können verzögert aktualisiert werden
- Remoteverwaltung hängt von WinRM, Berechtigungen und Firewall ab
- eine fehlgeschlagene Verwaltungsverbindung beweist keinen Ausfall des Zielservers
- Aktionen können produktive Änderungen auslösen
- Erweiterungen können zusätzliche Berechtigungen benötigen

> Verwaltungsoberflächen fassen Zustände zusammen. Für belastbare Diagnosen müssen häufig Ereignisprotokolle, PowerShell-Ausgaben, Dienstprotokolle und Netzwerkdaten ergänzt werden.

24. Leistungsüberwachung auf Windows Server

Leistungsprobleme dürfen nicht allein anhand einer einzelnen CPU- oder RAM-Anzeige bewertet werden.

Wichtige Bereiche:

- Prozessor
- Arbeitsspeicher
- Datenträger
- Netzwerk
- Prozess
- System
- Serverdienst
- DNS
- AD DS
- DFS-R
- Hyper-V
- SQL Server oder weitere Anwendungsrollen

Leistungsindikatoren anzeigen

```
[RO][SENS] Get-Counter -ListSet *
```

Beispielhafte Systemindikatoren

```
[TEST][SENS] Get-Counter `
    "\Processor(_Total)\% Processor Time",
    "\Memory\Available MBytes",
    "\PhysicalDisk(_Total)\Avg. Disk sec/Transfer",
    "\System\Processor Queue Length"
```

Wichtige Regeln

- über einen repräsentativen Zeitraum messen
- Normalzustand als Vergleichswert besitzen
- Durchschnitt, Maximum und Verteilung unterscheiden
- Rolle des Servers berücksichtigen
- virtuelle und physische Ebene unterscheiden
- Wartungsfenster und Sicherungen berücksichtigen
- Ursache und Folge nicht verwechseln
- Zeitstempel mit Benutzerfehlern korrelieren

> Ein einzelner hoher Messwert beweist noch keinen Engpass. Entscheidend sind Dauer, Wiederholbarkeit, Warteschlangen, Antwortzeiten und Auswirkungen auf den Dienst.

25. Typische Fehlerbilder und geeignete Werkzeuge

Fehlerbild	Geeignete Prüfungen
Benutzer kann sich nicht anmelden	DNS, DC-Locator, Zeit, Secure Channel, Kerberos, Netlogon, Ereignisse
Anmeldung funktioniert nur manchmal	mehrere DCs vergleichen, Replikation, DNS, Standorte, Zeit
neues Kennwort funktioniert nicht überall	`repadmin`, verwendeten DC feststellen, PDC-Erreichbarkeit
neuer Benutzer ist auf einem Server unbekannt	AD-Replikation, verwendeten DC, DNS
Computer meldet fehlende Vertrauensstellung	Secure Channel, Computerkonto, DNS, Zeit
GPO wird nicht angewendet	`gpresult`, GroupPolicy-Log, OU, Filter, SYSVOL, Replikation
GPO besitzt auf verschiedenen Clients andere Werte	verwendeten DC, AD- und SYSVOL-Replikation, Filter
Netzlaufwerk fehlt	GPO, DNS, DFS, SMB, Berechtigungen, Benutzerkontext
Domain Controller wird nicht gefunden	DNS-Client, SRV-Records, DC-Locator, Firewall
Kerberos funktioniert nur mit bestimmtem Namen	DNS, SPN, Alias, Dienstkonto
Zugriff fällt auf NTLM zurück	Kerberos-Ticket, SPN, Zielname, DNS
Uhrzeit springt zurück	W32Time, Domänenhierarchie, Hypervisor-Zeitquelle
DHCP-Client erhält APIPA	DHCP-Server, Relay, VLAN, Bereich, Firewall
falscher DNS-Server per DHCP	Bereichs- und Serveroptionen prüfen
SYSVOL fehlt	DFS-R, Netlogon, DC-Zustand, Ereignisse
Dateien in DFS unterscheiden sich	DFS-R-Zustand, Rückstand, Konflikte, Dateisperren
Clusterrolle startet nicht	Ressourcenabhängigkeiten, Clusterlog, Systemlog, DNS, Speicher
Server Manager zeigt Server als offline	WinRM, Firewall, DNS, Berechtigungen, Zielzustand

26. Empfohlener Gesamtablauf bei Domänenproblemen

1. originale Fehlermeldung erfassen.

2. Benutzer, Computer und Zeitpunkt bestätigen.
3. Umfang der Störung bestimmen.
4. letzte Änderung dokumentieren.
5. lokale Netzwerkverbindung prüfen.
6. `ipconfig /all` erfassen.
7. konfigurierte DNS-Server prüfen.
8. Domänennamen und SRV-Einträge auflösen.
9. Domain Controller mit `nltest /dsgetdc` ermitteln.
10. verwendeten Standort prüfen.
11. Domain Controller gezielt erreichen.
12. Uhrzeit und Zeitquelle vergleichen.
13. Secure Channel prüfen.
14. Kerberos-Tickets untersuchen.
15. bei Dienstproblemen SPNs prüfen.
16. System- und Anwendungsprotokolle auswerten.
17. auf Domain Controllern `dcdiag` ausführen.
18. AD-Replikation mit `repadmin` prüfen.
19. bei GPO-Problemen `gpresult` sichern.
20. GroupPolicy-Betriebsprotokoll untersuchen.
21. SYSVOL auf mehreren DCs vergleichen.
22. DFS-R-Ereignisse prüfen.
23. Hypothese aus mehreren Befunden formulieren.
24. kleinste reversible Maßnahme planen.
25. Sicherung und Rückfallplan prüfen.
26. Änderung kontrolliert durchführen.
27. Funktion mit demselben Testszenario erneut prüfen.
28. Replikation und Monitoring nachkontrollieren.
29. temporäre Debugprotokollierung deaktivieren.
30. Ursache, Maßnahme und Ergebnis dokumentieren.

27. Beispiel – Gruppenrichtlinie wird auf CLIENT1 nicht angewendet

Ausgangslage

Eine auf `DC1` erstellte und mit einer OU verknüpfte GPO soll auf `CLIENT1` angewendet werden. Die konfigurierte Einstellung ist auf dem Client nicht wirksam.

Vorgehensweise

1. Benutzer- und Computername auf `CLIENT1` bestätigen.
2. prüfen, ob die Einstellung eine Benutzer- oder Computerrichtlinie ist.
3. tatsächliche OU des Zielobjekts kontrollieren.
4. GPO-Verknüpfung in der Gruppenrichtlinienverwaltung prüfen.

5. GPO-Status und Verknüpfungsstatus prüfen.
6. Sicherheitsfilter und Delegierung kontrollieren.
7. WMI-Filter prüfen.
8. `gpresult` vor einer Änderung erzeugen:

```
[RO][SENS] gpresult /h "%TEMP%\gpresult-vorher.html"
```

9. verwendeten Domain Controller und DNS-Zustand prüfen:

```
[RO][SENS] set LOGONSERVER
[TEST][SENS] nltest /dsgetdc:<DOMÄNE>
[RO][SENS] ipconfig /all
```

10. GroupPolicy-Betriebsprotokoll untersuchen.
11. SYSVOL auf dem verwendeten DC prüfen.
12. AD- und DFS-R-Replikation zwischen `DC1` und weiteren DCs prüfen.
13. kontrollierte Aktualisierung durchführen:

```
[CHANGE][REMOTE] gpupdate /force
```

14. erforderliche Abmeldung oder Neustart durchführen.
15. neuen Bericht erzeugen:

```
[RO][SENS] gpresult /h "%TEMP%\gpresult-nachher.html"
```

16. beide Berichte vergleichen.

Mögliche Befunde

- `CLIENT1` befindet sich in der falschen OU.
- GPO enthält eine Benutzereinstellung, wurde aber nur für das Computerkonto erwartet.
- Sicherheitsfilter schließt den Benutzer oder Computer aus.
- GPO wird durch eine höher priorisierte Einstellung überschrieben.
- WMI-Filter trifft nicht zu.
- Client verwendet einen anderen DC mit älterem Replikationsstand.
- SYSVOL enthält auf einem DC nicht den aktuellen Dateianteil.
- Richtlinie benötigt Neustart oder Abmeldung.
- Einstellung wird von der Clientedition nicht unterstützt.
- Loopback-Verarbeitung verändert das Ergebnis.

28. Beispiel – Benutzer kann sich nur an manchen Computern anmelden

Mögliche Ursachen

- unterschiedliche Domain Controller liefern unterschiedliche AD-Stände
- Kennwortänderung ist noch nicht vollständig repliziert
- ein Standort verweist auf einen gestörten DC
- DNS liefert veraltete oder falsche Einträge
- ein Computer besitzt einen fehlerhaften Secure Channel
- Zeitabweichung verhindert Kerberos
- lokale Benutzerrechte unterscheiden sich
- GPO verweigert eine Anmeldeart
- Benutzerprofil oder Anmeldeskript schlägt fehl
- Netzwerk ist beim Start noch nicht verfügbar

Prüfungen auf funktionierendem und betroffenem Computer

```
[RO][SENS] ipconfig /all
[TEST][SENS] nltest /dsgetdc:<DOMÄNE>
[RO][SENS] nltest /dsgetsite
[TEST][PRIV][SENS] nltest /sc_verify:<DOMÄNE>
[RO][SENS] w32tm /query /status
[RO][SENS] w32tm /query /source
[RO][SENS] klist
[RO][SENS] gpresult /r
```

Anschließend müssen die Ergebnisse miteinander verglichen werden:

- DNS-Server
- Domain Controller
- Standort
- Uhrzeit
- Ticketstatus
- GPOs
- Gruppenmitgliedschaften
- Ereignisprotokolle
- Secure Channel

29. Beispiel – Active-Directory-Änderung erscheint nicht auf DC2

Ausgangslage

Ein auf `DC1` angelegtes oder geändertes Objekt ist auf `DC2` nicht sichtbar.

Vorgehensweise

1. Objekt und Änderungszeitpunkt dokumentieren.
2. sicherstellen, dass tatsächlich unterschiedliche DCs abgefragt werden.
3. AD-Replikationsübersicht erstellen:

```
[RO][PRIV][SENS] repadmin /replsummary
```

4. eingehende Partner von `DC2` untersuchen:

```
[RO][PRIV][SENS] repadmin /showrepl DC2
```

5. betroffenen Namenskontext bestimmen.
6. DNS-Auflösung zwischen `DC1` und `DC2` prüfen.
7. RPC- und Firewall-Erreichbarkeit berücksichtigen.
8. Uhrzeit vergleichen.
9. Ereignisprotokoll `Directory Service` untersuchen.
10. Replikationsmetadaten des Objekts vergleichen:

```
[RO][PRIV][SENS] repadmin /showobjmeta DC1 "<DISTINGUISHED-NAME>"
```

```
[RO][PRIV][SENS] repadmin /showobjmeta DC2 "<DISTINGUISHED-NAME>"
```

11. erst nach Ursachenprüfung eine kontrollierte Replikation auslösen.
12. anschließend automatische Replikation weiter beobachten.

> Das manuelle Kopieren, erneute Anlegen oder Löschen des Objekts kann Konflikte erzeugen und die ursprüngliche Replikationsursache verdecken.

30. Gefährliche Fehlinterpretationen vermeiden

Beobachtung	Nicht automatisch bewiesen
Ping zum DC funktioniert	LDAP, Kerberos, SMB und RPC funktionieren
Domänenname wird aufgelöst	alle benötigten SRV-Records sind korrekt

Beobachtung	Nicht automatisch bewiesen
Anmeldung funktioniert	Anmeldung erfolgte aktuell gegen einen DC
`LOGONSERVER` zeigt DC1	jeder Domänendienst verwendet DC1
`gpupdate` war erfolgreich	gewünschte GPO wurde angewendet
GPO ist verknüpft	Zielobjekt darf sie anwenden
GPO erscheint in `gpresult`	jede einzelne Einstellung wurde erfolgreich verarbeitet
Benutzer ist Gruppenmitglied	aktuelles Token enthält die neue Mitgliedschaft
`klist` zeigt Tickets	Ticket gehört zum richtigen Dienst und SPN
SPN existiert	SPN ist dem richtigen Konto eindeutig zugeordnet
Uhrzeit sieht gleich aus	Zeitquelle und tatsächliche Abweichung sind korrekt
`repadmin /replsummary` zeigt wenig Fehler	alle Partitionen und Objekte sind aktuell
SYSVOL ist erreichbar	SYSVOL besitzt auf allen DCs denselben Stand
DHCP-Lease existiert	Optionen, VLAN und DNS-Daten sind korrekt
Clusterressource ist online	Anwendung ist fachlich funktionsfähig
Ereignis-ID ist bekannt	Ursache ist ohne Ereignistext eindeutig

31. Sicherheits- und Datenschutzanforderungen

Diagnosedaten können enthalten:

- Benutzernamen
- Gruppenmitgliedschaften
- Computernamen
- Domänennamen
- interne DNS-Zonen
- IP- und MAC-Adressen
- Distinguished Names
- Gruppenrichtlinien
- Anmeldeserver
- Sicherheitskennungen
- Kerberos-Ticketinformationen
- Dienstkonten
- SPNs
- Freigaben
- interne Dateipfade
- Cluster- und Servernamen
- DHCP-Leases

- Ereignisprotokolle
- Netzwerkstruktur
- administrative Konten

Vor der Weitergabe müssen:

1. Zweck und Empfänger bestimmt werden.
2. benötigte Daten begrenzt werden.
3. Kennwörter, Schlüssel und Tokens ausgeschlossen werden.
4. personenbezogene Angaben redigiert werden.
5. Dateien verschlüsselt übertragen werden.
6. Zugriffsrechte beschränkt werden.
7. Aufbewahrungsfristen festgelegt werden.
8. temporäre Debuglogs wieder deaktiviert werden.
9. nicht mehr benötigte Diagnosedaten sicher gelöscht werden.
10. externe Analysedienste organisatorisch freigegeben sein.

> Kennwörter dürfen nicht in Befehlszeilen, Dokumentationen, Screenshots oder Protokolldateien eingetragen werden.

32. Dokumentationsvorlage

```
Ticket:
Datum und Uhrzeit:
Bearbeiter:

Betroffener Benutzer:
Betroffener Computer:
Windows-Version:
Serverrolle:
Domäne:
Active-Directory-Standort:
IP-Adresse:
DNS-Server:
Gateway:
VPN:
Verwendeter Domain Controller:
LOGONSERVER:
```

Originale Fehlermeldung:

Fehlerzeitpunkt:

Reproduzierbar:

Betroffene Systeme:

Letzte funktionierende Nutzung:

Letzte Änderung:

DC-Locator-Ergebnis:

Secure-Channel-Ergebnis:

Zeitquelle:

Zeitabweichung:

Kerberos-Tickets:

Verwendeter KDC:

Untersuchter SPN:

SPN-Zuordnung:

Doppelte SPNs:

DCDiag-Ergebnis:

Fehlgeschlagener Test:

Repadmin-Replikationsübersicht:

Betroffener Quell-DC:

Betroffener Ziel-DC:

Betroffener Namenskontext:

Letzte erfolgreiche Replikation:

Replikationsfehlercode:

Replikationsmetadaten geprüft:

DNS-Zone:

DNS-Record:

SRV-Records:

Dynamische Registrierung:

DNS-Ereignisse:

DNS-Debuglog verwendet:

Netlogon-Debuglog verwendet:

Debuglogging wieder deaktiviert:

GPO:

GPO-ID:

Benutzer- oder Computerrichtlinie:

Verknüpfte OU:

Sicherheitsfilter:

Delegierung:

WMI-Filter:

Vererbungsreihenfolge:

Loopback-Modus:

GPResult vorher:

GPUpdate-Ergebnis:

GPResult nachher:

GroupPolicy-Ereignisse:

Abmeldung erforderlich:

Neustart erforderlich:

SYSVOL erreichbar:

NETLOGON erreichbar:

GPO-Dateianteil vorhanden:

DFS-R-Status:

DFS-R-Ereignisse:

Replikationsrückstand:

DHCP-Server:

DHCP-Bereich:

Lease:

Bereichsauslastung:

Router-Option:

DNS-Option:

DNS-Suffix:

DHCP-Relay:

DHCP-Failover:

Cluster:

Clusterknoten:

Clusterrolle:

Fehlgeschlagene Ressource:

Abhängige Ressourcen:

Quorum:

```
Witness:
Clusterlog:
Failover-Zeitpunkt:

Vermutete Ursache:
Belege:
Geplante Maßnahme:
Sicherung:
Rückfallplan:
Änderung:
Ergebnis:
Wiederholungstest:
Monitoring:
Abschluss:
```

Merksatz

> Bei Fehlern in Windows-Domänen muss die Abhängigkeitskette vollständig betrachtet werden: Netzwerk ermöglicht die Verbindung, DNS findet den Dienst, Zeit und Secure Channel schaffen die Vertrauensbasis, Kerberos authentifiziert, Active Directory liefert die Objekte, Replikation verteilt den Zustand und SYSVOL stellt die Gruppenrichtliniendateien bereit.

Quellen und weiterführende Dokumentation

- Microsoft Learn – DCDiag
- Microsoft Learn – Repadmin
- Microsoft Learn – Problembehandlung der Active-Directory-Replikation
- Microsoft Learn – Häufige Active-Directory-Replikationsfehler
- Microsoft Learn – NLTest
- Microsoft Learn – Test-ComputerSecureChannel
- Microsoft Learn – Active Directory Domain Services und DNS
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – DNS-Server-PowerShell
- Microsoft Learn – Kerberos-Problembehandlung
- Microsoft Learn – Klist

- Microsoft Learn – SetSPN
- Microsoft Learn – W32tm
- Microsoft Learn – Funktionsweise des Windows-Zeitdienstes
- Microsoft Learn – GPResult
- Microsoft Learn – GPUpdate
- Microsoft Learn – Gruppenrichtlinien-Problembehandlung
- Microsoft Learn – Group Policy Operational Log
- Microsoft Learn – DHCP-Server-PowerShell
- Microsoft Learn – DHCP-Problembehandlung
- Microsoft Learn – DFS Namespaces und DFS Replication
- Microsoft Learn – Problembehandlung bei DFS Replication
- Microsoft Learn – Failover Clustering
- Microsoft Learn – Failovercluster erstellen und validieren
- Microsoft Learn – Get-ClusterLog
- Microsoft Learn – Windows Admin Center
- Microsoft Learn – Get-Counter
- Microsoft Learn – Netzwerkports für Windows-Dienste