

Was man über FSMO Rollen wissen sollte

Beigesteuert von Carola 'Cat' Helfert

bei diesem Artikel werden die einzelnen Rollen der Flexible Single Master Operation vorgestellt und deren Bedeutung im Active Directory. Wie immer, hat auch dieser Artikel kein Anrecht auf Vollständigkeit ;)

Was man über FSMO wissen sollte ...1. Was ist FSMO?

FSMO steht für Flexible Single Master Operations und steht für die 5 Rollen eines Domain Controllers im AD um die es in diesem kleinen Artikel geht.

Da diese Operation Masters für eine langfristige Performance des AD sorgen, müssen sie für alle Domain Controller und Clients zugänglich sein, die ihren Service benötigen. Deswegen ist eine umsichtige Positionierung umso wichtiger, desto mehr Domänen es in dem Forest gibt.

Die einzelnen Rollen werden in diesem Artikel kurz vorgestellt.2. FSMO Rollen2.1. Schemamaster

Der Schemamaster ist der einzige Domain Controller der Änderungen am Schema des Active Directory verarbeiten kann. Ist der Schemamaster nicht verfügbar, können keine Änderungen am Schema durchgeführt werden.

LDAP:

LDAP://CN=Schema,CN=Configuration,DC=Unterwegs-im,DC=Net

Hinweis:

- • Es darf immer nur ein Schemamaster in einem Forest vorhanden sein!
- • Der Domain Controller, der die Funktion des Schemamasters bekommt, sollte immer auch Global Catalog Server sein.
- • Schemamaster und Domain Naming Master sollte auf demselben DC laufen, da sie selten verwendet werden und engmaschig kontrolliert werden sollten.

Der Domain Naming Masters steuert das Hinzufügen und Entfernen von Domänen und Verzeichnis Partitionen im Forest. Er kann auch Querverweise zu Domänen in externen Verzeichnissen hinzufügen, oder aus diesen entfernen. Der Domain Controller, der diese Funktion hat, muss für folgende Aufgaben verfügbar sein:

- • Hinzufügen von neuen Domänen oder Application Verzeichnis Partitionen im Forest
- • entfernen von Domänen oder Application Verzeichnis Partitionen aus dem Forest
- • hinzufügen von Replikationen existierender Application Verzeichnis Partitionen zu weiteren Domain Controllern.
- • hinzufügen oder entfernen von cross-reference objects zu oder von externen Verzeichnissen.
- • vorbereiten des Forest für eine Umbenennung

Ist der Domain Naming Master nicht verfügbar, können keine Domains hinzugefügt, oder gelöscht, oder umbenannt werden, Auch können keine Applikation Directory Partitionen hinzugefügt oder gelöscht werden.

LDAP:

LDAP://CN=Partitions,CN=Configuration,DC=Unterwegs-im,DC=Net

Hinweis:

- • Es darf nur ein Domain Naming Master in einem Forest vorhanden sein.
- • Der Domain Controller, der die Funktion des Domain Naming Masters bekommt, sollte immer auch Global Catalog Server sein.
- • Schemamaster und Domain Naming Master sollte auf demselben DC laufen, da sie selten verwendet werden und engmaschig kontrolliert werden sollten.

Der PDC - Emulator ist innerhalb einer Firmenumgebung für die Synchronisation der Uhrzeit nötig. Der Windows Zeitdienst (w32time) ist wiederum für die Kerberos Authentifizierung nötig.

Der PDC - Emulator einer Domäne ist für die Domäne zuständig, der PDC - Emulator am Stamm des Forest ist für die gesamte Firmenumgebung zuständig und sollte so konfiguriert sein, dass er die Zeit mit einer externen Quelle abgleicht. Alle PDC-FSMO Rolleninhaber folgen bei der Auswahl ihrer eingehenden Zeitpartner der Domainhierarchie.

Folgende Aufgaben erfüllt der PDC - Emulator:

- • Kennwortänderungen, die von anderen Domain Controllern in der Domain ausgeführt werden, werden bevorzugt auf den PDC - Emulator repliziert.
- • Fehler bei der Authentifizierung, die auf einem bestimmten Domain Controller in einer Domain aufgrund eines fehlerhaften Kennwortes auftreten, werden dem PDC - Emulator weitergeleitet, bevor dem Benutzer eine Meldung zu einem Kennwortfehler angezeigt wird.
- • Die Kennwortsperrung wird auf dem PDC - Emulator verarbeitet.

Wenn die Domain Computer umfasst, auf denen keine Windows 2000 Clientsoftware ausgeführt wird, oder wenn die Domain Windows NT 4.0 Backup Domain Controller (BDC's) enthält, fungiert der PDC - Emulator als Windows NT PDC.

• Der PDC - Emulator übernimmt alle Aufgaben, die ein Microsoft Windows NT 4.0-basierter PDC (oder früher) für alle Windows NT 4.0-Clients (oder früher) ausfüllt.

Ist der PDC - Emulator nicht verfügbar, können keine Passwortänderungen von nicht AD Clients (NT4 oder älter) durchgeführt werden. Es erfolgt keine Replikation zu NT4 BDC's. Bei AD Clients kann es zufallsmässig zu Logon Fehlern kommen, und die Anmeldung braucht unter Umständen sehr lange.

LDAP:

LDAP://DC=Unterwegs-im,DC=Net

Hinweis:

- • Pro Domain in einem Forest kann nur ein PDC - Emulator vorhanden sein!
- • Bei Windows Server 2003 ist der PDC Emulator verantwortlich für das Management der „bekanntesten Sicherheits-Prinzipals" deswegen ist es wichtig, dass der PDC Emulator recht früh upgegradet wird, so dass der "CN=WellKnown Security Principals,CN=Configuration,DC=unterwegs-im,DC=Net" Container upgedatet wird.
- • PDC Emulator und RID Master sollten auf einem Domain Controller sein

Der Infrastructuremaster ist für die Aktualisierung der Sicherheitskennungen und definierten Namen von domänenübergreifenden Objektverweisen zuständig, wenn sich der Name eines Objektes ändert.

Der Infrastructuremaster ist für die Aktualisierung der der Objekt Referenzen seiner Domain zuständig, die auf ein Objekt in einer anderen Domain zeigen. Diese Referenzen aktualisiert er lokal und verwendet die Replikation, um alle anderen Domänen aktuell zu halten. Die Objekt Referenz enthält die global eindeutige ID (GUID), den Distinguished Name und eventuell eine SID. Distinguished Name und SID werden periodisch aktualisiert, um Änderungen am aktuellen Objekt anzuzeigen. Diese Änderungen umfassen verschieben und löschen des betreffenden Objekts.

Ist der Infrastructuremaster nicht verfügbar, werden Objekt Aktualisierungen verschoben, bis er wieder verfügbar ist.

LDAP:

LDAP://CN=Infrastructure,DC=Unterwegs-im,DC=Net

Hinweis:

- • Pro Domain in einem Forest darf nur ein Domaincontroller als Infrastructuremaster fungieren.
 - • Der Infrastructuremaster sollte niemals mit dem Global Catalog Server zusammen auf einem Domaincontroller laufen. Ist die Trennung nicht möglich, müssen alle Domaincontroller Global Catalog Server werden.
- 2.5. RID Master
Der RID Master ist innerhalb einer Domain der Verantwortliche für die Zuweisung der relativen Kennungen (Relative IDs, RIDs). Sobald ein Domain Controller ein Benutzer-, Gruppen- oder Computerobjekt erstellt, weist der der RID-Master diesem Objekt eine eindeutige Sicherheits - ID zu. Die Sicherheitskennung (SID, Security Identifier) (Erklärung hier: <http://techtalk.unterwegs-im.net/content/view/25/3/>) enthält eine Domänenkennung sowie einen Relativen Bezeichner, der für jede in der Domain erstellte SID eindeutig ist. Darüber hinaus ist er dafür zuständig, Objekte aus seiner Domain zu entfernen oder es bei einer Objektverschiebung in eine andere Domain zu versetzen.

Sollte der RID Master nicht verfügbar sein, kann es passieren, dass die Domain Controller keine neuen Directory Objekte mehr anlegen können, sofern jeder ihrer individuellen RID-Pools erschöpft sind.

LDAP:

LDAP://CN=Rid Manager\$,CN=System,DC=Unterwegs-im,DC=Net

Hinweis:

- • Pro Domain in einem Forest darf nur ein RID Master vorhanden sein!
- • PDC Emulator und RID Master sollten auf einem Domain Controller sein

Auch wenn der Global Catalog nicht als FSMO Rolle definiert ist, ist er im Active Directory für die Benutzeranmeldung sehr wichtig, ist er nicht erreichbar, ist keine Anmeldung am Active Directory möglich, außer das Caching für Universelle Gruppen ist aktiviert (Mitglieder der Gruppe der Domain Admins können sich in jedem Fall weiterhin anmelden).

Der Global Catalog übernimmt im Active Directory zwei Aufgaben:

- • Er ermöglicht das Auffinden von Informationen im Verzeichnis, unabhängig davon in welcher Domäne der Gesamtstruktur.
- • Er ermöglicht die Netzwerkanmeldung, indem einem Domain Controller, bei Initialisierung eines Anmeldeprozesses, Informationen zu Mitgliedschaften in universellen Gruppen zur Verfügung gestellt werden.

Aufgrund verschiedener Ursachen kann es dazu kommen, dass die bestehende FSMO Verteilung nicht mehr passt.

Wenn man diesen Regeln hier folgt, ist es ganz einfach, die Rollen auf andere Domain Controller zu übertragen ;)

- • Die beiden Rollen, die einmalig im Forest sind, sollten auf einem Domain Controller an der root des Forests sein.
- • Auch sollten diese auf einem Global Catalog laufen.
- • Die domänenweiten Rollen sollten auf demselben Domain Controller sein.
- • In einem Forest, der viele Domänen enthält, sollten die domänenweiten Rollen nicht auf einem Global Catalog Server sein, außer alle anderen Domain Controller sind ebenfalls Global Catalog Server.
- • Die domänenweiten Rollen sollten auf einem performanteren Domain Controller laufen.

Hinweis:

- • Active Directory erfordert einen ordentlich konfigurierten DNS (Domain Name System), so dass die Domain Controller problemlos die DNS Namen der Replikations Partner auflösen können.

Für die Verwaltung der Operations Master Rollen gibt es verschiedene Rechte, die an Gruppen oder User im Forest vergeben werden können. Folgende Benutzer-Rechte sind nötig, um die Operations Master Rollen zu verändern.

- • Das „Change Schema Master" Recht ist nötig um den Schema Master zu verschieben oder festzulegen. Normalerweise haben nur Mitglieder der Gruppe „Schema Administrators" dieses Recht.
- • Das „Change Domain Master" Recht ist richtig nötig um den Domain Naming Master zu verschieben oder

festzulegen. Normalerweise haben nur Mitglieder der Gruppe "Enterprise Admins" dieses Recht.

- Das "Change PDC" Recht ist nötig um den PDC Emulator zu verschieben oder festzulegen. Normalerweise haben nur Mitglieder der Gruppe "Domain Admins" dieses Recht.
- Das "Change Infrastructure Master" Recht ist nötig um den Infrastructure Master zu verschieben oder festzulegen. Normalerweise haben nur Mitglieder der Gruppe "Domain Admins" dieses Recht.
- Das "Change RID Master" Recht ist nötig um den RID zu verschieben oder zu festzulegen. Normalerweise haben nur Mitglieder der Gruppe "Domain Admins" dieses Recht.

3.2. Verschieben von FSMO Rollen (Transfer)

Bei einer Übertragung einer FSMO Rolle zwischen zwei Domänencontrollern werden die rollenspezifischen Daten, zwischen dem alten FSMO Inhaber und dem neuen Server, der die FSMO Rolle erhalten soll, zuerst synchronisiert, damit alle Änderungen vor der Rollenänderung aufgezeichnet wurden.

Es gibt so genannte Betriebsattribute, die die FSMO Rollen darstellen. Diese werden beim Übertragen der Rollen automatisch bei dem neuen Rolleninhaber hinzugefügt und bei dem alten entfernt. Diese Attribute sind nicht im Schema definiert, sondern werden vom Server selber verwaltet. Erhält ein Server so ein Attribut, wird dieses in eine Aktion umgesetzt.

- becomeRidMaster

- becomeSchemaMaster

- becomeDomainMaster

- becomePDC

- becomeInfrastructureMaster

Wird ein Domain Controller demotet, so wird das Vorgangsattribut "GiveAwayAllFsmoRoles" geschrieben, sodass der Domain Controller andere Domain Controller sucht, denen er alle Rollen, die er inne hat, geben kann. Um einen passenden Domain Controller zu finden, werden folgende Regeln verwendet:

1. Suche eines Servers auf der gleichen Site.
2. Suche eines Servers, zu welchem RPC-Konnektivität besteht.
3. Verwendung eines Servers über asynchronen Transport (wie z.B. SMTP).

Domänenspezifische Rollen können dabei nur innerhalb der Domäne übertragen werden. Ansonsten kommt jeder beliebige Domänencontroller infrage.

Hinweis:

- Das Verschieben von FSMO Rollen zwischen Domänencontrollern kann nur vom Administrator oder durch Herabstufen eines Domänencontrollers ausgelöst werden, es wird jedoch nicht automatisch durch das Betriebssystem initiiert. FSMO Rollen werden nicht automatisch während des Herunterfahrens verschoben.

3.3. Festlegen von FSMO Rolle (Seizure)

Beim Festlegen einer FSMO Rolle, wird einem Domain Controller diese zugewiesen, ohne die Interaktion mit dem vorigem Inhaber. Das sollte nur dann ausgeführt werden, wenn der ursprüngliche Besitzer der FSMO-Rolle nicht wieder in die Umgebung zurückversetzt wird. Sollte der vorige Inhaber wieder zurückkommen, kann es zu inkonsistenten Daten im Active Directory kommen!!!

Wird eine FSMO Rolle einem Domain Controller zugewiesen, wird das Attribut fsmoRoleOwner modifiziert. Sobald diese Änderung repliziert wird, werden weitere Domain Controller über die Änderung der FSMO Rolle unterrichtet.

3.4. Tools

Für das erfolgreiche Managen der FSMO Rollen, sollte man folgende Tool kennen ;)

3.4.1. dcpromo.exedcpromo promotet einen Server zu einem Domain Controller, bzw. demotet ihn wieder. Beim demoten werden alle FSMO Rollen, die er innehat automatisch an einen anderen Domain Controller übergeben (siehe 3.2.)

3.4.2. ntdsutil.exe

Ntdsutil.exe ist ein Command Line Tool zum Management von Active Directory. Ntdsutil wird für Datenbank Maintenance des Active Directory, dem Management und der Kontrolle von FSMO Rollen verwendet. Insbesondere wird ntdsutil zum Entfernen von Metadaten verwendet, die durch das ungeplante entfernen von Domain Controllern entstanden sind (vgl. auch 3.3.) Dieses Tool sollten nur erfahrene Administratoren anwenden.

1. öffnen einer Command Line
2. Eingabe von:
ntdsutil
3. an der ntdsutil Eingabeaufforderung eingeben:
roles
4. an der FSMO Maintenance Eingabeaufforderung eingeben:
connection
5. an der Serververbindungs Eingabeaufforderung eingeben:
set creds <network> Administrator <Passwort>
6. an der Serververbindungs Eingabeaufforderung eingeben:

connect to server <Domain Controller>

7. an der Serververbindungs Eingabeaufforderung eingeben:

quit

8. an der FSMO Maintenance Eingabeaufforderung eingeben:

transfer <Rolle>

so siehts in "echt" aus: zum Textfile hier klicken

3.4.3. dsa.msc

Hinter dsa.msc verbirgt sich die MMC „Active Directory - Benutzer und Computer" mit der man über eine GUI die FSMO Rollen ändern kann.

1. öffnen von „Active Directory - Benutzer und Computer"

2. in der Konsolenstruktur mit der rechten Maustaste auf die root gehen und „Verbindung mit Domain Controller herstellen" auswählen

3. da dann den Namen des Domain Controllers angeben (oder aus der Liste auswählen), der die entsprechende Rolle in Zukunft verwalten soll.

4. in der Konsolenstruktur mit der rechten Maustaste auf „Alle Tasks" und „Betriebsmaster" auswählen

5. bei den „Tabs" die entsprechende Rolle auswählen und auf „ändern" drücken4. Operations Master Protokolle4.1. Lightweight directory access protocol (LDAP)

LDAP ist das primäre Directory Service Protokoll, das überwiegend den TCP/IP Stack verwendet. Doch auch UDP wird verwendet, wie zum Beispiel vom Domain Controller Locator Prozess. LDAP wird von den Clients verwendet, um Informationen anzufragen, erstellen, aktualisieren und zu löschen. Dafür wird eine TCP Verbindung über Port 389 verwendet. Active Directory unterstützt die LDAP Formate 2 und 3. LDAP ist der bevorzugte und am meisten verbreitete Weg, um mit Active Directory zu interagieren.

vgl.:

LDAP v2 - RFC 1777

LDAP v3 - RFC 22514.2. Remote procedure call (RPC)

RPC ist das Protokoll, das von der Replikation, der Domänen Management Kommunikation und aller Kommunikation bezüglich SAM verwendet wird. RPC ist ein sicherer Interprocess Kommunikation (IPC) Mechanismus, der Datenaustausch ermöglicht.

vgl.:

RPC - RFC 1050 und 1831

IPC - RFC 1504.3. Simple mail transfer protocol (SMTP)

SMTP ist das Protokoll, das für die Replikation verwendet wird, wenn es keine dauerhafte Netzwerkverbindung zu den anderen Domain Controllern gibt. SMTP kann die Konfiguration, die Application Directory Partition, das Schema und den Global Catalog replizieren.

vgl.:

SMTP - RFC 821 und 8224. Network Ports

Service Name

UDP

TCP

LDAP

389

389

LDAP

686 (Secure Sockets Layer [SSL])

RPC/REPL

135 (endpoint mapper)

NetLogon

137

Kerberos

88

88

DNS

53

53

SMB over IP

445
445

Quellen:

How Operations Masters Works

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/795229a5-8a74-4edb-a2f4-d5794d31c2a7.msp>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/795229a5-8a74-4edb-a2f4-d5794d31c2a7.msp>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/795229a5-8a74-4edb-a2f4-d5794d31c2a7.msp>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/795229a5-8a74-4edb-a2f4-d5794d31c2a7.msp>

Übertragung und Übernahme von FSMO

<http://support.microsoft.com/default.aspx?scid=kb;de;223787>

FSMO-Platzierung und -Optimierung auf Windows 2000-Domänen

<http://support.microsoft.com/kb/223346/DE/>

BOL

Using ntdsutil

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/5b1d983d-ffab-4514-a95e-6aa0420dacb5.msp>

© Carola ‘Cat' Helfert, unterwegs-im.net 2005