# Migration eines Windows Domain Controllers: Server 2016 -> Server 2022

Ziel: Einen bestehenden Domain Controller (Windows Server 2016) durch einen neuen Domain Controller (Windows Server 2022) ersetzen.

Ausgangslage: 2 Domain Controller im Forest/der Domain, davon ist einer bereits Windows Server 2022.

Hinweis: Dies ist die empfohlene „Swing Migration“ (neuen 2022-DC hinzufügen, dann 2016-DC demoten) statt In-Place-Upgrade.

## Vorbereitung

#### Voraussetzungen

- Der vorhandene Server 2022 DC repliziert sauber und ist voll funktionsfähig.
- Der Server 2016 DC soll ersetzt (demoted) werden.
- Admin-Zugriff (Domain Admin / Enterprise Admin je nach Schritt) ist vorhanden.

#### Vorbereitung (Checkliste)

1. Wartungsfenster festlegen
2. Backups erstellen:
    1. System State (mindestens) von allen DCs
    2. Alternativ/zusätzlich: Bare-Metal/VM-Backup (Snapshots nur mit Vorsicht bei DCs)
3. Dokumentation erfassen:
    1. Hostnames, IPs, Sites/Subnetze, DNS-Forwarder, Rollen/Dienste (DHCP/NPS/CA/DFS/etc.)
4. Namens-/IP-Plan:
    1. Soll der neue 2022-DC später Hostname/IP des alten 2016-DC übernehmen? (optional)

## 1. Bestandsaufnahme & Health-Check (vor Änderungen)

#### 1.1 Replikation & DC-Gesundheit prüfen

Auf einem DC oder Admin-System mit RSAT:

- DCDIAG:
    - `dcdiag /v`
- Replikationsübersicht:
    - `repadmin /replsummary`
- Detail (optional):

    - `repadmin /showrepl * /csv > showrepl.csv`

Erwartung: Keine wiederkehrenden Fehler (DNS, Replication, KCC, SYSVOL).

#### 1.2 Rollen/Dienste ermitteln

- FSMO-Rollen prüfen:
    - `netdom query fsmo`
- DNS-Design prüfen:
    - Läuft DNS auf beiden DCs?
    - Forwarder / Conditional Forwarder korrekt?
- Global Catalog prüfen:
    - „Active Directory Sites and Services“ → Server → NTDS Settings → Global Catalog
- Zeitquelle prüfen:
    - `w32tm /query /status`
    - `w32tm /query /source`

## 2. Migrationsmuster festlegen

#### Option A (empfohlen): Neuer 2022-DC -> 2016-DC entfernen

- Sauberer, geringeres Risiko, Standardvorgehen in der Praxis.

#### Option B: In-Place-Upgrade 2016 -> 2022

- Möglich, aber bei DCs meist nur wählen, wenn es Gründe dafür gibt.

Diese Anleitung beschreibt Option A.

## 3. Neuen Windows Server 2022 vorbereiten

1. Windows Server 2022 installieren
2. Patchen (Windows Update), Reboot
3. Statische IP konfigurieren
4. DNS-Server auf bestehenden Domain DNS zeigen lassen (typisch: 2022-DC als Primary, 2016-DC als Secondary oder umgekehrt gemäß Policy)
5. Server in die Domain aufnehmen, Reboot

Optional:

1. Temporären Namen/IP verwenden, wenn später Name/IP des alten 2016-DC übernommen werden soll.

# 4. AD DS Rolle installieren & zum Domain Controller promoten

Auf dem neuen 2022-Server:

1. Server Manager → Add roles and features
2. Rolle: „Active Directory Domain Services“
3. Optional/typisch: „DNS Server“ (wenn DNS auf DCs betrieben wird)
4. Danach: „Promote this server to a domain controller“

Wizard-Auswahl:

1. „Add a domain controller to an existing domain“
2. Credentials: Domain Admin
3. Optionen:
    1. DNS: aktivieren (wenn geplant)
    2. Global Catalog: aktivieren (typisch)
    3. RODC: deaktiviert
4. DSRM-Passwort setzen
5. Installieren und Reboot

# 5. Nach dem Promote: Validierung

### 5.1 Replikation prüfen

- `repadmin /replsummary`
- `dcdiag /q`

### 5.2 DNS prüfen

- Auf Clients/Servern:
    - `nslookup domain.tld`
    - `nslookup _ldap._tcp.dc._msdcs.domain.tld`
- DNS-Manager:
    - AD-integrierte Zonen vorhanden (inkl. _msdcs)
    - SRV Records vorhanden
    - Forwarders/Conditional Forwarders korrekt

### 5.3 SYSVOL/NETLOGON prüfen

- `\\NEUERDC\SYSVOL` erreichbar?
- `\\NEUERDC\NETLOGON` erreichbar?

# 6. FSMO-Rollen auf Server 2022 verschieben (falls noch auf 2016)

### 6.1 Prüfen, wo FSMO liegt

- `netdom query fsmo`

### 6.2 Rollen verschieben (PowerShell)

Auf einem System mit AD-Modul (z.B. DC/Management-Server):

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2022-Haupt" -
OperationMasterRole 0,1,2,3,4
```

Rollen-IDs:

- 0 = PDC Emulator
- 1 = RID Master
- 2 = Infrastructure Master
- 3 = Schema Master
- 4 = Domain Naming Master

Danach erneut prüfen:

- `netdom query fsmo`

# 7. Zeitdienst (W32Time) sauber konfigurieren

Wenn der PDC Emulator gewechselt hat, muss der PDC eine saubere Zeitquelle haben.

Auf dem PDC Emulator (Beispiel mit pool.ntp.org):

```
w32tm /config /manualpeerlist:"0.pool.ntp.org 1.pool.ntp.org"
/syncfromflags:manual /reliable:yes /update
net stop w32time && net start w32time
w32tm /resync /force
w32tm /query /status
```

# 8. Dienste/Abhängigkeiten vom 2016-DC migrieren (falls vorhanden)

Vor der Demotion klären/migrieren (Beispiele):

1. DNS (falls 2016 DNS-Server ist):

    1. Sicherstellen, dass 2022 DNS die Zonen/SRV sauber hat (AD-integriert i.d.R. automatisch)
    2. Forwarder/Conditional Forwarder prüfen
2. DHCP (falls auf 2016-DC):
    1. Export/Import oder DHCP-Failover neu konfigurieren
    2. DHCP Option 006 (DNS) auf beide 2022-DCs setzen
3. NPS/RADIUS, AD CS (CA), DFS (Namespace/Replication), File/Print, ADFS, WSUS etc.:
    1. Je Dienst eigener Migrationspfad

Wichtig:

1. Statische DNS-Einträge auf Clients/Servern auf den alten 2016-DC identifizieren und umstellen.

# 9. Server 2016 DC demoten (Herabstufen)

Voraussetzungen:

- Replikation ist fehlerfrei
- FSMO-Rollen liegen nicht mehr auf dem 2016-DC
- DNS/Dienste/Abhängigkeiten sind migriert

Vorgehen:

1. Server Manager → AD DS → More… → „Demote this domain controller“
2. Optional: „Remove DNS delegation“ (falls relevant)
3. Lokales Admin-Passwort setzen (Server wird Mitgliedsserver)
4. Demotion abschließen, Reboot

# 10. Aufräumen nach Demotion

### 10.1 AD-Objekte prüfen

1. „Active Directory Users and Computers“:
    1. Computerobjekt unter „Domain Controllers“ sollte entfernt sein
2. „Active Directory Sites and Services“:
    1. Serverobjekt und „NTDS Settings“ sollten entfernt sein

### 10.2 DNS Cleanup

1. Alte A/AAAA Records, SRV Records prüfen/entfernen
2. _msdcs Einträge müssen auf aktive DCs zeigen

### 10.3 Metadaten-Cleanup (nur wenn Demotion nicht sauber war)

1. `ntdsutil` (Metadata cleanup)
2. Sites/DNS manuell bereinigen (nur bei Bedarf)

# 11. Optional: Hostname/IP des alten DC übernehmen

Nur falls erforderlich (Legacy-Abhängigkeiten):

1. Alten 2016-Server nach Demotion aus der Domain entfernen oder endgültig abschalten
2. Sicherstellen, dass Name in AD/DNS nicht mehr existiert
3. Neuen 2022-Server umbenennen und/oder IP auf die alte IP setzen
4. Reboot
5. Prüfen: DNS, SPNs, Replikation, Eventlogs

Hinweis: Wenn möglich, ist „kein Name/IP-Recycling“ oft die robustere Variante.

# 12. Abschlusskontrollen

- Replikation:
  - `repadmin /replsummary`
- DC Health:
  - `dcdiag /q`
- Client-Checks:
  - Anmeldung testen, GPO-Verarbeitung:
    - `gpupdate /force`
    - `gpresult /r`
- Eventlogs prüfen:
  - Directory Service, DNS Server, System (keine wiederkehrenden Errors)

Ergebnis:

1. Beide DCs sind Windows Server 2022
2. Der alte Windows Server 2016 DC ist sauber entfernt
3. DNS/Time/FSMO/Replication sind stabil

From:
https://wiki.sebastianhetzel.net/ - **Sebastians IT-Wiki**

Permanent link:
**https://wiki.sebastianhetzel.net/win_server:dc_mig**

Last update: **2026/02/26 17:23**