8.3 Datei-, Freigabe-, Rechte- und Druckdienste analysieren

Datei- und Druckdienstfehler entstehen häufig nicht durch eine einzelne Komponente. Namensauflösung, Netzwerk, Authentifizierung, Freigabeberechtigungen, Dateisystemrechte, Gruppenmitgliedschaften, SMB-Einstellungen, DFS, Speicherplatz und Druckwarteschlangen wirken zusammen.

Grundregel:

> Zuerst feststellen, ob bereits die Verbindung, die Authentifizierung, die Freigabe, die Datei oder erst die konkrete Aktion fehlschlägt.

---

1. Diagnosekette bei Dateizugriffen

```
Client
  ↓
DNS-Auflösung
  ↓
Netzwerk und TCP 445
  ↓
SMB-Dienst
  ↓
Authentifizierung
  ↓
Freigabeberechtigung
  ↓
NTFS-Berechtigung
  ↓
Datei, Ordner, Sperre oder Anwendung
  ↓
Datenträger und Backend
```

Jede Stufe muss getrennt geprüft werden.

Prüfschritt	Typische Frage
Namensauflösung	Zeigt der Servername auf die richtige IP-Adresse?

Prüfschritt	Typische Frage
Netzwerk	Ist der Server über den vorgesehenen Pfad erreichbar?
SMB-Port	Ist TCP 445 erreichbar?
SMB-Dienst	Nimmt der Server SMB-Verbindungen an?
Authentifizierung	Mit welchem Konto erfolgt der Zugriff?
Freigaberecht	Darf das Konto die Freigabe verwenden?
NTFS-Recht	Darf das Konto den Ordner oder die Datei verwenden?
Objektzustand	Existiert die Datei und ist sie verfügbar?
Sperre	Wird die Datei von einem Prozess blockiert?
Speicher	Sind Datenträger, Quota und Backend funktionsfähig?

---

2. Fehler exakt aufnehmen

Zu dokumentieren sind:

- vollständiger UNC-Pfad;
- Servername und Freigabename;
- betroffener Benutzer;
- betroffener Client;
- genaue Aktion;
- vollständiger Fehlertext;
- Fehlercode;
- Zeitpunkt mit Zeitzone;
- verwendete Netzwerkverbindung;
- funktioniert der Zugriff über IP-Adresse, Kurzname oder FQDN;
- funktioniert eine andere Freigabe auf demselben Server;
- funktioniert dieselbe Freigabe für einen anderen Benutzer;
- funktioniert derselbe Benutzer an einem anderen Client;
- trat der Fehler nach einer Rechte-, Gruppen-, GPO-, DNS- oder Serveränderung auf.

Beispiele für unterschiedliche Aktionen:

- Freigabe auflisten;
- Ordner öffnen;
- Datei lesen;
- Datei erstellen;
- Datei ändern;
- Datei löschen;
- Datei umbenennen;
- Unterordner erstellen;
- Berechtigungen ändern;

- Eigentümer übernehmen.

Ein Benutzer kann einen Ordner möglicherweise öffnen, aber keine Datei erstellen oder löschen. Deshalb genügt die Aussage „Zugriff funktioniert nicht“ nicht.

---

3. UNC-Pfad und Ziel bestimmen

Typischer UNC-Pfad:

```
\\fileserver01\Daten
```

Mit FQDN:

```
\\fileserver01.ad.example.local\Daten
```

Über DFS:

```
\\ad.example.local\Daten\Abteilung
```

Zu unterscheiden sind:

- tatsächlicher Dateiserver;
- DNS-Name oder Alias;
- DFS-Namespace;
- Freigabename;
- lokaler Pfad auf dem Server;
- verbundenes Netzlaufwerk;
- eventuell verwendeter Cluster- oder Failovername.

Ein Netzlaufwerk wie `H:` verdeckt den tatsächlichen UNC-Pfad. Dieser kann beispielsweise mit folgendem Befehl geprüft werden:

```
net use
```

PowerShell:

```
Get-SmbMapping
```

---

4. DNS-Auflösung prüfen

```
Resolve-DnsName fileserver01
```

```
Resolve-DnsName fileserver01.ad.example.local
```

```
nslookup fileserver01
```

Zusätzlich prüfen:

```
ping fileserver01
```

Der Ping dient hier hauptsächlich dazu, den aufgelösten Namen und die Zieladresse zu sehen. Er beweist nicht, dass SMB funktioniert.

Zu vergleichen sind:

- Kurzname;
- FQDN;
- IP-Adresse;
- erwartete Serveradresse;
- IPv4- und IPv6-Ergebnis;
- DNS-Alias;
- DFS-Namespace-Name.

Unterschiedliche Ergebnisse können auf Folgendes hinweisen:

- falscher oder veralteter DNS-Eintrag;
- falsches DNS-Suffix;
- DNS-Cache;
- `hosts`-Datei;
- alter Serveralias;
- DFS verweist auf ein anderes Ziel;
- IPv4 und IPv6 führen über unterschiedliche Pfade;
- Kerberos-SPN passt nicht zum verwendeten Namen.

---

5. SMB-Port prüfen

Windows:

```
Test-NetConnection fileserver01 -Port 445
```

Ausführlicher:

```
Test-NetConnection fileserver01 `
    -Port 445 `
    -InformationLevel Detailed
```

Linux:

```
nc -vz fileserver01 445
```

Ein erfolgreicher Test auf TCP 445 zeigt:

- der Name wurde aufgelöst;
- eine Route zum Ziel ist vorhanden;
- der TCP-Verbindungsaufbau war möglich;
- auf dem Ziel oder einem vorgeschalteten System wurde die Verbindung angenommen.

Er beweist noch nicht:

- erfolgreiche SMB-Authentifizierung;
- Zugriff auf eine bestimmte Freigabe;
- ausreichende Berechtigungen;
- Verfügbarkeit einer bestimmten Datei;
- Funktionsfähigkeit des Storage-Backends.

---

6. SMB-Clientverbindungen prüfen

Aktuelle SMB-Verbindungen:

```
Get-SmbConnection
```

Ausgewählte Informationen:

```
Get-SmbConnection |
    Select-Object ServerName,
                  ShareName,
                  UserName,
                  Credential,
                  Dialect,
                  NumOpens
```

SMB-Zuordnungen:

```
Get-SmbMapping
```

Klassische Anzeige:

```
net use
```

Dabei sind besonders zu prüfen:

- Servername;
- Freigabename;
- verwendetes Benutzerkonto;
- Verbindungsstatus;
- SMB-Dialekt;
- bereits bestehende Verbindungen zum selben Server;
- Verbindung über Alias, Kurzname oder FQDN.

---

7. Konflikt durch unterschiedliche Anmeldedaten

Windows verwendet für Verbindungen zu einem Server nicht beliebig viele verschiedene Anmeldeinformationen innerhalb desselben Benutzerkontexts.

Typisches Fehlerbild:

```
Mehrfache Verbindungen zu einem Server oder einer freigegebenen Ressource
von demselben Benutzer unter Verwendung mehrerer Benutzernamen sind nicht zulässig.
```

Bestehende Verbindungen anzeigen:

```
net use
```

Gespeicherte Anmeldeinformationen anzeigen:

```
cmdkey /list
```

Mögliche Ursachen:

- alte Verbindung zum selben Server;
- Verbindung über einen anderen Freigabenamen;

- gespeicherte falsche Anmeldedaten;
- Dienst oder Skript verwendet ein anderes Konto;
- Server wird einmal über Kurzname und einmal über Alias angesprochen;
- Laufwerkszuordnung wurde bereits mit anderen Anmeldedaten hergestellt.

Verbindungen dürfen nicht pauschal gelöscht werden, ohne ihre Verwendung zu prüfen. Ein Trennen kann geöffnete Dateien oder Anwendungen unterbrechen.

Gezieltes Trennen einer Zuordnung:

```
net use Z: /delete
```

Gezieltes Trennen eines UNC-Ziels:

```
net use \\fileserver01\Daten /delete
```

---

8. Freigaben auf dem Server prüfen

Vorhandene SMB-Freigaben:

```
Get-SmbShare
```

Bestimmte Freigabe:

```
Get-SmbShare -Name Daten
```

Wichtige Eigenschaften:

```
Get-SmbShare -Name Daten |
    Select-Object Name,
                  Path,
                  Description,
                  ScopeName,
                  FolderEnumerationMode,
                  EncryptData,
                  ConcurrentUserLimit
```

Klassische Anzeige:

```
net share
```

Zu prüfen sind:

- Freigabe existiert;
- Freigabename ist korrekt;
- lokaler Zielpfad existiert;
- Datenträger oder Mountpoint ist verfügbar;
- Freigabe zeigt nicht auf einen alten Pfad;
- Freigabe ist im richtigen Server- oder Cluster-Scope vorhanden;
- erforderliche SMB-Einstellungen sind aktiv;
- versteckte Freigabe mit `$` wurde korrekt angegeben.

Administrative Freigaben wie `C$` benötigen normalerweise administrative Berechtigungen und sind kein geeigneter allgemeiner Funktionstest für normale Benutzer.

---

9. Freigabeberechtigungen prüfen

```
Get-SmbShareAccess -Name Daten
```

Beispielausgabe:

```
Name   AccountName             AccessControlType   AccessRight
----   -----------             -----------------   -----------
Daten  AD\GG-Dateidienst-Lesen    Allow            Read
Daten  AD\GG-Dateidienst-Ändern   Allow             Change
```

Wichtige Freigaberechte:

Freigaberecht	Grundsätzliche Wirkung
Lesen	Inhalte anzeigen und Dateien lesen
Ändern	zusätzlich erstellen, ändern und löschen
Vollzugriff	zusätzlich Freigabeberechtigungen verwalten

Die genaue wirksame Berechtigung ergibt sich nicht allein aus dieser Tabelle. Verweigerungen, Gruppenmitgliedschaften und NTFS-Berechtigungen müssen zusätzlich berücksichtigt werden.

---

10. NTFS-Berechtigungen prüfen

PowerShell:

```
Get-Acl 'D:\Freigaben\Daten' |
    Format-List
```

Einzelne Zugriffsregeln:

```
(Get-Acl 'D:\Freigaben\Daten').Access |
    Select-Object IdentityReference,
                  FileSystemRights,
                  AccessControlType,
                  IsInherited,
                  InheritanceFlags,
                  PropagationFlags
```

Kommandozeile:

```
icacls D:\Freigaben\Daten
```

Rekursives Auslesen kann bei großen Verzeichnisstrukturen sehr umfangreich und belastend sein. Es sollte nur gezielt eingesetzt werden.

Zu prüfen sind:

- Benutzer- und Gruppeneinträge;
- Zulassen oder Verweigern;
- Vererbung;
- nur für diesen Ordner geltende Rechte;
- Rechte für Unterordner und Dateien;
- Eigentümer;
- explizite Einträge;
- geerbte Einträge;
- unterbrochene Vererbung;
- abweichende Rechte auf dem betroffenen Unterordner oder der Datei.

---

11. Freigabe- und NTFS-Rechte gemeinsam bewerten

Bei einem SMB-Zugriff wirken grundsätzlich beide Ebenen:

```
wirksames Freigaberecht
        +
wirksames NTFS-Recht
```

```
      ↓
restriktivere wirksame Kombination
```

Beispiele:

Freigabe	NTFS	Ergebnis über SMB
Lesen	Ändern	Lesen
Ändern	Lesen	Lesen
Vollzugriff	Ändern	Ändern
Vollzugriff	Vollzugriff	Vollzugriff
Ändern	keine Berechtigung	kein Zugriff

Beim lokalen Zugriff auf den Serverpfad gelten die Freigabeberechtigungen nicht. Dort werden nur die Dateisystemberechtigungen ausgewertet.

Deshalb kann ein lokaler Test auf dem Server funktionieren, während der Zugriff über SMB fehlschlägt.

---

12. Lesen, Ändern und Vollzugriff unterscheiden

Typische NTFS-Rechte:

Recht	Bedeutung
Ordnerinhalt anzeigen	Ordner durchsuchen und Inhalte auflisten
Lesen	Inhalte und Eigenschaften lesen
Schreiben	Dateien oder Daten erstellen beziehungsweise schreiben
Lesen und Ausführen	Dateien lesen und ausführbare Dateien starten
Ändern	lesen, schreiben, ausführen und löschen
Vollzugriff	zusätzlich Berechtigungen und Eigentum verwalten

Für normale gemeinsame Datenordner reicht häufig `Ändern`. `Vollzugriff` sollte nicht ohne fachlichen Grund vergeben werden.

---

13. Löschen benötigt besondere Beachtung

Zum Löschen eines Objekts kann abhängig von der ACL eines der folgenden Rechte entscheidend sein:

- `Löschen` auf der Datei oder dem Ordner;

- `Unterordner und Dateien löschen` auf dem übergeordneten Ordner.

Dadurch können scheinbar widersprüchliche Situationen entstehen:

- Benutzer kann eine Datei ändern, aber nicht löschen;
- Benutzer kann eine Datei löschen, obwohl die Datei selbst keinen offensichtlichen Lösch-Eintrag zeigt;
- Benutzer kann Dateien erstellen, aber nicht umbenennen;
- Benutzer kann Ordner öffnen, aber bestimmte Unterordner nicht auflisten.

Die Berechtigungen müssen deshalb auf dem betroffenen Objekt und dem übergeordneten Ordner geprüft werden.

---

14. Vererbung kontrollieren

```
(Get-Acl 'D:\Freigaben\Daten\Abteilung').AreAccessRulesProtected
```

Mögliche Zustände:

- Vererbung aktiv;
- Vererbung deaktiviert und geerbte Einträge kopiert;
- Vererbung deaktiviert und geerbte Einträge entfernt;
- einzelne explizite Rechte ergänzen die geerbten Rechte;
- explizite Verweigerung schränkt geerbte Zulassung ein.

Typische Fehler:

- neuer Unterordner übernimmt unerwartete Rechte;
- Vererbung wurde an einer Zwischenebene unterbrochen;
- Berechtigung gilt nur für den aktuellen Ordner;
- Berechtigung gilt nur für Unterordner;
- migrierte Dateien besitzen alte ACLs;
- Eigentümer oder Vererbungsquelle stimmt nicht mehr.

Berechtigungen sollten nicht rekursiv ersetzt werden, bevor Umfang, Vererbung und Rückweg vollständig geklärt sind.

---

15. Gruppenmitgliedschaften prüfen

AD-Mitgliedschaften eines Benutzers:

```
Get-ADPrincipalGroupMembership max.mustermann |
    Select-Object Name
```

Aktuelle Gruppen im Anmeldetoken:

```
whoami /groups
```

Aktuelles Konto:

```
whoami
```

Benutzer-SID:

```
whoami /user
```

Berechtigungen des aktuellen Tokens:

```
whoami /priv
```

Wichtige Unterscheidung:

```
Mitgliedschaft im Active Directory
        ≠
Mitgliedschaft im bereits erzeugten Anmeldetoken
```

Wurde ein Benutzer gerade einer Gruppe hinzugefügt, kann eine erneute Anmeldung erforderlich sein. Eine bloße Sperrung und Entsperrung des Bildschirms erzeugt normalerweise kein vollständig neues interaktives Anmeldetoken.

---

16. Effektive Berechtigungen bewerten

Die grafische Registerkarte befindet sich üblicherweise unter:

```
Eigenschaften
→ Sicherheit
→ Erweitert
→ Effektiver Zugriff
```

Dabei muss der richtige Benutzer beziehungsweise Sicherheitsprinzipal ausgewählt werden.

Zu berücksichtigen sind:

- direkte Benutzerrechte;
- verschachtelte Gruppen;
- Domänen- und lokale Gruppen;
- geerbte Rechte;
- explizite Rechte;
- Verweigerungen;
- aktuelles Token;
- Share- und NTFS-Ebene;
- Zugriff über DFS oder direkt auf den Zielserver.

Die Anzeige der effektiven NTFS-Rechte ersetzt nicht die Prüfung der Freigabeberechtigungen.

---

17. Zulassen und Verweigern

Eine explizite Verweigerung kann ein ansonsten gewährtes Recht blockieren. Trotzdem darf nicht vereinfacht angenommen werden, dass jede sichtbare Verweigerung immer sämtliche Zulassungen überschreibt.

Die Auswertung hängt unter anderem ab von:

- expliziten und geerbten Einträgen;
- Benutzer- und Gruppenzugehörigkeit;
- Reihenfolge der kanonischen ACL;
- betroffenem Einzelrecht;
- Objekt- und Vererbungsbereich;
- Share- und NTFS-Ebene.

Verweigerungen sollten sparsam verwendet werden. Eine saubere Gruppen- und Ordnerstruktur ist häufig leichter zu analysieren.

---

18. Access-Based Enumeration

Access-Based Enumeration kann Ordner vor Benutzern ausblenden, die darauf keine Berechtigung besitzen.

Einstellung anzeigen:

```
Get-SmbShare -Name Daten |
    Select-Object FolderEnumerationMode
```

Mögliche Folge:

- Ordner existiert;
- direkter Zugriff kann abhängig von den Rechten möglich sein;

- Ordner erscheint beim Auflisten der Freigabe nicht.

Ein ausgeblendeter Ordner wurde daher nicht zwangsläufig gelöscht oder nicht repliziert.

---

19. Geöffnete Dateien und SMB-Sitzungen prüfen

Auf dem Dateiserver:

```
Get-SmbSession
```

Geöffnete Dateien:

```
Get-SmbOpenFile
```

Gefiltert nach Pfad:

```
Get-SmbOpenFile |
    Where-Object {
        $_.Path -like '*\Daten\*'
    }
```

Wichtige Informationen:

- Clientcomputer;
- Benutzername;
- Sitzungs-ID;
- Dateipfad;
- Anzahl geöffneter Dateien;
- verbundene Zeit;
- Leerlaufzeit;
- verwendeter SMB-Dialekt.

Eine Sitzung oder Datei darf nicht ungeprüft geschlossen werden. Nicht gespeicherte Daten können verloren gehen.

---

20. Dateisperren untersuchen

Typische Meldungen:

- Datei wird von einem anderen Prozess verwendet;
- Zugriff verweigert;

- Dokument ist für die Bearbeitung gesperrt;
- schreibgeschützter Zugriff;
- Umbenennen oder Löschen nicht möglich.

Mögliche Ursachen:

- Datei ist auf einem anderen Client geöffnet;
- Anwendung verwendet eine eigene Sperrdatei;
- Virenscanner oder Indexdienst greift auf die Datei zu;
- Backup- oder Synchronisationssoftware hält ein Handle;
- Prozess auf dem Server verwendet die Datei;
- vorherige Anwendungssitzung wurde nicht sauber beendet;
- Benutzer besitzt kein Änderungs- oder Löschrecht;
- Datei oder Ordner ist schreibgeschützt;
- Anwendung verwendet ein eigenes Check-out-Verfahren.

Werkzeuge:

- `Get-SmbOpenFile`;
- Computerverwaltung → Freigegebene Ordner → Geöffnete Dateien;
- Sysinternals Handle;
- Process Explorer;
- Process Monitor;
- anwendungsspezifische Protokolle.

Nicht jede Meldung über eine „gesperrte Datei“ beweist eine technische SMB-Sperre. Anwendungen können eigene Sperrmechanismen verwenden.

---

21. SMB-Serverkonfiguration prüfen

```
Get-SmbServerConfiguration
```

Ausgewählte Werte:

```
Get-SmbServerConfiguration |
    Select-Object EnableSMB1Protocol,
                  EnableSMB2Protocol,
                  RequireSecuritySignature,
                  EncryptData,
                  EnableLeasing,
                  EnableOplocks,
                  AuditSmb1Access
```

Clientkonfiguration:

```
Get-SmbClientConfiguration
```

Zu prüfen sind:

- unterstützter SMB-Dialekt;
- SMB-Signierung;
- SMB-Verschlüsselung;
- Gastzugriff;
- alte SMB-Versionen;
- Richtlinienänderungen;
- Kompatibilität mit NAS, Scanner oder Altgerät;
- Abweichungen zwischen funktionierendem und betroffenem Client.

SMB 1 darf nicht pauschal als Problemlösung aktiviert werden. Das Protokoll ist veraltet und besitzt erhebliche Sicherheitsnachteile. Bei Altgeräten ist eine Aktualisierung, Segmentierung oder Ablösung zu prüfen.

---

22. Verwendeten SMB-Dialekt bestimmen

```
Get-SmbConnection |
    Select-Object ServerName,
                  ShareName,
                  Dialect,
                  Signed,
                  Encrypted
```

Mögliche Beobachtungen:

- moderner Client verwendet unerwartet alten Dialekt;
- Signierung wird verlangt, aber nicht unterstützt;
- Verschlüsselung wird verlangt, aber nicht ausgehandelt;
- Verbindung zu einem alten NAS scheitert;
- Verbindung über einen anderen Namen erzeugt einen anderen Authentifizierungsweg.

Die tatsächlich verwendete Verbindung muss geprüft werden. Eine allgemeine Servereinstellung beweist noch nicht, welcher Dialekt in einer bestimmten Sitzung ausgehandelt wurde.

---

23. Kerberos und NTLM bei SMB

Tickets prüfen:

```
klist
```

Für SMB ist typischerweise ein Dienstticket für einen SPN nach folgendem Muster relevant:

```
cifs/fileserver01
```

SPN suchen:

```
setspn -Q cifs/fileserver01
```

Mit FQDN:

```
setspn -Q cifs/fileserver01.ad.example.local
```

Mögliche Ursachen für NTLM statt Kerberos:

- Zugriff über IP-Adresse;
- fehlender oder falscher SPN;
- Zugriff über nicht registrierten Alias;
- DNS-Problem;
- keine geeignete Vertrauensbeziehung;
- Anwendung oder Gerät unterstützt Kerberos nicht;
- Kerberos schlägt fehl und NTLM-Fallback ist möglich.

Ein erfolgreicher SMB-Zugriff beweist nicht automatisch, dass Kerberos verwendet wurde.

---

24. Zugriff über Alias prüfen

Beispiel:

```
\\fileserver01\Daten
\\datenserver\Daten
```

Beide Namen können auf dieselbe IP-Adresse zeigen, aber für Kerberos unterschiedliche Dienstidentitäten darstellen.

Zu prüfen sind:

- DNS-Eintrag des Alias;
- CIFS-SPN für den verwendeten Namen;

- Konto, dem der SPN zugeordnet ist;
- Cluster- oder Computerkonto;
- doppelte SPNs;
- vorhandene Kerberos-Tickets;
- Server- und SMB-Konfiguration.

Ein zusätzlicher DNS-CNAME allein stellt noch nicht sicher, dass Kerberos über den Alias funktioniert.

---

25. DFS-Namespace untersuchen

Ein DFS-Pfad kann Benutzer auf einen oder mehrere tatsächliche Zielserver verweisen:

```
\\ad.example.local\Daten\Abteilung
```

DFS-Namespace-Informationen:

```
Get-DfsnRoot
```

Ordner und Ziele:

```
Get-DfsnFolder
```

```
Get-DfsnFolderTarget
```

Clientseitige DFS-Informationen:

```
dfsutil /pktinfo
```

DFS-Cache anzeigen:

```
dfsutil /pktinfo
```

Zu prüfen sind:

- Namespace erreichbar;
- DFS-Ordner vorhanden;
- Zielserver korrekt;
- Ziel aktiviert;

- Client verwendet das erwartete Ziel;
- Standortzuordnung korrekt;
- Zielserver erreichbar;
- DNS-Auflösung des tatsächlichen Zielservers;
- Berechtigungen auf jedem Ziel;
- Replikationsstatus;
- veralteter Client-Referral-Cache.

---

26. DFS-Namespace und DFS-Replikation unterscheiden

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

Ein funktionierender Namespace beweist nicht, dass die Daten repliziert wurden. Umgekehrt kann die Replikation funktionieren, während ein Namespace-Ziel falsch konfiguriert oder nicht erreichbar ist.

Typisches Fehlerbild:

- Benutzer erreicht den DFS-Pfad;
- abhängig vom ausgewählten Zielserver fehlen Dateien;
- Dateien besitzen unterschiedliche Versionen;
- Rechte unterscheiden sich zwischen Zielen;
- ein Replikationspartner ist verzögert oder gestört.

---

27. DFS-Replikation prüfen

Relevanter Ereignisprotokollpfad:

```
Ereignisanzeige
→ Anwendungs- und Dienstprotokolle
→ DFS Replication
```

PowerShell:

```
Get-WinEvent -FilterHashtable @{
    LogName   = 'DFS Replication'
    StartTime = (Get-Date).AddHours(-4)
} |
    Select-Object TimeCreated,
```

```
    Id,
    LevelDisplayName,
    Message
```

Replikationsgruppen:

```
Get-DfsReplicationGroup
```

Mitgliedschaften:

```
Get-DfsrMembership
```

Verbindungen:

```
Get-DfsrConnection
```

Zu dokumentieren sind:

- Replikationsgruppe;
- replizierter Ordner;
- Quell- und Zielserver;
- betroffene Richtung;
- letzter Fehler;
- Zeitpunkt;
- freier Speicherplatz;
- Datenbankzustand;
- Backlog;
- Konflikt- oder Staging-Bereich;
- letzte Änderungen.

Eine manuell erzwungene Synchronisation ist keine erste Diagnosemaßnahme.

---

28. Offline Files und Clientcache

Windows kann Netzwerkdateien lokal zwischenspeichern. Dadurch können Benutzer zeitweise mit einer lokalen Kopie arbeiten.

Mögliche Fehlerbilder:

- alte Dateiversion wird angezeigt;
- Synchronisierung schlägt fehl;
- Datei ist offline verfügbar, obwohl der Server erreichbar sein sollte;

- Konflikt zwischen lokaler und serverseitiger Änderung;
- Netzlaufwerk wird als offline angezeigt;
- unterschiedliche Benutzer sehen unterschiedliche Stände;
- Anwendung arbeitet weiter, obwohl der Server nicht erreichbar ist.

Zu prüfen sind:

- Synchronisierungscenter;
- Offlineverfügbarkeit;
- Netzwerkstatus;
- verwendeter UNC- beziehungsweise DFS-Pfad;
- Konflikte;
- Ereignisprotokolle;
- GPO-Konfiguration;
- Speicherplatz im lokalen Cache.

Der Offlinecache darf nicht ungeprüft zurückgesetzt werden. Nicht synchronisierte Benutzerdaten könnten verloren gehen.

---

29. Quotas und freier Speicherplatz

Freien Speicherplatz prüfen:

```
Get-Volume
```

Dateisystemlaufwerke:

```
Get-PSDrive -PSProvider FileSystem
```

FSRM-Quotas:

```
Get-FsrmQuota
```

Mögliche Symptome:

- Datei kann nicht gespeichert werden;
- Kopieren bricht ab;
- „Nicht genügend Speicherplatz“;
- Benutzer kann kleine, aber keine großen Dateien speichern;
- Anwendung meldet nur einen allgemeinen Schreibfehler;
- Freigabe ist erreichbar, Änderungen schlagen jedoch fehl;
- DFS-R oder Druckspooler arbeitet nicht mehr.

Zu unterscheiden sind:

- physischer Datenträger voll;
- Thin-Provisioning-Pool voll;
- Benutzer- oder Ordnerquota erreicht;
- VSS- oder Snapshotbereich belegt Speicher;
- temporärer Speicherplatz erschöpft;
- Dateisystem besitzt ein anderes Limit;
- Backend-Speicher des NAS oder SAN ist voll.

---

30. Lange Pfade und Dateinamen

Mögliche Ursachen:

- gesamter Pfad ist zu lang;
- Anwendung unterstützt lange Pfade nicht;
- Dateiname enthält nicht unterstützte Zeichen;
- Name endet problematisch mit Punkt oder Leerzeichen;
- reservierter Gerätename wird verwendet;
- Anwendung besitzt ein eigenes kürzeres Pfadlimit;
- Archiv- oder Synchronisationssoftware kann den Pfad nicht verarbeiten;
- Quell- und Zielsystem verwenden unterschiedliche Namensregeln.

Typische reservierte Namen unter Windows sind beispielsweise:

```
CON
PRN
AUX
NUL
COM1
LPT1
```

Die Unterstützung langer Pfade hängt nicht nur vom Betriebssystem ab. Auch Anwendung, API und Konfiguration müssen sie unterstützen.

---

31. Eigentümer und ACL-Zustand

Eigentümer anzeigen:

```
(Get-Acl 'D:\Freigaben\Daten').Owner
```

Mögliche Probleme:

- nicht mehr auflösbare SID;
- migriertes Benutzer- oder Gruppenkonto;
- Eigentümer ist nicht mehr vorhanden;
- ACL wurde bei Kopie oder Restore verändert;
- Vererbung ist beschädigt oder unerwartet unterbrochen;
- Backup wurde ohne Sicherheitsinformationen wiederhergestellt;
- Dateien stammen aus einer anderen Domäne;
- NAS bildet Windows-SIDs nicht korrekt ab.

Nicht auflösbare SIDs beweisen allein keinen Fehler. Sie können noch wirksame Sicherheitskennungen ehemaliger oder nicht erreichbarer Domänenkonten darstellen und müssen vor einer Entfernung zugeordnet werden.

---

32. Ereignisprotokolle für SMB prüfen

Wichtige Protokollpfade können sein:

```
Microsoft
→ Windows
→ SMBClient
→ Connectivity
```

```
Microsoft
→ Windows
→ SMBClient
→ Security
```

```
Microsoft
→ Windows
→ SMBServer
→ Operational
```

```
Microsoft
→ Windows
→ SMBServer
→ Security
```

PowerShell-Beispiel:

```
Get-WinEvent -FilterHashtable @{
    LogName   = 'Microsoft-Windows-SMBClient/Connectivity'
    StartTime = (Get-Date).AddHours(-2)
} |
    Select-Object TimeCreated,
                  Id,
                  LevelDisplayName,
                  Message
```

Zusätzlich können relevant sein:

- System;
- Sicherheit;
- DNS Client Events;
- Kerberos;
- NETLOGON;
- DFS Replication;
- Failover Clustering;
- NTFS;
- Disk;
- StorPort;
- anwendungsspezifische Protokolle.

Event-ID, Provider, Zeitpunkt, Server, Client und vollständiger Ereignistext müssen gemeinsam bewertet werden.

---

33. SMB-Netzwerkverkehr untersuchen

Bei unklarem Netzwerk- oder Protokollfehler kann ein Paketmitschnitt erforderlich sein.

Typische Filter:

```
tcp.port == 445
```

```
smb2
```

```
ip.addr == 192.0.2.20 && tcp.port == 445
```

Zu untersuchen sind:

- TCP-Verbindungsaufbau;
- Retransmissions;
- TCP Reset;
- SMB-Negotiation;
- Session Setup;
- Tree Connect;
- Authentifizierungsfehler;
- SMB-Statuscodes;
- lange Antwortzeiten;
- Verbindungsabbruch;
- Server- oder Clientverzögerung.

Ein Paketmitschnitt kann Datei- und Benutzernamen sowie weitere vertrauliche Informationen enthalten und muss geschützt gespeichert werden.

---

34. Druckpfad verstehen

```
Anwendung
  ↓
Druckertreiber
  ↓
Windows-Druckwarteschlange
  ↓
Spooler
  ↓
Druckserver oder direkter TCP/IP-Port
  ↓
Netzwerk
  ↓
Drucker
  ↓
Druckwerk, Papier und Verbrauchsmaterial
```

Die Meldung „Drucker druckt nicht“ kann daher verursacht werden durch:

- Anwendung;
- Treiber;
- Spooler;
- Queue;
- Druckserver;
- Berechtigung;
- Netzwerk;

- DNS;
- Portkonfiguration;
- SNMP;
- Druckerzustand;
- Papier oder Toner;
- mechanische Störung.

---

35. Druckerfehler exakt eingrenzen

Zu dokumentieren sind:

- Druckername;
- Freigabename;
- Druckserver;
- Drucker-IP;
- DNS-Name;
- Treibername und Version;
- verwendeter Port;
- betroffener Client;
- betroffener Benutzer;
- Anwendung;
- Dokumenttyp;
- Zeitpunkt;
- Status der Warteschlange;
- vollständiger Fehlertext;
- funktioniert eine Windows-Testseite;
- funktioniert ein anderes Dokument;
- funktioniert der Druck aus einer anderen Anwendung;
- funktioniert ein anderer Benutzer;
- funktioniert ein anderer Drucker;
- betrifft es einen oder alle Clients.

Diese Tests trennen Anwendung, Benutzer, Client, Treiber, Queue, Server und Gerät voneinander.

---

36. Drucker und Warteschlangen anzeigen

PowerShell:

```
Get-Printer
```

Ausgewählte Eigenschaften:

```
Get-Printer |
    Select-Object Name,
                  ComputerName,
                  DriverName,
                  PortName,
                  Shared,
                  ShareName,
                  PrinterStatus,
                  JobCount
```

Bestimmter Drucker:

```
Get-Printer -Name 'Drucker-01'
```

Druckaufträge:

```
Get-PrintJob -PrinterName 'Drucker-01'
```

Druckerkonfiguration:

```
Get-PrintConfiguration -PrinterName 'Drucker-01'
```

---

37. Print Spooler prüfen

```
Get-Service Spooler
```

Ausführlicher:

```
Get-CimInstance Win32_Service `
    -Filter "Name='Spooler'" |
    Select-Object Name,
                  State,
                  StartMode,
                  StartName,
                  ProcessId
```

Abhängigkeiten:

```
Get-Service Spooler -DependentServices
```

Ein Neustart des Spoolers:

```
Restart-Service Spooler
```

verändert den Zustand und kann alle lokalen beziehungsweise serverseitigen Druckaufträge beeinflussen. Vorher sind zu prüfen:

- betrifft der Fehler alle Drucker;
- hängen einzelne oder alle Aufträge;
- befinden sich wichtige Aufträge in der Queue;
- stürzt der Spooler wiederholt ab;
- welcher Treiber oder Print Processor ist beteiligt;
- was zeigen Ereignisprotokolle;
- besteht ein Wartungs- oder Freigabefenster.

---

38. Druckaufträge kontrollieren

```
Get-PrintJob -PrinterName 'Drucker-01' |
    Select-Object ID,
                  DocumentName,
                  UserName,
                  SubmittedTime,
                  JobStatus,
                  Size
```

Einzelnen Auftrag entfernen:

```
Remove-PrintJob `
    -PrinterName 'Drucker-01' `
    -ID 17
```

Vor dem Entfernen prüfen:

- gehört der Auftrag zum untersuchten Fehler;
- handelt es sich um einen produktiv wichtigen Auftrag;
- wird die Queue dadurch für andere Benutzer freigegeben;
- tritt der Fehler mit einem neuen Testauftrag wieder auf.

Nicht sofort die gesamte Warteschlange leeren, wenn ein einzelner Auftrag die Ursache sein könnte.

---

39. Druckerport prüfen

```
Get-PrinterPort
```

Bestimmter Port:

```
Get-PrinterPort -Name 'IP_192.0.2.50'
```

Zu prüfen sind:

- richtige IP-Adresse;
- richtiger DNS-Name;
- Standard-TCP/IP-Port;
- Raw oder LPR;
- TCP-Port 9100;
- LPR-Queue-Name;
- SNMP aktiviert;
- SNMP-Community;
- WSD statt festem TCP/IP-Port;
- Druckeradresse nach DHCP-Änderung;
- alter Port nach Druckeraustausch.

Porttest für RAW Printing:

```
Test-NetConnection 192.0.2.50 -Port 9100
```

Mögliche weitere Protokolle hängen vom Drucksystem ab, beispielsweise IPP, IPPS, LPR oder SMB.

---

40. SNMP-Statusfehler

Ein Drucker kann erreichbar und druckfähig sein, aber in Windows als offline erscheinen, wenn die SNMP-Statusabfrage fehlschlägt.

Mögliche Ursachen:

- SNMP auf dem Drucker deaktiviert;
- falsche Community;
- UDP 161 blockiert;
- SNMP-Version nicht kompatibel;

- Drucker beantwortet Statusabfragen fehlerhaft;
- falscher Port verweist auf ein anderes Gerät;
- Sicherheitsrichtlinie verhindert die Abfrage.

Das Deaktivieren des SNMP-Status kann als kontrollierter Diagnosetest dienen. Es ist jedoch keine allgemeine Lösung, weil dadurch echte Gerätestatusinformationen verloren gehen können.

---

41. Druckertreiber untersuchen

Installierte Treiber:

```
Get-PrinterDriver
```

Mögliche Treiberprobleme:

- falsches Druckermodell;
- alter Treiber;
- beschädigtes Treiberpaket;
- herstellerspezifischer und universeller Treiber kollidieren;
- Architektur- oder Betriebssysteminkompatibilität;
- Treiber verursacht Spooler-Absturz;
- Point-and-Print-Richtlinie verhindert Installation;
- Treiber unterstützt Gerätefunktion nicht;
- Druckdatenformat passt nicht zum Drucker;
- Upgrade hinterließ alte Treiberkomponenten.

Treiber dürfen nicht ungeprüft auf einem produktiven Druckserver ersetzt werden. Dadurch können mehrere Warteschlangen und Benutzer betroffen sein.

---

42. Windows-Testseite verwenden

Eine Testseite trennt die Anwendung teilweise vom restlichen Druckpfad.

PowerShell über WMI/CIM:

```
Invoke-CimMethod `
    -ClassName Win32_Printer `
    -MethodName PrintTestPage `
    -Arguments @{} `
    -Filter "Name='Drucker-01'"
```

Bewertung:

Ergebnis	Wahrscheinlicher Bereich
Testseite funktioniert, Anwendung nicht	Anwendung, Dokument, Format oder anwendungsspezifische Einstellungen
Testseite bleibt in Queue	Spooler, Treiber, Port oder Druckserver
Auftrag verlässt Queue, Drucker reagiert nicht	Port, Netzwerk, Protokoll oder Gerät
Auftrag wird gedruckt, Ausgabe fehlerhaft	Treiber, Druckersprache, Gerätekonfiguration oder Hardware
alle Drucker betroffen	Spooler, Server, Richtlinie oder gemeinsamer Dienst
nur ein Drucker betroffen	Queue, Port, Treiber oder Gerät

---

43. Druckereignisse prüfen

Wichtiger Protokollpfad:

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

Das Operational-Protokoll muss je nach System zunächst aktiviert werden.

PowerShell:

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

Zusätzlich prüfen:

- PrintService/Admin;
- System;
- Anwendung;

- Spooler-Absturzereignisse;
- Treiberereignisse;
- Netzwerkereignisse;
- Protokolle des Druckservers;
- Weboberfläche und Ereignisprotokoll des Druckers.

---

44. CUPS unter Linux und macOS prüfen

Druckerstatus:

```
lpstat -t
```

Standarddrucker:

```
lpstat -d
```

Warteschlange:

```
lpq
```

Druckaufträge:

```
lpstat -o
```

Auftrag abbrechen:

```
cancel <Auftrags-ID>
```

Alle Aufträge eines Druckers abbrechen:

```
cancel -a <Druckername>
```

CUPS-Dienst unter systemd:

```
systemctl status cups
```

Protokoll:

```
journalctl -u cups
```

Je nach System können die CUPS-Protokolle zusätzlich unter folgendem Pfad liegen:

```
/var/log/cups/
```

Zu prüfen sind:

- CUPS-Dienst;
- Queue-Zustand;
- deaktivierte oder angehaltene Queue;
- Geräte-URI;
- Treiber beziehungsweise PPD;
- Filterfehler;
- Berechtigungen;
- Erreichbarkeit des Druckers;
- IPP-, LPR- oder RAW-Verbindung;
- vollständiger CUPS-Fehlertext.

---

45. Typische Fehlerbilder

Symptom	Mögliche Ursache	Nächster Test
Servername nicht erreichbar	DNS oder Netzwerk	`Resolve-DnsName`, `Test-NetConnection`
IP funktioniert, Name nicht	DNS, Alias oder SPN	Kurzname, FQDN und DNS-Einträge vergleichen
TCP 445 nicht erreichbar	Firewall, Routing oder SMB-Dienst	Porttest und Serverstatus
Freigabe nicht gefunden	falscher Name oder Freigabe fehlt	`Get-SmbShare`, `net share`
Freigabe öffnet sich, Unterordner nicht	NTFS-Rechte oder ABE	ACL und effektiven Zugriff prüfen
Datei lesbar, aber nicht änderbar	fehlendes Schreib- oder Änderungsrecht	Share- und NTFS-Rechte
Datei änderbar, aber nicht löschbar	Löschrecht oder Eltern-ACL	Datei- und Ordner-ACL prüfen
Zugriff lokal möglich, über SMB nicht	Freigaberecht oder SMB-Pfad	`Get-SmbShareAccess`
neuer Gruppeneintrag wirkt nicht	altes Anmeldetoken	`whoami /groups`, erneute Anmeldung
Zugriff verweigert trotz Gruppenmitgliedschaft	Verweigerung, falsches Token oder NTFS-Recht	effektiven Zugriff prüfen
Datei angeblich in Verwendung	offenes Handle oder Anwendungssperre	`Get-SmbOpenFile`
Zugriff über Alias schlägt fehl	SPN oder Kerberos	`klist`, `setspn -Q`

Symptom	Mögliche Ursache	Nächster Test
DFS-Pfad zeigt alte Daten	falsches Ziel oder DFS-R-Störung	`dfsutil /pktinfo`, DFS-R-Ereignisse
Dateien unterscheiden sich je nach Client	unterschiedliche DFS-Ziele	Zielserver und Replikation vergleichen
Speichern schlägt ab bestimmter Größe fehl	Quota oder freier Speicher	Volume und FSRM prüfen
Drucker für alle Benutzer offline	Netzwerk, Port oder Gerät	Porttest und Druckerstatus
nur ein Benutzer kann nicht drucken	Berechtigung oder Benutzerprofil	Druckerrechte und Vergleichsbenutzer
nur eine Anwendung druckt nicht	Anwendung oder Dokument	Windows-Testseite
alle Drucker eines Servers betroffen	Spooler oder Druckserver	Dienst und Ereignisse
nur eine Queue betroffen	Auftrag, Treiber oder Port	Queue, Treiber und Port
Auftrag bleibt in Warteschlange	Spooler, Treiber oder Port	PrintService-Protokoll
Auftrag verschwindet, kein Ausdruck	Protokoll, Gerät oder Druckersprache	Druckerprotokoll und Port
Drucker fälschlich offline	SNMP-Statusabfrage	SNMP-Konfiguration prüfen
Spooler stürzt wiederholt ab	Treiber oder Print Processor	Ereignisse und Treiberzuordnung

---

46. Vorgehensweise bei „Zugriff verweigert“

1. vollständigen UNC-Pfad dokumentieren.
2. Benutzer und Client bestimmen.
3. konkrete fehlgeschlagene Aktion erfassen.
4. verwendetes Konto mit `whoami` prüfen.
5. aktuelle Gruppen mit `whoami /groups` prüfen.
6. Servername und Zieladresse prüfen.
7. SMB-Verbindung und verwendete Anmeldedaten prüfen.
8. Freigabeberechtigungen auslesen.
9. NTFS-Berechtigungen des betroffenen Objekts prüfen.
10. Vererbung und Eigentümer berücksichtigen.
11. Berechtigungen des übergeordneten Ordners prüfen.
12. explizite Verweigerungen untersuchen.
13. Test mit einem funktionierenden Benutzer durchführen.
14. genau eine kontrollierte Korrektur umsetzen.
15. Zugriff mit der ursprünglichen Aktion erneut testen.
16. Rechte nach dem Minimalprinzip dokumentieren.

---

47. Vorgehensweise bei „Datei ist gesperrt“

1. Dateiname und vollständigen Pfad erfassen.
2. Benutzer, Client und Anwendung bestimmen.

3. prüfen, ob Lesen oder nur Bearbeiten fehlschlägt.
4. `Get-SmbOpenFile` auf dem Dateiserver auswerten.
5. Anwendungssperrdateien berücksichtigen.
6. Serverprozesse mit Handle oder Process Explorer prüfen.
7. Virenscanner, Backup und Synchronisation berücksichtigen.
8. Rechte zum Ändern und Löschen prüfen.
9. Benutzer kontaktieren, der die Datei geöffnet hält.
10. ungespeicherte Daten ausschließen.
11. erst danach gezielt das Handle oder die Sitzung schließen.
12. Datei erneut öffnen, ändern und speichern.
13. Ursache und Auswirkung dokumentieren.

---

48. Vorgehensweise bei DFS-Problemen

1. logischen DFS-Pfad dokumentieren.
2. Client und Benutzer bestimmen.
3. DFS-Referral des Clients prüfen.
4. tatsächlichen Zielserver dokumentieren.
5. Zielserver per DNS und TCP 445 prüfen.
6. direkten UNC-Pfad zum Zielserver testen.
7. Namespace-Ordner und Ziele prüfen.
8. AD-Site und Zielpriorität berücksichtigen.
9. Rechte auf allen Zielen vergleichen.
10. Dateistände und Zeitstempel vergleichen.
11. DFS-R-Ereignisse prüfen.
12. Replikationsrichtung und Backlog untersuchen.
13. nur die nachgewiesene Ursache korrigieren.
14. Clientzugriff und Replikation erneut prüfen.

---

49. Vorgehensweise bei Druckproblemen

1. Drucker, Queue, Server und Port dokumentieren.
2. genaue Meldung und Zeitpunkt erfassen.
3. Umfang bestimmen: ein Benutzer, Client, Drucker oder alle.
4. Warteschlange und Auftragsstatus prüfen.
5. Windows-Testseite auslösen.
6. Spoolerstatus prüfen.
7. PrintService-Ereignisse auswerten.
8. Druckername und IP-Adresse prüfen.
9. tatsächlichen Druckerport testen.
10. SNMP-Status kontrollieren.
11. Treibername und Version prüfen.
12. Berechtigungen der Queue prüfen.
13. Gerätestatus und Verbrauchsmaterial prüfen.
14. genau eine kontrollierte Maßnahme durchführen.

15. Testseite und ursprüngliches Dokument erneut drucken.
16. Ereignisse und Queue nachkontrollieren.

---

50. Maßnahmen und Rückwege

Ursache: falsche Freigabeberechtigung

Nachweis:

- SMB-Verbindung funktioniert;
- Freigabe existiert;
- `Get-SmbShareAccess` zeigt kein ausreichendes Recht;
- NTFS-Berechtigung wäre ausreichend.

Maßnahme:

- vorgesehene Sicherheitsgruppe mit minimal erforderlichem Freigaberecht eintragen.

Rollback:

- ursprüngliche Freigabe-ACL dokumentiert wiederherstellen.

Verifikation:

- Verbindung neu testen;
- konkrete Dateiaktion ausführen;
- Freigabe- und NTFS-Rechte erneut kontrollieren.

Ursache: fehlende NTFS-Berechtigung

Nachweis:

- Freigaberecht ist ausreichend;
- effektiver NTFS-Zugriff zeigt das fehlende Einzelrecht;
- Fehler tritt am konkreten Ordner oder Objekt auf.

Maßnahme:

- Berechtigung über die vorgesehene Sicherheitsgruppe und passende Vererbung korrigieren.

Rollback:

- vorherige ACL sichern und bei Bedarf wiederherstellen.

Verifikation:

- Lesen, Erstellen, Ändern und Löschen entsprechend dem Sollzustand einzeln testen.

Ursache: altes Anmeldetoken

Nachweis:

- AD-Gruppenmitgliedschaft ist vorhanden;
- `whoami /groups` enthält die Gruppe noch nicht;
- Berechtigungen der Gruppe sind korrekt.

Maßnahme:

- Benutzer kontrolliert ab- und erneut anmelden.

Rollback:

- nicht erforderlich, wenn keine Konfiguration verändert wurde.

Verifikation:

- `whoami /groups`;
- Zugriff auf die vorgesehene Ressource;
- keine zusätzlichen Rechte vergeben.

Ursache: falsches DFS-Ziel

Nachweis:

- Client-Referral zeigt auf unerwarteten Server;
- direkter Zugriff auf das vorgesehene Ziel funktioniert;
- Namespace-Konfiguration oder Zielstatus ist fehlerhaft.

Maßnahme:

- Zielstatus, Priorität oder Namespace-Zuordnung nach dokumentiertem Sollzustand korrigieren.

Rollback:

- ursprüngliche DFS-Konfiguration dokumentiert wiederherstellen.

Verifikation:

- Referral erneut prüfen;
- DFS-Pfad öffnen;
- Dateistand und Rechte kontrollieren.

Ursache: fehlerhafter Druckerport

Nachweis:

- Queue und Spooler funktionieren;
- Port zeigt auf eine alte oder falsche Adresse;
- vorgesehener Drucker ist unter der richtigen Adresse erreichbar.

Maßnahme:

- Queue kontrolliert auf den korrekten Port umstellen.

Rollback:

- ursprünglichen Port und seine Einstellungen dokumentieren.

Verifikation:

- Windows-Testseite;
- ursprüngliches Dokument;
- Queue- und Druckerstatus;
- PrintService-Ereignisse.

---

51. Nachkontrolle

Nach einer Maßnahme sind mindestens folgende Punkte zu prüfen:

- vorgesehener Servername wird korrekt aufgelöst;
- TCP 445 ist erreichbar;
- SMB-Verbindung verwendet das vorgesehene Konto;
- SMB-Dialekt und Sicherheitsanforderungen sind plausibel;
- Freigabe zeigt auf den richtigen Pfad;
- Freigabeberechtigungen entsprechen dem Sollzustand;
- NTFS-Berechtigungen entsprechen dem Minimalprinzip;
- Vererbung funktioniert wie vorgesehen;
- aktuelles Token enthält die benötigten Gruppen;
- Lesen, Erstellen, Ändern und Löschen wurden getrennt getestet;
- keine unerwünschten zusätzlichen Rechte wurden vergeben;
- keine wichtigen Dateien oder Sitzungen wurden getrennt;
- DFS verweist auf das vorgesehene Ziel;
- replizierte Daten sind konsistent;
- ausreichend Speicherplatz ist vorhanden;
- Quotas sind plausibel;
- Druckwarteschlange verarbeitet neue Aufträge;
- Druckerport zeigt auf das richtige Gerät;

- Treiber und Spooler arbeiten stabil;
- praktische Benutzerfunktion wurde getestet;
- temporäre Diagnoseänderungen wurden zurückgenommen;
- Ursache, Maßnahme, Rückweg und Ergebnis wurden dokumentiert.

---

52. Dokumentationsbeispiel

Symptom:
Der Benutzer konnte Dateien in der Freigabe lesen, aber keine neue Datei im Unterordner „Projekte“ erstellen.

Zeitpunkt:
02.08.2026, 11:26 Uhr MESZ

Benutzer:
max.mustermann

Client:
CLIENT-17

Pfad:
\\fileserver01.ad.example.local\Daten\Projekte

Nachweis:
DNS-Auflösung und TCP 445 waren erfolgreich.
Die SMB-Verbindung verwendete das vorgesehene Domänenkonto.
Die Freigabeberechtigung gewährte der zuständigen Gruppe „Ändern“.
Die NTFS-Auswertung zeigte jedoch nur Leserechte auf dem Unterordner.
Die Vererbung war an diesem Unterordner deaktiviert worden.

Ursache:
Bei einer früheren manuellen ACL-Änderung wurde die Vererbung auf dem Unterordner unterbrochen. Dadurch fehlte der vorgesehenen Gruppe das Änderungsrecht.

Maßnahme:
Nach Sicherung der bestehenden ACL wurde die freigegebene Berechtigungsstruktur des übergeordneten Ordners wiederhergestellt.

Rollback:

Die zuvor exportierte ACL kann wieder eingespielt werden.

Verifikation:

Der Benutzer kann Dateien lesen, erstellen, ändern und löschen.

Er kann keine Berechtigungen verändern.

Andere Abteilungsordner bleiben weiterhin unzugänglich.

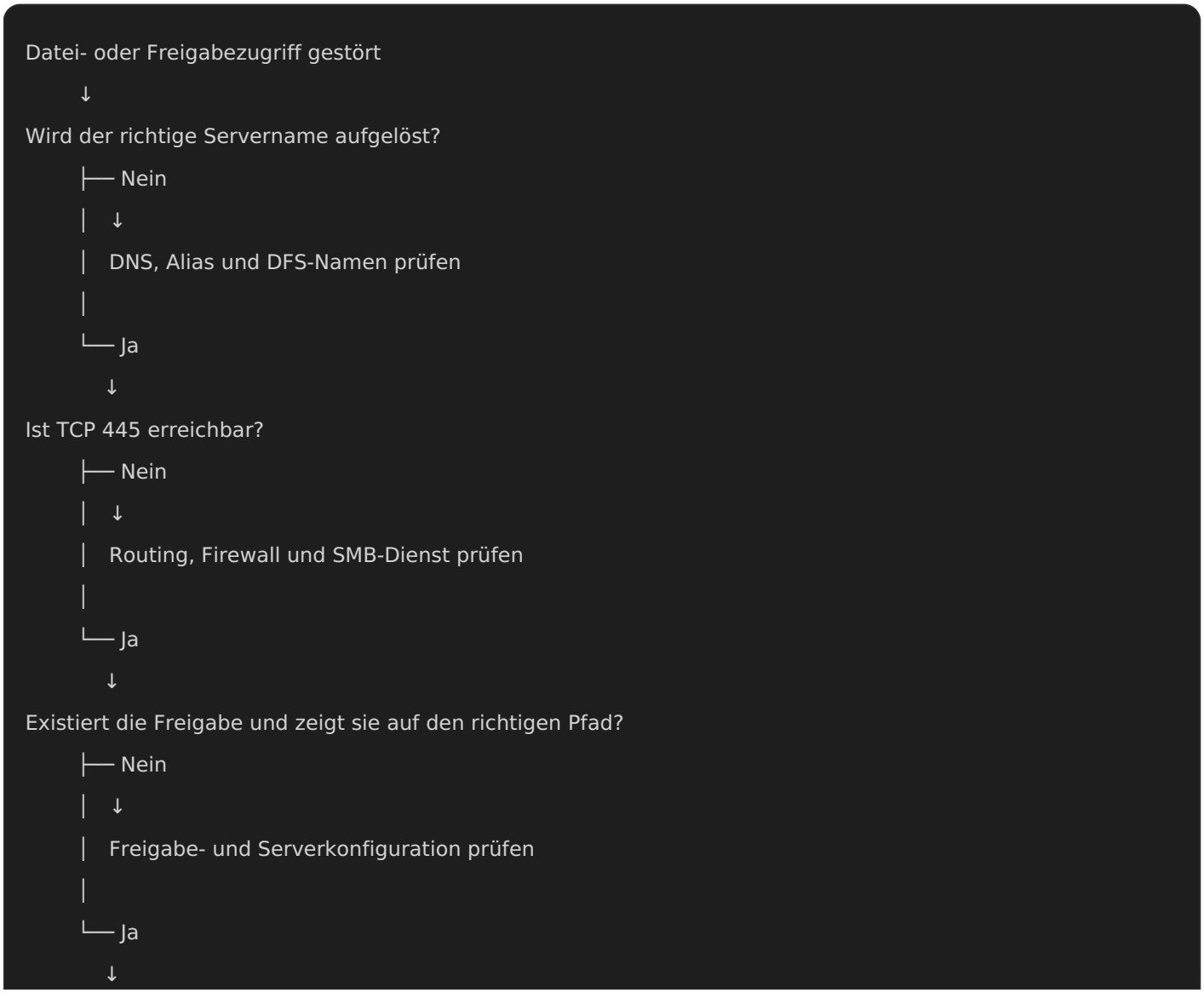
Es wurden keine zusätzlichen administrativen Rechte vergeben.

Prävention:

Berechtigungsänderungen erfolgen künftig ausschließlich über dokumentierte Sicherheitsgruppen und werden durch einen Test des effektiven Zugriffs geprüft.

---

53. Entscheidungsbaum



```
Wird das vorgesehene Benutzerkonto verwendet?
    ├── Nein
    │   ↓
    │   bestehende Verbindungen und Anmeldedaten prüfen
    │
    └── Ja
        ↓
Sind Freigabeberechtigungen ausreichend?
    ├── Nein
    │   ↓
    │   Freigabe-ACL kontrolliert korrigieren
    │
    └── Ja
        ↓
Sind NTFS-Berechtigungen ausreichend?
    ├── Nein
    │   ↓
    │   ACL, Vererbung, Gruppen und Token prüfen
    │
    └── Ja
        ↓
Ist nur eine Datei oder Aktion betroffen?
    ├── Ja
    │   ↓
    │   Sperre, Einzel-ACL, Pfad, Quota und Anwendung prüfen
    │
    └── Nein
        ↓
DFS, Storage, Serverzustand und zentrale Abhängigkeiten prüfen
```

---

54. Typische Prüfungsfragen

Warum reicht ein erfolgreicher Ping zum Dateiserver nicht als Funktionsnachweis?

Antwort anzeigen

Ein Ping prüft eine bestimmte ICMP-Kommunikation. Er beweist weder die Erreichbarkeit von TCP 445 noch eine erfolgreiche SMB-Authentifizierung oder ausreichende Freigabe- und NTFS-Berechtigungen.

Welche Berechtigungen wirken bei einem SMB-Zugriff auf einen NTFS-Ordner?

Antwort anzeigen

Es wirken sowohl die Freigabe- als auch die NTFS-Berechtigungen. Für den Zugriff über das Netzwerk ergibt sich die wirksame Berechtigung aus der restriktiveren Kombination beider Ebenen.

Warum kann der lokale Zugriff auf einen Serverordner funktionieren, während der SMB-Zugriff fehlschlägt?

Antwort anzeigen

Beim lokalen Zugriff werden keine SMB-Freigabeberechtigungen ausgewertet. Über das Netzwerk wirken zusätzlich zu den NTFS-Rechten auch die Freigabeberechtigungen und die SMB-Authentifizierung.

Warum kann eine neue Gruppenmitgliedschaft noch nicht wirksam sein?

Antwort anzeigen

Die Gruppe kann bereits im Active Directory eingetragen sein, aber im aktuellen Anmeldetoken fehlen. Häufig ist eine erneute Benutzeranmeldung erforderlich, damit ein neues Token erzeugt wird.

Worin unterscheiden sich DFS Namespace und DFS Replication?

Antwort anzeigen

DFS Namespace stellt einen einheitlichen logischen Zugriffspfad bereit. DFS Replication synchronisiert Ordnerinhalte zwischen mehreren Servern. Beide Funktionen können unabhängig voneinander gestört sein.

Warum sollte eine geöffnete SMB-Datei nicht sofort zwangsweise geschlossen werden?

Antwort anzeigen

Die zugehörige Anwendung kann noch nicht gespeicherte Änderungen besitzen. Ein erzwungenes Schließen kann Datenverlust oder beschädigte Anwendungszustände

verursachen.

Warum beweist ein erfolgreicher Zugriff über einen Alias nicht automatisch die Verwendung von Kerberos?

Antwort anzeigen

Fehlt ein passender CIFS-SPN für den Alias, kann der Zugriff abhängig von der Umgebung über NTLM erfolgen. Tickets und SPN-Zuordnung müssen gesondert geprüft werden.

Welche Funktion besitzt der Print Spooler?

Antwort anzeigen

Der Print Spooler nimmt Druckaufträge entgegen, verarbeitet beziehungsweise zwischenspeichert sie und übergibt sie über die konfigurierte Warteschlange und den Druckerport an das Ziel.

Warum kann ein Drucker fälschlich als offline angezeigt werden?

Antwort anzeigen

Die eigentliche Druckverbindung kann funktionieren, während die SNMP-Statusabfrage fehlschlägt. Ursachen können eine falsche Community, blockiertes UDP 161 oder eine fehlerhafte SNMP-Konfiguration sein.

---

55. Prüfungsfallen

- erfolgreichen Ping mit funktionierendem SMB gleichsetzen;
- nur die IP-Adresse, aber nicht den verwendeten Namen prüfen;
- verbundenes Laufwerk prüfen, ohne den UNC-Pfad zu bestimmen;
- Freigabe- und NTFS-Berechtigungen verwechseln;
- nur die ACL der Freigabeebene prüfen;
- nur die ACL des übergeordneten Ordners prüfen;
- Vererbung und Einzelrechte nicht berücksichtigen;
- Lesen, Schreiben, Ändern und Löschen gleichsetzen;
- Gruppenmitgliedschaft im AD mit aktuellem Token gleichsetzen;
- Benutzer direkt statt über Sicherheitsgruppen berechtigen;
- Benutzer zur Fehlerbehebung in eine Administratorgruppe aufnehmen;
- pauschal Vollzugriff gewähren;

- Verweigerung ungeprüft entfernen;
- ACLs rekursiv ersetzen, ohne Rückweg festzulegen;
- Eigentümer übernehmen, ohne die ursprüngliche ACL zu sichern;
- alte oder unbekannte SID ungeprüft löschen;
- alle SMB-Verbindungen pauschal trennen;
- Datei-Handle schließen, ohne ungespeicherte Daten auszuschließen;
- SMB 1 als schnelle Kompatibilitätslösung aktivieren;
- erfolgreichen Zugriff mit Kerberos-Authentifizierung gleichsetzen;
- DNS-Alias ohne CIFS-SPN verwenden;
- DFS-Namespace und DFS-Replikation verwechseln;
- DFS-Cache leeren, bevor das verwendete Ziel dokumentiert wurde;
- Replikation ungeprüft erzwingen;
- Offlinecache zurücksetzen, ohne nicht synchronisierte Daten zu prüfen;
- nur freien Speicherplatz, aber keine Quota prüfen;
- Druckwarteschlange vollständig leeren, obwohl nur ein Auftrag betroffen ist;
- Spooler sofort neu starten, ohne Ereignisse und Queue zu sichern;
- Treiber auf einem produktiven Druckserver ungeprüft ersetzen;
- SNMP dauerhaft deaktivieren, ohne die eigentliche Ursache zu prüfen;
- Drucker per IP neu installieren, obwohl nur DNS oder Port falsch ist;
- mehrere Änderungen gleichzeitig durchführen;
- nur eine Testseite, aber nicht die ursprüngliche Benutzerfunktion prüfen.

---

56. Checkliste

- [ ] vollständiger UNC-Pfad wurde dokumentiert.
- [ ] betroffener Benutzer wurde bestimmt.
- [ ] betroffener Client wurde bestimmt.
- [ ] genaue fehlgeschlagene Aktion wurde erfasst.
- [ ] Fehlertext und Fehlercode wurden dokumentiert.
- [ ] Zeitpunkt und Zeitzone wurden erfasst.
- [ ] Servername wurde aufgelöst.
- [ ] Ziel-IP wurde mit dem Sollzustand verglichen.
- [ ] Kurzname, FQDN und Alias wurden unterschieden.
- [ ] TCP 445 wurde geprüft.
- [ ] tatsächliche SMB-Verbindung wurde geprüft.
- [ ] verwendetes Benutzerkonto wurde geprüft.
- [ ] bestehende Verbindungen wurden berücksichtigt.
- [ ] gespeicherte Anmeldedaten wurden berücksichtigt.
- [ ] Freigabe und lokaler Zielpfad wurden geprüft.
- [ ] Freigabeberechtigungen wurden geprüft.

- [ ] NTFS-Berechtigungen wurden geprüft.
- [ ] Vererbung wurde geprüft.
- [ ] Eigentümer wurde geprüft.
- [ ] explizite Verweigerungen wurden geprüft.
- [ ] Rechte des übergeordneten Ordners wurden berücksichtigt.
- [ ] AD-Gruppenmitgliedschaften wurden geprüft.
- [ ] aktuelles Anmeldetoken wurde geprüft.
- [ ] effektiver Zugriff wurde bewertet.
- [ ] Lesen, Erstellen, Ändern und Löschen wurden getrennt getestet.
- [ ] Access-Based Enumeration wurde bei unsichtbaren Ordnern berücksichtigt.
- [ ] geöffnete SMB-Dateien wurden geprüft.
- [ ] Anwendungssperren wurden berücksichtigt.
- [ ] SMB-Dialekt wurde geprüft.
- [ ] Signierung und Verschlüsselung wurden berücksichtigt.
- [ ] Kerberos und NTLM wurden unterschieden.
- [ ] CIFS-SPN wurde bei Aliasproblemen geprüft.
- [ ] DFS-Referral wurde bei DFS-Pfaden geprüft.
- [ ] tatsächlicher DFS-Zielserver wurde bestimmt.
- [ ] DFS-Replikation wurde bei abweichenden Datenständen geprüft.
- [ ] Offline Files wurden berücksichtigt.
- [ ] freier Speicherplatz wurde geprüft.
- [ ] Quotas wurden geprüft.
- [ ] Pfadlänge und Dateiname wurden berücksichtigt.
- [ ] SMB- und Systemereignisse wurden geprüft.
- [ ] Drucker, Queue, Server und Port wurden dokumentiert.
- [ ] Spoolerstatus wurde geprüft.
- [ ] Druckaufträge wurden geprüft.
- [ ] Druckerport und Zieladresse wurden geprüft.
- [ ] SNMP-Status wurde geprüft.
- [ ] Treibername und Version wurden geprüft.
- [ ] PrintService-Protokolle wurden geprüft.
- [ ] Windows-Testseite wurde verwendet.
- [ ] ursprüngliche Benutzerfunktion wurde erneut getestet.
- [ ] genau eine kontrollierte Maßnahme wurde durchgeführt.

- [ ] Rückweg wurde festgelegt.
- [ ] keine unnötigen Rechte wurden vergeben.
- [ ] Ursache, Maßnahme und Ergebnis wurden dokumentiert.

---

57. Schnellreferenz

Beobachtung	Nächstes Werkzeug
Servername zeigt auf falsche IP	`Resolve-DnsName`, `nslookup`
SMB-Port nicht erreichbar	`Test-NetConnection -Port 445`
bestehende Netzlaufwerke unklar	`net use`, `Get-SmbMapping`
verwendetes SMB-Konto unklar	`Get-SmbConnection`
Freigabe fehlt	`Get-SmbShare`, `net share`
Freigaberecht unklar	`Get-SmbShareAccess`
NTFS-Recht unklar	`Get-Acl`, `icacls`
aktuelle Gruppen unklar	`whoami /groups`
Datei gesperrt	`Get-SmbOpenFile`, Handle
SMB-Sitzung unklar	`Get-SmbSession`
SMB-Version unklar	`Get-SmbConnection`
Alias funktioniert nicht	`klist`, `setspn -Q`
DFS-Ziel unklar	`dfsutil /pktinfo`
DFS-Konfiguration unklar	`Get-DfsnFolderTarget`
DFS-R-Störung	DFS-Replication-Protokoll
Speicherplatz unklar	`Get-Volume`, `Get-PSDrive`
Quota vermutet	`Get-FsrmQuota`
Druckerstatus unklar	`Get-Printer`
Druckaufträge hängen	`Get-PrintJob`
Spoolerstatus unklar	`Get-Service Spooler`
Druckerport unklar	`Get-PrinterPort`
Treiber unklar	`Get-PrinterDriver`
Druckereignis gesucht	PrintService/Operational
CUPS-Status unklar	`lpstat -t`, `journalctl -u cups`

Merksatz

> Bei Datei- und Freigabefehlern wird vom Namen über TCP 445, SMB-Sitzung und Authentifizierung bis zu Freigabe- und NTFS-Rechten geprüft. Bei Druckfehlern wird der Weg von Anwendung und Treiber über Queue, Spooler und Port bis zum physischen Drucker verfolgt. Rechte, Sitzungen, Dateien und Druckaufträge werden erst verändert, wenn Ursache, Auswirkung und Rückweg geklärt sind.

Quellen und weiterführende Dokumentation

Offizielle Microsoft-Dokumentation

- Microsoft Learn – SMB troubleshooting
- Microsoft Learn – Get-SmbConnection
- Microsoft Learn – Get-SmbShare
- Microsoft Learn – Get-SmbShareAccess
- Microsoft Learn – Get-SmbSession
- Microsoft Learn – Get-SmbOpenFile
- Microsoft Learn – Get-SmbServerConfiguration
- Microsoft Learn – Get-Acl
- Microsoft Learn – Icacls
- Microsoft Learn – File and folder permissions
- Microsoft Learn – DFS Namespaces overview
- Microsoft Learn – DFS Replication overview
- Microsoft Learn – DFSR troubleshooting
- Microsoft Learn – Get-DfsnFolderTarget
- Microsoft Learn – Get-DfsReplicationGroup
- Microsoft Learn – Get-Printer
- Microsoft Learn – Get-PrintJob
- Microsoft Learn – Get-PrinterPort
- Microsoft Learn – Get-PrinterDriver
- Microsoft Learn – Windows print troubleshooting

Offizielle CUPS-Dokumentation

- OpenPrinting – CUPS Command-Line Printing
- OpenPrinting – CUPS Administration
- OpenPrinting – CUPS Documentation
