

Windows 2000 FSMO Roles

Mark E. Donaldson

Introduction

In Windows 2000 all domain controllers are equal, and through a process known as multi-master replication changes are replicated to all domain controllers in the domain. Multi-master replication resolves conflicts however in some situations it is better to stop the conflict before it happens and to this end there are five different Flexible Single Master of Operations (FSMO) roles (formally known as Floating Single Master of Operations as the roles were originally going to be dynamically changeable) each managing an aspect of the domain/forest. These roles can be moved between domain controllers but not dynamically, they must be manually moved in the same manner as a BDC has to be manually promoted to a PDC.

There are two types of roles, some are per domain, some are per forest. Only a domain controller in the domain can hold a domain specific FSMO role, any domain controller in the forest can hold a forest FSMO role. Domain controllers cannot hold FSMO roles in other domains/forests. These roles are assigned in different GUI ways or using the **NTDSUTIL** utility.

The five roles are defined below:

- **Schema Master** - At the heart of the Active Directory is the schema which is like the blueprint of all objects/containers. Since the schema has to be the same throughout the entire forest only one machine can authorize modifications to the schema. One per forest.
- **Domain Naming Master** - To add a domain to the forest its name has to be verifiably unique and so the Domain naming master FSMO's of the forest is contacted to authorize the domain name operation. One per forest.
- **RID Master** - Any domain controller can create new objects (such as a user, group, computer account) however after creating 512 user objects the domain controller must contact the domains RID master for another 512 RID's (it actually contacts when it has less than 100 RID's left, this means the RID master can be unavailable for short periods of time without causing object creation problems). This is to ensure each object has a unique RID. When a DC creates a security principal object it attaches a unique SID to the object. The SID is created using the domain SID and a relative ID (the RID). The RID master has to be available when attempting to move objects between domains with the resource kit movetree utility. One per domain.
- **PDC Emulator** - For backwards compatibility reasons one domain controller in each 2000 domain must emulate a PDC for the benefit of 4.0 and 3.5 domain controllers and clients. One per domain.
- **Infrastructure Master** - When a user and group are in different domains there can be a lag between changes to the user (e.g. name) and its display in the group. The infrastructure master of the groups domain is responsible for fixing up the group-to-user reference to reflect the rename. The infrastructure master performs its fixups locally and relies upon replication to bring all other replicas of the domain up to date. One per domain.

RID Master

To modify the role of the RID Master, perform the following:

- Start the Active Directory Users and Computers MMC snap-in on the Domain Controller (Start - Programs - Administrative Tools - Active Directory Users and Computers).
- In the left hand pane right click on the domain and select 'Connect to Domain Controller'.

Windows 2000 FSMO Roles

Mark E. Donaldson

- Select the domain controller you wish to make the FSMO role owner and click OK.
- Right click on the domain again and select 'Operations Masters' from the context menu.
- Select the 'RID Pool' tab.
- The current machine holding the RID master FSMO role will be shown. To change click 'Change'.
- Click OK to the confirmation dialog.
- A dialog confirming the role change will be displayed.

This can also be accomplished using the **NTDSUTIL.EXE** utility.

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server <server name>
server connections: quit
fsmo maintenance: transfer rid master
```

Click Yes to the role transfer dialog.

```
Server "Domain Name" knows about 5 roles Schema:
CN=NTDSSettings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=savilltech,DC=com Domain
CN=NTDSSettings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=savilltech,DC=comPDC - CN=NTDSSettings,CN=DOMAIN
NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com RID - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com Infrastructure - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=savilltech,DC=com
fsmo maintenance: quit
ntdsutil: quit
```

PDC Emulator FSMO

To modify the role perform the following:

- Start the Active Directory Users and Computers MMC snap-in on the Domain Controller (Start - Programs - Administrative Tools - Active Directory Users and Computers).
- In the left hand pane right click on the domain and select 'Connect to Domain Controller'.
- Select the domain controller you wish to make the FSMO role owner and click OK.
- Right click on the domain again and select 'Operations Masters' from the context menu.
- Select the 'PDC' tab.

Windows 2000 FSMO Roles

Mark E. Donaldson

- The current machine holding the PDC emulator FSMO role will be shown. To change click 'Change'.
- Click OK to the confirmation dialog.
- A dialog confirming the role change will be displayed.

This can also be accomplished using the **NTDSUTIL.EXE** utility.

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server <server name>
server connections: quit
fsmo maintenance: transfer pdc
```

Click Yes to the role transfer dialog.

```
Server "Domain Name" knows about 5 roles Schema - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com Domain - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com PDC - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com RID - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com Infrastructure - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com
```

```
fsmo maintenance: quit
ntdsutil: quit
```

Infrastructure FSMO

To modify the role perform the following:

- Start the Active Directory Users and Computers MMC snap-in on the Domain Controller (Start - Programs - Administrative Tools - Active Directory Users and Computers).
- In the left hand pane right click on the domain and select 'Connect to Domain Controller'.
- Select the domain controller you wish to make the FSMO role owner and click OK.
- Right click on the domain again and select 'Operations Masters' from the context menu.
- Select the 'Infrastructure' tab.
- The current machine holding the Infrastructure FSMO role will be shown. To change click 'Change'.
- Click OK to the confirmation dialog.

Windows 2000 FSMO Roles

Mark E. Donaldson

- A dialog confirming the role change will be displayed.

This can also be accomplished using the **NTDSUTIL.EXE** utility.

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server <server name>
server connections: quit
fsmo maintenance: transfer infrastructure master
```

Click Yes to the role transfer dialog.

```
Server "Domain Name" knows about 5 roles Schema - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com Domain - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com PDC - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com RID - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com Infrastructure - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com
fsmo maintenance: quit
ntdsutil: quit
```

Domain Naming Master FSMO

To modify the role perform the following however make sure the machine is a global catalog:

- Start the Active Directory Domains and Trusts MMC snap-in on the Domain Controller (Start - Programs - Administrative Tools - Active Directory Domains and Trusts).
- In the left hand pane right click on 'Active Directory Domains and Trusts' and select 'Connect to Domain Controller' from the context menu.
- Enter the domain controller to connect.
- Right click on 'Active Directory Domains and Trusts' and select 'Operations Master' from the context menu.
- The current machine holding the Domain name operations FSMO role will be shown. To change click 'Change'.
- Click OK to the confirmation dialog.
- A dialog confirming the role change will be displayed.

This can also be accomplished using the **NTDSUTIL.EXE** utility.

Windows 2000 FSMO Roles

Mark E. Donaldson

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server <server name>
server connections: quit
fsmo maintenance: transfer domain naming master
```

Click Yes to the role transfer dialog.

```
Server "Domain Name" knows about 5 roles Schema - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com Domain - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=savilltech,DC=com PDC - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com RID - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com Infrastructure - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=savilltech,DC=com
```

```
fsmo maintenance: quit
ntdsutil: quit
```

Schema Master FSMO

To modify the role perform you must use the 'Active Directory Schema Manager' and you must first register the .dll for the MMC snap-in:

```
C:\> regsvr32 schmmgmt.dll
```

You can now start the Schema Manager via the Resource Kit Tools console or by creating a custom MMC and add the Active Directory Schema snap-in to it (Start - Run - MMC - Console menu - Add/Remove Snap-in - Add - Active Directory Schema - Add - Close - OK):

- Start the Active Directory Schema MMC snap-in on the Domain Controller (using on of the methods above).
- In the left hand pane right click on 'Active Directory Schema' and select 'Change Domain Controller' from the context menu.
- Enter the domain controller to connect.
- Right click on 'Active Directory Domains Schema' and select 'Operations Master' from the context menu.
- The current machine holding the Domain name operations FSMO role will be shown. To change click 'Change..'
- You can also set the registry to allow changes to the Schema by checking the Schema modification box. Also notice this machine is already the schema master.
- Click OK to the confirmation dialog.

Windows 2000 FSMO Roles

Mark E. Donaldson

- A dialog confirming the role change will be displayed.

To modify the role from the command line enter the following:

```
C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server <server name>
server connections: quit
fsmo maintenance: transfer schema master
```

Click Yes to the role transfer dialog.

```
Server "Domain Name" knows about 5 roles Schema - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=name,DC=com Domain - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=name,DC=com PDC - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=name,DC=com RID - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Sites
,CN=Configuration,DC=name,DC=com Infrastructure - CN=NTDS
Settings,CN=DOMAIN NAME,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,DC=name,DC=com
fsmo maintenance: quit
ntdsutil: quit
```

Multi-Master Replication

In a Windows 2000 domain, all domain controllers are equal which means changes can be made on ANY domain controller and each servers complete domain directory has to be kept up-to-date with each other through a process of multi-master replication.

Each time a change is made to the Active Directory the servers Update Sequence Number, or USN, where the change is implemented is incremented by one and this USN is also stored along with the change to the property of the object modified. These changes have to be replicated to all domain controllers in the domain and the Update Sequence Number provides the key to the multi-master replication.

Update Sequence Number increments are atomic in operation which means that the increment to the USN and the actual change occurs simultaneously, if one part fails the whole change fails which means its not possible for a change to be made without the USN to be incremented, which means changes will never be "lost". Each domain controller keeps track of the highest USN's of the other domain controllers that it replicates with so it can calculate which changes it needs to be replicated on each replication cycle.

At the start of the replication cycle each server checks its Update Sequence Number table and then queries the domain controllers it replicates with for their latest USN's. For example the table below represents the USN table for server A:

DC B	DC C	DC D	54	23	53
------	------	------	----	----	----

Windows 2000 FSMO Roles

Mark E. Donaldson

Server A then queries the domain controllers for their current USN's and gets the following:

DC B DC C DC D 58 23 64

From this server A can calculate the changes it needs from each server:

DC B DC C DC D 55,56,57,58 Up-to-date 54-64

It would then query each server for the changes needed.

It is possible for multiple changes to the same property of an object to occur, and collisions are detected via a Property Version Number (PVN) which every property has. These work like the USN's and each time a property is modified, the PVN is incremented by one.

In the event of a modification to the same property of the same object then the change with the highest PVN takes precedence, and if the PVN's are the same for a property update then a collision has occurred. If the PVN's match then the time stamp is used to resolve any conflicts. Each change is time stamped and this highlights the need for the domain controllers time to be accurate with one-another. In the highly unlikely event that the PVN's match AND the time stamp is the same then a binary buffer comparison is carried out with the larger buffer size change taking precedence. Property Version Numbers are only incremented on original writes and not on replication writes (unlike USN's) and are not server specific but rather travels with the property.

A propagation-dampening scheme is also use to stop changes being repeatedly sent to other servers which already have the change and to this end each server keeps a table of up-to-date vectors which are the highest originating writes that are received from each controller and take the form of:

<the change>,<domain controller making the original change>,<USN of the change>

For example:

<object name, property Password xxx>,Domain Name,54

Domain controllers then also send this information with the USN's so they can calculate if they already have the change the other domain controllers are trying to replicate.

Move Objects In Forest

The Windows 2000 Resource Kit ships with the **MOVETREE.EXE** utility which can be used to move organization units, users or computers between domains in a single forest. This is useful for the consolidation of domains or to reflect organization restructuring.

Certain objects cannot be moved with MOVETREE such as Local and Domain Global groups and if the container they are in is moved these objects will be placed in an "orphan" container in the "LostAndFound" container in the source domain.

Associated data is not moved with MOVETREE such as policies, profiles, logon scripts and personal data. To accomplish the movement of these items you should write custom scripts using the 'Remote Administration Scripts'.

The syntax of MOVETREE is:

Windows 2000 FSMO Roles

Mark E. Donaldson

```
MoveTree [/start | /continue | /check] [/s SrcDSA] [/d DstDSA] [/sdn SrcDN]
[/ddn DstDN] [/u Domain\Username] [/p Password] [/quiet]
```

- /start Start a move tree operation with
- /check option by default. Instead, you could be able to use
- /startnocheck to start a move tree operation without any check.
- /continue Continue a failed move tree operation.
- /check Check the whole tree before actually move any object.
- /s <SrcDSA> Source server's fully qualified primary DNS name. Required.
- /d <DstDSA> Destination server's fully qualified primary DNS name. Required.
- /sdn <SrcDN> Source sub-tree's root DN. Required in Start and Check case.
- /ddn <DstDN> Destination sub-tree's root DN. RDN plus Destination Parent DN. Required.
- /u <Domain\UserName> Domain Name and User Account Name. Optional.
- /p <Password> Password. Optional.
- /quiet Quiet Mode. Without Any Screen Output. Optional

You should first run in /check mode as this will perform a test without actually performing the move. Any errors will be displayed and also written to the file movetree.err in your current directory. If the test is OK run with the /start option.

An example use would be:

```
C:\> movetree /check /s Domain Name.market.name.com /d pluto.legal.name.com
/sdn OU=testing,DC=Market,DC=Name,DC=COM/ddnU=test2,DC=Legal,DC=Name,DC=COM
```