## Overview

FSMO stands for Flexible Single Master Operations, and FSMO roles (also known as operations master roles) help you prevent conflicts in your Active Directory.

In this article we'll examine the difference between the single and multi-master models in Windows Server 2000, 2003 and 2008 and we'll go through what you need to know about the different FSMO roles. We'll also take a look at FSMO reliability and availability and what's new with FSMO in Windows Server 2008.



For most Active Directory objects, the task of updating can be performed by any Domain Controller except those Domain Controllers that are read-only. Updates such as computer object properties, renamed organizational units, and user account password resets can be handled by any writable domain controller.

After an object is changed on one domain controller, those changes are propagated to the other domain controllers through replication. During replication all of the Domain Controllers share their updates. So a user that has their password reset in one part of the domain may have to wait until those changes are replicated to the Domain Controller that they are signing in from.

This model works very well for most objects. In the case of any conflicts, such as a user's password being reset by both the central helpdesk as well as an administrator working at the user's site, then conflicts are resolved by whichever made the last change. However, there are some changes that are too important, and are not well suited to this model.

## Windows 2000/2003/2008 Single-Master Model

There are 5 specific types of updates to Active Directory that are very specific, and conflicts should be avoided. To help alleviate any potential conflicts, those updates are all performed on a single Domain Controller. And though each type of update must be performed on a single Domain Controller, they do not all have to be handled by the same Domain Controller.

These types of updates are handled by Domain Controllers Flexible Single Master Operations roles, or FSMO roles. Each of the five roles is assigned to only one domain controller.

There are five of these FSMO roles in every forest. They are:

Schema Master
Domain Naming Master
Infrastructure Master
Relative ID (RID) Master
Primary Domain Controller (PDC) Emulator
Additionally, three of those FSMO roles are needed once in every domain in the forest:

Infrastructure Master
Relative ID (RID) Master
Primary Domain Controller (PDC) Emulator
Here is what you need to know about the different FSMO roles.

• All Schema Changes and Updates to Active Directory are Processed by the DC with the Schema Master Role

Whenever the schema is modified at all, those updates are always completed by the domain controller with the schema master role. Schema is updated during the normal replication, and the schema updates are replicated throughout all the domains in the forest. Since the schema master role is only needed once in the forest, it is kept in the forest root domain. It's advisable to place the schema master role on the same domain controller (DC) as the primary domain controller (PDC) emulator.

• Changes to Which Domains are Part of the Forest are Processed by the DC with the Domain Naming Master Role

As domains join or leave the forest, the domain naming master makes the updates into active directory. Only this DC actually commits those changes into the directory. The domain naming master also commits the changes to application partitions. Like the schema master role, this role is a forest level FSMO, and it is only needed once across all domains in a forest. Also like the schema master, it is suggested to let this role be handled by the same domain controller – the PDC emulator in the forest root.

• Each Domain in a Forest Translates Names for Other Domains Through Their Infrastructure Master

The infrastructure master is a translator, between globally unique identifiers (GUIDs), security identifiers (SIDs), and distinguished names (DNs) for foreign domain objects. If you've ever looked at group memberships of a domain local group which has members from other domains,

you can sometimes see those users and groups from the other domain listed only by their SID. The infrastructure master of the domain of which those accounts are in is responsible for translating those from a SID into their name.

Each domain has their own infrastructure master, including the forest root and every child domain. Usually, you do not put the infrastructure master role on a domain that holds the global catalog. However, if you're in a single domain forest, the infrastructure master has no work to do, since there is no translation of foreign principals. In that case it's acceptable to place the infrastructure master it on any domain controller (DC), even if it has the global catalog. For a forest with multiple domains, if there's even one domain controller that doesn't have the global catalog on it, then you need to put the infrastructure master role on a domain controller that does not have the global catalog.

• The Unique Part of a Security Identifier is Assigned from the Relative ID (RID) Master

One of the first things understood about a security identifier (SID) is that they are unique. There are two parts of a SID: the domain identifier (domain ID), and the relative ID (RID). The domain identifier part of the SID is uniform among all security principals in the domain. When looking at a list of SIDs in a domain, it's easy to identify the domain SIDs – they all look the same. On the contrary, the relative ID part of the SID is the unique part. The two parts together make up what we commonly identify as a SID.

It is conceivable, then, that if two or more domain controllers were responsible for determining the relative IDs for the SIDs that two domain controllers may come up with the same relative ID for two different objects before they've replicated with each other.

That is impossible when only one DC in a domain is responsible for the creation of the relative IDs for SIDs. The relative ID master, or RID master, hands out batches of relative IDs to individual domain controllers, then each domain controller can use their allotment to create new users, groups, and computers. When domain controllers need more relative IDs in reserve, they request them from, and are assigned by, the domain controller with the RID master FSMO role.

Every domain in a forest must have a domain controller with the RID master FSMO role assigned to it. It is recommended that the RID master FSMO role be assigned to whichever domain controller has the PDC emulator FSMO role.

• The Domain Controller (DC) That is the Primary Domain Controller (PDC) Emulator is the Authoritative DC in a Domain

The domain controller that has the PDC emulator FSMO role assigned to it has many duties and responsibilities in the domain. For example, the DC with the PDC emulator role is the DC that updates passwords for users and computers. When a user attempts to login, and enters a bad password, it's the DC with the PDC emulator FSMO role that is consulted to determine if the

password has been changed without the replica DC's knowledge. The PDC emulator is also the default domain controller for many administrative tools, and is likewise the default DC used when Group Policies are updated.

Additionally, it's the PDC emulator which maintains the accurate time that the domain is regulated by. It's the time on the PDC emulator which identifies when the last write time for an object was (to resolve conflicts, for example.) If it's a forest with multiple domains, then the forest root PDC is the authoritative time source for all domains in the forest.

Each domain in the forest needs its own PDC emulator.

FSMO Reliability and Availability

Due to the importance of the FSMO roles, the domain controllers need to be online at the time the services are needed. For some of the FSMO roles, such as schema master, this is not very much. It only needs to be online when the schema is updated. For other roles, such as the PDC emulator, it needs to be online and accessible all the time.

Ideally, you put the PDC emulator on the domain controller with the best hardware available, and ensure that it's in a reliable hub site. It should have other domain controllers in the same active directory domain and site to replicate with. Then, to reduce administration and complexity, you also assign at least some of the other FSMO roles to the same DC – the RID master to the PDC of each domain, and the schema master and domain naming master the PDC of the forest root.

In the event that a DC with one of the FSMO roles is unavailable, especially the PDC emulator, it is critical for the domain to get that FSMO role back. If, for example, you know that the PDC emulator is going to have to be turned off for scheduled maintenance, you should transfer the FSMO role to a different domain controller. In the unfortunate event that the PDC emulator has crashed and is now down with an unplanned outage, you will have domain errors until the PDC emulator is bought back online. If you cannot get the PDC emulator back online, you may have to seize the FSMO role to another domain controller. It is always better to transfer ahead of time then have to seize the role after a crash. Seizing a role should be done only as a last resort. In the event of a seizure, you cannot ever bring the DC that previously held the role back online.

New with Windows Server 2008 Active Directory is the ability to designate ahead of time a standby operations master. This domain controller is connected directly to the primary operations master role holders through replication to

Summary

When updating a part of Active Directory is too critical of an operation to risk a conflict, Windows Active Directory Domains utilize a single-server model to provide updates to those services. The right to update or perform certain duties in Active Directory is granted to domain controllers through the assignment of one of the Flexible Single-Master roles, or FSMO roles.

There are five FSMO roles. Two of them, schema master and domain naming master, are only assigned once in the forest, in the domain at the forest root. The other three FSMO roles: RID master, PCD emulator, and the infrastructure master, are assigned in each domain, typically all to the same domain controller.

The availability requirements of the domain controller with an FSMO role are dependent on the role. For example, the schema master may be offline without causing any concern until an update to the schema is attempted. FSMO roles can be transferred to another domain controller to improve performance or to allow for continued access during a scheduled outage. In the event of an unscheduled outage, FSMO roles may be seized as a last resort.