
## Windows Server

**Quilez's Blog**

# Roles Maestros en el Directorio Activo

**En el Directorio Activo, todos los controladores de dominio son iguales (al menos lo eran hasta Server 2008), a diferencia de NT4 en que un servidor era el principal (PDC) y el resto eran copias de sólo lectura de la base de datos del dominio (los BDC).**
**Sin embargo, hay una serie de roles que sólo pueden ser ejercidos por un único DC, al tratarse de funciones que requieren ser únicas en el bosque o dominio. Por así decirlo, el DC que ostenta en un momento dado un rol maestro realiza funciones de moderador o director de esa función. Un rol maestro puede transferirse de un DC a otro, incluso forzarse el cambio caso de desastre del DC que lo ostenta, pero en ningún momento puede haber más de un DC con el mismo rol. A estos roles se les conoce como FSMO (Flexible Single Master Operations).**
**Los tipos de roles maestros de operaciones son cinco, dos a nivel bosque y tres en cada dominio del mismo.**

**1) Bosque: A este nivel, y localizados siempre en algún DC del dominio ra´´iz del bosque (el primero que montas cuando lo creas) hay dos, el maestro de esquema y el maestro de nombres de dominio.**

**- Maestro de Esquema: es el DC que dirige todas las operaciones de cambio en el esquema del AD (la definición de clases de objeto, con sus atributos). Cuando se hace una modificación al esquema, siempre se realiza sobre el maestro de esquema (aunque la consola la lancemos desde otro DC), y a continuación se replica a todos los DCs del bosque. Esto permite asegurar que el esquema sea único para todo el AD.**

**- Maestro de Nombres de Dominio: El DC que ostenta este rol es el que controla que los nombres propuestos para nuevos dominios en el bosque no estén en uso, y además que la topología de nombres sea la correcta (por ejemplo, si tenemos un árbol con un dominio de nombre "españa.es", no podremos crear otro árbol de nombre "sevilla.españa.es", sino que tendrá que ser un subdominio del anterior.**

**2) Dominio: En cada dominio del bosque hay tres roles maestros, que pueden ser ejercidos por el mismo o por distintos DCs del dominio. Son los siguientes:**

**- Emulador de PDC: Entre otras, realiza todas aquellas tareas que los equipos anteriores a Windows 2000 esperaban que se realizasen en un PDC de NT4. Entre otras cosas, cuando un DC recibe una modificación de la contraseña de un usuario, al primero que se lo replica es al PDC, quien además ejerce de árbitro cuando se produce una autenticación incorrecta de la contraseña de un usuario (antes de generar el mensaje de error, el DC en que se valida la contraseña errónea le pregunta al PDC por si éste ya hubiera recibido un cambio de la contraseña).**
**Por otro lado, el PDC de un dominio es la cabeza jerárquica en el mismo para la sincronización de tiempo (los clientes sincronizan con el DC con que se validan, y éstos con el PDC de su dominio). A su vez, el PDC del dominio raíz del bosque es la cabeza jerárquica de sincronización de tiempo para todos los PDCs de los dominios del bosque. Normalmente, éste PDC y no otro es el que configuraremos para sincronizar con una fuente externa de tiempo fiable (si es que lo necesitamos).**
**También, cuando editamos una GPO desde cualquier equipo, por defecto se hace contra la copia**

**almacenada en el PDC del dominio y se guardan los cambios en el mismo, tras lo cual se replican al resto de DCs.**

**- RID Master (Relative Identifier Master): Como he comentado antes, al ser todos iguales, en cualquier DC del dominio se pueden crear objetos del AD. Al crear un objeto de tipo usuario, grupo o equipo se le asigna un identificador único de seguridad en el dominio (SID). Este identificador consta de una parte única para todo el dominio y de otra variable dentro del mismo, que le asigna el DC en que se crea el objeto. Para evitar que dos DCs distintos generen el mismo SID para un objeto, el DC que hace de RID master asigna al resto de DCs del dominio un número de IDs (un RID Pool), de tal forma que son distintos en cada DC. Cuando a un DC se le está acabando el número de IDs disponibles, solicita al RID Master que le asigne un nuevo pool de RIDs. Si el RID Master cayese y no forzásemos que otro DC pasase a llevar este rol, llegaría un momento en que no se podrían crear más objetos en el dominio por falta de IDs.**

**- Maestro de Infraestructura: Es el DC responsable de actualizar en otros dominios de su mismo bosque aquellos objetos del dominio propio que son referenciados por objetos de otros dominios. Por poner un ejemplo claro que lo explique, podemos tener un grupo de usuarios en un dominio, al que pertenecen cuentas de usuario de otros dominios. Si en un momendo dado cambiamos el nombre al grupo, el Maestro de Infraestructura es el encargado de notificar a los de otros dominios de este cambio. En un dominio, el Maestro de Infraestructura no puede ser al mismo tiempo Catálogo Global, salvo en el caso de un bosque de dominio único, debido al modo como ese DC consulta a los de otros dominios sobre los cambios de este tipo.**

**Los cambios de servidor para cada rol maestro se pueden hacer de dos formas: con las distintas herramientas gráficas de administración del AD (Usuarios y Equipos de AD, Sitios y Servicios de AD, Dominios y Confianzas de AD y cargando en una consola mmc el complemento de esquema), o bien con la herramienta de linea de comandos "ntdsutil". Para que te aparezca esta última tienes que instalar las support tools del CD del servidor. Además, con las herramientas gráficas se puede cambiar un rol de servidor siempre que tanto el de origen como el de destino estén en linea. Si el original hubiese caído, el forzamiento del cambio (seize) sólo se puede hacer con ntdsutil, siguiendo los pasos que describe el siguiente artículo: http://support.microsoft.com/kb/255504**

**Por fin, hay otro rol que no se define como tal como Maestro de Operaciones, que es el de Catálogo Global. En cada dominio tiene que haber al menos uno (el primero que promocionamos al crear un dominio lo será automáticamente, pero al resto se lo tendremos que especificar expresamente en las propiedades del DC en Sitios y Servicios de AD). Un Catálogo Global es un DC del dominio que además de tener toda la información de los atributos de todos los objetos de su propio dominio, tiene un subconjunto de los atributos de todos los objetos de todos los dominios del bosque. La réplica de estos datos se realiza de forma independiente entre los Catálogos Globales. Por defecto, el AD tiene marcado en su esquema cuales son los atributos de cada clase de objeto que se tienen que replicar entre Catálogos Globales, pero esto lo podemos modificar si fuera necesario editando las propiedades de cada atributo en el maestro de esquema del bosque.**
**Existen unas reglas para determinar cuantos DCs deben ser Catálogos Globales. En un bosque de dominio único, todos los DCs se pueden configurar como GCs, incluso el Maestro de Infraestructura, ya que éste no tiene realmente nada que hacer como tal. En un bosque de múltiples dominios, en cada Sitio de AD (definido en Sitios y Servicios de AD) tendremos que configurar como GCs la mitad de los DCs de cada dominio en ese Sitio. Además, en este caso el Maestro de Infraestructura de cada dominio no debe ser Catálogo Global, salvo que un dominio no tuviese más que un único DC.**

**Posted: Jul 01 2007, 07:16 PM by José Antonio Quílez | with no comments**


**Theme based on the Paperclip Blog Theme included in Community Server.**
**Enhanced to a Site-Wide Theme by Interscape Technologies.**