

Managing Active Directory FSMO Roles

Mitch Tullock

While Active Directory in general uses a multimaster replication scheme for replicating the directory database between domain controllers, there are certain directory functions that require they be performed on some specific domain controller. These functions are defined by flexible single master operations (FSMO) roles (pronounced "fiz-moe roles") and at any time these roles are uniquely assigned to specific domain controllers in different Active Directory domains. Let's begin by describing what these different FSMO roles are and why they are important, after which we'll outline some best practices for how you should assign these roles in your Active Directory environment.

Overview of FSMO Roles

There are five different FSMO roles and they each play a different function in making Active Directory work:

PDC Emulator

This role is the most heavily used of all FSMO roles and has the widest range of functions. The domain controller that holds the PDC Emulator role is crucial in a mixed environment where Windows NT 4.0 BDCs are still present. This is because the PDC Emulator role emulates the functions of a Windows NT 4.0 PDC. But even if you've migrated all your Windows NT 4.0 domain controllers to Windows 2000 or Windows Server 2003, the domain controller that holds the PDC Emulator role still has a lot to do. For example, the PDC Emulator is the root time server for synchronizing the clocks of all Windows computers in your forest. It's critically important that computer clocks are synchronized across your forest because if they're out by too much then Kerberos authentication can fail and users won't be able to log on to the network. Another function of the PDC Emulator is that it is the domain controller to which all changes to Group Policy are initially made. For example, if you create a new Group Policy Object (GPO) then this is first created in the directory database and within the SYSVOL share on the PDC Emulator, and from there the GPO is replicated to all other domain controllers in the domain. Finally, all password changes and account lockout issues are handled by the PDC Emulator to ensure that password changes are replicated properly and account lockout policy is effective. So even though the PDC Emulator emulates an NT PDC (which is why this role is called PDC Emulator), it also does a whole lot of other stuff. In fact, the PDC Emulator role is the most heavily utilized FSMO role so you should make sure that the domain controller that holds this role has sufficiently beefy hardware to handle the load. Similarly, if the PDC Emulator role fails then it can potentially cause the most problems, so the hardware it runs on should be fault tolerant and reliable. Finally, every domain has its own PDC Emulator role, so if you have N domains in your forest then you will have N domain controllers with the PDC Emulator role as well.

RID Master

This is another domain-specific FSMO role, that is, every domain in your forest has exactly one domain controller holding the RID Master role. The purpose of this role is to replenish the pool of unused relative IDs (RIDs) for the domain and prevent this pool from becoming exhausted. RIDs are used up whenever you create a new security principle (user or computer account) because the SID for the new security principle is constructed by combining the domain SID with a unique RID taken from the pool. So if you run out of RIDs, you won't be able to create any new user or computer accounts, and to prevent this from happening the RID Master monitors the RID pool and generates new RIDs to replenish it when it falls beneath a certain level.

Infrastructure Master

This is another domain-specific role and its purpose is to ensure that cross-domain object references are correctly handled. For example, if you add a user from one domain to a security group from a different domain, the Infrastructure Master makes sure this is done properly. As you can guess however, if your Active Directory deployment has only a single domain, then the Infrastructure Master role does no work at all, and even in a multi-domain environment it is rarely used except when

Managing Active Directory FSMO Roles

Mitch Tullock

complex user administration tasks are performed, so the machine holding this role doesn't need to have much horsepower at all.

Schema Master

While the first three FSMO roles described above are domain-specific, the Schema Master role and the one following are forest-specific and are found only in the forest root domain (the first domain you create when you create a new forest). This means there is one and only one Schema Master in a forest, and the purpose of this role is to replicate schema changes to all other domain controllers in the forest. Since the schema of Active Directory is rarely changed however, the Schema Master role will rarely do any work. Typical scenarios where this role is used would be when you deploy Exchange Server onto your network, or when you upgrade domain controllers from Windows 2000 to Windows Server 2003, as these situations both involve making changes to the Active Directory schema.

Domain Naming Master

The other forest-specific FSMO role is the Domain Naming Master, and this role resides too in the forest root domain. The Domain Naming Master role processes all changes to the namespace, for example adding the child domain vancouver.mycompany.com to the forest root domain mycompany.com requires that this role be available, so you can't add a new child domain or new domain tree, check to make sure this role is running properly.

To summarize then, the Schema Master and Domain Naming Master roles are found only in the forest root domain, while the remaining roles are found in each domain of your forest. Now let's look at best practices for assigning these roles to different domain controllers in your forest or domain.

FSMO Roles Best Practices

Proper placement of FSMO Roles boils down to three simple rules:

Rule One

In your forest root domain, keep your Schema Master and Domain Naming Master on the same domain controller to simplify administration of these roles, and make sure this domain controller contains a copy of the Global Catalog. This is not a hard-and-fast rule as you can move these roles to different domain controllers if you prefer, but there's no real gain in doing so and it only complicates FSMO role management to do so. If for reasons of security policy however your company decides that the Schema Master role must be fully segregated from all other roles, then go ahead and move the Domain Naming Master to a different domain controller that hosts the Global Catalog. Note though that if you've raised your forest functional level to Windows Server 2003, your Domain Naming Master role can be on a domain controller that doesn't have the Global Catalog, but in this case be sure at least to make sure this domain controller is a direct replication partner with the Schema Master machine.

Rule Two

In each domain, place the PDC Emulator and RID Master roles on the same domain controller and make sure the hardware for this machine can handle the load of these roles and any other duties it has to perform. This domain controller doesn't have to have the Global Catalog on it, and in general it's best to move these two roles to a machine that doesn't host the Global Catalog because this will help balance the load (the Global Catalog is usually heavily used).

Rule Three

In each domain, make sure that the Infrastructure Master role is not held by a domain controller that also hosts the Global Catalog, but do make sure that the Infrastructure Master is a direct replication partner of a domain controller hosting the Global Catalog that resides in the same site as the

Managing Active Directory FSMO Roles

Mitch Tullock

Infrastructure Master. Note however that this rule does have some exceptions, namely that the Infrastructure Master role can be held by a domain controller hosting the Global Catalog in two circumstances: when there is only one domain in your forest or when every single domain controller in the domain also hosts the Global Catalog.

To summarize these three rules then and make them easy to remember:

- Forest root domain - Schema Master and Domain Naming Master on the same machine, which should also host the Global Catalog.
- Every domain - PDC Emulator and RID Master on the same machine, which should have beefy hardware to handle the load.
- Every domain - Never place the Infrastructure Master on a machine that hosts the Global Catalog, unless your forest has only one domain or unless every domain controller in your forest hosts the Global Catalog.