FSMO ROLES

SERVER 2012R2

When you promote the first domain controller in a forest, is granted five *Operations Master* or *Flexible Single Master Operations* (FSMO) roles, pronounced “fizz-moe”.

Two of the roles are forest wide and the rest of them are domain specific, meaning if you have multiple domains, every domain will get the tree domain specific roles.

The two forest wide roles never change and they are barley used in the environment as you’ll see later. So if you have a forest with two domains this will mean a total of eight FSMO roles; Two forest wide and six domain wide; three for every domain.

Schema Master – controls updates and modifications to the schema. Once the schema is modified or updated, it will replicate to all domain controllers in the forest. As the best example of schema modification is Exchange, if you are familiar with the product. Before you install Exchange you need to extend the schema, and once is extended new tabs will appear on every user account, besides other things. There can be only one schema master in the whole forest. This role is necessary only when schema modifications are being made, meaning it can remain offline indefinitely until schema changes are necessary.

Domain Naming Master – controls the addition and removal of domains in the forest. There can be only one domain naming master in the whole forest. This role is only necessary when you add or remove a domain in the forest. The rest of the times the domain naming master role can remain offline for an indefinite period of time.

Infrastructure Master – when multiple domain exists in your forest, this role takes care of objects that reference objects in other domains. For example you can have a group in one domain that includes users from another domain. If members of that group are moved or renamed, the Infrastructure Master's job is to identify those changes and update the group membership.

The Infrastructure Master role needs to run on a domain controller that is not a Global Catalog (GC), or it will stop updating object information, since the Global Catalog server holds a partial replica of every object in the forest. Another way to eliminate this issue is to make all domain controllers a GC. There is an Infrastructure Master in every domain and is held by only one domain controller in that domain. If it fails users will not be affected, but it will be noticeable to administrators.

PDC Emulator – or Primary Domain Controller Emulator is a domain role that performs critical functions of a domain, like:

Password changes – when a user password is reset or changed, those changes are immediately replicated to the PDC emulator.

Backward compatibility – it gives a chance to those people who are still using Windows NT 4.0, to be able to locate a writable domain controller, since the domain controller that holds the PDC emulator registers itself as a PDC and performs all of the functionality that a Windows NT 4.0 Server performs for Windows NT 4.0 based clients.

Group Policy Objects – every time you open for editing a GPO, is alway done from the SYSVOL folder of a PDC emulator. This is to avoid situations where two administrators might edit the same GPO at the same time on different domain controllers. Without a PDC emulator the two GPO versions could not be reconciled.

Time synchronization – every PDC emulator in each domain synchronizes its time with the forest root PDC emulator so critical service like Active Directory, DFS-R, File Replication Service (FRS) function correctly.

Master Browser – acts as a domain master browser for the domain, and when clients browse the Windows Network, a list of computers, domain and servers will appear in that list.

There is a PDC emulator in every domain and is held by only one domain controller in that domain. If it fails, all normal operations and users will be immediately impacted. This role must be available at all times.

RID Master – or Relative ID (RID) Master is responsible for processing RID pool requests from domain controllers for security principals like users, groups and computers. The RID Master allocates a pool of RIDs to domain controllers, then those domain controllers generate SIDs by assigning a unique RID to the domain SID. The SID of every security principal must be unique. There is a RID Master in every domain and is held by only one domain controller in that domain. In case the RID master is not available the impact is not immediately noticeable, but when the RID pool is exhausted you will not be able to create objects in AD anymore.

These roles can all sit o a single domain controller (in small environments you will find this very often), or they can be spread out to multiple domain controllers. Now, as the title says, FSMO roles can be transferred or seized.