8.2 Active Directory, Gruppenrichtlinien und Kerberos analysieren

Active Directory Domain Services bilden in vielen Windows-Netzwerken die Grundlage für:

- Benutzer- und Computeranmeldung,
- zentrale Authentifizierung,
- Gruppen und Berechtigungen,
- Gruppenrichtlinien,
- DNS-basierte Diensterkennung,
- Kerberos-Tickets,
- Vertrauensstellungen,
- Zertifikatdienste,
- Datei-, Druck- und Anwendungszugriffe.

Eine scheinbar einfache Meldung wie „Anmeldung nicht möglich“, „Zugriff verweigert“ oder „Gruppenrichtlinie wird nicht angewendet“ kann deshalb unterschiedliche Ursachen haben:

- falsche DNS-Konfiguration,
- nicht erreichbarer Domänencontroller,
- fehlerhafte Zeitsynchronisation,
- gestörter Secure Channel,
- Replikationsfehler,
- falsche Gruppenmitgliedschaft,
- fehlerhafte GPO-Verknüpfung,
- Sicherheitsfilterung,
- WMI-Filter,
- Kerberos- oder SPN-Fehler,
- nicht repliziertes Kennwort,
- gesperrtes oder deaktiviertes Konto,
- beschädigtes Computer- oder Benutzerprofil,
- fehlende Netzwerkports,
- fehlerhafte Vertrauensstellung.

Die Komponenten müssen gemeinsam und in einer festen Reihenfolge untersucht werden.

---

1. Lernziele

Nach dieser Seite kannst du:

- Active-Directory-Fehler systematisch eingrenzen,
- Client-, Server- und Domänencontrollerprobleme unterscheiden,
- den verwendeten Domänencontroller bestimmen,
- DNS- und SRV-Einträge prüfen,

- Zeitsynchronisation untersuchen,
- den Secure Channel eines Clients bewerten,
- AD-Replikationsfehler erkennen,
- Gruppenrichtlinienergebnisse auswerten,
- Kerberos-Tickets und SPNs prüfen,
- typische Ereignisprotokolle zuordnen,
- zwischen Symptom, Ursache und Nebenbefund unterscheiden,
- Änderungen kontrolliert und mit Rückweg durchführen.

---

2. Vereinfachte Abhängigkeitskette

```
Benutzer oder Computer
        ↓
IP-Konnektivität
        ↓
DNS-Auflösung und SRV-Einträge
        ↓
Erreichbarer Domänencontroller
        ↓
Zeitsynchronisation
        ↓
Secure Channel und Computerkonto
        ↓
Kerberos oder NTLM
        ↓
Active-Directory-Replikation
        ↓
Gruppenmitgliedschaften und Berechtigungen
        ↓
Gruppenrichtlinien und Anwendungszugriff
```

Ein Fehler weiter oben kann zahlreiche Folgefehler auslösen.

Beispiele:

- Falsches DNS kann verhindern, dass ein Domänencontroller gefunden wird.
- Eine zu große Zeitabweichung kann Kerberos-Authentifizierung verhindern.
- Eine fehlerhafte AD-Replikation kann dazu führen, dass ein neues Kennwort nur an einem Domänencontroller bekannt ist.
- Eine fehlerhafte SYSVOL-Replikation kann dazu führen, dass eine GPO zwar im Verzeichnis vorhanden ist, ihre Dateien aber nicht überall verfügbar sind.

- Ein doppelter SPN kann verhindern, dass für einen Dienst ein gültiges Kerberos-Ticket ausgestellt wird.

---

3. Sicherheits- und Betriebsregeln

Vor Änderungen müssen mindestens folgende Informationen gesichert werden:

- genauer Fehlertext,
- Fehlercode,
- Zeitpunkt und Zeitzone,
- betroffener Benutzer,
- betroffener Computer,
- verwendeter Domänencontroller,
- betroffener Dienst oder Server,
- letzte Änderungen,
- aktuelle DNS-Konfiguration,
- Zeitquelle und Zeitabweichung,
- Gruppenrichtlinienergebnis,
- Replikationsstatus,
- relevante Ereignisse.

Nicht als erste Maßnahme durchführen:

- Computer aus der Domäne entfernen und wieder aufnehmen,
- Computerkonto löschen,
- Benutzerkonto neu erstellen,
- GPO löschen oder vollständig deaktivieren,
- AD-Replikation ungeprüft erzwingen,
- Kerberos-Konfiguration in der Registry ändern,
- Domänencontroller neu starten,
- DNS-Einträge wahllos löschen,
- SPNs ohne vorherige Prüfung verändern,
- große Berechtigungsgruppen hinzufügen,
- alle Gruppenrichtlinien gleichzeitig zurücksetzen.

Solche Maßnahmen verändern oder vernichten den Zustand, der für die Ursachenanalyse benötigt wird.

---

4. Fehlerbild exakt erfassen

Wichtige Fragen:

- Scheitert die lokale oder die Domänenanmeldung?
- Ist nur ein Benutzer betroffen?
- Ist nur ein Computer betroffen?

- Sind mehrere Computer einer OU oder eines Standorts betroffen?
- Funktioniert der Zugriff über IP-Adresse, aber nicht über Namen?
- Funktioniert die Anmeldung mit zwischengespeicherten Anmeldedaten?
- Tritt der Fehler nur bei einem bestimmten Domänencontroller auf?
- Betrifft das Problem Benutzer- oder Computerrichtlinien?
- Ist nur ein bestimmter Dienst betroffen?
- Funktioniert NTLM, während Kerberos scheitert?
- Trat der Fehler nach Kennwortänderung, Wiederherstellung, Snapshot, Migration oder GPO-Änderung auf?
- Ist der Fehler dauerhaft oder nur zeitweise vorhanden?
- Funktioniert ein vergleichbarer Benutzer oder Computer?

Ein Client, ein Benutzer und eine konkrete Zielressource sollten als kontrollierter Testfall verwendet werden.

---

5. Grundinformationen auf dem Client erfassen

Identität:

```
whoami
```

Benutzer-Domäne:

```
echo %USERDOMAIN%
```

Anmeldeserver:

```
echo %LOGONSERVER%
```

Vollständige Benutzerinformationen:

```
whoami /all
```

Computername:

```
hostname
```

Domänenzugehörigkeit:

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

IP-Konfiguration:

```
ipconfig /all
```

Dabei sind besonders zu prüfen:

- IPv4- und IPv6-Adresse,
- Subnetzmaske beziehungsweise Präfix,
- Standardgateway,
- DNS-Server,
- DNS-Suffix,
- DHCP-Status,
- Verbindungssuffix,
- mehrere aktive Netzwerkadapter,
- VPN-, virtuelle oder alte Adapter.

Domänenmitglieder sollten grundsätzlich die für die AD-Domäne zuständigen internen DNS-Server verwenden. Ein öffentlicher DNS-Server kennt die internen AD-SRV-Einträge normalerweise nicht.

---

6. Verwendeten Domänencontroller bestimmen

Anmeldeserver:

```
echo %LOGONSERVER%
```

Domänencontroller für die Domäne suchen:

```
nltest /dsgetdc:<Domänenname>
```

Beispiel:

```
nltest /dsgetdc:ad.example.local
```

Domänencontroller auflisten:

```
nltest /dclist:<Domänenname>
```

Aktuellen DC über PowerShell bestimmen:

```
Get-ADDomainController -Discover
```

Alle bekannten Domänencontroller:

```
Get-ADDomainController -Filter * |
    Select-Object HostName,
                  Site,
                  IPv4Address,
                  IsGlobalCatalog,
                  OperationMasterRoles
```

Die PowerShell-Befehle des Active-Directory-Moduls erfordern die entsprechenden RSAT-Komponenten oder die Ausführung auf einem geeigneten Verwaltungsserver.

Zu dokumentieren sind:

- Name des verwendeten Domänencontrollers,
- Standort beziehungsweise AD-Site,
- IP-Adresse,
- Global-Catalog-Status,
- Erreichbarkeit,
- Zeitpunkt des Tests.

---

7. DNS als erste technische Abhängigkeit prüfen

Hostauflösung:

```
nslookup <Domänencontroller>
```

Vollqualifizierten Namen prüfen:

```
nslookup <DC-Name>.<DNS-Domäne>
```

Domänencontroller über LDAP-SRV-Einträge suchen:

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.<DNS-Domäne>
```

Kerberos-Dienste suchen:

```
nslookup -type=SRV _kerberos._tcp.<DNS-Domäne>
```

Global Catalog suchen:

```
nslookup -type=SRV _gc._tcp.<DNS-Gesamtstruktur>
```

Standortspezifische Domänencontroller:

```
nslookup -type=SRV _ldap._tcp.<Standort>._sites.dc._msdcs.<DNS-Domäne>
```

PowerShell:

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

Zu prüfen sind:

- existieren die erwarteten SRV-Einträge,
- zeigen die Einträge auf vorhandene Domänencontroller,
- lassen sich deren Hostnamen auflösen,
- stimmen die IP-Adressen,
- antwortet der vorgesehene interne DNS-Server,
- werden alte oder stillgelegte Domänencontroller zurückgegeben,
- liefert ein anderer DNS-Server abweichende Ergebnisse,
- ist das DNS-Suffix korrekt,
- bestehen doppelte A- oder AAAA-Einträge.

Ein erfolgreicher Ping auf eine IP-Adresse beweist keine funktionierende AD-DNS-Struktur.

---

8. Erreichbarkeit benötigter Dienste prüfen

Grundlegende Verbindung:

```
Test-NetConnection <Domänencontroller>
```

DNS:

```
Test-NetConnection <Domänencontroller> -Port 53
```

Kerberos:

```
Test-NetConnection <Domänencontroller> -Port 88
```

LDAP:

```
Test-NetConnection <Domänencontroller> -Port 389
```

SMB für SYSVOL und NETLOGON:

```
Test-NetConnection <Domänencontroller> -Port 445
```

RPC Endpoint Mapper:

```
Test-NetConnection <Domänencontroller> -Port 135
```

Global Catalog:

```
Test-NetConnection <Domänencontroller> -Port 3268
```

LDAPS, sofern verwendet:

```
Test-NetConnection <Domänencontroller> -Port 636
```

Global Catalog über TLS, sofern verwendet:

```
Test-NetConnection <Domänencontroller> -Port 3269
```

Wichtige Dienste und Ports können unter anderem sein:

Funktion	Typischer Port
DNS	TCP/UDP 53
Kerberos	TCP/UDP 88

Funktion	Typischer Port
RPC Endpoint Mapper	TCP 135
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
dynamisches RPC	konfigurationsabhängiger TCP-Portbereich

Ein erfolgreich getesteter TCP-Port beweist nur, dass eine Verbindung zu diesem Port hergestellt werden konnte. Er beweist nicht, dass Authentifizierung, LDAP-Abfrage, Replikation oder Gruppenrichtlinienverarbeitung funktionieren.

---

9. SYSVOL und NETLOGON prüfen

Freigaben des Domänencontrollers:

```
net view \\<Domänencontroller>
```

SYSVOL öffnen:

```
dir \\<Domänencontroller>\SYSVOL
```

NETLOGON öffnen:

```
dir \\<Domänencontroller>\NETLOGON
```

Direkter Domänenpfad:

```
dir \\<DNS-Domäne>\SYSVOL
```

Zu prüfen sind:

- Freigaben vorhanden,
- Namensauflösung funktioniert,
- Zugriff unter dem vorgesehenen Benutzer möglich,
- benötigte GPO-Verzeichnisse vorhanden,

- Skripte und Vorlagen erreichbar,
- unterschiedliche Domänencontroller liefern denselben erwarteten Inhalt.

Eine GPO besteht aus zwei zusammengehörigen Teilen:

Bestandteil	Speicherort
Group Policy Container	Active Directory
Group Policy Template	SYSVOL

Sind die beiden Teile oder ihre Versionsstände nicht konsistent, kann die Gruppenrichtlinienverarbeitung fehlschlagen.

---

10. Zeitsynchronisation prüfen

Aktueller Status:

```
w32tm /query /status
```

Zeitquelle:

```
w32tm /query /source
```

Konfiguration:

```
w32tm /query /configuration
```

Domänenhierarchie überwachen:

```
w32tm /monitor
```

Vergleich mit einem bestimmten Domänencontroller:

```
w32tm /stripchart /computer:<Domänencontroller> /samples:10 /dataonly
```

Windows-Zeitdienst:

```
Get-Service W32Time
```

Zu prüfen sind:

- aktuelle Zeit,
- Zeitzone,
- Zeitquelle,
- Zeitabweichung,
- Dienststatus,
- Domänenhierarchie,
- Erreichbarkeit der Zeitquelle,
- Virtualisierung und Host-Zeitsynchronisation,
- PDC-Emulator als maßgebliche Domänenzeitquelle.

Kerberos reagiert empfindlich auf Zeitabweichungen. Der konkrete Fehler muss jedoch anhand von Ereignissen, Ticketstatus und Zeitmessung nachgewiesen werden.

Eine manuelle Änderung der Uhrzeit beseitigt nicht automatisch die Ursache einer falschen Zeitquelle.

---

11. Secure Channel des Computers prüfen

Der Secure Channel ist die geschützte Beziehung zwischen einem Domänenmitglied und der Domäne.

Prüfung mit PowerShell:

```
Test-ComputerSecureChannel -Verbose
```

Prüfung mit NLTEST:

```
nltest /sc_verify:<DNS-Domäne>
```

Verwendeten sicheren Kanal anzeigen:

```
nltest /sc_query:<DNS-Domäne>
```

Mögliche Symptome eines gestörten Secure Channels:

- „Die Vertrauensstellung zwischen dieser Arbeitsstation und der primären Domäne ist fehlgeschlagen“,
- Anmeldung funktioniert nur mit zwischengespeicherten Daten,
- Gruppenrichtlinien schlagen fehl,
- Zugriff auf Domänenressourcen scheitert,
- Computerkonto-Kennwort stimmt zwischen Client und AD nicht überein.

Mögliche Ursachen:

- Rücksetzen auf einen alten VM-Snapshot,
- geklontes System mit fehlerhafter Identität,
- wiederhergestelltes Computerkonto,
- Replikationsfehler,
- doppelt verwendeter Computername,
- beschädigtes Computerkonto,
- lange getrenntes oder falsch wiederhergestelltes System.

Eine Reparatur des Secure Channels ist eine Änderung und darf erst nach Sicherung der Diagnoseergebnisse erfolgen.

Mögliche kontrollierte Reparatur auf einem Domänenmitglied:

```
Test-ComputerSecureChannel -Repair `
    -Credential <Domäne>\<Administratorkonto>
```

Vorher müssen geprüft werden:

- DNS funktioniert,
- Domänencontroller ist erreichbar,
- Zeit stimmt,
- Computerkonto ist vorhanden und eindeutig,
- keine Replikationsstörung liegt vor,
- Berechtigung zur Reparatur ist vorhanden,
- Rückweg und Wartungsfenster sind festgelegt.

`Test-ComputerSecureChannel` ist vor allem für Domänenmitglieder vorgesehen. Bei Domänencontrollern müssen DC-spezifische Diagnose- und Reparaturverfahren verwendet werden.

---

12. Benutzer- und Computerkonto prüfen

Benutzerkonto:

```
Get-ADUser -Identity <Benutzername> -Properties * |
    Select-Object SamAccountName,
                  UserPrincipalName,
                  Enabled,
                  LockedOut,
                  PasswordExpired,
                  PasswordLastSet,
```

```
        LastBadPasswordAttempt,
        BadLogonCount,
        AccountExpirationDate
```

Computerkonto:

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

Gruppenmitgliedschaften:

```
Get-ADPrincipalGroupMembership <Benutzername> |
  Select-Object Name,
        GroupScope,
        GroupCategory
```

Aktuelles Benutzer-Token:

```
whoami /groups
```

Zu unterscheiden sind:

- im Active Directory gespeicherte Gruppenmitgliedschaften,
- Gruppen im aktuellen Anmeldetoken,
- verschachtelte Gruppen,
- lokale Gruppen,
- universelle, globale und domänenlokale Gruppen,
- Änderungen nach der letzten Anmeldung.

Eine neu hinzugefügte Gruppenmitgliedschaft ist nicht automatisch im bereits bestehenden Benutzer-Token enthalten. Ab- und erneute Anmeldung kann erforderlich sein. Bei bestimmten Dienstkonten kann ein Dienstneustart notwendig sein.

---

13. Kontosperrung untersuchen

Zu prüfen sind:

- ist das Konto tatsächlich gesperrt,
- auf welchem Domänencontroller wurde die Sperrung registriert,
- welcher Client oder Dienst sendet falsche Anmeldedaten,
- existieren gespeicherte Anmeldedaten,
- läuft ein Dienst oder eine geplante Aufgabe mit altem Kennwort,
- verwendet ein Smartphone, VPN oder Netzlaufwerk alte Zugangsdaten,
- tritt die Sperrung unmittelbar nach dem Entsperren erneut auf.

Benutzerstatus:

```
Get-ADUser <Benutzername> `
   -Properties LockedOut,
               LastBadPasswordAttempt,
               BadLogonCount,
               PasswordLastSet
```

Gesperrte Konten suchen:

```
Search-ADAccount -LockedOut -UsersOnly
```

Relevante Sicherheitsereignisse können unter anderem betreffen:

- fehlgeschlagene Anmeldung,
- Kontosperrung,
- Kerberos-Vorauthentifizierungsfehler,
- Ticketanforderungen,
- Anmeldungen mit expliziten Anmeldedaten.

Ein Konto lediglich wiederholt zu entsperren beseitigt die Quelle der falschen Anmeldedaten nicht.

---

14. Domänencontroller grundsätzlich prüfen

Ausführliche Diagnose:

```
dcdiag /v
```

Ausgabe in Datei:

```
dcdiag /v /c /d /e > C:\Temp\dcdiag.txt
```

DNS-Test:

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

Replikationstest:

```
dcdiag /test:replications /v
```

SYSVOL-Test:

```
dcdiag /test:sysvolcheck /v
```

Werbungsstatus des Domänencontrollers:

```
dcdiag /test:advertising /v
```

NETLOGON-Freigabe:

```
dcdiag /test:netlogons /v
```

Zu prüfen sind:

- welcher Test fehlschlägt,
- welcher Domänencontroller betroffen ist,
- genauer Fehlercode,
- Zeitpunkt,
- DNS-Abhängigkeit,
- Replikationspartner,
- Verzeichnispartition,
- Warnung oder tatsächlicher Fehler.

Nicht jede Warnung in einer umfangreichen `dcdiag`-Ausgabe erklärt das untersuchte Symptom. Der Befund muss zeitlich und technisch zum Fehler passen.

---

15. AD-Replikation prüfen

Gesamtübersicht:

```
repadmin /replsummary
```

Eingehende Replikation eines DCs:

```
repadmin /showrepl <Domänencontroller>
```

Gesamtstrukturweite Anzeige:

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

PowerShell-Auswertung:

```
repadmin /showrepl * /csv |
    ConvertFrom-Csv |
    Out-GridView
```

Replikationsfehler über PowerShell:

```
Get-ADReplicationFailure `
    -Target * `
    -Scope Forest
```

Status der Replikationspartner:

```
Get-ADReplicationPartnerMetadata `
    -Target * `
    -Scope Forest |
    Select-Object Server,
                  Partner,
                  Partition,
                  LastReplicationAttempt,
                  LastReplicationSuccess,
                  LastReplicationResult
```

Replikationswarteschlange:

```
repadmin /queue
```

Zu dokumentieren sind:

- Quell- und Ziel-DC,
- Verzeichnispartition,
- letzte erfolgreiche Replikation,
- letzter Replikationsversuch,
- Anzahl aufeinanderfolgender Fehler,
- Fehlercode,
- Fehlertext,
- betroffene Standorte,
- Richtung des Fehlers.

---

16. Replikationsfehler richtig bewerten

AD-Replikation hängt unter anderem ab von:

- DNS,
- Netzwerkverbindungen,
- RPC,
- Authentifizierung,
- Autorisierung,
- Zeit,
- Replikationstopologie,
- Verzeichnisdatenbank,
- Zustand der Domänencontroller.

Befund	Mögliche Ursache
Fehler 1722	RPC-Server nicht verfügbar, DNS, Firewall oder Dienstproblem
Fehler 5	Zugriff verweigert, Authentifizierung oder Berechtigung
Zielprinzipalname ist falsch	Kerberos-, SPN- oder Computerkonto-Problem
letzter Erfolg lange her	dauerhafte oder standortbezogene Störung
nur eine Partition betroffen	partitions- oder DNS-bezogenes Problem
nur ein Partner betroffen	Verbindung, DNS oder Zustand dieses Partners
Änderungen fehlen nur auf einem DC	eingehende Replikation dieses DCs prüfen
verschiedene Kennwörter funktionieren je nach DC	Kennwortreplikation oder allgemeine Replikation prüfen
GPO fehlt nur auf einem DC	AD- und SYSVOL-Replikation gemeinsam prüfen

Eine erzwungene Synchronisation ist keine erste Diagnosemaßnahme. Sie kann zusätzliche Last erzeugen und verdeckt möglicherweise die Richtung oder den ursprünglichen Zustand des Fehlers.

---

17. FSMO-Rollen prüfen

```
netdom query fsmo
```

PowerShell:

```
Get-ADForest |
    Select-Object SchemaMaster,
                  DomainNamingMaster

Get-ADDomain |
    Select-Object PDCEmulator,
                  RIDMaster,
                  InfrastructureMaster
```

Die Rollen sind:

Rolle	Ebene	Wichtige Funktion
Schema-Master	Gesamtstruktur	Schemaänderungen
Domänennamen-Master	Gesamtstruktur	Domänen und Partitionen
RID-Master	Domäne	RID-Pools für Sicherheitskennungen
PDC-Emulator	Domäne	Zeit, Kennwortpriorität und weitere Funktionen
Infrastruktur-Master	Domäne	domänenübergreifende Objektbezüge

Der Ausfall eines FSMO-Rolleninhabers erklärt nicht automatisch jede Anmeldestörung. Die betroffene Funktion und die Ausfalldauer müssen berücksichtigt werden.

---

18. Gruppenrichtlinien-Grundlagen

Die normale Verarbeitungsreihenfolge lautet:

```
Lokal → Site → Domäne → OU → untergeordnete OU
```

Diese Reihenfolge wird häufig mit `LSDOU` bezeichnet.

Grundsätzlich gilt:

- Gruppenrichtlinien werden kumulativ verarbeitet.
- Näher am Benutzer- oder Computerobjekt verknüpfte Einstellungen können frühere Einstellungen überschreiben.

- Die genaue Wirkung hängt von Verknüpfungsreihenfolge, Vererbung, Erzwingen, Sicherheitsfilterung und Richtlinientyp ab.
- Computer- und Benutzerkonfiguration werden getrennt verarbeitet.
- Nicht jede Erweiterung wird bei jeder Hintergrundaktualisierung vollständig verarbeitet.
- Loopbackverarbeitung kann die Benutzerkonfiguration abhängig vom Computerstandort verändern.

Mögliche Ursachen für eine nicht angewendete GPO:

- GPO nicht an der richtigen Site, Domäne oder OU verknüpft,
- Link deaktiviert,
- GPO vollständig oder teilweise deaktiviert,
- Objekt befindet sich in der falschen OU,
- Sicherheitsfilterung schließt Benutzer oder Computer aus,
- fehlende Leseberechtigung,
- WMI-Filter liefert `False`,
- Vererbung blockiert,
- andere GPO besitzt höhere Priorität,
- Einstellung gilt nur für Benutzer oder nur für Computer,
- langsame Netzwerkverbindung,
- erforderliche synchrone Verarbeitung noch nicht erfolgt,
- Neustart oder erneute Anmeldung fehlt,
- SYSVOL nicht erreichbar,
- AD- oder SYSVOL-Replikation gestört,
- Client Side Extension schlägt fehl.

---

19. Gruppenrichtlinienergebnis erfassen

Kurzübersicht:

```
gpresult /r
```

Computerrichtlinien mit erhöhten Rechten:

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

Benutzerrichtlinien:

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

Ausführlicher HTML-Bericht:

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

Bericht für einen bestimmten Benutzer:

```
gpresult /user <Domäne>\<Benutzer> /h C:\Temp\gpresult-benutzer.html
```

Ausführliche Textausgabe:

```
gpresult /z
```

Resultant Set of Policy:

```
rsop.msc
```

Im Bericht sind besonders zu prüfen:

- angewendete GPOs,
- abgelehnte GPOs,
- Ablehnungsgrund,
- Sicherheitsgruppen,
- verwendeter Domänencontroller,
- WMI-Filter,
- Benutzer- und Computerbereich,
- Loopbackmodus,
- langsame Verbindung,
- Verarbeitungszeit,
- Fehler einzelner Erweiterungen.

`gpresult` muss im passenden Benutzer- und Berechtigungskontext ausgeführt werden. Ein Bericht aus einem anderen Konto kann ein anderes Ergebnis zeigen.

---

20. Gruppenrichtlinien kontrolliert aktualisieren

Standardaktualisierung:

```
gpupdate
```

Erneute Verarbeitung aller Einstellungen:

```
gpupdate /force
```

Nur Computerrichtlinien:

```
gpupdate /target:computer /force
```

Nur Benutzerrichtlinien:

```
gpupdate /target:user /force
```

Eine erzwungene Aktualisierung kann:

- zusätzliche Netz- und Serverlast verursachen,
- erneut alle Richtlinienerweiterungen anstoßen,
- Ab- oder Anmeldung verlangen,
- einen Neustart verlangen,
- laufende Benutzersitzungen beeinflussen.

`gpupdate /force` ist ein Test beziehungsweise Auslöser, aber noch keine Ursachenanalyse. Danach müssen Ergebnisbericht und Ereignisprotokolle geprüft werden.

---

21. Gruppenrichtlinien-Ereignisse prüfen

Wichtiger Protokollpfad:

```
Ereignisanzeige
→ Anwendungs- und Dienstprotokolle
→ Microsoft
→ Windows
→ GroupPolicy
→ Operational
```

PowerShell:

```
Get-WinEvent -FilterHashtable @{
    LogName   = 'Microsoft-Windows-GroupPolicy/Operational'
    StartTime = (Get-Date).AddHours(-2)
} |
    Select-Object TimeCreated,
```

```
    Id,
    LevelDisplayName,
    Message
```

Zusätzlich prüfen:

- Systemprotokoll,
- Anwendungsprotokoll,
- DNS Client Events,
- NETLOGON,
- Kerberos,
- Benutzerprofildienst,
- einzelne Client Side Extensions.

Nicht nur die Event-ID verwenden. Provider, vollständiger Text, Zeitpunkt, Benutzer, Computer und Verarbeitungsschritt müssen gemeinsam bewertet werden.

---

22. GPO-Verknüpfung und Filterung prüfen

In der Gruppenrichtlinienverwaltung sind zu kontrollieren:

- richtige GPO,
- richtige Verknüpfung,
- richtige OU,
- Link aktiviert,
- GPO-Status,
- Verknüpfungsreihenfolge,
- Vererbung,
- erzwungene Links,
- Sicherheitsfilterung,
- Delegierung,
- WMI-Filter,
- Benutzer- oder Computerteil,
- GPO-Version,
- Replikationsstatus.

Sicherheitsfilterung benötigt grundsätzlich die passenden Berechtigungen zum Lesen und Anwenden der Gruppenrichtlinie.

Typische Fehlinterpretation:

> „Ein Benutzer ist Mitglied einer Gruppe, die „Gruppenrichtlinie übernehmen“ besitzt. Im aktuellen Anmeldetoken fehlt diese neue Gruppenmitgliedschaft

> jedoch noch.

Deshalb müssen AD-Mitgliedschaft und aktuelles Token getrennt geprüft werden.

---

23. Loopbackverarbeitung verstehen

Loopbackverarbeitung wird für Computer verwendet, bei denen die Benutzerumgebung vom verwendeten Computer abhängen soll, beispielsweise:

- Schulungsräume,
- Kiosksysteme,
- Terminalserver,
- gemeinsam verwendete Arbeitsplätze.

Modi:

Modus	Wirkung
Zusammenführen	Benutzerrichtlinien des Benutzerobjekts werden verarbeitet, danach kommen die für den Computer ermittelten Benutzerrichtlinien hinzu
Ersetzen	Benutzerrichtlinien des Benutzerobjekts werden durch die für den Computer ermittelten Benutzerrichtlinien ersetzt

Wenn Benutzereinstellungen nur auf bestimmten Computern unerwartet sind, muss Loopback geprüft werden.

---

24. Kerberos-Grundprinzip

Vereinfacht:

```
Benutzeranmeldung
      ↓
Authentication Service Request
      ↓
Ticket Granting Ticket
      ↓
Ticket Granting Service Request
      ↓
Dienstticket für einen SPN
      ↓
Zugriff auf den Zieldienst
```

Wichtige Begriffe:

Begriff	Bedeutung
KDC	Key Distribution Center auf einem Domänencontroller
TGT	Ticket Granting Ticket
Dienstticket	Ticket für einen konkreten Dienst
SPN	eindeutiger Dienstbezeichner eines Kontos
Realm	Kerberos-Sicherheitsbereich, in AD meist zur Domäne zugeordnet
PAC	enthält unter anderem Autorisierungsinformationen
Delegierung	Weitergabe von Anmeldeinformationen unter definierten Bedingungen

Kerberos benötigt insbesondere:

- funktionierende DNS-Auflösung,
- erreichbaren KDC,
- korrekte Zeit,
- gültige Konten,
- korrekte Kennwörter,
- eindeutige SPNs,
- einen zum Zielnamen passenden Dienstprinzipal.

---

25. Kerberos-Tickets prüfen

Tickets des aktuellen Anmeldekontexts:

```
klist
```

TGT anzeigen:

```
klist tgt
```

Zwischengespeicherte Tickets auflisten:

```
klist tickets
```

KDCs anzeigen:

```
klist query_bind
```

Zu prüfen sind:

- Clientname,
- Servername beziehungsweise SPN,
- Kerberos-Realm,
- Tickettyp,
- Start- und Ablaufzeit,
- Erneuerungszeit,
- Verschlüsselungstyp,
- Flags,
- verwendeter KDC.

Das Löschen des Ticketcaches verändert den Diagnosezustand:

```
klist purge
```

`klist purge` sollte erst eingesetzt werden, wenn:

- vorhandene Tickets dokumentiert wurden,
- klar ist, welcher Sicherheitskontext betroffen ist,
- erneute Authentifizierung möglich ist,
- keine kritische Sitzung unterbrochen wird,
- der Test gezielt ein neues Ticket anfordern soll.

Nach dem Löschen kann ein erneuter Zugriff auf die Zielressource ein neues Ticket auslösen.

---

26. Service Principal Names prüfen

SPNs eines Kontos anzeigen:

```
setspn -L <Kontoname>
```

Bestimmten SPN suchen:

```
setspn -Q <Dienst>/<Hostname>
```

Beispiel:

```
setspn -Q HTTP\webserver.ad.example.local
```

Doppelte SPNs domänen- beziehungsweise gesamtstrukturweit suchen:

```
setspn -X
```

Mögliche SPN-Probleme:

- SPN fehlt,
- SPN ist dem falschen Konto zugeordnet,
- SPN ist doppelt vorhanden,
- Client verwendet Alias statt registriertem Hostnamen,
- Dienstkonto wurde geändert,
- Server wurde umbenannt,
- Dienst läuft unter anderem Konto als erwartet,
- alter SPN blieb nach Migration erhalten.

SPNs dürfen nicht ohne vorherige Suche, Dokumentation und Prüfung verändert werden. Ein falsches Entfernen kann andere Dienste oder Benutzer beeinträchtigen.

---

27. Kerberos und NTLM unterscheiden

Anmeldesitzungen:

```
klist sessions
```

Tickets:

```
klist
```

Für bestimmte Verbindungen können zusätzlich Ereignisprotokolle, Dienstprotokolle oder geeignete Netzwerkaufzeichnungen erforderlich sein.

Mögliche Hinweise auf NTLM statt Kerberos:

- kein passendes Dienstticket vorhanden,
- Zugriff erfolgt über IP-Adresse,
- SPN für den verwendeten Namen fehlt,
- Ziel befindet sich außerhalb der Kerberos-Vertrauensbeziehung,
- Anwendung fordert ausdrücklich NTLM,
- DNS- oder Namensproblem,

- Kerberos-Anforderung schlägt fehl und ein Fallback ist möglich.

Ein funktionierender Zugriff beweist deshalb nicht automatisch, dass Kerberos verwendet wurde.

---

28. Zugriff über IP-Adresse und Hostname vergleichen

Beispiel:

```
\\192.0.2.10\Freigabe
\\server01\Freigabe
\\server01.ad.example.local\Freigabe
```

Unterschiedliche Ergebnisse können auf Folgendes hinweisen:

- DNS-Problem,
- Alias-Problem,
- SPN-Problem,
- Kerberos funktioniert nur für einen bestimmten Namen,
- Zertifikat passt nicht zum verwendeten Namen,
- Anwendung verwendet unterschiedliche Sicherheitszonen,
- IPv4 und IPv6 führen zu unterschiedlichen Zielen.

Der Zugriff per IP-Adresse ist kein allgemeiner Ersatz für korrekte Namensauflösung. Bei Kerberos ist der verwendete Zielname für die SPN-Zuordnung entscheidend.

---

29. Kerberos-Ereignisse untersuchen

Relevante Protokolle können sein:

- Sicherheitsprotokoll auf Client, Server und DC,
- Systemprotokoll,
- Kerberos-Key-Distribution-Center-Protokoll,
- NETLOGON-Protokoll,
- dienstspezifische Protokolle.

PowerShell-Beispiel für aktuelle Sicherheitsereignisse:

```
Get-WinEvent -FilterHashtable @{
    LogName   = 'Security'
    StartTime = (Get-Date).AddHours(-2)
} |
    Where-Object {
```

```
    $_.Id -in 4768, 4769, 4771, 4776
} |
Select-Object TimeCreated,
              Id,
              Message
```

Typische Ereigniskategorien:

Kategorie	Mögliche Bedeutung
TGT wurde angefordert	Benutzer- oder Computerauthentifizierung
Dienstticket wurde angefordert	Zugriff auf einen bestimmten SPN
Kerberos-Vorauthentifizierung fehlgeschlagen	Kennwort, Zeit, Kontostatus oder anderer Authentifizierungsfehler
Anmeldeinformationen wurden validiert	häufig NTLM-bezogene Prüfung
Kontosperrung	wiederholte fehlerhafte Authentifizierung

Event-IDs müssen mit dem vollständigen Ereignistext und dem jeweiligen System ausgewertet werden.

---

30. Typische Fehlerbilder

Symptom	Mögliche Ursache	Nächster Test
Domäne kann nicht gefunden werden	DNS oder DC-Erreichbarkeit	`ipconfig /all`, SRV-Abfrage, `nltest /dsgetdc`
Anmeldung funktioniert offline, aber nicht im Firmennetz	DC-, DNS-, Zeit- oder Secure-Channel-Problem	DC-Suche, Zeit und Secure Channel
Vertrauensstellung fehlgeschlagen	Computerkennwort oder Computerkonto inkonsistent	`Test-ComputerSecureChannel`, Replikation
neues Kennwort funktioniert nur manchmal	unterschiedliche DC-Daten	verwendeten DC und Replikation prüfen
Benutzer bleibt trotz Entsperrung gesperrt	gespeicherte alte Anmeldedaten	Sperrquelle und Sicherheitsereignisse
GPO wird nicht angezeigt	falsche OU, Filterung oder Link	`gpresult`, GPMC
GPO wird angezeigt, Einstellung fehlt	Überschreibung oder Erweiterungsfehler	Detailbericht und GroupPolicy-Protokoll
Computerrichtlinie fehlt	Computerobjekt, Neustart oder Computerbereich	`gpresult /scope computer`
Benutzerrichtlinie fehlt	Benutzerobjekt, Token oder Benutzerbereich	`gpresult /scope user`

Symptom	Mögliche Ursache	Nächster Test
GPO funktioniert nur an einem Standort nicht	Site, DC, Replikation oder Netzwerk	DC-Zuordnung und Replikation
SYSVOL nicht erreichbar	DNS, SMB, DC oder DFSR	Port 445, Freigabe und DC-Protokolle
Kerberos-Ticket fehlt	SPN, DNS, KDC oder Anwendung	`klist`, `setspn -Q`
Kerberos scheitert nur über Alias	fehlender SPN für Alias	verwendeten Namen und SPN prüfen
Zugriff funktioniert per IP, nicht per Name	DNS, SPN oder Zertifikat	Namen einzeln prüfen
Zugriff funktioniert per Name, nicht per IP	Kerberos- oder Anwendungsanforderung	Ticket und Zielkonfiguration
Dienst funktioniert nur mit NTLM	SPN oder Delegierung	Dienstkonto und SPNs
Replikation meldet RPC-Fehler	DNS, Firewall, RPC oder Partner offline	Namensauflösung und Ports
Benutzer hat neue Gruppe, aber keinen Zugriff	altes Anmeldetoken	`whoami /groups`, erneute Anmeldung
Fehler nur auf einem Client	lokaler DNS-, Cache-, Konto- oder Profilfehler	Vergleichsclient und lokale Konfiguration
Fehler auf vielen Clients	zentrale AD-, DNS-, GPO- oder Netzwerkstörung	DCs, Replikation und Änderungen
Fehler nach VM-Snapshot	Secure Channel oder Zeit zurückgesetzt	Zeit, Computerkonto und Secure Channel

---

31. Vorgehensweise bei einer nicht angewendeten GPO

1. Betroffenen Benutzer und Computer bestimmen.
2. Prüfen, ob Benutzer- und Computerobjekt in den erwarteten OUs liegen.
3. Verwendeten Domänencontroller dokumentieren.
4. DNS- und DC-Erreichbarkeit prüfen.
5. SYSVOL-Zugriff prüfen.
6. `gpresult` als HTML-Bericht erstellen.
7. angewendete und abgelehnte GPOs prüfen.
8. Sicherheitsfilterung und WMI-Filter prüfen.
9. Verknüpfung, Reihenfolge und Vererbung prüfen.
10. Loopbackverarbeitung berücksichtigen.
11. GroupPolicy-Operational-Protokoll auswerten.
12. AD- und SYSVOL-Replikation prüfen.
13. genau eine kontrollierte Korrektur durchführen.
14. Richtlinien erneut verarbeiten.
15. Ergebnisbericht und Benutzerfunktion erneut prüfen.

---

32. Vorgehensweise bei einer fehlgeschlagenen Anmeldung

1. Exakte Meldung und Zeitpunkt erfassen.
2. Lokale und Domänenanmeldung unterscheiden.
3. Netzwerkverbindung prüfen.
4. DNS-Server und DNS-Suffix prüfen.
5. Domänencontroller über SRV-Einträge suchen.
6. verwendeten DC bestimmen.
7. Zeit und Zeitquelle prüfen.
8. Benutzerkonto auf Sperre, Ablauf und Deaktivierung prüfen.
9. Secure Channel des Clients prüfen.
10. Replikationsstatus der DCs prüfen.
11. Sicherheits- und Kerberos-Ereignisse auswerten.
12. gespeicherte Anmeldedaten, Dienste und Aufgaben berücksichtigen.
13. genau eine Maßnahme durchführen.
14. Anmeldung und Ressourcenabruf erneut testen.

---

33. Vorgehensweise bei Kerberos-Problemen

1. verwendeten Zielnamen dokumentieren.
2. DNS-Auflösung dieses Namens prüfen.
3. Zeit von Client, Server und DC vergleichen.
4. KDC beziehungsweise DC-Erreichbarkeit prüfen.
5. vorhandene Tickets mit `klist` dokumentieren.
6. nach passendem Dienstticket suchen.
7. erwarteten SPN bestimmen.
8. SPN mit `setspn -Q` suchen.
9. Dienstkonto und tatsächlichen Dienstprozess vergleichen.
10. doppelte SPNs prüfen.
11. Sicherheits- und Kerberos-Ereignisse korrelieren.
12. Vertrauensstellung und Delegierung berücksichtigen.
13. Ticketcache nur kontrolliert leeren.
14. Zugriff erneut auslösen.
15. neues Ticket und Funktion prüfen.

---

34. Maßnahmen und Rückwege

Ursache: falscher DNS-Server am Client

Nachweis:

- Client verwendet einen nicht zuständigen DNS-Server,
- AD-SRV-Einträge werden nicht korrekt aufgelöst,
- interner DNS-Server liefert die erwarteten Einträge.

Maßnahme:

- DNS-Konfiguration kontrolliert auf die vorgesehenen internen DNS-Server korrigieren.

Rollback:

- ursprüngliche Adapter- oder DHCP-Konfiguration dokumentiert wiederherstellen.

Verifikation:

- SRV-Abfrage,
- DC-Suche,
- Anmeldung,
- GPO-Verarbeitung,
- Anwendungszugriff.

Ursache: fehlerhafter Secure Channel

Nachweis:

- Secure-Channel-Prüfung schlägt fehl,
- Computerkonto ist vorhanden,
- DNS, Zeit und DC-Erreichbarkeit funktionieren,
- Replikation ist ausreichend gesund.

Maßnahme:

- Secure Channel mit berechtigtem Konto kontrolliert reparieren.

Rollback:

- vorab dokumentierte Computer- und Domänenkonfiguration verwenden;
- bei Fehlschlag nach freigegebenem Wiederherstellungsverfahren vorgehen.

Verifikation:

- Secure Channel erneut prüfen,
- Neustart oder Anmeldung testen,
- Gruppenrichtlinien und Ressourcen testen.

Ursache: GPO durch Sicherheitsfilterung ausgeschlossen

Nachweis:

- `gpresult` nennt die GPO als abgelehnt,
- Benutzer oder Computer besitzt nicht die erforderlichen Berechtigungen.

Maßnahme:

- Sicherheitsfilterung nach dem Minimalprinzip korrigieren.

Rollback:

- ursprüngliche ACL beziehungsweise Gruppenmitgliedschaft wiederherstellen.

Verifikation:

- neues Token berücksichtigen,
- GPO aktualisieren,
- `gpresult` erneut erzeugen,
- konkrete Einstellung prüfen.

Ursache: doppelter SPN

Nachweis:

- `setspn -Q` oder `setspn -X` zeigt den SPN mehrfach,
- Kerberos-Ereignisse passen zum Fehler,
- Dienstkonto und Zielname wurden bestätigt.

Maßnahme:

- falsche SPN-Zuordnung nach Freigabe entfernen und korrekte eindeutige Zuordnung sicherstellen.

Rollback:

- vorherige SPN-Zuordnungen vollständig dokumentieren.

Verifikation:

- neue Tickets anfordern,
- Dienstticket prüfen,
- Zugriff mit vorgesehenem Namen testen.

Ursache: AD-Replikationsfehler

Nachweis:

- `repadmin` oder PowerShell zeigt konkrete Fehler,
- betroffene Objekte oder Kennwörter unterscheiden sich zwischen DCs,
- Fehlercode und Abhängigkeit wurden bestimmt.

Maßnahme:

- zugrunde liegendes DNS-, Netzwerk-, RPC-, Zeit-, Authentifizierungs- oder DC-Problem beheben.

Rollback:

- abhängig von der konkreten Änderung;
- keine erzwungene Replikations- oder Metadatenbereinigung ohne Wiederherstellungsplan.

Verifikation:

- `repadmin /replsummary`,
- `repadmin /showrepl`,
- Objektvergleich,
- Anmeldung und GPO-Verarbeitung.

---

35. Nachkontrolle

Nach jeder Maßnahme sind mindestens folgende Punkte erneut zu prüfen:

- Client verwendet die vorgesehenen DNS-Server.
- AD-SRV-Einträge werden korrekt aufgelöst.
- vorgesehene Domänencontroller sind erreichbar.
- Zeit und Zeitquelle sind plausibel.
- Secure Channel funktioniert.
- Benutzer- und Computerkonto sind aktiv.
- Replikation zeigt keine zum Fehler gehörenden Störungen.
- SYSVOL und NETLOGON sind erreichbar.
- benötigte Gruppenmitgliedschaften sind im aktuellen Token enthalten.
- erwartete GPOs werden angewendet.
- abgelehnte GPOs sind fachlich erklärbar.
- Gruppenrichtlinienprotokoll zeigt keine neuen relevanten Fehler.
- erforderliches Kerberos-Ticket wird ausgestellt.
- SPN ist eindeutig und dem richtigen Konto zugeordnet.
- Benutzerfunktion wurde praktisch getestet.
- keine unnötigen Berechtigungen wurden vergeben.
- temporäre Diagnose- oder Protokollierungsfunktionen wurden beendet.
- Ursache, Maßnahme, Rückweg und Ergebnis wurden dokumentiert.

---

36. Dokumentationsbeispiel

```
Symptom:
Die Laufwerkszuordnung aus der Gruppenrichtlinie wurde auf einem
Client nicht erstellt.
```

Zeitpunkt:
02.08.2026, 10:18 Uhr MESZ

Betroffener Benutzer:
max.mustermann

Betroffener Computer:
CLIENT-17

Verwendeter Domänencontroller:
DC02.ad.example.local

Nachweis:
DNS-Auflösung, Zeit und SYSVOL-Zugriff waren erfolgreich.
Der gpresult-Bericht zeigte die GPO als abgelehnt.
Als Ablehnungsgrund wurde die Sicherheitsfilterung angegeben.
Die erforderliche Benutzergruppe war im Active Directory eingetragen,
fehlte aber im aktuellen Anmeldetoken.

Ursache:
Die Gruppenmitgliedschaft wurde erst nach Beginn der bestehenden
Benutzersitzung hinzugefügt.

Maßnahme:
Der Benutzer meldete sich kontrolliert ab und erneut an.
An der GPO und ihren Berechtigungen wurde nichts verändert.

Rollback:
Nicht erforderlich, da keine Konfiguration geändert wurde.

Verifikation:
whoami /groups zeigt die vorgesehene Gruppe.
gpresult zeigt die angewendete GPO.
Das Laufwerk wurde verbunden.
Keine neuen Fehler im GroupPolicy-Protokoll.

Prävention:
Bei Änderungen an Gruppenmitgliedschaften wird künftig berücksichtigt,

dass bestehende Anmeldetoken nicht automatisch vollständig erneuert werden.

---

37. Entscheidungsbaum

```
Domänenanmeldung, GPO oder Ressourcenzugriff gestört
        ↓
Stimmen IP-Konfiguration und interne DNS-Server?
        ├── Nein
        │   ↓
        │   Netzwerk- und DNS-Konfiguration korrigieren
        │
        └── Ja
            ↓
Werden AD-SRV-Einträge und DCs gefunden?
        ├── Nein
        │   ↓
        │   DNS-Zone, SRV-Einträge und DC-Dienste prüfen
        │
        └── Ja
            ↓
Sind DC und benötigte Ports erreichbar?
        ├── Nein
        │   ↓
        │   Routing, Firewall, Standort und Dienste prüfen
        │
        └── Ja
            ↓
Stimmen Zeit und Secure Channel?
        ├── Nein
        │   ↓
        │   Zeitquelle oder Vertrauensbeziehung untersuchen
        │
        └── Ja
            ↓
Ist die AD-Replikation fehlerfrei?
        ├── Nein
        │   ↓
        │   Replikationsfehler nach Code und Richtung analysieren
```

```
        │
        └── Ja
            ↓
Betrifft der Fehler Gruppenrichtlinien?
        ├── Ja
        │   ↓
        │   gpresult, SYSVOL, Filter, OU und Ereignisse prüfen
        │
        └── Nein
            ↓
Betrifft der Fehler Kerberos oder einen Dienst?
        ├── Ja
        │   ↓
        │   Tickets, SPNs, Zielname und Dienstkonto prüfen
        │
        └── Nein
            ↓
Konto, Gruppen, Berechtigungen und Anwendung untersuchen
```

---

38. Typische Prüfungsfragen

Warum ist DNS für Active Directory besonders wichtig?

Antwort anzeigen

Active Directory verwendet DNS und insbesondere SRV-Einträge, damit Clients Domänencontroller, Kerberos-Dienste und Global Catalogs finden. Eine reine Auflösung externer Internetnamen reicht für eine funktionierende Domänenumgebung nicht aus.

Warum kann ein neues Kennwort an einem Client funktionieren und an einem anderen nicht?

Antwort anzeigen

Die Clients können unterschiedliche Domänencontroller verwenden. Bei einer Replikationsstörung ist das neue Kennwort möglicherweise noch nicht auf allen benötigten Domänencontrollern verfügbar.

Wozu dient `gpresult`?

Antwort anzeigen

`gpresult` zeigt die resultierenden Gruppenrichtlinien für einen Benutzer oder Computer. Es kann angewendete und abgelehnte GPOs, Sicherheitsgruppen, Filter und weitere Verarbeitungsinformationen darstellen.

Warum ist `gpupdate /force` noch keine Fehlerbehebung?

Antwort anzeigen

Der Befehl löst eine erneute Verarbeitung der Gruppenrichtlinien aus. Er erklärt jedoch nicht, warum eine GPO zuvor nicht angewendet wurde. Dafür müssen Ergebnisbericht, Ereignisse, Filterung, Verknüpfung und Abhängigkeiten geprüft werden.

Warum kann eine neue Gruppenmitgliedschaft trotz korrektem AD-Eintrag noch wirkungslos sein?

Antwort anzeigen

Das aktuelle Anmeldetoken wurde möglicherweise vor der Gruppenänderung erzeugt. Die neue Mitgliedschaft ist dann noch nicht im Token enthalten und wird häufig erst nach erneuter Anmeldung wirksam.

Welche drei grundlegenden Abhängigkeiten benötigt Kerberos besonders?

Antwort anzeigen

Kerberos benötigt insbesondere funktionierende DNS-Auflösung, ausreichend genaue Zeitsynchronisation und korrekte beziehungsweise eindeutige Dienstidentitäten in Form von SPNs.

Was ist ein SPN?

Antwort anzeigen

Ein Service Principal Name identifiziert eine konkrete Dienstinstanz und ist einem Active-Directory-Konto zugeordnet. Der KDC verwendet ihn, um ein Dienstticket für den richtigen Dienst auszustellen.

Warum kann ein doppelter SPN die Kerberos-Authentifizierung verhindern?

Antwort anzeigen

Der KDC kann den Dienst nicht eindeutig einem Konto zuordnen. Dadurch kann kein korrektes Dienstticket für die erwartete Dienstidentität ausgestellt werden.

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

Antwort anzeigen

Dadurch wird der für die Diagnose wichtige Zustand verändert. Außerdem kann die Maßnahme zusätzliche Probleme mit Computerkonto, Profilen, Berechtigungen, Zertifikaten und verwalteter Konfiguration erzeugen.

Worin unterscheiden sich AD- und SYSVOL-Replikation bei einer GPO?

Antwort anzeigen

Der Group Policy Container mit den Verzeichnisinformationen liegt im Active Directory. Das Group Policy Template mit den dateibasierten Richtlinieninhalten liegt in SYSVOL. Beide Bestandteile müssen verfügbar und konsistent sein.

---

39. Prüfungsfallen

- öffentlichen DNS-Server auf einem Domänenmitglied eintragen.
- erfolgreichen Ping als Nachweis für funktionierendes Active Directory bewerten.
- nur den A-Eintrag, aber keine SRV-Einträge prüfen.
- IP-Erreichbarkeit mit funktionierender Authentifizierung gleichsetzen.
- Zeitabweichung übersehen.
- Domänencontroller und DNS-Server ungeprüft neu starten.
- Computer sofort aus der Domäne entfernen.
- Computerkonto ohne Sicherung löschen.
- Secure Channel reparieren, obwohl DNS oder Replikation gestört ist.
- Gruppenmitgliedschaft im AD mit dem aktuellen Token gleichsetzen.
- Benutzer wegen fehlender Berechtigung in eine weitreichende Administratorgruppe aufnehmen.
- `gpupdate /force` als alleinige Fehleranalyse verwenden.
- Benutzer- und Computerrichtlinien verwechseln.
- falschen Benutzerkontext für `gpresult` verwenden.
- OU des Benutzers prüfen, obwohl eine Computerrichtlinie betroffen ist.

- Sicherheitsfilterung, WMI-Filter oder Loopback übersehen.
- GPO löschen, statt Verknüpfung und Filterung zu untersuchen.
- SYSVOL-Zugriff nicht prüfen.
- AD-Replikation prüfen, aber SYSVOL-Replikation übersehen.
- Replikation ungeprüft erzwingen.
- einzelne `dcdiag`-Warnung ohne Zusammenhang als Ursache bewerten.
- Event-ID ohne Provider und vollständigen Text interpretieren.
- Kerberos und NTLM nicht unterscheiden.
- Zugriff per IP-Adresse als dauerhafte Lösung verwenden.
- Ticketcache vor der Dokumentation löschen.
- SPN ohne vorherige Suche verändern.
- gültigen SPN dem falschen Dienstkonto zuordnen.
- doppelten SPN ungeprüft entfernen.
- mehrere Änderungen gleichzeitig durchführen.
- nach einer Maßnahme weder Ticket noch GPO-Ergebnis erneut prüfen.
- keine praktische Benutzerfunktion testen.

---

40. Checkliste

- [ ] exakter Fehlertext wurde dokumentiert.
- [ ] Fehlerzeitpunkt und Zeitzone wurden erfasst.
- [ ] betroffener Benutzer wurde bestimmt.
- [ ] betroffener Computer wurde bestimmt.
- [ ] betroffener Zielserver oder Dienst wurde bestimmt.
- [ ] lokale und Domänenanmeldung wurden unterschieden.
- [ ] IP-Konfiguration wurde geprüft.
- [ ] vorgesehene interne DNS-Server werden verwendet.
- [ ] DNS-Suffix wurde geprüft.
- [ ] AD-SRV-Einträge wurden geprüft.
- [ ] verwendeter Domänencontroller wurde bestimmt.
- [ ] Standort beziehungsweise AD-Site wurde berücksichtigt.
- [ ] DC-Erreichbarkeit wurde geprüft.
- [ ] benötigte Ports wurden geprüft.
- [ ] SYSVOL wurde geprüft.
- [ ] NETLOGON wurde geprüft.
- [ ] Zeit und Zeitzone wurden geprüft.
- [ ] Zeitquelle wurde geprüft.
- [ ] Secure Channel wurde geprüft.
- [ ] Benutzerkonto wurde auf Sperre und Ablauf geprüft.

- [ ] Computerkonto wurde geprüft.
- [ ] AD-Gruppenmitgliedschaften wurden geprüft.
- [ ] aktuelles Benutzertoken wurde geprüft.
- [ ] AD-Replikation wurde geprüft.
- [ ] letzter erfolgreicher Replikationszeitpunkt wurde dokumentiert.
- [ ] Replikationsrichtung wurde berücksichtigt.
- [ ] `dcdiag` wurde bei DC-Problemen ausgewertet.
- [ ] FSMO-Rollen wurden bei passendem Fehlerbild geprüft.
- [ ] Benutzer- und Computerrichtlinien wurden unterschieden.
- [ ] `gpresult` wurde im richtigen Kontext erzeugt.
- [ ] angewendete und abgelehnte GPOs wurden geprüft.
- [ ] OU und GPO-Verknüpfung wurden geprüft.
- [ ] Sicherheitsfilterung wurde geprüft.
- [ ] WMI-Filter wurde geprüft.
- [ ] Vererbung und Erzwingen wurden geprüft.
- [ ] Loopbackverarbeitung wurde berücksichtigt.
- [ ] GroupPolicy-Operational-Protokoll wurde geprüft.
- [ ] vorhandene Kerberos-Tickets wurden dokumentiert.
- [ ] verwendeter Zielname wurde dokumentiert.
- [ ] benötigter SPN wurde bestimmt.
- [ ] SPN-Zuordnung wurde geprüft.
- [ ] doppelte SPNs wurden bei Bedarf gesucht.
- [ ] Kerberos- und Sicherheitsereignisse wurden zeitlich korreliert.
- [ ] letzte Änderungen wurden berücksichtigt.
- [ ] funktionierender Vergleichsclient wurde verwendet.
- [ ] genau eine kontrollierte Maßnahme wurde durchgeführt.
- [ ] Rückweg wurde festgelegt.
- [ ] Anmeldung wurde erneut getestet.
- [ ] GPO-Ergebnis wurde erneut geprüft.
- [ ] Kerberos-Ticket wurde erneut geprüft.
- [ ] konkrete Benutzerfunktion wurde getestet.
- [ ] Ursache, Maßnahme und Ergebnis wurden dokumentiert.
- [ ] vorbeugende Maßnahme wurde festgelegt.

41. Schnellreferenz

Beobachtung	Nächstes Werkzeug
Domäne wird nicht gefunden	`ipconfig /all`, `nslookup`, `nltest /dsgetdc`
falscher DNS-Server	Adapter-, DHCP- und DNS-Konfiguration
DC wird nicht gefunden	SRV-Abfragen und `nltest`
Anmeldung nur offline möglich	DC-Erreichbarkeit, Zeit, Secure Channel
Vertrauensstellung fehlgeschlagen	`Test-ComputerSecureChannel`, `nltest`
neues Kennwort funktioniert nicht überall	`repadmin`, verwendeten DC bestimmen
Replikationsfehler	`repadmin /replsummary`, `repadmin /showrepl`
DC-Zustand unklar	`dcdiag /v`
DNS auf DC fehlerhaft	`dcdiag /test:dns /v`
GPO fehlt	`gpresult`, GPMC
GPO abgelehnt	`gpresult /h`, Sicherheitsfilterung
GPO-Einstellung fehlt	Detailbericht und GroupPolicy-Protokoll
SYSVOL nicht erreichbar	DNS, SMB-Port und Freigaben
Gruppenänderung wirkt nicht	`whoami /groups`, erneute Anmeldung
Konto wird wiederholt gesperrt	Sicherheitsprotokoll und gespeicherte Anmeldedaten
Kerberos-Ticket fehlt	`klist`, DNS, Zeit
Dienstticket fehlt	`klist`, `setspn -Q`
doppelter SPN vermutet	`setspn -X`
Fehler nur über Alias	DNS- und SPN-Zuordnung
Zugriff nur über IP möglich	DNS, Zielname, SPN und Kerberos
Fehler nur an einem Standort	AD-Site, DC-Auswahl und Replikation
Fehler nur auf einem Client	lokale DNS-, Konto-, Token- oder Profilprüfung

---

Merksatz

> Active-Directory-Fehler werden von unten nach oben analysiert: Netzwerk, DNS, Domänencontroller, Zeit, Secure Channel, Replikation, Konten, Gruppenrichtlinien und Kerberos. Erst wenn die Abhängigkeiten nachweislich funktionieren, wird die betroffene Richtlinie, Berechtigung oder Anwendung verändert. Jede Änderung benötigt einen Rückweg und eine erneute Funktionsprüfung.

Quellen und weiterführende Dokumentation

Offizielle Microsoft-Dokumentation

- Microsoft Learn – AD DS Troubleshooting
- Microsoft Learn – Troubleshooting Active Directory Replication Problems
- Microsoft Learn – Diagnose Active Directory Replication Failures
- Microsoft Learn – Active Directory Replication Error 1722
- Microsoft Learn – Active Directory Replication Error 5
- Microsoft Learn – Group Policy Processing
- Microsoft Learn – Applying Group Policy Troubleshooting Guidance
- Microsoft Learn – Kerberos Authentication Troubleshooting Guidance
- Microsoft Learn – Domain Controller Is Not Functioning Correctly
- Microsoft Learn – Repadmin
- Microsoft Learn – Dcdiag
- Microsoft Learn – Gpresult
- Microsoft Learn – Gpupdate
- Microsoft Learn – Klist
- Microsoft Learn – Setspn
- Microsoft Learn – W32tm
- Microsoft Learn – Test-ComputerSecureChannel
- Microsoft Learn – Get-ADReplicationFailure
- Microsoft Learn – Get-ADReplicationPartnerMetadata