### MAESTROS DE OPERACIONES.

En el antiguo Windows NT los controladores de dominio se dividían en controladores principales (uno por dominio) y controladores secundarios. Desde Windows 2000 esto ya no es así, todos los controladores de dominio trabajan al mismo nivel.

Sin embargo, hay controladores de dominio que realizan una serie de operaciones especiales y por lo tanto son más importantes que el resto, estos son **los maestros de operaciones**.

FSMO 🡪 Flexible Singel Master Operatións --- FSMO roles

Las funciones de maestro de operaciones permiten llevar a cabo tareas que no resultaría práctico realizar con varios maestros.

**Las funciones de maestro de operaciones son funciones específicas en las que se organizan las operaciones que utilizan la replicación de maestro único.**

La replicación de maestro único designa un controlador de dominio como el único controlador de dominio en el que pueden realizarse ciertos cambios en el directorio activo. Esto se hace para evitar conflictos de replicación que pueden presentarse si dos controladores de dominio realizan actualizaciones al mismo tiempo en el mismo atributo de objeto (dos controladores que cambian el nombre de un usuario al mismo tiempo, por ejemplo).

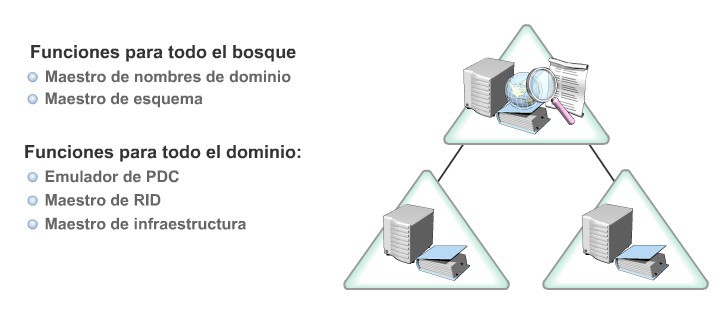
**Active Directory utiliza la replicación de maestro único para cambios importantes, como la adición de un nuevo dominio o un cambio en el esquema de todo el bosque.**

El controlador de dominio que es responsable de una función particular se llama maestro de operaciones de esa función. Active Directory almacena la información acerca del controlador de dominio que tiene una función específica. Active Directory define cinco funciones de maestro de operaciones, con una ubicación predeterminada para cada una.

**Tenemos 2 funciones de maestro de operaciones que abarcan todo el bosque Y 3 funciones que abarcan todo el dominio.**

Imagen que contiene Tabla

Descripción generada automáticamente

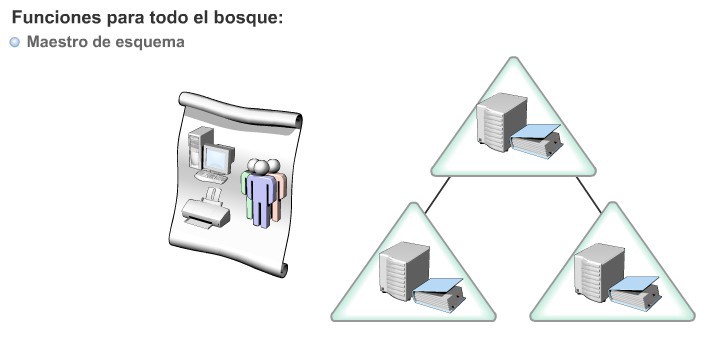


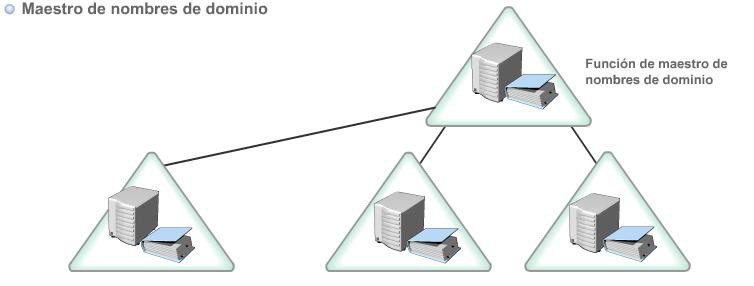
**Las funciones que abarcan todo el bosque:**

**Maestro de esquema** que controla todas las actualizaciones y los cambios del esquema. El esquema contiene una lista general de clases de objetos y atributos que se utilizan para crear todos los objetos de Active Directory como, por ejemplo, usuarios, equipos e impresoras. Para determinar qué servidor es el maestro de esquema actual del dominio escriba **dsquery server –hasfsmo schema** en el símbolo del sistema.

**Maestro de nombres de dominio**, controla la adición o eliminación de dominios en el bosque. Sólo el controlador de dominio que tiene la función de maestro de nombres de dominio puede agregar un nuevo dominio por lo tanto para agregar o eliminar dominios debe tener acceso al maestro de nombres de dominio. Para determinar qué servidor es el maestro de nombres de dominio actual escriba **dsquery server –hasfsmo name** en el símbolo del sistema.

**Las funciones que afectan a todo el bosque deben ser únicas en el bosque. Es decir en un mismo bosque sólo puede haber un maestro de esquema y un maestro de nombres de dominio**





**Las siguientes funciones deben estar disponibles en todos los dominios Active Directory.**

Las funciones que abarcan todo el dominio son el **emulador del controlador principal de dominio (PDC**), el **maestro de identificadores relativos (RID**) y el **maestro de infraestructura**. Cada dominio de un bosque tiene su propio emulador de PDC, maestro de RID y maestro de infraestructura.

**El emulador de PDC**, el primer controlador de dominio que se crea en un nuevo dominio tiene esta función. Encargado de procesar las solicitudes de replicación de Controladores de dominio. Encargado de procesar todas las actualizaciones de contraseñas de clientes. Necesario para la sincronización de la hora.

Para determinar qué servidor es el maestro emulador de PDC actual del dominio escriba **dsquery server –hasfsmo pdc** en el símbolo del sistema.

**El maestro de RID** asigna bloques de identificadores relativos a cada controlador de dominio en el dominio. Los controladores de dominio asignan un identificador de seguridad único a cada objeto de usuario, grupo o equipo que se cree. Este identificador utiliza como prefijo el identificador de seguridad del dominio y como sufijo, un identificador relativo único asignado por el **maestro RID.**

Que es RID (Relative Identifier). Las cuentas de usuario, las de grupo, y las de equipo, cuando son creadas en un dominio, se les asigna un SID (Security ID). Lo podemos considerar en forma análoga a un documento personal. Es un identificador único y que nunca es reutilizado, aunque la cuenta original fuera eliminada.

Este SID, tiene tres partes principales. La primera parte (S-1-5-21-..) es un identificador de seguridad asignado a Microsoft, para uso en dominios, etc.  
La segunda parte es el identificador del Dominio, todas las cuentas de usuario, grupo y equipo de un dominio comparten estos datos.  
La tercera y última (los números que siguen al último “-“ corresponden al RID, que es asignado en forma secuencial a partir del número 1000 a cada cuenta que se crea en el Dominio.

Una cuenta puede crearse en cualquier Controlador de Dominio ya que cualquiera de ellos puede escribir en la base de Active Directory, pero sin embargo debemos asegurarnos de que no se repitan los SIDs asignados a cada cuenta.

La solución pasa por tener un Controlador de Dominio que es el “dueño” de todos los RIDs, y que ha pedido le asigna a cada Controlador de Dominio del Dominio rangos de RIDs. Cuando en un Controlador de Dominio este rango asignado comienza a agotarse (asigna de a 500, y cuando quedan sólo 50 disponibles) los Controladores de Dominio solicitarán al RID Master, otro rango de RIDs.

Para determinar qué servidor es el actual Maestro RID relatico del dominio escriba **dsquery server –hasfsmo rid** en el símbolo del sistema.

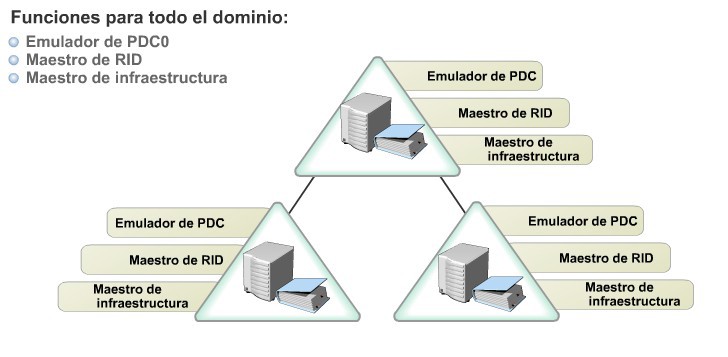
**El maestro de infraestructura**

Cuando se mueven objetos de un dominio a otro, el maestro de infraestructura actualiza las referencias a objetos en su dominio que apuntan al objeto en el otro dominio. La referencia al objeto contiene el identificador único global (GUID) y un identificador de seguridad (SID). Active Directory actualiza periódicamente el nombre completo y el SID en la referencia al objeto para que se reflejen los cambios realizados en el objeto propiamente dicho, como los movimientos dentro de los dominios y entre éstos y la eliminación del objeto.

Supongamos que nuestro Active Directory consistiera en tener varios Dominios. En un ambiente como este se puede dar el caso que un usuario de un Dominio-A, esté “dentro” de un grupo de otro Dominio-B.

Por las capacidades propias de Active Directory y necesidad podríamos tener que mover la cuenta del usuario (que está en Dominio-A) a otro Dominio-C  
En este caso, en los grupos del Dominio-B se deberían actualizar todas las referencias a la cuenta de usuario; antes era “usuario de Dominio-A”, ahora debe ser “usuario de Dominio-C”.  
Esta es justamente la función del Maestro de Infraestructura.

Para determinar qué servidor es el actual Maestro de infraestructura actual del dominio escriba **dsquery server –hasfsmo infr** en el símbolo del sistema.



Estas funciones que afectan a todos los dominios deber ser únicas en cada uno de ellos. Es decir, solo se asigna un Maestro ID relativo, un Maestro emulador de PDC y un maestro de infraestructuras en un dominio en particular.

Para ver todas las funciones en conjunto:

Netdom query fsmo

Netdom query /domain:valle.local fsmo

Las funciones del **MAESTRO DE OPERACIONES** se suelen asignar automáticamente, **pero si es posible** cambiar dicha asignación a posterior. Al instalar una nueva red se asignarán todas las funciones del maestro de operaciones al primer controlador de dominio del primer dominio. Si posteriormente, crea un nuevo dominio hijo o un dominio raíz en un árbol nuevo, también se le asignaran automáticamente las funciones de maestro de operaciones al primer controlador de dominio del nuevo dominio.

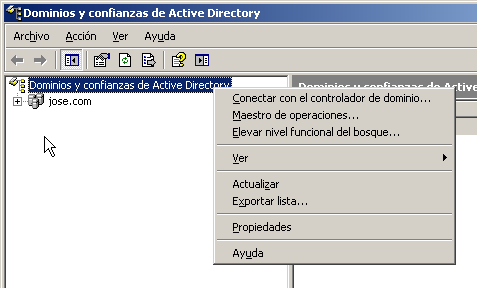
En un bosque de dominios nuevo, al controlador de dominio se le asignan todas las funciones de maestro de operaciones. Si el nuevo dominio está en el mismo bosque, las funciones que se asignan son las de maestro RID relativo, maestro de emulador de PDC y maestro de infraestructuras. Las funciones de maestro de esquema y de nombres de dominio permanecen en el primer dominio del bosque.Si un dominio tiene un único controlador de dominios ése será el encargado de todas las funciones de maestro de operaciones.

Si un dominio dispone de dos o más controladores de dominio, debería configurar dos controladores de ellos para que se encarguen de las funciones de maestro de operaciones. En este caso uno de los controladores de dominio será el maestro de operaciones y otro el maestro de operaciones secundario, utilizado en caso de que el principal no funciones. Asegúrese de que los controladores de dominio sean socios de réplica y estén conectados correctamente.

Las funciones de maestro de esquema y maestro de nombres de dominio no deberían estar separadas. Asigne siempre estas dos funciones al mismo servidor.

### CAMBIAR EL MAESTRO DE OPERACIONES PARA NOMBRES DE DOMINIO.

Windows Server irá asignando estas funciones de maestros de operaciones a los primeros controladores de dominio creados. Si queremos modificar estas asignaciones podemos hacerlo desde la consola MMC de Dominios y Confianzas de Active Directory. Para ello pulsamos con botón derecho sobre Dominios y confianzas de Active Directory y escogemos la opción Maestro de Operaciones, que nos permitirá cambiar el CD que realiza la función de maestro de nombres de dominio.

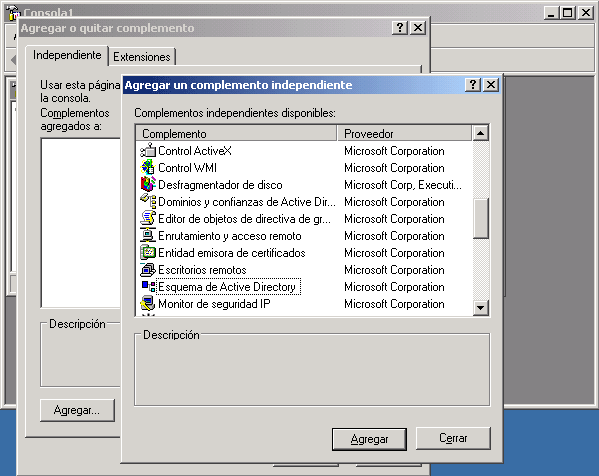


La función de maestro de nombres de dominio recordemos que es la encargada de añadir y eliminar dominios de nuestro árbol, por lo que es muy importante tener controlado que CD realiza esta función, ya que, si dicho CD está apagado, no se podrán añadir ni eliminar ramas a nuestro árbol, o arboles a nuestro bosque.

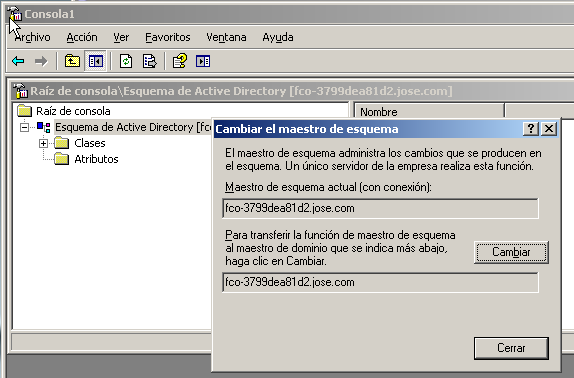
Para llevar a cabo este procedimiento, debemos ser miembros del grupo Administradores de dominio o del grupo Administradores de organización de Active Directory o Administradores de Empresa.

### CAMBIAR EL MAESTRO DE OPERACIONES PARA MAESTRO DE ESQUEMA.

Se realiza dicho cambio desde la MMC de Esquema de Active Directory. Recordamos que dicha MMC no se instala por defecto, ya explicamos anteriormente como instalarla, ejecutando en una terminal el comando regsvr32 schmmgmt.dll.Una vez hecho nos aparecerá un mensaje de éxito en pantalla, volveremos a Inicio -> Ejecutar y una vez allí ejecutaremos “mmc” lo que nos abrirá una consola vacía, navegamos a Archivo -> Agregar o quitar complemento.. y seleccionar Esquema de Active Directory.

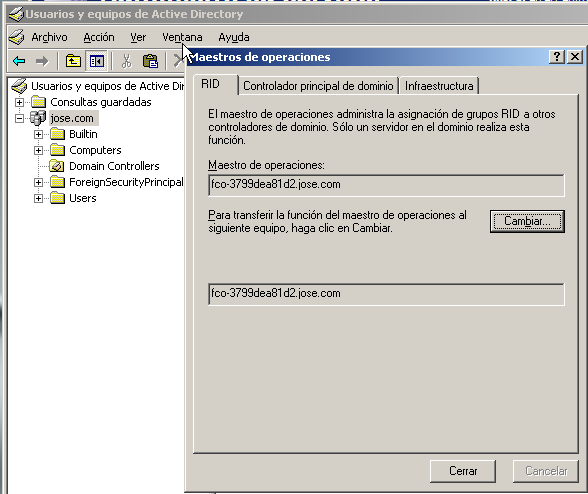
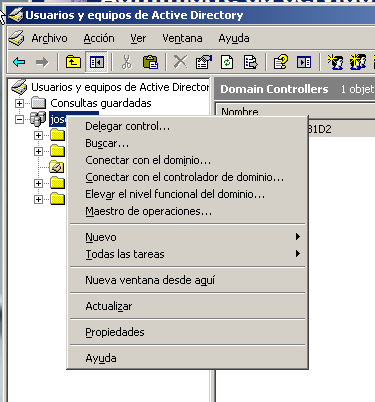


Una vez hecho esto, pulsamos botón derecho sobre Esquema de Active Directory y escogemos como siempre, la opción de cambiar el maestro de operaciones.



### CAMBIAR EL MAESTRO DE OPERACIONES PARA EMULADOR DE PDC, MAESTRO DE RID Y MAESTRO DE INFRAESTRUCTURA.

**Para cambiar estas funciones que trabajan a nivel de dominio**, tenemos que ejecutar la consola Usuarios y Equipos de Active Directory. Pulsamos con botón derecho sobre el nombre de nuestro dominio y escogemos la opción Maestro de operaciones.



Veremos cómo nos aparece un formulario que nos permita cambiar el maestro de RID, el Controlador principal de dominio que realiza las funciones de emulador de PDC y el maestro de infraestructura.