

Domaincontrollerrollen übertragen

Der Text wurde bei einem Domaincontrollerumzug von Server 2003 auf Server 2012 geschrieben. Daher sind auch einzelne Hinweise für Server 2003 enthalten.

Ermittlung des DC mit allen FSMO-Rollen

```
netdom query fsmo
```

oder für ältere Systeme (Server 2003)

```
dsquery server -hasfsmo schema  
dsquery server -hasfsmo name  
dsquery server -hasfsmo rid  
dsquery server -hasfsmo pdc  
dsquery server -hasfsmo infr
```

Ergbnis:

```
Schema owner          OldDC.srv.domainname.local  
Domain role owner     OldDC.srv.domainname.local  
PDC role              OldDC.srv.domainname.local  
RID pool manager      OldDC.srv.domainname.local  
Infrastructure owner  OldDC.srv.domainname.local
```

DHCP-Server Konfigurieren

DHCP Adressbereiche müssen manuell eingerichtet werden da der Ex/Import von Server 2003 auf Server 2012 nicht funktioniert.

```
Pool:          192.168.1.120 - 192.168.1.179 /24 \\  
Lease :        8 tage \\  
Router:        192.168.1.3 \\  
DNS-Server:    192.168.1.7, 192.168.1.18, 192.168.1.25 \\  
DNS-Domänenname: srv.domainname.local \\  
Reservierungen: 36 (siehe tabelle unten) \\
```

```
Get-DhcpServerv4Reservation -ScopeId 192.168.1.0
```

Ergebnis:

IPAddress Type	ScopeId Description	ClientId	Name
----- -----	----- -----	-----	-----
192.168.1.120 aastra5380ip00085...	192.168.1.0 Both Palm	00-08-5d-90-fe-49	
192.168.1.121 aastra5380ip00085...	192.168.1.0 Both Tölke	00-08-5d-90-fe-4a	
...			
192.168.1.128 aastra5370ip00085...	192.168.1.0 Both Thinius	00-08-5d-90-c7-a0	
192.168.1.129 aastra5370ip00085...	192.168.1.0 Both Schmidt	00-08-5d-90-c7-a2	

aastra5370ip00085... = aastra5380ip<MAC-Adresse>.srv.domainname.local

DNS-Server Konfigurieren

1. DNS-Manager öffnen
2. DNS-Server anwählen
3. Weiterleitungen öffnen
4. externe Weiterleitungen eintragen

```
192.168.1.7      OldDC.srv.domainname.local \\
192.168.1.18   FirstDC.srv.domainname.local \\
```

Replizierungstest

```
repadmin /showrepl
```

Domaincontroller Diagnose

```
dcdiag
```

DNSZones verschieben

DomainDNSZones:

```
fsmoRoleOwner=CN=NTDS Settings,CN=OldDC,CN=Servers,CN=AD-Musterstadt-KHW01,CN=Sites,CN=Configuration,DC=srv,DC=domainname,DC=local
```

geändert in:

```
fsmoRoleOwner=CN=NTDS Settings,CN=SecondDC,CN=Servers,CN=AD-Musterstadt-KHW01,CN=Sites,CN=Configuration,DC=srv,DC=domainname,DC=local
```

ForestDNSZones:

```
fsmoRoleOwner=CN=NTDS Settings,CN=OldDC,CN=Servers,CN=AD-Musterstadt-KHW01,CN=Sites,CN=Configuration,DC=srv,DC=domainname,DC=local
```

geändert in:

```
fsmoRoleOwner=CN=NTDS Settings,CN=SecondDC,CN=Servers,CN=AD-Musterstadt-KHW01,CN=Sites,CN=Configuration,DC=srv,DC=domainname,DC=local
```

Umziehen der FSMO-Rollen

per Konsole

```
NTDSUTIL
ROLES // mit ROLES wechselt man zur "fsmo maintenance" in
dieser Ebene gibt man Connections ein.
Connect to Server SecondDC // zukünftiger Rolleninhaber
quit // In der „server connections“ Ebene muss man mit "quit"
oder „q“ erneut zur „fsmo maintenance“ Ebene wechseln.
// Nun können die Betriebsmasterrollen auf den fokussierten
DC übertragen werden: Transfer <Rolle>
Transfer schema master
Transfer domain naming master (gilt bis einschließlich Windows Server
2003!)
Transfer naming master (gilt ab Windows Server 2008!)
Transfer RID master
Transfer PDC
Transfer infrastructure master
```

per MMC

Active Directory-Schema	[schema]
Active Directory-Domänen und -Vertrauensstellungen	[name]
Active Directory-Benutzer und -Computer	[rid, pdc, infr]

NETDOM QUERY FSMO

Replizierungstest

```
repadmin /showrepl
```

Ergebnis:

Repadmin: Befehl "/showrepl" wird für den vollständigen DC "localhost" ausgeführt

AD-Musterstadt-KHW01\SecondDC

DSA-Optionen: IS_GC

Standortoptionen: (none)

DSA-Objekt-GUID: 655222cc-3dcc-4624-a010-9b258eebf6a1

DSA-Aufrufkennung: 53277abd-a966-4b4a-a432-776b8b39d91d

==== EINGEHENDE NACHBARN=====

DC=srv,DC=domainname,DC=local

AD-Musterstadt-KHW01\FirstDC über RPC

DSA-Objekt-GUID: f447de0e-8194-46ed-880f-398bb69dcf57

Letzter Versuch am 2015-08-24 13:21:42 war erfolgreich.

AD-Musterstadt-KHW01\OldDC über RPC

DSA-Objekt-GUID: b3e36e13-632f-4198-9ffc-17210cec326b

Letzter Versuch am 2015-08-24 13:21:43 war erfolgreich.

CN=Configuration,DC=srv,DC=domainname,DC=local

AD-Musterstadt-KHW01\OldDC über RPC

DSA-Objekt-GUID: b3e36e13-632f-4198-9ffc-17210cec326b

Letzter Versuch am 2015-08-24 13:08:38 war erfolgreich.

AD-Musterstadt-KHW01\FirstDC über RPC

DSA-Objekt-GUID: f447de0e-8194-46ed-880f-398bb69dcf57

Letzter Versuch am 2015-08-24 13:08:40 war erfolgreich.

CN=Schema,CN=Configuration,DC=srv,DC=domainname,DC=local

AD-Musterstadt-KHW01\OldDC über RPC

DSA-Objekt-GUID: b3e36e13-632f-4198-9ffc-17210cec326b

Letzter Versuch am 2015-08-24 13:07:55 war erfolgreich.

AD-Musterstadt-KHW01\FirstDC über RPC

DSA-Objekt-GUID: f447de0e-8194-46ed-880f-398bb69dcf57

Letzter Versuch am 2015-08-24 13:08:10 war erfolgreich.

DC=ForestDnsZones,DC=srv,DC=domainname,DC=local

AD-Musterstadt-KHW01\FirstDC über RPC

DSA-Objekt-GUID: f447de0e-8194-46ed-880f-398bb69dcf57

Letzter Versuch am 2015-08-24 13:07:38 war erfolgreich.

AD-Musterstadt-KHW01\OldDC über RPC

DSA-Objekt-GUID: b3e36e13-632f-4198-9ffc-17210cec326b

Letzter Versuch am 2015-08-24 13:07:41 war erfolgreich.

DC=DomainDnsZones,DC=srv,DC=domainname,DC=local

AD-Musterstadt-KHW01\FirstDC über RPC

DSA-Objekt-GUID: f447de0e-8194-46ed-880f-398bb69dcf57

Letzter Versuch am 2015-08-24 13:08:02 war erfolgreich.

AD-Musterstadt-KHW01\OldDC über RPC

DSA-Objekt-GUID: b3e36e13-632f-4198-9ffc-17210cec326b

Letzter Versuch am 2015-08-24 13:08:05 war erfolgreich.

Domaincontroller Diagnose

```
dcdiag -v
```

Domaincontrollerzertifikat

Ereignis-ID 82:

Fehler bei der Zertifikatregistrierung für Lokales System bei der Authentifizierung für alle URLs für den Registrierungsserver, der folgender Richtlinien-ID zugeordnet ist:
{DED11DE7-4422-4DD7-BED5-4761609EA841} (Der RPC-Server ist nicht verfügbar. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)).
Fehler bei der Registrierung für Vorlage: DomainController

Ereignis-ID 13:

Die Zertifikatregistrierung für Lokales System konnte sich nicht für ein Zertifikat DomainController mit der Anforderungs-ID N/A von FirstDC.srv.domainname.local\CA (Der RPC-Server ist nicht verfügbar. 0x800706ba (WIN32: 1722 RPC_S_SERVER_UNAVAILABLE)) registrieren.

Ereignis-ID 6:

Bei der automatischen Zertifikatregistrierung für lokales System ist ein Fehler aufgetreten
(0x800706ba) Der RPC-Server ist nicht verfügbar.

Lösung:

Prüfung der DCOM Sicherheisteinstellungen
Auf dem CA-Server folgenden Befehl ausführen: dcomcnfg.exe
Komponentendienst->Computer->Arbeitsplatz[Eigenschaften->COM-Sicherheit->Limits bearbeiten...(2x)]
Berechtigung für die Gruppen "Zertifikatdienst-DCOM-Zugriff" und "Jeder" kontrollieren.
(CERTSVC_DCOM_ACCESS war gesetzt jedoch fehlte die Domänengruppe "Zertifizierungsdienst-DCOM_Zugriff")

From:
<http://dokuwiki.atlas-brb.net/> - Wissensdatenbank

Permanent link:
http://dokuwiki.atlas-brb.net/doku.php?id=windows_server:dc:changedomaincontrollerroles&rev=1479996367

Last update: 2016/11/24 15:06

