Rollen im Active Directory

Welche gibt es?

1. FSMO / Betriebsmaster:

- Schemamaster
- Domänennamen-Master
- RID-Master
- PDC-Emulator
- Infrastrukturmaster

2. Globaler Katalog

Verteilung

Es gelten folgende Regeln

1. RID-Master und PDC-Emulator sollten zusammen auf einem DC sein.
2. Der Infrastrukturmaster darf kein GC sein.
3. Schemamaster- und Domänennamen-Master sollten auf einem DC sein.
4. Der Domänennamenmaster-FSMO soll auch ein globaler Katalogserver sein.

Beispiel mit einer Domäne:

DC1: Schemamaster, Domänennamenmaster und globaler Katalog
DC2: Infrastrukturmaster, RID-Master und PDC-Emulator

Abfrage der vorhandenen Rollen

NETDOM - Support Tools müssen installiert sein:

```
C:\Programme\Support Tools>netdom /query fsmo
Schema owner               ADAM.hetzel-netz.lan

Domain role owner          ADAM.hetzel-netz.lan

PDC role                   atom.hetzel-netz.lan

RID pool manager           atom.hetzel-netz.lan

Infrastructure owner       atom.hetzel-netz.lan

The command completed successfully.
```

DSQUERY

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

Alle Global Catalog abfragen

```
nslookup gc._msdcs.%userdnsdomain%
```

Alle Bridgeheads abfragen

```
repadmin /bridgeheads
```

Rollen auf andere DC's übertragen

Manchmal kommt man in den Genuss die FSMO's auf andere Systeme zu übertragen, wenn beispielsweise ein alter Server vom Netz genommen wird. Und so geht's...

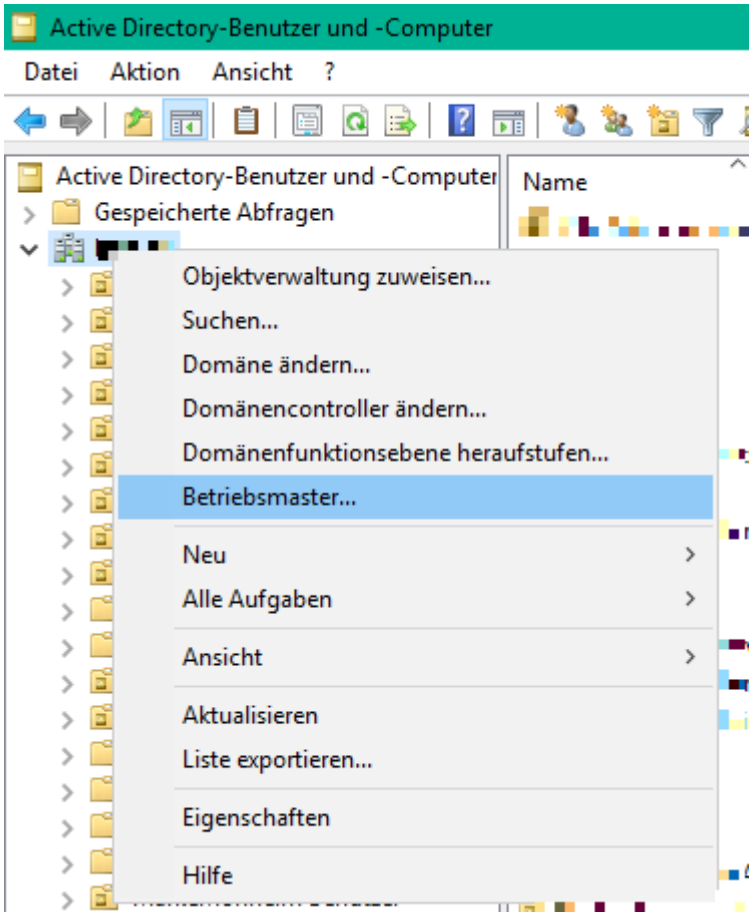
Vorbereitungen

Zunächst einen Überblick verschaffen!

1. Welche Server haben welche Rolle inne? - Abfrage mit oben erwähnten Befehlen!
2. Ist der Server, der abgeschaltet werden soll, ein Global Catalog?

RID-Master, PDC-Emulator und Infrastrukturmaster

Man öffne das Snapin „Active Directory Users and Computers“:



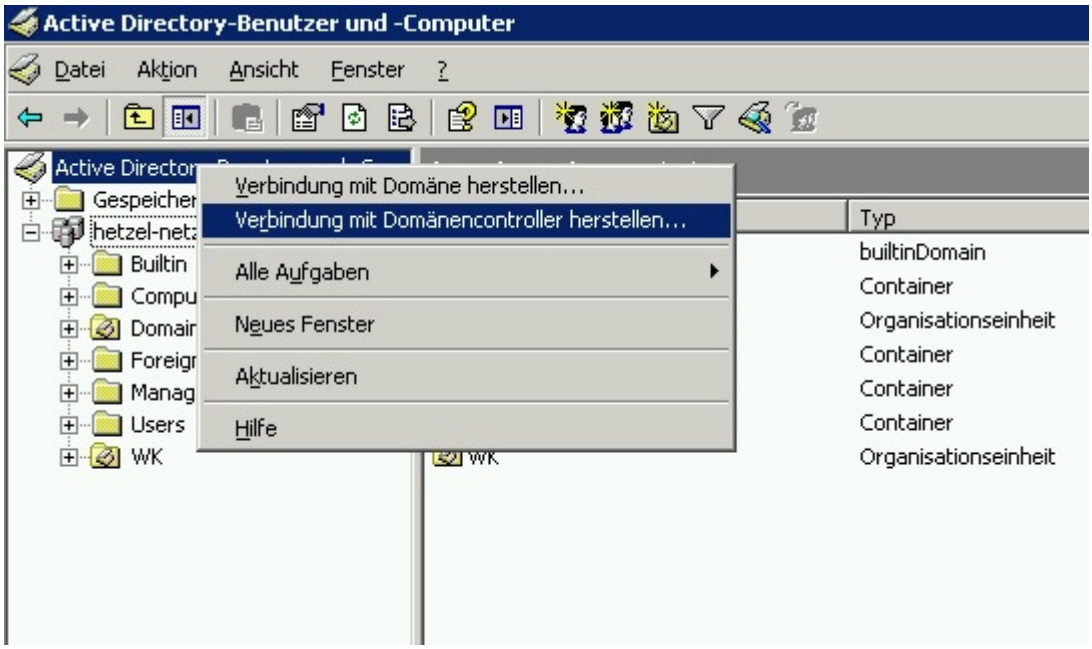
Ein Rechtsklick auf die Stammdomäne öffnet die Karteireiter der Betriebsmaster.



Wir befinden uns auf dem Server, der auch gleichzeitig der Rolleninhaber ist. Mit einem Klick auf „Ändern“ können wir den RID-Master nun auf einen anderen Server übertragen. Dies geht aber nicht!



Wir bedienen uns eines Tricks und verbinden uns mit dem zukünftigen Rolleninhaber:



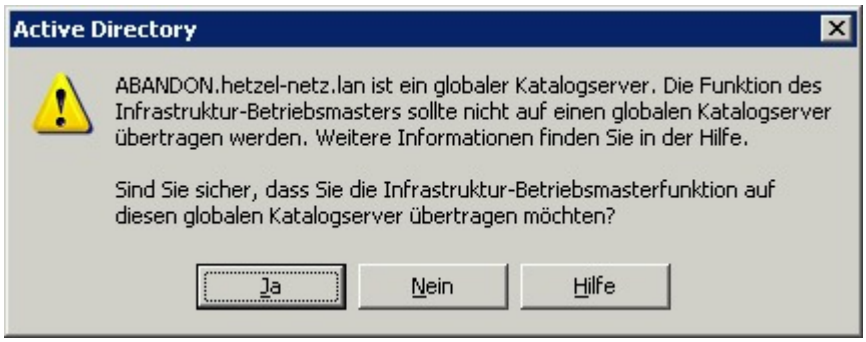
Nun können wir uns mit einem Klick auf „Ändern“ die Rolle ziehen:



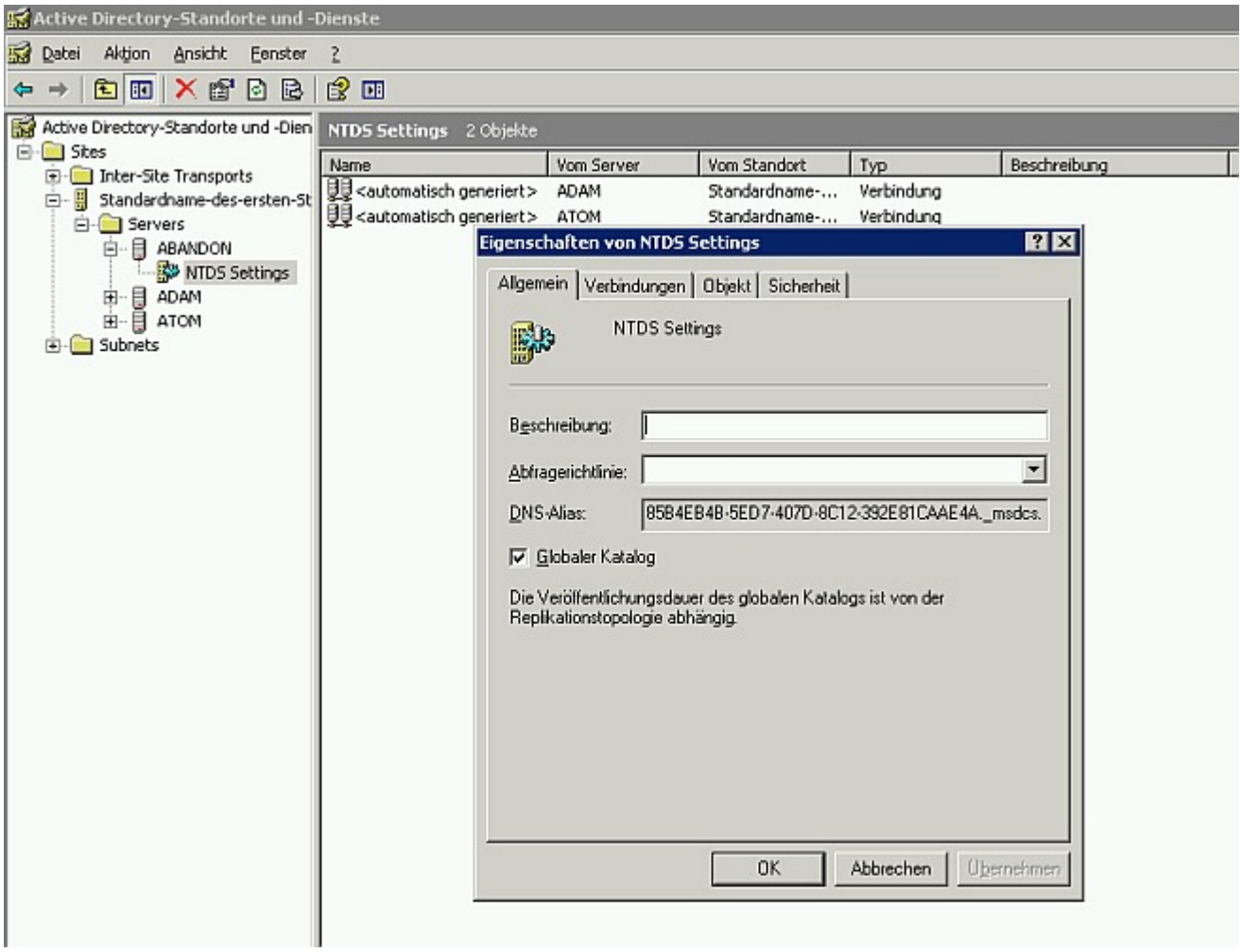
Selbiges führen wir für den PDC-Emulator und den Infrastrukturmaster durch!

Globalen Katalog umziehen

Bei oben aufgeführter Prozedur könnte es zu folgendem Hinweis gekommen sein:

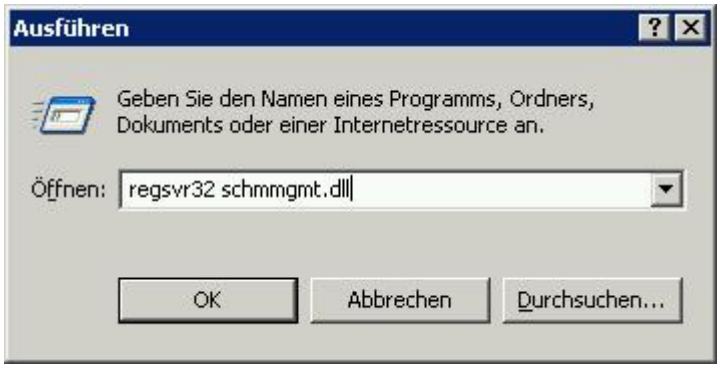


Wo kann ich das einstellen, welcher Server GC ist? Das Snapin lautet „Active Directory Sites and Services“:



Schema-Master übertragen

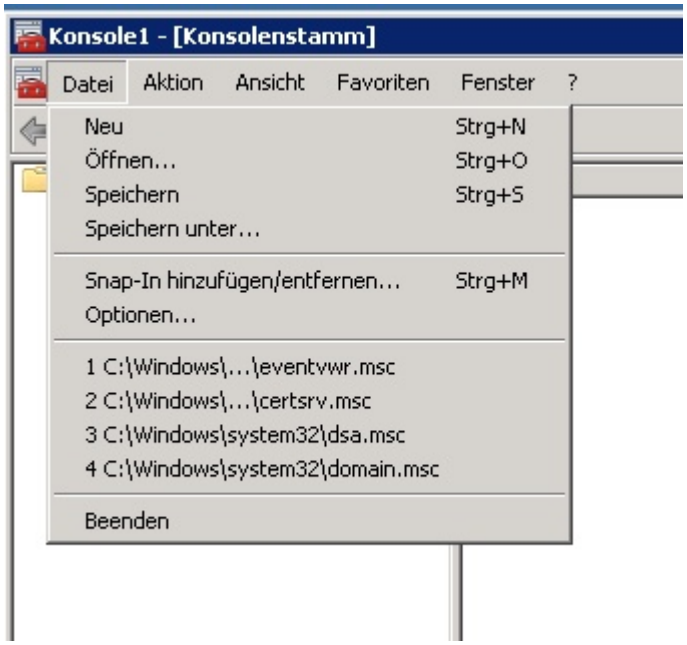
Zunächst muss das MMC-Snapin freigeschaltet werden. Dazu muss die DLL registriert werden.



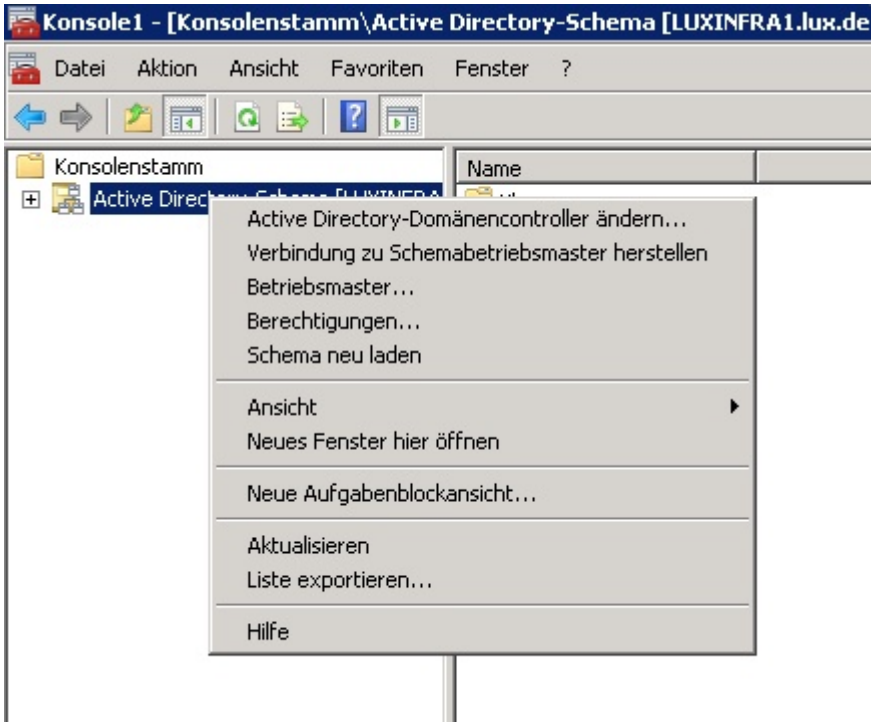
War der Vorgang erfolgreich, erscheint folgende Meldung.



Nun kann man über Start - Ausführen den MMC aufrufen und darin das Snapin für das AD-Schema laden.

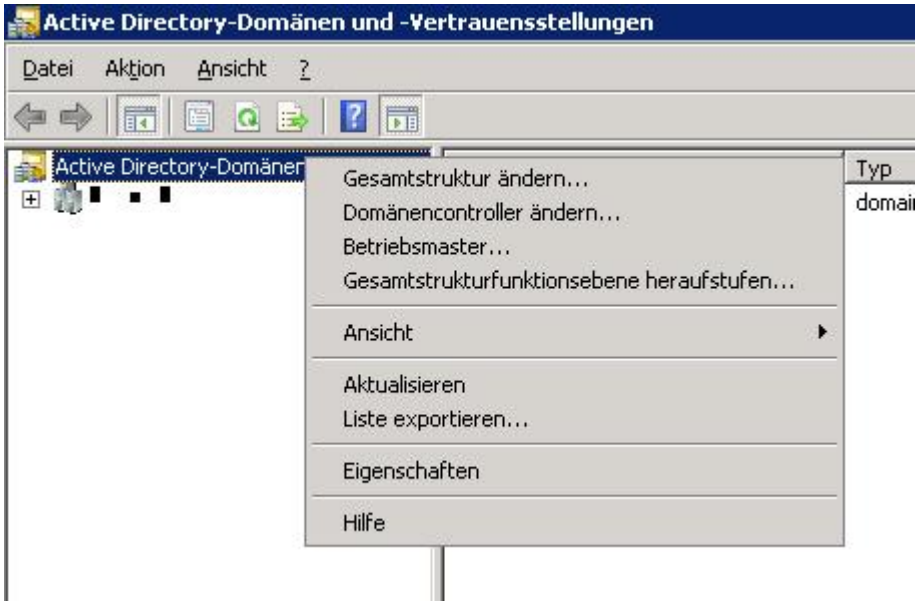


Mit Rechtsklick auf das Schema erscheint ein Kontextmenü, wo „Betriebsmaster“ ausgewählt werden kann.

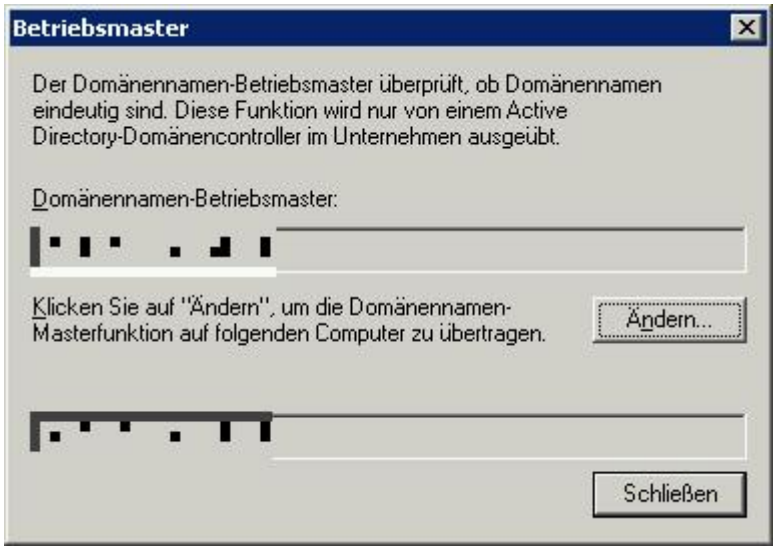


Dort kann man die Rolle übertragen.

Domänennamen-Master übertragen



Hier „Betriebsmaster“ anwählen und es erscheint folgendes Menü:



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

Permanent link:
https://wiki.sebastianhetzel.net/win_server:ad_rollen?rev=1713879035

Last update: **2024/04/23 13:30**