

Zusätzlicher Domänen Controller einrichten

Beschreibung:

Es gibt Situationen, da möchte man einen alten Domänencontroller ersetzen oder einfach nur für die Sicherheit einen zweiten Domänencontroller haben.

Dies ist mittlerweile sehr einfach. Denn das PDC (PrimaryDomainController) und BDC (BackupDomainController) gibt es Gott sei dank schon lange nicht mehr.

Beides sind Master Master und replizieren sich gegenseitig. So können Benutzer und andere Änderungen vorgenommen werden, auf egal welchem der beiden. Es wird immer synchronisiert.

Vorraussetzungen:

Der alte Server sollte die Mindest Forest Domain Version des neuen Domain Controller haben. Beispiel bei Server 2025 darf der vorhandene Domain Controller nicht kleiner als Server 2016 sein. Es gibt unter Umständen die Fehlermeldung dass es kein 2016 ist, obwohl er es ist.

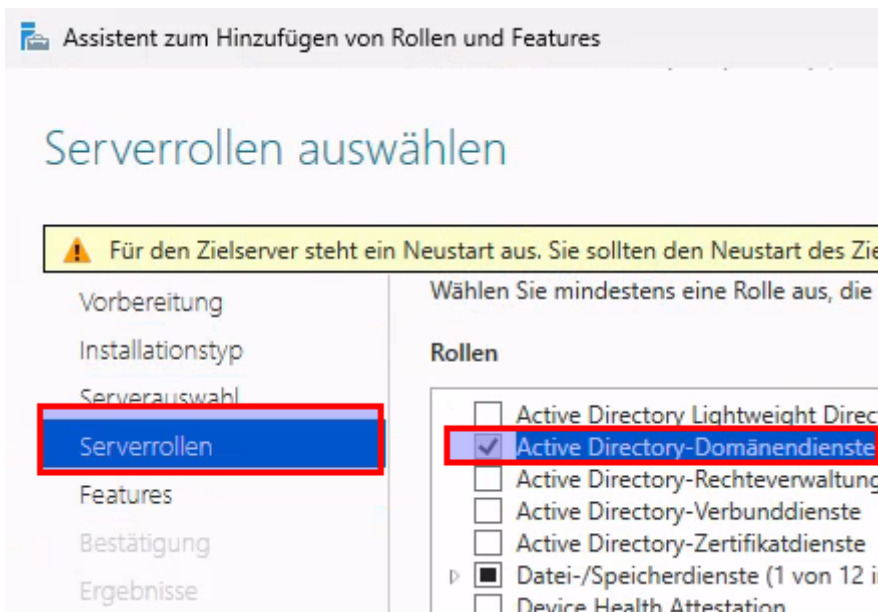
Das liegt daran, dass bei jedem Update vergessen wurde den Domänencontroller hochzustufen. Der Server ist zwar 2016 aber der Domänencontroller immer noch als Beispiel 2008, weil das einfach vergessen wurde.

Kann man aber fix nachholen, kein Beinbruch. Dazu aber später

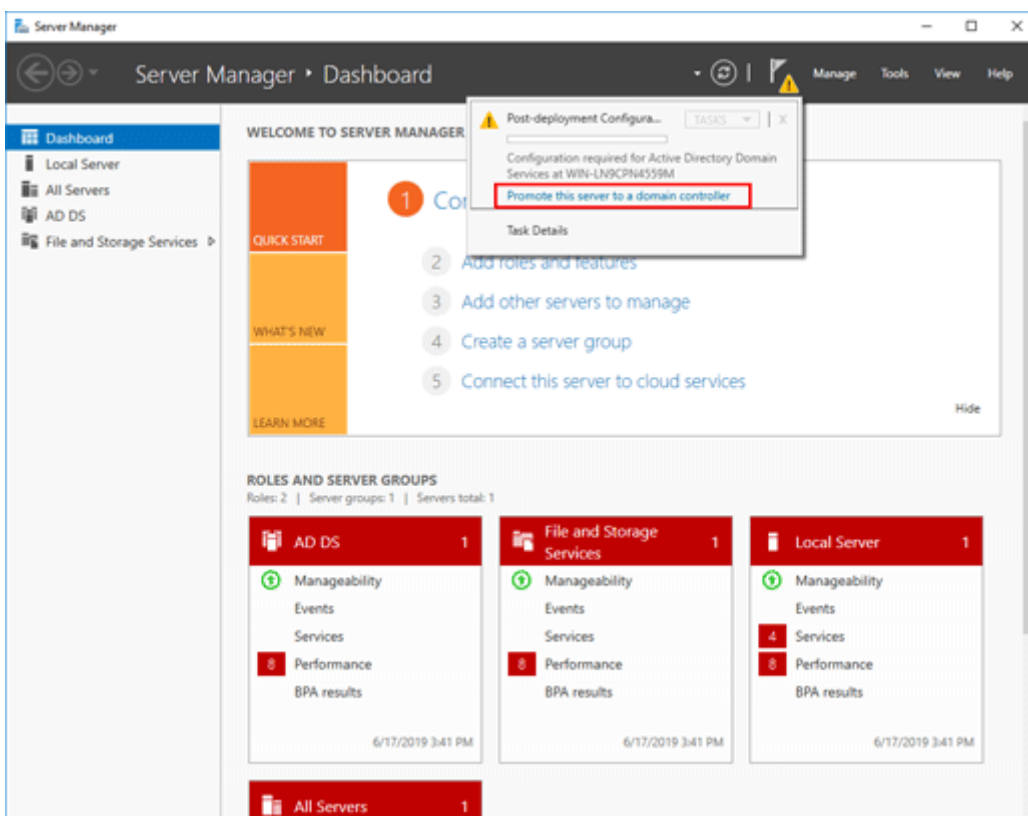
Das war auch schon alles an Voraussetzungen.

Durchführung:

1. Server installieren feste IP geben und dann in die vorhandene Domäne einfach erstmal aufnehmen
2. Dann über den Server Manager die Rolle Active Directory Domänendienste ->



Wenn die Rolle installiert ist, dann neustart und dann über die Flagge den Domain Controller konfigurieren.



Nun Domäne zu einer vorhandenen Domäne hinzufügen anklicken. Den Administrator das Kennwort und die Domäne mit Endung angeben (in der Regel .local)

Sollte dieser Fehler auftauchen was meistens der fall ist, deshalb hab ich die Meldung mit abfotografiert.

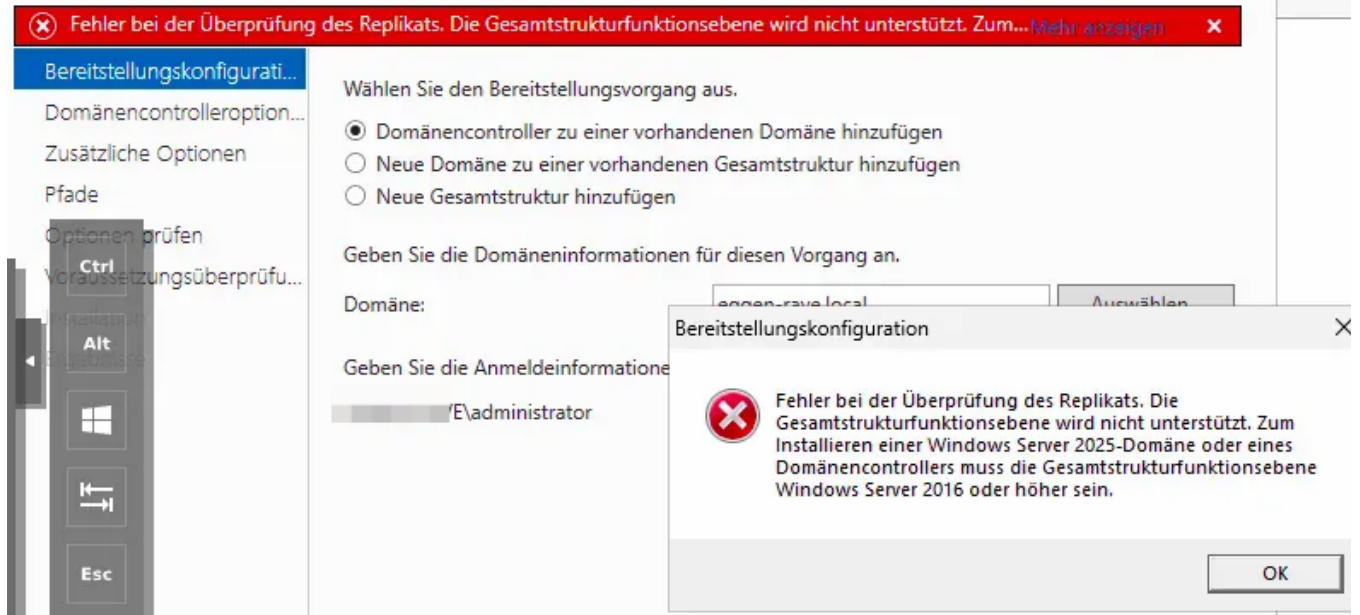
Dann liegt es daran, das der alte Server noch auf einer älteren Struktur als 2016 läuft. Hat nichts damit zu tun.

das der Server an sich schon 2016 ist.

Die Active Directory Struktur wurde aber nie aktualisiert. Muss man sich vorstellen ich aktualisiere ein Programm, aber die Datenbankstruktur wird nicht aktualisiert

Bereitstellungskonfiguration

ZIELSERVER
DC01. .local



Mit ein paar Befehlen bekommen wir raus, ob alles vorhanden ist und welche Version wir haben.

Erstmal Freigaben Checken, läuft auf dem bestehenden/alten Server DC überhaupt ein Domaincontroller.

Und den Replikationsdienst überprüfen, der kopiert ja die Daten auf den neuen DC

Dazu führen wir ein Powershell als Admin auf dem bestehenden/alten DC Server aus

```
# DFSR Status prüfen
dfsrdiag pollad
repadmin /replsummary

# SYSVOL-Freigabe vorhanden?
net share | findstr SYSVOL
```

Ausgabe:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\administrator> # DFSR Status prüfen
PS C:\Users\administrator> dfsrdiag pollad

Vorgang erfolgreich

PS C:\Users\administrator> repadmin /replsummary
```

Startzeit der Replikationszusammenfassung: 2025-12-05 15:41:46

Datensammlung für Replikationszusammenfassung wird gestartet.

Dieser Vorgang kann einige Zeit dauern.

....

Quell-DSA	Größtes Delta	Fehler/gesamt %%	Fehler
-----------	---------------	------------------	--------

Ziel-DSA	Größtes Delta	Fehler/gesamt %%	Fehler
----------	---------------	------------------	--------

```
PS C:\Users\administrator> # SYSVOL-Freigabe vorhanden?
```

```
PS C:\Users\administrator> net share | findstr SYSVOL
```

```
NETLOGON C:\Windows\SYSVOL\sysvol\<domainname>.local\SCRIPTS
```

```
SYSVOL C:\Windows\SYSVOL\sysvol Ressource für Anmeldeserver
```

Da das alles in Ordnung ist, checken wir jetzt die Version vom DC

```
Get-ADForest | Select-Object ForestMode
```

```
Get-ADDomain | Select-Object DomainMode
```

Ausgabe, wie wir sehen, sogar noch 2008R2 Version:

```
PS C:\Users\administrator> Get-ADForest | Select-Object ForestMode
```

```
ForestMode
```

```
-----
```

```
Windows2008R2Forest
```

```
PS C:\Users\administrator> Get-ADDomain | Select-Object DomainMode
```

```
DomainMode
```

```
-----
```

```
Windows2008R2Domain
```

Aber kein Ding, diese Stufen wir einfach auf 2016 hoch. Dazu einfach die fragen mit ja beantworten

```
# Erst Domäne anheben
Set-ADDomainMode -Identity "<domainname>.local" -DomainMode Windows2016Domain
#Dann den Forest anheben
Set-ADForestMode -Identity "<domainname>.local" -ForestMode Windows2016Forest
```

Ausgabe:

```
PS C:\Users\administrator> # Erst Domäne anheben
PS C:\Users\administrator> Set-ADDomainMode -Identity "<domainname>.local" -DomainMode
Windows2016Domain

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Set" für das Ziel "DC=<domainname>,DC=local".
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"): j
PS C:\Users\administrator>
PS C:\Users\administrator> # Dann Forest anheben
PS C:\Users\administrator> Set-ADForestMode -Identity "<domainname>.local" -ForestMode
Windows2016Forest

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Set" für das Ziel
"CN=Partitions,CN=Configuration,DC=<domainname>,DC=local".
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"): j
```

Nun nochmals überprüfen obs geklappt hat

```
Get-ADForest | Select-Object ForestMode
Get-ADDomain | Select-Object DomainMode
```

Ausgabe, wie wir sehen, endlich 2016

```
PS C:\Users\administrator> Get-ADForest | Select-Object ForestMode

ForestMode
-----
Windows2016Forest
```

```
PS C:\Users\administrator> Get-ADDomain | Select-Object DomainMode
```

```
DomainMode
```

```
-----
```

```
Windows2016Domain
```

nun können wir auf dem neuen/weiteren DC auf weiter klicken zbd die fehlermeldung ist weg.

Und alle Objekte werden repliziert. Nach einem neustart haben wir MASTER <-> MASTER DC

Alten DC entfernen:

Wenn man möchte und den alten DC los werden will, müssen wir den neuen als Primären machen: Dazu auf den neuem DC eine Powershell als Admin öffnen

1. FSMO-Rollen auf den neuen übertragen:
(DC01 durch den Namen deines neuen Servers ersetzen)

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC01" -OperationMasterRole  
SchemaMaster,DomainNamingMaster,PDCEmulator,RIDMaster,InfrastructureMaster
```

Prüfen obs geklappt hat.

```
PS C:\Users\administrator> netdom query fsmo  
Schemamaster          DC01.e<domainname>.local  
Domänennamen-Master  DC01.e<domainname>.local  
PDC                   DC01.e<domainname>.local  
RID-Pool-Manager     DC01.e<domainname>.local  
Infrastrukturmaster  DC01.e<domainname>.local  
Der Befehl wurde ausgeführt.
```

2. **NS umstellen** – überall wo der alte DC als DNS eingetragen ist (DHCP-Scope, Router, Drucker, Geräte mit statischer IP) auf den neuen zeigen lassen.
3. **Alten DC sauber demoten** (nicht einfach ausschalten!):
Erst nach dem Demote kannst du ihn abschalten. Wenn du ihn einfach ausknipst ohne Demote, hast du Leichen im AD und musst manuell aufräumen – das willst du nicht.

WICHTIG!!!!!! Auf dem alten DC Server eine Powershell als Admin öffnen

```
Uninstall-ADDSDomainController -DemoteOperationMasterRole:$true -  
RemoveApplicationPartitions:$true
```

Version #10

Erstellt: 6 Dezember 2025 12:03:28 von Admin

Zuletzt aktualisiert: 13 Dezember 2025 17:28:19 von Admin