5

MIGRACIÓN A WINDOWS SERVER 2003: ARQUITECTURA TECNOLÓGICA PARA EL DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA

Luis García Marugan
Jefe de Área de Microinformática y Redes
Ministerio de Trabajo y Asuntos Sociales. Subdirección General de Proceso de Datos

1. INTRODUCCIÓN

La migración a Windows Server 2003 puede ser el camino a seguir en la elección de una arquitectura tecnológica para conseguir una base sólida en el desarrollo de la Administración Electrónica. Son varios los beneficios que se obtienen en la implantación de Windows Server 2003, que pueden ser interesantes para conseguir el objetivo indicado.

Algunos de los beneficios a obtener son: Una infraestructura segura, fácil de implementar, administrar y usar, fiabilidad, disponibilidad y escalabilidad, herramientas administrativas robustas, etc.

Dentro de la infraestructura segura, hay que destacar las funcionalidades más importantes que se van a obtener con vistas a la implementación de la Administración Electrónica. Estas son:

- Permite la administración de identidad en toda la red, garantizando la seguridad en toda la organización y constituye la base de un posible sistema de "single sign on".
- Es fácil encriptar datos sensibles para proteger los archivos de intrusos y trabajar con ellos de forma transparente, facilitando el cumplimiento de los requerimientos de la LOPD.
- Las políticas de control y automatización de actualizaciones de software pueden ser usadas para prevenir daños causados por virus.
- De igual modo, interviene en la prevención de virus aplicando políticas de actualización automática del sistema operativo, mediante la aplicación de "parches".
- Se pueden usar las Políticas de Grupo para definir las configuraciones y acciones permitidas para los usuarios y los ordenadores.
- Permite una forma ágil de disponer de copias de seguridad de volúmenes críticos de datos sin interrumpir el servicio así como la recuperación de versiones de archivos de documentos almacenados de forma transparente.

2. OBJETIVO

El objetivo de este documento es presentar una guía de la planificación y el despliegue de Windows Server 2003 y Directorio Activo realizados sobre la infraestructura actual del MTAS y proporcionando los niveles de calidad requeridos por cada una de los servicios a prestar.

3. ANTECEDENTES O ANÁLISIS DE LA SITUACIÓN DE INICIO

El diseño e implantación de una infraestructura basada en la plataforma Windows Server 2003 con los máximos niveles de calidad, requiere de una etapa de recogida de información que permita evaluar correctamente la situación inicial de la organización. Esta información ayuda además durante las siguientes etapas del proyecto, como son el análisis y el diseño, como mapa de la infraestructura de la red, en nuestro caso la preexistente, en el Ministerio de Trabajo y Asuntos Sociales.

Previo al diseño de la nueva solución se recogió la información necesaria para la correcta valoración de las diferentes alternativas a tener en cuenta durante la planificación. Entre otros datos, se hace un resumen de lo que se recoge en dicho documento.

3.1 Modelo de dominios NT

Los servicios centrales del MTAS, ámbito inicial del proyecto, disponía en esos momentos de 10 edificios cada una de ellos con un dominio Windows NT conformado por un solo PDC y, en algunos casos un BC que, además, realizaba otros servicios adicionales, principalmente servidor de ficheros e impresoras. En el dominio de la Sede Central, además del PDC, existían cuatro BDCs.

El soporte y administración de estos dominios se hacía ya de forma centralizada a través de la herramienta de control remoto "Remote Connect" de Microsoft SMS 2.0 y de las herramientas de administración de Windows NT.

De cada dominio se recogieron los siguientes datos: dirección del edificio, rango de la subred, nombre del PDC, nombre de los BDC's, las direcciones IP de los PDC's y BDC's y el número de usuarios de cada dominio. Éstos resultaron ser 946, 300, 219, 200, 200, 178, 54, 50, 39 y 30 usuarios respectivamente para cada uno de los edificios.

3.2 Topología de red

El MTAS tiene instalada una red de comunicaciones Multi-Servicio de Banda Ancha que utiliza como protocolo de transporte SDH (Synchronous Digital Hierarchy) sobre enlaces de fibra óptica de tipo mono-modo.

Todos los edificios-nodo u oficinas se interconectan con la Sede Central a través de enlaces de 2 Mbps y de 34 Mbps generados y controlados por la red SDH como anteriormente se ha comentado. Cada oficina cuenta con dos líneas de conexión con la Sede Central soportadas en dos equipos diferentes con objeto de conseguir un entorno redundante.

Se hizo un estudio del tráfico medio y de pico de la red en los dos sentidos, de la sede central a cada uno de los edificios-nodo y desde éstos a la Sede Central. En los resultados obtenidos se apreciaba que los tráficos medios en cada uno de los edificios estaban soportados sobre enlaces suficientemente holgados como para deducir que las líneas actuales soportarían el tráfico sin ningún problema, sea cual fuere la organización elegida.

Las Inspecciones Provinciales se encontraban conectadas vía Frame-Relay a 64 Mb y las Consejerías Laborales carecían de comunicaciones estables.

3.3 Direccionamiento

El MTAS utiliza como rango de IPs para uso interno el X.Y.0.0/16 (Clase B), conforme al Plan de Direccionamiento de la Administración General del Estado. Lógicamente, y como ya se mencionó anteriormente, en el análisis se recogían los rangos de cada subred así como los números IP asignados en ese momento a los servidores.

3.4 Resolución de Nombres

La resolución DNS externa la realizaba un servidor con Windows NT 4.0 que, además, se usaba como servidor web. La resolución de nombres por DNS de forma interna la efectuaba un servidor con Windows NT 4.0, que no cumplía ninguna otra función, y no había DNS secundario interno. El nombre de dominio interno o zona DNS que alojaba este servidor era "mtas.es", igual que el que alojaba el DNS externo.

3.5 WINS y NetBIOS

El PDC del dominio de los servicios centrales era, además, el servidor WINS para la resolución de nombres interna y no había WINS secundario.

3.6 Topología de SMS

En el MTAS se utiliza SMS 2.0 para la gestión de los sistemas y los puestos de trabajo.

Existe un "SMS site" para la Sede Central, y uno para cada oficina remota de Madrid, y cada Inspección provincial, distribuidos en cerca de 60 sites. En este estudio se recogían los servicios que llevaban instalados cada uno de los servidores de la sede central y los de los edificios nodo.

4. DISEÑO DE DIRECTORIO ACTIVO

Este capítulo analiza y evalúa las soluciones óptimas a tomar para el despliegue de Windows Server 2003 y el Directorio Activo dentro de la organización.

4.1. Oficinas Remotas

Las decisiones a tomar en el despliegue de Windows 2003 en el MTAS tuvieron especialmente en cuenta los siguientes parámetros:

- Una cantidad de oficinas remotas con controladores de dominio y dominios independientes.
- Un reducido número de usuarios en cada oficina.
- Un número medio de controladores de dominio.
- Una topología de estrella (hub and spoke) en la red.
- Conexiones rápidas entre la sede central y el resto los otros edificios de Madrid.
- Conexiones lentas entre la sede central y sedes provinciales e internacionales.
- Modelo de administración centralizado.

4.1.1 Cantidad de oficinas remotas con DC

En un despliegue con oficinas remotas no es siempre necesaria la existencia de controladores de dominio en cada una de las delegaciones. Esto es así siempre que las redes de comunicaciones sean de alta disponibilidad y de un ancho de banda suficiente para proporcionar comunicación durante el proceso de logon de los usuarios.

Sin embargo, al disponer ya el MTAS de PDCs en cada oficina remota, y al requerir que los servicios de archivos e impresión estén localizados en los servidores remotos, **se hizo clara la elección de un modelo distribuido de DCs.**

4.1.2 Número medio de controladores de dominio

El MTAS no dispone de más de 100 controladores de dominio ni de más de 100 puntos en los que implementar Windows Server 2003, lo cual sitúa la valoración del tamaño de la implantación en una implantación de tipo "medio".

4.1.3 Topología de HUB en la red

El MTAS dispone de una red en estrella simple (*hub and spoke*) que le une con todas las oficinas remotas de Madrid, tal y como se puede ver en el capítulo "Antecedentes o Análisis de la Situación Inicial".

4.1.4 Conexiones con oficinas remotas

Las conexiones entre los edificios-nodo de Madrid y la sede central son lo suficientemente rápidas como para que el tráfico de logon, replicación y acceso a aplicaciones y servicios no tenga impacto sobre la utilización de la red.

Sin embargo, las conexiones entre las Inspecciones Provinciales de Trabajo y las Consejerías de Trabajo y la Central son de menor ancho de banda, por lo que requerirán un tratamiento diferente.

4.1.5 Modelo de administración en oficinas remotas

Básicamente hay dos modelos de administración a tener en cuenta en la administración de oficinas remotas: el centralizado y el descentralizado.

De acuerdo con el modelo centralizado todos los cambios serán hechos desde la sede central y serán replicados al resto de oficinas. En el modo de administración descentralizado las oficinas remotas podrán realizar la administración de sus OU's delegadas, que después serán replicadas a la sede central y al resto de las oficinas.

En la realización de ciertas labores administrativas (relacionadas con usuarios, grupos y políticas de grupo) se deberá observar un especial cuidado pues éstas pueden provocar grandes tráficos de replicación.

Cada uno de los dos modelos de administración tiene pros y contras respecto a la administración de usuarios y grupos.

En general, éste no será el caso del MTAS por el alto ancho de banda y disponibilidad de la red.

En el MTAS se ha optado por un modelo de administración centralizada.

4.2. Planteamiento estructural

4.2.1 Introducción

En este capítulo se razonan las decisiones a tomar en cuanto al aspecto de la distribución lógica del directorio activo, incluido el particionado del "forest" y de los dominios, los Global Catalog, los roles FSMO, DNS y Bridgeheads.

El planteamiento estructural por lo tanto tiene dos objetivos: definir el particionado del forest y de los dominios.

4.2.2 Particionado del Forest

Existen dos razones para que una organización tenga más de un Forest:

- razones Políticas/Organizacionales/Legales (que requieran schemas diferentes divisiones de la organización, o que estas sean administradas de forma totalmente independiente)

- la existencia de demasiados objetos en el directorio (el límite esta determinado por la capacidad de disco y memoria de los DCs)

Ninguna de estas razones son aplicables al MTAS por lo cual **no es necesaria la existencia de mas de un Forest.**

4.2.3 Particionado del Dominio

Particionar la red en múltiples dominios reduce la cantidad de datos a replicar durante la replicación del "DomainNamingContext" pero incrementa la cantidad de datos en la replicación del Global Catalog. El tráfico de red para la generación y cambios de los objetos es menor cuando existen múltiples dominios.

Las otras consideraciones sobre sencillez de diseño (y por tanto de administración) y el hecho de que es más sencillo mover un usuario entre una OU y otra, en vez de entre dominios diferentes del forest, hace aconsejable el uso de **un solo dominio** para el MTAS, pudiéndose contemplar otro dominio en el momento de integrar las Inspecciones Provinciales de Trabajo y Seguridad Social.

4.2.4 Ubicación de Domain Controllers

Uno de los aspectos más importantes a decidir es la colocación de los controladores de dominio y de los catálogos globales, entre otras cosas por los efectos que esto supone en la replicación.

Los factores a tener en cuenta son: número de sitios, número de usuarios, replicación y disponibilidad de un proveedor de logon.

Cuando una oficina remota tiene un número muy reducido de usuarios y la línea es suficiente como para poder validar a través de la WAN, puede que el coste del hardware más la administración no justifiquen la colocación de un DC. **En el MTAS, aunque se produce este caso en algunas oficinas, se acordó poner un servidor de archivos e impresión y un Controlador de Dominio (DC) en cada oficina.**

4.2.5 Tráfico de replicación

Cada uno de los DC necesita replicar su "Domain Naming Context", el "Schema Context" y el "Configuration Context" para poder funcionar correctamente, un cambio en cualquiera de estos contextos afecta de forma diferente a la replicación que fluye por la red.

4.2.6 Disponibilidad de un proveedor de logon

Tanto las aplicaciones como los usuarios requieren de un servidor DC que les permita hacer logon. Si queremos que se pueda hacer logon con las líneas no disponibles tendremos que colocar un servidor en cada edificio.

Si un puesto no pudiera encontrar un servidor en el que validar al usuario, este usuario podría validar en el puesto a través de las "cached credentials" pero no podría acceder a shares o aplicaciones en el servidor.

4.2.7 Ubicación de Global Catalogs

Un Global Catalog es un DC que almacena una réplica completa de una partición de directorio de dominio y una réplica parcial de todas las demás particiones de directorio de dominio

del "forest". La réplica es parcial porque sólo incluye los atributos más necesarios para realizar búsquedas, haciendo así posible la búsqueda de objetos del directorio en todos los dominios del forest.

Se consideró que cada site que contuviese un DC sería además Global Catalog.

4.2.8 Unidades Organizativas

En general es buena práctica, cuando se migra desde un entorno de dominios de Windows NT a un entorno de Active Directory de Windows Server 2003, crear Unidades Organizativas (OUs) que representen los dominios de Windows NT originales.

Además, dentro de cada OU inicial, que en el caso del MTAS se corresponderá con una localización física, se pueden crear OUs "hijas" para organizar los equipos, servidores y usuarios de cada site.

Alternativamente se puede organizar de tal forma que haya tres OUs de primer nivel (Equipos, Usuarios y Servidores), y dentro de cada una de ellas, OUs para representar a cada uno de los sites.

El modelo a elegir dependerá de las acciones de administración que se lleven a cabo más habitualmente con los usuarios y equipos.

- En el caso de que habitualmente se apliquen directivas de grupo a equipos, usuarios y servidores, de forma específica según su localización, entonces es más conveniente el primer modelo.
- En el caso de que habitualmente se apliquen directivas de grupo a equipos, usuarios o servidores, independientemente donde estén, entonces es más conveniente el segundo modelo.

Las directivas de grupo (GPO) se pueden asociar a una OU, un dominio o un site, ya que en el caso del MTAS, cada site de Directorio Activo se corresponde con una sede a representar por una OU, y las configuraciones de seguridad son iguales independientemente de la localización.

En cualquier caso, al contrario que la definición de forests y dominios, la estructura de OUs es muy flexible, pudiendo modificarse y reorganizarse en el futuro sin ningún problema.

4.2.9 Consideraciones de DNS

La disponibilidad de un servidor DNS es clave en el proceso de encontrar servidores DC y los DC confían en el DNS para encontrar otros DC.

El MTAS ha implantado un servidor DNS en cada site y las zonas serán de tipo "AD Integrated". Todos los puestos han de ser configurados con al menos un servidor principal en su mismo sitio y uno de reserva (en la sede central).

4.2.10 Número de sites

Los factores que hay que tener en cuenta para la definición del número de sites son: Número de localizaciones independientes, Conectividad y Existencia o no de un DC en cada localización.

La estructura definida en el MTAS ha derivado en la creación de los siguientes sites:

- Site central
- Un site por cada oficina que tenga un DC (en principio todas)

4.2.11 Modelo de dominios propuesto

El modelo de dominios implementado se basa en las siguientes premisas:

- Un solo forest
- Un solo dominio
- Un site central y un site por cada oficina remota
- Una estructura de OUs jerárquica

4.3. Replicación

La replicación de Windows 2003 a nivel de dominio y de forest tiene principalmente dos elementos:

- Replicación del directorio
- Replicación del SYSVOL usando FRS

Los dos tipos de replicación usan la misma topología. La replicación del AD empieza de forma aleatoria dentro de los primeros 15 minutos de la ventana de replicación para distribuir la concurrencia en el uso de la ventana de replicación. La replicación FRS empieza en cuanto la ventana de replicación es abierta, por lo tanto la replicación del AD con los partners no es simultánea mientras la de FRS si lo es.

Los componentes de la topología de replicación comprenden la KCC, los objetos "Connection", los "Site Links" y los "Site Link Bridges".

El MTAS tiene una topología lógica en estrella simple lo cual hace que solo se pueda llegar a cada oficina remota a partir de la central.

4.3.1 Cálculo de número de DCs

El número mínimo de DC's para soportar la replicación se calcula en función de tablas teniendo en cuenta el número de usuarios en el site y las características de las CPU's. Además, para soportar la replicación con los sites remotos, el site central deberá tener DC's extras en función del número de partners de replicación.

4.3.1.1 DCs en oficina central

En la sede central se han instalado 2 DC's iniciales de acuerdo con el número de usuarios.

Durante la fase de integración de los dominios de los edificios nodo de Madrid este número de DCs será suficiente para soportar el tráfico de replicación.

Una vez se integren las Inspecciones Provinciales de Trabajo y las Consejerías de Trabajo, al añadir más partners de replicación, hará necesario añadir 3 o 4 DC's más como bridgeheads para soportar la replicación. El número definitivo dependerá del calendario y ventanas de replicación definidas para los enlaces con sites.

4.3.1.2 DCs en oficinas hasta 100 usuarios

En las oficinas de hasta 100 usuarios conviene tener un servidor que haga las funciones de:

- SERVIDOR
  - Domain Controller (DC) con rol de Global Catalog (GC)
  - Archivos e Impresión
  - DNS, WINS

4.3.1.3 DCs en oficinas de más de 100 usuarios

En las oficinas de más de 100 usuarios se debe evaluar la posibilidad de tener al menos dos servidores que hagan las siguientes funciones:

- SERVIDOR1
  - Domain Controller (DC) con rol de Global Catalog (GC)
  - DNS, WINS
- SERVIDOR2
  - Domain Controller (DC)
  - Archivos e Impresión

4.4. Planteamiento para la Sede Central

En las oficinas centrales serán necesarios inicialmente 5 servidores:

- DC principal (DNS, Infrastructure Master, Domain Naming Master, Schema Master)
- DC principal (DNS, Global Catalog, PDC Emulator, RID Master)
- 3 DCs adicionales cuando se integren las Inspecciones Provinciales de Trabajo

5. GRUPOS DE SEGURIDAD

Los grupos de seguridad simplifican las tareas para asignar permisos sobre recursos de red (impresoras, carpetas compartidas, aplicaciones, etc.) a los usuarios del sistema.

En Windows Server 2003 se permite la creación de 3 tipos diferentes de grupos de seguridad de usuarios: Locales de dominio, Globales y Universales.

5.1. Estrategia de acceso a recursos

En el MTAS sólo hay un dominio, por lo que la utilidad de los grupos universales no es mayor que la de usar grupos globales y locales de dominio.

Usando Grupos Globales y Grupos Locales de Dominio, una estrategia recomendada para administrar y gestionar el acceso a recursos es la siguiente:

- Los usuarios pertenecen a un Grupo Global
- Los permisos en recursos (carpetas compartidas, impresoras, etc.) se asignan a Grupos Locales de Dominio
- Se añade el Grupo Global correspondiente como miembro del Grupo Local de Dominio

En resumen, los Grupos Globales se definen de manera que agrupen usuarios con un mismo cometido y requisitos de acceso similares. Los Grupos Locales de Dominio se definen por cada recurso a proteger.

5.2. Planteamiento inicial de grupos

5.2.1 Grupos Globales

Inicialmente es conveniente crear al menos:

- Un Grupo Global por cada OU de usuarios. Estos tendrán permisos de acceso a las carpetas compartidas y a las impresoras de red correspondientes de su site.

- Un Grupo Global de Administradores
  Personal con rol de administrador de sistema o red que no necesite ser administrador de Directorio Activo.
- Los grupos preexistentes de "Administradores de Dominio", etc. Idealmente con pocos usuarios en estos grupos.

5.2.2 Grupos Locales de Dominio

Inicialmente, se sugiere la creación de:

- Un Grupo Local de Dominio por cada conjunto de carpetas compartidas a las que tengan que acceder usuarios de ese site o OU.
- Un Grupo Local de Dominio por cada grupo de impresoras de cada site (en la Sede Central se pueden definir varios grupos si hay muchas)
- Un Grupo Local de Dominio por cada aplicación que se deba acceder por red
- Un Grupo Local de Dominio por cada grupo de usuarios de dominios externos con los que se tiene relaciones de confianza (Injuve, IMSERSO, Instituto de la Mujer, Seguridad Social, etc.) que necesiten acceso a recursos del dominio "trabajo.dom" (carpetas, impresoras, aplicaciones web, etc.)

6. MIGRACIÓN DE USUARIOS Y RECURSOS

Existen dos formas principales de realizar la migración desde un modelo de dominios NT a Directorio Activo: Actualización del dominio y Reestructuración del dominio.

En el MTAS se ha abordado el proceso como una reestructuración, lo que ha permitido crear una infraestructura paralela, con objeto de realizar una migración progresiva, con posibilidad de "roll back" en caso de problemas. Una vez terminado el proceso y migrados todos los usuarios de cada dominio, se fueron eliminando los dominios NT originales.

6.1. Active Directory Migration Tool

La ADMT v2.0 (Active Directory Migration Tool) es una herramienta de Microsoft que permite realizar migraciones de dominios NT a Windows 2000/2003 de forma sencilla, así como reestructurar dominios Windows 2000/2003. Permite migrar usuarios, grupos, máquinas, relaciones de confianza, etc. por medio de un conjunto de asistentes (wizards)

Los requisitos para migrar de NT a 2003 son que el PDC del dominio NT tenga Service Pack 4 o superior instalado. Además para soportar SIDHistory es necesario que el dominio destino (2003) esté en modo nativo.

ADMT v2.0 permite migrar contraseñas de usuarios utilizando un Password Export Server (PES) en el dominio origen NT.

Además el Agente ADMT, instalado por la herramienta automáticamente en las máquinas a migrar, corre en NT 4.0 (SP4 o superior), Windows 2000, Windows XP y Windows Server 2003.

Otros requisitos para realizar la migración son:

- Configurar el dominio de origen para que confíe en el dominio de destino.
- Configurar el dominio de destino para que confíe en el dominio de origen.

- Agregar el grupo global "Admins. del dominio" que está en el dominio de origen al grupo local "Administradores" del dominio de destino.
- Agregar el grupo global "Admins. del dominio" que está en el dominio de destino al grupo local "Administradores" del dominio de origen.
- Crear un nuevo grupo local en el dominio de origen denominado "Source Domain$$$" (sin ningún miembro)
- En el PDC del dominio de origen, agregar el valor TcpipClientSupport: REG_DWORD:0x1 a la siguiente clave del Registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
- Se debe usar ADMT desde una cuenta de usuario que:
  - Tenga permisos de Administrador de Dominio en el dominio destino
  - Sea miembro del grupo Administradores del dominio origen
  - Tenga permisos de administración en cada máquina que se vaya a migrar

6.2. SIDHistory

En Windows 2003 la reestructuración de dominios se hace más fácil gracias a un nuevo atributo de Directorio Activo llamado "sIDHistory" que se usa para almacenar los anteriores SID (identificador interno de un objeto de AD) cuando se mueve un objeto entre dominios.

De esta forma se pueden mover grupos, máquinas y usuarios entre dominios, manteniendo la identidad que les permita acceder a recursos no migrados.

Para que esto funcione el dominio de destino tiene que estar en modo nativo.

7. LABORATORIO DE PRUEBAS

Con objeto de asegurar la compatibilidad de las aplicaciones existentes en el MTAS, se estableció un laboratorio para realizar las pruebas previas a la implantación del Directorio Activo. De las pruebas realizadas solo se detectó problemas en el IPLANET WEB SERVER 6.2 SP2, cuya versión no estaba homologada para Windows 2003.