

# Übungsprotokoll

SYTS – Systemtechnik Systemintegration und Infrastruktur

 htlkrems Bautechnik & IT	<b>Übungsdatum:</b> KW 3/2024 – KW 10/2024	<b>Klasse:</b> 5AHIT	<b>Name:</b> Felix Schneider
	<b>Abgabedatum:</b> 05.03.2024	<b>Gruppe:</b> SYTS_2	<b>Note:</b>
<b>Leitung:</b> DI (FH) Alexander MESTL	<b>Mitübende:</b> Clemens Schlipfinger und Yanik Latzka		
<b>Übungsbezeichnung:</b>		Domain Controller stürzt ab	

## **Inhaltsverzeichnis:**

1	Aufgabenstellung.....	3
2	Abstract (English).....	3
3	Theoretische Grundlagen .....	4
3.1	FSMO-Rollen .....	4
3.1.1	Hintergrund .....	4
3.1.2	Arten von FSMO-Rollen .....	4
3.1.2.1	Forestweite FSMO-Rollen .....	4
3.1.2.2	Domänenweite FSMO-Rollen.....	4
3.1.2.3	Zuweisung der FSMO-Rollen.....	4
3.2	Netdom query.....	4
3.2.1	Überblick über Netdom .....	4
3.2.2	Netdom Query .....	5
3.3	ntdsutil .....	5
3.3.1	Überblick über ntdsutil .....	5
3.3.2	Verschieben von FSMO-Rollen mit ntdsutil.....	5
4	Übungsdurchführung .....	6
4.1	Vorbereitung des ersten Domain Controllers.....	6
4.2	Aufsetzung eines zweiten Domain Controllers .....	7
4.3	Adressen und Namen einstellen .....	8
4.4	Features und Rollen installieren und konfigurieren .....	9
4.5	FSMO Rollen verschieben (Domain Ebene) .....	10
4.6	FSMO Rollen verschieben (Domain Name Master) .....	13
4.7	FSMO Rollen verschieben (Schema Master).....	14
4.8	Standort umbenennen.....	18
4.9	Replikation funktionsfähig .....	19
4.10	Ausfall.....	20
4.11	FSMO-Rollen zurückholen.....	22
4.12	Benutzer anlegen .....	24
4.13	DHCP und DNS reparieren .....	25
5	Ergebnisse.....	28
6	Kommentar.....	28

## 1 Aufgabenstellung

Wir werden in unserer Domäne den Ausfall eines DCs simulieren und versuchen, darauf zu reagieren.

Tasks:

- Sofern kein zweiter DC aktiv ist, einen neuen DC mit AD DS, DNS und DHCP (Failover) in Betrieb nehmen
- Standort umbenennen auf bspw. "Zentrale" und in "Standorte und Dienste" die DCs des Standortes überprüfen
- FSMO-Rollen zwischen den DCs verteilen
- Einen der DCs "crashen" lassen - d. h. im Wesentlichen die entsprechende VM löschen
- Domäne wieder vollständig lauffähig machen - was ist zu tun?

Dokumentation der funktionierenden Replikation vor dem Ausfall, der Auswirkungen des Ausfalls und aller Schritte zur Wiederherstellung!

## 2 Abstract (English)

We will simulate the failure of a DC in our domain and try to react to it. Tasks:

- If no second DC is active, start up a new DC with AD DS, DNS and DHCP (failover)
- Rename the location to "Headquarters", for example, and check the DCs of the location in "Locations and services"
- Distribute FSMO roles between the DCs
- Have one of the DCs "crashed" - i.e. essentially delete the corresponding VM
- Make the domain fully operational again - what needs to be done?

Document the functioning replication before the failure, the effects of the failure and all steps for recovery!

## 3 Theoretische Grundlagen

### 3.1 FSMO-Rollen

Flexible Single Master Operation (FSMO) Rollen sind in Microsoft Active Directory-Umgebungen entscheidend für die Verwaltung und Koordination von Operationen. Diese Rollen sind auf Domaincontrollern verteilt und spielen eine wichtige Rolle bei der Aufrechterhaltung der Integrität und Konsistenz der Active Directory-Datenbank. Hier sind die theoretischen Grundlagen zu FSMO-Rollen:

#### 3.1.1 Hintergrund

FSMO-Rollen wurden eingeführt, um sicherzustellen, dass nur eine Instanz innerhalb einer Active Directory-Domäne bestimmte Änderungen durchführt, um Datenkonsistenz und -integrität zu gewährleisten.

#### 3.1.2 Arten von FSMO-Rollen

Es gibt zwei Hauptkategorien von FSMO-Rollen: Forestweite FSMO-Rollen und domänenweite FSMO-Rollen.

##### 3.1.2.1 Forestweite FSMO-Rollen

- Schema Master: Verwaltet Änderungen am Schema der gesamten Forest.
- Domain Naming Master: Koordiniert die Vergabe von Namen für neue Domänen und Anwendungspartitionen im Forest.

##### 3.1.2.2 Domänenweite FSMO-Rollen

- PDC Emulator: Behandelt Konflikte bei der Kontensynchronisierung und dient als primärer Zeitgeber in der Domäne.
- RID Master: Steuert die Vergabe von RIDs (Relative Identifiers), um sicherzustellen, dass Objekte eindeutige Sicherheitskennungen erhalten.
- Infrastructure Master: Aktualisiert und pflegt Verweise auf Objekte in anderen Domänen.

##### 3.1.2.3 Zuweisung der FSMO-Rollen

Bei der Installation des ersten Domain Controllers in einer Active Directory-Domäne werden alle FSMO-Rollen diesem Server zugewiesen.

## 3.2 Netdom query

Netdom ist ein Befehlszeilentool von Microsoft, das Administratoren bei der Verwaltung von Active Directory-Domänen und Computern unterstützt. Das query-Untercommand von Netdom ermöglicht es, Informationen über Domänen und deren Objekte abzurufen. Hier sind einige theoretische Grundlagen zu Netdom und insbesondere zum query-Befehl:

### 3.2.1 Überblick über Netdom

Netdom ist Teil der Windows Server-Betriebssysteme und wird verwendet, um verschiedene Active Directory-Operationen durchzuführen, einschließlich Domänenbeitritt, Namensänderungen, Trust-Verwaltung und mehr.

Netdom ermöglicht die Automatisierung von Aufgaben und ist besonders nützlich in Skripten und Skriptumgebungen.

### 3.2.2 Netdom Query

Das query-Untercommand von Netdom wird verwendet, um Informationen über Domänen und Computer abzurufen.

Beispiele für query-Optionen:

- netdom query /domain: Zeigt Informationen über die aktuelle Domäne an.
- netdom query fsmo: Gibt die FSMO-Rollen und ihre aktuellen Inhaber für die Domäne aus.
- netdom query dc: Listet alle Domain Controller in der Domäne auf.
- netdom query trust: Zeigt Informationen über Trust-Beziehungen zu anderen Domänen an.

## 3.3 ntdsutil

Ntdsutil ist ein Befehlszeilentool von Microsoft, das in Windows Server-Betriebssystemen enthalten ist und speziell für die Verwaltung von Active Directory-Datenbanken und -Operationen entwickelt wurde. Es ermöglicht fortgeschrittene Funktionen, darunter das Verschieben von FSMO-Rollen. Hier sind einige theoretische Grundlagen zu ntdsutil, insbesondere im Kontext der Verschiebung von FSMO-Rollen.

### 3.3.1 Überblick über ntdsutil

Ntdsutil ist ein leistungsstarkes Dienstprogramm, das Administratoren erweiterte Funktionen für die Verwaltung von Active Directory-Instanzen bietet.

Es wird oft verwendet, um spezifische Active Directory-Aufgaben auszuführen, die nicht direkt über grafische Benutzeroberflächen erledigt werden können.

### 3.3.2 Verschieben von FSMO-Rollen mit ntdsutil

Ntdsutil kann verwendet werden, um FSMO-Rollen zwischen Domain Controllern zu verschieben. Die Rollen, die mit ntdsutil verschoben werden können, sind der PDC Emulator, RID Master, Schema Master, Domain Naming Master und der Infrastructure Master.

- roles
- connections
- connect to server <Servername>
- quit
- seize <FSMO Rolle>

ntdsutil-Kommando	übertragene FSMO-Rolle
seize infrastructure master	Infrastruktur-Master
seize naming master	Domänennamen-Master
seize PDC	PDC-Emulator
seize RID master	RID-Master
seize schema master	Schemamaster

## 4 Übungsdurchführung

### 4.1 Vorbereitung des ersten Domain Controllers

Ein langwieriger, jedoch eher einfacherer Prozess ist das Aufsetzen eines Domain Controllers. Bevor wir jedoch damit anfangen können, richten wir den ersten Domain Controller noch optimal her und bereiten diesen für den zweiten DC vor.

Um uns das Leben später einfacher zu machen, deaktivieren wir alle Gruppenrichtlinienobjekte aus vorherigen Übungen, damit das Testen der Funktionalität auf Clients später nicht unnötig erschwert wird.

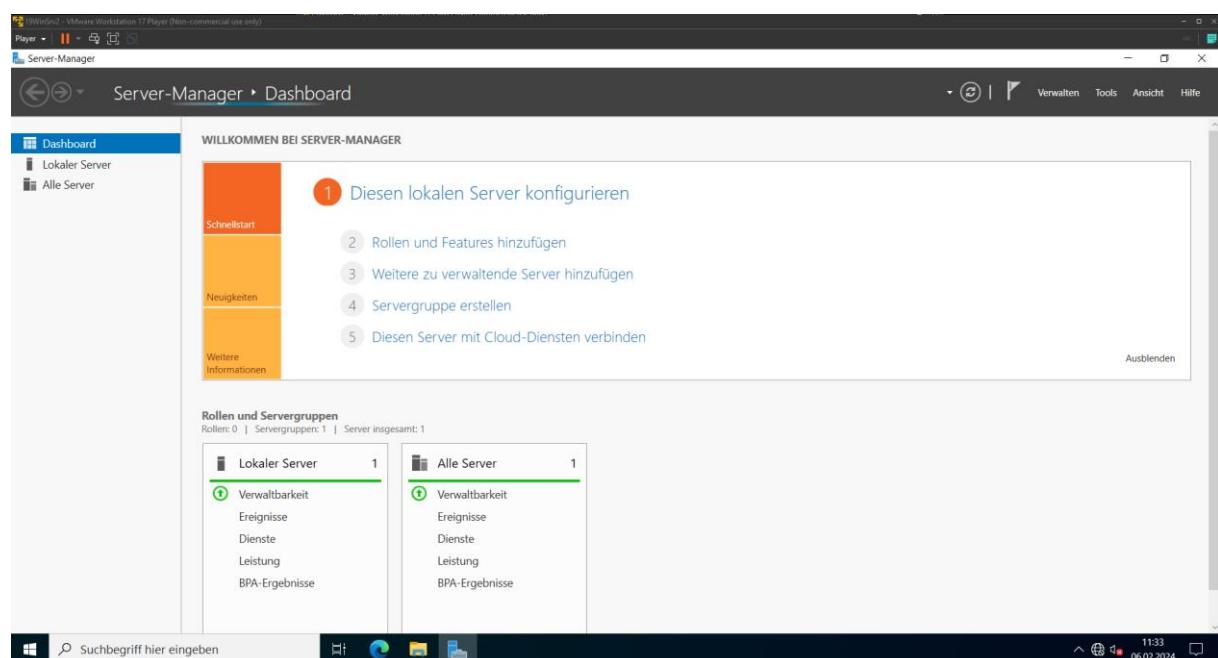
Außerdem deaktivieren wir die Firewall von Windows, um nochmals sicherzustellen, dass der `ping` Befehl nicht versehentlich blockiert wird. Diesen Schritt muss man auch unbedingt beim zweiten Domain Controller umsetzen, damit man sich nicht eine Stunde fragt, warum man nur in eine Richtung pingen kann...

## 4.2 Aufsetzung eines zweiten Domain Controllers

Wenn alle Maßnahmen und Vorbereitungen auf dem ersten Domain Controller getroffen sind, erstellen wir eine zweite neue Virtuelle Maschine mit dem Namen `19WinSrv2`. Dies wird unser zweiter Domain Controller, weshalb wir beim Aufsetzen auch wieder das Windows Server Image 2022 auswählen.

Nachdem wir dem Server genügend RAM und Speicherplatz zugeschrieben haben, können wir ihn starten und mit der Installation beginnen. Dieses Standardprozedere wird hier nicht nochmals näher erläutert.

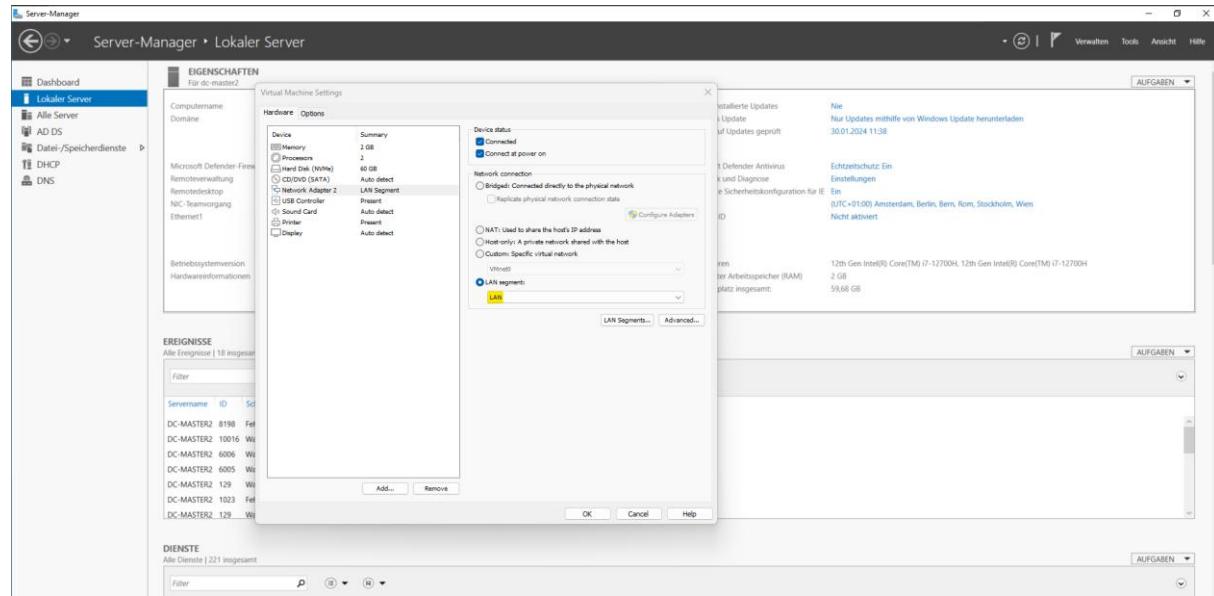
Anschließend sollten wir einen einfachen Server Manager sehen, welcher uns in seinem grellsten Light-Mode, lächelnd und begrüßend anstrahlt und unsere die Dunkelheit gewohnten Augen ruinert. Danke, Windows!



## 4.3 Adressen und Namen einstellen

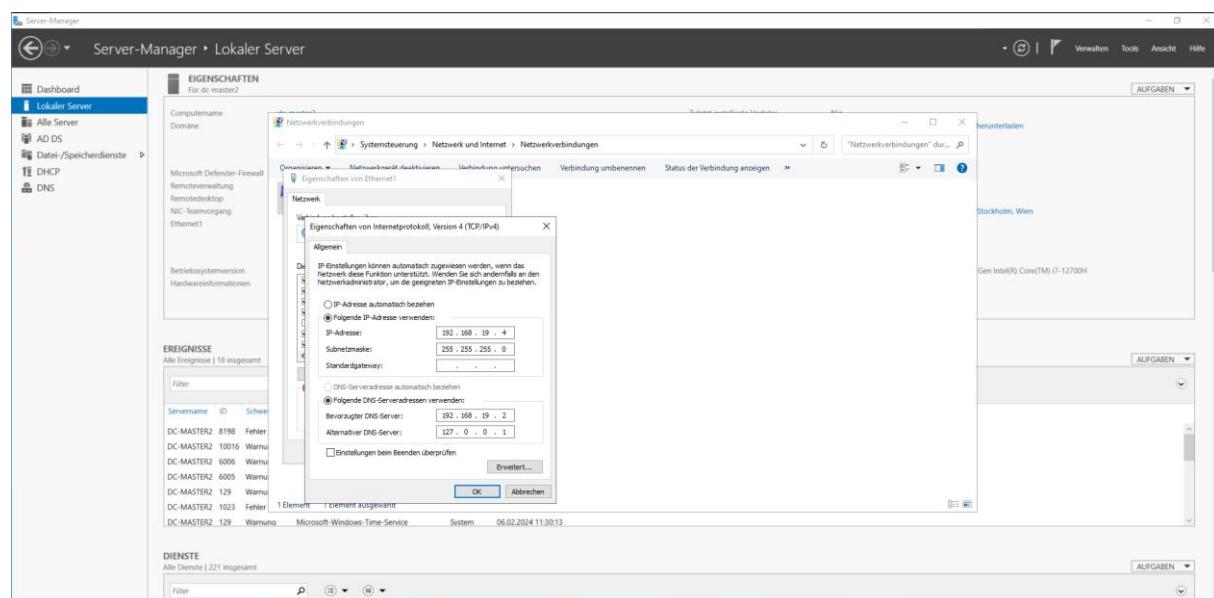
Als erstes stellen wir den PC-Namen um, indem wir unter 'Lokaler Server' auf den Link bei Computername klicken und hinter dem Button 'Ändern' den Namen umstellen. Nach ausführlicher Speicherung starten wir den Server neu, um sicherzustellen, dass der Name aktualisiert wird.

Bei Verwendung von Virtual Box darf man gleich wieder herunterfahren, um eine weiter **Netzwerkkarte** einzulegen, welche im gleichen LAN sein soll, wie der erste Domain Controller. Wenn VMWare verwendet wird, machen wir dies nun bei laufendem Betrieb.



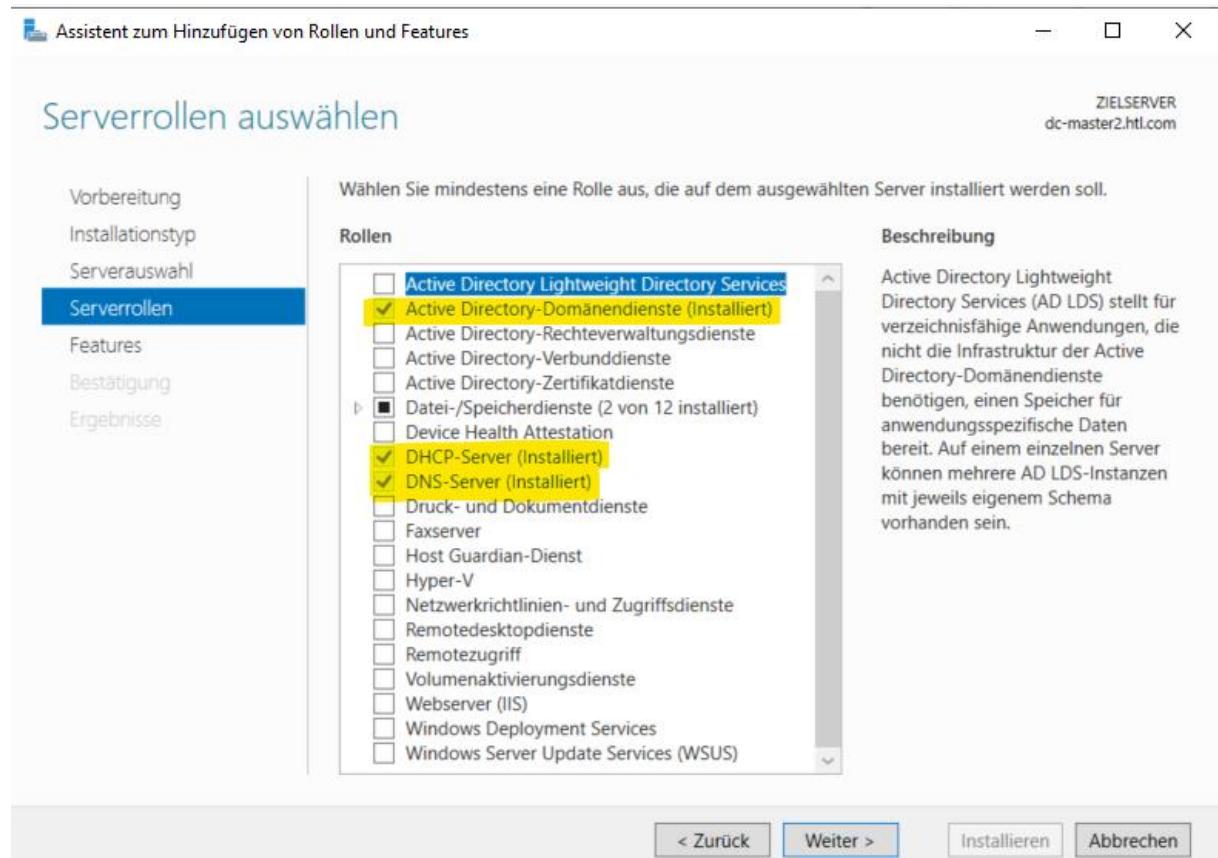
*Bitte beachten Sie, dass einige Screenshots erst später aufgenommen wurden, weswegen hier beispielsweise schon alle Tabs der jeweiligen Features sichtbar sind.*

Mittels neuer Netzwerkkarte können wir nun auch die IP-Adresse richtig einstellen. Hierbei kann man gleich auf die Einstellungen für das ausgekreuzte DNS-Verhalten einstellen, welches später sehr hilfreich sein wird.



## 4.4 Features und Rollen installieren und konfigurieren

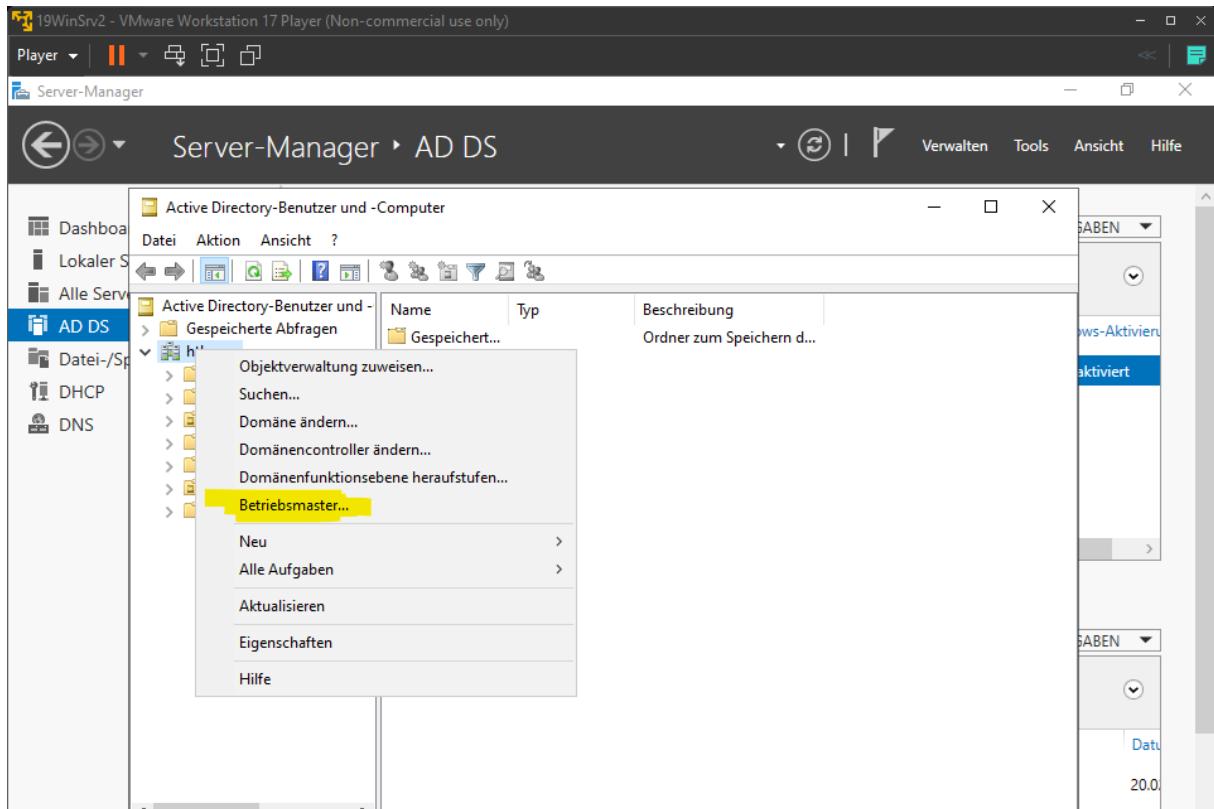
Fügen Sie nun die Features `AD-Domänendienste`, `DHCP-Server` und `DNS-Server` hinzu und installieren Sie diese. Anschließend müssen Sie neustarten.

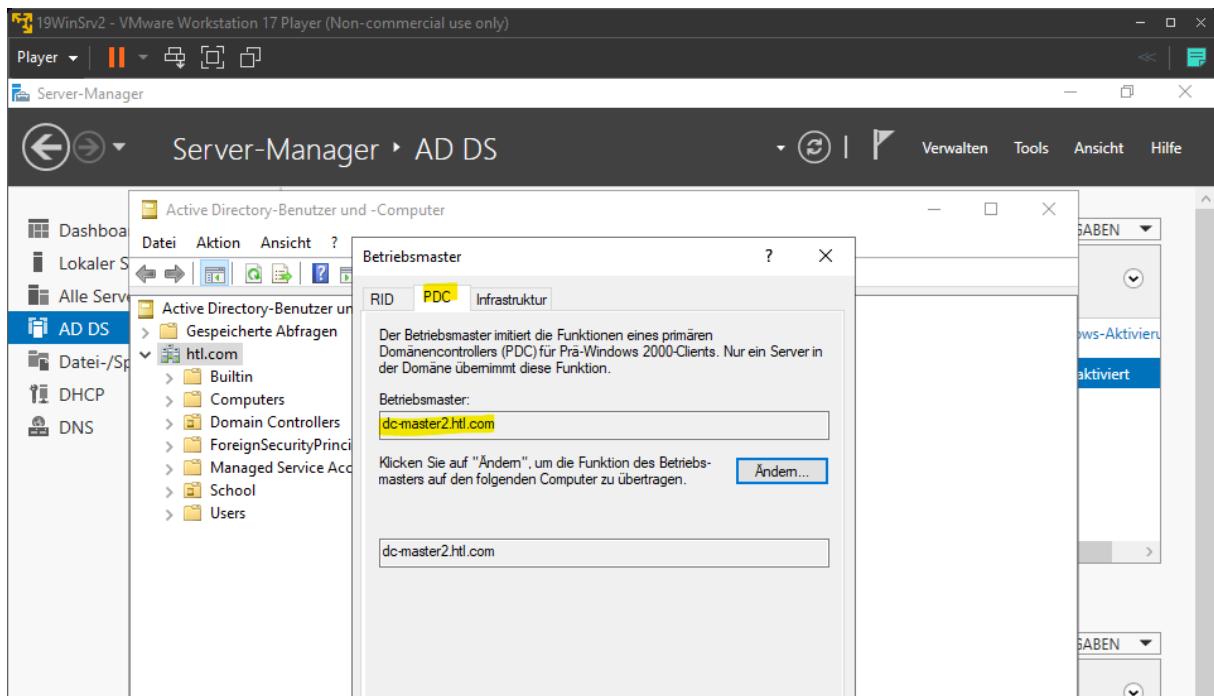
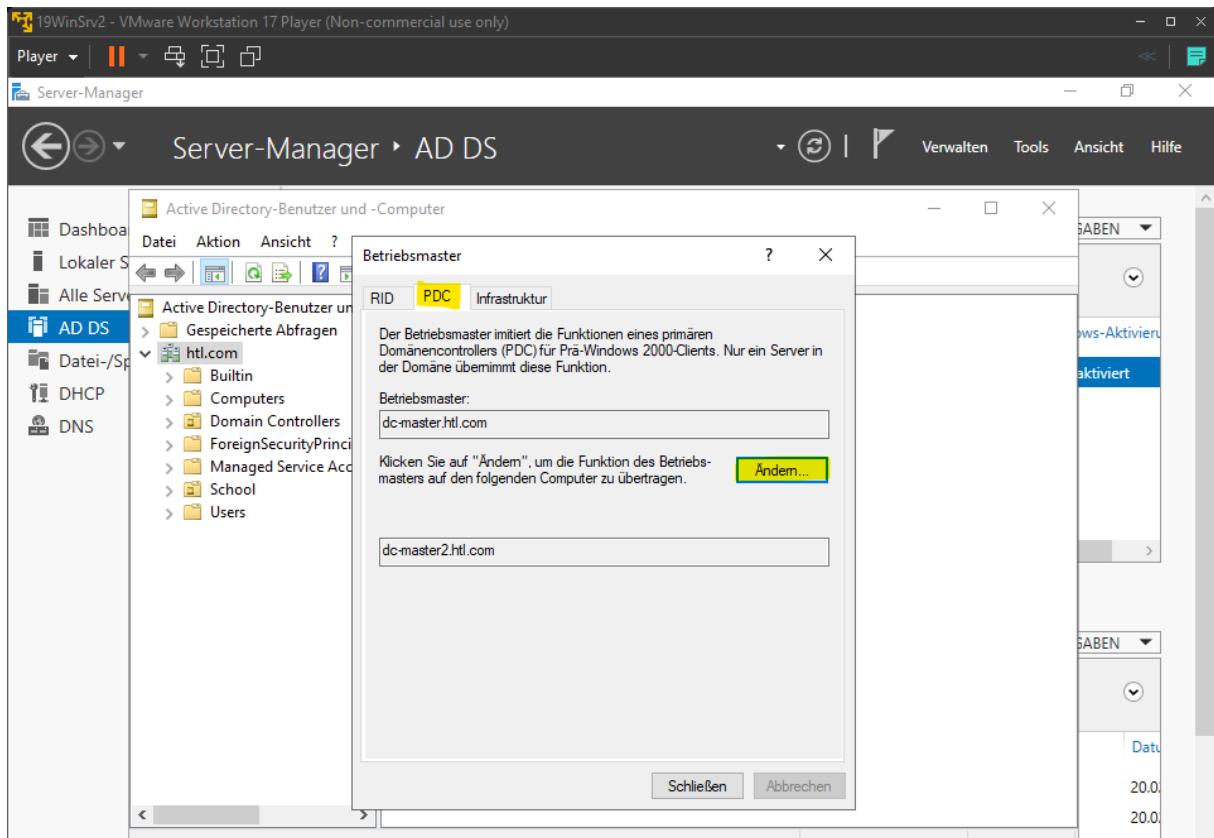


Empfehlenswert ist es, zuerst den AD-Domänendienst zu konfigurieren, denn dadurch müssen Sie den DHCP bzw DNS Server nicht neu autorisieren, da diese beim Konfigurieren automatisch autorisiert werden.

## 4.5 FSMO Rollen verschieben (Domain Ebene)

Die FMSO Rollen können ganz einfach in der GUI mit AD verschoben werden. Dafür ist keine Zeile Powershell notwendig. Clemens hat sich jedoch für die kreative und unmögliche Methode der Powershell mittels Get-Help entschieden. Legenden besagen, dass er schon seit 1000 Jahren keine FSMO-Rolle mehr verschoben hat.





```
Ping-Statistik für 192.168.19.2:  
  Pakete: Gesendet = 2, Empfangen = 2, Verloren = 0  
    (% Verlust),  
Ca. Zeitangaben in Millisek.:  
  Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms  
STRG-C  
PS C:\Users\Administrator.HTML> netdom query fsmo  
Schemamaster          dc-master.html.com  
Domänennamen-Master   dc-master.html.com  
PDC                dc-master.html.com  
RID-Pool-Manager      dc-master.html.com  
Infrastrukturmaster   dc-master.html.com  
Der Befehl wurde ausgeführt.  
  
PS C:\Users\Administrator.HTML> netdom query fsmo  
Schemamaster          dc-master.html.com  
Domänennamen-Master   dc-master.html.com  
PDC                dc-master2.html.com  
RID-Pool-Manager      dc-master.html.com  
Infrastrukturmaster   dc-master.html.com
```

## 4.6 FSMO Rollen verschieben (Domain Name Master)

Um den Domain Name Master zu verschieben, muss man in andere Einstellungen reinschauen.  
Halten Sie sich an die Screenshots!

The screenshot shows a Windows Server 2012 R2 environment with a PowerShell window open. The command entered is:

```
server connections: connect to server dc-master2
Bindung mit "dc-master2" ...
Eine Verbindung mit "dc-master2" wurde unter Verwendung der Benutzerinformationen des lokal angemeldeten Benutzers
wurde hergestellt.
server connections: q
fsmo maintenance: q
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: ?

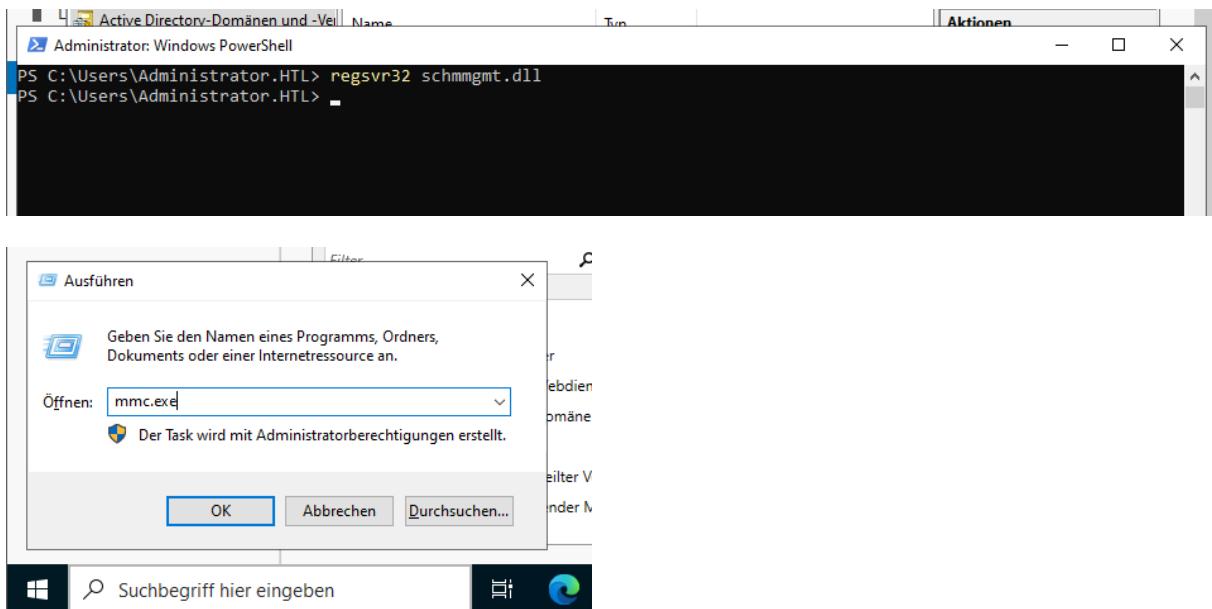
?                               - Zeigt diese Hilfeinformation
Connections                  - Verbindung mit einer bestimmt...
Help                         - Zeigt diese Hilfeinformatio...
Quit                          - Zum vorherigen Menü wechseln
Seize infrastructure master  - Funktion der Infrastruktur...
Seize naming master          - Überschreibt die Namensmast...
Seize PDC                      - Funktion des primären Domä...
Seize RID master              - Funktion der RID auf dem ve...
Seize schema master           - Funktion des Schemas auf de...
Select operation target       - Standorte, Server, Domänen, ...
Transfer infrastructure master - Den verbundenen Server zum Infrastrukturmast...
Transfer naming master        - Legt den verbundenen Server als ...
Transfer PDC                   - Den verbundenen Server zum primären Domänencontroller machen
Transfer RID master            - Den verbundenen Server zum RID-Master machen
Transfer schema master         - Den verbundenen Server zum Schemamaster machen

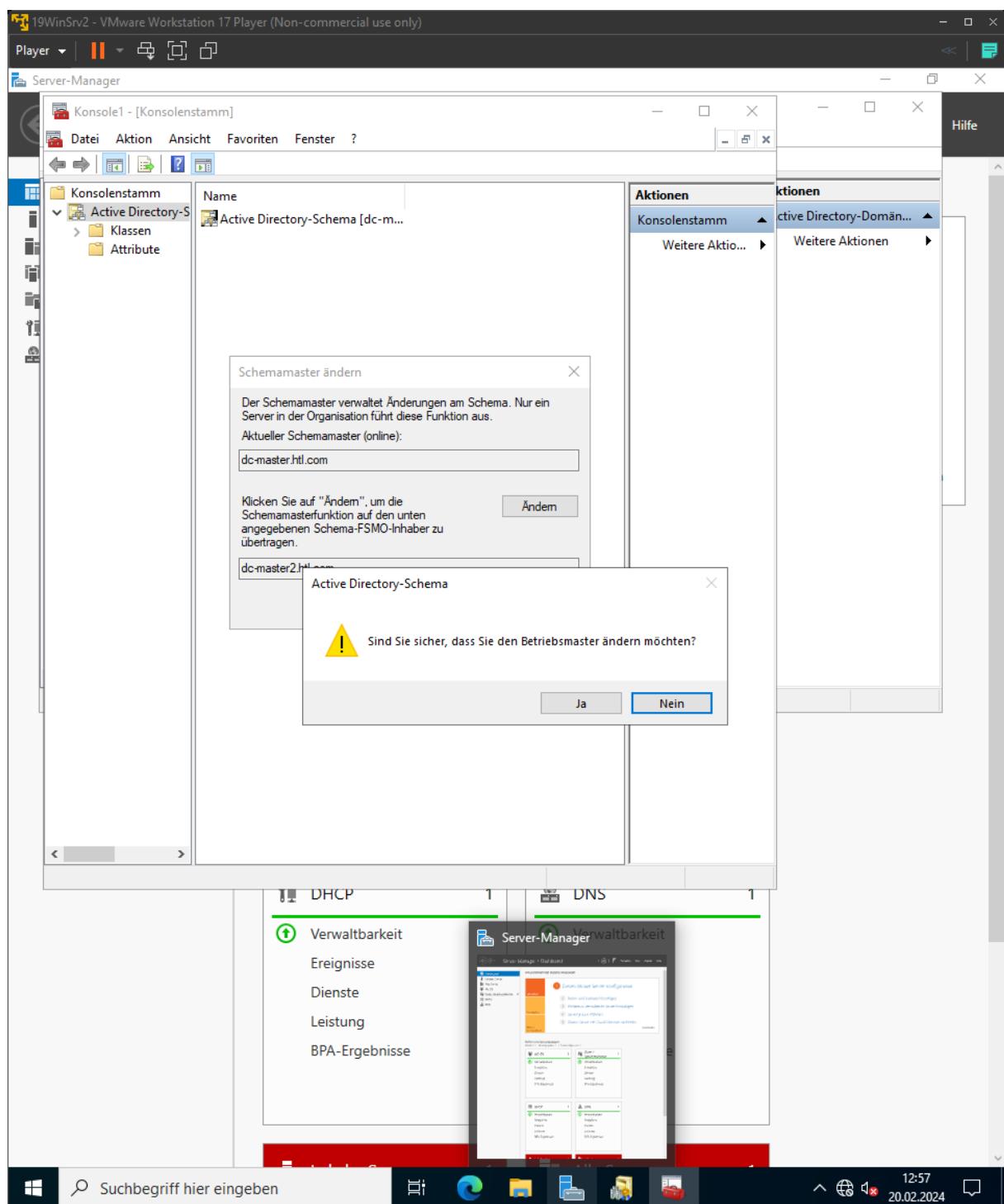
fsmo maintenance: transfer naming master
```

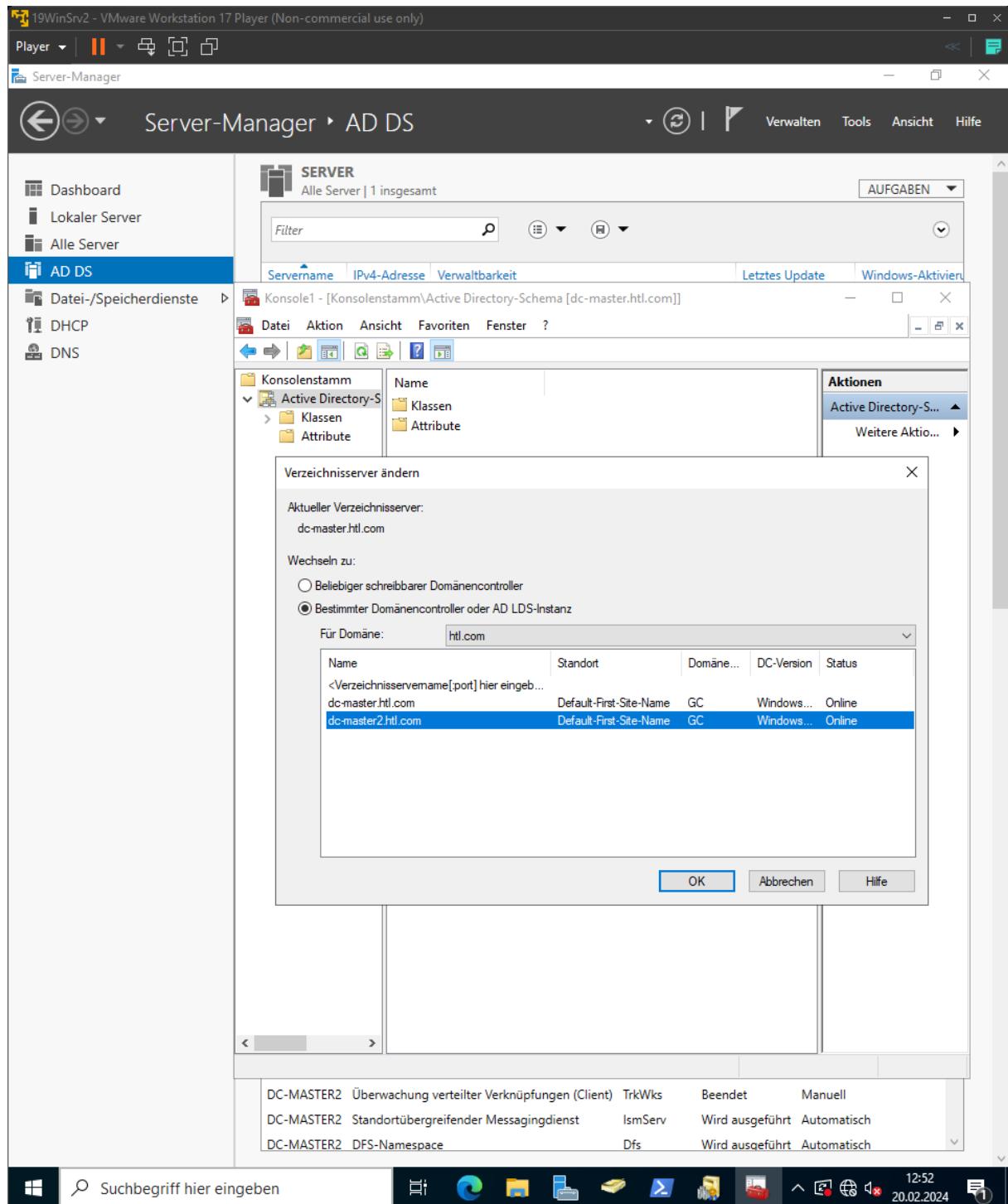
A confirmation dialog box titled "Bestätigung der Funktionenübertragung" (Confirmation of function transfer) is displayed, asking "Sind Sie sicher, dass Sie die Namensmasterfunktion auf den Server "dc-master2" übertragen möchten?" (Are you sure you want to transfer the Naming Master function to the server "dc-master2"?). The "Ja" (Yes) button is highlighted.

## 4.7 FSMO Rollen verschieben (Schema Master)

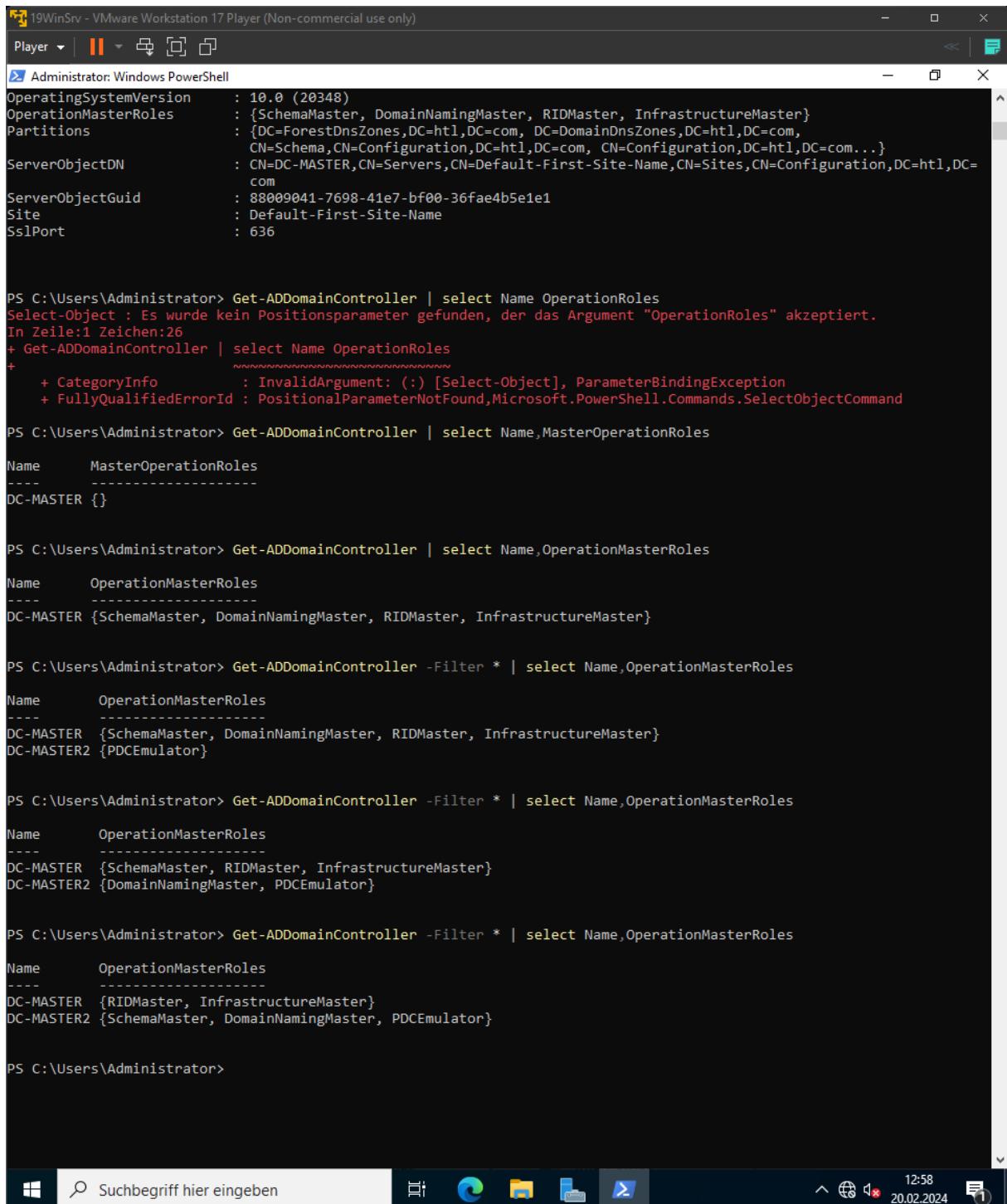
Beim Schema Master ist ein ganz besonderer Prozess von Nöten. Denn er benötigt das Tool Schmmgmt.dll. Anschließend öffnet man das MMC Tool und kann dort zuerst das Snap-In hinzufügen und anschließend die Rolle verschieben.







Schlussendlich sieht man, dass die Rollen verschoben wurden:



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell" running on a VM named "9WinSrv - VMware Workstation 17 Player (Non-commercial use only)". The window displays several commands related to domain controllers:

```
OperatingSystemVersion : 10.0 (20348)
OperationMasterRoles   : {SchemaMaster, DomainNamingMaster, RIDMaster, InfrastructureMaster}
Partitions             : {DC=ForestDnsZones,DC=htl,DC=com, DC=DomainDnsZones,DC=htl,DC=com,
                        CN=Schema,CN=Configuration,DC=htl,DC=com, CN=Configuration,DC=htl,DC=com...}
ServerObjectDN         : CN=DC-MASTER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=htl,DC=
                        com
ServerObjectGuid       : 88009041-7698-41e7-bf00-36fae4b5e1e1
Site                  : Default-First-Site-Name
SslPort                : 636

PS C:\Users\Administrator> Get-ADDomainController | select Name OperationRoles
Select-Object : Es wurde kein Positionsparameter gefunden, der das Argument "OperationRoles" akzeptiert.
In Zeile:1 Zeichen:26
+ Get-ADDomainController | select Name OperationRoles
+ ~~~~~
+ CategoryInfo          : InvalidArgument: () [Select-Object], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SelectObjectCommand

PS C:\Users\Administrator> Get-ADDomainController | select Name,MasterOperationRoles

Name      MasterOperationRoles
----      -----
DC-MASTER {}

PS C:\Users\Administrator> Get-ADDomainController | select Name,OperationMasterRoles

Name      OperationMasterRoles
----      -----
DC-MASTER {SchemaMaster, DomainNamingMaster, RIDMaster, InfrastructureMaster}

PS C:\Users\Administrator> Get-ADDomainController -Filter * | select Name,OperationMasterRoles

Name      OperationMasterRoles
----      -----
DC-MASTER {SchemaMaster, RIDMaster, InfrastructureMaster}
DC-MASTER2 {PDCEmulator}

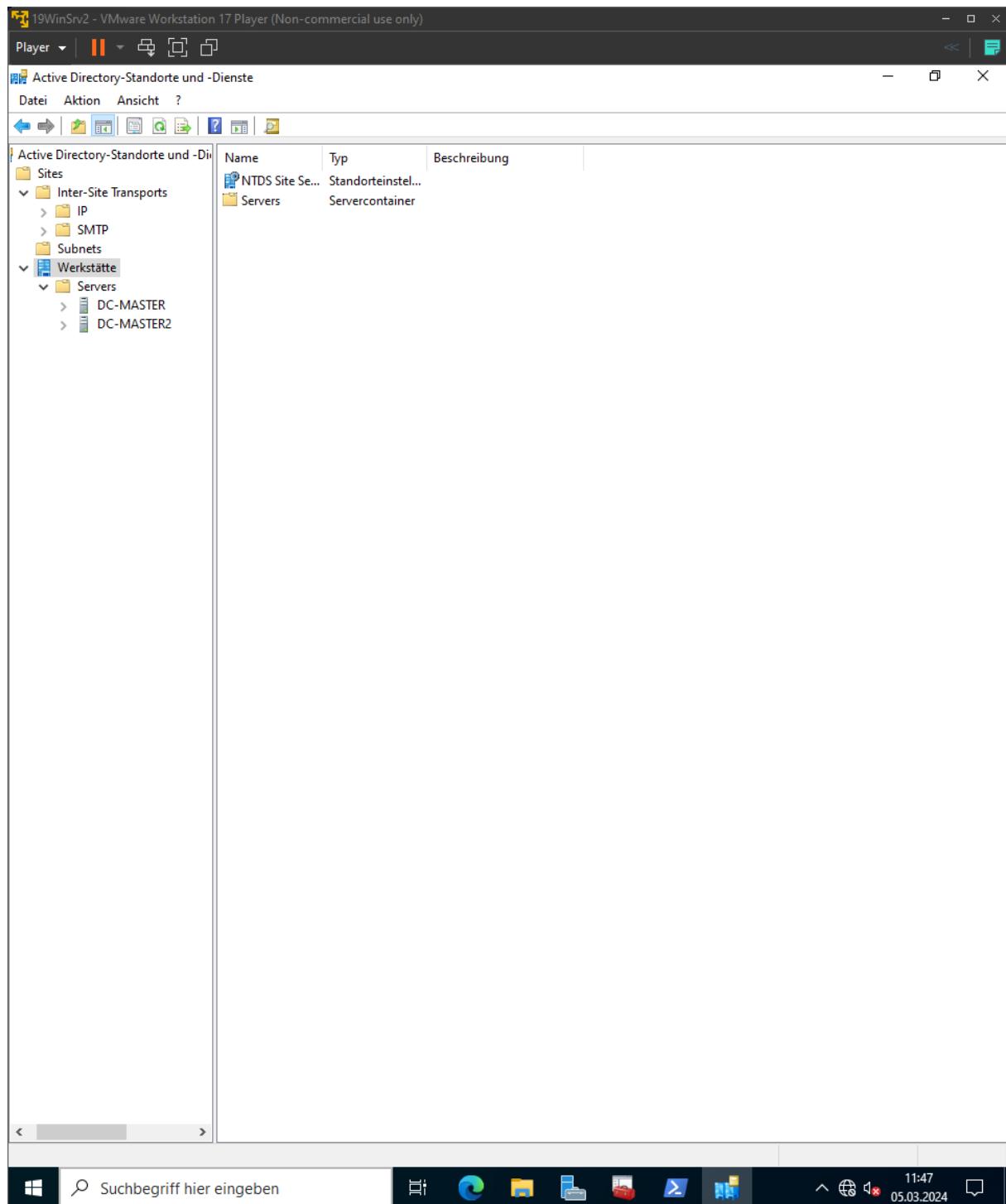
PS C:\Users\Administrator> Get-ADDomainController -Filter * | select Name,OperationMasterRoles

Name      OperationMasterRoles
----      -----
DC-MASTER {RIDMaster, InfrastructureMaster}
DC-MASTER2 {SchemaMaster, DomainNamingMaster, PDCEmulator}

PS C:\Users\Administrator>
```

## 4.8 Standort umbenennen

Mittels „Active-Directory-Standorte und -Dienste“ kann man den Standort in Werkstätte umbenennen:



## 4.9 Replikation funktionsfähig

Wie man hier sieht, werden die Replikation von den verschiedenen Domain Controllern in einer bestimmten Reihenfolge beantwortet (kleinere Zeit, schnellere Antwort):

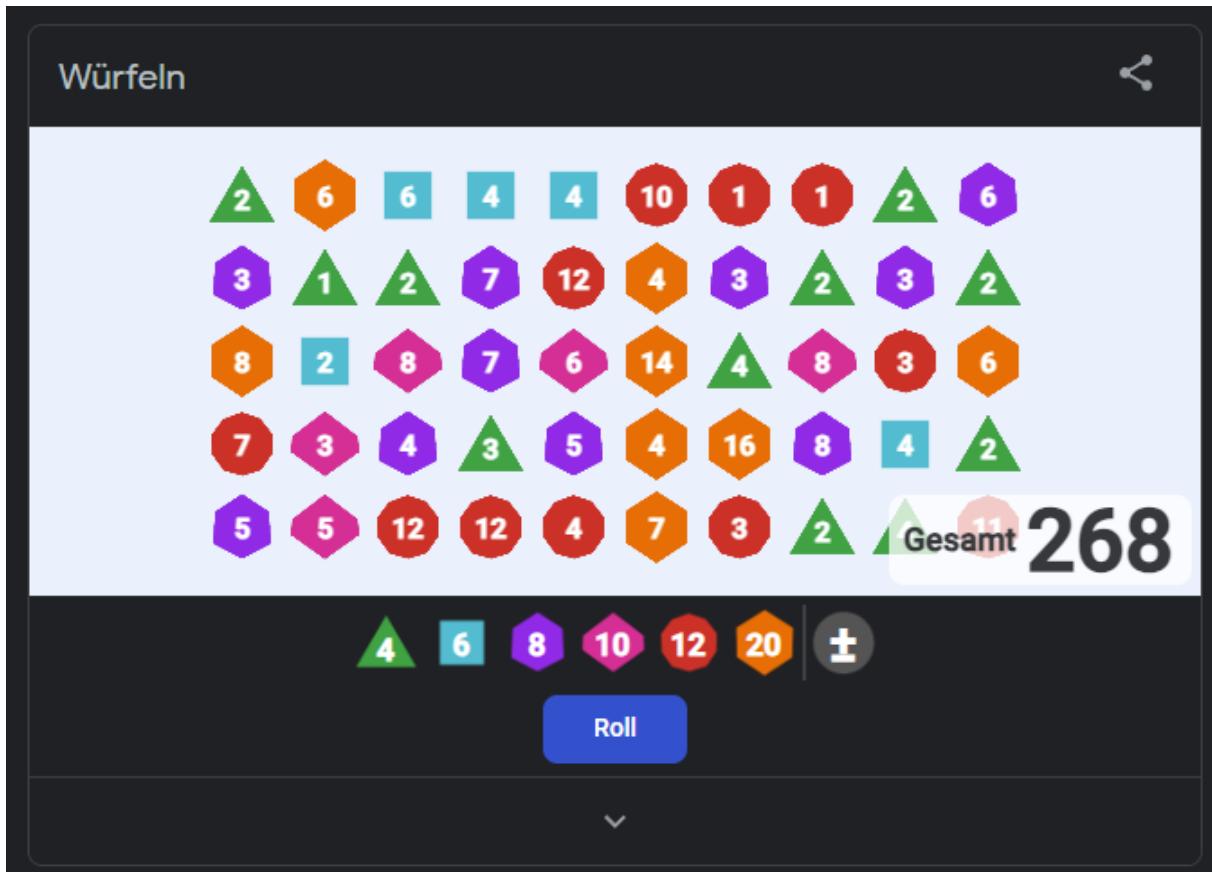
```
PS C:\Users\Administrator> Repadmin /replsummary
Startzeit der Replikationszusammenfassung: 2024-03-05 11:54:59
Datensammlung für Replikationszusammenfassung wird gestartet.
Dieser Vorgang kann einige Zeit dauern.

Quell-DSA      Größtes Delta    Fehler/gesamt %% Fehler
DC-MASTER          01m:10s      0 /   5   0
DC-MASTER2         09m:25s      0 /   5   0

Ziel-DSA      Größtes Delta    Fehler/gesamt %% Fehler
DC-MASTER          09m:25s      0 /   5   0
DC-MASTER2         01m:11s      0 /   5   0
```

## 4.10 Ausfall

Jetzt wird's ernst. Wir öffnen den Google Random Number Generator und lassen eine zufälligen DC ausfallen. Wenn die Nummer gerade ist, wird es DC 2, ungerade Nummer bedeutet DC 1:



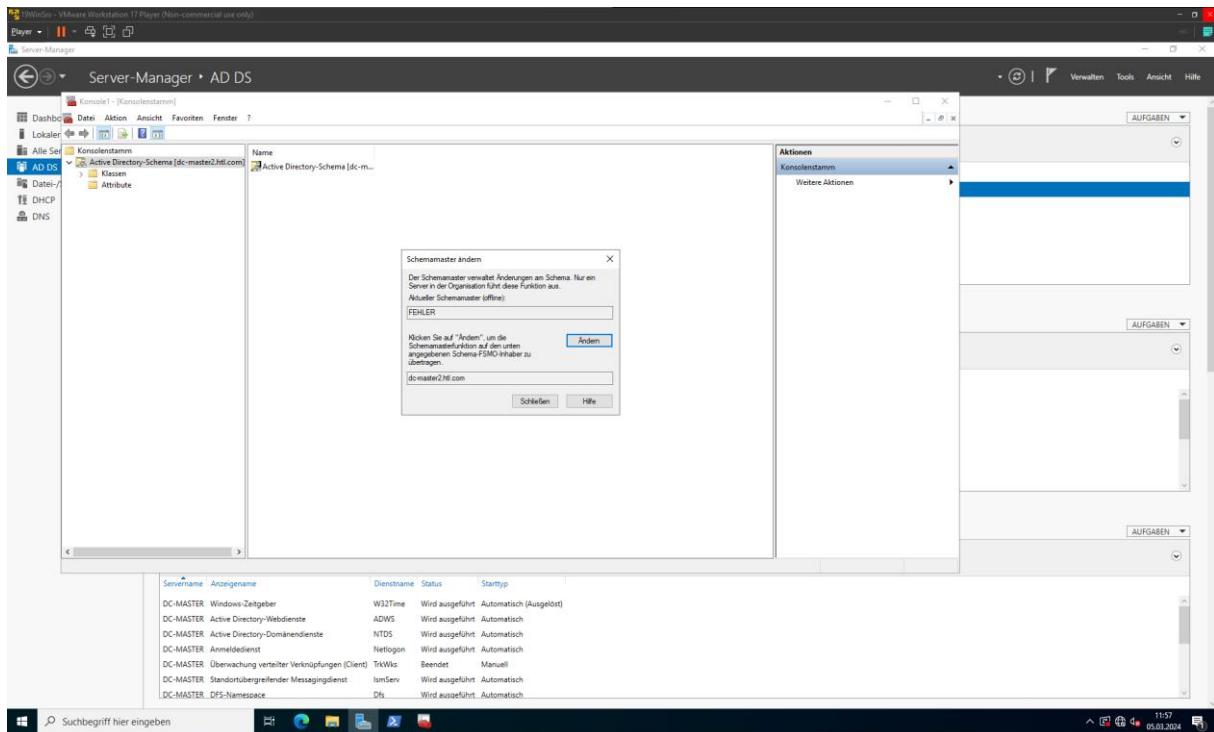
Okay, dann wird wohl DC 2 ausfallen. Sprich, wir löschen die VM. Ich habe jedoch vorher noch alle FSMO Rollen auf DC 2 verschoben. Juhu!

Kurzfristig werden alle Funktionalitäten noch funktionieren, weil Temporär die Berechtigungen aus Ausfallgründen auf von anderen DCs gemacht werden können. Auch wenn diese Aktionen länger dauern, als erwartet. Beispielsweise konnte ich einen neuen Nutzer erstellen, obwohl dieser DC keine FSMO Rollen mehr hat.

Name	Typ	Beschreibung
Anton Xaver Edlinger	Benutzer	
Clemens Schneider	Benutzer	
Felix Schneider	Benutzer	
Yanik Latzka	Benutzer	

Nach einiger Zeit, ist es jedoch unmöglich gewisse Aktionen durchzuführen (dazu zählen zB Objekte erstellen, DCs erstellen, Timesynchronisierung, ...).

Beispielsweise sieht man im FSMO Manager, dass der andere Server nicht mehr erreichbar ist:



## 4.11 FSMO-Rollen zurückholen

Mittels diesen Artikels kann man die FSMO-Rollen zurückforcieren:

<https://www.windowspro.de/andreas-kroschel/fsmo-rollen-im-ad-schema-uebernehmen>

```
roles
connections
connect to server <Servername>
q
seize <FSMO-Rolle>
```

<Servername> ist dabei derjenige Server, welcher die Rolle erhält. Die für die FSMO-Rollen verwendeten Schlüsselwörter sind

ntdsutil-Kommando	übertragene FSMO-Rolle
seize infrastructure master	Infrastruktur-Master
seize naming master	Domänennamen-Master
seize PDC	PDC-Emulator
seize RID master	RID-Master
seize schema master	Schemamaster

Hier sieht man, wie die RID und Schema Rollen übertragen werden:

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered was "seize RID master". A confirmation dialog box titled "Bestätigung der Funktionenübernahme" appears, asking if the user is sure about taking over the RID Master function for the server "dc-master". The dialog lists the current settings: "CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com". The "Ja" (Yes) button is highlighted.

```
Administrator: Windows PowerShell
)
Abhängig vom Fehlercode kann dies auf
einen Verbindungs-, LDAP- oder Funktionsübertragungsfehler hinweisen.
Fehler bei Übertragung von schema FSMO. Die Übernahme der Funktionen wird fortgesetzt...
Server "dc-master" kennt 5 Funktionen.
Schema - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Namensmaster - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
PDC - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
RID - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Infrastruktur - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
fsmo maintenance: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Users\Administrator> netdom query fsmo
Sch
Dom Bestätigung der Funktionenübernahme
PDC
RID
Inf
Der
Sind Sie sicher, dass der Server "dc-master" die Funktion RID
Master mit dem Wert unten übernehmen soll?
Ja Nein
CN=NTDS
Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
fsmo maintenance: seize RID master
```

```
PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe:
C:\Windows\system32\ntdsutil.exe:
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server dc-master
Bindung mit "dc-master" ...
Eine Verbindung mit "dc-master" wurde unter Verwendung der Benutzerinformationen des lokal angemeldeten Benutzers hergestellt.
server connections: q
fsmo maintenance: seize schema master
Eine sichere Übertragung von schema FSMO vor der Übernahme der Funktionen wird versucht.
ldap_modify_sw-Fehler 0x34(52 (Nicht verfügbar).
LDAP-Fehlermeldung: 000020AF: SvcErr: DSID-03210512, problem 5002 (UNAVAILABLE), data 1722
Win32-Fehler: 0x20af(Der angeforderte FSMO-Vorgang konnte nicht ausgeführt werden. Der aktuelle FSMO-Inhaber war nicht erreichbar.)
)
Abhängig vom Fehlercode kann dies auf
einen Verbindungs-, LDAP- oder Funktionsübertragungsfehler hinweisen.
Fehler bei Übertragung von schema FSMO. Die Übernahme der Funktionen wird fortgesetzt...
Server "dc-master" kennt 5 Funktionen.
Schema - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Namensmaster - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
PDC - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
RID - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Infrastruktur - CN=NTDS Settings,CN=DC-MASTER2,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
fsmo maintenance: q
C:\Windows\system32\ntdsutil.exe: q
```

Wie man sieht, wurden die FSMO-Rollen übertragen (alle übertragen):

```
PS C:\Users\Administrator>
RID - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Infrastruktur - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
fsmo maintenance: seize naming master
Eine sichere Übertragung von domain naming FSMO vor der Übernahme der Funktionen wird versucht.
ldap_modify_sw-Fehler 0x34(52 (Nicht verfügbar).
LDAP-Fehlermeldung: 000020AF: SvcErr: DSID-03210512, problem 5002 (UNAVAILABLE), data 1722
Win32-Fehler: 0x20af(Der angeforderte FSMO-Vorgang konnte nicht ausgeführt werden. Der aktuelle FSMO-Inhaber war nicht erreichbar.)
)
Abhängig vom Fehlercode kann dies auf
einen Verbindungs-, LDAP- oder Funktionsübertragungsfehler hinweisen.
Fehler bei Übertragung von domain naming FSMO. Die Übernahme der Funktionen wird fortgesetzt...
Server "dc-master" kennt 5 Funktionen.
Schema - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Namensmaster - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
PDC - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
RID - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
Infrastruktur - CN=NTDS Settings,CN=DC-MASTER,CN=Servers,CN=Werkstätte,CN=Sites,CN=Configuration,DC=htl,DC=com
fsmo maintenance: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Users\Administrator> netdom query fsmo
Schemamaster          dc-master.htl.com
Domänennamen-Master    dc-master.htl.com
PDC                  dc-master.htl.com
RID-Pool-Manager      dc-master.htl.com
Infrastrukturmast...    dc-master.htl.com
Der Befehl wurde ausgeführt.

PS C:\Users\Administrator>
```

## 4.12 Benutzer anlegen

Anschließend kann man einfach einen Benutzer wieder anlegen, da der RID Master wieder online ist (für diese Aktion zum Beispiel).

The screenshot shows the Windows Server Active Directory management console. On the left, a tree view shows 'Domain Controllers' under 'htl.com'. On the right, a table lists existing users:

Name	Typ	Beschreibung
Anton Xaver Edlinger	Benutzer	
Clemens Schneider	Benutzer	
Felix Schneider	Benutzer	
Yanik Latzka	Benutzer	

A modal dialog box titled 'Neues Objekt - Benutzer' is open in the center. It contains the following information:

Erstellen in: htl.com/School/Students

Wenn Sie auf "Fertig stellen" klicken, wird das folgende Objekt erstellt:

Vollständiger Name: Benjamin Riedl  
Anmeldename des Benutzers: b.riedl@htl.com  
Der Benutzer kann Kennwort nicht ändern.  
Das Kennwort läuft nie ab.

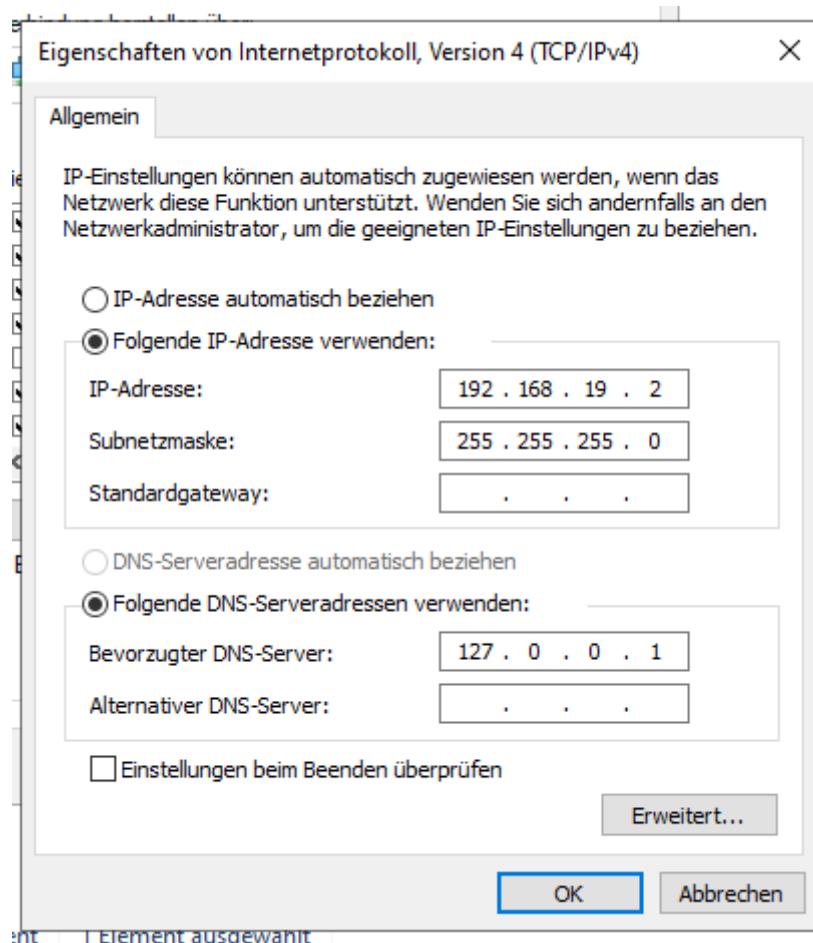
Buttons at the bottom: Zurück, Fertig stellen (highlighted), Abbrechen.

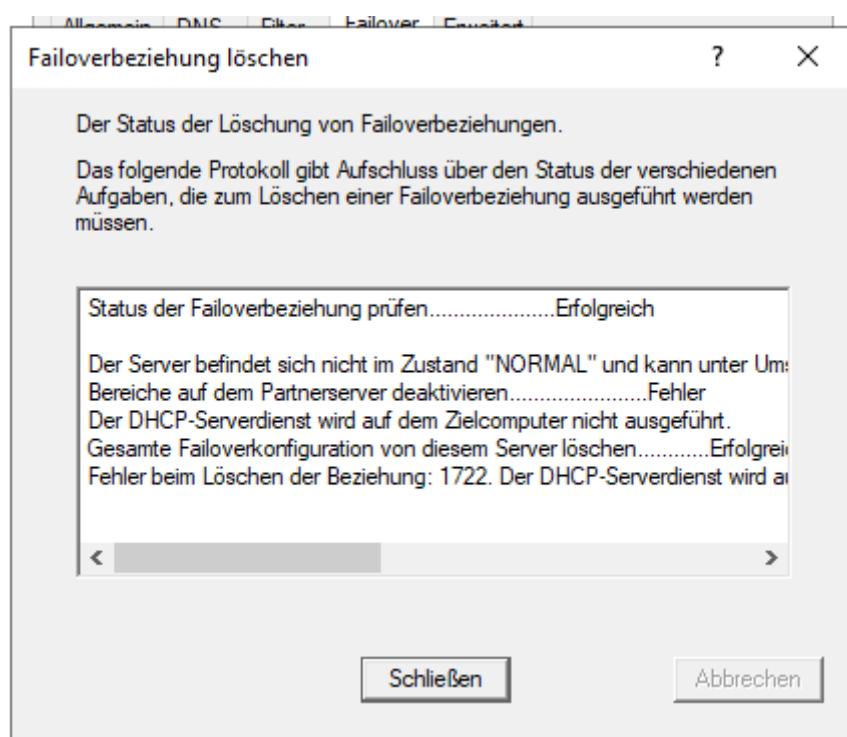
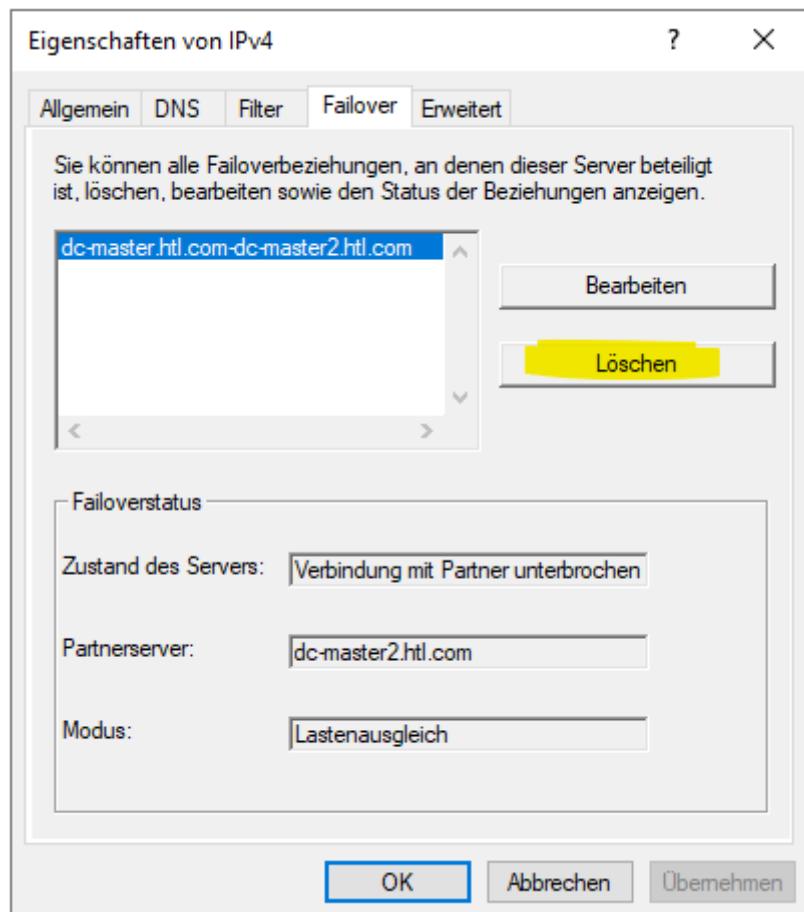
The screenshot shows the same Active Directory interface after creating a new user. The 'New Object - User' dialog was used to create a user named 'Benjamin Riedl'. This user now appears in the list of users:

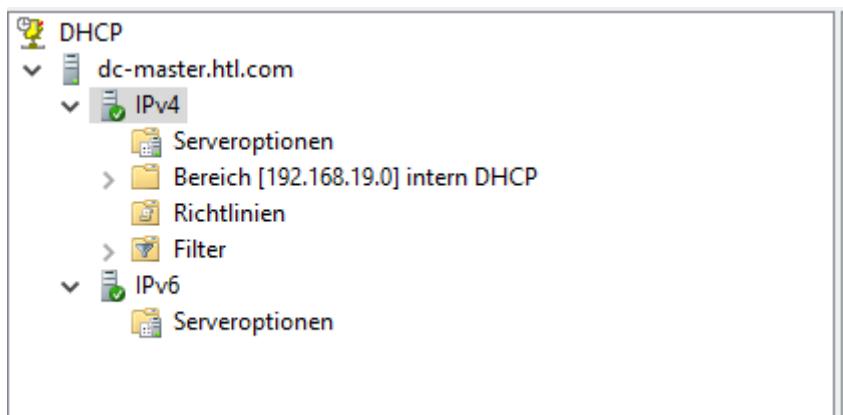
Name	Typ	Beschreibung
Anton Xaver Edlinger	Benutzer	
Benjamin Riedl	Benutzer	
Clemens Schneider	Benutzer	
Felix Schneider	Benutzer	
Yanik Latzka	Benutzer	

## 4.13 DHCP und DNS reparieren

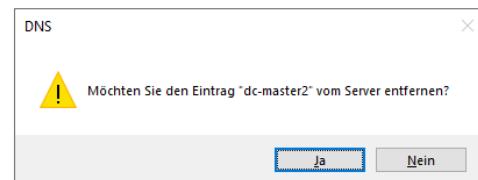
Damit DHCP und DNS wieder funktioniert muss man manuell wieder den zweiten DNS-Server austragen (bei den Ethernet-Einstellungen und DNS-Einstellungen) und das Failover deaktivieren.



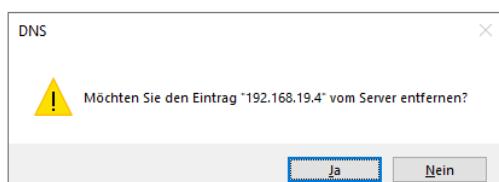




dc-master	Host (A)	192.168.19.2	Static
dc-master2	Host (A)	192.168.19.4	Static
firewall	Host (A)	192.168.19.1	Static



192.168.19.4	Zeiger (PTR)	dc-master2.htl.com.	30.01.2024 12:00:00
--------------	--------------	---------------------	---------------------



## 5 Ergebnisse

Alle FSMO-Rollen sind wieder auf DC1, also genau wie vor dieser Übung...

DNS und DHCP + AD funktionieren wieder.

The screenshot shows the Windows Server Management Console. On the left, there's a navigation pane with icons for DNS, DHCP, and Active Directory. Under 'DHCP', 'dc-master.htl.com' is selected, showing sub-options for Forward-Lookupzonen, Reverse-Lookupzonen, Vertrauenspunkte, and Bedingte Weiterleitungen. The main pane displays two views: 'DNS' and 'Active Directory Users'. The 'Active Directory Users' view is currently active, showing a list of five users:

Name	Typ	Beschreibung
Anton Xaver Edlinger	Benutzer	
Benjamin Riedl	Benutzer	
Clemens Schneider	Benutzer	
Felix Schneider	Benutzer	
Yanik Latzka	Benutzer	

## 6 Kommentar

Super Übung für die Matura 😊