|  |  |  |  |
| --- | --- | --- | --- |
| **Übungsprotokoll**  **SYTS – Systemtechnik Systemintegration und Infrastruktur** | | | |
|  | **Übungsdatum:**  KW 3/2024 –  KW 10/2024 | **Klasse:**  5AHIT | **Name:**  Felix Schneider |
| **Abgabedatum:**  05.03.2024 | **Gruppe:**  SYTS\_2 | **Note:** |
| **Leitung:**  DI (FH) Alexander MESTL | **Mitübende:**  Clemens Schlipfinger und Yanik Latzka | | |
| **Übungsbezeichnung**:  Domain Controller stürzt ab | | | |

**Inhaltsverzeichnis:**

[1 Aufgabenstellung 3](#_Toc160790818)

[2 Abstract (English) 3](#_Toc160790819)

[3 Theoretische Grundlagen 4](#_Toc160790820)

[3.1 FSMO-Rollen 4](#_Toc160790821)

[3.1.1 Hintergrund 4](#_Toc160790822)

[3.1.2 Arten von FSMO-Rollen 4](#_Toc160790823)

[3.1.2.1 Forestweite FSMO-Rollen 4](#_Toc160790824)

[3.1.2.2 Domänenweite FSMO-Rollen 4](#_Toc160790825)

[3.1.2.3 Zuweisung der FSMO-Rollen 4](#_Toc160790826)

[3.2 Netdom query 4](#_Toc160790827)

[3.2.1 Überblick über Netdom 4](#_Toc160790828)

[3.2.2 Netdom Query 5](#_Toc160790829)

[3.3 ntdsutil 5](#_Toc160790830)

[3.3.1 Überblick über ntdsutil 5](#_Toc160790831)

[3.3.2 Verschieben von FSMO-Rollen mit ntdsutil 5](#_Toc160790832)

[4 Übungsdurchführung 6](#_Toc160790833)

[4.1 Vorbereitung des ersten Domain Controllers 6](#_Toc160790834)

[4.2 Aufsetzung eines zweiten Domain Controllers 7](#_Toc160790835)

[4.3 Adressen und Namen einstellen 8](#_Toc160790836)

[4.4 Features und Rollen installieren und konfigurieren 9](#_Toc160790837)

[4.5 FSMO Rollen verschieben (Domain Ebene) 10](#_Toc160790838)

[4.6 FSMO Rollen verschieben (Domain Name Master) 13](#_Toc160790839)

[4.7 FSMO Rollen verschieben (Schema Master) 14](#_Toc160790840)

[4.8 Standort umbenennen 18](#_Toc160790841)

[4.9 Replikation funktionsfähig 19](#_Toc160790842)

[4.10 Ausfall 20](#_Toc160790843)

[4.11 FSMO-Rollen zurückholen 22](#_Toc160790844)

[4.12 Benutzer anlegen 24](#_Toc160790845)

[4.13 DHCP und DNS reparieren 25](#_Toc160790846)

[5 Ergebnisse 28](#_Toc160790847)

[6 Kommentar 28](#_Toc160790848)

# 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!

# 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!

# Theoretische Grundlagen

## 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:

### 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.

### Arten von FSMO-Rollen

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

#### 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.

#### 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.

#### Zuweisung der FSMO-Rollen

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

## 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:

### 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.

### 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.

## 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.

### 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.

### 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>

A screenshot of a computer program

Description automatically generated

# Übungsdurchführung

## 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…

## 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 Standardprozeder 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 ruiniert. Danke, Windows!

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

## 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.

Ein Bild, das Text, Software, Computersymbol, Webseite enthält.

Automatisch generierte Beschreibung

*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.

Ein Bild, das Text, Software, Computersymbol, Webseite enthält.

Automatisch generierte Beschreibung

## 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.

Ein Bild, das Text, Screenshot, Software, Webseite enthält.

Automatisch generierte Beschreibung

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.

## 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.

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

Automatisch generierte Beschreibung

## 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!

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

Automatisch generierte Beschreibung

## 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.

Ein Bild, das Text, Screenshot, Software, Computer enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte BeschreibungEin Bild, das Text, Screenshot, Software, Computersymbol enthält.

Automatisch generierte Beschreibung

Schlussendlich sieht man, dass die Rollen verschoben wurden:

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

Automatisch generierte Beschreibung

## Standort umbenennen

Mittels „Active-Directory-Standorte und -Dienste” kann man den Standort in Werkstätte umbennen:

A screenshot of a computer

Description automatically generated

## Replikation funktionsfähig

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

A computer screen shot of a computer

Description automatically generated

## 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:

Ein Bild, das Screenshot, Text, Multimedia, Software enthält.

Automatisch generierte Beschreibung

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.

Ein Bild, das Text, Screenshot, Software, Schrift enthält.

Automatisch generierte Beschreibung

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:

A screenshot of a computer

Description automatically generated

## FSMO-Rollen zurückholen

Mittels diesen Artikels kann man die FSMO-Rollen zurückforcieren: <https://www.windowspro.de/andreas-kroschel/fsmo-rollen-im-ad-schema-uebernehmen>

A screenshot of a computer program

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

## Benutzer anlegen

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## DHCP und DNS reparieren

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer error message

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Ergebnisse

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

DNS und DHCP + AD funktionieren wieder.

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Kommentar

Super Übung für die Matura 🤣