# Capítulo 1
# Introducción a Windows Server 2003

***¡Bienvenido a la nueva familia de Servidores Microsoft!***
***A lo largo de este curso iremos aprendiendo sobre las nuevas tecnologías 2003 y cómo aplicarlas.***

Las nuevas características de Windows Server 2003 hacen que sea, hasta el momento, el sistema operativo más estable, robusto, escalable y sobre todo mejor orientado a perfeccionar la performance y las prestaciones para Servidores en distintos roles: Aplicación, Servicios Web, Servicios de Directorio, Servicios File & Print y Servicios de Infraestructura. La optimización de todas estas características, sin duda, también configuran a la familia Windows Server 2003, como la plataforma más que recomendable para los negocios, reduciendo notablemente aspectos tales como el TCO.

## Un poco de historia

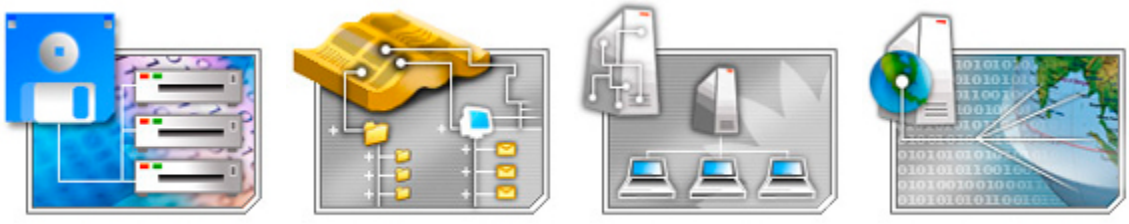
Desde el lanzamiento de los sistemas operativos de Redes, pasando por Windows NT, los sistemas se fueron perfeccionando a la medida de las necesidades de las empresas. Desde las ya conocidas diferencias que introdujo Windows 2000 sobre su predecesor Windows NT 4.0, llegamos hoy en día al Sistema Operativo óptimo para las exigencias del mercado Informático, donde se han implementado notables mejoras con respecto a su predecesor Windows 2000.

En el caso de Windows Server 2003, éste está basado en experiencias del mercado consumidor Informático, y es por eso que en él encontraremos muchas características de las que siempre nos preguntamos ¿Se puede hacer esto?....¿y aquello? Hasta el momento sin respuesta, pero a partir de ahora, esas preguntas encuentran posibles respuestas en Windows Server 2003.

Durante este módulo estaremos haciendo una introducción a las nuevas características y funcionalidades de la familia de Servidores Windows Server 2003. Al finalizar este capítulo Usted tendrá los conocimientos necesarios para describir funcionalidades, características y requerimientos de los distintos sistemas operativos de esta familia.

## 1. Nuevas Características

*Storage* *Active Directory* *Instalación* *Servicios Web*



### 1.1. Automated System Recovery

Esta nueva herramienta permite recuperar el sistema operativo a su estado anterior. ¿Cómo funciona? Utiliza un Diskette con información de la configuración y un set de backup. Cuando Usted quiera iniciar el proceso de Recovery tendrá que tener ese diskette, el set de Backup de la System Patition y el Cd-Rom de instalación de Windows Server 2003.

Para este proceso, necesitará el diskette y los medios de ASR que contienen los archivos de Backup. El sistema operativo será restaurado al mismo estado que tenía en el momento del Backup ASR, permitiéndole arrancar su sistema.

Para crear un set ASR, vea el siguiente link en el TechNet(Ingles):

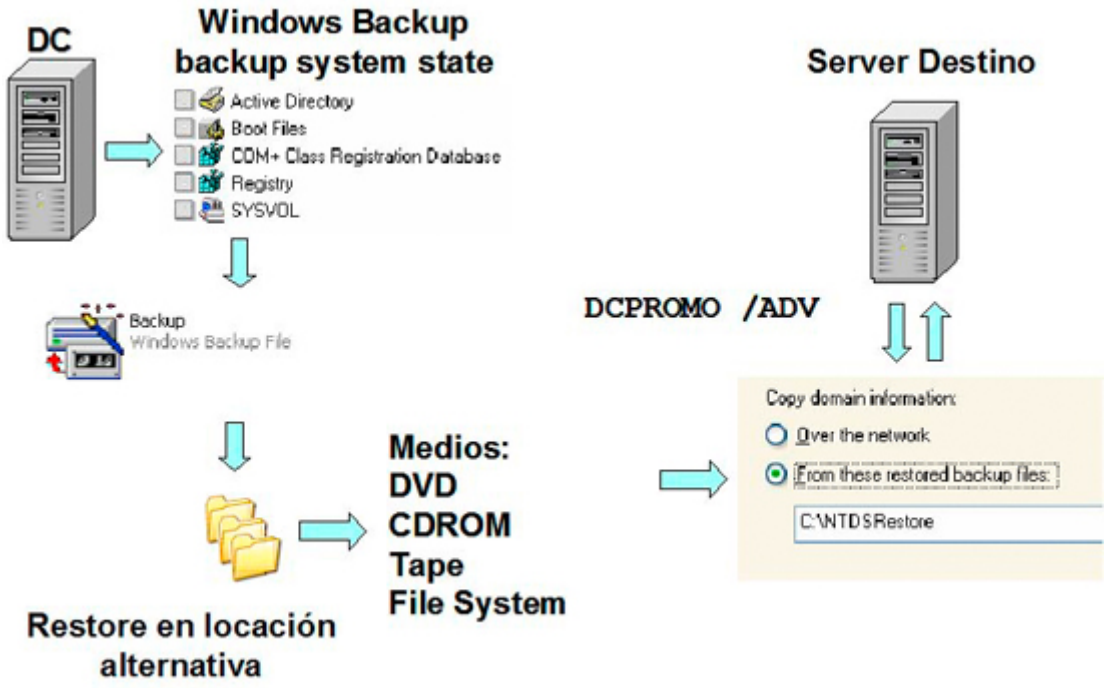
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/recovery_automatic_sr.asp

**Nota:** Durante el proceso de Restore la System Partition será formateada destruyendo todos los datos, y el backup será restaurado a su locación original. Todos los archivos modificados con posterioridad al momento del backup, se perderán.

## 1.2. Snapshot Infraestructura (Replica from Media DS)

***Esta nueva y asombrosa característica le permite resolver el siguiente problema:***

Escenario con dos locaciones: un Controlador de Dominio en la Locación A y la necesidad de instalar un Controlador de Dominio en la Locación B. A simple vista esto no sería un problema, pero si le agregamos que el vínculo WAN que une los dos puntos es de 64 Kbps y que el directorio inicial contiene 20000 ó más objetos, ahora sí hay una dificultad: el tiempo necesario para la replicación inicial, sumado que durante ese proceso, obviamente no se podrá usar el vínculo normalmente. Solución: en Windows Server 2003 Usted podrá instalar el Controlador de Dominio en la Locación B a partir de un Backup del Controlador existente en la Locación A. Este proceso será descripto detalladamente en el Capitulo 4.




## 1.3. Volume Shadow Copy

Este nuevo servicio ayuda a recuperar archivos perdidos erróneamente. Para ello el servicio Shadow Copy guarda versiones anteriores de archivos para su posterior recuperación, eliminando la necesidad de recurrir al

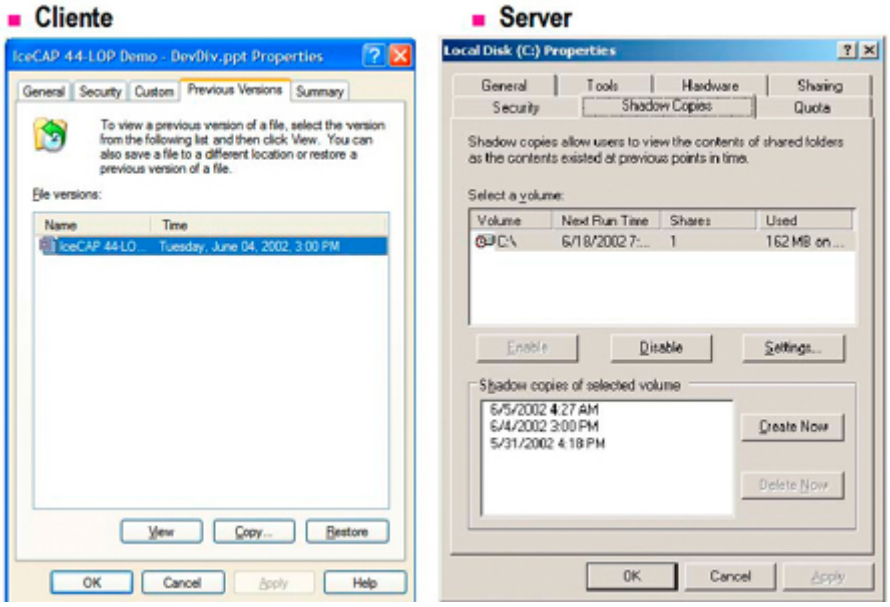
Restore de backup. ¿Cómo funciona? Utiliza un cache en disco para el almacenamiento de versiones de archivos, que luego se pueden recuperar cuando sea necesario desde esa copia.

**Animación Interactiva:**

Usted proda simular mediante la siguiente animación el uso de Volume Shadow Copy.

Si quiere bajar la animación haga click acá.

Si quiere ver la animación en Internet Explorer haga click acá.




Si quiere profundizar en este tema le recomendamos el siguiente link en el TechNet (Ingles):

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/snapshot_enable.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/accessing_shadow_copies_top.asp

## 1.4. Encrypted File System (EFS)

La nueva funcionalidad del EFS en Windows Server 2003 permite realizar una encripción del sistema de archivos en forma segura y también que otros usuarios tengan acceso a esos archivos. Esta funcionalidad es muy importante puesto que si bien en ocasiones es necesario darle seguridad a ciertos archivos, también es importante poder compartirlos entre usuarios. El sistema de encripción que utiliza EFS es una combinación de dos métodos, encripción Asimétrica y Public Key Infrastructure (PKI), puntos que serán explicados detalladamente en el capitulo 8 "Seguridad".

## 1.5. Driver Rollback

Esta es una nueva utilidad para el manejo de versiones en Drivers de dispositivos y permite volver a la versión anterior del Driver. Si este ocasiona problemas, también hay mejoras en cuanto a la verificación de funcionamiento de los drivers con la nueva versión del "Driver Verifier V2" y firmado de Drivers.

Si quiere profundizar en este tema le recomendamos el siguiente link en el TechNet (Ingles):

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/devmgr_overview_01.asp

## 1.6. Active Directory

***Veamos las nuevas funcionalidades del Servicio de Directorio que trae Windows Server 2003.***

### *ADMT versión 2.0*

Ahora es sencillo migrar a Active Directory utilizando las mejoras de Active Directory Migration Tool (ADMT). ADMT 2.0 permite migrar passwords desde Microsoft Windows NT® 4.0 a Windows 2000 y Windows Server 2003, o desde Windows 2000 a Dominios Windows Server 2003.

### *Renombrado de Dominios*

Este es el soporte para cambiar nombres Domain Name System (DNS) y/o NetBIOS de dominios existentes en un forest, conservando toda la estructura del Directorio. En escenarios de reestructuración de dominios, esto otorga una gran flexibilidad.

### *Schema*

La flexibilidad de Active Directory, ahora permite la desactivación de atributos y definición de clases en Active Directory Schema. Asimismo se agrega una nueva funcionalidad que permite borrado de Schema.

### *Group Policy*

Junto con Windows Server 2003, Microsoft lanzó una herramienta para la administración de GPO Group Policy Management Console (GPMC), que permite administrar múltiples dominios, activar y desactivar Policies y hacer soporte para drag-and-drop en la herramienta. También incluye la funcionalidad de Backup, Restore y copia de Policies, y trae una herramienta de Reportes para analizar la utilización de Policies. Encontrará mejoras sustanciales de las Policies y muchas más configuraciones para administrar en forma centralizada.

### *Relaciones de confianza*

Windows Server 2003 trae también sustanciales mejoras en cuanto al manejo de las relaciones de confianza Inter-Forest. La característica **"Cross-Forest Authentication"** permite a un usuario de Forest acceder en forma segura a recursos en otro Forest, utilizando Kerberos ó NTLM, sin sacrificar los beneficios del "Single sing-on" y facilitando la administración. Asimismo permite seleccionar fácilmente usuarios y grupos para incluirlos en grupos locales de otros Forest, manteniendo la seguridad y los SID de cada objeto, a pesar de tratarse de diferentes Forest.

### *Policies de Restricción de Software*

Por medio de estas Policies se pueden proteger los entornos de Software no autorizados, especificando el Software que sí lo está. También se pueden realizar excepciones creando reglas específicas.

### *Replicación de miembros en los grupos*

Anteriormente los miembros de un grupo eran un atributo del mismo, con lo cual, si durante la replicación se modificaba el grupo en dos Controladores de Dominio diferentes, el resultado era que la última modificación se replicaba. Es decir, si se agregaban dos usuarios a grupos, uno no era añadido, pero se tenía una limitación en cuanto a la cantidad de usuarios por grupo (Limitación del Atributo) de máximo 5000. A partir de Windows Server 2003, ahora cada usuario en un grupo es un atributo diferente, eliminando la limitación de 5000 usuarios y resolviendo los problemas de replicación.

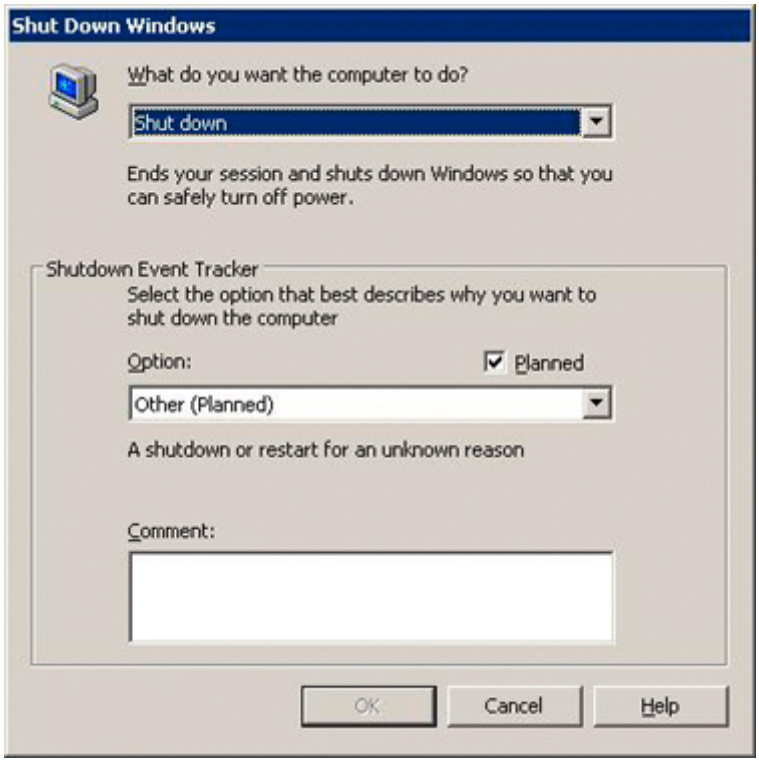
### *Manejo de Sites*

El manejo de sites incluye un nuevo algoritmo de Inter-Site Topology Generator (ISTG), eliminando la limitación del número máximo de Sites en 500 a 5000 Sites (Probado en laboratorio 3000).

**Nota:** Todas estas características están explicadas con más detalle en el Capitulo 4 "Active Directory"

## 1.7. Reboot Reason Collector "Event Tracker"

El Event Tracker es una nueva herramienta que permite recolectar para futuros análisis, los motivos por los cuales un Server se reinicia, se apaga, o fue apagado por falta de energía. En este caso la herramienta le preguntará, en el shutdown o restart, el motivo del desperfecto para almacenarlo.




## 1.8. "Remote Installation Services" RIS

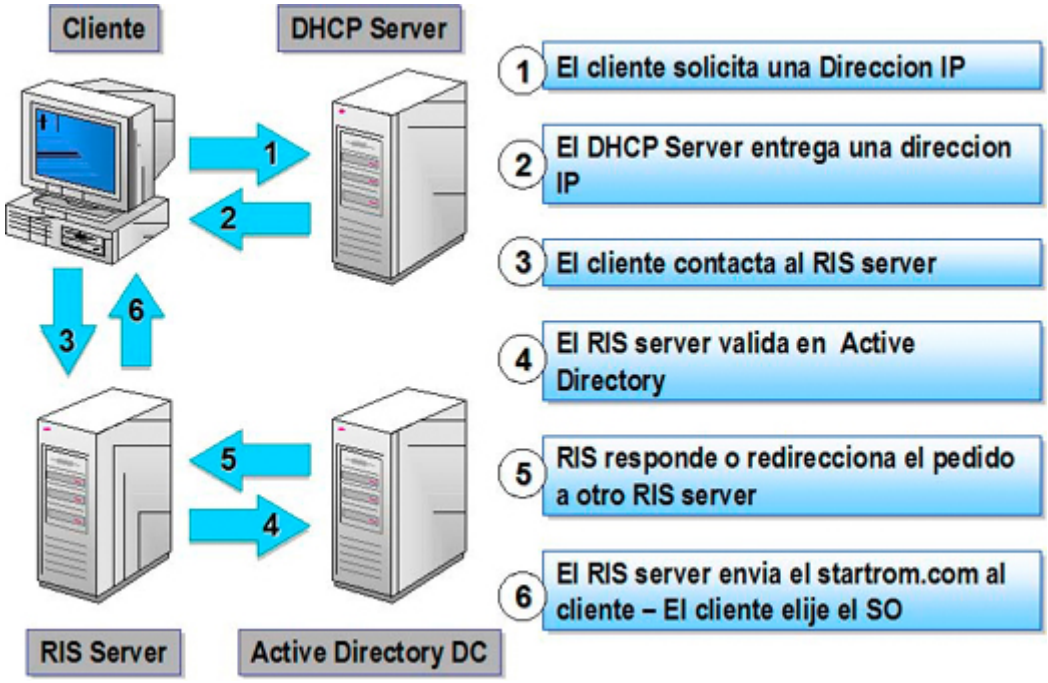
Mejoras en el soporte para instalación:

- Todas las versiones de Windows 2000 (incluidas Server y Advanced Server)
- Windows XP Professional
- Todas las versiones de Windows Server 2003

Todas las versiones de 64-bit Windows XP y Windows Server 2003

Si quiere profundizar en este tema le recomendamos el siguiente link en el TechNet (Ingles):

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_RIS_Architecture.asp




## 1.9. IIS 6.0 - Internet Information Services 6.0

Este componente del sistema operativo tuvo significantes cambios con respecto a la versión anterior, que a continuación se detallan:

### *Arquitectura de procesos Fault-tolerant*

IIS 6.0 aísla web sites y aplicaciones en unidades llamadas "Application Pools". Los Application Pools proveen una forma conveniente de administrar web sites y aplicaciones e incrementan la confiabilidad, puesto que errores en un Application Pool no causan errores en otros, o fallas en el server.

### *Health monitoring*

IIS 6.0 chequea periódicamente el estatus de los Application Pools y los reinicia automáticamente en caso de falla de web sites o aplicaciones dentro de ese Application Pool, incrementando la disponibilidad. Asimismo protege el server y otras aplicaciones, deshabilitando en forma automática web sites y aplicaciones, si fallan en un período de tiempo corto.

### *Nuevo driver kernel-mode , HTTP.sys*

Windows Server 2003 introduce un nuevo driver kernel-mode , protocolo HTTP protocol (HTTP.sys), incrementando la performance y escalabilidad. Este driver está especialmente diseñado para mejorar el tiempo de respuesta del Web Server.

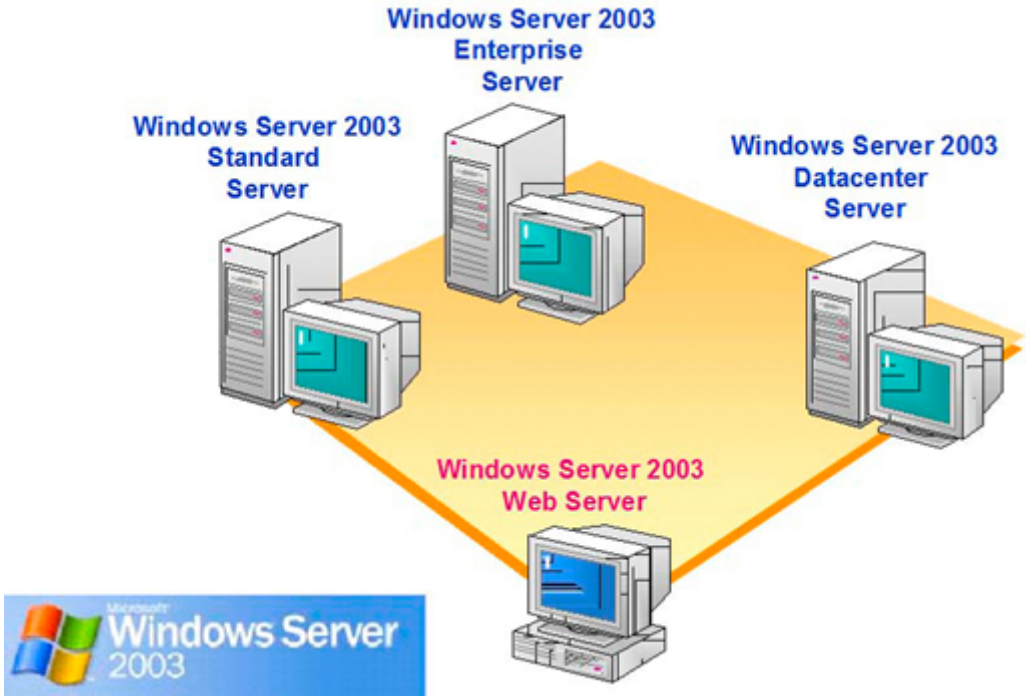
### *Integración con Aplicaciones*

IIS 6.0 ofrece integración con ASP.NET, Microsoft .NET Framework y XML Web Services, pasando a ser la plataforma especialmente diseñada para aplicaciones .Net.

### *Seguridad*

IIS 6.0 es **"Locked-down server By default"**, en otras palabras, está seguro desde su instalación, requiriendo que el administrador habilite las funciones especiales y necesarias para correr el Web Site. Sin estas tareas sólo puede ofrecer contenido estático y extensiones dinámicas deshabilitadas. Todo esto hace de IIS 6.0 el Web Server más seguro.

## 1.10. Versiones



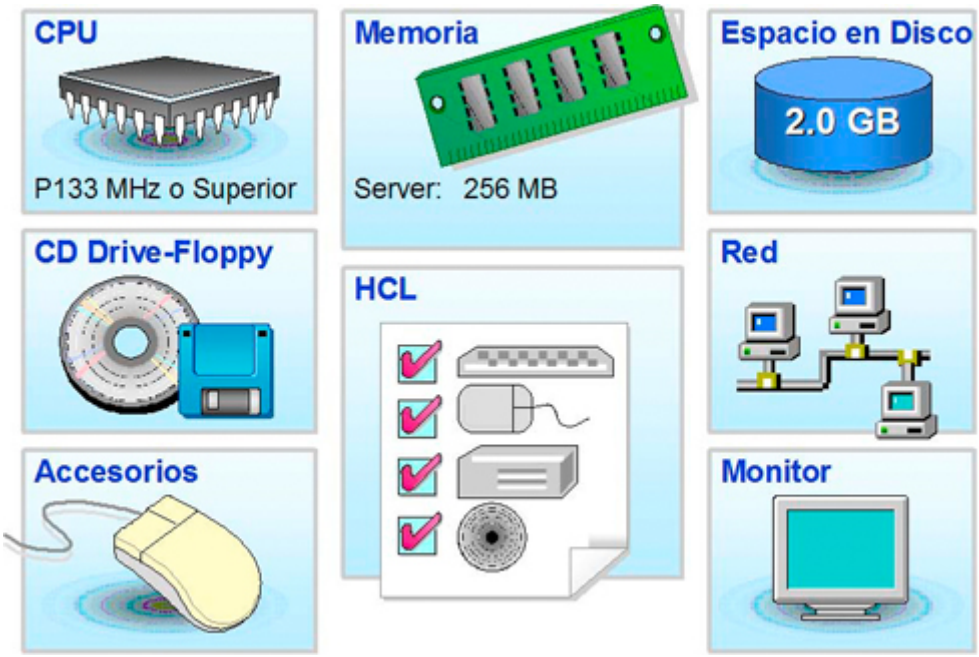
Windows Sever 2003 presenta cuatro versiones con diferentes funcionalidades que están descriptas en el siguiente cuadro

| | |
|---|---|
| Microsoft Windows Server 2003 Web Edition | Para servicios web y hosting, esta versión provee una plataforma para el desarrollo y la instalación rápida de servicios y aplicaciones web. Solo Versión OEM |
| Microsoft Windows Server 2003 Standard Edition | Para servicios de administración de Redes, esta versión de Windows Server 2003 es ideal para file and print servers, web servers, y workgroups. También provee acceso remoto a redes. |
| Microsoft Windows Server 2003 Enterprise Edition | Contiene todas las características de Windows Server 2003 Standard y provee escalabilidad y disponibilidad incrementada. Esta versión es ideal para servers utilizados en grandes redes y para bases de datos de uso intensivo. |
| Microsoft Windows Server 2003 Datacenter Edition | Contiene todas las características de Windows Server 2003 Enterprise Edition y, además, soporte para más memoria y más CPU por computadora. Esta versión es ideal para uso de datawarehouses de gran tamaño, procesamiento online, transacciones (OLTP) y proyectos de consolidación de servidores. |

El soporte en cuanto a memoria, procesadores y funcionalidad varía en las diferentes versiones. Es por ello que Usted deberá tener en cuenta las necesidades al momento de la elección del Sistema operativo.

| - | *Server* | *Web Server* | *Enterprise Server* | *Datacenter* |
|---|---|---|---|---|
| CPU / RAM | 2 CPU<br>4 GB | 2 CPU<br>2GB | 8 CPU<br>32 GB (x86)<br>64 GB (64-Bit) | 8-64 CPU<br>64GB (x86)<br>512 GB (64-Bit) |
| Caracteristicas | **Nuevas Caracteristicas:**<br>•NLBS<br>•Personal Firewall | **Puede correr:**<br>•IIS 6.0<br>•NLBS<br>•DNS, DHCP, WINS<br><br>**Limitaciones:**<br>•No DC Promo<br>•No Aplicaciones<br>•No TS App<br>•Mode | **All features from Standard plus:**<br>•8-node Clustering<br>•64-bit Version | **All features from Enterprise, plus:**<br>•Datacenter program<br>-Datacenter HCL<br>-Maintenance<br>•Multi-instance support |

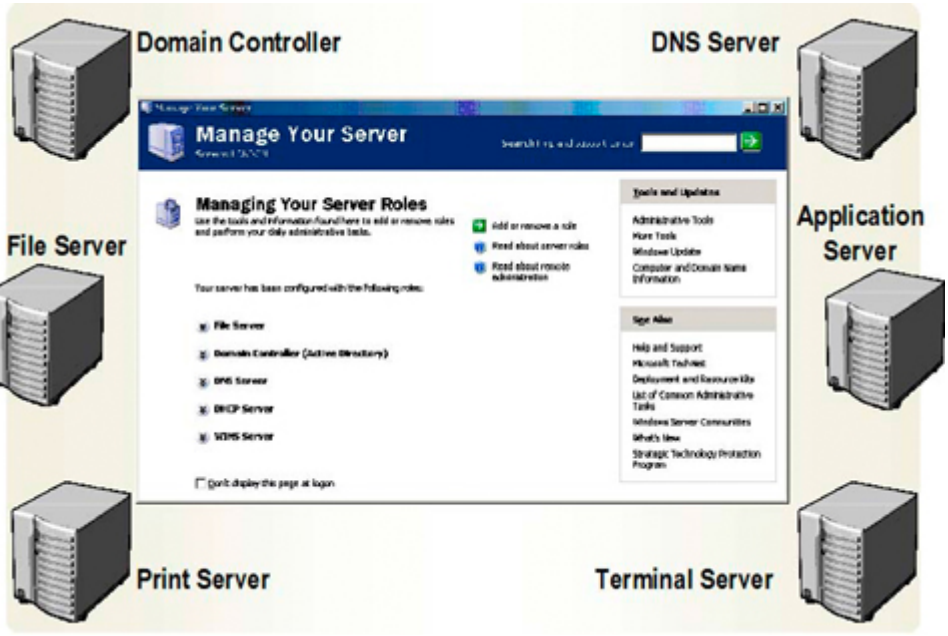
### 1.11. Requerimientos




En el siguiente cuadro se presentan los requerimientos mínimos y recomendados para cada versión de Windows Server 2003.

| Windows Server 2003 Requerimientos del Sistema | | | | |
|---|---|---|---|---|
| **Requerimiento** | **Standard Edition** | **Enterprise Edition** | **Datacenter Edition** | **Web Edition** |
| **Velocidad de CPU mínima** | 133 MHz | 133 MHz para arquitectura x86<br><br>733 MHz para arquitectura Itanium | 400 MHz para arquitectura x86<br><br>733 MHz para arquitectura Itanium | 133 MHz |
| **Velocidad de CPU Recomendada** | 550 MHz | 733 MHz | 733 MHz | 550 MHz |
| **RAM Mínima** | 128 MB | 128 MB | 512 MB | 128 MB |
| **RAM Recomendada** | 256 MB | 256 MB | 1 GB | 256 MB |
| **RAM Máxima** | 4 GB | 32 GB for para arquitectura x86<br><br>512 GB para arquitectura Itanium | 64 GB para arquitectura x86<br><br>512 GB para arquitectura Itanium | 2 GB |
| **Soporte Multiprocesador SMP** | Hasta 4 | Hasta 8 | Requerido 8 Mínimo<br><br>Máximo 64 | Hasta 2 |
| **Espacio Mínimo en Disco** | 1.5 GB | 1.5 GB para arquitectura x86<br><br>2.0 GB para arquitectura Itanium | 1.5 GB para arquitectura x86<br><br>2.0 GB para arquitectura Itanium | 1.5 GB |

## 2. Funcionalidades




Los servidores desempeñan muchos papeles en el ambiente client/server de una red. Algunos servidores se configuran para proporcionar la autentificación y otros se configuran para funcionar con otros usos. Asimismo, muchos proporcionan los servicios de red que permiten a usuarios comunicar o encontrar otros servidores y recursos en la red. Como administrador de sistemas, de Usted se espera que sepa los tipos primarios de servidores y qué funciones realizan en su red.

### 2.1. Domain controller (Active Directory)

Los Controladores de dominio almacenan datos del directorio y manejan la comunicación entre los usuarios y los dominios, incluyendo procesos de conexión del usuario, autentificación y búsquedas del directorio. Cuando Usted instala Active Directory en una computadora que corre Windows Server 2003, la computadora se convierte en Controlador de dominio (Domain Controler).

**Nota:** En una red Windows Server 2003, todos los servidores en el dominio que no sean Domain Controlers se llaman Member Servers. Los servidores no asociados a un dominio se llaman workgroup Servers.

### 2.2. File server

Un File Server proporciona una localización central en su red donde puede almacenar y compartir archivos con los usuarios a través de su red. Cuando los usuarios requieren un archivo importante, tal como un plan de proyecto, pueden tener acceso al archivo en el File Server en vez de pasar el archivo entre sus computadoras separadas.

### 2.3. Print Server

Un Print Server proporciona una localización central en su red, donde los usuarios pueden imprimir. El Print Server provee a los clientes los drivers actualizados de la impresora y maneja la cola de impresión y la seguridad.

### 2.4. DNS server

El Domain Name System (DNS) es un servicio estándar de Internet y de TCP/IP. El servicio de DNS permite a las computadoras cliente, colocar en su red y resolver nombres de dominio DNS. Una computadora configurada para proporcionar servicios del DNS en una red, es un servidor DNS, lo que es necesario para poner en funcionamiento Active Directory.

### 2.5. Application Server

Un servidor de Aplicaciones proporciona la infraestructura y los servicios de Aplicaciones en un sistema. Los servidores típicos de aplicaciones incluyen los siguientes servicios:

- Resource pooling (por ejemplo, pool de conexiones de base de datos y pool de objetos)
- Administración de transacciones distribuidas
- Comunicación asincrónica, típicamente message queuing
- Un modelo de objetos de activación just-in-time
- Automatic Extensible Markup Language (XML) e Interfaces de Web Service para acceso a objetos de negocio
- Servicios de detección de Failover y funcionamiento de aplicaciones con seguridad integrada

Microsoft Internet Information Services (IIS) proporciona las herramientas y las características necesarias para manejar fácilmente un Web Server seguro. Si Usted planea hacer hosting de Web y Sitios File Transfer Protocol (FTP) con IIS, configure el Server como Application Server.

### 2.6. Terminal server

Un Terminal Server provee a las computadoras alejadas, el acceso a los programas basados en Windows que funcionan en Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition o Windows Server 2003 Datacenter Edition. Con un Terminal Server, Usted instala una aplicación en un solo punto y en un solo servidor. Los usuarios múltiples, entonces, podrán tener acceso a la aplicación sin la instalación de la misma en sus computadoras. Los usuarios pueden correr programas, y utilizar los recursos de la red de una posición remota, como si éstos recursos fueran instalados en su propia computadora. Veremos mas de este tema en el capitulo 6

### 2.7. La herramienta Manage Your Server

Cuando Windows Server 2003 es instalado y un administrador realiza el logon por primera vez, la herramienta Manage Your Server corre automáticamente. Usted utiliza esta herramienta para agregar o para quitar Roles a Servers. Cuando agregue un Rol de Server a una computadora, la herramienta Manage Your Server agregará ese rol de la lista de roles disponibles. Después que el Server Role se agregue a la lista, usted podrá utilizar varios wizards que le ayudarán a administrar roles específicos del Server. La herramienta Manage Your Server también provee archivos de ayuda específicos a los Roles de Servers, tiene checklists y recomendaciones de troubleshooting.

# Capítulo 2
# Instalación y Migración

## 1. Introducción

A lo largo de este capítulo Usted irá descubriendo los métodos de instalación de Windows Server 2003, como así también los métodos de migración desde otras versiones.

Para poder realizar las prácticas contenidas en esta unidad deberá tener una copia de evaluación de Windows Server 2003 que se encuentra en:

http://www.microsoft.com/windowsserver2003/evaluation/trial/default.mspx

También será necesario que cuente con el hardware apropiado, el cual debe cubrir los requerimientos para la instalación de Windows Server 2003 descriptos durante el Capítulo 1. De no contar con hardware adicional, sugerimos utilizar el software de emulación de Computadoras Virtuales, que lo puede obtener en:

http://www.microsoft.com/windowsxp/virtualpc/

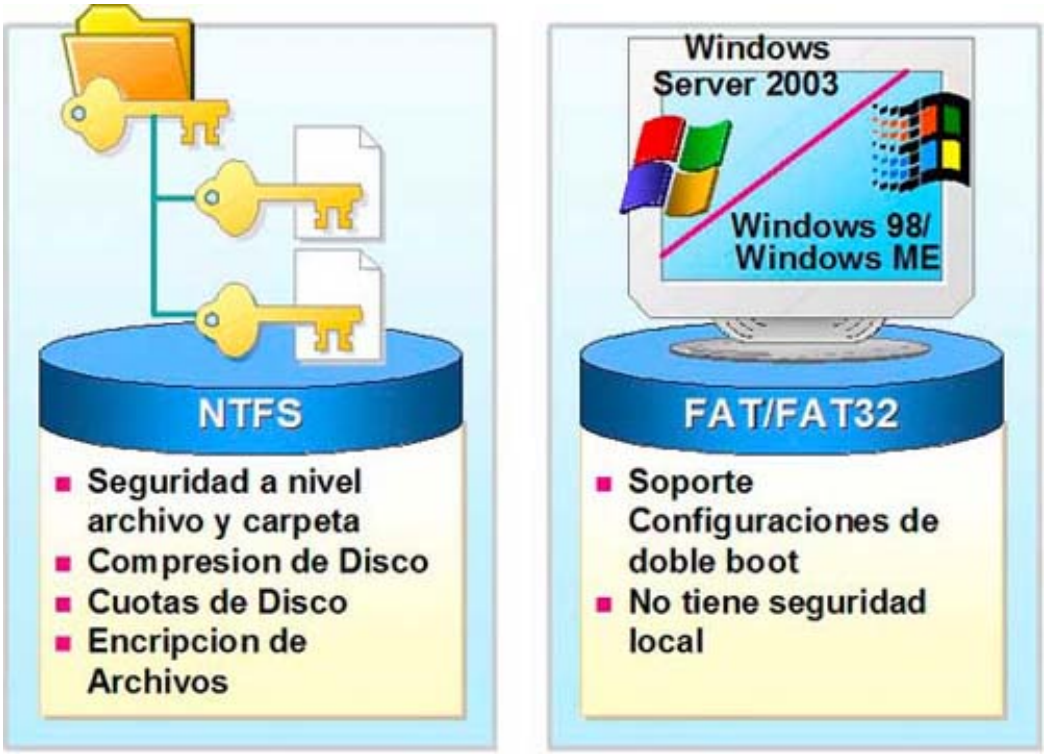
Este software permite crear Computadoras Virtuales dentro de su sistema y asignarle recursos de disco y memoria, es decir, una computadora dentro de su computadora.

Recuerde que esta unidad contiene también prácticas de migración desde Windows NT Server 4.0 y Windows 2000 Server, por lo que será necesario que cuente con CD de evaluación de estos productos.

Al finalizar este capítulo Usted tendrá la habilidad de:

- Prepararse para una instalación de Windows Server 2003.
- Instalar Windows Server 2003 desde un CD.
- Instalar Windows Server 2003 desde la red.
- Solucionar problemas de instalación.
- Examinar la activación de Windows Server 2003.
- Describir cómo automatizar instalaciones de Windows Server 2003.

## 2. Instalación




### 2.1. Introducción a la instalación de Windows Server 2003

La instalación y configuración de Windows Server 2003 es similar al proceso de instalación de Windows 2000 Server, por lo que los administradores expertos en este último podrán utilizar sus conocimientos para llevarla a cabo. Sin embargo, hay un importante número de mejoras:

- ***Nuevo Asistente para instalación:*** el nuevo Asistente para instalación de Windows Server 2003 conserva la mayor parte del diseño del Asistente para la instalación de Windows 2000 Server. No obstante, su diseño ha mejorado para que sea más fácil encontrar información y tareas relacionadas con la instalación. El nuevo Asistente refleja el diseño basado en tareas de Windows Server 2003, mediante la agrupación de las tareas comunes con documentación e información necesarias para ayudar a los administradores a realizarlas.

- ***Actualización dinámica:*** ahora el Asistente proporciona a los usuarios la opción de descargar archivos de instalación y controladores actualizados de Microsoft. Esta opción también se puede incluir en una secuencia de comandos como parte de una instalación desatendida.

- ***Comprobación de compatibilidad:*** el Asistente permite a los usuarios realizar una prueba de compatibilidad detallada en sus PCs. Como parte del proceso de comprobación de compatibilidad, Usted puede visitar el sitio Web de Microsoft en busca de actualizaciones dinámicas. Existe también una herramienta adicional que puede utilizar para comprobar compatibilidad de aplicaciones "Application Compatibility Toolkit", herramienta que puede obtener de:

http://www.microsoft.com/windowsserver2003/compatible/appcompat.mspx

***Asistente para instalación de Windows Server 2003***


Para obtener información sobre compatibilidad de hardware:

http://www.microsoft.com /whdc/hcl/default.mspx

## 2.2. Seleccionando File System

Una vez que Usted haya creado la partición donde planea instalar Windows Server 2003, la instalación permitirá que seleccione el sistema de archivos para darle formato. Como con Windows NT 4.0, Windows 2000 y Windows XP Professional, Windows Server 2003 soporta sistema de archivos NTFS y FAT16/FAT32.

***NTFS***

Utilizar NTFS para las particiones, requiere:

- ***Seguridad a nivel archivo y carpeta.*** NTFS permite controlar el acceso a los archivos y a las carpetas.
- ***Compresión de disco.*** NTFS permite comprimir archivos para crear más espacio disponible.
- ***Cuotas de disco.*** NTFS permite controlar el uso del disco por usuario.
- ***Encripción de archivos.*** NTFS permite transparentemente encriptar, archivos y carpetas.

La versión de NTFS en Windows Server 2003 soporta remote storage y mounting de volúmenes en carpetas. Microsoft Windows 2000, Windows XP Profesional, Windows Server 2003 y Windows NT son los únicos sistemas operativos que pueden tener acceso a datos sobre un disco duro local que tenga formato NTFS.

Para compatibilidad en NTFS y Windows NT 4.0 en configuraciones de doble boot, Windows NT 4.0 requiere Service Pack 4 mínimo. Para obtenerlo se recomienda usar Service Pack 6.

http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/x86Lang.asp

### *FAT y FAT32*

Normalmente, Usted no utilizaría FAT o FAT32 para dar formato a la partición del sistema, a menos que requiera un dual boot entre Windows Server 2003 y otro sistema operativo. FAT y FAT32 no ofrecen las características de seguridad que provee NTFS. Si Usted requiere las características de NTFS, particularmente seguridad a nivel archivos y carpetas, es recomendable que use sistema NTFS.

**Nota:** Si elige dar formato a la partición usando FAT, la instalación automáticamente dará formato a particiones que son mayores de 2 GB en FAT32.

## 2.3. Seleccionando Modo de Licenciamiento

### 2.3.1. Modelo de licenciamiento para Windows Server 2003: lo que no se ha modificado

Aunque hubo cambios en el modelo de licenciamiento de Windows Server 2003, éstos son los elementos que no han cambiado:

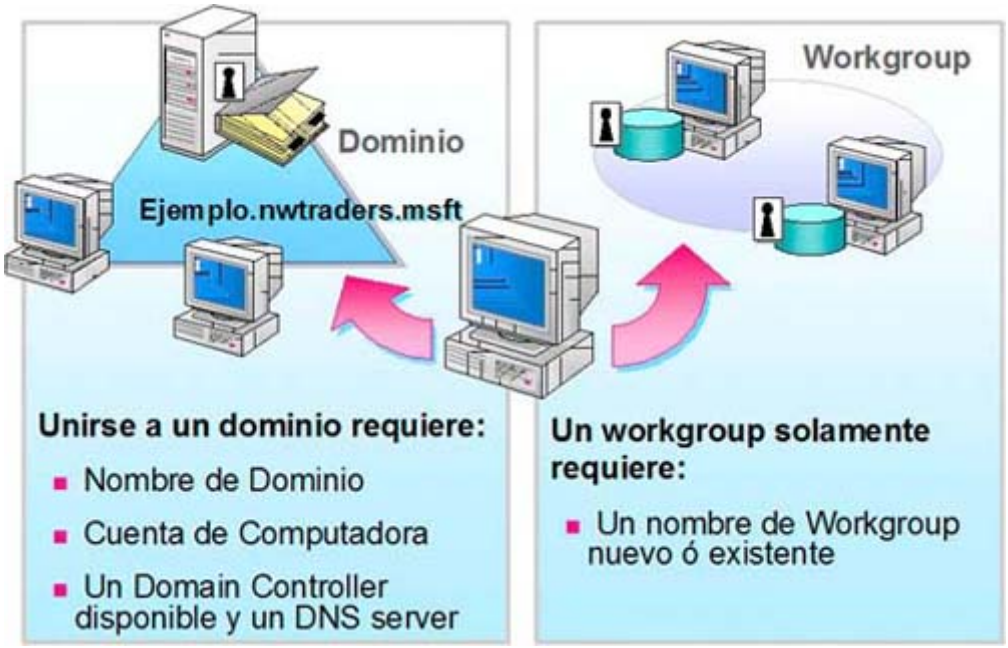
- Cada copia instalada del software de servidor requiere la compra de una licencia de servidor de Windows.
- Se requiere una Licencia de Acceso para Cliente de Windows (CAL de Windows) para poder acceder al uso del software del servidor.
- No se requiere una CAL si el acceso al servidor es a través de Internet y no está "autentificado" - por ejemplo el acceder a un sitio Web para obtener información general donde no se intercambian credenciales de identificación-.
- Una CAL de Windows (Per Server) puede aún ser designada para su uso con un solo servidor, autorizando acceso por medio de cualquier dispositivo o usuario, cuando la modalidad de software de licencia para el servidor esté definida en "Per Server". En esta modalidad, el número de CAL's de Windows es igual al numero máximo de conexiones corrientes.
- Una CAL de Windows (Per Device o Per User) puede ser designada para su uso con cualquier número de servidores, autorizando el acceso por medio de un dispositivo específico o usuario, cuando la modalidad de licencia del software de servidor esté definida en "Per Device o Per User" (anteriormente llamada modalidad "Per Seat").
- Se requiere una licencia de Acceso de Cliente a Terminal Server (CAL TS) para utilizar un Servidor Terminal u hospedar una sesión de interfase de usuario gráfica remota (GUI), excepto para una sesión de consola. En Windows 2000, había una excepción a este requerimiento de licencia y eso cambiará.

### 2.3.2. Cambios en el licenciamiento de Windows Server 2003

- ***CAL basada en Nuevo Usuario***. Microsoft ha introducido un nuevo tipo de CAL. Además del CAL existente basado en dispositivo (CAL Per Device), un nuevo CAL basado en usuario (CAL Per User) estará disponible. Usted puede escoger entre un CAL Per Device para Windows para cada dispositivo que acceda sus servidores, o un CAL Per User Windows para cada nombre de usuario que acceda a sus servidores. Al tener dos tipos de CAL's, Usted podrá utilizar el modelo que tenga más sentido para su organización. Por ejemplo, una CAL para Usuario Windows quizás tenga más sentido si su compañía tiene la necesidad que sus empleados tengan acceso remoto utilizando múltiples dispositivos. Los CAL de Dispositivo Windows pueden tener más sentido si su compañía tiene múltiples trabajadores que comparten dispositivos. Similarmente, los Servidores Terminales (TS) ofrecerán tanto CAL's basadas en Dispositivo como en Usuario: CAL Per Device TS y CAL Per User TS.

Para obtener mas información: http://www.microsoft.com/windowsserver2003/howtobuy/licensing/overview.mspx

### 2.4. Determinando pertenencia a Workgroup o Dominio




Durante la instalación, Usted debe elegir un dominio o un workgroup como grupo de seguridad para la pertenencia de la computadora.

#### 2.4.1. Dominio

Durante la instalación Usted puede agregar la computadora a un dominio existente como member server, operación que requiere lo siguiente:

- Un nombre de Dominio. Un ejemplo de un nombre de dominio DNS válido es .microsoft.com.
- Una cuenta de computadora. Antes de unir una computadora a un dominio, tiene que existir una cuenta para esa computadora en el Dominio. Usted puede crear la cuenta antes de la instalación o, si tiene privilegios administrativos en el dominio suficientes, puede crear esta cuenta durante la instalación. Si la cuenta de la computadora se crea durante la instalación, el programa de instalación le pedirá que ingrese usuario y contraseña con autoridad para agregar cuentas de computadoras al dominio.
- Un domain controller disponible y un server corriendo el servicio DNS Server. Por lo menos un domain controller y un DNS server deben estar online al momento de agregar una computadora al dominio

#### 2.4.2. Workgroup

Como con Windows NT 4.0, Usted puede agregar la computadora a un workgroup, únicamente si está en una red pequeña sin un dominio o si se está preparando para agregar a un dominio más adelante. El nombre del workgroup que Usted asigne puede ser el nombre de un workgroup existente o de un workgroup nuevo que cree durante la instalación

## 2.5. Checklist

Antes de instalar Windows Server 2003, complete las siguientes tareas:

- Verificar que todo el hardware esté listado en la HCL.
- Verificar que los componentes cumplan el mínimo hardware requerido.
- Seleccionar el sistema de archivos para la partición, en cual instalará Windows Server 2003, a menos que usted necesite una configuración dual boot de formato usando NTFS.
- Determinar si utilizará Per Device o Per User como modo de licenciamiento.
- Determinar el nombre del dominio al que Usted quiere agregar o el workgroup que creará. Si va a usar un dominio, el nombre estará en formato DNS: server.domain (donde server es el nombre de su computadora y dominio es el nombre del dominio al cual pertenece su computadora). Si agrega a un workgroup, el nombre estará en formato (NetBIOS).
- Crear una cuenta de computadora en el dominio, usando el nombre de la computadora que Usted está instalando. Aunque un administrador de dominio puede crear una cuenta de computadora antes de la instalación, Usted puede crear también una cuenta de computadora durante la instalación si tiene privilegios administrativos suficientes en el dominio. Por defecto, los usuarios pueden crear hasta 10 cuentas de computadora en el dominio.
- Determinar la contraseña para la cuenta del Administrador local.

## 2.6. Instalando desde Compact Disc


La instalación de Windows Server 2003 desde compact disc implica encender la computadora de compact disc o floppy disks y proceder con varios wizards. Aunque el proceso de instalación no es perceptiblemente diferente de Windows NT 4.0 o Windows 2000, tener experiencia con el proceso de la instalación de Windows Server 2003 le ayudará a realizar este proceso más eficientemente.

### 2.6.1. Funcionamiento del Programa de instalación

La porción de modo texto de instalación en Windows Server 2003 no es diferente a la porción de instalación en modo texto de Windows NT 4.0 y Windows 2000. Realizar una instalación implica los pasos siguientes:

- Para comenzar la instalación hay que apagar la computadora, insertar el CD-ROM en la lectora y encender la computadora. Como alternativa, se puede correr Winnt.exe. Una versión mínima de Windows Server 2003 se copia en memoria y entonces la porción de instalación en modo texto se inicia. TIP: Si utiliza un floppy de DOS con carga de Drivers para la lectora de CD-ROM, asegúrese de cargar el driver SmartDrive. De lo contrario, la instalación puede demorar más de lo normal.

- Seleccionar la partición en la cual instalará Windows Server 2003.

- Seleccionar un sistema de archivos para la partición nueva. También se puede elegir dar formato a la partición nueva.

La instalación copia archivos al disco y graba parámetros de configuración. Luego se reinicia la computadora y se inicia el Wizard de instalación de Windows Server 2003. La locación por defecto de los archivos de la instalación de los sistemas operativos Windows Server 2003 es la carpeta Windows.

### 2.6.2. Iniciando el Wizard de instalación de Windows Server 2003

Después de instalar las características de seguridad y configurar los dispositivos, el Wizard le solicitará la siguiente información:

- Configuración Regional
- Nombre y organización
- Product key (de 25 caracteres)
- Modo de Licenciamiento
- Nombre para la computadora y contraseña para la cuenta del Administrador local.
- Componentes opcionales de Windows Server 2003.

### 2.6.3. Instalación de Componentes para Networking

Después de recopilar la información sobre su computadora, el Wizard lo guiará a través de la instalación de componentes para networking. Este segmento del proceso de instalación comienza con la detección de las tarjetas de red. Para continuar con el Wizard, se deben seguir los pasos siguientes:

En primer lugar tiene que instalar componentes de networking en configuración típica o custom. La instalación típica incluye:

- Cliente para Redes Microsoft
- Compartir archivos e impresoras para Redes Microsoft
- Internet Protocol (TCP/IP) en una instalación típica, que se configura para dirección IP dinámica. Para configurar TCP/IP, deberá elegir una instalación custom.
- Agregar a workgroup o a dominio.

### 2.6.4. Fin de la instalación

Después de instalar los componentes de networking, el programa de instalación termina de la siguiente manera:

- Copia los archivos restantes, por ejemplo los accesorios y BITMAPS.
- Aplica la configuración que Usted especificó anteriormente.
- Guarda la configuración al disco duro local.
- Quita archivos temporales y reinicia la computadora.

Obtenga más información sobre la instalación nueva:

http://support.microsoft.com/default.aspx?scid=kb;en-us;326218

### 2.6.5. Practica 1

#### 2.6.5.1. Objetivos

Después de terminar esta práctica, Usted podrá instalar Windows Server 2003, como member server de un workgroup.

#### 2.6.5.2. Pre-requisitos

Antes de trabajar en esta práctica, deberá tener una computadora que cumpla con el mínimo hardware requerido para instalar Windows Server 2003 o el software Connectix Virtual PC for Windows.

Para terminar esta práctica, necesitará lo siguiente:

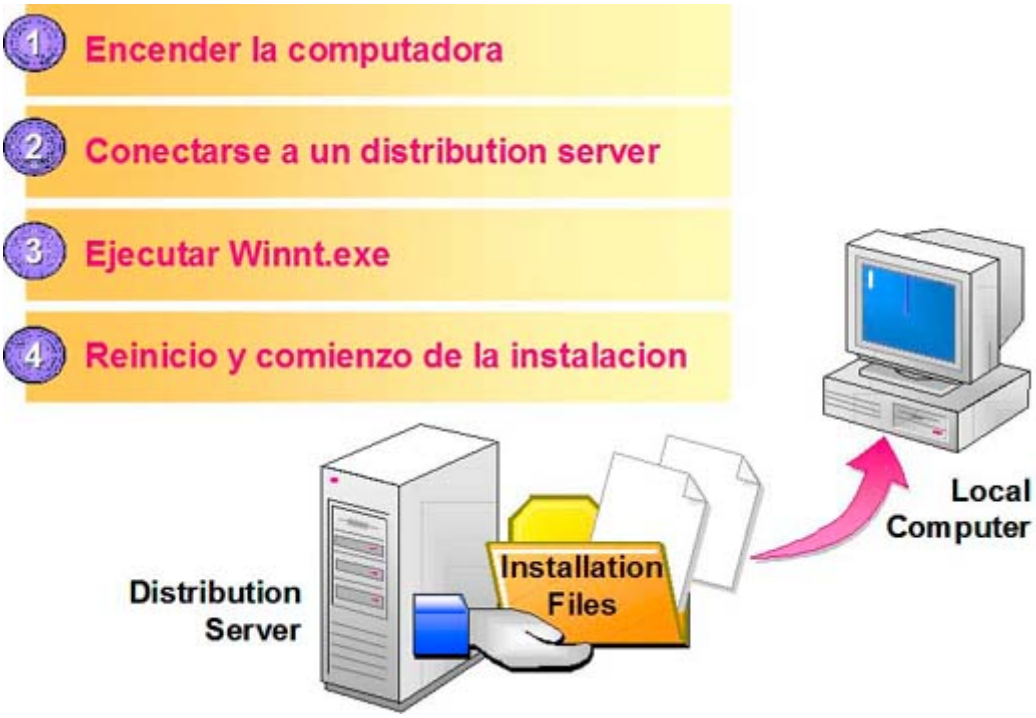
- El compact disc Windows Server 2003 Evaluation Edition.
- El Floppy disk MS-DOS para boot (optional). Si su computadora se configura para arrancar de CD-ROM, usted puede instalar Windows Server 2003 sin usar el Floppy Disk.
- Información para instalación en sistemas sin opción de arranque desde CD-ROM: http://support.microsoft.com/default.aspx?scid=kb;en-us;810562
- Un nombre de computadora y una IP address.

## Ejercicio 1

### Instalación de Windows Server 2003

1. Encender la computadora con el CD-ROM Windows Server 2003.
2. Presionar ENTER cuando aparezca la notificación del Setup en la pantalla.
3. Presionar ENTER cuando aparezca el mensaje ***Welcome to Setup*** en la pantalla. Leer el ***Windows Server 2003 Licensing Agreement*** y presionar F8 para aceptar los términos de licenciamiento.
4. Presionar C en la lista de particiones existentes para crear una partición en el disk 0.
5. Cuando se pida seleccionar el tamaño de la partición en el cuadro ***Create partition of size (in MB)***, borrar el valor existente, agregar un valor de ***2000 a 4000*** y presionar ENTER.
6. Presionar ENTER en la lista de particiones existentes para seleccionar ***C: New (Unformatted) XXXX MB*** partition.
7. Presionar ENTER para seleccionar ***Format the partition using the NTFS file system***.
8. Quitar el floppy disk del drive si usted comenzó con él la instalación.
9. Dejar el compact disc de Windows Server 2003 en la lectora de CD-ROM.
10. ***La computadora se reiniciará automáticamente***.
11. Esperar la finalización del proceso de detección de dispositivos.
12. Hacer click en ***Next*** de la página ***Regional Settings,***.
13. Ingresar nombre y organización. Hacer click en Next.
14. Escribir el product key en la página ***Your Product Key***. Lo puede obtener en el Site desde donde descargó el producto.
15. Elegir Per Device = 20 en el modo de licenciamiento
16. Usar el siguiente password= ***Pass@w0rd*** (donde 0 es zero) para la cuenta del Administrador local
17. No instalar componentes adicionales
18. Ajustar fecha y hora en la página Date and Time ***Settings***, y hacer click en ***Next***.
19. Hacer click en ***Custom settings*** del cuadro de diálogo ***Network Settings***, y presionar ***NEXT***.
20. Hacer click en properties de TCP/IP y colocar los siguientes parámetros: IP address: 192.168.1.200 subnet mask: 255.255.255.0
21. Hacer click en ***Next*** de la página ***Networking Components***.
22. Agregar un Workgroup llamado "Workgroup"
23. Dejar el CD-ROM de Windows Server Server 2003 en la lectora durante el resto del proceso.
24. Una vez completado el proceso de instalación la computadora se reiniciará automáticamente

## 2.7. Instalando desde la red




Las instalaciones desde la red funcionan del mismo modo que en Windows NT4.0 y Windows 2000. Todavía hay tres requisitos para comenzar una instalación desde la red:

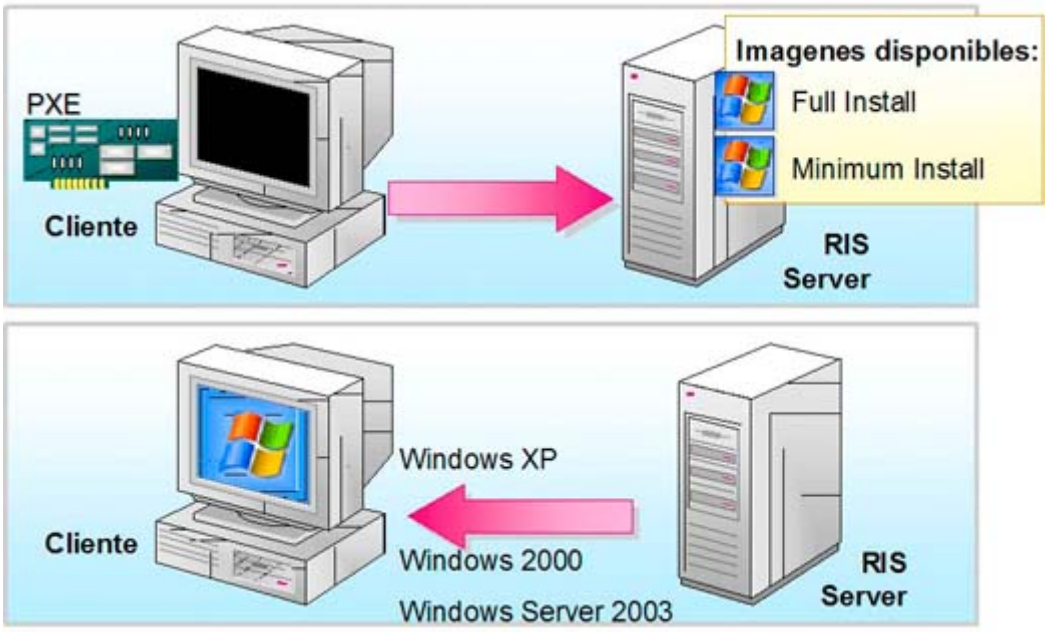
- Un Distribution Server que contenga los archivos de la instalación i386. (Las computadoras Itanium usan la carpeta ia64. Estas carpetas se encuentran en el CD-ROM de Windows Server 2003).
- Una partición disponible de 2gb en la computadora.
- Un cliente de red para poder conectarse al Distribution Server.

**Nota:** Microsoft Windows Preinstallation Environment (WinPE) permitirá a un cliente conectarse al Distribution Server. Obtenga información en:

http://www.microsoft.com/licensing/programs/sa/sam/winPe.asp

Los pasos para la instalación son similares a Windows NT 4.0 y Windows 2000; sólo se tiene que conectar al Distribution Server y ejecutar Winnt.exe. Durante el proceso inicial se copian los archivos necesarios en el disco local y luego la computadora reinicia y ejecuta. A partir de ese momento, el proceso de instalación es normal.

## 2.8. Usando Remote Instalation Services (RIS)




El Servicio Remote Installation Services (RIS) permite a las computadoras cliente conectarse con un servidor durante la fase de inicial de encendido e instalar remotamente Windows 2000 (en todas sus versiones),Windows XP (32 y 64 Bit) o Windows Server 2003 (en todas sus versiones). Es un proceso totalmente diferente a la instalación desde la red ya que ésta se realiza ejecutando Winnt.exe. Una instalación remota no requiere que los usuarios sepan dónde se encuentran los archivos de instalación o la información a suministrarle al programa de instalación.

RIS permite configurar las opciones de la instalación. Por ejemplo, usted podría tener una alternativa que provea a los usuarios una instalación mínima sin opciones y otra que provea a los usuarios opciones adicionales. Por defecto, todas las imágenes están disponibles para todos los usuarios. Sin embargo, Usted puede restringir las imágenes que están disponibles para los usuarios utilizando permisos NTFS en el archivo de respuesta. Los pasos siguientes permiten determinar qué imágenes puede seleccionar y descargar un usuario.

1. Instalar RIS.
2. Configurar los componentes opcionales que Usted planea instalar en la computadora del cliente.
3. Las imágenes que se almacenan en el RIS server.
4. El cliente se conecta usando Pre-Boot Execution Environment (PXE) en el adaptador de red, o usando "Network Boot Disk" que es creado por RIS.
5. El sistema operativo se instala en el cliente desde el RIS server con poca o ninguna intervención del usuario.

Usted puede controlar la información requerida por usuario, creando y usando scripts. También puede crear a éstos manualmente o puede utilizar el Setup Manager Wizard.

Obtenga información acerca del Setup Manager:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323438

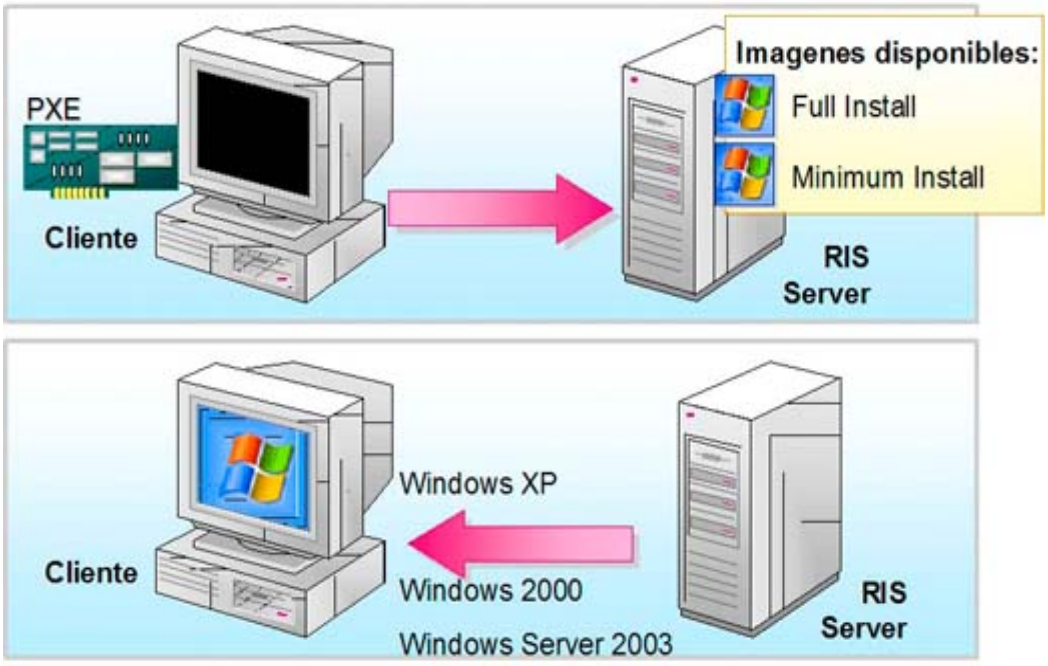
### 2.8.1. Requisitos para RIS Server

- Active Directory
- DHP Server
- DNS Server

Obtenga información acerca de RIS Server:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325862

## 2.9. Usando System Preparation Tool (sysprep)



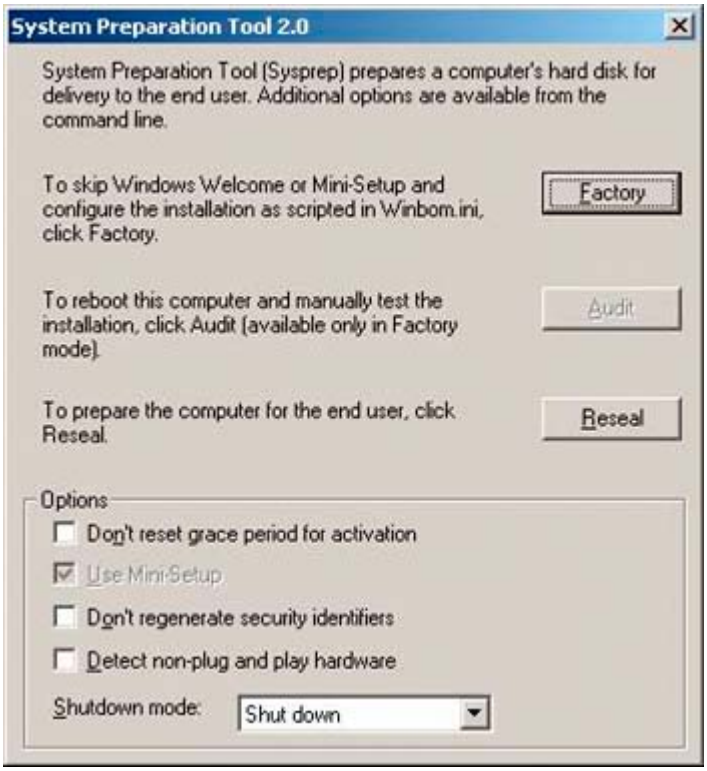

Cuando Usted quiera instalar Windows 2000,Windows XP o Windows Server 2003 en varias computadoras que tienen idéntico hardware, uno de los métodos que podría seguir para ello es utilizar la duplicación de disco. Creando una imagen del disco de una instalación de Windows 2000, Windows XP o Windows Server 2003, y copiando esa imagen sobre las computadoras múltiples de destino, Usted ahorra tiempo en deployment de Windows 2000, Windows XP o Windows Server 2003.

Para instalar Windows 2000, Windows XP o Windows Server 2003 usando duplicación de disco, configure una computadora de referencia y duplique una imagen de disco al server, usando Sysprep.inf para preparar la computadora a duplicar. El proceso de la duplicación de disco consiste en los pasos siguientes:

- Instalar y configurar el sistema operativo en la computadora de referencia.
- Instalar y configurar los aplicativos en la computadora de referencia.
- Ejecutar sysprep.exe en la computadora de referencia.

También puede ejecutar el Setup Manager Wizard para crear el archivo Sysprep.inf. Sysprep.inf proporciona respuestas, como por ejemplo, el nombre de computadora al Mini-Setup que se ejecuta en las computadoras destino. Además, este archivo se puede utilizar para especificar drivers especiales. El Setup Manager Wizard crea una carpeta Sysprep en el root del disco y coloca el archivo Sysprep.inf en esa carpeta. El Mini-Setup chequea la carpeta Sysprep en busca de ese archivo para realizar la instalación del sistema operativo.

- Luego se debe apagar la computadora de referencia y ejecutar el Software de duplicación de disco.
- Colocar el disco duplicado en la computadora destino.
- Encender la computadora destino. Un Mini-Setup se ejecutará inmediatamente solicitando: Nombre de computadora, Password del Administrador local y Product Key.




Obtenga información acerca de Sysprep Versión 2.0 en:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325858

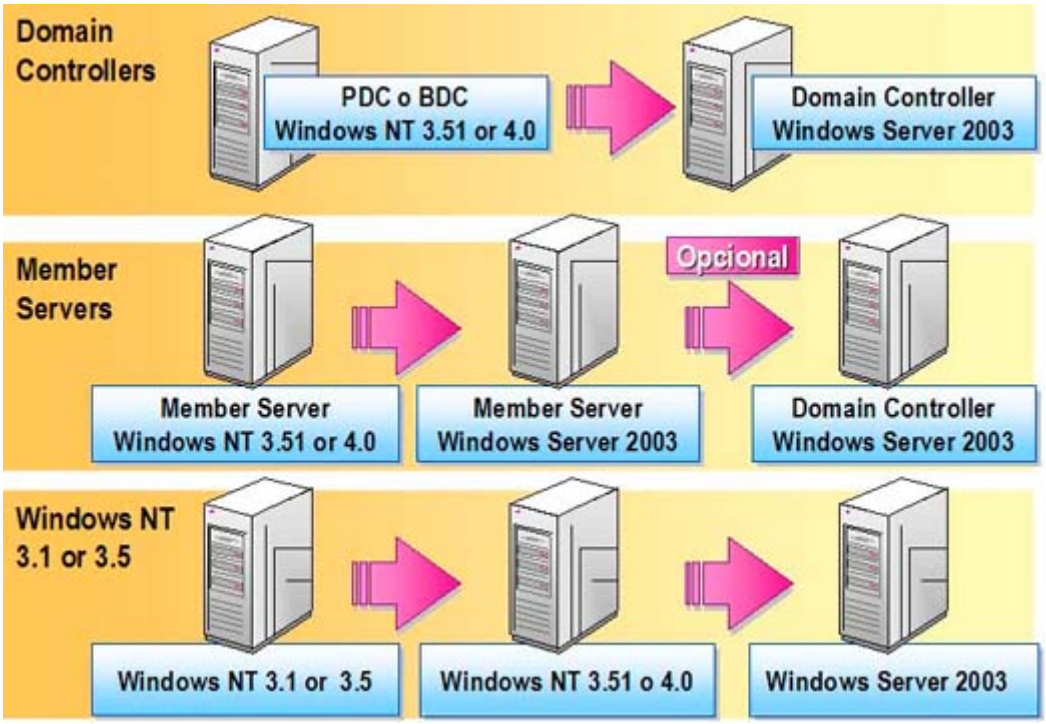
### 2.10. Activando la Copia de Windows Server 2003

Debido a la piratería y a otras formas de uso desautorizado, los compradores no pueden estar siempre seguros de tener una copia genuina de Windows Server 2003. Es por ello que Microsoft desarrolló para Windows Server 2003 la herramienta "Product Activation" para asegurarle que cada instalación de su producto Windows Server 2003 tenga una licencia válida del producto.

**Importante:** Clientes que compran Volume License Agreement no necesitarán activar su producto. Si Usted no tiene un contrato Volume License, tiene 60 días de período de gracia en el cual podrá activar la instalación de su producto. Si expira el período de gracia y Usted no ha terminado la activación aún, todas las características dejarán de funcionar, a excepción de la característica de la activación del producto. Después de instalar Windows Server 2003, se ejecutará el wizard de activación y registración. Usted puede cancelar el wizard y activar Windows Server 2003 más adelante. Para activar Windows Server 2003 usando el Wizard Product Activation:

- Haga click en Start y Activate Windows.
- Ingrese la identificación "product key".
- El wizard intentará establecer una conexión a Microsoft por Internet.
- Si usted no tiene una conexión a Internet pero tiene un módem conectado con una línea telefónica, el wizard detectará el módem e intentará hacer una conexión directa a Microsoft.
- Si la conexión no puede ser establecida, usted puede activar su copia de Windows Server 2003 llamando un representante de clientes de Microsoft.

## 3. Migración desde Windows NT 4.0



A continuación se detalla la migración de Domain Controllers y Member Servers ejecutando Windows NT 4.0 a Windows Server 2003 para sistemas operativos de Server.

| Desde | Resultado |
|---|---|
| Windows NT 3.51 o 4.0 PDC o BDC | Windows Server 2003 Domain Controller |
| Windows NT 3.51 o 4.0 Member Server | Windows Server 2003 Member Server |
| Windows NT 3.1 o 3.5 | Primero debe migrar a Windows NT 3.51 ó 4.0 |

Tenga en cuenta para la migración de Windows NT 3.1/3.5/3.51, los requerimientos de hardware necesarios para Windows Server 2003.

Obtenga más información en:

http://www.microsoft.com/windowsserver2003/upgrading/nt4/default.mspx

### 3.1. Migración de Member Servers

Antes que Usted migre a Windows Server 2003, es importante que haga back up de los archivos críticos para asegurar que sus datos sean preservados si el proceso falla. Para preservar sus archivos críticos y configuraciones deberá realizar las siguientes tareas:

- Resolver los errores listados en Event Viewer
- Hacer Full Backup de todos los discos
- Hacer Backup de la Registry
- Actualizar el Disco de reparación de emergencia (Rdisk)
- Remover el software de protección antivirus

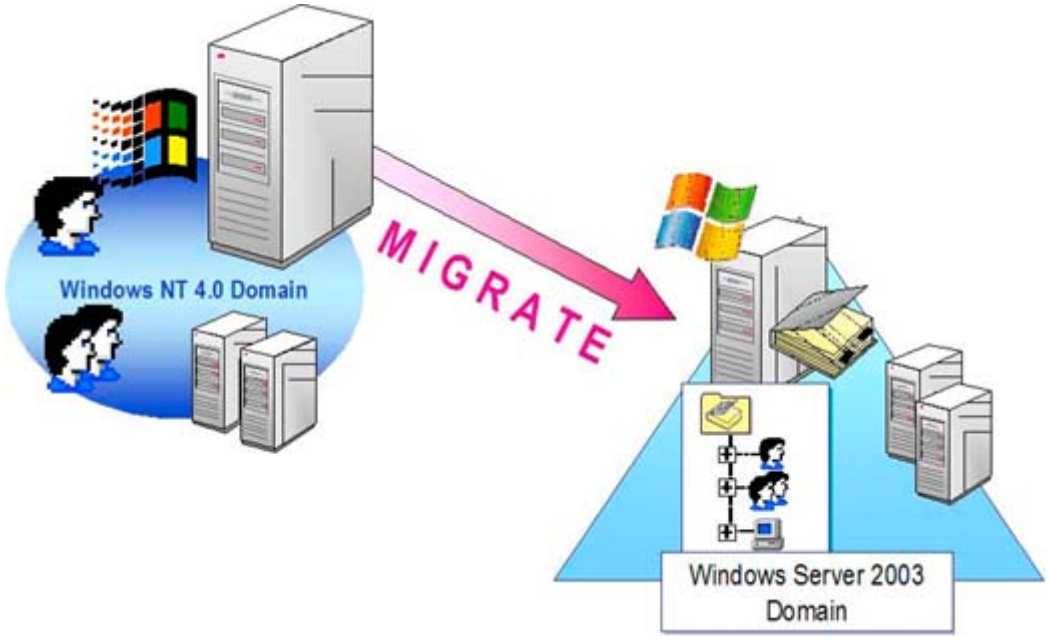
Después de completar estas tareas, introduzca el CD-ROM de Windows Server 2003 y comience el proceso de instalación. Este proceso es similar a una instalación nueva. Si lo realiza desde la red ejecute Winnt32.exe.

**Nota:** Se puede dar el caso que la partición de sistema no tenga espacio para el proceso de migración. No obstante, en el mismo disco Usted posee espacio adicional para obtener información sobre cómo expandir esa partición.

http://support.microsoft.com/default.aspx?scid=kb;en-us;325857

Al finalizar el proceso, su Server pasará a ser un Windows Server 2003 member Server.

### 3.2. Migración de Dominios




Para comprender el proceso de migración, lo dividiremos en dos posibles procesos: Migración Directa ( In-Place) o reestructuración.

### 3.2.1. Terminologías

En la siguiente tabla se enumeran los términos y sus significados relacionados con el proceso de migración:

- ***Domain Migration.*** Es el proceso de mover al usuario, las cuentas de grupo y cuentas las de la computadora de un dominio Windows NT 4.0 a un dominio Windows Server 2003. La migración del dominio se puede realizar haciendo upgrade del dominio Windows NT 4.0 a Windows Server 2003, o creando un nuevo forest Windows Server 2003 y copiando el usuario, el grupo, y las cuentas de la computadoras desde el dominio Windows NT 4.0 al nuevo forest. También se puede alcanzar la migración del dominio usando una combinación de estos dos métodos.
- ***Source Domain.*** Es el dominio desde el cual los Security Principals deben ser migrados.
- ***Target Domain.*** Es el dominio en el cual serán migrados los Security Principals. Un Target Domain puede estar en el mismo forest Windows Server 2003 o en un forest diferente al del Source Domain.
- ***Account Domain.*** Contiene las cuentas de usuarios y grupos en el modelo Multiple Master Domain de Windows NT 4.0.
- ***Resource Domain.*** Es un dominio de Windows NT 4.0 utilizado para file, print Server y otros servicios de aplicaciones. Además, contiene las cuentas principales de computadoras.
- ***Consolidate Domains.*** Sirve para reestructurar un número grande de dominios en un número pequeño.
- ***Levels of domain and forest functionality.*** Es una característica en Windows Server 2003 que proporciona la compatibilidad hacia atrás para los diversos sistemas operativos de Windows que utilizan Active Directory. Windows Server 2003 utiliza niveles del dominio y de la funcionalidad del forest para identificar la funcionalidad que se puede introducir en el dominio y los niveles del forest. La implementación de funcionalidad de dominio o forest habilita para introducir nuevas características en Windows Server 2003, las cuales no se pueden activar hasta que todos los Domain Controllers sean migrados en la organización. De este modo los niveles proveen Backward Compatibility. Los niveles del dominio y de la funcionalidad del forest substituyen la característica del modo de dominio de Windows 2000.
- ***Clone.*** Sirve para crear nuevas cuentas en el Target Domain. Es una copia de las cuentas en el Source domain pero también mantiene el Source Account Primary Security Identifier (SID) en su atributo SID-History. En el único momento que usted puede clonar cuentas es cuando está migrando cuentas entre forest.
- ***SID-History.*** Es un atributo de Active Directory Security Principals que es usado para almacenar SIDs de objetos movidos como cuentas de usuarios y grupos de seguridad.

### 3.2.2. Migración In-Place

Este proceso determina las acciones necesarias para conservar la estructura anterior. Por lo tanto si Usted tenía 4 dominios Windows NT 4.0, al finalizar obtendrá los mismos 4 dominios con la misma estructura en Windows Server 2003.

***El proceso a llevar a cabo incluye:***

- Migración en primer término del PDC de Windows NT 4.0. Tip: Instale un nuevo BDC, retírelo de la red, promueva a PDC e instale Windows Server 2003 en esa computadora.
- A continuación ponga nuevamente en la red esa computadora y despromueva en PDC productivo a BDC.
- Luego migre todos los BDC del Dominio.

La estructura completa es conservada en la nueva estructura Windows Server 2003.

### 3.2.3. Reestructuración de Dominio

Este proceso determina las acciones necesarias para reestructurar la estructura anterior (consolidación de Dominios). Por lo tanto si Usted tenía 4 dominios Windows NT 4.0, al finalizar obtendrá 1 dominio Windows Server 2003 que contendrá todas las cuentas.

***El proceso a llevar a cabo incluye:***

- Migrar en primer término de un PDC de Windows NT 4.0 o instalación de un forest nuevo.
- Utilizar la herramienta Active Directory Migration Tool (ADMT v2) para copiar objetos. Esta herramienta permite conservar el SID-History de los objetos y en esta nueva versión permite la migración de passwords.

**Nota:** ADMT v2 está disponible en el CD-ROM de Windows Server 2003.

Obtenga más información acerca de ADMT:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325851

## 4. Migración desde Windows 2000

Un primer paso es elegir el mejor sistema operativo equivalente al que usted está utilizando actualmente. La siguiente tabla muestra las equivalencias:

| Windows Server 2003 | Windows 2000 Server |
|---|---|
| Standard Edition | Windows 2000 Server |
| Enterprise Edition | Windows 2000 Advanced Server |
| Datacenter Edition | Windows 2000 Datacenter Server |
| Web Edition | No Equivalent |

### 4.1. Migración de Member Servers Windows 2000

Antes que Usted migre a Windows Server 2003, es importante que haga backup de archivos críticos para asegurar que sus datos sean preservados en el caso que el proceso falle. Las siguientes tareas sirven para preservar sus archivos críticos y configuraciones:

- Resolver los errores listados en Event Viewer
- Hacer Full Backup de todos los discos
- Hacer Backup de la Registry
- Actualizar el Disco de reparación de emergencia (Rdisk)
- Remover el software de protección antivirus

Después de completar estas tareas, introduzca el CD-ROM de Windows Server 2003 y comience el proceso de instalación. Este proceso es similar a una instalación nueva, si lo realiza desde la red ejecute Winnt32.exe.

**Nota:** Se puede dar el caso que la partición del sistema no tenga espacio para el proceso de migración, sin embargo, en el mismo disco Usted posee espacio adicional para obtener información sobre cómo expandir esa partición:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325857

Al finalizar el proceso su server pasará a ser un Windows Server 2003 Member Server.

### 4.2. Migración de Dominios

El upgrade de Active Directory puede ser gradual y realizado sin interrupción de las operaciones. Si Usted sigue las recomendaciones del upgrade de dominio, no será necesario poner offline el dominio para migrar los Domain Controllers, los Member Servers o las Workstations.

En Active Directory, un dominio es una colección de computadoras, usuarios y grupos definidos por el administrador. Estos objetos comparten una base de datos común de directorio, Security Policies y Security Relationships con otros dominios. Un forest es una colección de uno o más dominios Active Directory que comparten clases y atributos (schema), información de sites y replicación (configuration) y capacidades de búsquedas forest-wide (global catalog). Los dominios en el mismo forest contienen relaciones de confianza two-way transitivas.

Para prepararse para upgrade de dominios que contienen Windows 2000 Domain Controllers, es recomendable que aplique Service Pack 2 o superior a todos los Domain Controllers Windows 2000.

Antes de migrar un Domain Controller Windows 2000 a Windows Server 2003, o instalar Active Directory en el primer Domain Controller Windows Server 2003, asegúrese que el dominio está preparado.

Estas dos herramientas command-line lo ayudarán en la migración de Domain Controller:

**Winnt32.** Use Winnt32 para comprobar la compatibilidad de upgrade del server.
**Adprep.** Use Adprep en el Schema Operations Master para preparar el forest.

Adprep está contenido en el CD-ROM de Windows Server 2003 en la carpeta I386 o IA64. Tenga en cuenta que esta herramienta modifica el Schema, por lo cual la cantidad de objetos que contenga el Active Directory será el tiempo requerido para completar las operaciones. Por otra parte es aconsejable que corra esta herramienta únicamente en el Schema Master, puesto que en caso de corte de comunicaciones en la red no correrá el riesgo que la operación quede a la mitad del proceso.

#### El proceso a llevar a cabo incluye:

- Ejecutar adprep.exe / foretprep para preparar el forest
- Ejecutar adprep.exe / domainprep para preparar el Dominio
- Migrar los Domain Controllers gradualmente o bien instalar una copia nueva de Windows Server 2003, promoviendo esa instalación a Domain Controller.

Al finalizar estas tareas habrá elevado de versión el Active Directory existente.

Obtenga más información acerca de la migración de Windows 2000

http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/win2k/w2ktows03-2.mspx

### 4.2.1. Práctica 2

Durante esta práctica Usted realizará un proceso de migración de Windows NT 4.0 Member Server a Windows Server 2003 y un proceso de migración de Windows 2000 Member Server a Windows Server 2003.

***Pasos a seguir.***

- Primero instale un Windows NT Server 4.0, en instalación Member Server.
- Siga los pasos descriptos en la práctica 1, iniciando la instalación desde el sistema operativo, es decir, ejecute Winnt32.exe o ejecute la instalación colocando el CD-ROM.

***Resultado:*** Proceso de migración de Windows NT 4.0 a Windows Server 2003

- Instale ahora Windows 2000 Server como Member Server.
- Siga los pasos descriptos en la práctica 1, iniciando la instalación desde el sistema operativo, es decir, ejecute Winnt32.exe o ejecute la instalación colocando el CD-ROM.

**Resultado:** Proceso de migración de Windows 2000 a Windows Server 2003

**Nota:** Recuerde que para realizar estas prácticas puede utilizar el software Connectix Virtual PC.

**Opcional:** Si tiene tiempo puede realizar la misma práctica, desde Windows NT 4.0 PDC y desde Windows 2000 Domain Controller, realizando el proceso de upgrade In-Place.

# Capitulo 3
# Instalación y Configuración de Servicios DHCP, DNS y WINS

## 1. Introducción

Durante este capítulo Usted irá asimilando conocimientos acerca de los servicios de red tales como DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Name System) y DNS (Domain Name System). Este último, en particular, le será de mucha utilidad para el desarrollo del capítulo 4.

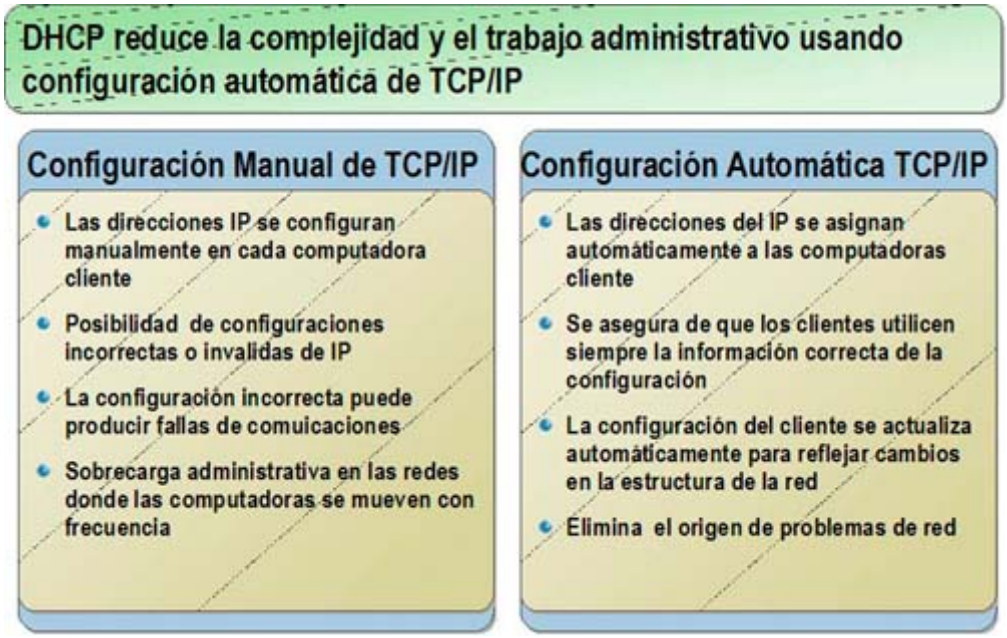
Para la realización de las prácticas contenidas en el presente módulo, necesitará la instalación de Windows Server 2003 que realizó en la práctica 1 del capítulo 2, y una instalación adicional.

***Al finalizar este capítulo Usted tendrá la habilidad de:***

- Describir las características de los servicios DHCP, DNS y WINS.
- Instalar y configurar servicios de red.
- Solucionar problemas de servicios de red.

## 2. DHCP - Dynamic Host Configuration Protocol

### 2.1. ¿Por qué utilizar DHCP?



### 2.1.1. Definición

***Dynamic Host Configuration Protocol (DHCP)*** es un estándar IP para simplificar la administración de la configuración del IP del cliente. El estándar DHCP permite que Usted utilice los servidores de DHCP para manejar la asignación dinámica de las direcciones y la configuración de otros parámetros IP para clientes DHCP en su red.

### 2.1.2. ¿Por qué utilizar DHCP?

En redes TCP/IP, DHCP reduce la complejidad y el trabajo administrativo de re-configurar las computadoras cliente.
Para entender por qué DHCP es útil para configurar clientes TCP/IP, es importante comparar la configuración manual de TCP/IP con la configuración automática que utiliza DHCP.

### 2.1.3. Configuración manual de TCP/IP

Cuando Usted realiza la configuración IP para cada cliente, ingresando manualmente información como la IP address, subnet mask o default gateway, pueden llegar a producirse errores de tipeo, que es probable deriven en problemas de comunicación o problemas asociados a la IP duplicada. Por otra parte, hay carga administrativa adicional en las redes donde las computadoras se mueven con frecuencia de una subnet a otra y, en adición, cuando necesita cambiar un valor IP para varios clientes, tiene que actualizar la configuración IP de cada cliente.

### 2.1.4. Configuración automática TCP/IP

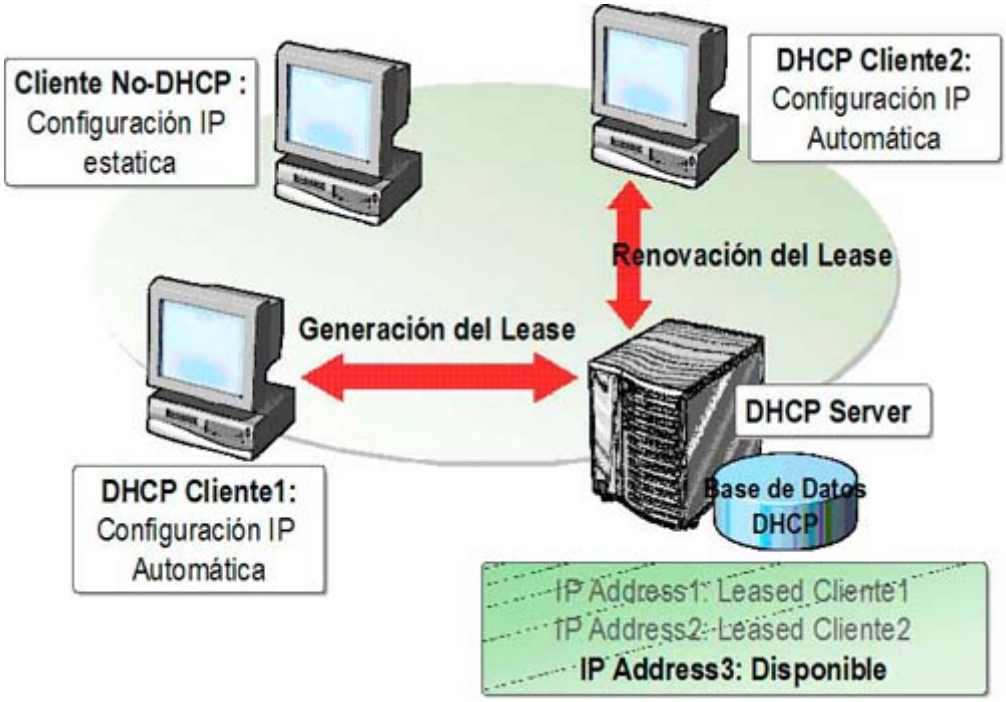
Cuando Usted configura un DHCP Server para dar soporte a clientes DHCP, éste provee automáticamente la información de la configuración a clientes DHCP y también se asegura que los clientes de la red utilicen la configuración correcta. Además, si Usted necesita realizar un cambio en la configuración IP de varios clientes, podrá realizarlo una vez en el DHCP Server, para que el DCHP actualice automáticamente la configuración del cliente reflejando el cambio.

***Ejemplo***

Usted necesita configurar 100 computadoras con la configuración IP, pero sin DHCP no le quedará otra alternativa que configurar manualmente cada una de las computadoras individualmente. A esto hay que sumarle que se tiene que documentar la configuración IP de cada cliente, y que si se tiene que realizar un cambio en la configuración IP de los clientes, también tendría que re-configurarla manualmente en cada uno de ellos.

Pero DHCP tiene la solución a esto. Con DHCP Usted sólo tendrá que agregar la configuración al DHCP Server, que actualiza los 100 clientes de la red. Además, cuando necesite realizar un cambio de configuración IP, el mismo será efectuado una vez solamente en el DHCP Server, requiriendo simplemente que cada cliente TCP/IP renueve su configuración.

## 2.2 ¿Cómo el DHCP asigna direcciones IP?




### 2.2.2.1 Introducción

DHCP permite manejar la asignación de IP de una localización central, y por lo tanto Usted puede configurar el DHCP Server para asignar direcciones de IP a una sola subnet o múltiples subnets. Asimismo, el DHCP Server puede asignar la configuración IP a los clientes en forma automática.

### 2.2.2.2 Definición

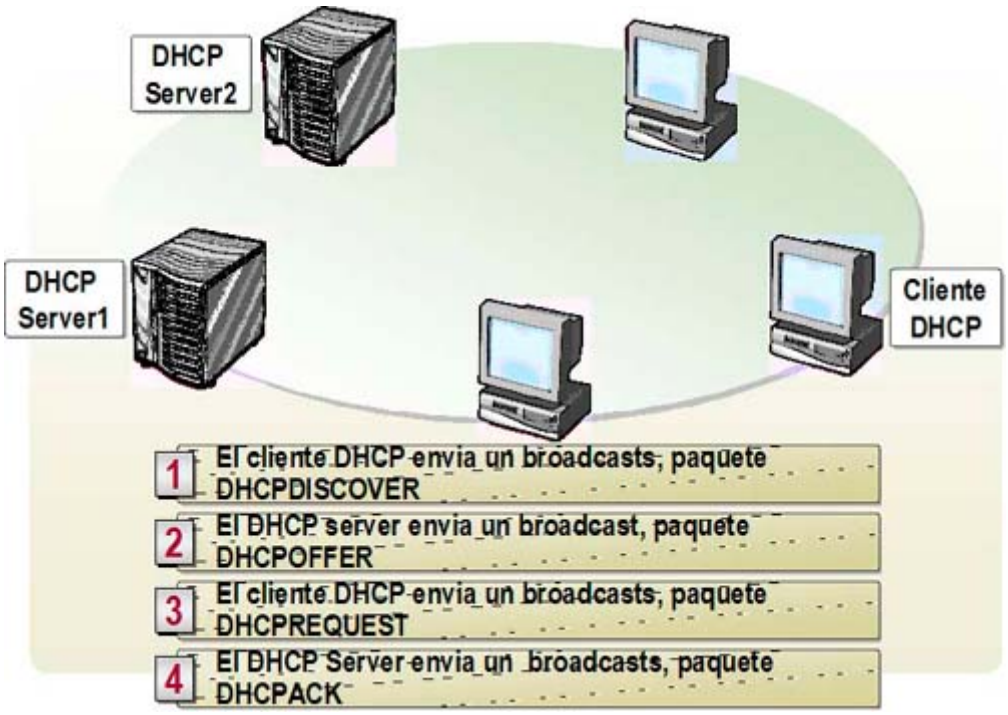
El ***lease*** es el espacio de tiempo en el cual un cliente DHCP puede utilizar una configuración dinámicamente asignada de IP. Antes de la expiración del tiempo de lease, el cliente debe renovarlo u obtener un nuevo lease del DHCP.

### 2.2.2.3 Asignación de direcciones IP

El DHCP administra la asignación y el release de la configuración IP, concediendo la configuración IP al cliente. El estado del DHCP lease depende del tiempo en que el cliente pueda utilizar los datos de la configuración IP antes de liberarla y después de renovar los datos. El proceso de asignar la configuración IP se conoce como ***DHCP Lease Generation Process***, y el proceso de renovar los datos de la configuración IP se conoce como ***DHCP Lease Renewal Process***.

La primera vez que un cliente DHCP se agrega a la red, el mismo debe solicitar la configuración IP al DHCP Server para que, cuando éste reciba la solicitud, el server seleccione una dirección IP del rango de direcciones que el administrador ha definido en el scope. El DHCP Server ofrece la configuración IP al cliente de DHCP. Si el cliente acepta la oferta, el DHCP Server asignará la dirección IP al cliente por un período de tiempo especificado. El cliente entonces utilizará la dirección IP para tener acceso a la red.

### 2.3. ¿Cómo funciona el proceso DHCP Lease Generation?




***El cliente DHCP envía un broadcasts, paquete DHCPDISCOVER para localizar al DHCP Server.*** Este paquete DHCPDISCOVER es el mensaje que los clientes DHCP envían la primera vez que se conectan a la red y solicitan la información IP de un DHCP Server. Existen dos formas de comenzar el proceso DHCP Lease Generation. La primera ocurre cuando una computadora cliente se enciende o se inicia TCP/IP por primera vez, y la segunda ocurre cuando un cliente intenta renovar su lease y recibe una denegación (DHCP NACK). (Por ejemplo, un cliente puede no lograr una renovación cuando Usted lo mueve a otra subnet.)

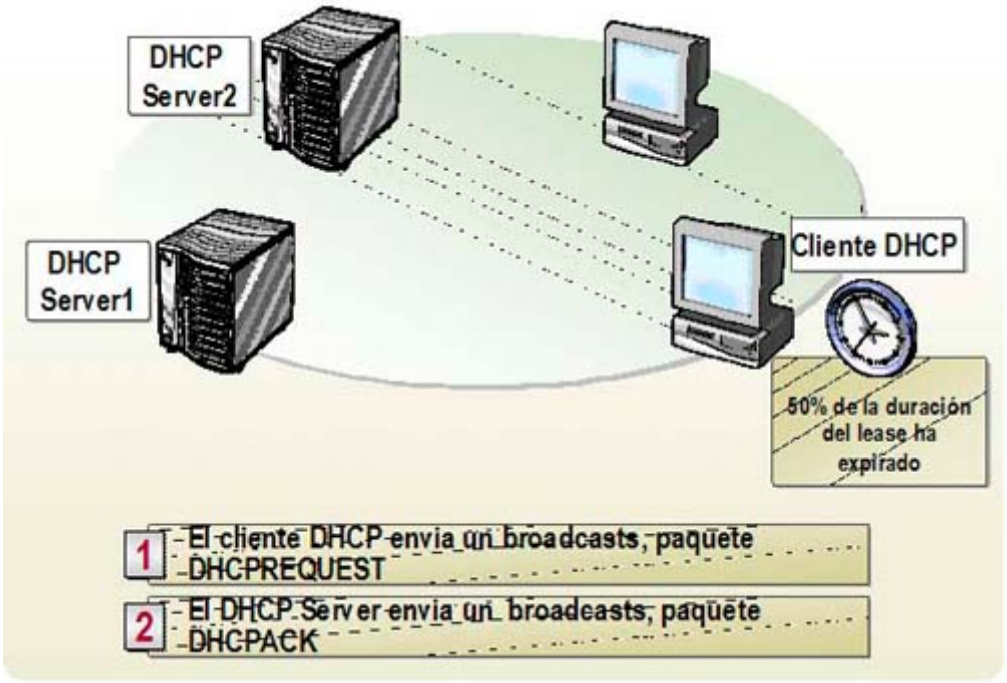
***El DHCP Server envía un broadcast paquete DHCPOFFER al cliente.*** El paquete DHCPOFFER es un mensaje que el DHCP Server utiliza para ofrecer el lease de una dirección IP al cliente, cuando éste se conecta a la red. Cada DHCP Server que responde, reserva la dirección IP ofrecida para no ofrecerla nuevamente a otro cliente DHCP, antes de la aceptación del cliente inicial. Si el cliente no recibe una oferta después de cuatro peticiones, utiliza una IP en la gama reservada a partir del 169.254.0.1 a 169.254.255.254. El uso de una de estas direcciones auto-configuradas IP asegura que los clientes situados en una subnet DHCP Server inaccesible, puedan comunicarse con otros clientes. Mientras tanto el cliente DHCP continúa buscando un DHCP Server disponible cada cinco minutos. Cuando el DHCP Server llegue a estar disponible, los clientes recibirán direcciones válidas IP, permitiendo que esos clientes se comuniquen con clientes en su subnet y en otras también.

***El cliente DHCP envía un broadcasts, paquete DHCPREQUEST.*** El paquete DHCPREQUEST es el mensaje que un cliente envía al DHCP Server para solicitar o renovar su lease de IP. El cliente DHCP responde al primer paquete DHCPOFFER que recibe con un broadcasts de DHCPREQUEST para aceptar la oferta. El paquete DHCPREQUEST incluye la identificación del server que oferta y el cliente que aceptó. Todos los otros DHCP Servers después eliminan sus ofertas y conservan sus direcciones de IP para otros lease.

***El DHCP server envía un broadcast, DHCPACK al cliente.*** El paquete DHCPACK es un mensaje que DHCP Server envía a un cliente como acuse de recibo y finalización del proceso de lease. Este mensaje contiene un lease válido para la dirección IP y la otros datos de configuración IP. Cuando el cliente DHCP recibe el acknowledgment, inicia TCP/IP usando la configuración IP provista por el DHCP Server.

**Nota:** Usted puede ver todo el proceso de lease capturando los paquetes con Network Monitor. Tenga en cuenta que el cliente y el server utilizan los puertos 67 y 68 UDP. Para realizar el proceso en ambientes seguros será necesario que permita la comunicación de esos puertos entre el cliente y el server.

## 2.4 ¿Cómo funciona el proceso DHCP Lease Renewal?




### 2.4.1. Definiciones

***DHCP Lease Renewal Process*** es el proceso por el cual un cliente DHCP renueva o actualiza sus datos de configuración IP con el DHCP Server.

El cliente DHCP renueva la configuración IP antes de la expiración del tiempo de lease. Si el período de lease expira y el cliente DHCP todavía no ha renovado su configuración IP, pierde los datos de la configuración IP y comienza nuevamente el proceso DHCP Lease Generation.

### 2.4.2. Período de Lease

El proceso de Lease Renewal es el resultado del valor de tiempo del lease. El valor de período de lease se asegura que el DHCP mantenga la información IP y que los clientes actualicen o renueven regularmente sus datos de configuración IP. Teniendo DHCP se mantiene esta información e implica que puede administrar el direccionamiento IP desde el DHCP Server. El cliente debe renovar su configuración IP antes de la expiración del período de lease. En los intervalos específicos, un cliente DHCP intenta renovar su lease para asegurarse tener actualizada su configuración. En cualquier momento durante el período de lease, el cliente DHCP puede enviar un paquete de DHCPRELEASE al DHCP Server para liberar la configuración IP y para cancelar el lease restante.

### 2.4.3. Proceso automático "Lease Renewal"

Un cliente DHCP intenta renovar automáticamente su lease al 50% del tiempo de expiración. El cliente DHCP también intenta renovar su lease cada vez que la computadora se reinicie, y para intentarlo envía paquete de DHCPREQUEST al DHCP Server directamente, del cual obtuvo el lease. Si el DHCP Server está disponible, renueva el lease y envía al cliente un paquete de DHCPACK con la nueva duración del lease y cualquier parámetro de configuración actualizado. El cliente actualiza su configuración cuando recibe el acknowledgment. Si el DHCP Server no está disponible, el cliente continuará utilizando sus parámetros actuales de configuración. Si el cliente DHCP no puede renovar su lease la primera vez, entonces el cliente DHCP enviará un broadcasts DHCPDISCOVER para actualizar su lease de la dirección cuando expira al 87.5 % de la duración del lease. En esta etapa, el cliente DHCP acepta el lease que cualquier DHCP Server le ofrezca.

Si el cliente DHCP reinicia su computadora y el DHCP Server no responde al paquete DHCPREQUEST, el cliente DHCP intentará conectar con el Default Gateway. Si esta tentativa falla, el cliente cesará el uso de la dirección IP. Si el DHCP Server responde con un paquete DHCPOFFER para actualizar el lease del cliente, éste puede renovar su lease de acuerdo a la oferta del mensaje del server y continúa la operación. Pero si el lease expiró, el cliente deberá suspender inmediatamente el uso de la dirección IP actual. El cliente DHCP, entonces, comenzará un nuevo proceso de DHCP Lease Discovery, intentando obtener un nuevo lease de una nueva IP. Si el cliente DHCP falla al recibir la IP, el cliente se asignará una dirección usando la asignación automática de IP en el rango 169.254.0.0.

### 2.4.4. Proceso manual Lease Renewal

Si necesita actualizar la configuración DHCP inmediatamente, Usted puede renovar manualmente el lease IP.(Por ejemplo, si quiere que los clientes DHCP obtengan rápidamente la dirección del DHCP Server de un nuevo router instalado en la red, renueve el lease del cliente para actualizar la configuración.)

**Ejemplo:** c:\inconfig /renew

## 2.5. Práctica 1: ¿Cómo agregar el servicio DHCP Server?

Para agregar un DHCP Server, Usted deberá instalar DHCP Service en una computadora corriendo Microsoft® Windows® Server 2003.

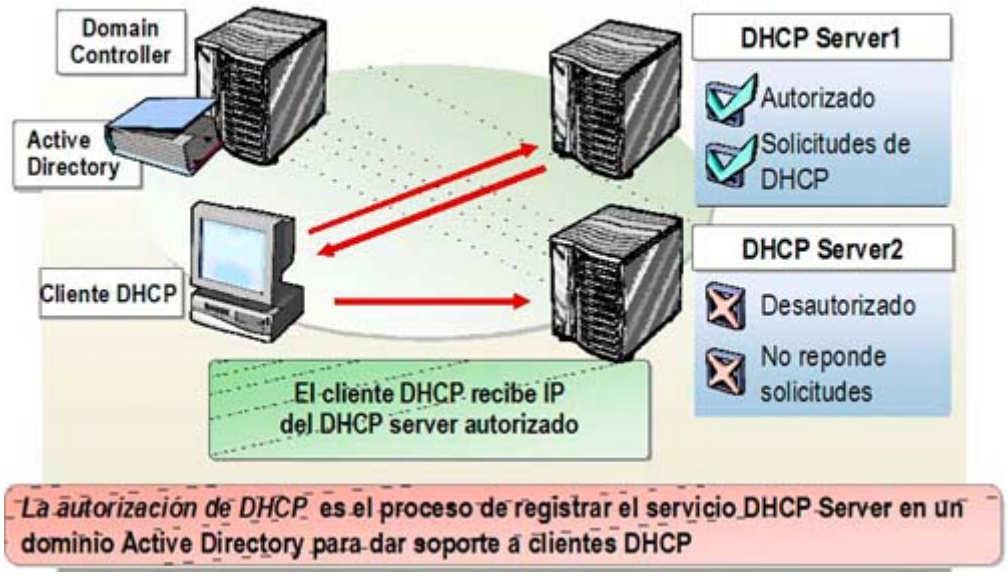
***Antes de agregar el servicio DHCP Server:***

- Verificar que la configuración IP en el servidor esté correcta.
- Verificar que la configuración IP del servidor contenga una dirección IP estática y una subset mask en ambientes ruteados un Default Gateway.
- Verificar que la cuenta de usuario tenga los permisos necesarios.

***Para agregar el servicio DHCP Server deberá:***

1. Iniciar sesión usando una cuenta no-administrativa.
2. Hacer click en ***Start*** y después en ***Control Panel***.
3. Abrir las ***Administrative Tools*** en el Control Panel y hacer click derecho en ***Manage Your Server***, seleccionando ***Run as***.
4. Seleccionar ***The following user*** en el cuadro ***Run As*** e ingresar una cuenta de usuario y password que tenga los permisos apropiados para realizar la tarea, haciendo click en ***OK***.
5. Hacer click ***Add or remove a role*** de la ventana Manage Your Server.
6. Hacer click en ***Next*** de la página ***Preliminary Steps***.
7. Seleccionar ***DHCP server*** en el wizard Configure Your Server, y en ***Next***.
8. Hacer click en ***Next*** de la página ***Summary of Selections***,
9. Hacer click en ***Cancel*** del wizard New Scope para no crear el scope en ese momento.
10. Hacer click en ***Finish*** del wizard Configure Your Server.

## 2.6. ¿Cómo se autoriza el servicio DHCP Server?




### 2.6.1. Definiciones

***La autorización de DHCP*** es el proceso de registrar el servicio DHCP Server en un dominio Active Directory, con el propósito de dar soporte a clientes DHCP. La autorización DHCP es solo para DHCP Servers corriendo Windows Server 2003 y Windows 2000 en Active Directory.

### 2.6.2. ¿Por qué autorizar el DHCP Server?

Autorizar al DHCP Server provee la capacidad de controlar la adición de los DHCP Servers al dominio. La autorización debe ocurrir antes que el DHCP Server pueda otorgar leases a clientes DHCP. Solicitar la autorización de DHCP Servers previene que DHCP Servers desautorizados ofrezcan direcciones IP inválidas a clientes.

Si Usted está configurando un DHCP Server, la autorización debe ocurrir como parte del dominio Active Directory. Si Usted no autoriza el DHCP Server en Active Directory, el servicio DHCP no se podrá iniciar correctamente y entonces el DHCP Server no podrá responder a los pedidos de clientes. El DHCP Server controla el direccionamiento IP enviado a los clientes DHCP en la red. Si el DHCP

Server se configura incorrectamente, los clientes recibirán una configuración incorrecta de direccionamiento IP.

### 2.6.3. ¿Por qué un DHCP Server autorizado requiere Active Directory?

Active Directory se requiere para autorizar un DHCP Server. Con Active Directory, los DHCP Servers no autorizados no pueden responder a los pedidos de clientes. El servicio DHCP Server, en un server miembro de Active Directory, verifica su registración con un Domain Controller de Active Directory. Si el DHCP Server no está registrado, el servicio no se iniciará y consecuentemente el DHCP Server no asignará direcciones a clientes.

### 2.6.4. Stand-alone DHCP Server

Bajo ciertas circunstancias, un DHCP Server corriendo Windows 2000 o Windows Server 2003, se inicia si incluso no está autorizado. Si el DHCP Server corriendo Windows Server 2003 o Windows 2000 está instalado como stand-alone server no es miembro de Active Directory. Y si está situado en una subnet donde DHCPINFORM no será transmitido a otros DHCP Servers autorizados, el servico DHCP Server inicializará y proveerá leases a clientes en la subnet.

Un stand-alone server corriendo Windows 2000 o Windows Server 2003 envía un paquete broadcast DHCPINFORM. Si no hay respuesta al paquete DHCPINFORM, entonces el servicio DHCP Server inicializará y comenzará a atender a los clientes. Si un DHCP Server autorizado recibe un paquete DHCPINFORM, responde con un paquete DHCPACK y entonces el servicio DHCP Server parará. Un stand-alone DCHP Server continuará funcionando si recibe un DHCPACK de otro DHCP Server que no sea miembro de Active Directory.

## 2.7. Práctica 2: ¿Cómo autorizar el servicio DHCP Server?

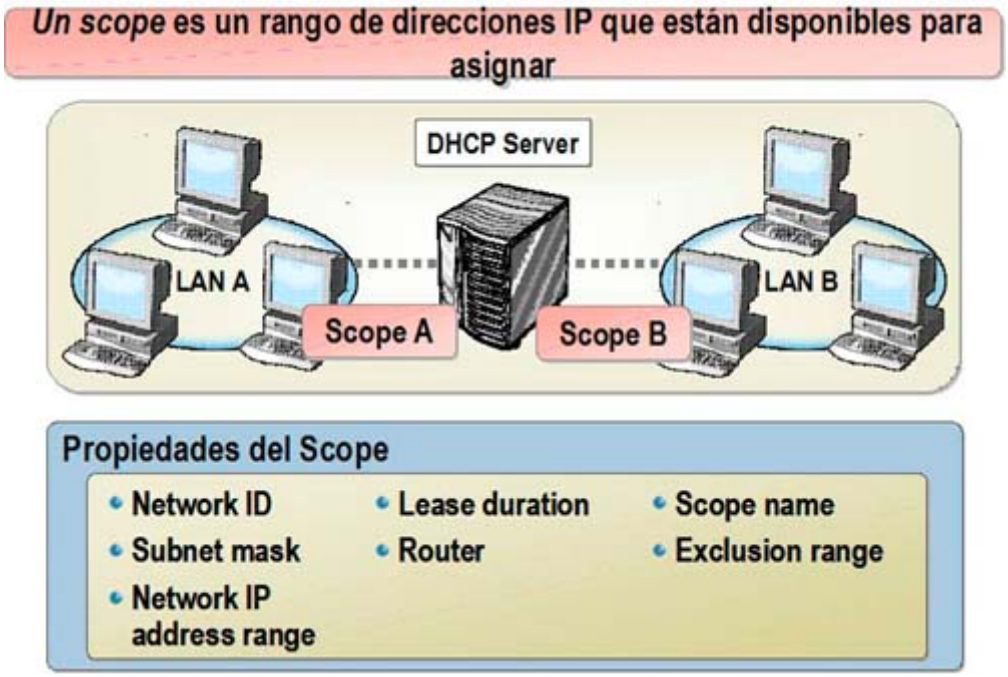
**IMPORTANTE:** No realice esta práctica hasta haber terminado la teoría y la práctica del Capitulo 4.

Para autorizar el servicio DHCP Server, un miembro del grupo Enterprise Administrators lo agrega a una lista de DHCP Servers autorizados, los cuales pueden dar servicio a clientes DHCP en el dominio. El proceso de autorización funciona solamente con servers corriendo Windows Server 2003 y Windows 2000 en un dominio. La autorización no es posible si los DHCP Servers corren versiones anteriores como Microsoft Windows NT® u otros software DHCP Server.

***Para autorizar el servicio DHCP Server deberá:***

1. Abrir la consola DHCP.
2. Seleccionar el server en la consola
3. Hacer click en ***Authorize*** del menú ***Action***,
4. Para verificar que el DHCP server esté autorizado: en la consola, presionar F5 para refrescar la vista, y verificar que el DHCP Server ahora se visualice con una flecha verde hacia arriba.

## 2.8. ¿Qué son los DHCP Scopes?




### 2.8.1. Definición

Un ***scope*** es un rango de direcciones válidas IP que están disponibles para asignar a computadoras cliente en una subnet en particular. Usted puede configurar un scope en el DHCP Server para determinar el pool de direcciones IP que ese server asignará a clientes.

Los scopes determinan las direcciones IP que se asignan a los clientes. Usted debe definir y activar un scope antes que los clientes puedan usar el DHCP Server para una configuración dinámica TCP/IP. Asimismo puede configurar tantos scopes en el DHCP Server como lo necesite para su ambiente de red.

### 2.8.2. Propiedades de Scope

***Un scope tiene las siguientes características:***

- ***Network ID:*** El Network ID para el rango de direcciones IP
- ***Subnet mask:*** La subnet mask para el Network ID
- ***Network IP address range:*** El rango de direcciones IP disponibles para los clientes
- ***Lease duration:*** El período de tiempo que el DHCP Server asigna a la dirección del cliente
- ***Router:*** La dirección del Default Gayeway
- ***Scope name:*** Identificador para propósitos administrativos
- ***Exclusion range:*** El rango de direcciones IP en el scope excluidas para la asignación.

Cada subnet puede tener un DHCP scope que contenga un solo y continuo rango de direcciones IP. Direcciones específicas o grupos de direcciones se pueden excluir del rango del DHCP scope. En general, solamente un scope puede ser asignado a una subnet. Si más de un scope se requiere en una subnet, los scopes deberán crearse primero y luego combinarse en un superscope.

## 2.9. Práctica 3: ¿Cómo configurar un DHCP Scope?

***Para configurar un DHCP scope:***

1. Abrir la consola DHCP.
2. Hacer click en el DHCP Server de la consola.
3. Hacer click en ***New Scope*** del menú ***Action***.
4. Hacer click en ***Next*** del ***New Scope Wizard***.
5. Configurar el ***Nombre*** y ***Descripción*** en la página ***Scope Name***.
6. Configurar, en la página ***IP Address Range***, la dirección IP inicial 192.168.1.1, la dirección IP final 192.168.1.254 y la ***Subnet mask*** 255.255.255.0.
7. Configurar, en la página ***Add Exclusions***, la dirección IP inicial 192.168.1.20 y la dirección IP final 192.168.1.30, si es aplicable.
8. Configurar, en la página ***Lease Duration***, los ***Días***, ***Horas*** y ***Minutos***. (El default es 8 días).
9. Configurar ***DHCP Options*** y seleccionar ***No, I will configure these options later***.
10. Click ***Finish*** en la página ***Completing the New Scope Wizard***.

***Para activar el DHCP scope:***

Hacer click derecho sobre el scope de la consola, y en Activate

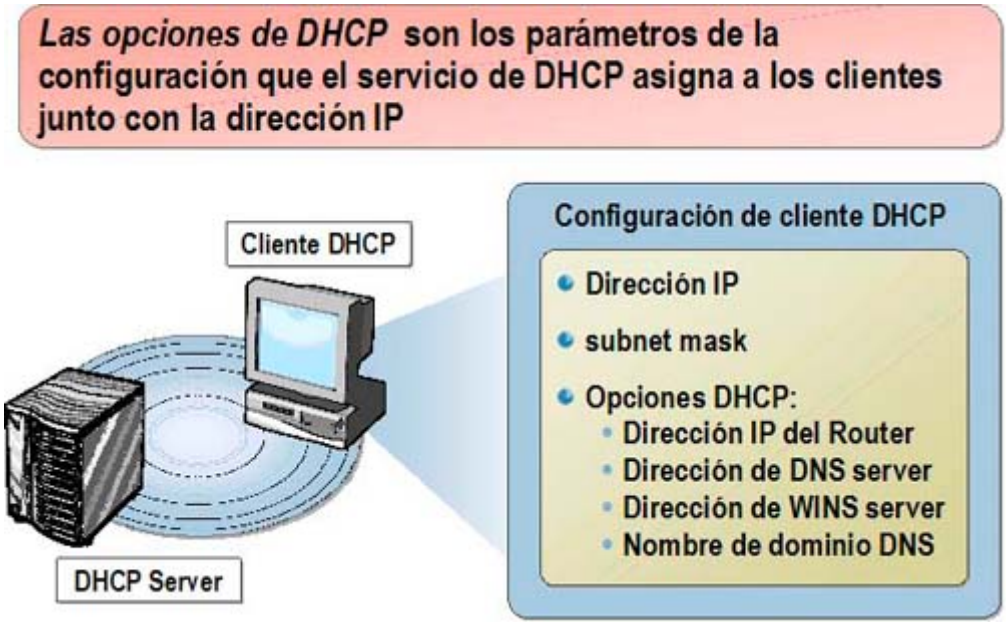
## 2.10 ¿Qué es una reserva DHCP?

***Una reserva*** es una dirección IP permanente reservada a un cliente específico. Usted puede reservar una dirección IP permanente a un dispositivo en la red. La reserva se realiza a la dirección MAC del dispositivo.

### 2.10.1 Práctica 4: Actividades para configurar una reserva DHCP:

1. Abrir la consola DHCP.
2. Hacer click en ***Reservations*** de la consola,
3. Hacer click en ***New Reservation*** del menú ***Action***
4. Ingresar, en el cuadro ***New Reservation***, los valores siguientes:
   a. Nombre de la reserva
   b. Dirección IP
   c. Dirección MAC (sin guiones)
   d. Descripción
5. Seleccionar, en ***Supported types***, una de las opciones siguientes:
   a. Both
   b. DHCP only
   c. BOOTP only
6. Hacer click en ***Add*** del cuadro ***New Reservations***, y después en ***Close***.

## 2.11. ¿Qué son las opciones de DHCP?




***Las opciones de DHCP*** son los parámetros de configuración que un servicio de DHCP asigna a los clientes cuando asigna la dirección IP.

### 2.11.1. Opciones comunes de DHCP

***Router (Default Gateway):*** Es la dirección de cualquier Default Gateway o router. El router se refiere comúnmente como Default Gateway.
***Domain name:*** Un Domain Name DNS define el dominio DNS al cual pertenece una computadora cliente. La computadora cliente puede utilizar esta información para actualizar el DNS Server de modo que otras computadoras puedan localizar al cliente.
***DNS and WINS Servers:*** Son las direcciones de los DNS y WINS Servers para los clientes, a utilizar en la comunicación de red.

## 2.12. Práctica 5: ¿Cómo configurar opciones de DHCP?

***Para configurar una opción de DHCP Server deberá:***

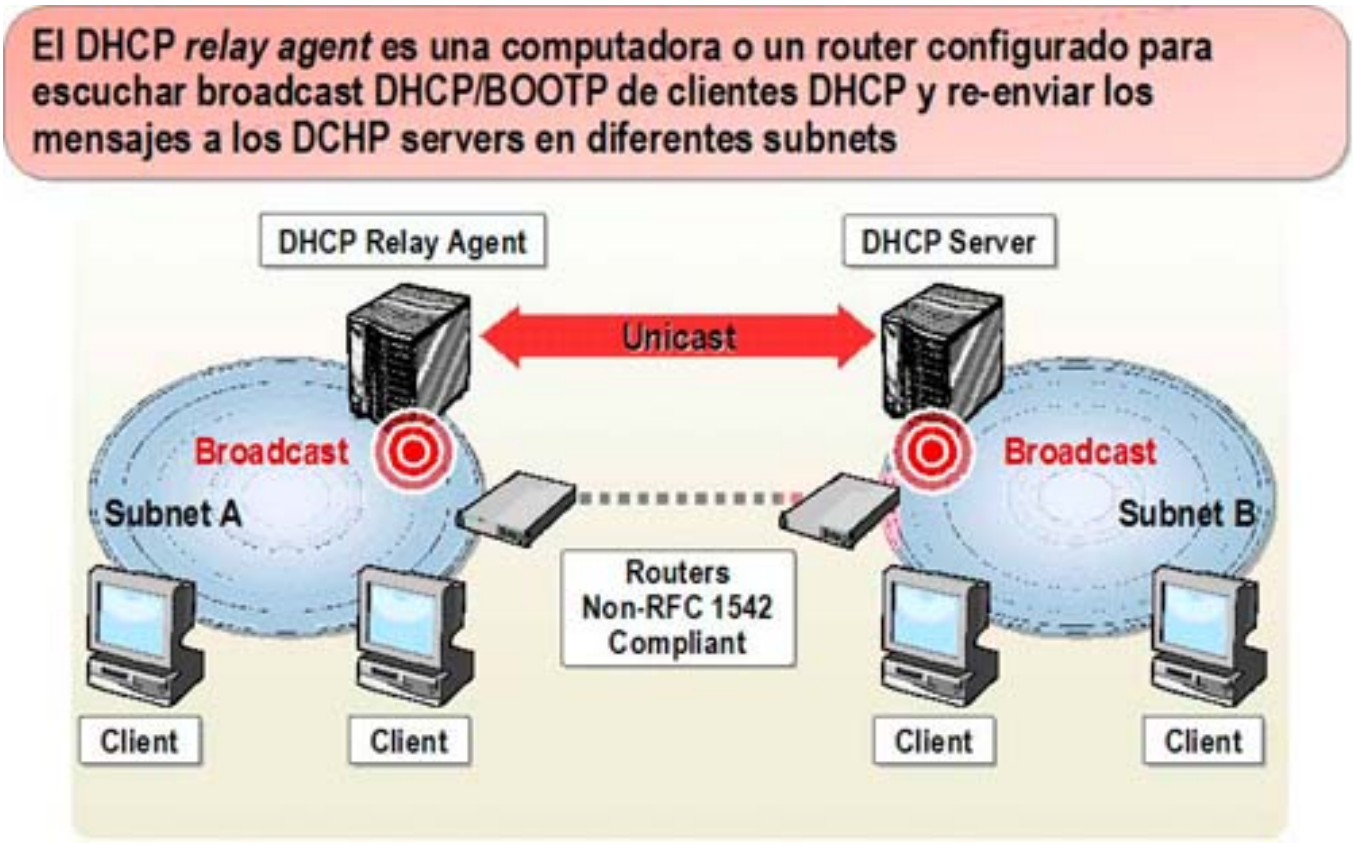
1. Abrir la consola DHCP.
2. Hacer click en ***Server Options*** de la consola, bajo el nombre del server
3. Hacer click en ***Configure Options*** del menú ***Action***.
4. Seleccionar la opción que Usted desea configurar en el cuadro ***Server Options*** de la lista ***Available Options***.
5. Completar, bajo ***Data entry***, la información que se requiere para configurar esta opción.
6. Hacer click en ***OK*** del cuadro ***Server Options***.

***Para configurar un scope DHCP deberá:***

1. Abrir la consola DHCP y bajo el scope apropiado, hacer click en ***Scope Options***.
2. Hacer click en ***Configure Options*** del menú ***Action***
3. Seleccionar, en el cuadro ***Scope Options***, la opción que usted desea configurar de la lista ***Available Options***

4. Completar, bajo ***Data entry***, la información que se requiere para configurar esta opción.
5. Hacer click en ***OK*** del cuadro ***Scope Options***.

## 2.13. ¿Qué es el DHCP Relay Agent?



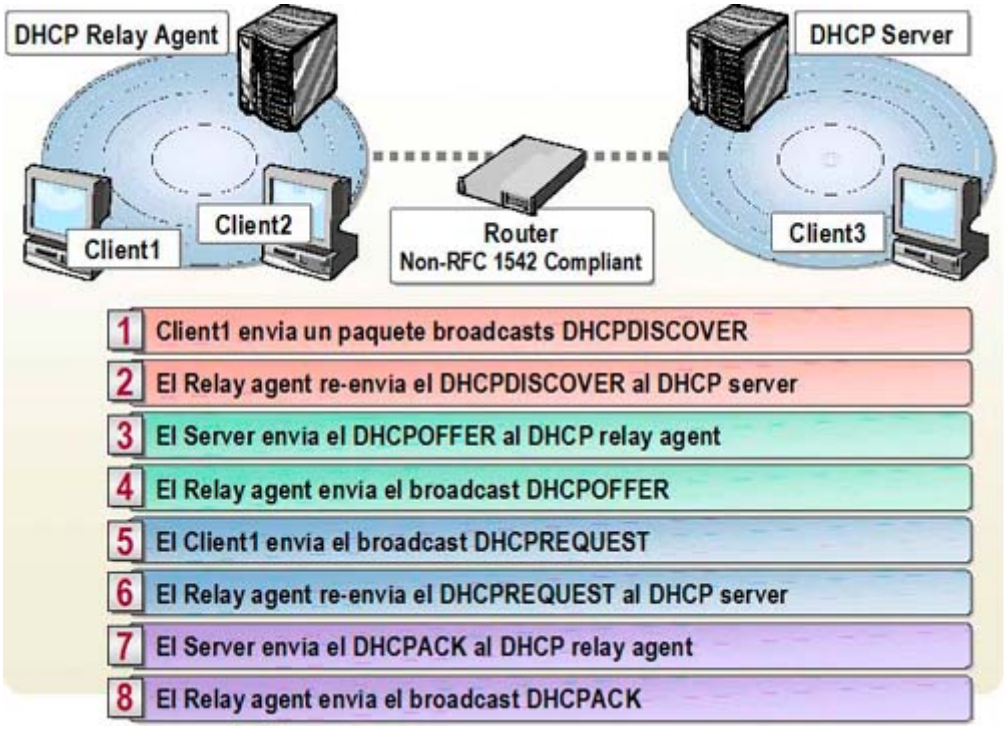

### 2.13.1. Definición

El ***DHCP Relay Agent*** es una computadora o router configurado para escuchar broadcast DHCP/BOOTP de clientes DHCP y reenviar esos mensajes a los DCHP Servers en diferentes subnets. DHCP/BOOTP Relay Agents es parte de los estándares DHCP y BOOTP, y funciona según los documentos estándar ***Request for Comments*** (RFCs) que describen el diseño del protocolo y el comportamiento relacionado.

Un ***RFC 1542-Compliant Router*** es un router que soporta el reenvío de tráfico DHCP broadcast.

Los clientes DHCP utilizan broadcasts para obtener el lease del DHCP Server. Los Routers normalmente no pasan broadcasts excepto que estén configurados específicamente para dejarlos pasar. Por lo tanto, sin configuración adicional, los DHCP Servers solo proveen direcciones IP a clientes en su subset local. Para que Usted pueda asignar direcciones a clientes en otros segmentos, deberá configurar la red para que los DHCP broadcasts puedan llegar desde el cliente al DCHP Server. Esto se puede hacer de dos maneras: configurando los routers que conectan las subnets para dejar pasar DHCP broadcasts, o configurando DCHP Relay Agents. Windows Server 2003 soporta el servicio Routing and Remote Access configurado para funcionar como DHCP Relay Agent.

## 2.14. ¿Cómo funciona el DHCP Relay Agent?




El DHCP Relay Agent soporta el proceso Lease Generation entre el cliente DHCP y el DHCP Server, cuando se separan por un router. Esto habilita al cliente DHCP para recibir una dirección IP del DHCP Server.

***Los siguientes pasos describen el funcionamiento de DHCP Reaky Agent:***

1. El cliente DHCP envía un paquete broadcast DHCPDISCOVER.
2. El DHCP Relay Agent, desde la subnet del cliente, reenvía el mensaje DHCPDISCOVER al DHCP Server usando unicast.
3. El DHCP Server usa unicast para enviar el mensaje DHCPOFFER al DHCP Relay Agent.
4. El DHCP Relay Agent envía un paquete broadcast DHCPOFFER al cliente DHCP en su subnet.
5. El cliente DHCP envía un paquete broadcast DHCPREQUEST.
6. El DHCP Relay Agent, desde la subnet del cliente, reenvía el mensaje DHCPREQUEST al DHCP Server, usando unicast.
7. El DHCP Server usa unicast para enviar el mensaje DHCPACK al DHCP Relay Agent.
8. El DHCP Relay Agent envía un paquete broadcast DHCPACK al cliente DHCP en su subnet.

### 2.14.1 Práctica 6: ¿Cómo configurar el DHCP Relay Agent?

***Para agregar un DHCP Relay Agent deberá:***

1. Abrir la consola Routing and Remote Access.
2. Hacer click derecho en el server y después en ***Configure and Enable Routing and Remote Access***.
3. Hacer click en Next de la pantalla del wizard ***Welcome to the Routing and Remote Access Server Setup Wizard***.
4. Seleccionar ***Custom configuration*** en la página ***Configuration***, y hacer click en ***Next***.
5. Seleccionar ***LAN routing*** en la página ***Custom Configuration*** y hacer click en ***Next***.
6. Hacer click en ***Finish*** de la página ***Completing the Routing and Remote Access Server Setup Wizard***.
7. Hacer click en ***Yes*** del cuadro de advertencia de ***Routing and Remote Access***, para iniciar el servicio.
8. Hacer click en ***Finish*** de la página ***This Server is Now a Remote Access/VPN Server***
9. Expandir el server y el ***IP Routing*** en la consola, y seleccionar ***General***.
10. Hacer click derecho en ***General*** y después en ***New Routing Protocol***.
11. Hacer click en ***DHCP Relay Agent*** del cuadro ***New Routing Protocol*** y después en ***OK***.

***Para configurar la dirección IP del DHCP Server en el DHCP Relay Agent deberá:***

12. Abrir la consola Routing and Remote Access.
13. Seleccionar ***DHCP Relay Agent*** en la consola.
14. Hacer click derecho en ***DHCP Relay Agent*** y después en ***Properties***.
15. Ingresar la dirección IP del DHCP Server al que quiere enviar los pedidos DHCP, en ***General*** del campo ***Server address***.
16. Hacer click en ***Add***, y después en ***OK***.

***Para habilitar el DHCP Relay Agent en una interfase del router deberá:***

17. Abrir la consola ***Routing and Remote Access***.
18. Seleccionar ***DHCP Relay Agent*** en la consola
19. Hacer click derecho en ***DHCP Relay Agent*** y después en ***New Interface***.
20. Seleccionar la interfase donde quiere habilitar el DHCP Relay Agent, y después hacer click en ***OK***.
21. Verificar si está seleccionado el cuadro ***Relay DHCP packets*** en ***General*** del cuadro ***DHCP Relay Properties***, en ***General***.

Para obtener más información acerca de DHCP:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323416

http://support.microsoft.com/default.aspx?scid=kb;en-us;325473

http://support.microsoft.com/default.aspx?scid=kb;en-us;306104

http://support.microsoft.com/default.aspx?scid=kb;en-us;323360

http://support.microsoft.com/default.aspx?scid=kb;en-us;323355

## 3. Descripción de Domain Name System

DNS es un servicio de resolución de nombres que resuelve direcciones legibles (como www.microsoft.com) en direcciones IP (como 192.168.0.1).

***Domain Name System (DNS)*** es una base de datos jerárquica distribuida, que contiene mapeos de nombres de host DNS a direcciones IP. DNS habilita la localización de computadoras y servicios usando nombres alfanuméricos, más fáciles de recordar. DNS también habilita la localización de servicios de red, como E-mail Servers y Domain Controllers en Active Directory®.

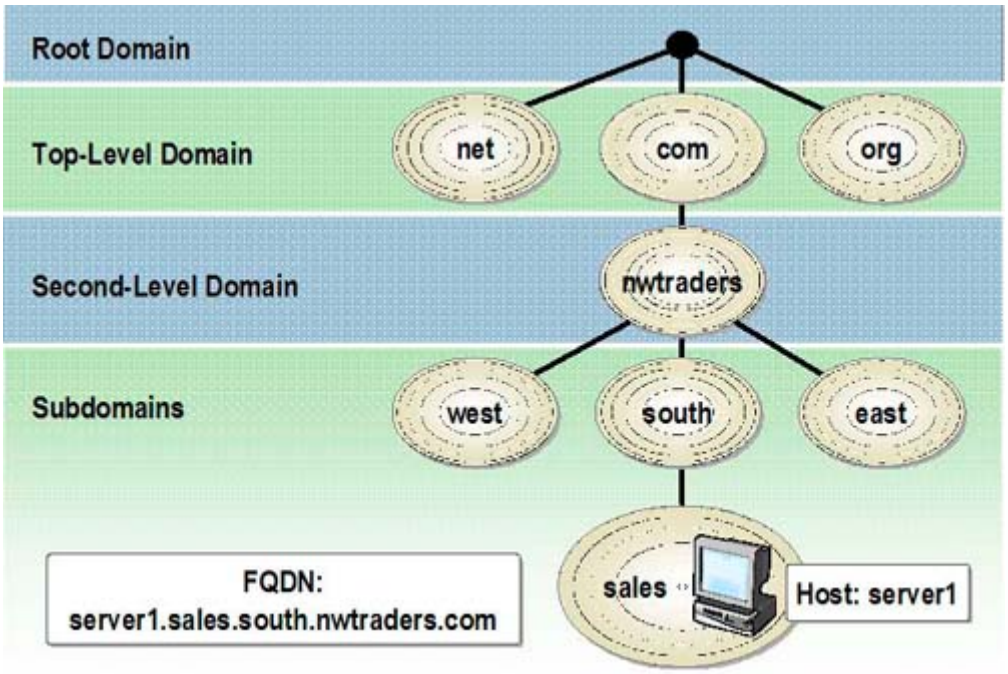
Con DNS, los nombres de host residen en una base de datos distribuida en múltiples servers, disminuyendo la carga en un servidor y la capacidad para administrar este sistema de nombres. Asimismo, dado que se distribuye la base de datos de DNS, su tamaño es ilimitado y el funcionamiento no se degrada cuanto más servidores se agregan.

InterNIC es responsable de delegar la responsabilidad administrativa de porciones del Namespace de dominio, y también de registrar nombres de dominio. Estos últimos son administrados a través del uso de la base de datos distribuida y almacenada en Name Servers, localizados en toda la red. Cada Name Server contiene archivos de base de datos que poseen información para una región, dominio etc., creando así la jerarquía.

Para obtener más información acerca de InterNic:

http://www.internic.net

### 3.1 ¿Qué es el Domain Namespace?




El ***Domain Namespace*** es un árbol de nombres jerárquico que utiliza DNS para identificar y localizar un host en un dominio dado, concerniente a la raíz del árbol. Los nombres en la base de datos DNS establecen una estructura lógica llamada Domain Namespace, que identifica la posición de un dominio en el árbol y su dominio superior. La convención principal es simplemente ésta: para cada nivel de dominio, un período (.) se utiliza para separar a cada descendiente del subdominio y de su dominio de nivel superior.

El ***Fully Qualified Domain Name (FQDN)*** es el nombre de dominio DNS que indica con certeza la localización del host al que se refiere, y su ubicación en el Domain Namespace.

### 3.1.1 Práctica 7: ¿Cómo instalar el servicio DNS Server?

Para agregar un DNS Server, Usted debe instalar DNS service en una computadora corriendo Microsoft® Windows® Server 2003.

***Antes de agregar el servicio DNS Server deberá:***

- Verificar que la configuración IP en el servidor esté correcta.
- Verificar que la configuración IP del servidor contenga una dirección IP estática, una subnet mask y un Default Gateway en ambientes ruteados.
- Verificar que la cuenta de usuario tenga los permisos adecuados.

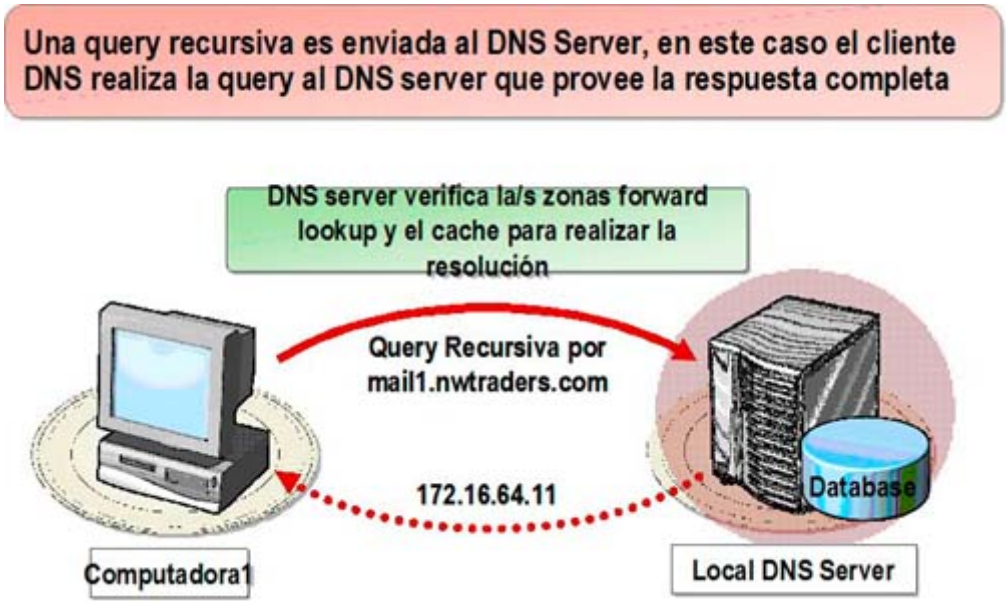
***Para agregar el servicio DNS Server deberá:***

1. Iniciar sesión usando una cuenta no-administrativa.
2. Hacer click en ***Start*** y después en ***Control Panel***.
3. Abrir las ***Administrative Tools*** en el ***Control Panel*** y hacer click derecho en ***Manage Your Server***, seleccionando ***Run as***.
4. Seleccionar ***The following user*** en el cuadro ***Run As***, ingresar una cuenta de usuario y password que tenga los permisos apropiados para realizar la tarea, y hacer click en ***OK***.
5. Hacer click en ***Add or remove a role*** de la ventana Manage Your Server.
6. Hacer click en ***Next*** de la página ***Preliminary Steps***.
7. Seleccionar ***DNS server*** en el wizard ***Configure Your Server***, y hacer click en ***Next***.
8. Hacer click en ***Next*** de la página ***Summary of Selections***,
9. Ingresar el CD Microsoft Windows Server 2003, si se lo pide.
10. Hacer click en ***Cancel*** de la página ***Welcome to the Configure a DNS Server Wizard***,
11. Hacer click en ***Finish*** de la página ***Configure Your Server wizard***.

## 3.2 ¿Qué es una Query DNS?

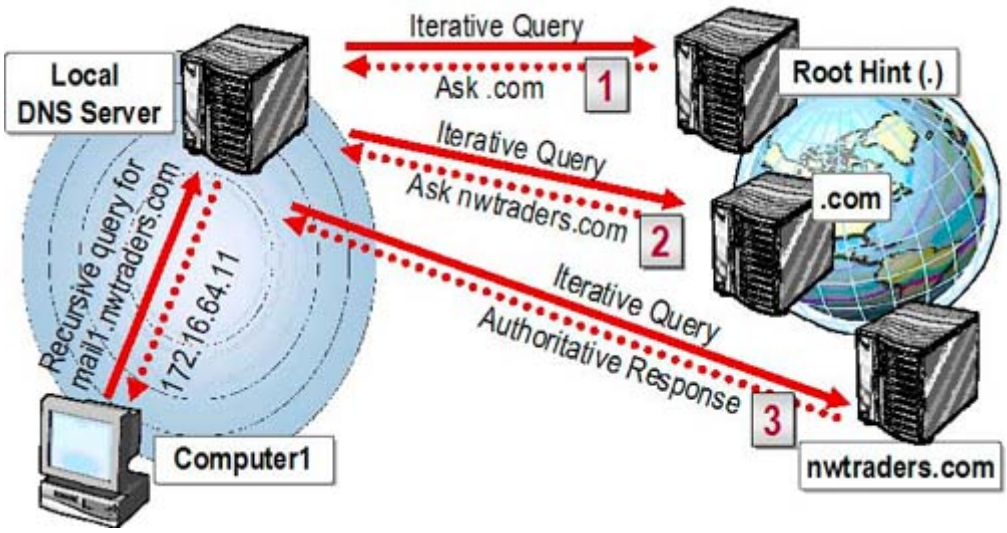
Una ***Query*** es una solicitud de resolución de nombre enviado a un DNS Server. Hay dos tipos de Query: Recursiva e Iterativa.

### 3.2.1 ¿Cómo funciona una Query Recursiva?




Una ***Query Recursiva*** es una solicitud de resolución al DNS Server, en el caso que el cliente realice la Query directamente al DNS Server. La única respuesta aceptable a una Query Recursiva es la respuesta completa o la respuesta en donde el nombre no puede ser resuelto. Una Query Recursiva nunca se redirecciona a otro DNS Server. Si el DNS consultado no obtiene la respuesta de su propia base o del cache o de otros DNS, la respuesta es un error, indicando que no puede resolver el nombre.

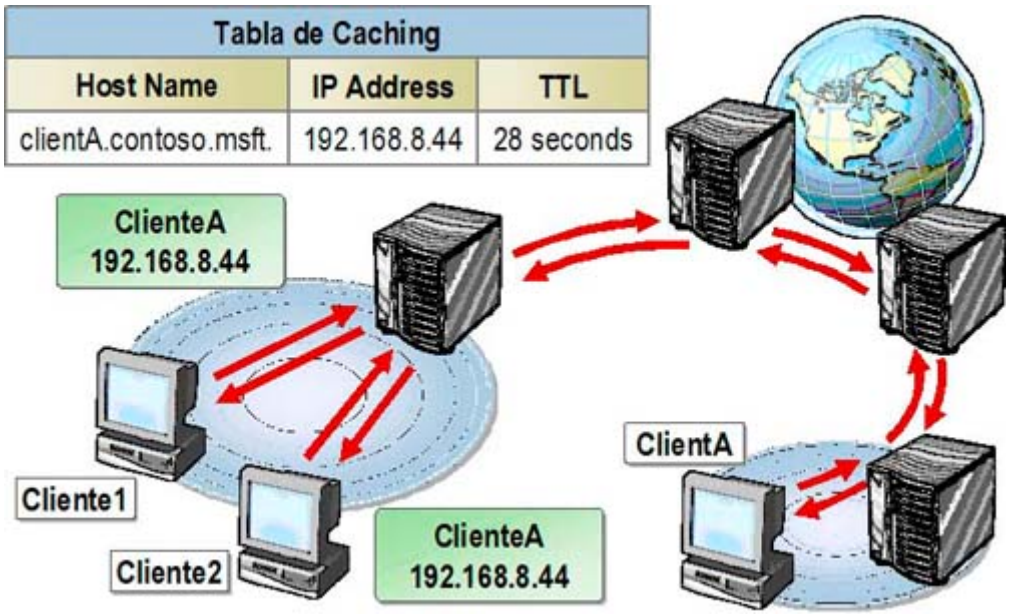
### 3.2.2 ¿Cómo funciona una Query Iterativa?




A diferencia de las Querys Recursivas, cuando un cliente realiza un pedido de resolución y el DNS Server no obtiene la respuesta de su propia base o del cache, la Query Iterativa consulta a otros DNS Servers en nombre del cliente para devolver la respuesta. Ejemplo: si usted necesita acceder a un sitio Web en Internet, normalmente consultaría al DNS de su ISP, y éste último se encargaría de

contactar a otros DNS Servers hasta lograr la respuesta. Pero analice lo siguiente: es imposible en Internet que el DNS de su ISP contenga todas las resoluciones posibles en toda la red Internet, y por eso las bases de DNS se distribuyen y se resuelven nombres de forma Iteractiva.

### 3.2.3 ¿Cómo funciona el caching de DNS Server?




***Caching*** es el proceso de almacenar la información reciente temporalmente, y resulta en un subsistema especial de la memoria para un acceso más rápido.

Cuando un server está procesando una Query Recursiva, puede ser que se requiera enviar varias Querys para encontrar la respuesta definitiva. En el peor de los casos para resolver un nombre, el server local comienza en el Root DNS y trabaja hacia abajo hasta que encuentra los datos solicitados.

El server guarda la información de la resolución en su cache por un tiempo determinado. Este periodo de tiempo se denomina Time to Live (TTL) y es especificado en segundos. El administrador del server que contiene la primary zone donde están los datos, decide el valor del TTL. Cuanto más pequeño sea el valor del TTL, le ayudará a mantener datos más consistentes en caso de cambios. Sin embargo, esto también generará más carga de trabajo sobre el Name Server.

Después que el DNS Server guarda en cache los datos, el TTL comienza a decrecer hacia abajo hasta llegar a 0 (zero) y en ese punto el registro es eliminado del cache de DNS Server. Mientras el valor de TTL está activo, el DNS Server resuelve los pedidos utilizando el registro de cache.

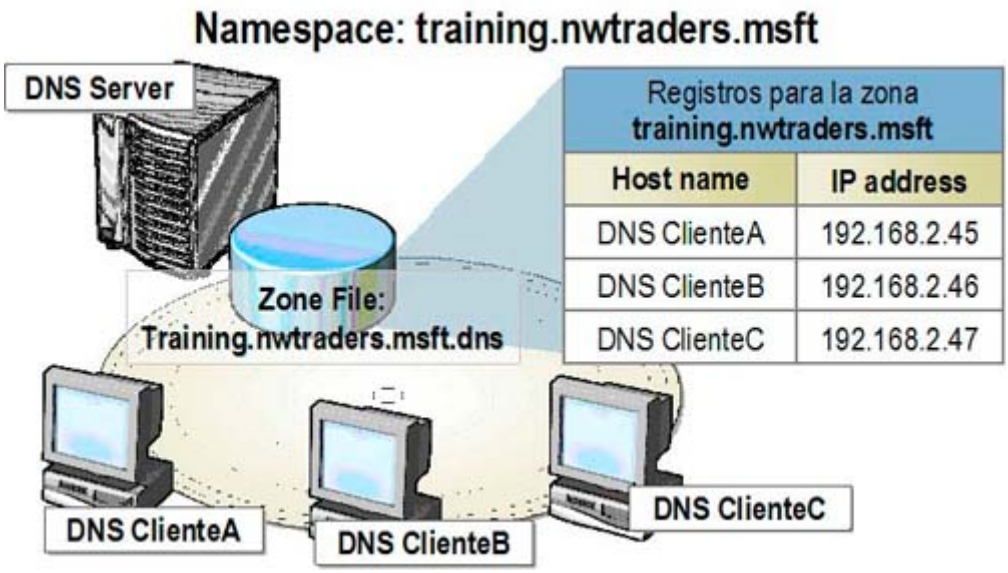
### 3.3. Práctica 8: ¿Cómo configurar propiedades del servicio DNS Server?

Para configurar propiedades del servicio DNS Server, Usted necesita actualizar los Root Hints en el DNS Server. Los Root Hints determinan si su server consulta a los root de Internet o si el root es un server interno.

***Para actualizar los Root Hints en el DNS Server deberá:***

1. Abrir la consola de DNS.
2. Seleccionar el server apropiado en la consola DNS.
3. Hacer click en ***Properties*** del menú ***Action***.
4. En ***Root Hints***, Usted puede hacer click en:
   - ***Add***, para agregar un Name Server. Agregue la IP de su server.
   - ***Edit***, para editar un Name Server.
   - ***Remove***, para quitar un Name Server.
   - ***Copy from Server***, para copiar la lista de Name Servers desde otro DNS Server.
5. Hacer click en ***OK*** para cerrar el cuadro ***Properties***.
6. Cerrar la consola DNS

### 3.4 ¿Cómo se almacenan y se mantienen los datos DNS?




Una ***zona*** es una parte contigua del espacio de nombres de dominio en el que un servidor DNS tiene autoridad para resolver consultas DNS. El espacio de nombres DNS se puede dividir en diferentes zonas, que almacenan información de nombres acerca de uno o varios dominios DNS, o partes de ellos. Para cada nombre de dominio DNS incluido en una zona, ésta se convierte en el origen autorizado de la información acerca de ese dominio.

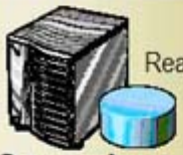
***Antes de crear zonas, debe comprender los siguientes conceptos:***

- ***Tipos de zonas.*** Los servidores DNS pueden alojar varios tipos de zona. Para limitar el número de servidores DNS en la red, puede configurar uno solo que admita o aloje varias zonas. También puede configurar varios servidores para alojar una o varias zonas con el fin de proporcionar tolerancia a errores y distribuir la carga de trabajo administrativa y de resolución de nombres.

- ***Archivo de zona.*** Los registros de recursos que se almacenan en un archivo de zona definen a ésta. El archivo de zona almacena información que se utiliza para convertir nombres de host en direcciones IP y viceversa.

**Importante:** Para crear zonas y administrar un servidor DNS que no se ejecuta en un controlador de dominio, debe ser miembro del grupo de administradores en ese equipo. Para configurar un servidor DNS que se ejecuta en un controlador de dominio, debe ser miembro de los grupos administradores de DNS, administradores de dominio o administradores Enterprise.

### 3.4.1. Identificación de tipos de zonas

| Zonas | Descripción |
|---|---|
|   Primary | Copia Read/write de una base de datos DNS |
|   Secondary | Copia Read-only de una base de datos DNS |
|  Stub | Copia de una zona conteniendo recursos limitados |

En la tabla siguiente se describen los cuatro tipos de zonas que se pueden configurar, así como los archivos de zona asociados con ellas.

**Estándar Principal:** Contiene una versión de lectura y escritura del archivo de zona que se almacena en un archivo de texto estándar. Los cambios realizados en la zona se registran en dicho archivo.

**Estándar Secundario:** Contiene una versión de sólo lectura del archivo de zona que se almacena en otro archivo de texto estándar. Los cambios efectuados en la zona se registran en el archivo de zona principal y se replican en el archivo de zona secundaria. Cree una zona secundaria estándar para crear una copia de una zona existente y de su archivo de zona. De esta forma se puede distribuir la carga de trabajo de la resolución de nombres entre varios servidores DNS.

**Integrada de Active Directory:** En lugar de almacenar la información de zona en un archivo de texto, se almacena en Active Directory. Las actualizaciones de la zona se producen automáticamente durante la replicación de Active Directory. Cree una zona integrada de Active Directory para simplificar el planeamiento y la configuración de un espacio de nombres DNS. No es necesario configurar servidores DNS para especificar cómo y cuándo se producen las actualizaciones, ya que Active Directory mantiene la información de zona.

**Zona Stub:** La zona Stub son las copias de una zona que contienen solamente los registros que son necesarios identificar en el server autoritativo DNS para esa zona. Una zona stub contiene un subconjunto de datos de la zona que consisten en registros SOA, NS, y A. Las zona Stub puede ser utilizada donde un servidor interno DNS representa al Root en lugar de los Root Servers de Internet.

### 3.4.1.1 Zonas Estándar Principales

El servidor principal de una zona actúa como punto de actualización de la zona. Las zonas recién creadas son siempre de este tipo. Con Windows Server 2003, las zonas principales se pueden utilizar de una de dos formas: como zonas estándar principales o como zonas principales integradas con Active Directory. En las zonas estándar principales, sólo un servidor puede alojar y cargar la copia maestra de la zona. Si crea una zona y la mantiene como zona estándar principal, no se permite ningún servidor principal adicional para la zona. Sólo un servidor puede aceptar actualizaciones dinámicas y procesar los cambios de zona.

El modelo principal estándar supone un punto de concentración de errores. Por ejemplo, si por cualquier motivo el servidor principal de una zona no está disponible para la red, no se puede realizar ninguna actualización dinámica de la zona. Tenga en cuenta que las consultas de nombres en la zona no se ven afectadas y pueden continuar sin interrupción, siempre y cuando los servidores secundarios de la zona estén disponibles para responderlas.

La adición de una nueva zona principal a un servidor existente puede llevarse a cabo siempre que se necesiten dominios o subdominios adicionales en el espacio de nombres de dominio DNS. Por ejemplo, podría tener una zona para un dominio de segundo nivel como microsoft.com y desear agregar una zona principal para el nuevo subdominio como itppro.microsoft.com. En este ejemplo puede crear la zona nueva para el subdominio con el Asistente para configuración de zona nueva del complemento DNS. Cuando haya finalizado, debe crear una delegación en la zona principal del nuevo dominio (como la zona microsoft.com) para completar la adición del nuevo subdominio y su zona principal.

En las zonas principales estándar, algunas veces puede ser necesario cambiar el servidor principal designado para una zona. Por ejemplo, supongamos que el servidor principal actual de una zona principal estándar es Servidor A y el nuevo servidor principal de la zona es Servidor B. Para influir en el cambio de estado del Servidor A al Servidor B, realice los siguientes cambios de zona:

1. Agregue un nuevo registro de recursos (RR) de host (A) para el Servidor B.
2. Actualice el registro de recursos de servidor de nombres (NS) de la zona para quitar el Servidor A e incluir el Servidor B como servidor autorizado y configurado, que apunta al nuevo registro de recursos RR A agregado en el paso 1.
3. Cambie el nombre del campo de propietario del registro de recursos de inicio de autoridad (SOA) para la zona del Servidor A al Servidor B.
4. Quite el registro de recursos A antiguo del Servidor A.
5. Compruebe la zona principal para asegurarse que los registros de delegación (registros de recursos NS o A) utilizados se actualizan para hacer referencia al Servidor B.

### 3.4.1.2 Zonas Estándar Secundarias

Las especificaciones de diseño de DNS recomiendan el uso de al menos dos servidores DNS para alojar cada zona. Para las zonas de tipo estándar principal, se necesita un servidor secundario para agregar y configurar la zona que aparece ante otros servidores DNS de la red. Los servidores secundarios pueden proporcionar un medio para aliviar el tráfico de consultas DNS en áreas de la red en las que una zona se consulta y utiliza mucho. Además, si un servidor principal deja de ser operativo, un servidor secundario puede realizar parte de la resolución de nombres en la zona hasta que el servidor principal esté disponible.

Si agrega un servidor secundario, intente ubicarlo lo más cerca posible de los clientes que requieran muchos nombres en la zona. Además, es recomendable colocar servidores secundarios a través de un router, ya sea en otras subredes (si se utiliza una LAN ruteada) o en vínculos WAN. De esta manera, se usa eficazmente un servidor secundario como copia de seguridad local en aquellos casos en los que un vínculo de red intermedio se convierte en un punto de concentración de errores entre servidores y clientes DNS que utilizan la zona.

Como el servidor principal siempre mantiene la copia maestra de las actualizaciones y cambios efectuados en la zona, el servidor secundario depende de mecanismos de transferencia de zonas DNS para obtener su información y mantenerla actualizada. Algunas cuestiones como los métodos de transferencia de zona, ya sea mediante transferencias de zona completas o incrementales, se simplifican cuando se utilizan servidores secundarios. Al considerar el impacto de las transferencias de zona causadas por los servidores secundarios, tenga en cuenta su ventaja como origen de copia de seguridad de información y compárela con el costo agregado que suponen en la infraestructura de red.

Una regla sencilla es que por cada servidor secundario que se agrega, aumenta el uso de la red (debido al tráfico adicional generado en la replicación de zona) y el tiempo necesario para sincronizar la zona en todos los servidores secundarios.

### 3.4.1.3 Zonas Integradas de Active Directory

En Windows Server 2003 puede agregar más servidores principales para una zona, mediante las características integradas de almacenamiento y replicación de directorios del servicio DNS. Para ello, es necesario cambiar una zona e integrarla en Active Directory.

Para integrar una zona existente en Active Directory, cambie el tipo de una zona en el servidor principal de origen donde se creó por primera vez. Una vez que el tipo de zona haya cambiado de estándar principal a Integrada de Active Directory, podrá agregar la zona a otros servidores DNS. A tal efecto, deberá configurarlos de modo que usen la opción para iniciar desde servicios de directorio cuando inicialicen el servicio DNS.

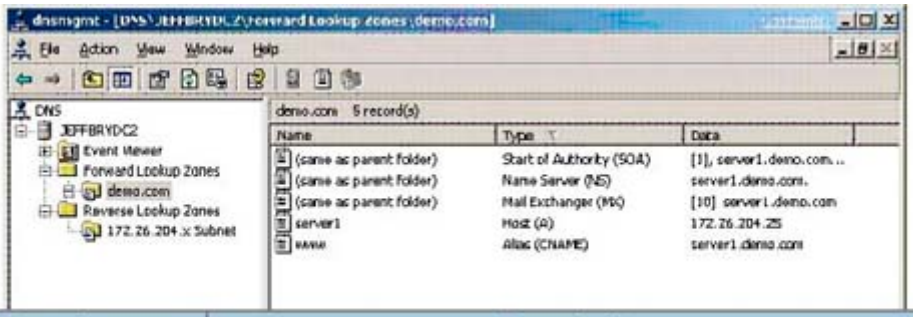
Cuando se selecciona esta opción, otros servidores DNS que funcionan como controladores de dominio para el dominio de Active Directory y tienen instalado el servicio DNS pueden consultar el directorio y cargar automáticamente todas las zonas integradas de él, que se almacenan en la base de datos de directorios. No se requiere ningún otro paso. Cualquier servidor DNS que funcione como parte de Active Directory es también, de manera predeterminada, servidor principal para las zonas integradas de directorio.

En las zonas principales integradas de directorio, los servidores secundarios se admiten pero no son necesarios para ofrecer tolerancia a errores. Por ejemplo, dos servidores DNS que funcionan como controladores de dominio de Windows Server 2003 pueden ser servidores principales redundantes para una zona y ofrecer las mismas ventajas que supone agregar un servidor secundario, además de otras adicionales.

Como el archivo de zona se mantiene en el contexto de nombres de dominio de Active Directory, los controladores de dominio deben estar en el mismo dominio para actuar como servidores principales redundantes en una zona. Cuando sea necesario compartir esta información de zona entre dominios, deberá crearse un servidor de zona secundaria estándar.

**Nota:** Este tipo de zona se verá más claramente en el capítulo 4 "Active Directory".

### 3.5 ¿Qué son Resource Records y Record Types?




| Record type | Descripción |
|---|---|
| A | Resuelve nombres de host name a IP |
| PTR | Resuelve IP a nombres host |
| SOA | El primer registro en cualquier archivo de zona |
| SRV | Resuelve nombres de servers que proveen servicios |
| NS | Identifica el DNS server para cada zona |
| MX | El server de mail |
| CNAME | Resoluciones desde nombres de host a nombres de host |

Los archivos de zona contienen la información a la que un servidor DNS hace referencia para realizar dos tareas distintas: convertir nombres de host en direcciones IP y convertir direcciones IP en nombres de host. Esta información se almacena como registros de recursos que llenan el archivo de zona. Un archivo de zona contiene los datos de resolución de nombres para una zona, incluidos los registros de recursos con información para responder a consultas DNS. Los registros de recursos son entradas de base de datos que incluyen varios atributos de un equipo, como el nombre de host o el nombre de dominio completo, la dirección IP o el alias.

***Los servidores DNS pueden contener los siguientes tipos de registros de recursos:***

**A (host):** Contiene la información de asignaciones de nombre a dirección IP, que se utiliza para asignar un nombre de dominio DNS a una dirección IP de host en la red. Los registros de recursos A también se conocen como registros de host.

**NS (name server):** Designa los nombres de dominio DNS de los servidores que tienen autoridad en una zona determinada o que contienen el archivo de zona de ese dominio.

**CNAME (canonical name):** Permite proporcionar nombres adicionales a un servidor que ya tiene un nombre en un registro de recursos A. Por ejemplo, si el servidor llamado webserver1.nwtraders.msft aloja el sitio web de nwtraders.msft, debe tener el nombre común ww.nwtraders.msft. Los registros de recursos CNAME también se conocen como registros de alias.

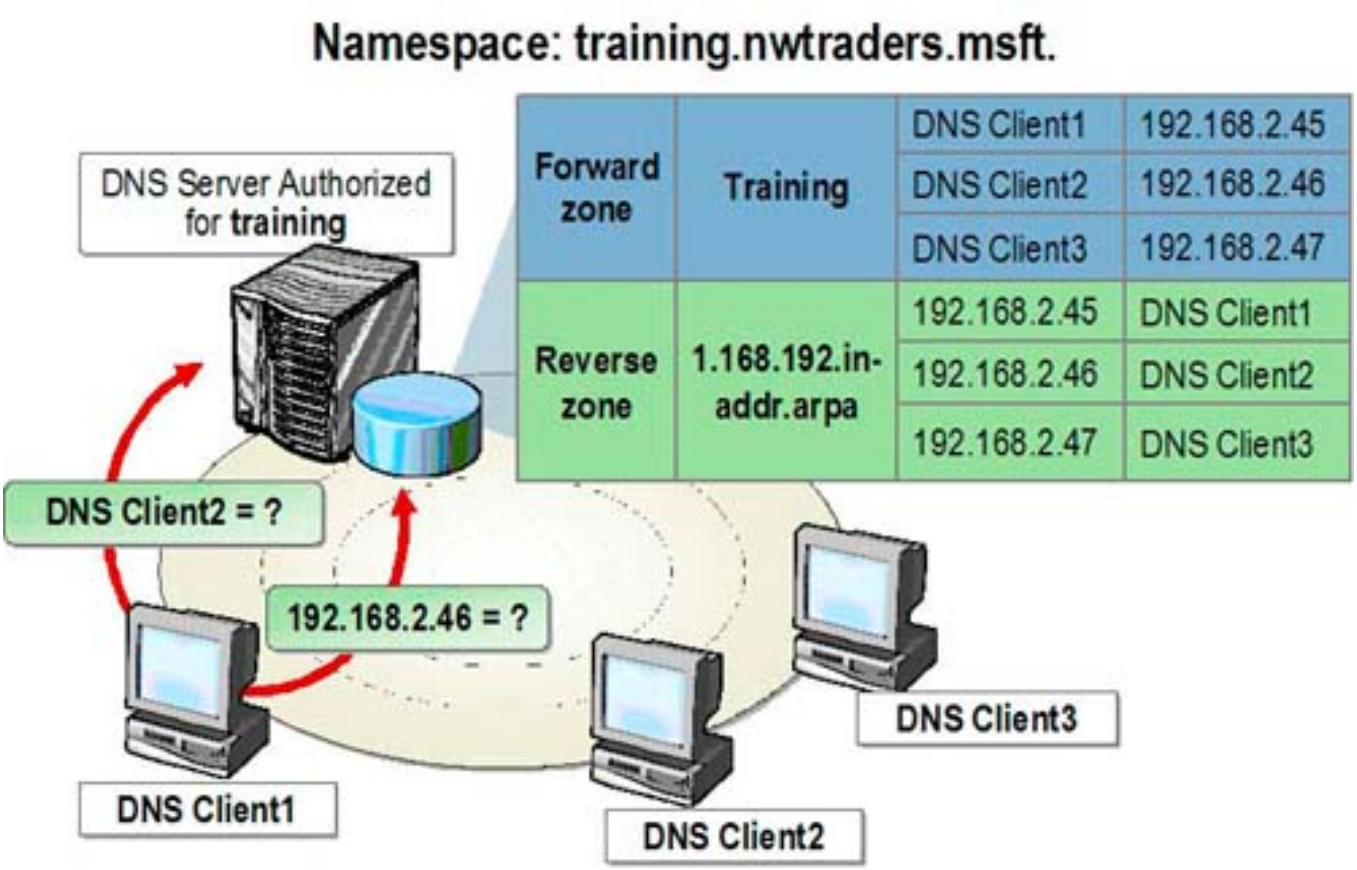
**MX (mail exchanger):** Especifica el servidor en el que las aplicaciones de correo electrónico pueden entregar correo. Por ejemplo, si tiene un servidor de correo que se ejecuta en un equipo llamado mail1.nwtraders.msft y desea que todo el correo de nombreDeUsuario@nwtraders.msft se entregue en este servidor, es necesario que el registro de recursos MX exista en la zona de nwtraders.msft y apunte al servidor de correo de ese dominio.

**SOA (Start Authority):** Indica el punto de partida o el punto original de autoridad para la información almacenada en una zona. El registro de recursos SOA es el primero que se crea cuando se agrega una zona nueva. Contiene también varios parámetros que utilizan otros equipos que emplean DNS para determinar cuánto tiempo utilizarán la información de la zona y con cuánta frecuencia hay que realizar actualizaciones.

**PTR (pointer):** Se utiliza en una zona de búsqueda inversa creada en el dominio in-addr.arpa para designar una asignación inversa de una dirección IP de host a un nombre de dominio DNS de host.

**SRV (service):** Lo registran los servicios para que los clientes puedan encontrar un servicio mediante DNS. Los registros SRV se utilizan para identificar servicios en Active Directory y también se conocen como registros de ubicación de servicio.

## 3.6 Creación de zonas de búsqueda estándar




En la mayoría de las búsquedas de DNS los clientes suelen realizar una búsqueda directa, que es una solicitud para asignar un nombre de equipo a una dirección IP. DNS proporciona también un proceso de búsqueda inversa, que permite a los clientes solicitar un nombre de equipo en función de la dirección IP del equipo.

### 3.6.1. Creación de una zona de búsqueda directa

Para crear una zona de búsqueda directa, haga click en ***Búsqueda directa*** en la página ***Zona de búsqueda directa o inversa*** del Asistente para zona nueva. El asistente lo guía por el proceso de asignar un nombre a la zona y al archivo de zona, y asimismo crea automáticamente la zona, el

archivo de zona y los registros de recursos necesarios para el servidor DNS en el que se crea la zona.

### 3.6.2. Creación de una zona de búsqueda inversa

Para crear una zona de búsqueda inversa, haga click en ***Búsqueda inversa*** en la página ***Zona de búsqueda directa o inversa*** del Asistente para zona nueva. El asistente le indica cómo especificar la identificación de la red o el nombre de zona y cómo comprobar el nombre del archivo de zona según la información de identificación de la red. Asimismo crea automáticamente la zona, el archivo de zona y los registros de recursos necesarios para el servidor DNS en el que se crea la zona.

El dominio in-addr.arpa es un dominio DNS especial de nivel superior que está reservado para la asignación inversa de direcciones IP en nombres de host DNS. Para crear el espacio de nombres inverso, se forman subdominios en el dominio in-addr.arpa con el orden inverso de los números en notación decimal con puntos de las direcciones IP.

Para cumplir los estándares RFC, el nombre de la zona de búsqueda inversa requiere el sufijo de dominio in-addr.arpa. Al crear una zona de búsqueda inversa, este sufijo se agrega automáticamente al final de la identificación de la red. Por ejemplo, si la red utiliza el identificador de red de clase B 172.16.0.0, el nombre de la zona de búsqueda inversa se convierte en 16.172.in-addr.arpa.

## 3.7. Configuración de zonas estándar


Para cada zona, el servidor que mantiene los archivos de zona principal estándar se llama ***servidor principal***, y los servidores que alojan los archivos de zona secundaria estándar se llaman ***servidores secundarios***. Un servidor DNS puede alojar el archivo de zona principal estándar (como servidor principal) de una zona y el archivo de zona secundaria estándar (como servidor secundario) de otra zona.

***Puede configurar uno o varios servidores DNS para alojar:***

- Una o varias zonas principales estándar.
- Una o varias zonas secundarias estándar.
- Una combinación de zonas principales estándar y zonas secundarias estándar.

**Nota:** Para crear una zona secundaria estándar, debe crear primero una zona principal estándar.

### 3.7.1 Especificación de un Master Server DNS para una zona secundaria

Al agregar una zona secundaria estándar, debe designar uno o varios servidores DNS en donde obtener la información de zona. El servidor o servidores designados se conocen como Master Servers DNS. Un ***Master Server DNS*** transfiere información de zona al servidor DNS secundario. Usted puede designar un servidor principal u otro servidor secundario como Master Server DNS para una zona secundaria estándar.

Para especificar un Master Server DNS en la página Masters Servers del Asistente para zona nueva, escriba la dirección IP del Master Server en el cuadro Dirección IP y haga click en Agregar.

## 3.8 Práctica 9: Configurando zonas DNS

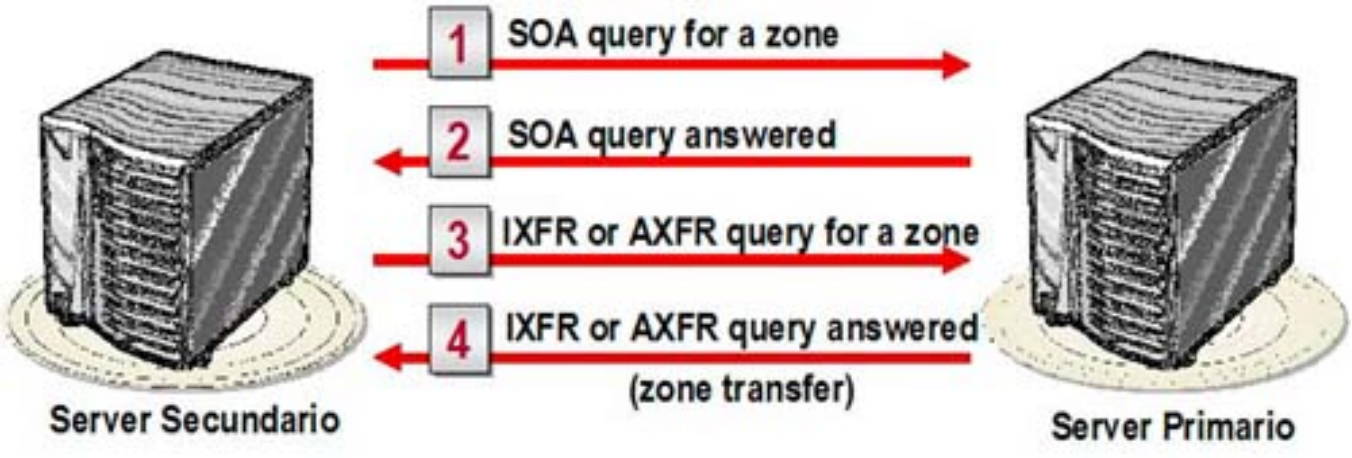
Configurar una zona de búsqueda del tipo primario

**Nombre de zona**: ***nwtraders.msft***

Después de terminar esta tarea, obtendrá una zona primaria configurada.

1. Abrir la consola DNS.
2. Hacer click derecho en el DNS Server de la consola DNS, y después en ***New Zone***.
3. Hacer click en ***Next*** de la página ***Welcome to the New Zone Wizard***
4. Seleccionar ***Primary zone*** en la página ***Zone Type*** y después hacer click en ***Next***.
5. Seleccionar ***Forward lookup zone*** en la página ***Forward or Reverse Lookup Zone***, y después hacer click en ***Next***.
6. Ingresar el nombre DNS para la zona en la página ***Zone Name***, y hacer click en ***Next***.
7. Hacer click en ***Next*** de la página ***Zone File*** para aceptar los defaults.
8. Hacer click en ***Finish*** de la página ***Completing the New Zone Wizard***.
9. Cerrar la consola DNS.

## 3.9. Proceso de transferencia de zona




Para proporcionar disponibilidad y tolerancia a errores en la resolución de nombres, los datos de la zona deben estar disponibles desde más de un servidor DNS de una red. Por ejemplo, si se utiliza un solo servidor DNS y éste no responde, las consultas de nombres fallarán. Cuando se configura más de un servidor para alojar una zona, se requieren transferencias de zona para replicar y sincronizar los datos de la zona entre todos los servidores que están configurados para alojarla.

### 3.9.1. Transferencia de zona

La ***transferencia de zona*** es el proceso en el que un archivo de zona se replica en otro servidor DNS. Las transferencias de zona se producen cuando las asignaciones de nombres y direcciones IP cambian en el dominio. Cuando esto ocurre, los archivos de zona modificados se copian desde un Master Server a sus servidores secundarios.

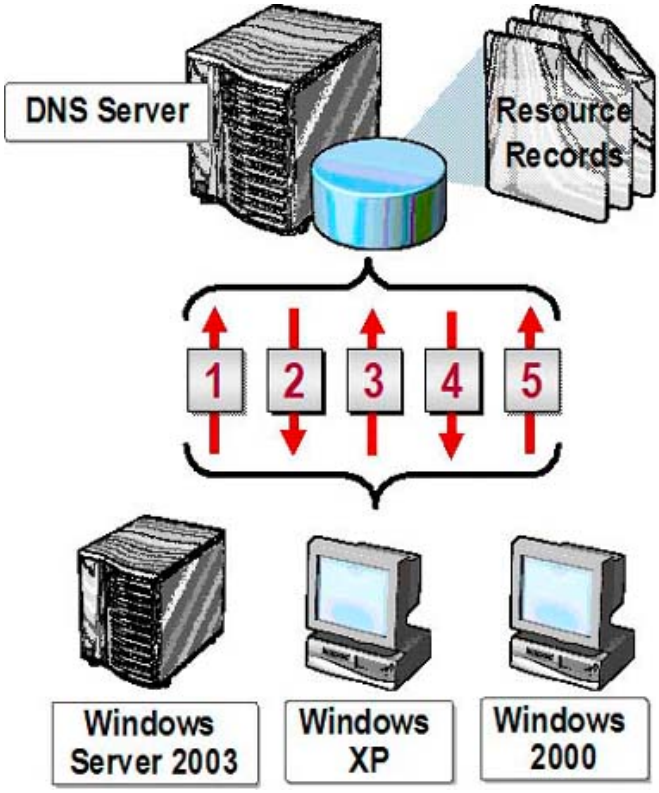
### 3.9.2. Transferencia de zona incremental

En Windows Server 2003, la información de una zona se actualiza mediante ***transferencias de zona incrementales (IXFR)***, que sólo replican los cambios realizados en el archivo de zona, en lugar de replicar todo el archivo. Los servidores DNS que no admiten IXFR solicitan el contenido entero de un archivo de zona cuando inician una transferencia de zona. Esto se conoce como AXFR o ***transferencia de zona completa***.

***El proceso de transferencia de zona se inicia cuando se produce una de las siguientes situaciones:***

- Un servidor maestro envía al servidor o servidores secundarios una notificación anunciando que se ha producido un cambio en la zona. Cuando el servidor secundario recibe la notificación, consulta los cambios en el Master Server.
- Cada servidor secundario consulta periódicamente un servidor maestro para comprobar si hubo cambios en el archivo de zona, incluso si no se le ha notificado ningún cambio. Esto ocurre cuando se inicia el servicio Servidor DNS en el servidor secundario o cuando transcurre el intervalo de actualización en el servidor secundario.

## 3.10. Introducción a las actualizaciones dinámicas



Usted puede configurar servidores DHCP para asignar automáticamente direcciones IP a equipos cliente. Cuando un cliente recibe una nueva dirección IP de un servidor DHCP, se debe actualizar la información de asignaciones de nombres a direcciones IP almacenadas en el servidor DNS. En Windows 2003, los servidores y los clientes DHCP pueden registrar y actualizar dinámicamente esta información de los servidores DNS configurados para permitir actualizaciones dinámicas.

### 3.10.1 Protocolo de actualización dinámica

El protocolo de actualización dinámica permite a los equipos cliente actualizar automáticamente sus registros de recursos en un servidor DNS sin necesidad de intervenir el administrador. De forma predeterminada, los equipos con Windows 2000, Windows XP y Windows Server 2003 se configuran para realizar actualizaciones dinámicas cuando también se configuran con una dirección IP estática.

### 3.10.2 Proceso de actualización dinámica

Cuando un servidor DHCP asigna una dirección IP a un cliente DHCP basado en Windows 2000 ó Windows Server 2003, se produce el siguiente proceso:

1. El cliente inicia un mensaje de solicitud DHCP al servidor DHCP, en el que solicita una dirección IP. Este mensaje incluye el nombre de dominio completo.
2. El servidor DHCP devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
3. El cliente envía al servidor DNS una solicitud de actualización DNS de su propio registro de búsqueda directa, el registro de recursos A (dirección).
4. El servidor DHCP envía actualizaciones para el registro de búsqueda inversa del cliente DHCP, el registro de recursos PTR (puntero). Para realizar esta operación, el servidor DHCP utiliza el nombre de dominio completo que obtuvo en el primer paso.

### 3.10.3. Actualizaciones dinámicas para clientes con versiones anteriores de Windows

Los equipos cliente que ejecutan versiones anteriores de Windows no admiten actualizaciones dinámicas. Debe configurar el servidor DHCP para que actualice siempre los registros de recursos A y PTR de esos clientes. En tal caso, se produce el proceso siguiente:

1. El cliente inicia un mensaje de solicitud DHCP al servidor DHCP, en el que solicita una dirección IP. A diferencia de los mensajes de solicitud DHCP de los clientes DHCP basados en Windows 2000, la solicitud no incluye un nombre de dominio completo.
2. El servidor devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
3. El servidor DHCP envía al servidor DNS actualizaciones de los registros de recursos A y PTR del cliente.

### 3.10.4. Configuración del DNS Server para permitir actualizaciones dinámicas

Para configurar un servidor DNS de modo que permita actualizaciones dinámicas, abra el cuadro de diálogo ***Propiedades*** de la zona en el servidor DNS que desee configurar. En la ficha ***General***, en el cuadro de lista ***¿Allow Dynamic updates?***, haga click en ***Yes***. En la tabla siguiente se describen las opciones disponibles para las actualizaciones dinámicas.

***No*** Deshabilita las actualizaciones dinámicas para la zona
***Yes*** Habilita las actualizaciones dinámicas para la zona
***Only secure updates*** Permite las actualizaciones dinámicas seguras de una zona integrada de Active Directory realizadas desde equipos cliente autorizados.

Para obtener más información acerca de DNS:

http://www.microsoft.com/Windows2000/technologies/communications/dns/default.asp

http://support.microsoft.com/default.aspx?scid=kb;en-us;814591

http://support.microsoft.com/default.aspx?scid=kb;en-us;323445

http://support.microsoft.com/default.aspx?scid=kb;en-us;323380

http://support.microsoft.com/default.aspx?scid=kb;en-us;323383

http://support.microsoft.com/default.aspx?scid=kb;en-us;323419

http://support.microsoft.com/default.aspx?scid=kb;en-us;324259

http://support.microsoft.com/default.aspx?scid=kb;en-us;324260

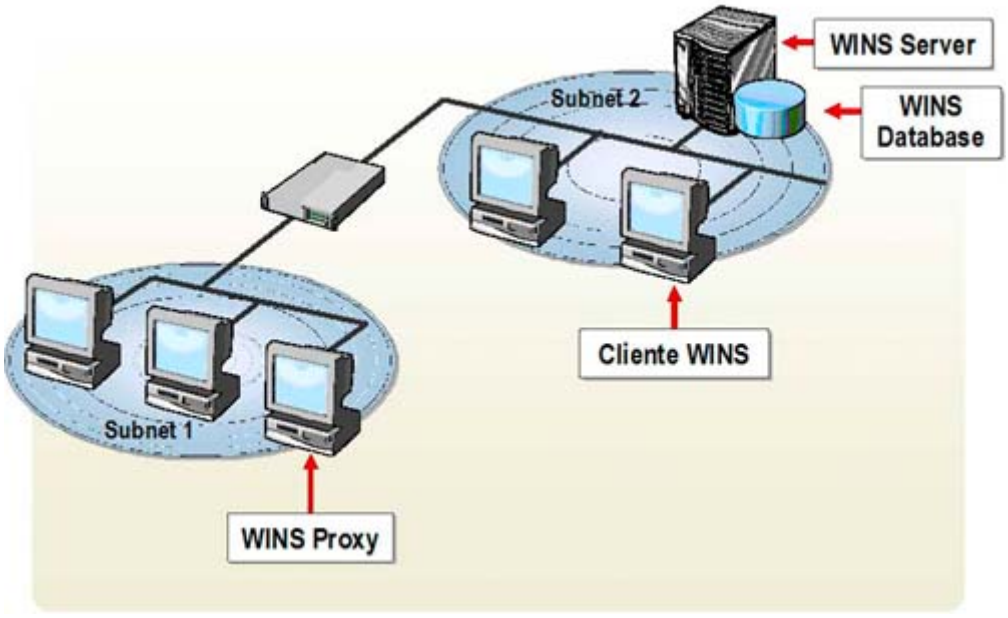
http://support.microsoft.com/default.aspx?scid=kb;en-us;323417

http://support.microsoft.com/default.aspx?scid=kb;en-us;816518

http://support.microsoft.com/default.aspx?scid=kb;en-us;816567

http://support.microsoft.com/default.aspx?scid=kb;en-us;323418

## 4. Descripción de WINS (Windows Internet Name System)




El método más habitual para resolver nombres NetBIOS remotos y locales es el uso de un servidor de nombres NetBIOS.

Cuando un usuario ejecuta determinados comandos, como ***net use***, o hace que una aplicación NetBIOS interactúe con la red, se inicia el proceso de resolución de nombres NetBIOS. En la caché de nombres NetBIOS es donde se

comprueba si se encuentra la asignación de nombre NetBIOS en dirección IP del host de destino. En caso que el nombre NetBIOS no se encuentre en la caché, el cliente intentará determinar la dirección IP del host de destino mediante otros métodos.

Si el nombre no se puede resolver con la caché, el nombre NetBIOS del host de destino se envía al servidor de nombres NetBIOS configurado para el host de origen. Una vez que el nombre se convierte en una dirección IP, se devuelve al host de origen.

WINS es la implementación de Microsoft de un servidor de nombres NetBIOS.

***Para que WINS funcione correctamente en una red, cada cliente debe:***

- Registrar su nombre en la base de datos WINS. Al iniciar un cliente, éste registra su nombre en el servidor WINS configurado.
- Renovar el registro a intervalos configurables. Los registros de los clientes son temporales y, por lo tanto, los clientes WINS deben renovar regularmente su nombre o, de lo contrario, su concesión caducará.
- Liberar los nombres de la base de datos al cerrarse. Si el cliente WINS ya no necesita su nombre, por ejemplo cuando se apaga, envía un mensaje para indicar al servidor WINS que lo libere.

***Una vez que se ha configurado con WINS como método de resolución de nombres, el cliente lo usará para llevar a cabo resoluciones de nombres NetBIOS. Para ello debe realizar las acciones siguientes:***

1. Si el cliente no puede resolver el nombre en su caché, envía una consulta de nombre a su servidor WINS principal. Si éste no responde, el cliente enviará la solicitud dos veces más.
2. Si el cliente no recibe una respuesta del servidor WINS principal, vuelve a enviar la solicitud a todos los servidores WINS adicionales, configurados en el cliente. Si un servidor WINS resuelve el nombre, responderá al cliente con la dirección IP del nombre NetBIOS solicitado.
3. En caso que no se reciba ninguna respuesta, el servidor WINS enviará un mensaje indicando que el nombre no se encuentra, y el cliente pasará al siguiente método de resolución de nombres configurado.

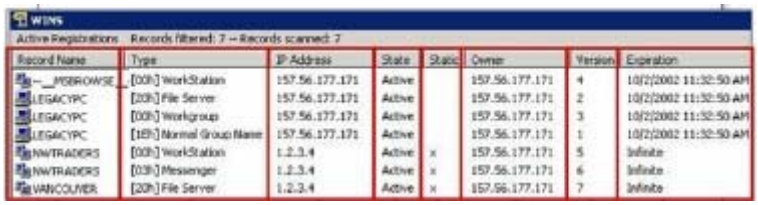
## 4.1 Práctica 10: Instalación de WINS

Para crear un servidor WINS, instale WINS en un equipo donde se ejecute ***Windows Server 2003***.

***Para instalar WINS deberá:***

1. Hacer doble click en ***Add / remove programs*** del Panel de control.
2. Hacer click en ***Add / remove Windows components***.
3. Hacer click en Network Services y en Details de la página ***Windows components*** del Asistente para componentes de Windows, en ***Components***.
4. Activar la casilla de verificación ***WINS Service*** En el cuadro de diálogo ***Network Services***, en ***Subcomponents***, y hacer click en ***Ok***.
5. Hacer click en ***Next***.

## 4.2. Estudio de los registros de la base de datos WINS




La snap-in WINS de Microsoft Management Console (MMC) permite al usuario ver el contenido de la base de datos WINS y buscar entradas específicas.

**Apertura de la base de datos WINS**

***Para abrir la base de datos WINS deberá:***

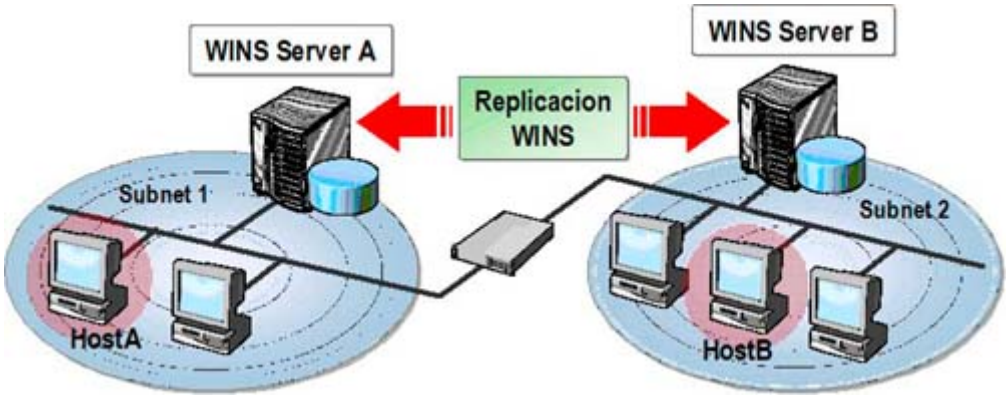
1. Expandir el nombre del servidor en WINS y hacer click en ***Active registries***.
2. Hacer click con el botón secundario del mouse en ***Active registries*** y luego hacer click en ***find by owner***.
3. Hacer click en ***All Owners*** del cuadro de diálogo ***find by owner***, en la ficha ***Owners***, y luego hacer click en ***Find***.

### 4.2.1. Estudio de la información de registro de WINS

WINS muestra todos los registros de la base de datos y organiza la información de registro de WINS en las columnas siguientes:

- ***Nombre de registro.*** El nombre NetBIOS registrado, que puede ser un nombre único o puede representar a un grupo, un grupo de Internet o un equipo multitarjeta.
- ***Tipo.*** El servicio que registró la entrada, incluido el identificador de tipo hexadecimal.
- ***Dirección IP.*** La dirección IP correspondiente al nombre registrado.
- ***Estado.*** El estado de la entrada de la base de datos, que puede ser Activo, Liberado o Desechado. Si el estado de la entrada es Desechado, ésta ya no estará activa y se quitará de la base de datos.
- ***Propietario.*** El servidor WINS desde que se origina la entrada. Debido a la replicación, no es necesariamente el mismo servidor desde el que se está viendo la base de datos.
- ***Versión.*** Número hexadecimal único, asignado por el servidor WINS durante el registro de nombres. Los asociados del servidor lo utilizan para identificar nuevos registros durante la replicación.
- ***Caducidad.*** Muestra la fecha de caducidad de la entrada. Cuando un replicado se almacena en la base de datos, los datos de caducidad correspondientes se establecen de acuerdo con la hora del servidor WINS de recepción, además del intervalo de renovación establecido en el cliente.

## 4.3. Replicación de WINS




Aunque un servidor WINS puede admitir más de 5.000 clientes en condiciones normales de carga de trabajo, puede instalar también un segundo servidor para proporcionar tolerancia a errores en la resolución de nombres NetBIOS. Dicho servidor permitirá, al mismo tiempo, localizar el tráfico de resolución. De esta forma, si se produce un error en uno de los servidores WINS, el otro servidor continuará realizando la resolución de nombres NetBIOS en la red.

Cada servidor WINS de una red mantiene su propia base de datos WINS. Por lo tanto, si hay varios servidores WINS en la red, deberán configurarse para replicar los registros de su base de datos en el resto de los servidores WINS. La replicación de bases de datos WINS garantiza que un cliente WINS configurado para usar un servidor WINS distinto, pueda resolver nombres registrados con un servidor WINS.

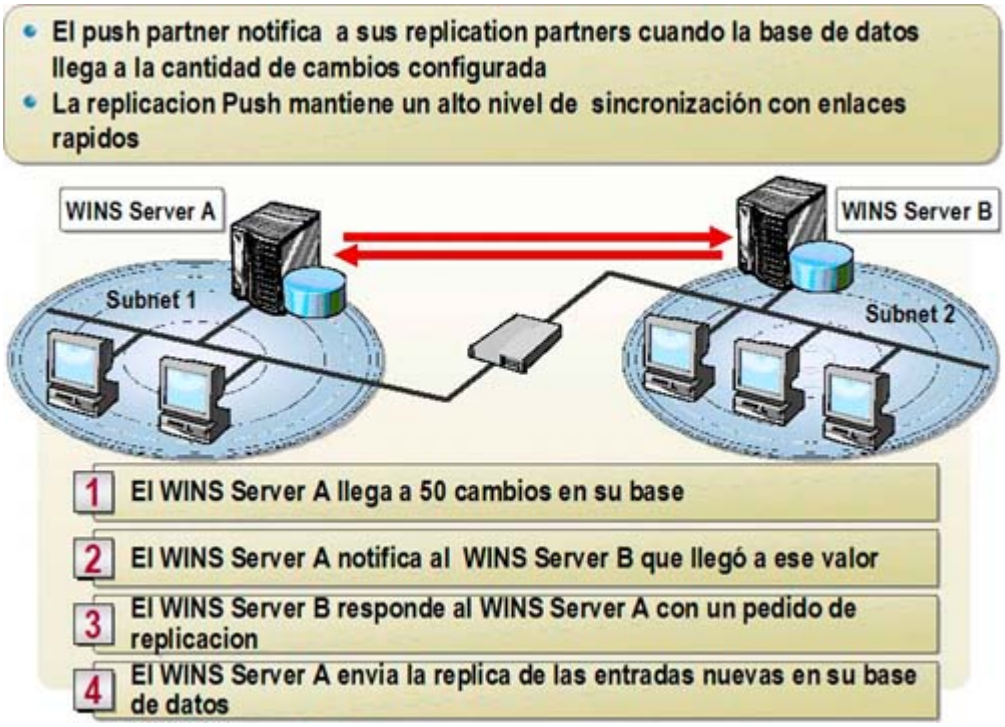
***Por ejemplo:***

- El host A de la subred 1 se registra con el servidor WINS A de la subred 1.
- El host B de la subred 2 se registra con el servidor WINS B de la subred 2.
- Cuando se produce una replicación de WINS, cada servidor WINS actualiza su base de datos con la nueva entrada procedente de la base de datos del otro servidor.

Como resultado de la replicación, ambos servidores WINS disponen de información acerca de ambos hosts, y los hosts A y B pueden resolver mutuamente sus nombres si se ponen en contacto con su servidor WINS local.

Para que se produzca la replicación, cada servidor WINS deberá configurarse con un asociado de replicación, como mínimo. Al configurar un asociado de replicación para un servidor WINS, puede especificarlo como asociado de extracción, como asociado de inserción o como asociado de extracción e inserción para el proceso de replicación.

### 4.3.1 ¿Cómo funciona la replicación Push?




#### 4.3.1.1. Definición

La replicación ***Push*** es el proceso de copia de los registros actualizados desde un WINS Server a otros, siempre que el WINS Server que contenga datos actualizados, alcance un valor especificado de cambios.

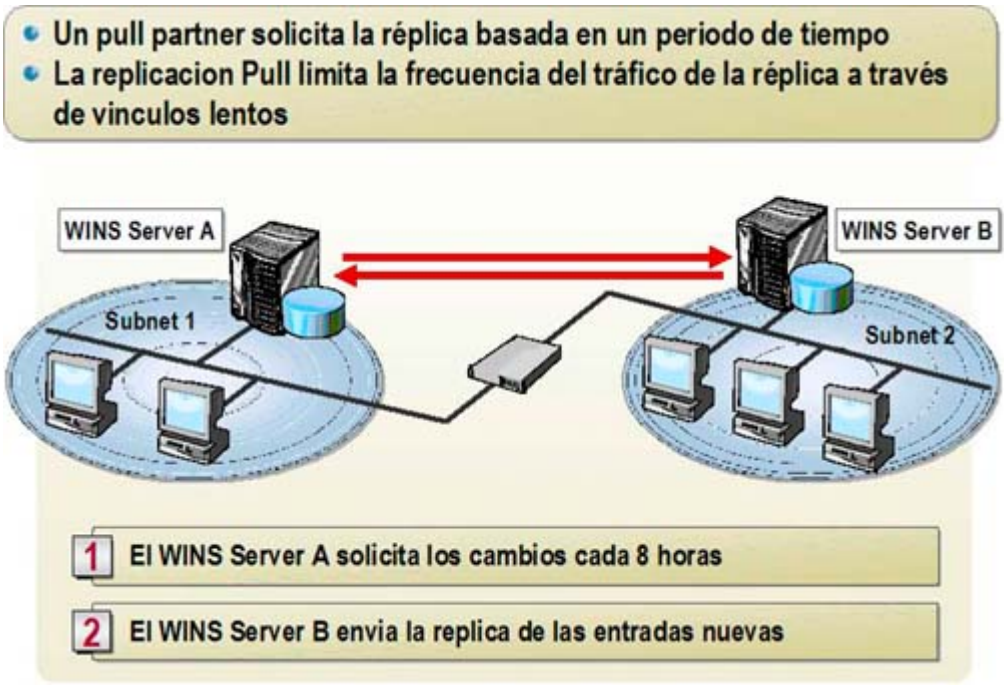
***El proceso de replicación Push funciona de la siguiente forma:***

1. El Push Partner notifica a sus Replication Partners, siempre que el número de cambios a su base de datos del WINS pase un valor específico configurable. Por

ejemplo, Usted puede configurar el Push Partner para notificar a los Replication Partners cuando ocurran 50 cambios en la base.

2. Cuando los Replication Partners respondan a la notificación con un pedido de réplica, el Push Partner envía la réplica de las entradas nuevas en la base.

### 4.3.2 ¿Cómo funciona una replicación Pull?




#### 4.3.2.1. Definición

La replicación ***Pull*** es el proceso de copia de los registros actualizados desde un WINS Server a otros WINS Servers, en intervalos específicos de tiempo.

***El proceso de replicación Pull funciona de la siguiente forma:***

1. El Pull Partner solicita los cambios en la base de WINS en intervalos de tiempo. Por ejemplo, Usted puede configurar un Pull Partner para solicitar los cambios cada 8 horas.
2. Los Replication Partners responden enviando las entradas nuevas de la base.

También existe la posibilidad de configurar Replications Partners de modo Push/Pull. Esto le asegura que bajo determinada cantidad de cambios, se produzca la replicación en intervalos de tiempo.

## 4.4. Práctica 11: ¿Cómo configurar una replicación WINS?

Para poder hacer esta práctica Usted necesitará dos instalaciones de Windows Server 2003 con el servicio de WINS instalado.

Por default, los WINS Replication Partners son configurados como Push/Pull Partners. Para modificar esta configuración y satisfacer las necesidades de su red, Usted puede especificar los parámetros Push y Pull para cada Replication Partner.

***Para configurar una replicación WINS deberá:***

1. Seleccionar, en la consola WINS, el WINS Server al que quiere agregar un Replication Partner, y hacer click en ***Replication Partners***.
2. Hacer click en ***New Replication Partner*** del menú ***Action***,
3. Ingresar, en el campo ***WINS Server***, el nombre o la IP del WINS Server a agregar como Replication Partner. (Segunda Computadora)
4. Hacer click en ***OK***.

***Para modificar el tipo de Replication Partner deberá:***

1. Expandir el WINS Server en la consola WINS.
2. Hacer click en ***Replication Partners*** de la consola WINS.
3. Hacer click derecho en el server apropriado del cuadro de detalles, y luego hacer click en ***Properties***
4. Seleccionar una de las siguientes opciones en el cuadro Server ***Properties***, en ***Advanced***, en el campo: ***Replication partner type***:
   - ***Push.***
   - ***Pull.***
   - ***Push/Pull.***
5. Hacer click en ***OK*** del cuadro ***Server Properties***.
6. Cerrar la consola WINS.

Para obtener más información acerca de WINS:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323429

## 4.5. Mantenimiento

### 4.5.1. Backup

Usted debe realizar tareas de mantenimiento en períodos de tiempo específico. Para ayudarle en esta tarea, el WINS Server puede ser configurado para realizar los backups automáticamente. Tenga en cuenta que todos los software de backup no realizan esta tarea ya que la base de datos es un archivo con privilegios exclusivos del sistema operativo, siempre que el servicio esté iniciado.

***Para especificar el directorio de backup de WINS deberá:***

1. Hacer click derecho sobre el WINS Server de la consola WINS, y después hacer click en ***Properties***.
2. Ingresar el directorio donde quiere realizar los backups del WINS Server, en ***General*** en el campo ***Default backup path***.

**Nota:** El WINS Server realizará un backup automáticamente cada 24 horas.

### 4.5.2. Compactar la base de datos

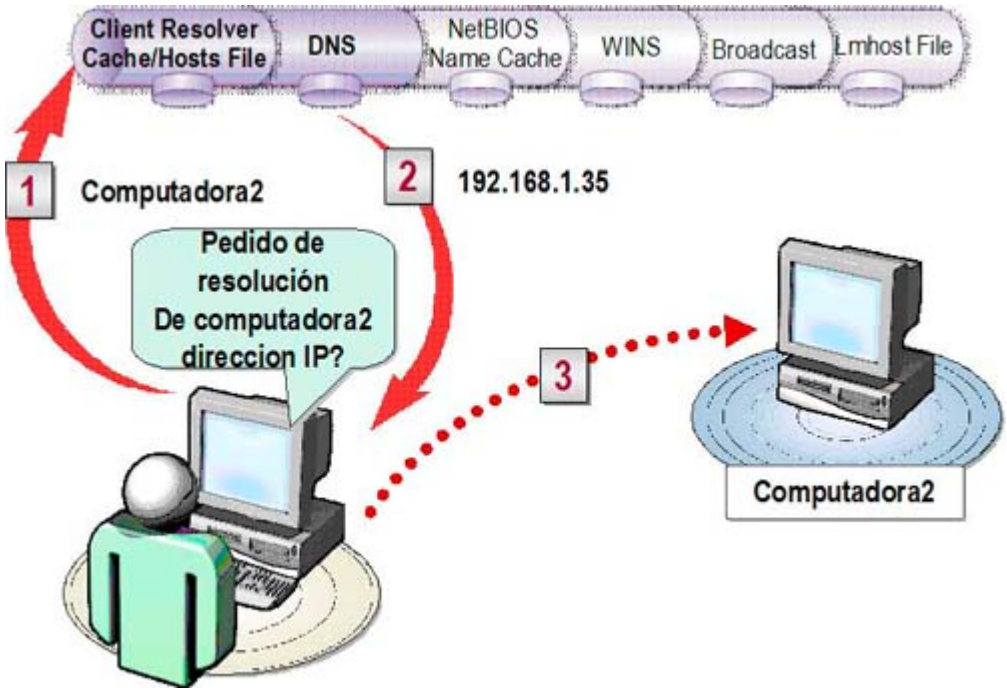
Para realizar las operaciones de reparación y/o compactación debe utilizar la herramienta apropiada: la base de WINS, que es un archivo que se encuentra en \Windows\system32\Wins y su nombre es Wins.mdb. La herramienta que usted debe utilizar es jetpack, y el comando es:

***jetpack %Systemroot%\System32\Wins\Wins.mdb Temp.mdb***

Donde %systemroot% es el directorio de instalación del sistema operativo y temp,mdb es una base temporal.
Luego debe copiar la base temporal con el nombre Wins.mdb y eliminar la base anterior. Recuerde que para realizar esta tarea debe estar detenido el servicio de WINS Server.

## 4.6. Procesos de resolución de nombres e integración WINS / DNS

### 4.6.1. Resolución de nombres de host




***El proceso de resolución de nombres de HOST en un cliente cumple con el siguiente diagrama:***

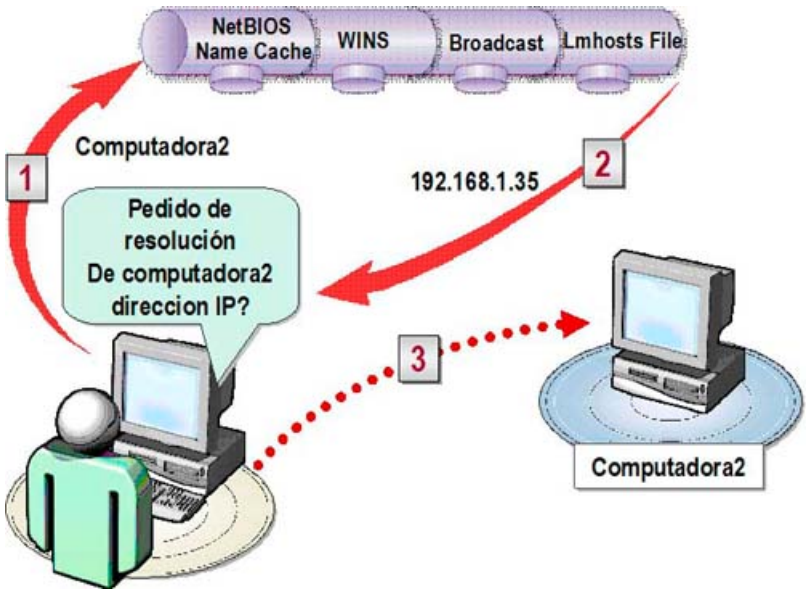
1. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así la resolución se encuentra en el DNS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
2. El cliente realiza una query al DNS primario. Si el DNS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
3. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así, la resolución se encuentra en el NetBIOS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
4. El cliente realiza una query al WINS primario. Si el WINS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
5. Si hasta el momento no pudo resolver el nombre, el cliente realiza un Broadcast local. Si resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
6. Por último tendrá que consultar el archivo local LMHOSTS que se encuentra en %systemroot%\system32\drivers\etc. Este archivo es una base estática de resolución; no tiene extensión y tampoco se actualiza. Si este último proceso no es exitoso, el cliente no logra la resolución.

**Ejemplo de archivo HOSTS**

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

### 4.6.2. Resolución de nombres NetBIOS



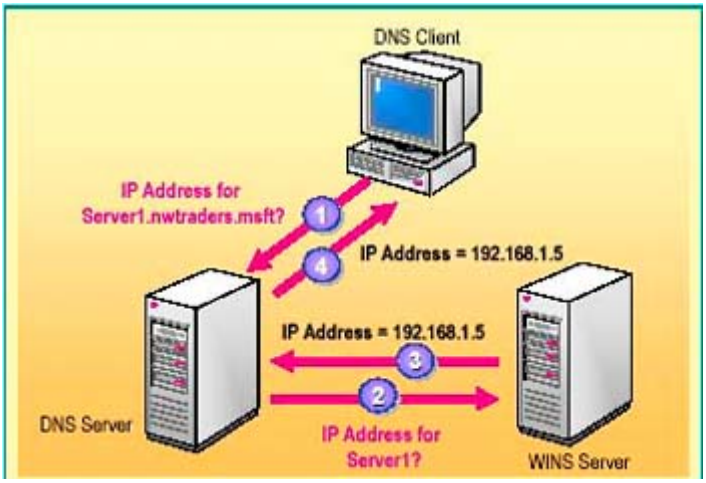
***El proceso de resolución de nombres de NetBIOS en un cliente cumple con el siguiente diagrama:***

1. El cliente verifica si ya obtuvo la resolución en otra oportunidad. De ser así, la resolución se encuentra en el NetBIOS caché local del cliente y finaliza el proceso. Si no obtiene la resolución, sigue al paso siguiente.
2. El cliente realiza una query al WINS primario. Si el WINS resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
3. Si hasta el momento no pudo resolver el nombre, el cliente realiza un Broadcast local. Si resuelve la consulta, el proceso finaliza. Si no obtiene la resolución, sigue al paso siguiente.
4. Por último tendrá que consultar el archivo local LMHOSTS que se encuentra en %systemroot%\system32\drivers\etc. Este archivo es una base estática de resolución; no tiene extensión y tampoco se actualiza. Si este último proceso no es exitoso, el cliente no logrará la resolución.

**Ejemplo de Archivo LMHOST**

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino          #PRE #DOM:networking    #net group's DC
# 102.54.94.102    "appname  \0x14"                       #special app server
# 102.54.94.123    popular              #PRE              #source server
# 102.54.94.117    localsrv             #PRE              #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
```

### 4.6.3. Introducción a la integración WINS y DNS




El integrar WINS con DNS habilita a los clientes a usar exclusivamente DNS para la resolución de nombres. Los clientes podrán acceder a los datos de WINS a través del DNS server. Sin embargo, el DNS Server no puede localizar recursos sin realizar una query a WINS. En Windows Server 2003, Usted puede configurar integración entre WINS y DNS para habilitar a clientes no-WINS para resolver nombres NetBIOS, usando un DNS Server.

Usted puede configurar DNS integrado con WINS Servers.

***Para configurar una zona DNS para uso de WINS lookup deberá:***

1. Abrir DNS en el menú ***Administrative Tools***.
2. Expandir, en la consola DNS, el server donde está la zona a configurar, expandir ***Forward Lookup Zones***, y luego hacer click en la zona.
3. Hacer click derecho en la zona, y luego en ***Properties***.
4. Seleccionar el cuadro Use ***WINS forward lookup***, del cuadro ***Properties***, en ***WINS***.
5. Ingresar la dirección IP del WINS Server, del cuadro ***IP address***, y luego hacer click en ***Add***.

# Capítulo 4
# Active Directory Services

## 1. Introducción

Durante este capítulo Usted irá asimilando conocimientos acerca de los servicios de directorio (Active Directory Services) de Windows Server 2003, en particular, sobre algunas características nuevas de este servicio.

Para el desarrollo de las prácticas contenidas en esa unidad, necesitará la instalación de Windows Server 2003 realizada en la práctica 1 del capítulo 2 y una instalación adicional.

***Al finalizar este capítulo Usted tendrá las habilidades de:***

- Describir las características del servicio de directorio Active Directory.
- Identificar estructuras lógicas y físicas.
- Instalar y configurar Active Directory en la red.
- Identificar características referentes a la replicación.
- Solucionar problemas de Active Directory.

### 1.1. Definición

En una red de Microsoft® Windows® Server 2003, el servicio de directorio Active Directory® proporciona la estructura y las funciones para organizar, administrar y controlar el acceso a los recursos de red. Para implementar y administrar una red de Windows Server 2003, deberá comprender el propósito y la estructura de Active Directory.

Active Directory proporciona también la capacidad de administrar centralmente la red de Windows Server 2003. Esta capacidad significa que puede almacenar centralmente información acerca de la empresa, por ejemplo, información de usuarios, grupos e impresoras, y que los administradores pueden administrar la red desde una sola ubicación.

Active Directory admite la delegación del control administrativo sobre los objetos de él mismo. Esta delegación permite que los administradores asignen a un grupo determinado de administradores, permisos administrativos específicos para objetos, como cuentas de usuario o de grupo.

Active Directory es el servicio de directorio de una red de Windows Server 2003, mientras que un ***servicio de directorio*** es aquel que almacena información acerca de los recursos de la red y permite que los mismos resulten accesibles a los usuarios y a las aplicaciones. Los servicios de directorio proporcionan una manera coherente de nombrar, describir, localizar, tener acceso, administrar y asegurar la información relativa a los recursos de red.

### 1.2. La funcionalidad

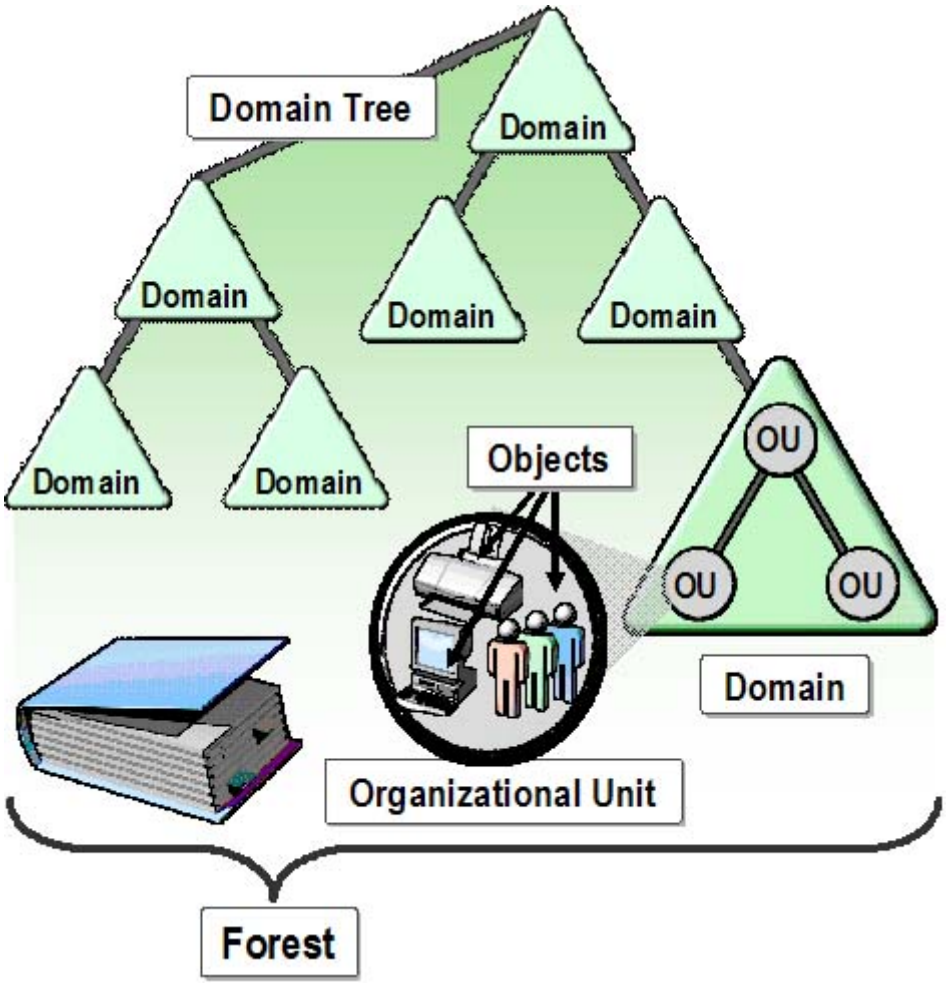
Active Directory proporciona funcionalidad de servicio de directorio, como medio para organizar, administrar y controlar centralmente el acceso a los recursos de red. Asimismo hace que la topología física de red y los protocolos pasen desapercibidos, de manera que un usuario de una red pueda tener acceso a cualquier recurso sin saber dónde está el mismo o cómo está conectado físicamente a la red. Un ejemplo de este tipo de recurso es una impresora.

Active Directory está organizado en secciones que permiten el almacenamiento de una gran cantidad de objetos. Como resultado, es posible ampliar Active Directory a medida que crece una organización, permitiendo que una organización que tenga un único servidor con unos cuantos centenares de objetos, crezca hasta tener miles de servidores y millones de objetos.

Un servidor que ejecuta Windows Server 2003 almacena la configuración del sistema, la información de las aplicaciones y la información acerca de la ubicación de los perfiles de usuario en Active Directory. En combinación con las directivas de grupo, Active Directory permite a los administradores controlar escritorios distribuidos, servicios de red y aplicaciones desde una ubicación central, al tiempo que utiliza una interfaz de administración coherente.

Además, Active Directory proporciona un control centralizado del acceso a los recursos de red, al permitir que los usuarios sólo inicien sesión una sola vez para obtener pleno acceso a los recursos mediante Active Directory.

### 1.3. Estructura Lógica de Active Directory



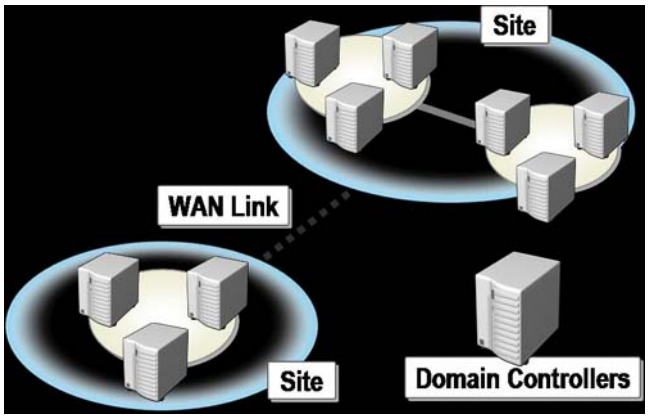

Active Directory proporciona el almacenamiento seguro de la información sobre objetos en su estructura jerárquica lógica. Los objetos de Active Directory representan usuarios y recursos, como por ejemplo, las computadoras y las impresoras. Algunos objetos pueden llegar a ser containers para otros objetos.

Entendiendo el propósito y la función de estos objetos, Usted podrá realizar una variedad de tareas, incluyendo la instalación, la configuración, la administración y la resolución de problemas de Active Directory.

***La estructura lógica de Active Directory incluye los siguientes componentes:***

- ***Objects.*** Estos son los componentes básicos de la estructura lógica.
- ***Object classes.*** Son las plantillas o los modelos para los tipos de objetos que se pueden crear en Active Directory. Cada clase de objeto es definida por un grupo de atributos, los cuales definen los valores posibles que se pueden asociar a un objeto. Cada objeto tiene una combinación única de los valores de atributos.
- ***Organizational units.*** Usted puede utilizar estos container objects para organizar otros objetos con propósitos administrativos. Organizando objetos en Organizational Unit, se hace más fácil localizar y administrar objetos. Usted puede también delegar la autoridad para administrar las Organizational Unit. Estas últimas pueden contener otras Organizational Units para simplificar la administración de objetos.
- ***Domains.*** Son las unidades funcionales core de la estructura lógica de Active Directory, y asimismo es una colección de los objetos administrativos definidos, que comparten en una base de datos común del directorio, políticas de la seguridad y relaciones de confianza con otros Domains. Los Domains proporcionan las tres funciones siguientes:
  - Un límite administrativo para los objetos
  - Medios de administrar la seguridad para los recursos compartidos
  - Una unidad de réplica para los objetos
- ***Domain trees.*** Son Domains agrupados en estructuras de jerarquía. Cuando se agrega un segundo dominio a un tree, se convierte en Child del tree Root Domain. El dominio al cual un Child Domain se une, se llama Parent Domain. El Child Domain puede tener sus propios Child Domain, y su nombre se combina con el nombre de su Parent Domain para formar su propio y único nombre, Domain Name System (DNS). Un ejemplo de ellos sería corp.nwtraders.msft. De este modo, un tree tiene un Namespace contiguo.
- ***Forests.*** Un Forest es una instancia completa de Active Directory, y consiste en uno o más trees. En un solo two-level tree, el cual se recomienda para la mayoría de las organizaciones, todos los Child Domains se hacen Children del Forest Root Domain para formar un tree contiguo. El primer dominio en el forest se llama Forest Root Domain, y el nombre de ese dominio se refiere al forest, por ejemplo, nwtraders.msft. Por defecto, la información en Active Directory se comparte solamente dentro del forest. De esta manera, la seguridad del forest estará contenida en una sola instancia de Active Directory.

## 1.4. La estructura física de Active Directory




En contraste con la estructura lógica y los requisitos administrativos de los modelos, la estructura física de Active Directory optimiza el tráfico de la red, determinando cómo y cuándo ocurre la replicación y el tráfico de logon. Para optimizar el uso del ancho de banda de la red Active Directory, Usted debe entender la estructura física del mismo.

***Los elementos de la estructura física de Active Directory son:***

- ***Domain controllers.*** Estas computadoras corren Microsoft® Windows® Server 2003 o Windows 2000 Server y Active Directory. Cada Domain Controller realiza funciones de almacenamiento y replicación, y además soporta solamente un domain. Para asegurar una disponibilidad contínua de Active Directory, cada domain debe tener más de un Domain Controller.

- ***Active Directory sites.*** Los sites son grupos de computadoras conectadas. Cuando Usted establece sites, los Domain Controllers que están dentro de un solo site pueden comunicarse con frecuencia. Esta comunicación reduce al mínimo el estado de la latencia dentro del site, esto es, el tiempo requerido para un cambio que se realice en un Domain Controller y sea replicado a otros domain controllers. Usted crea sites para optimizar el uso del ancho de banda entre domain controllers en diversas locaciones.

- ***Active Directory partitions.*** Cada Domain Controller contiene las siguientes particiones de Active Directory:

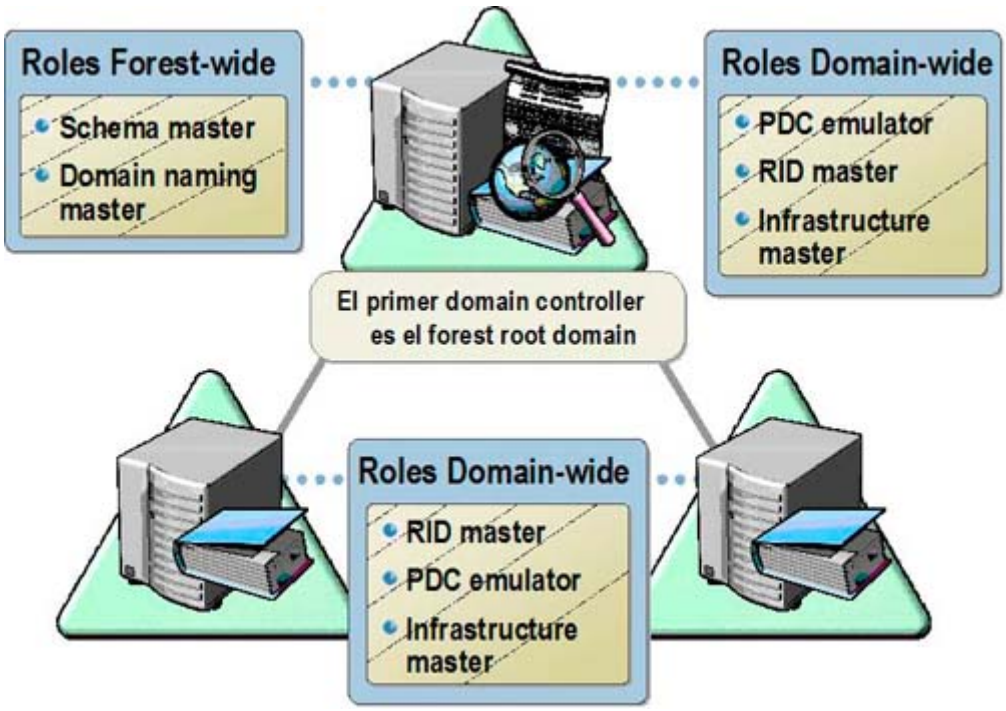
    - Domain Partition, que contiene la réplica de todos los objetos en ese domain. Esta partición es replicada solamente a otros Domain Controllers en el mismo domain.

    - Configuration Partition, que contiene la topologia del forest. La topología registra todas las conexiones de los Domain Controllers en el mismo forest.

    - Schema Partition, que contiene el schema del forest. Cada forest tiene un schema de modo que la definición de cada clase del objeto sea constante. Las particiones Configuration y Schema Partitions son replicadas a cada Domain Controller en el forest.

- Application Partitions Ppcionales. que contienen los objetos relacionados a la seguridad y son utilizados por una o más aplicaciones. Las Application Partitions son replicadas a Domain Controllers específicos en el forest.

## 1.5. ¿Qué son los Operations Masters?



Cuando un cambio se realiza a un domain, el cambio se replica a todos los Domain Controllers del mismo. Algunos cambios, por ejemplo los que se hacen en el schema, son replicados a todos los domains en el forest. Este tipo de replicación es llamada ***Multimaster Replication***.

### 1.5.1. Operaciones Single Master

Durante la replicación multimaster, puede ocurrir un conflicto de réplica donde se originen actualizaciones concurrentes en el mismo atributo del objeto y en dos Domain Controllers. Para evitar conflictos de réplica, Usted puede utilizar **Single Master Replication**, la cual asigna un Domain Controller como el único y en el que se pueden realizar cambios de directorio.

De esta manera, los cambios no pueden ocurrir en diversos lugares de la red al mismo tiempo. Active Directory usa Single Master Replication para los cambios importantes, por ejemplo, la adición de un nuevo domain o cambios al schema del forest.

### 1.5.2. Operations Master Roles

Las operaciones que utilizan Single Master Replication van junto a roles específicos en el forest o en el domain. Estos roles se llaman ***Operations Master Roles***. Para cada Operation Master Role, solamente el Domain Controller que tiene el rol puede realizar los cambios asociados al directorio. El Domain Controller que es responsable de un rol en particular se llama Operations ***Master para ese rol***. Active Directory, por su parte, almacena la información sobre el Domain Controller que cumple un rol especifico.

Los Operations Master Roles son a nivel forest o nivel domain, y Active Directory define cinco de ellos, los cuales tienen una localización por defecto.

***Roles Forest-wide. Únicos en el forest, los roles forest-wide son:***

- ***Schema master.*** Controla todas las actualizaciones al schema. El schema contiene la definición de clases de objetos y atributos que se utilizan para crear todos los objetos de Active Directory, como usuarios, computadoras, e impresoras.

- ***Domain Naming Master.*** Controla la adición o el retiro de domains en el forest. Cuando se agrega un nuevo domain al forest, solamente el Domain Controller que tenga el rol Domain Naming Master, podrá agregar el nuevo domain. Hay solamente un Schema Master y un Domain Naming Master por forest. Ambos roles están en el primero domain controller del root domain

***Roles Domain-wide. Para cada domain en el forest, los roles domain-wide son:***

- ***Primary domain controller emulator (PDC).*** Actúa como un PDC Windows NT para soportar a los Backup Domain Controllers (BDCs) que corren Microsoft Windows® NT en domains, en modo mixto. Este tipo de domain tiene Domain Controller corriendo Windows NT 4.0. El PDC Emulator es el primer Domain Controller que se crea en un nuevo domain.

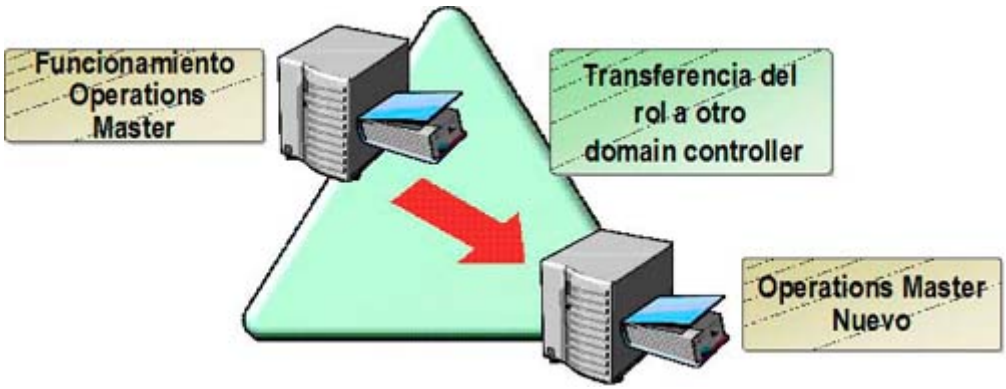
- ***Relative identifier master.*** Cuando se crea un nuevo objeto, el Domain Controller crea un nuevo Security Principal, que representa al objeto, asignándole un Unique Security Identifier (SID). El SID consiste en un Domain SID, que es igual para todos los Security Principals creados en el domain, y un relative identifier (RID), el cual es único para cada security principal creado en el domain. El RID Master asigna bloques de RIDs a cada Domain Controller en el domain. El Domain Controller entonces asigna el RID a los objetos se crean del bloque asignado de RIDs.

- ***Infrastructure master.*** Cuando los objetos se mueven de un domain a otro, el Infrastructure Master actualiza las referencias al objeto en ese domain y la referencia al objeto en el otro dominio. La referencia del objeto contiene el Object Globally Unique Identifier (GUID), el Distinguished Name y el SID. Active Directory actualiza periódicamente el Distinguished Name y el SID, en la referencia

al objeto para reflejar los cambios realizados en el objeto real, por ejemplo, movimientos en y entre domains o la eliminación del objeto.

Cada domain en el forest tiene su propio PDC Emulator, RID Master e Infrastructure Master.

### 1.5.3. Transferencia de Operations Master Roles




Usted colocará los Operations Master Roles en un forest cuando implemente una estructura de forest y dominio. Los Operations Master Roles se transfieren, solamente cuando se realiza un cambio importante en la infraestructura del dominio. Tales cambios incluyen el desarme de un Domain Controller que haya tenido un rol, y la adición de un nuevo Domain Controller que satisfaga mejor las operaciones de un rol específico.

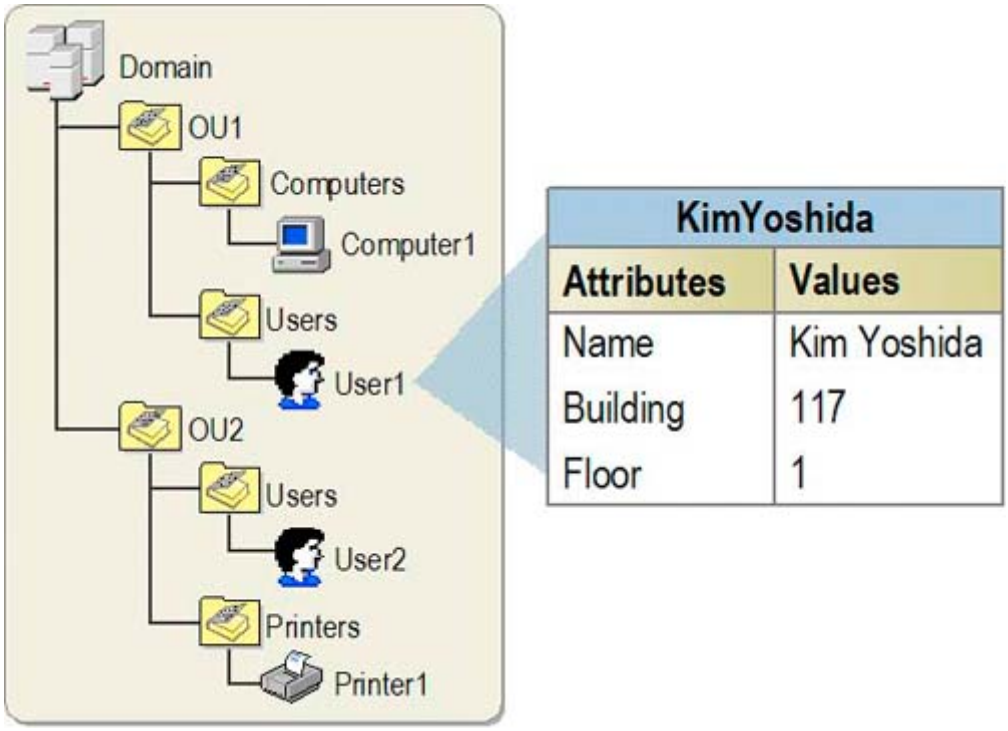
La transferencia de Operations Master Roles implica mover el rol de un Domain Controller a otro. Para transferir roles, los dos Domain Controllers deben estar funcionando y conectados a la red.

Ninguna pérdida de datos ocurre cuando Usted transfiere Operations Master Role. Active Directory replica el actual Operation Master Role al nuevo Domain Controller, asegurando que el nuevo Operation Master Role obtendrá la información necesaria para dicho rol. Esta transferencia utiliza el mecanismo de la réplica del directorio.

Para obtener información sobre el proceso de transferencia:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324801

## 2. ¿Qué es el servicio de directorio?




Un servicio de directorio es un depósito estructurado de la información sobre personas y recursos en una organización. En una red Windows Server 2003, el servicio de directorio es Active Directory.

### 2.1. Active Directory tiene las siguientes capacidades:

- ***Permite a usuarios y aplicaciones tener acceso a la información sobre objetos.*** Esta información se almacena en forma de valores atributos. Usted buscará objetos basándose en su clase, atributo, valor del atributo, localización dentro de la estructura de Active Directory, o cualquier combinación de estos valores.

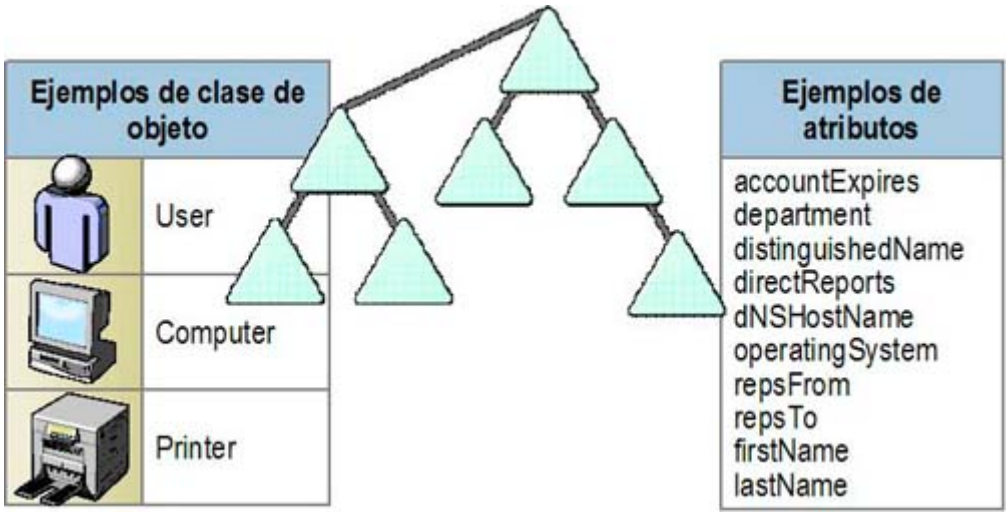
- ***Hace transparentes la topología y los protocolos físicos de la red.*** De esta manera, un usuario en una red puede tener acceso a cualquier recurso, por ejemplo a una impresora, sin saber dónde está el recurso o dónde está conectado físicamente con la red.
o Permite el almacenamiento de un número muy grande de objetos. Dado que se organiza en particiones, Active Directory puede ampliarse mientras que una organización crece. Por ejemplo, un directorio puede ampliarse de un solo servidor con algunos objetos a millares de servidores y millones de objetos.

- new ! ***Puede funcionar como servicio Non-Operating System.*** Active Directory in Application Mode (AD/AM) es una nueva capacidad de Microsoft Active Directory y actúa en escenarios de aplicaciones Directory-Enabled. AD/AM funciona como servicio Non-Operating System que, como tal, no requiere instalación sobre un Domain Controller. Correr servicios Non-Operating System significa que múltiples instancias de AD/AM pueden funcionar concurrentemente en un solo servidor, siendo cada instancia independientemente configurable.

  Para obtener más información acerca de ADAM (Active Directory Aplication Mode):

  http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx

### 2.2. ¿Qué es el Schema?




El Schema de Active Directory contiene las definiciones de todos los objetos, como por ejemplo usuarios, computadoras e impresoras almacenados en Active Directory. Sobre Domain Controllers corriendo Windows Server 2003, hay solamente un Schema para todo el forest. De esta manera, todos los objetos que se crean en Active Directory cumplen con las mismas reglas.

El Schema tiene dos tipos de definiciones: Object Classes y atributos. Un ejemplo de Object Classes son los usuarios, la computadora y la impresora, que describen los objetos posibles que se pueden crear en el directorio. Cada Object Class es una colección de atributos. Los atributos se definen separadamente de los Object Classes. Cada atributo se define solamente una vez y puede ser utilizado en múltiples Object Classes. Por ejemplo, el atributo de la descripción se utiliza en muchos Object Classes, pero se define solamente una vez en el Schema para asegurar consistencia.

Asimismo Usted puede crear nuevos tipos de objetos en Active Directory extendiendo el Schema. Por ejemplo, para un aplicación E-mail Server, se podría ampliar el User Class en Active Directory con nuevos atributos que contengan información adicional, como la dirección y el e-mail de los usuarios.

new! Sobre Domain Controllers Windows Server 2003, Usted puede revertir cambios al Schema desactivándolos y permitiendo a las organizaciones, de esta forma, mejorar el uso de las características de extensibilidad de Active Directory.

new! También se puede redefinir una clase o atributo del Schema, por ejemplo, cambiar la sintaxis de la secuencia de Unicode del atributo llamado SalesManager a Distinguished Name.

## 2.3 ¿Qué es el Global Catalog?


El ***global Catalog*** es un repositorio de información que contiene un subconjunto de atributos de todos los objetos en Active Directory. Los miembros del grupo Schema Admins pueden cambiar los atributosque son almacenados en el Global Catalog, dependiendo de los requerimientos de la organización.

***El Global Catalog contiene:***

- Los atributos que se utilizan con más frecuencia en queries, por ejemplo, first name, last name y logon name de los usuarios.
- La información que es necesaria para determinar la localización de cualquier objeto en el directorio.
- Un subconjunto por defecto de los atributos para cada tipo de objeto.
- Los permisos de acceso para cada objeto y atributos, que son almacenados en el Global Catalog. Si Usted busca un objeto y no tiene los permisos apropiados para verlo, el objeto no aparecerá en los resultados de la búsqueda. Los permisos de acceso aseguran que los usuarios puedan encontrar solamente los objetos a los cuales les han asignado el acceso.

El ***Global Catalog Server*** es un Domain Controller que procesa eficientemente queries intraforest al Global Catalog. El primer Domain Controller que Usted crea en Active Directory se convierte automáticamente en Global Catalog Server. Usted puede configurar Global Catalog Servers adicionales para balancear el tráfico para logon y queries.

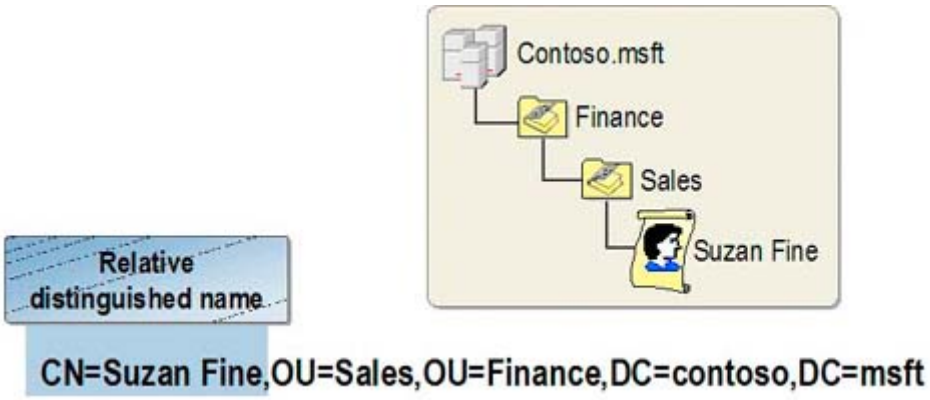
***El Global Catalog permite a usuarios realizar dos funciones importantes:***

- Buscar información en Active Directory en todo el forest, sin importar la localización de los datos.
- Usar información del membership del Universal Group en el proceso de logon a la red.

new! Los Global Catalog Servers replican su contenido en un esquema de replicación. Hasta Windows 2000 estas réplicas eran del tipo full sync, pero a partir de Windows Server 2003 se hacen de modo partial sync, es decir, solo se replican cambios en lugar de enviar el catalogo completo.

new! Para poder utilizar esta nueva característica de Windows Server 2003, Usted puede tener el nivel funcional del forest en modo Windows 2000 o Windows server 2003, pero solamente se harán réplicas parciales entre los servidores Global Catalog que corran Windows Server 2003.

## 2.4 ¿Qué son los Distinguished y Relative Distinguished Names?




LDAP utiliza un nombre que representa objetos en Active Directory por una serie de componentes que se relacionan con la estructura lógica. Esta representación es llamada ***Distinguished Name*** del objeto, e identifica el domain donde se localiza el objeto y la trayectoria completa por la cual el objeto es alcanzado. El Distinguished Name debe ser único en el Active Directory forest.

El ***Relative Distinguished Name*** de un objeto identifica únicamente el objeto en su container. Dos objetos en el mismo container no pueden tener el mismo nombre. El Relative Distinguished Name siempre es el primer componente del Distinguished Name, pero puede no ser siempre un Common Name.

Para un usuario llamado Suzan Fine de Sales Organizational Unit en Contoso.msft domain, cada elemento de la estructura lógica se representa en el siguiente Distinguished Name:

**CN=Suzan Fine,OU=Sales,DC=contoso,DC=msft**

- CN es el Common Name del objeto en su container.
- OU es la Organizational Unit que contiene el objeto. Puede haber más de un valor de OU si el objeto reside en una Organizational Unit anidada a más niveles.
- DC es el Domain Component, por ejemplo .com. o .msft.. Hay siempre al menos dos Domain Components, pero posiblemente más si el domain es un child domain.

Los domain components de los Distinguished Name están basados en Domain Name System (DNS).

## 2.5. Active Directory Snap-ins y Herramientas

Windows Server 2003 proporciona un número de snap-ins y herramientas command-line para administrar Active Directory. Usted puede también administrar Active Directory usando Active Directory Service Interfaces (ADSI). ADSI es una interfaz simple de gran alcance para crear scripts reutilizables para administrar Active Directory.

**Nota:** La herramienta ADSI Edit puede instalarse, desde el CD de Windows Server 2003. La misma se encuentra en la carpeta \Support\Tools.

*La tabla siguiente describe los snap-ins administrativos comunes para administración de Active Directory.*

| Snap-in | Descripción |
|---|---|
| Active Directory Users and Computers | Es una Microsoft Management Console (MMC) que se utiliza para administrar y publicar la información en Active Directory. Usted puede administrar cuentas de usuario, grupos, y cuentas de computadora, agregar computadoras al domain, administrar políticas de cuentas, derechos de usuario, y políticas de auditoria. |
| Active Directory Domains and Trusts | Es una MMC que se utiliza para administrar Domain Trusts y Forest Trusts, agregar sufijos user principal name, y cambiar niveles de funcionamiento de domains y forest.<br>Active Directory Sites and Services Es una MMC que usted utiliza para administrar replicacion de directorio. |
| Active Directory Schema | Es una MMC que se utiliza para administrar el Schema. No está disponible por defecto en el menu |
| Administrative Tools. | Usted debe agregarlo manualmente. |

*La tabla siguiente describe las herramientas de command-line para utilizar cuando se quiera administrar Active Directory.*

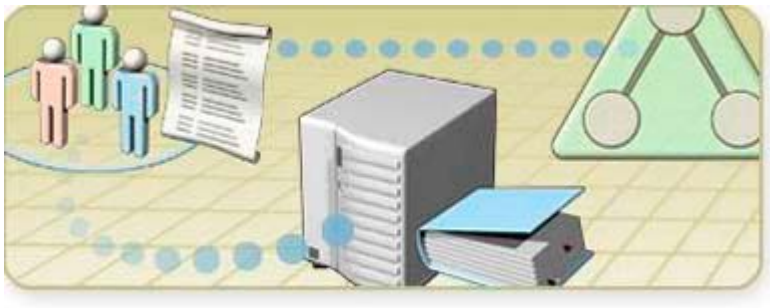
| Herramienta | Descripción |
|---|---|
| Dsadd | Agrega objetos a Active Directory, tales como computadoras, usuarios, grupos, organizational units y contactos. |
| Dsmod | Modifica objetos en active Directory, tales como computadoras, servidores, usuarios, grupos, organizational units y contactos. |
| Dsquery | Corre queries en Active Directory según criterios especificados. Usted puede correr queries contra servidores, computadoras, grupos, usuarios, sites, organizational units, y particiones. |
| Dsmove | Mueve objetos dentro de un dominio, a una nueva localización en Active Directory o renombra un solo objeto sin moverlo. |
| Dsrm | Suprime un objeto de Active Directory. |
| Dsget | Muestra atributos seleccionados de una computadora, contacto, grupo, organizational unit, servidor o usuario de Active Directory. |
| Csvde | Importa y exporta datos de Active Directory usando formato separado por comas. |
| Ldifde | Crea, modifica y borra objetos de Active Directory. Puede también extender el Schema de Active Directory y exportar información de usuarios y grupos a otras aplicaciones o servicios. |

Para obtener más información acerca de las herramientas command-line:

http://support.microsoft.com/default.aspx?scid=kb;en-us;322684

## 3. Instalación de Active Directory

### 3.1. Requisitos para instalar Active Directory



Antes de instalar Active Directory, Usted debe asegurarse que la computadora puede ser configurada como Domain Controller, cumpliendo con los requisitos de hardware y del sistema operativo. Además, el Domain Controller deberá tener acceso al DNS Server, que deberá cumplir con ciertos requisitos para soportar la integración con Active Directory.

***La lista siguiente identifica los requisitos para la instalación de Active Directory:***

- Una computadora corriendo Microsoft® Windows® Server 2003 Standard Edition, Enterprise Edition o Datacenter Edition. Windows Server 2003 Web Edition no soporta Active Directory.

- Un mínimo de 250 megabytes (MB) de espacio en disco.200 MB para la base de datos de Active Directory y 50 MB para logs de transacciones de Active Directory. Los requisitos de tamaño del archivo para la base de Active Directory y los archivos log, dependen del número y el tipo de objetos en el domain. Se requerirá el espacio de disco adicional si el Domain Controller también es Global Catalog Server.

- Una partición o un volumen con formato NTFS. La partición NTFS se requiere para la carpeta SYSVOL.

- Los privilegios administrativos necesarios para crear un domain, si es que Usted está creando uno en una red existente Windows Server 2003.

- TCP/IP instalado y configurado para utilizar DNS.

- Un DNS Server autoritativo para el DNS Domain y soporte para los requisitos enumerados en la siguiente tabla.

- ***SRV Resource Records (Mandatory) Service Locator Resource (SRV).*** Son registros DNS que identifican los servicios específicos que ofrecen las computadoras en una red Windows Server 2003. El DNS Server que soporta la instalación de Active Directory necesita soporte de SRV Resource Records. De lo contrario, Usted deberá configurar el DNS localmente durante la instalación de Active Directory o configurar el DNS manualmente después de la instalación de Active Directory.

- ***Dynamic Updates (Opcional).*** Microsoft recomienda que los servidores DNS también soporten actualizaciones dinámicas. El protocolo dinámico de actualización permite a los servidores y a los clientes, en un ambiente DNS, agregar y actualizar la base de datos del DNS automáticamente, lo que reduce esfuerzos administrativos. Si Usted utiliza software DNS que soporta SRV Resource Records pero que no soporta el protocolo dinámico de actualización, deberá ingresar los SRV Resource Records manualmente en la base DNS.

- ***Incremental Zone Transfers (Opcional).*** En una transferencia incremental de zona, los cambios realizados en una zona en el Master DNS Server, deben ser replicados a los DNS Servers secundarios de esa zona. Las transferencias incrementales de la zona son opcionales, pero se recomiendan porque ahorran

ancho de banda de la red, replicando solamente los registros nuevos o modificados entre los DNS Servers, en vez del archivo de base de datos entero de la zona.

### 3.2 El proceso de instalación de Active Directory


***El proceso de la instalación realiza las siguientes tareas:***

- ***Inicia el protocolo de autenticación Kerberos version 5***

- ***Aplica la politica Local Security Authority (LSA).*** Esta configuración indica que el server es un Domain Controller.

- ***Crea las particiones de Active Directory.*** Una partición del directorio es una porción del Directory Namespace. Cada partición del directorio contiene una jerarquía o subtree de los objetos del directorio en el árbol del directorio. Durante la instalación, se crean las particiones siguientes en el primer domain controller del forest:

    - Schema Directory Partition
    - Configuration Directory Partition
    - Domain Directory Partition
    - Forest DNS Zone si está integrada en el active directory
    - Domain DNS Zone Partition si está integrada en el active directory

Las particiones, entonces, se actualizarán a través de la réplica, en cada uno de los Domain Controllers creados subsiguientemente en el forest.

- ***Crea la base de datos y los logs de Active Directory.*** La locación por defecto para la base de datos y los archivos de logs es %systemroot%\Ntds.

- ***Crea el forest root domain.*** Si el servidor es el primer Domain Controller en la red, el proceso de la instalación crea el Forest Root Domain, y entonces le asignará los Operations Master Roles al Domain Controller, incluyendo:

    - Primary Domain Controller (PDC) Emulator
    - Relative Identifier (RID) Operations Master
    - Domain-Naming Master
    - Schema Master
    - Infrastructure Master

- ***Crea la carpeta compartida del volumen del sistema.*** Esta estructura de carpetas reside en todos los Windows Server 2003 Domain Controllers y contiene las siguientes carpetas:

- La carpeta compartida SYSVOL, que contiene información de Group Policy.
- La carpeta compartida Net Logon, que contiene los logon scripts para computadoras que no corren Windows Server 2003.

- ***Configura pertenencia al site apropiado para el Domain Controller.*** Si la IP del servidor que Usted está promoviendo a Domain Controller está dentro de una subnet definida en Active Directory, el wizard colocará el Domain Controller en el site asociado con la subnet. Si no se define ningún objeto de subnet o si la IP del servidor no está dentro del rango de la subnet presente en Active Directory, el servidor se colocará en el site Default-First-Site-Name. El primer site se instala automáticamente cuando Usted crea el primer Domain Controller en el forest. El wizard de instalación de Active Directory crea un objeto servidor del Domain Controller en el site apropiado. El objeto servidor contiene la información requerida para la réplica y asimismo contiene una referencia al objeto de la computadora en la OU Domain Controllers, representando que el Domain Controller está siendo creado.

- ***Permite seguridad en el Directory Service y en File Replication Folders.*** Esto implica controlar el acceso de usuario a objetos de Active Directory.

- ***Aplica el password para la cuenta del administrador DSRM.*** Usted utiliza la cuenta para iniciar el Domain Controller en Directory Services Restore Mode.

### 3.2.1. Practica 1: ¿Cómo crear la estructura del Forest y el Domain?

Usted utiliza Active Directory Installation Wizard para crear la estructura de forest y domain. Cuando instale Active Directory por primera vez en una red, tendrá que crear el Forest Root Domain, y después de ello utilizar el wizard para crear trees y Child Domains adicionales.

El Active Directory Installation Wizard guíará a Usted en el proceso de la instalación y le solicitará la información necesaria, que varía según las opciones que seleccione.

***Para crear el Forest Root Domain, deberá realizar los siguientes pasos:***

1. Hacer click en ***Start***, después en ***Run*** y escribir ***dcpromo***. Luego presionar Enter. El Wizard verificará:
   - Si el usuario actualmente validado es un miembro del grupo de administradores locales.
   - Si en la computadora está funcionando en un sistema operativo que soporte Active Directory.
   - Si una instalación o un retiro anterior de Active Directory no ha ocurrido sin reiniciar la computadora, o que una instalación o un retiro de Active Directory no está en marcha. Si cualesquiera de estas cuatro verificaciones fallan, un mensaje de error aparecerá y Usted saldrá del wizard.
2. En la página ***Welcome,*** hacer click en ***Next***.
3. En la página ***Operating System Compatibility***, hacer click en ***Next***.
4. En la página ***Domain Controller Type***, hacer click en ***Domain controller for a new domain***, y después hacer click en ***Next***.
5. En la página ***Create New Domain***, hacer click en Domain in a new forest, y después en ***Next***.
6. En la página ***New Domain Name***, ingresar el DNS Name para el nuevo domain (nwtraders.msft), y después hacer click en ***Next***.
7. En la página NetBIOS Domain Name, verificar NetBIOS Name (NWTRADERS), y después hacer click en Next.
   El nombre NetBIOS identifica el domain a las computadoras de cliente corriendo versiones anteriores de Windows y Windows NT. El wizard verifica que le nombre NetBIOS sea único. Si no lo es, le pedirá cambiar el nombre.
8. En la página ***Database and Log Folders***, especificar la localización en la cual se desea instalar las carpetas de la base de datos y de los logs. Después hacer click en ***Next***.
9. En la página ***Shared System Volume***, especificar la locación en la cual se desea instalar la carpeta de SYSVOL, o hacer click en ***Browse*** para elegir una locación, y después hacer click en ***Next***.
10. En la pagina ***DNS Registration Diagnostics***, verificar si un servidor existente de DNS es autoritario para este forest o, en caso de necesidad, hacer click en ***Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server***, y después hacer click en ***Next***.
11. En la pagina ***Permissions***, especificar se si asignan los permisos por defecto en los objetos usuario y grupo compatible con los servidores que funcionan con versiones anteriores de Windows o Windows NT, o solamente con los servidores Windows Server 2003.
12. Cuando se pregunte, especificar el password para Directory Services Restore Mode. Los Domain Controllers Windows Server 2003 mantienen una versión pequeña de la base de datos de cuentas de Microsoft Windows NT 4.0. La única cuenta en esta base de datos es la cuenta del administrador y la misma se requiere para la autentificación al encender la computadora en Directory Services Restore mode, porque Active Directory no se inicia de este modo.
13. Repasar la página ***Summary***, y después hacer click en ***Next*** para comenzar la instalación.
14. Cuando se pregunte, reiniciar la computadora.

### 3.2.2 Práctica 2 (Opcional): ¿Cómo agregar un Domain Controller adicional?

Para llevar a cabo esta práctica Usted necesitará dos computadoras o dos Virtual PC, con un Domain Controller instalado (Práctica 1) y un Windows Server 2003.

El procedimiento es similar a la creación de un nuevo Domain Controller; solamente se debe seleccionar, en la primera pantalla del wizard, la opción ***Add additional Domain Controller for existing domain***. El resto del proceso se puede realizar de dos formas:

1. ***Over the network:*** Esto requiere, en el caso que Usted tenga gran cantidad de objetos, un enlace con ancho de banda suficiente o bastante tiempo para la replica inicial.
2. new! ***Replicate from Media:*** Esta nueva característica de Windows Server 2003, permite realizar la replica inicial por medio de un backup, de la siguiente manera:
   - Primero debe realizar un backup del System State en el Domain Controller existente.
   - Luego debe hacer llegar ese backup a la computadora destino.
   - En la computadora destino deberá realizar la operación de restore en una locación alternativa ( Elija una carpeta ej: C:\NTDSRestore)
   - Por último corra el wizard ***dcpromo /adv***
   - El wizard le permitirá seleccionar la opción ***From Media***

## 3.3. new! ¿Cómo renombrar un Domain Controller?

En Windows Server 2003, Usted puede renombrar un Domain Controller después que haya sido instalado. Para renombrar un Domain Controller, deberá tener derechos de Domain Admin.

Cuando Usted renombre un Domain Controller, deberá agregar el nuevo nombre del Domain Controller y remover el nombre viejo de las bases de DNS y Active Directory. El renombrado de un Domain Controller es solamente posible si el Domain Functional Level es configurado como Windows Server 2003.

***Para renombrar un Domain Controller, deberá realizar los siguientes pasos:***

1. En Control Panel, hacer doble-click en ***System***.
2. En el cuadro ***System Properties***, en ***Computer Name***, hacer click ***Change***.
3. Cuando se pregunte, confirmar si se desea renombrar el Domain Controller.
4. Incorporar el nombre de computadora completo (incluyendo el primary DNS suffix), y después hacer click en ***OK***.

Usted podrá cambiar el Primary DNS suffix de un Domain Controller cuando renombre el Domain Controller. Sin embargo, el cambiar el Primary DNS suffix no mueve el Domain Controller a un nuevo Active Directory domain. Por ejemplo, si Usted renombra dc2.nwtraders.msft a dc1.contoso.msft, la computadora sigue siendo un Domain Controller del dominio nwtraders.msft, aunque su Primary DNS suffix es contoso.msft. Para mover un Domain Controller a otro domain, Usted debe primero degradar el Domain Controller y entonces promoverlo en el nuevo dominio.

Obtenga información acerca de instalación de Active Directory:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324753

http://support.microsoft.com/default.aspx?scid=kb;en-us;816106

http://support.microsoft.com/default.aspx?scid=kb;en-us;816108

### 3.4. ¿Cómo solucionar problemas en la instalación de Active Directory?

Al instalar Active Directory, Usted puede encontrar problemas. Éstos pueden ser credenciales incorrectas de seguridad, el uso de nombres que no son únicos, una red no fiable o recursos escasos.

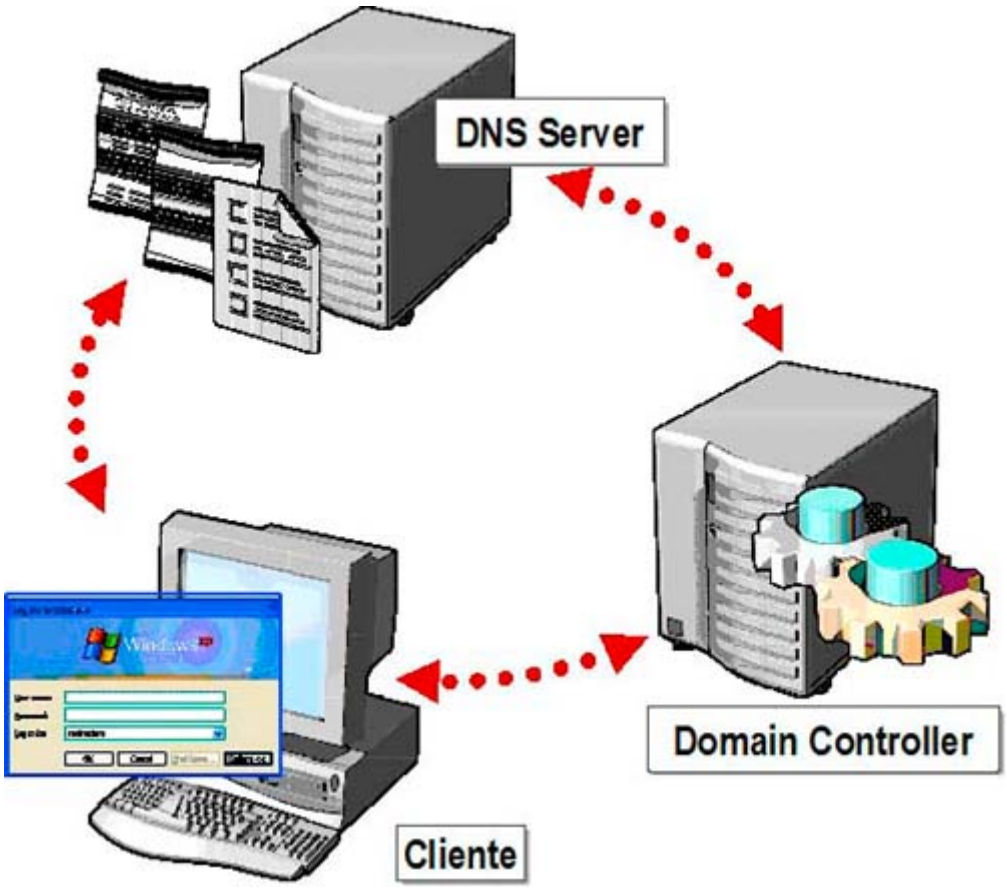
A continuación se describen algunos problemas comunes que Usted puede llegar a encontrar mientras instala Active Directory, y algunas estrategias para resolverlos.

***Tener acceso negado mientras que crea o agrega Domain Controllers.*** Cerrar la sesión y después iniciar con una cuenta que pertenezca al grupo local de administradores. Las credenciales deben ser de un usuario que sea miembro de Domain Admins o Enterprise Admins.

***El nombre DNS o NetBIOS del domain no es único*** Cambiar el nombre a un nombre único.

***El domain no puede ser contactado*** Comprobar que haya conectividad de red entre el servidor que Usted está promoviendo a Domain Controller y que por lo menos haya un Domain Controller en el dominio. Utilizar el comando ping desde command prompt para probar la conectividad con cualquier Domain Controller del dominio. Verificar que el DNS proporcione la resolución de nombres, por lo menos a un Domain Controller en el dominio.

## 4. ¿Qué son las zonas DNS Active Directory Integrated?



## 4.1. Introducción

Una ventaja de integrar el DNS y Active Directory es la capacidad de integrar zonas de DNS en la base de datos de Active Directory. Una zona es una porción del Domain Namespace, que agrupa registros lógicamente, permitiendo transferencias de zona de éstos registros para funcionar como una unidad.

## 4.2. Zonas Active Directory Integrated

Los Microsoft DNS Servers almacenan la información que es utilizada para resolver nombres de host a direcciones IP y direcciones IP a nombres de host, usando una base de datos en formato de archivo que tenga una extensión .dns para cada zona.

***Las Zonas Active Directory Integrated*** son primarias y stub, y se almacenan como objetos en la base de Active Directory. Usted puede almacenar objetos de zona en Active Directory Application Partition o en Active Directory Domain Partition. Si los objetos de zona se almacenan en Active Directory Application Partition, solamente los Domain Controllers que suscriban a esa Application Partition pueden participar en la réplica de esta partición. Sin embargo, si los objetos de zona se almacenan en Active Directory Domain Partition, se replican a todos los Domain Controllers en el dominio.

## 4.3. Ventajas de Zonas Active Directory Integrated

***Las Zonas Active Directory Integrated ofrecen las siguientes ventajas.***

- ***Multimaster replication.*** Cuando Usted configura Zonas Active Directory Integrated, las actualizaciones dinámicas al DNS se basan en el modelo multimaster. En este modelo, cualquier servidor autoritativo DNS, por ejemplo un Domain Controller corriendo DNS Server, es primario para la zona. Dado que la Master Copy de la zona se mantiene en la base de Active Directory (la cual se replica completamente a todos Domain Controllers del dominio), la zona se puede actualizar por los DNS Servers funcionando en cualquier Domain Controller del dominio.

- ***Secure dynamic updates.*** Debido a que las zonas de DNS son objetos de Active Directory en Zonas Active Directory Integrated, Usted puede aplicar permisos a los registros dentro de esas zonas y también puede controlar qué computadoras pueden actualizar sus registros. De esta manera, las actualizaciones que utilizan el protocolo dinámico de actualización pueden venir solamente de las computadoras autorizadas.

Para obtener más información acerca de Zonas Active Directory Integrated:

http://support.microsoft.com/default.aspx?scid=kb;en-us;816101

## 4.4. Práctica 3: Verificación de Zona integrada con Active Directory

Durante esta práctica Usted verificará si su DNS Server, tiene la zona integrada con Active Directory.

***Para verificar DNS:***

1. Abrir la consola de DNS.
2. Hacer click en el nombre del server.
3. Hacer click en la zona a verificar.
4. Hacer click derecho en la zona, y después en ***Properties***.
5. En el cuadro ***zone type***, verificar ***Active Directory Integrated***
6. Para cambiar el tipo de zona, hacer click en ***Change***.

## 5. ¿Qué es la funcionalidad de Forest y Domain?

| Ambiente de red | Domain functional levels | Forest functional levels |
|---|---|---|
| Windows 2000 mixed-mode domain | ✓ | |
| Windows 2000 native-mode domain | ✓ | ✓ |
| Windows Server 2003 Domain | ✓ | ✓ |
| Windows Server 2003 Interim | ✓ | |

### 5.1. Introducción

En Windows Server 2003, la funcionalidad de forest y domain proporciona una manera de permitir características nuevas forest-wide o domain-wide de Active Directory en su ambiente de red. Diversos niveles de la funcionalidad del forest y del dominio están disponibles, dependiendo de su ambiente de red.

### 5.2. ¿Qué es la funcionalidad de dominio?

La funcionalidad del dominio habilita las características que afectarán el dominio entero y solamente ese dominio. Cuatro niveles funcionales de dominio están disponibles:

- ***Windows 2000 mixed.*** Éste es el nivel funcional por defecto. Usted puede levantar el nivel funcional del dominio a Windows 2000 native o Windows Server 2003. Los dominios Mixed-mode pueden contener Windows NT 4.0 backup Domain Controllers, pero no pueden utilizar grupos de seguridad universales, anidamiento de grupos o capacidades de Security Identifier (SID) History.
- ***Windows 2000 native.*** Usted puede utilizar este nivel funcional si el dominio contiene solamente Domain Controllers Windows 2000 y Windows Server 2003. Aunque los Domain Controllers funcionen en Windows 2000 Server, no están preparados para la funcionalidad de dominio. Características de Active Directory, como grupos de seguridad universales, anidamiento de grupos y capacidades de Security Identifier (SID) History, están disponibles.
- ***Windows 2003 Server.*** Este es el nivel funcional más alto para un dominio. Usted puede utilizarlo solamente si todos los Domain Controllers en el dominio funcionan en Windows Server 2003. Todas las características de Active Directory para el dominio están disponibles para su uso.
- new! ***Windows 2003 Interim.*** Este nivel es un nivel funcional especial que soporta Domain Controllers Windows NT 4.0 y Windows server 2003.

### 5.3. new! ¿Qué es la funcionalidad de forest?

La funcionalidad de forest habilita características a través de todos los dominios dentro de su forest. Dos niveles funcionales de forest están disponibles: Windows 2000 y Windows Server 2003. Por defecto, los forests funcionan en nivel funcional Windows 2000. Usted puede elevar el nivel funcional del forest a Windows Server 2003, para que habilite las características que no están disponibles en el nivel funcional Windows 2000, incluyendo:

- Relaciones de confianza entre forest
- Replicación mejorada

**Importante:** Usted no puede bajar el nivel funcional del dominio o del forest después que se haya elevado.

## 5.4. new! Requisitos para habilitar nuevas características en Windows Server 2003

| Requisito | Domain | Forest |
|---|---|---|
| **Domain controllers corriendo:** | Windows Server 2003 | Windows Server 2003 |
| **El nivel funcional del dominio debe ser :** | Elevado a Windows Server 2003 | Capaz de ser elevado a Windows Server 2003 |
| **Administrator:** | Administrador del dominio para elevar el nivel funcional del dominio | Enterprise administrator para elevar el nivel funcional del forest |

### 5.4.1 new! Introducción

Además de las características básicas de Active Directory en Domain Controllers individuales, nuevas características forest-wide y domain-wide están disponibles cuando se cumplen ciertas condiciones.

Para habilitar las nuevas características domain-wide, todos los Domain Controllers en el dominio deben correr Windows Server 2003, y el nivel funcional del dominio se debe elevar a Windows Server 2003. Usted debe ser administrador del dominio para elevar el nivel funcional del dominio.

Para habilitar las nuevas características forest-wide, todos los Domain Controllers en el forest deberán correr Windows Server 2003, y el nivel funcional del forest se debe elevar a Windows Server 2003. Usted debe ser Enterprise Administrator para elevar el nivel funcional del forest.

Para obtener mas información acerca de niveles de funcionalidad:

http://support.microsoft.com/default.aspx?scid=kb;en-us;322692

### 5.4.2 Práctica 4: ¿Cómo elevar el nivel funcional?

Elevar la funcionalidad del forest y del dominio a Windows Server 2003 habilita ciertas características, por ejemplo, forest trusts, que no está disponible en otros niveles funcionales. Usted puede elevar la funcionalidad del forest y del dominio usando Active Directory Domains and Trusts.

***Para elevar el nivel funcional del dominio, debe realizar los siguientes pasos:***

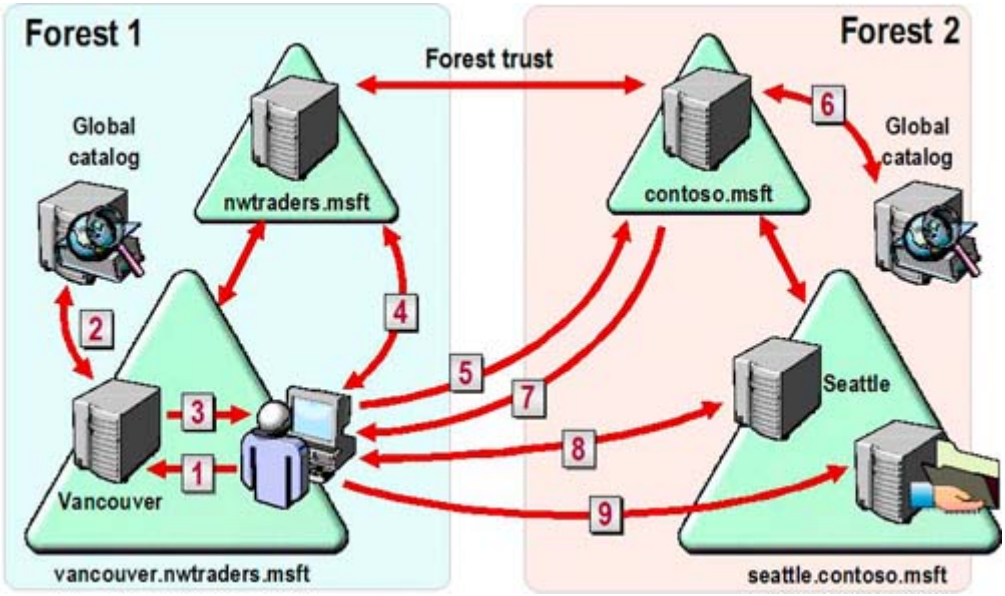
1. Abrir Active Directory Domains and Trusts.
2. Hacer click derecho en la consola, en el nodo para el nivel funcional de dominio que usted desea elevar, y después hacer click en ***Raise Domain Functional Level***.
3. Seleccionar el nivel funcional Windows Server 2003 en el cuadro ***Select an available domain functional level***, y después hacer click en ***Raise***.

***Para elevar el nivel funcional del forest, deberá realizar los siguientes pasos:***

1. En Active Directory Domains and Trusts, en la consola, hacer click derecho en ***Active Directory Domains and Trusts***, y después click en ***Raise Forest Functional Level***.
2. En el cuadro ***Select an available forest functional level***, seleccionar ***Windows Server 2003***, y después hacer click en ***Raise***.

**Nota:** Usted debe elevar el nivel funcional de todos los dominios en un forest a Windows 2000 native o más alto, antes de elevar el nivel funcional del forest.

## 6. ¿Cómo funcionan los Trusts entre Forests?




### 6.1. Introducción

Windows Server 2003 soporta cross-forest trusts, el cual permite que los usuarios en un forest tengan acceso a recursos en otro forest. Cuando un usuario intente tener acceso a un recurso en un trusting forest, Active Directory primero localizará el recurso.

Después de localizar el recurso, el usuario podrá ser autenticado y tener acceso al recurso. Entender cómo este proceso trabaja, le ayudará a localizar problemas que pueden presentarse con cross-forest trusts.

### 6.2. ¿Cómo es accedido un recurso?

Lo que sigue es una descripción de cómo un cliente Windows 2000 Professional o Windows XP Professional localiza y tiene acceso a un recurso en otro forest que tenga Windows 2000 Server o Windows Server 2003 server.

1. Un usuario que inicia sesión al dominio vancouver.nwtraders.msft intenta tener acceso a una carpeta compartida en el forest contoso.msft. La computadora del usuario contacta al KDC en un domain controller en vancouver.nwtraders.msft y solicita un service ticket usando el SPN de la computadora, donde reside el recurso. Un SPN puede ser el nombre de DNS de un host o dominio, o puede ser el Distinguished Name de un Service Connection Point Object.
2. El recurso no se encuentra en vancouver.nwtraders.msft y el Domain Controller de vancouver.nwtraders.msft realiza queries al Global Catalog para ver si el recurso está situado en

otro dominio en el forest. Dado que el Global Catalog contiene solamente la información sobre su propio forest, no encuentra el SPN. El Global Catalog entonces comprueba su base de datos para saber si hay información sobre forest trusts establecidos con su forest. Si el Global Catalog encuentra uno, compara los name suffixes que están listados en el forest trust TDO para el suffix de destino SPN. Después de encontrar una igualdad, el Global Catalog proporciona la información de routing sobre cómo localizar el recurso al Domain Controller en vancouver.nwtraders.msft.

3. El Domain Controller en vancouver.nwtraders.msft envía una referencia para su dominio Parent, nwtraders.msft, a la computadora del usuario.
4. La computadora del usuario contacta al Domain Controller en nwtraders.msft por la referencia al Domain Controller del Forest Root Domain del forest contoso.msft.
5. Usando la referencia del Domain Controller en nwtraders.msft, la computadora contacta al Domain Controller en el forest contoso.msft para el pedido de servicio al service ticket.
6. El recurso no está situado en el Forest Root Domain del forest contoso.msft, y por eso el Domain Controller contacta a su Global Catalog para buscar el SPN. El Global Catalog busca el SPN y lo envía al Domain Controller.
7. El Domain Controller envía la referencia seattle.contoso.msft a la computadora del usuario.
8. La computadora del usuario contacta al KDC en el Domain Controller en seattle.contoso.msft y negocia el ticket para el acceso del usuario al recurso en el dominio seattle.contoso.msft.
9. La computadora envía el server service ticket a la computadora en la cual está el recurso compartido, donde se leen las credenciales de seguridad del usuario y se construye el access token, que da el acceso de usuario al recurso.

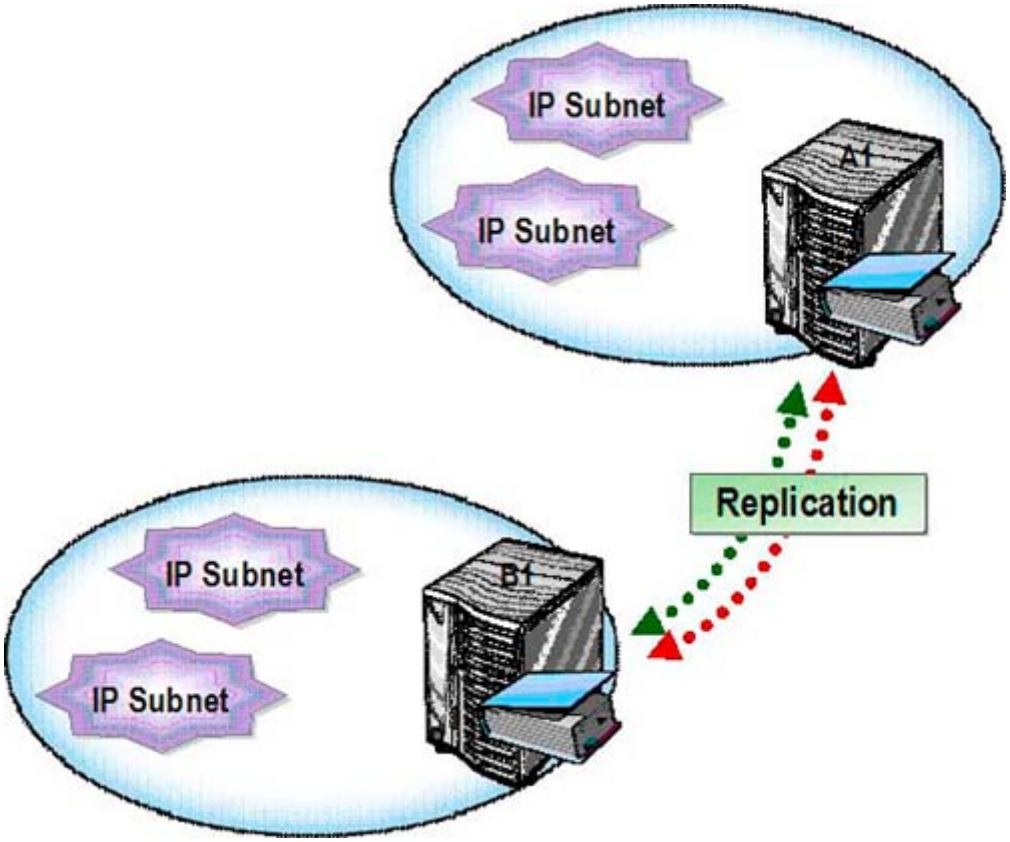
**Nota:** Recuerde que para poder utilizar esta nueva característica, debe tener los dos forest en nivel Windows Server 2003. Los trust entre forest en Windows Server 2003 le permiten validar usuarios usando Kerberos v5, utilizando la seguridad propia del protocolo. También le permite que los trust sean transitivos entre dos forest, no así, en múltiples forest. Por ejemplo: El forestA tiene establecido un trust con el forest B, y todos los dominios en los dos forest pueden utilizar el trust. Pero si a su vez el forest B tiene un trust con el forest C, no existe ningún tipo de relación entre el forest A y el forest C.

Para obtener más información acerca de trust:

http://support.microsoft.com/default.aspx?scid=kb;en-us;325874

http://support.microsoft.com/default.aspx?scid=kb;en-us;816301

## 7. Replicación en Active Directory




### 7.1. Replicación dentro de Sites

***Los puntos dominantes de la replicación de Active Directory dentro de site son:***

- ***La replicación ocurre cuando hay:***
  - Una adición de un objeto a Active Directory.
  - Una modificación de los valores de un atributo de objeto.
  - Un cambio de nombre de un contenedor de objetos.
  - Una eliminación de un objeto del directorio.

- ***Change notification.*** Cuando un cambio ocurre en un domain controller, el domain controller notifica a sus replication partners en el mismo site. Este proceso se llama change notification.

- ***Replication latency.*** Retraso entre el tiempo que ocurre un cambio y el tiempo que la actualización alcanza a todos los Domain Controllers en el site. Por defecto la Replication Latency es 15 segundos.

- ***Urgent replication.*** En lugar de esperar el tiempo por defecto, los atributos sensibles de seguridad que se actualizan disparan un inmediato mensaje de change notification.

- ***Convergence.*** Cada actualización en Active Directory eventualmente propaga a todos los Domain Controllers en el site que contiene la partición en la cual la actualización fue hecha. Esta propagación completa se llama convergence.

- ***Propagation dampening.*** El proceso de prevenir la réplica innecesaria. Cada Domain Controller asigna a cada cambio de atributo y objeto un Update Sequence Number (USN) para prevenir la réplica innecesaria.

- ***Conflicts.*** Cuando actualizaciones concurrentes que originan en dos réplicas master separadas son inconsistentes, los conflictos pueden presentarse. Active Directory resuelve tres tipos de conflictos: atributo, Contenedores eliminados, y conflictos de Relative Distinguished Name (RDN).

- ***Globally unique stamp.*** Active Directory mantiene un stamp que contiene el version number, timestamp, y server globally unique identifier (GUID) que Active Directory creado durante la actualización originaria.

## 7.2. new! Linked Multivalued Attributes

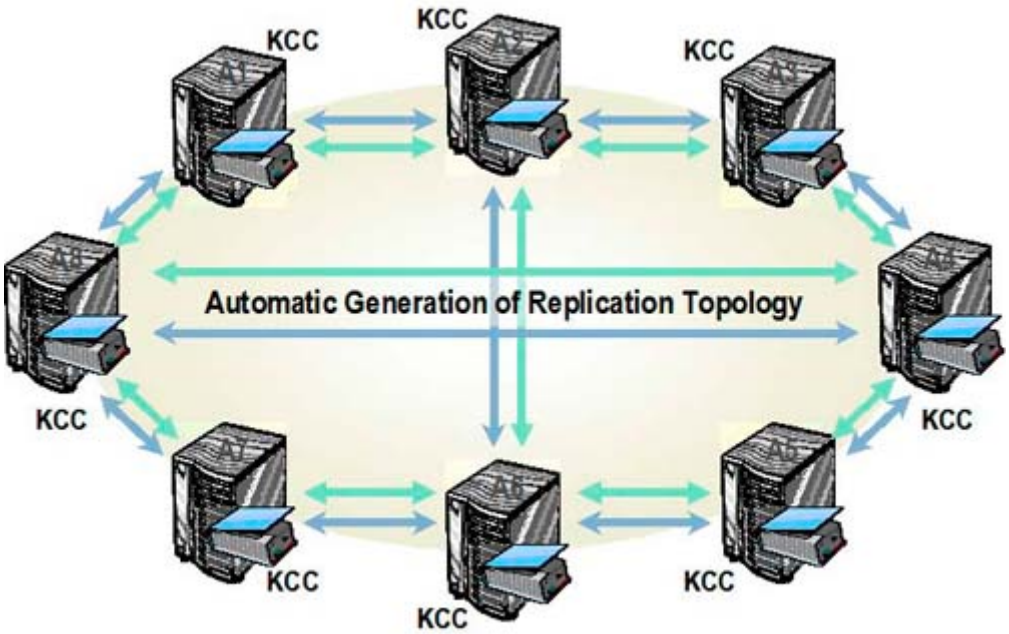
***El proceso por el cual linked multivalued attributes se replican varía, dependiendo del nivel funcional del forest:***

Cuando el nivel funcional del forest es menor que Windows Server 2003, cualquier cambio que fuera realizado a un atributo de miembros de grupo dispara la réplica de la lista entera del atributo miembro. El multivalued **member** attribute se considera un solo atributo con el fin de la réplica en este caso. Esta réplica aumenta la probabilidad de sobreescribir un cambio del atributo miembro que otro administrador realizó en otro domain controller, antes que el primer cambio fuera replicado.

Cuando el nivel funcional del forest se cambia a Windows Server 2003, un valor individual replica cambios a linked multivalued attributes. Esta funcionalidad mejorada replica solamente cambios del atributo miembro de grupo y no a la lista entera del atributo de miembro.

De esta forma se elimina la restricción de 5000 usuarios máximo por grupo, esta restricción estaba dada en Windows 2000 por el valor máximo que puede tener el atributo de miembros de un grupo.

## 7.3. new! Generación automática de la topología de replicación



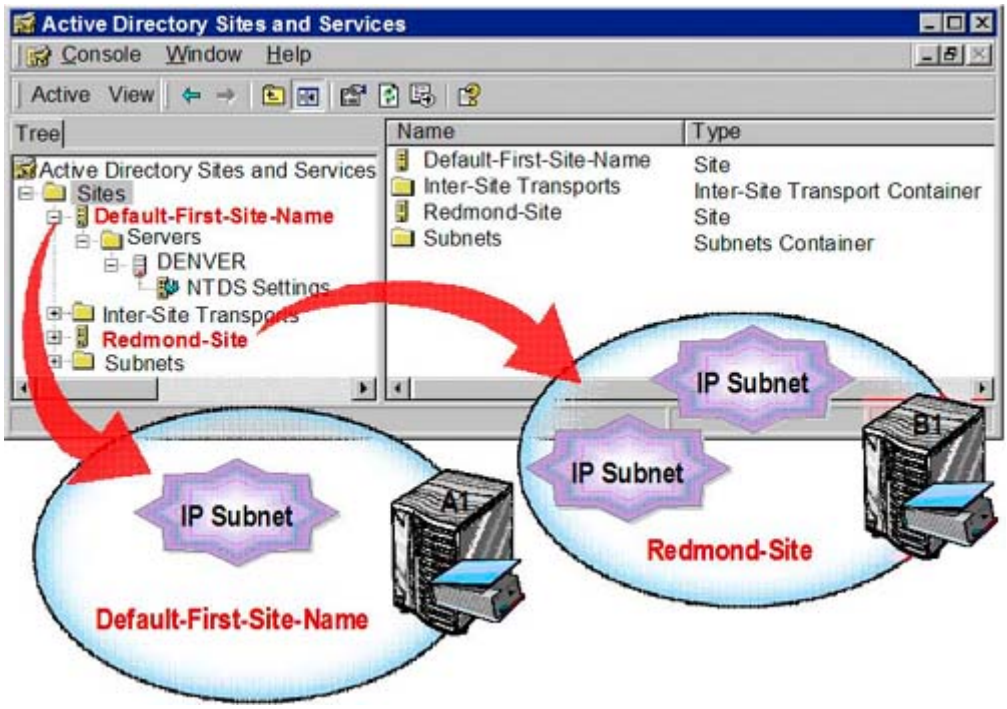

Cuando usted agrega Domain Controllers a un site, Active Directory usa el Knowledge Consistency Checker (KCC) para establecer una trayectoria de la réplica entre Domain Controllers.

El KCC es un proceso que funciona en cada Domain Controller y genera la topología de la réplica para todas las particiones del directorio que se contengan en ese Domain Controller. El KCC corre en los intervalos específicos cada 15 minutos por defecto y diseña las rutas de replicación entre Domain Controllers de las conexiones más favorables que están disponibles en ese momento.

Este proceso fue mejorado con respecto al proceso de Windows 2000, haciendo que esta nueva característica elimine la limitación existente de un máximo de 500 sites en Active Directory. Actualmente se ha probado hasta 3000 sites y el soporte máximo es de 5000 sites.

**Nota:** Para aprovechar esta característica usted debe tener el forest en nivel funcional Windows Server 2003 ó Windows Server 2003 Interim.

## 7.4. Creando y Configurando Sites




Usted utiliza sites para controlar el tráfico de replicación, tráfico de logon y las queries del cliente al Global Catalog Server.

### 7.4.1. ¿Qué son los sites?

En Active Directory, los sites ayudan a definir la estructura física de una red. Una o más subnets TCP/IP en una rango definido de direcciones define un site, el cual define alternadamente un grupo de Domain Controllers que tienen velocidad y costo similares. Los Sites consisten en objetos server, que contienen objetos de conexión que permiten la réplica.

### 7.4.2. ¿Qué son objetos subnet?

Los objetos subnet identifican las direcciones de red las cuales utilizan las computadoras en los sites. Una subnet es un segmento de una red TCP/IP a la cual se asigna un sistema de direcciones lógicas IP. Dado que objetos subnet representan la red física, éstos hacen sites. Por ejemplo, si tres subnets están situados en tres campus en una ciudad, y estos campus están conectados con high-speed, conexiones altamente disponibles, usted podría asociar cada una de esas subnets a un site. Un site puede consistir en una o más subnets. Por ejemplo, en una red que tiene tres subnets en Redmond y dos en París, usted puede crear un site en Redmond, un site en Paris, y entonces agregar las subnets a los sites respectivos.

### 7.4.3. ¿Qué son los Site Links?

***Los Site Links son conexiones que usted puede hacer entre sites para***:

- Habilitar la replicación
- Manejar los horarios en los cuales usted quiere replicar,
- Manejar un costo de acuerdo al enlace que este utilizando, y el protocolo de replicación IP (RPC) o SMTP.

Para obtener mas información acerca de sites:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323349

### 7.4.4 Práctica 5: Creando y Configurando Sites y Subnets

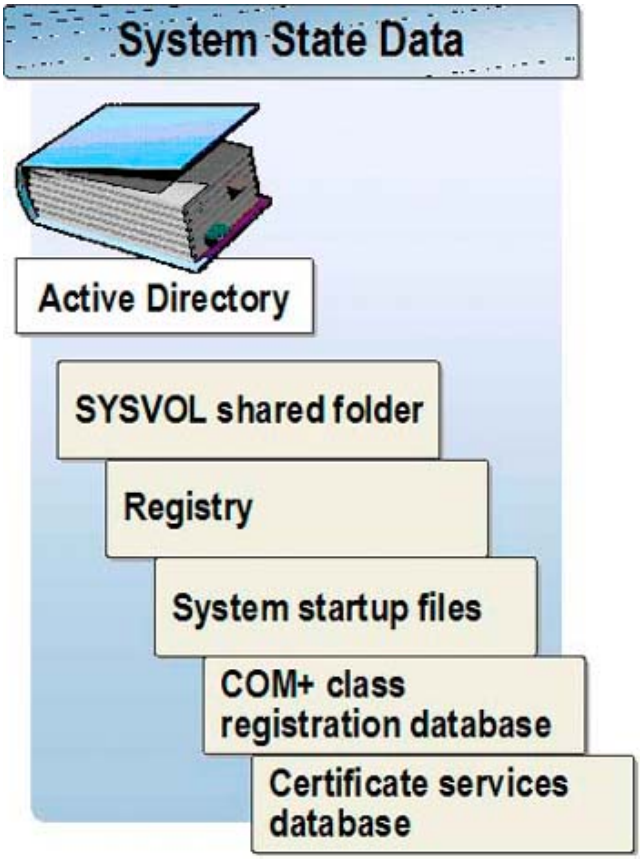
***Para crear un site, deberá realizar los siguientes pasos:***

1. Abrir Active Directory Sites and Services del menu ***Administrative Tools***.
2. Hacer click derecho en ***Sites*** en la consola, y después hacer click en ***New Site***.
3. Ingresar el nombre del nuevo site en el cuadro ***Name***.
4. Hacer click en un site link object, y después hacer click en ***OK*** dos veces.

***Para crear un subnet object, deberá realizar los siguientes pasos:***

1. En Active Directory Sites and Services, en la consola, hacer doble-click en ***Sites***, hacer click derecho en ***Subnets***, y después hacer click en ***New Subnet***.
2. En el cuadro ***Address***, ingresar la dirección IP de la subnet.
3. En el cuadro ***Mask***, ingresar la subnet mask que describe el rango de direcciones de la subnet.
4. Seleccionar el site a asociar con la subnet, y después hacer click en ***OK***.

## 8. Haciendo backup de Active Directory




Hacer backup de Active Directory es esencial para mantener la base de datos de Active Directory. Usted puede hacer backup de Active Directory usando una graphical user interface (GUI) y herramientas command-line, que provee Windows Server 2003.

Usted con frecuencia debe hacer backup del System State data en Domain Controllers de modo que pueda restaurar los datos más actuales. Estableciendo un schedule regular de backup, Usted tiene una mejor ocasión de recuperación de datos cuando sea necesario.

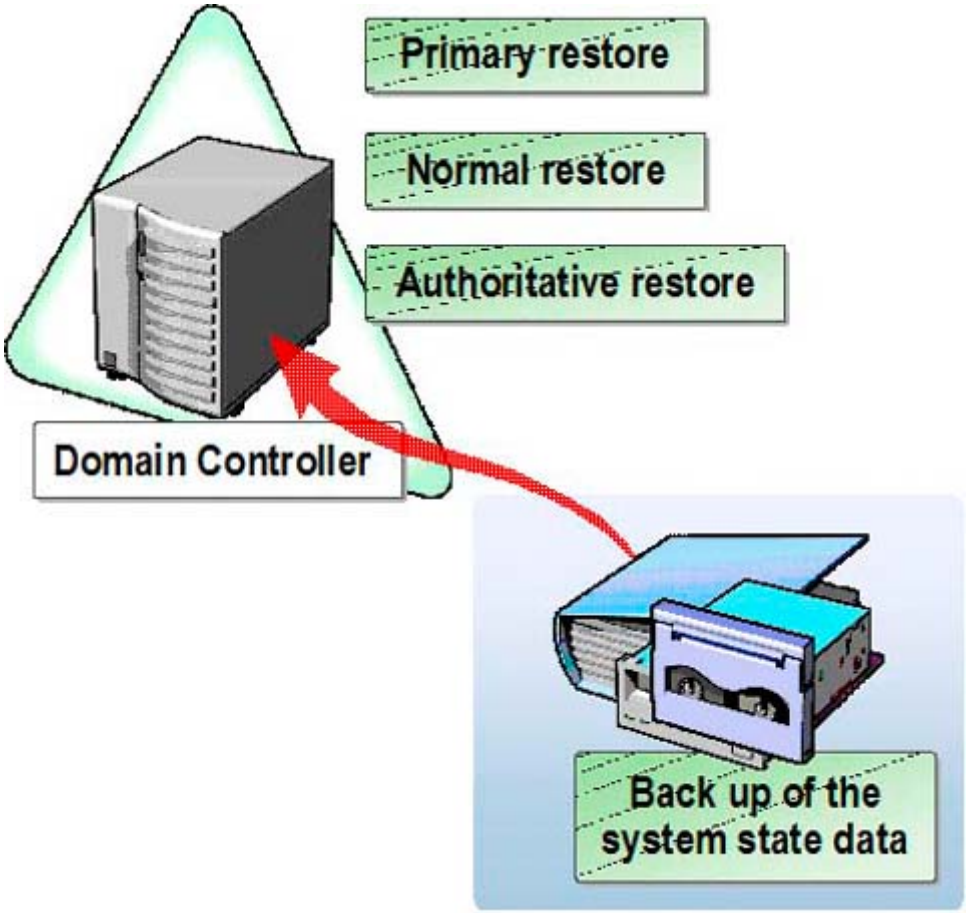
***El System State Data en un Domain Controller incluye los siguientes componentes:***

***Active Directory.*** El System State Data no contiene Active Directory a menos que el servidor en el cual Usted está haciendo backup del System State Data sea un Domain Controller. Active Directory está presente solamente en Domain Controllers.
***The SYSVOL shared folder.*** Esta carpeta compartida contiene plantillas de Group Policy y logon scripts. La carpeta compartida SYSVOL está presente solamente en domain controllers.
***The registry.*** Este repositorio base de datos contiene la información sobre la configuración de la computadora.
***System startup files.*** Windows Server 2003 requiere estos archivos durante su fase de encendido inicial. Incluyen los boot y archivos de sistema que están protegidos por Windows file protection.
***The COM+ Class Registration database.*** La base de datos Class Registration contiene información sobre Component Services applications.
***The Certificate Services database.*** Esta base de datos contiene los certificados del servidor que Windows Server 2003 utiliza para autenticar usuarios. Esta base solamente está presente si el servidor está funcionando como certificate server.

***Para realizar la operación de backup usted puede utilizar la herramienta provista por Windows Server 2003:***

1. Hacer click en ***Backup*** en el menu ***Start***, ***All Programs***, ***Accessories***, ***System Tools***.
2. Hacer click en ***Next*** en la página ***Welcome to the Backup or Restore Wizard***.
3. En la página ***Backup or Restore***, hacer click en ***Backup files and settings***, y después hacer click en ***Next***.
4. En la página ***What to Back Up***, hacer click en ***Let me choose what to back up***, y después hacer click en ***Next***.
5. En la página ***Items to Back Up***, expandir ***My Computer***, seleccionar el ***System State***, y después hacer click en ***Next***.
6. En la página ***Backup Type, Destination, and Name***, hacer click en ***Browse***, seleccionar una locación para el backup, hacer click en ***Save***, y después hacer click en ***Next***.
7. En la página ***Completing the Backup or Restore Wizard***, hacer click en ***Finish***.
8. En la página ***Backup Progress***, hacer click en ***Close***.

## 8.1 Restauración de Active Directory



Usted puede utilizar uno de los tres métodos para restaurar Active Directory de medios de backup: primary restore, normal (nonauthoritative) restore, y authoritative restore.

1. ***Primary restore.*** Este método reconstruye el primer domain controller en el dominio cuando no hay otra manera de reconstruir el dominio. Realizar un primary restore solamente cuando todos los domain controllers en un domain se perdieron, y usted desea reconstruir el dominio usando el backup.

2. ***Normal restore.*** Este método reinstala los datos de Active Directory al estado antes del backup, actualiza los datos con el proceso normal de réplica. Realizar un normal restore solamente cuando usted desea restaurar un solo domain controller a un buen estado previamente conocido.

3. ***Authoritative restore.*** Usted realiza este método en tándem con un restore normal. Un restore autoritativo marca datos específicos y evita que la réplica sobreescriba esos datos. Los datos autoritativos entonces se replican a través del dominio.

***Para realizar un primary restore de Active Directory, deberá realizar los siguientes pasos:***

1. Reiniciar su domain controller en Directory Services Restore Mode.
2. Iniciar la utilidad de Backup.
3. Hacer click en ***Advanced Mode*** en la página ***Welcome to the Backup or Restore Wizard***,
4. En la página ***Welcome to Backup Utility Advanced Mode***, sobre ***Restore and Manage Media***, seleccioar qué desea restaurar, y después hacer click en ***Start Restore***.
5. En el cuadro ***Warning***, hacer click en ***OK***.
6. En el cuadro ***Confirm Restore***, hacer click en ***Advanced***.
7. En el cuadro ***Advanced Restore Options***, hacer click en ***When restoring replicated data sets, mark the restored data as the primary data for all replicas***, y después hacer click en ***OK*** dos veces.
8. En el cuadro ***Restore Progress***, hacer click en ***Close***.
9. En el cuadro ***Backup Utility***, hacer click en ***Yes***.

# Capítulo 5
# Implementación, Administración y Monitoreo de Group Policy

Durante este capítulo Usted irá asimilando los conocimientos que necesita para hacer una correcta administración, diseño e implementación de Group Policy.

Para poder realizar las prácticas de esta unidad es necesario que haya concluido las prácticas de los capítulos 2 y 3.

## 1. Introducción

Usted utiliza Group Policy en Active Directory® para centralizar el manejo de usuarios y computadoras en una empresa. Configurando Group Policy puede centralizar policies para una organización entera, dominio, sitio u organizational unit, y asimismo puede descentralizar la configuración de Group Policy, configurándolo para cada departamento en el nivel organizational unit.

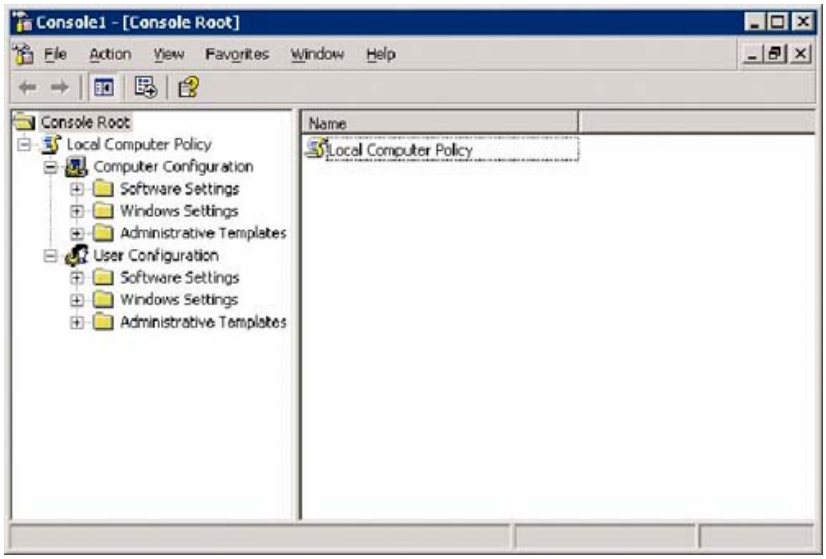
Usted puede asegurarse que los usuarios tengan los ambientes que requieren para realizar sus trabajos y hacer cumplir las políticas de las organizaciones, incluyendo reglas de negocio, metas y requisitos de seguridad. Además, puede bajar el Total Cost of Ownership controlando ambientes del usuario y de computadora, de modo tal que se reduzca el nivel de ayuda técnica a los usuarios y la productividad perdida de los mismos a causa de sus errores.

***Al terminar este capítulo Usted podrá:***

- Crear y configurar Group Policy objects (GPOs).
- Configurar intervalos de actualización de Group Policy y configuraciones de Group Policy.
- Administrar GPOs.

### 1.1. ¿Qué es Group Policy?

Group Policy le otorga control de administración sobre los usuarios y las computadoras de su red, y por lo tanto le permite definir el estado del ambiente de trabajo de los usuarios una sola vez, confiando en Microsoft® Windows® Server 2003 para hacer cumplir continuamente la configuración de Group Policy que definió. También podrá aplicar configuraciones de Group Policy a través de una organización entera o a grupos específicos de usuarios y de computadoras.




Para más información acerca de Group Policy:

Microsoft IntelliMirror®.

Group Policy Settings Overview.

## 1.2. ¿Qué son User y Computer Configuration Settings?

Usted puede hacer cumplir los Group Policy Settings para las computadoras y los usuarios usando Computer Configuration y User Configuration en Group Policy.


***Group Policy Settings*** para usuarios incluye configuraciones específicas del sistema operativo, configuraciones de escritorio, configuraciones de seguridad, opciones de aplicaciones assigned y published, configuraciones de aplicaciones, opciones de folder redirection, y scripts de user logon y logoff. Los Group Policy Settings de usuario se aplican cuando los usuarios inician sesión en la computadora y durante un ciclo de actualización periódico.

Group Policy Settings modifica el ambiente de escritorio del usuario para los requisitos particulares o hace cumplir lockdown policies en usuarios, y está contenido debajo de ***User Configuration*** en el editor de Group Policy Object.

***Debajo de User Confiugration, también se encuentran:***

- La carpeta Software Settings: contiene configuraciones de software que se aplican a los usuarios sin importar en qué computadora inicien sesión. Esta carpeta también contiene configuraciones que se coloquen allí de Independent Software Vendors (ISVs).

- La carpeta Windows Settings: contiene configuración Windows que se aplica a los usuarios sin importar en qué computadora inicien sesión. Esta carpeta también contiene los siguientes puntos: **Folder Redirection, Security Settings y Scripts**.

Group Policy Settings para las computadoras incluye la manera en que el sistema operativo se comporta, el comportamiento de escritorio, configuraciones de seguridad, scripts de startup y shutdown, opciones de aplicaciones assigned a la computadora y configuraciones de aplicaciones. Las Group Policy relacionadas a la computadora, se aplican cuando el sistema operativo se inicializa y durante un ciclo periódico de actualización. En general, las configuraciones de computadora Group Policy toman precedencia al estar en conflicto con Group Policy de usuario.

Las Group Policy Settings que modifican el ambiente para requisitos particulares de escritorio y para todos los usuarios de una computadora, o que hacen cumplir las políticas de seguridad en las computadoras de una red, se contienen debajo de ***Computer Configuration*** en el editor de Group Policy Object.

***Debajo de Computer Configuration, también se encuentran:***

- La carpeta Software Settings: contiene las configuraciones de software que se aplican a todos los usuarios que inicien sesión en la computadora. Esta carpeta posee configuración de instalación de software y puede contener otras configuraciones que se coloquen allí de ISVs.

- La carpeta Windows Settings: contiene configuraciones Windows que se aplican a todos los usuarios que inicien sesión en la computadora. Esta carpeta también contiene los siguientes puntos: **Security Settings y Scripts**.

***Security Settings*** está disponible debajo de la carpeta Windows Settings que se encuentra debajo de Computer Configuration y User Configuration en el editor de Group Policy Object. Security Settings o Security Policies son las reglas que Usted configura en una computadora o las computadoras múltiples que protegen recursos en una computadora o una red. Con Security Settings, Usted puede especificar Security Policy de una organizational unit, domain o site.

Para más información sobre extender Group Policy, ver los métodos Avanzados extendiendo Group Policy en:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SPconcepts_30.asp

## 1.3. Práctica 1: Configurando Local Computer Policy Settings

***Para agregar Group Policy Object Editor a una CustomMMC deberá:***

1. Abrir una CustomMMC.
2. Agregar el snap-in Group Policy Object Editor.
3. Guardar la CustomMMC.

***Para evitar que los usuarios apaguen el servidor usando Local Policy Setting deberá:***

1. Expandir, en la CustomMMC, el snap-in ***Local Computer Policy***.
2. Expandir, en la consola, ***User Configuration***. Expandir ***Administrative Templates*** y después hacer click en S***tart Menu and Taskbar***.
3. Hacer doble-click en ***Remove and prevent access to the Shut Down command***, del panel de los detalles
4. Hacer click en ***Enabled*** del cuadro ***Remove and prevent access to the Shut Down command Properties***, y después hacer click en ***OK***.
5. Cerrar y guardar todos los programas y hacer log off.

***Para probar la policy deberá:***

1. Iniciar sesión como ***User*** con una contraseña.
2. Hacer Click en ***Start*** y verificar que el botón ***Shut Down*** se haya quitado del menú ***Start***.
3. Cerrar y guardar todos los programas y hacer log off.

## 1.4. Las herramientas usadas para crear GPOs

- ***Active Directory Users and Computers***

Usted puede abrir el editor de Group Policy Object desde Active Directory Users and Computers para administrar GPOs para dominios y organizational units. En el cuadro Properties para un dominio u organizational unit, hay una lengüeta Group Policy, con la cual se puede manejar GPOs para el dominio u organizational units.

- ***Active Directory Sites and Services***

Usted puede abrir el editor de Group Policy Object desde Active Directory Sites and Services para manejar GPOs de sites. En el cuadro Properties para el site, hay una lengüeta Group Policy, con la cual se puede manejar GPOs para el site.

- ***Group Policy Management Console***

La Group Policy Management Console es un sistema de interfases programables para el manejo de Group Policy, así como las MMC snap-in que se construyen en estas interfases programables también. Los componentes de Group Policy Management, por su parte, consolidan la administración de Group Policy a través de la empresa.

La Group Policy Management Console combina la funcionalidad de componentes múltiples en una sola interfaz de usuario (UI). La UI se estructura para emparejar la manera en que se utiliza y maneja Group

Policy. Asimismo incorpora la funcionalidad relacionada con Group Policy de las herramientas siguientes en una sola MMC snap-in:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Resultant Set of Policy (RSoP)

Group Policy Management también proporciona las siguientes capacidades extendidas que no estaban disponibles en herramientas anteriores de Group Policy. Con Group Policy Management, Usted puede:

Hacer Back up y restore de GPOs.

- Copiar e importar GPOs.
- Usar filtros Windows Management Instrumentation (WMI).
- Generar reportes de GPO y RSoP.
- Búscar para GPOs.

***Group Policy Management vs. default Group Policy tools***

Antes de Group Policy Management, Usted administraba Group Policy usando una variedad de herramientas Windows, incluyendo Active Directory Users and
Computers, Active Directory Sites and Services y RSoP. Pero ahora, Group Policy Management consolida la administración de todas las tareas base de Group Policy en una sola herramienta. Gracias a esta administración consolidada, la funcionalidad de Group Policy ya no es requerida en las otras herramientas.

Después de instalar Group Policy Management, Usted aún utiliza cada una de las herramientas de Active Directory para sus propósitos previstos de administración de directorio, por ejemplo, crear un usuario, computadora y grupo. Sin embargo, usted puede utilizar Group Policy Management para realizar todas las tareas relacionadas con Group Policy. La funcionalidad de Group Policy ya no estará disponible con las herramientas de Active Directory cuando instale Group Policy Management.

Group Policy Management no sustituye al editor de Group Policy Object. Usted todavía debe editar GPOs, usando el editor de Group Policy Object. Group Policy Management integra la funcionalidad de edición proporcionando acceso directo al editor de Group Policy Object.

**Nota:** La Group Policy Management Console no viene con Windows Server 2003.

**Usted debe descargarlo de:**

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

### 1.5. Práctica 2: ¿Cómo crear una GPO?

Utilice los procedimientos siguientes para crear un nuevo GPO o un link a una GPO existente, usando Active Directory Users and Computers, y para crear una GPO en un site, dominio u organizational unit.

***Para crear una GPO nueva o hacer un link a una GPO existente usando Active Directory Users and Computers:***

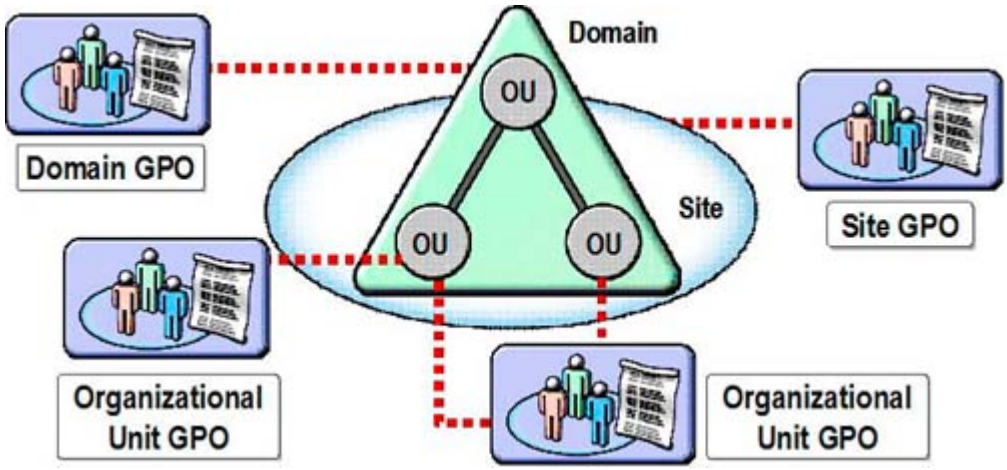
1. Hacer click derecho en el ***contenedor de Active Directory*** (dominio u organizational unit), que está en el Active Directory Users and Computers, para crear una GPO. Después hacer click en ***Properties***.
2. Elegir una de las opciones siguientes, en el cuadro ***Properties***, sobre la lengüeta ***Group Policy***:

   - ***Para crear una GPO nueva***, hacer click en New, ingresar un nombre para la GPO nueva y presionar ENTER.

   - ***Para hacer un link a una GPO existente***, hacer click en Add y seleccionar la GPO de la lista.

La GPO o el link que usted crea, se exhibe en la lista de GPOs que están linkeadas al contenedor de Active Directory.

### 1.6. ¿Qué es un GPO Link?




Todas las GPOs se almacenan en un contenedor de Active Directory llamado Group Policy Objects. Cuando una GPO es utilizada por un site, dominio u organizational unit, la GPO es linkeada al contenedor Group Policy Objects. Consecuentemente, Usted puede centralizar la administración y el deploy de GPOs a muchos dominios u organizational units.

Cuando Usted crea un GPO link a un site, dominio u organizational unit, podrá realizar dos operaciones separadas: crear la GPO nueva y linkearla al site, dominio u organizational unit. Al delegar permisos para linkear una GPO al dominio, organizational unit o site, Usted tendrá que modificar los permisos para el dominio, organizational unit o site que desee delegar.

Por defecto, solamente miembros de los grupos Domain Admins y Enterprise Admins tienen los permisos necesarios para linkear GPOs a domains y organizational units. Únicamente los miembros del grupo Enterprise Admins tienen los permisos para linkear GPOs a sites. Miembros del grupo Group Policy Creator Owners pueden crear GPOs, pero no pueden linkear.

Cuando Usted crea una GPO en el contenedor Group Policy Objects, la GPO no se aplica a ningún usuario o computadora hasta que el GPO link sea creado. Usted puede crear una unlinked GPO usando Group Policy Management y también puede llegar a crear unlinked GPOs en una organización grande, donde un grupo cree GPOs y otro grupo cree links de GPOs al site, dominio u organizational unit.

## 1.7. Práctica 3: ¿Cómo crear un GPO Link?

Para realizar esta práctica deberá instalar previamente GPMC. (Vea el punto 4.3 más adelante) Utilice los procedimientos siguientes para crear y linkear GPOs.

- Para linkear una GPO cuando usted lo crea:

1. En la Group Policy Management de la consola, expandir el forest conteniendo el dominio en el cual Usted desea crear y linkear la GPO. Expandir ***Domains*** y realizar uno de los siguientes pasos:

- ***Para crear una GPO y linkearla al dominio***, hacer click derecho en el dominio y después hacer click en Create and Link a GPO Here.

- ***Para crear una GPO y linkearla a una organizational unit***, expandir el dominio que contiene la organizational unit, hacer click derecho en la organizational unit, y después hacer click en ***Create and Link a GPO Here***.

2. En el cuadro ***New GPO***, ingresar el nombre para la GPO nueva y después hacer click en ***OK***.

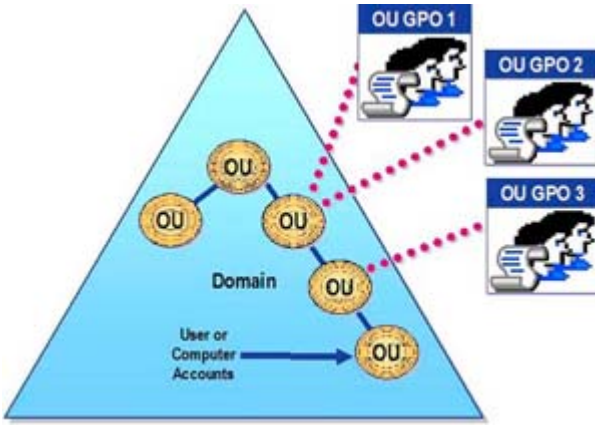
- Para linkear una GPO existente al site, dominio u organizational unit:

1. En Group Policy Management de la consola, expandir el forest conteniendo el dominio en el cual Usted desea linkear una GPO existente. Expandir ***Domains*** y el dominio.
2. Hacer click derecho en el dominio, site u organizational unit. Después hacer click en ***Link an Existing GPO***.
3. En el cuadro ***Select GPO***, hacer click en la GPO que Usted desea linkear y después hacer click en ***OK***.

## 1.8. ¿Cómo se heredan permisos de Group Policy en Active Directory?

La orden en la cual Windows Server 2003 aplica GPOs depende del contenedor de Active Directory al cual es linkeada la GPO. Las GPOs se aplican primero al site, después a dominios y por último a organizational units en los dominios.

Un contenedor child hereda GPOs del contenedor parent. Esto significa que un contenedor child puede tener muchos Group Policy Settings aplicados a sus usuarios y computadoras, sin tener un GPO linkeado a él. Sin embargo, no hay jerarquía de dominios como en las organizational units, por ejemplo, las parent organizational units y child organizational units.




Las GPOs son acumulativas, implicando que están heredadas. La herencia de Group Policy es el orden en el cual Windows Server 2003 aplica GPOs. Este orden y la herencia de GPOs determinan, en última instancia, qué configuraciones afectan a usuarios y computadoras. Si hay GPOs múltiples que se fijan en el mismo valor, por defecto la GPO que se aplicó última, tomará precedencia.

Usted puede también tener GPOs múltiples linkeadas al los mismos contenedores. Por ejemplo, puede tener tres GPOs linkeadas a un solo dominio. El orden en el cual se aplican las GPOs puede afectar el resultado de

la configuración de Group Policy. Hay también un orden o prioridad de Group Policy y de GPOs para cada contenedor.

## 1.9. ¿Qué sucede cuando hay conflicto de GPOs?

Las combinaciones complejas de GPOs pueden crear conflictos y consecuentemente requerir modificar el comportamiento de la herencia por defecto. Cuando una configuración de Group Policy se configura para una organizational unit parent y la misma configuración de Group Policy no se configura para la organizational unit child, los objetos de esta última heredan la configuración de Group Policy de la organizational unit parent.

Cuando se configura una Group Policy para ambas, organizacional unit parent y organizational units child, las configuraciones para estas organizational units se aplican. Si las configuraciones son incompatibles, la organizational unit child conserva sus propia configuración de Group Policy. Por ejemplo, una configuración de Group Policy para la organizational unit se aplica por último a la computadora o el usuario sobreescribe la que está en conflicto de configuración de Group Policy para un contenedor, que es de más alta jerarquía en Active Directory.

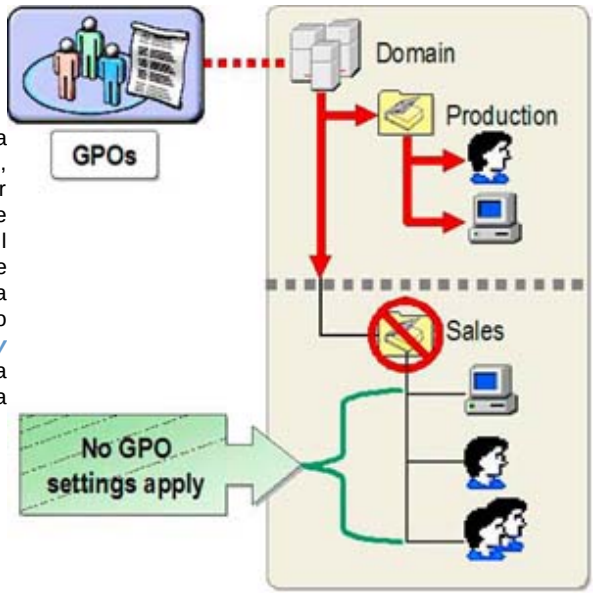
Si el orden de herencia por defecto no resuelve las necesidades de su organización, Usted puede modificar las reglas de herencia para GPOs específicas. Windows Server 2003 proporciona las dos siguientes opciones para cambiar el orden de herencia por defecto:

- ***No Override (Enforced)***
  Esta opción se utiliza para prevenir que contenedores child filtren GPOs con prioridad más alta de configuración. Esta alternativa es útil para hacer cumplir GPOs que representen reglas de negocio de la organización. La opción ***No Override*** se fija sobre una base individual de GPO. Usted puede fijar esta opción en una o más GPOs según lo requiera. Cuando se fija más de una GPO en ***No Override***, la GPO más alta en la jerarquía de Active Directory, fijada en ***No Override***, tomará precedencia.

- ***Block Policy inheritance***
  Esta opción se utiliza en contenedores child para bloquear herencia de todos los contenedores parent. Es útil cuando una organizational unit requiere una única configuración de Group Policy. ***Block Policy inheritance*** se fija basándose en el contenedor. En caso de conflicto, la opción ***No Override*** toma siempre precedencia sobre la opción ***Block Policy inheritance***.

## 1.10. Bloqueo de Deployment de GPO

Usted puede prevenir en un contenedor child la herencia de todas las GPOs de los contenedores parent, habilitando ***Block Policy inheritance*** en el contenedor child. De esta manera, evita que el contenedor herede todas las configuraciones Group Policy. Esto es útil cuando un contenedor de Active Directory requiere configuraciones únicas de Group Policy y Usted desea asegurarse que las configuraciones de Group Policy no se hereden. Por ejemplo, se puede utilizar ***Block Policy inheritance*** cuando el administrador de una organizational unit deba controlar todas las GPOs para ese container.

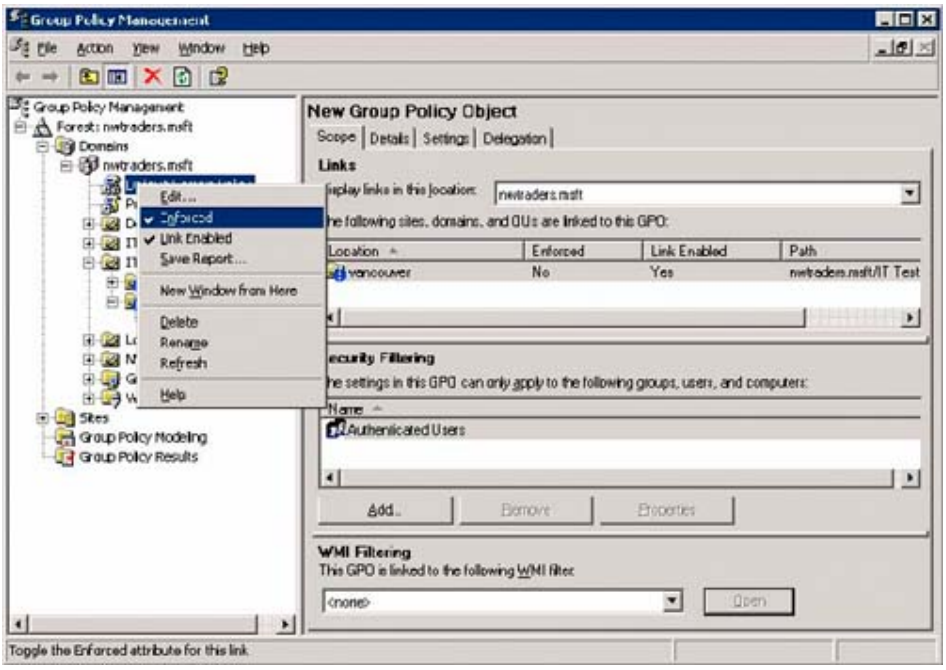


***Al usar Block Policy inheritance, deberá considerar lo siguiente:***

- No se puede elegir selectivamente qué GPOs bloquea. ***Block Policy inheritance*** afecta todas las GPOs de todos los contenedores parent, excepto las GPOs configuradas con la opción ***No Override*** sin GPMC instalada y ***Enforced*** con GPMC instalada.

- ***Block Policy inheritance*** no bloquea la herencia de una GPO linkeada a un contenedor parent, si el link se configura con la opción ***No Override***.

## 1.11. ¿Cómo configurar Group Policy Enforcement?




**Importante:** Antes de instalar Group Policy Management, la opción ***Enforced*** se llama No Override en Active Directory Users and Computers.

***Para configurar enforcement de GPO link deberá:***

1. En Group Policy Management de la consola, expandir el forest con el link en el cual Usted desea configurar el enforcement. Luego, seguir uno de siguientes pasos:

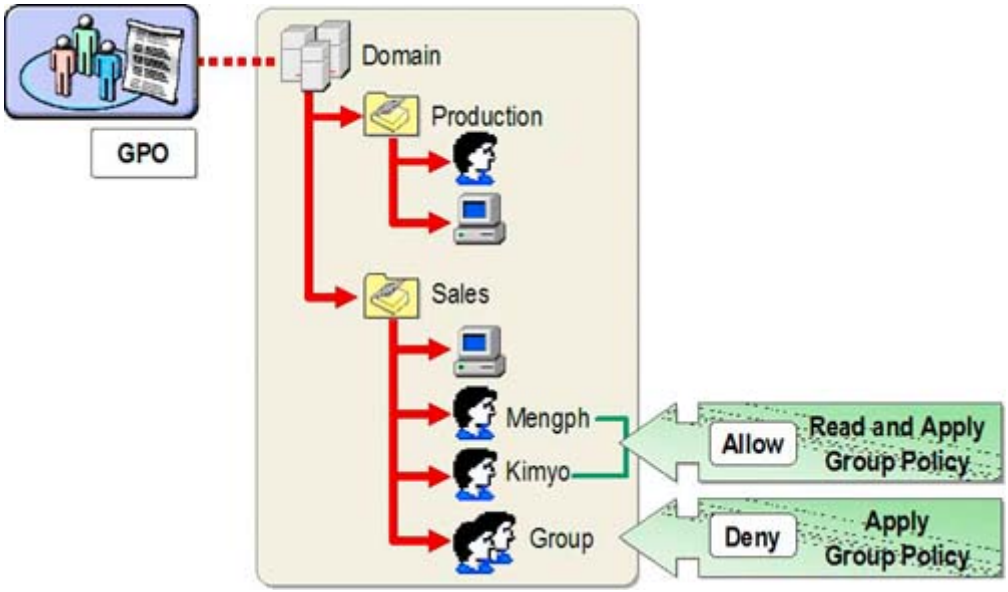
   - ***Para configurar enforcement de GPO link a un dominio***, expandir Domains y el dominio que contiene el GPO link.

   - ***Para configurar enforcement de GPO link a una organizational unit***, expandir Domains y el dominio que contiene la organizational unit. Después expandir la organizational unit que pueda incluir parent o child organizational unit y que contenga el GPO link.

   - ***Para configurar enforcement de GPO link a un site***, expandir Sites, y luego expandir el site que contiene el GPO link.

2. Hacer click derecho en el GPO link y después hacer click en ***Enforced*** para permitir o inhabilitar el enforcement.

### 1.12. Filtrado de Aplicación de GPO




Por defecto, todos los Group Policy Settings contenidos en las GPOs, afectan al contenedor y se aplican a todos los usuarios y computadoras de ese contenedor, el cual no puede producir los resultados que Usted desea. Usando la característica de filtrado, se puede determinar qué configuraciones se aplican a los usuarios y a las computadoras en el contenedor específico.

Usted puede filtrar el deployment de GPO fijando permisos en el GPO Link para determinar el acceso de lectura o negar el permiso en la GPO. Para que los Group Policy Settings se apliquen a una cuenta de usuario o de computadora, la cuenta debe tener por lo menos el permiso de lectura para una GPO y de aplicación. Los permisos por defecto para una GPO nueva tienen el siguiente Access Control Entries (ACEs):

- Authenticated Users. Permitir read y permitir apply Group Policy
- Domain Admins, Enterprise Admins and SYSTEM. Permitir read, Permitir Write, Permitir Create All Child objects, Permitir Delete All Child objects

***Usted puede utilizar los siguientes métodos de filtrado:***

- ***Explicitly deny***

  Este método se utiliza al negar el acceso a la Group Policy. Por ejemplo, Usted podría negar explícitamente el permiso al grupo de seguridad de los administradores, lo cual prevendría a los administradores en la organizational unit de la recepción de GPO Settings.
- ***Remove Authenticated Users***

  Usted puede omitir a los administradores de la organizational unit del grupo de seguridad, lo cual significa que no tienen ningún permiso explícito para la GPO.

Para más información acerca de Group Policy:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324743

http://microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/management/gp/default.asp

## 2. Administración del entorno de usuario

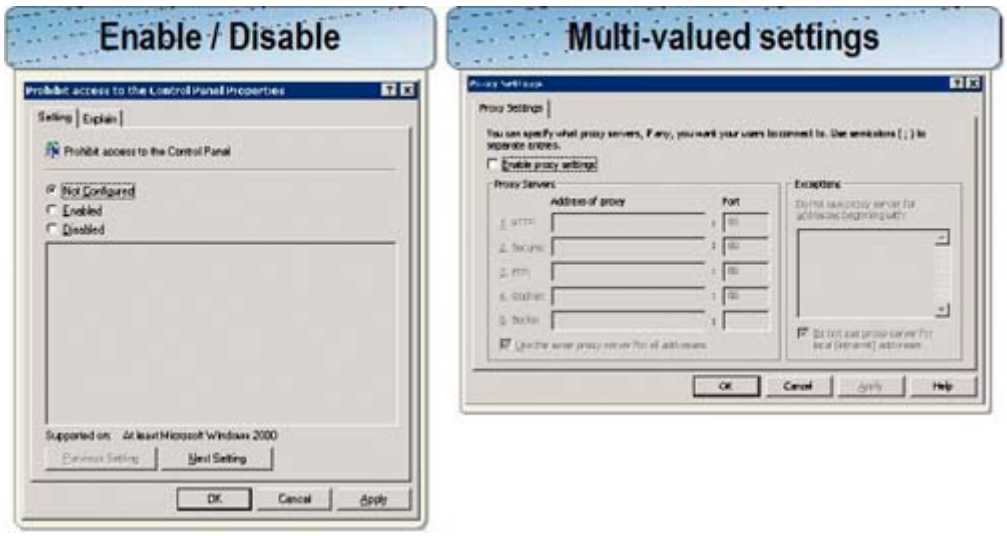
La administración del entorno de usuario implica controlar lo que éstos pueden hacer cuando inician sesión en la red. Esto se hace a través de Group Policy, controlando las computadoras de escritorio, las conexiones de red y las interfaces de usuario. Usted maneja los ambientes de usuario para asegurarse que los mismos tengan lo necesario para realizar sus trabajos. De esta manera, no podrán corromper o configurar incorrectamente sus ambientes.

***Cuando Usted configura y maneja ambientes de usuario de forma centralizada, puede realizar las siguientes tareas:***

- ***Manejar los usuarios y las computadoras.*** Esto es posible controlando la configuración de escritorio del usuario con policies basadas en registry. Así, Usted se asegura que los usuarios tengan los mismos ambientes, incluso si ellos inician sesión de diversas computadoras. Asimismo, Usted puede controlar cómo Microsoft Windows® Server 2003 maneja el user profiles, el cual conoce la forma en que los datos personales de un usuario están disponibles. Con redirecting user folders de los discos duros locales del usuario a una localización central en un servidor, Usted puede asegurarse que los datos del usuario estén disponibles para ellos, sin importar la computadora desde la cual inicien sesión.

- ***Deploy software.*** El software se instala en las computadoras o en los usuarios con servicio de directorio Active Directory®. Con la instalación del software, Usted puede asegurarse que los usuarios tengan sus programas requeridos, service packs, y hotfixes.

### 2.1. ¿Qué son los Group Policy Settings Enable o Disable?




Si Usted inhabilita un policy setting, está inhabilitando la acción del policy setting. Por ejemplo, los usuarios por defecto pueden tener acceso al Control Panel. Para ello, Usted no necesita inhabilitar el policy setting ***Prohibit access to the Control Panel***, a menos que previamente haya aplicado un policy setting habilitándolo. En esta situación, Usted habrá fijado otro policy setting para deshabilitar el aplicado previamente.

Esto es provechoso cuando se heredan policy settings y no se desea usar filtrado para aplicar policy settings a un grupo y a otro no. Usted puede aplicar una GPO que permita un policy setting en la parent organizational unit y otro policy setting que deshabilite la GPO en la child organizational unit.

Si Usted permite un policy setting, estará consintiendo la acción del policy setting. Por ejemplo, para revocar a alguien acceso al Control Panel, Usted puede habilitar el policy setting ***Prohibit access to the Control Panel***.

Un GPO lleva a cabo los valores que cambian registry para los usuarios y las computadoras que están conformes al GPO. La configuración por defecto para un policy setting es ***Not Configured***. Si Usted desea fijar a una computadora o a un usuario un policy setting, de nuevo al valor prefijado o de nuevo a la local policy, deberá seleccionar la opción ***Not Configured***. Por ejemplo, Usted puede permitir un policy setting para algunos clientes, y al usar la opción Not Configured, la policy invertirá a la policy por defecto, o local policy setting.

Algunas GPOs requieren proporcionar una cierta información adicional después de permitir el objeto. Ciertas veces Usted puede necesitar seleccionar un grupo o una computadora si el policy setting necesita volver a dirigir al usuario a una cierta información. Otras veces, por ejemplo,para permitir proxy settings, Usted deberá proporcionar el nombre o la dirección Internet Protocol (IP) del proxy server y el número de puerto. Si el policy setting es multi-valued y los settings están en conflicto con otro policy setting, el conflicto de multi-valued settings se substituyen por el último policy setting que fue aplicado.

## 2.2. Práctica 4: ¿Cómo editar un Group Policy Setting?

Como administrador de sistemas, Usted debe editar Group Policy settings. Utilice el siguiente procedimiento para realizar esta tarea.

1. En Group Policy Management de la consola, navegar los ***Group Policy Objects***.
2. Hacer click derecho en la GPO y después en ***Edit***.
3. En el editor de Group Policy Object, buscar el Group Policy setting que se desear editar, y después hacer doble-click.
4. En el cuadro ***Properties***, configurar el Group Policy setting y después hacer click en ***OK***.

## 2.3. ¿Qué son los scripts de Group Policy Settings?

Usted puede utilizar los scripts de Group Policy para configurar scripts centralizados que corran automáticamente cuando la computadora se inicia y se apaga, y también cuando los usuarios inician sesión y la cierran. Usted puede especificar cualquier script que corra en Windows Server 2003, incluyendo archivos batch, programas ejecutables y scripts soportados por Windows Script Host (WSH).

***Para ayudar al usuario a manejar y configurar sus ambientes, deberá:***

- Correr scripts que realicen las tareas que Usted no puede realizar con otros Group Policy settings. Por ejemplo, configurar el entorno de usuario con conexiones de red, conexiones de impresora, shortcuts a aplicaciones y documentos corporativos.

- Limpiar los escritorios cuando los usuarios cierran la sesión y apagan la computadora. Usted puede quitar las conexiones que agregó con los scripts de logon o startup, de modo que la computadora esté en el mismo estado que cuando el usuario la encendió.

- Correr scripts pre-existentes, fijados para manejar los ambientes de usuario hasta que se configure con otro Group Policy settings que remplace esos scripts

**Nota:** Desde Active Directory Users and Computers, Usted puede asignar scripts de logon individualmente a las cuentas del usuario en el cuadro ***Properties*** de cada uno de ellos. Sin embargo, Group Policy es el método preferido para correr scripts porque se pueden manejar estos scripts centralizados junto con startup, shutdown, y logoff scripts.

Para más información acerca de scripting, vea TechNet Script Center en:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp

## 2.4. Práctica 5: ¿Cómo asignar Scripts con Group Policy?

Para implementar script Usted utiliza Group Policy, agregándolo a la configuración apropiada en un Group Policy template. Esto indica que el script puede correr durante el startup, shutdown, logon o logoff.

***Para agregar un script a la GPO deberá:***

1. En Group Policy Management, editar la GPO.
2. En el editor de Group Policy Object de la consola, buscar User Configuration/Windows Settings/Scripts (Logon/Logoff).
3. En el panel de detalles, hacer doble-click en ***Logon***.
4. En el cuadro ***Logon Properties***, hacer click en ***Add***.
5. En el cuadro ***Add a Script***, configurar cualquiera de las configuraciones siguientes que se desee utilizar. Después, hacer click en ***OK***:
   - ***Script Name.*** Ingresar el path del script o hacer click en ***Browse*** para localizar el archivo de script en la carpeta compartida Netlogon del Domain controller.
   - ***Script Parameters.*** Ingresar los parámetros que se desean utilizar, de la misma manera que se ingresaría en command line.
6. En el cuadro ***Logon Properties***, configurar cualquiera de las siguientes configuraciones que se deseen utilizar:
   - ***Logon Scripts for.*** Esta lista enumera todas los scripts que están actualmente asignados a la GPO seleccionada. Si se asignan múltiples scripts, éstos serán procesados en el orden que se especificó. Para mover el script en la lista, hacer click en el script y después ***Up*** o ***Down***.

## 2.5. ¿Qué es Folder Redirection?

Cuando Usted redirecciona folders, cambia la locación de las carpetas del disco duro local de la computadora del usuario, a una carpeta compartida en un servidor de la red. Después de redireccionar una carpeta a un servidor, ésta seguirá apareciendo como local para el usuario. Cuatro son las carpetas que forman parte del user profile y que se pueden redireccionar: My Documents, Application Data, Desktop y Start Menu.

***Almacenando datos en la red, los beneficios de los usuarios son la disponibilidad creciente y los backup frecuentes de sus datos. Redireccionar carpetas tiene los siguientes beneficios:***

- Los datos en las carpetas están disponibles para el usuario, sin importar la computadora cliente desde la que el usuario inicie sesión.
- Los datos en las carpetas se almacenan centralizados, y por esto es más fácil la administración y el backup para su resguardo.
- Los archivos que se localizan adentro de carpetas redireccionadas, como los archivos de un roaming user profile, no se copian y no se guardan en la computadora del usuario que inicia sesión. Esto significa que cuando el usuario inicia sesión en la computadora cliente, no se utilizará espacio de almacenamiento para esos archivos y los datos que puedan ser confidenciales no quedan en dicha computadora.
- Los datos se almacenan en una carpeta compartida de red que puede ser parte de las áreas rutinarias de backup. Esto es más seguro porque no requiere ninguna acción de parte del usuario.
- Como administrador, Usted puede utilizar Group Policy para configurar disk quotas, limitando la cantidad de espacio que es tomado por los usuarios.

## 2.6. Carpetas que pueden ser redireccionadas

Usted puede redireccionar las carpetas My Documents, Application Data, Desktop y Start Menu. Una organización puede redireccionar estas carpetas para preservar datos y configuraciones importantes del usuario. Hay varias ventajas al redireccionar cada una de estas carpetas, que varían según las necesidades de la organización.

***Usted puede utilizar redirección para cualquiera de las siguientes carpetas en el user profile:***

***My Documents***
La redirección de My Documents es particularmente ventajosa porque la carpeta tiende a agrandarse con el tiempo.
La tecnología Offline Files da el acceso a usuarios a My Documents, incluso cuando los usuarios no están conectados a la red. Esto es particularmente útil para gente que utiliza las computadoras portátiles.

***Application Data***
Los Group Policy setting controlan el comportamiento de los Application Data cuando el caching del lado del cliente está habilitado. Esta configuración sincroniza los datos de aplicaciones centralizados en un servidor de la red con la computadora local. Consecuentemente, el usuario puede trabajar en línea o fuera de línea. Si algunos cambios se realizan a los datos de aplicación, la sincronización actualiza los datos del aplicativo sobre el cliente y el servidor.

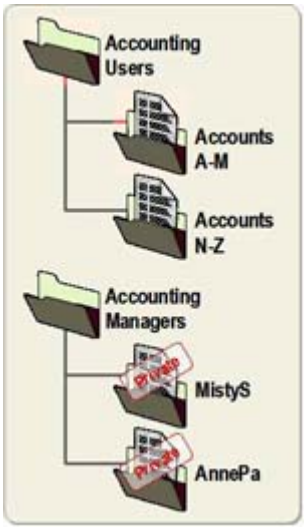
***Desktop***
Usted puede redireccionar el escritorio y todos los archivos, shortcuts y carpetas a un servidor centralizado.

***Start Menu***
Cuando se redirecciona el Start Menu, sus subfolders también se redireccionan.

## 2.7. Configuraciones requeridas para configurar Folder Redirection

Hay tres configuraciones disponibles para Folder Redirection: none, basic y advanced. Basic Folder Redirection es para los usuarios que deben redirigir sus carpetas a un área común o para los usuarios que necesitan que sus datos sean privados.

***Usted tiene las siguientes opciones básicas para Folder Redirection:***




- ***Redirect folder to the following location***
  Todos los usuarios redireccionan sus carpetas a un área común donde pueden ver o utilizar otros datos en carpetas redirecionadas. Para hacer esto, elija la configuración ***Basic*** y configure la ***Target folder location to Redirect folder to the following location.*** Es aconsejable utilizar esta opción para todas las carpetas que contengan los datos que no son privados.

- ***Create a folder for each user under the root path***
  Para los usuarios que necesitan sus carpetas redireccionadas con datos privados, elija configuración ***Basic*** y configure ***Target folder location to Create a folder for each user under the root path.*** Es aconsejable utilizar esta opción para los usuarios que necesitan sus datos privados, como los gerentes que guardan datos personales sobre empleados.

Cuando Usted selecciona ***Advanced . specify locations for various user groups***,
las carpetas son redireccionadas a diferentes locaciones, basadas en grupos de seguridad de los usuarios.

***Las opciones avanzadas para Folder Redirection son las siguientes:***

***Select a group(s).*** Aquí es donde se especifica a quién aplicar la redirección.
***Target Folder Location.*** Aquí se pueden elegir cualquiera de las siguientes opciones:

- ***Create a folder for each user under the root path.*** Utilizar para los datos confidenciales.
- ***Redirect to the following location.*** Utilizar para los datos compartidos.
- ***Redirect to the local userprofile location.*** Utilizar para los usuarios que utilizan una mezcla de computadoras cliente que no son parte de Active Directory por un lado y sí lo son por otro.

***Root Path.*** En este cuadro, se especifica el servidor y el nombre de la carpeta compartida a la que se desear redireccionar.

## 2.8. Práctica 6: ¿Cómo configurar Folder Redirection?

Usted configura Folder Redirection usando el editor de Group Policy Object.

***Para configurar Folder Redirection deberá:***

1. En Group Policy Management, editar o crear la GPO.
2. En el editor de Group Policy Object de la consola, expandir ***User Configuration***, expandir ***Windows Settings***, y después expandir ***Folder Redirection***. Los íconos para las cuatro carpetas que pueden ser redireccionadas se muestran.
3. Hacer click derecho en la carpeta que se desea redireccionar y después hacer click en ***Properties***.
4. En el cuadro ***Properties***, de la lengüeta ***Setting***, hacer click en una de las siguientes opciones:
   - ***Basic - Redirect everyone's folder to the same network share point.***
   Todas las carpetas afectadas por esta GPO se almacenan en la misma carpeta compartida de red.
   - ***Advanced - Redirect personal folders based on the user's membership in a Windows Server 2003 security group.***
   Las carpetas se redireccionan a otras compartidas de la red y basadas en los miembros de grupos de seguridad. Por ejemplo, carpetas que pertenecen a los usuarios del grupo de contabilidad se redireccionan al servidor de contabilidad, y
   las carpetas que pertenecen a los usuarios en el grupo de comercialización se redireccionan al servidor de comercialización.
5. En el cuadro ***Properties***, hacer Click en ***Add***.
6. Bajo ***Target folder location***, en el cuadro ***Root path***, ingresar el nombre de la carpeta compartida en la red a utilizar, o hacer click en ***Browse*** para localizarla.
7. En la lengüeta ***Settings***, configurar las opciones que se desean utilizar y después hacer click en ***OK***.

## 2.9. ¿Qué es Gpupdate?

```
gpupdate [/Target:{Computer | User}] [/Force]
[/Wait:Value] [/Logoff] [/Boot] [/Sync]
```

***Gpupdate*** es una herramienta command-line que actualiza los local Group Policy settings y Group Policy settings almacenados en Active Directory, incluidas las configuraciones de seguridad. Por defecto, las configuraciones de seguridad se actualizan cada 90 minutos en un puesto de trabajo o un servidor, y cada cinco minutos en un Domain Controller. Usted puede correr gpupdate para probar una Group Policy setting o aplicar inmediatamente un Group Policy setting

***Los ejemplos siguientes demuestran cómo Usted puede utilizar el comando gpupdate:***

```
C:\gpupdate
C:\gpupdate /target:computer
C:\gpupdate /force /wait:100
C:\gpupdate /boot
```

**Gpupdate tiene los siguientes parámetros.**

- ***/Target:{Computer | User}*** Especifica la actualización solamente de usuario o computadora para sus policy settings. Por defecto, la policy de usuario y computadora son actualizadas.

- ***/Force*** Reaplica todos los policy settings. Por defecto, solamente los policy settings que han cambiado se reaplican.

- ***/Wait:{Value}*** Fija el número de segundos para esperar el procesamiento de policy. Por defecto, es de 600 segundos. El valor ' 0 ' significa no esperar. El valor ' - 1 ' significa esperar indefinidamente.

- ***/Logoff*** Causa un logoff después de actualizar la configuración de Group Policy settings.

- ***/Boot*** Provoca que la computadora se reinicie después de la actualización de Group Policy settings.

- ***/Sync*** Provoca que la próxima configuración de policy setting se aplique sincrónicamente.

## 2.10. ¿Qué es Gpresult?

```
gpresult [/s Computer [/u Domain\User /p Password]]
[/user TargetUserName] [/scope {user|computer}] [/v]
[/z]
```

Debido a que Usted puede aplicar niveles traslapados de policy settings a cualquier computadora o usuario, Group Policy genera un reporte que resulta de aplicar policies al logon. ***Gpresult*** exhibe el reporte que resulta de aplicar policies que se hacen cumplir en la computadora para el usuario especificado al logon.

El comando ***gpresult*** exhibe los Group Policy settings y el Resultant Set of Policy (RSoP) para un usuario o una computadora. Usted puede utilizar ***gpresult*** para ver qué configuraciones de la GPO son efectivas y localizar problemas en la aplicación.

***Los ejemplos siguientes demuestran cómo se puede utilizar el comando gpresult:***

```
C:\gpresult /user targetusername /scope computer
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /scope USER
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /z >policy.txt
C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23
```

**Gpresult tiene los siguientes parámetros.**

- ***/s Computer*** Especifica el nombre o dirección IP de una computadora remota. Por defecto es la computadora local.

- ***/u Domain\User*** El comando funciona con los permisos de la cuenta del usuario que se especifica User o Domain/User. El defecto son los permisos del usuario que se encuentre autenticado en la computadora y que ejecute el comando.

- ***/p Password*** Especifica el password de la cuenta del usuario que se especifica en el parámetro /u.

- */user TargetUserNam*e Especifica el nombre del usuario del que se exhiben los datos RSoP.

- */scope {user|computer}* Exhibe los policy settings del usuario o computadora. Los valores válidos para el parámetro /scope son user o computer. Si se omite el parámetro /scope, gpresult exhibe a ambos, usuario y computadora.

- */v* Especifica que la salida exhibirá información verbose de la policy.

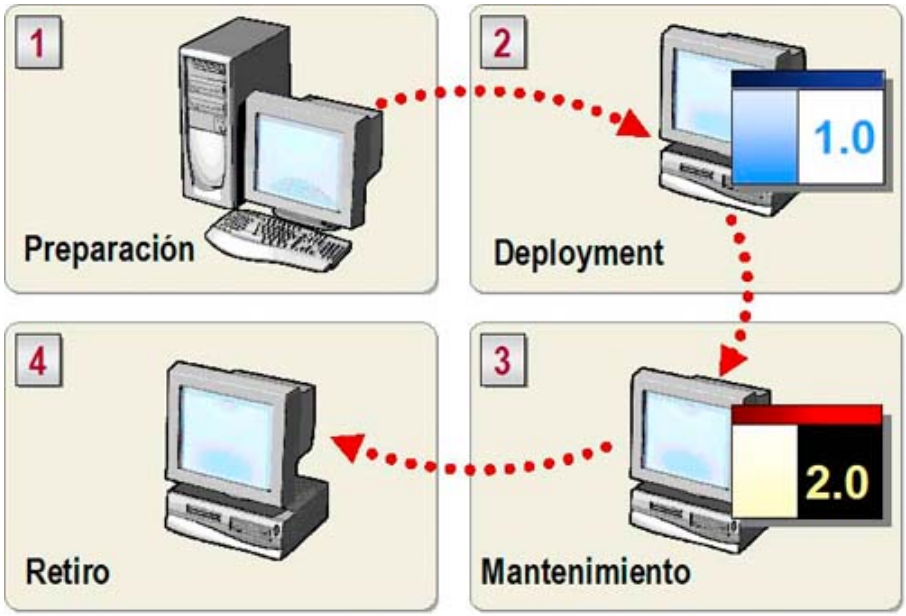
- */z* Especifica que la salida exhibirá toda la información disponible acerca de Group Policy. Dado que este parámetro produce más información que el parametro /v, se debe redireccionar la salida a un archivo de texto cuando se utilice este parámetro (por ejemplo, s puede escribir *gpresult /z >policy.txt*).

- */?* Exhibe la ayuda en la ventana de comandos.

## 3. Administración de instalación de Software

Microsoft® Windows® Server 2003 incluye una característica llamada Instalación y mantenimiento de software que utiliza el servicio de Active Directory®, Group Policy y Microsoft Windows Installer para instalar, mantener y quitar software en las computadoras en su organización. Usando el método de administración e instalación de software basado en policy, Usted puede asegurarse que los programas que los usuarios requirieran para realizar sus trabajos, estén disponibles siempre y donde sea necesario.

### 3.1. La instalación del Software y el proceso de mantenimiento




En Windows Server 2003, Usted puede utilizar Group Policy para manejar el proceso de instalación de software centralizado a partir de una localización. Además, Group Policy settings puede aplicarse a los usuarios o computadoras en un site, dominio u organizational unit para instalar automáticamente, actualizar o quitar software. Aplicando Group Policy settings al software, Usted puede manejar varias fases de la instalación del software sin instalar software en cada computadora individualmente.

***La lista siguiente describe cada fase en la instalación del software y proceso de mantenimiento:***

1. ***Preparation.*** Primero hay que instalar el software usando la estructura corriente de Group Policy object (GPO), y también identificar los riesgos al usar la infraestructura actual para instalar software. Para preparar los archivos que permitan a un programa ser instalado con Group Policy, Usted debe copiar los archivos Windows Installer package para un programa a un software distribution point, el cual puede ser una carpeta compartida en un servidor. Asimismo puede adquirir el archivo Windows Installer package del vendedor del programa o crear el archivo package usando una utilidad de terceras partes.
2. ***Deployment.*** Aquí hay que crear una GPO que instala el software en la computadora y linkea la GPO a un contenedor apropiado de Active Directory. El software estará instalado cuando la computadora se encienda o cuando un usuario inicie el programa.
3. ***Maintenance.*** El software se actualiza con una nueva versión o reinstalando el software con un service pack o un software update. De esta maner, estará automáticamente actualizado o reinstalado cuando la computadora se encienda o cuando el usuario inicie el programa.
4. ***Removal.*** Para eliminar el software que no es requerido, se necesita quitar el software package setting de la GPO que originalmente instaló el software. El software entonces se quitará automáticamente cuando la computadora se encienda o cuando un usuario inicie sesion.

### 3.2. ¿Qué es Windows Installer?

Para habilitar Group Policy para instalación y administración de software, Windows Server 2003 usa Windows Installer. Este componente automatiza la instalación y el retiro de programas, aplicando un sistema de reglas centralmente definidas durante el proceso de la instalación.

***Windows Installer contiene dos componentes:***

***Windows Installer service.*** Este servicio del lado del cliente automatiza completamente la instalación del software y proceso de la configuración. El servicio Windows Installer puede también modificar o reparar un programa instalado existente. Para instalar un programa lo hace directamente del Cd-ROM o usando Group Policy. Para ello, el servicio Windows Installer requiere un Windows Installer package.

***Windows Installer package.*** Este archivo package contiene toda la información que el Windows Installer service requiere para instalar o quitar software. El Archivo contiene:

- Es un archivo Windows Installer con extención .msi.
- Archivos fuente externos, que son requeridos para instalar o quitar el software.
- Información estándar sobre el software y el package.
- Archivos del producto o una referencia a un punto de instalación donde residen los archivos del producto.

***Las ventajas de usar tecnologia Windows Installer incluye:***

***Custom installations.*** Características opcionales de un aplicativo. Por ejemplo, clip art o un diccionario, puede ser visible en un programa sin que la característica sea instalada. Aunque los comandos de menú son accesibles, la característica no está instalada hasta que el usuario acceda al menú de comandos. Este método de instalación ayuda a reducir la complejidad y la cantidad de espacio de disco duro que el programa utiliza.

***Resilient applications.*** Si un archivo crítico se borra o se corrompe, el programa adquiere automáticamente una nueva copia del archivo de la fuente de la instalación, sin requerir la intervención del usuario.

***Clean removal.*** Windows Installer quita aplicaciones sin dejar archivos huérfanos o inadvertidamente romper otro aplicativo, por ejemplo, cuando un usuario borra un archivo compartido que otro aplicativo requiera. También, Windows Installer quita todas las configuraciones de registry relacionadas y almacena las transacciones de instalación en una base de datos y archivos de log subsecuentes.

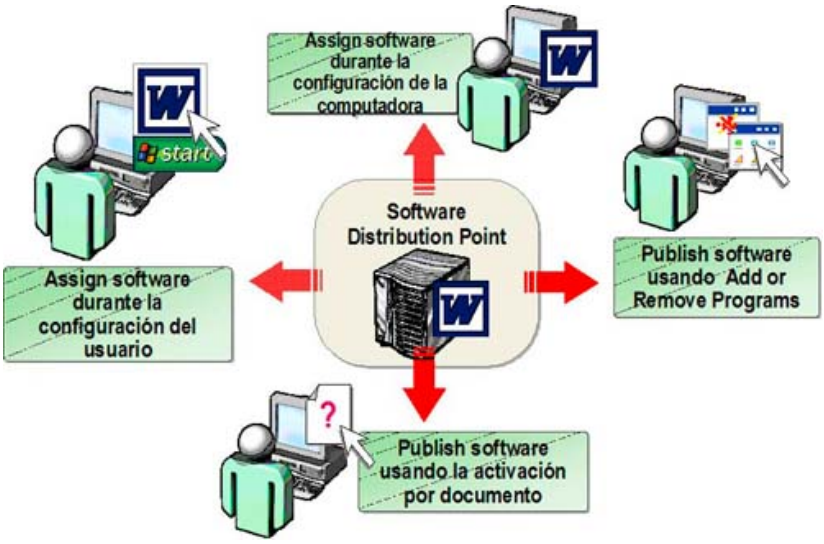
### 3.3. Descripción del proceso de Software Deployment


Cuando Usted instala software, está especificando cómo se instalan los aplicativos y cómo se mantienen los mismos en su organización.

***Para instalar nuevo Software, utilizando Group Policy, deberá:***

1. ***Crear un software distribution point.*** Esta carpeta compartida en su servidor contiene el package y los archivos del software para instalar. Cuando el software se instala en una computadora local, el Windows Installer copia archivos a la computadora.
2. ***Utilizar la GPO para instalar software.*** Usted debe crear o realizar cambios necesarios a la GPO para el contenedor en donde desea instalar el aplicativo. Al mismo tiempo puede configurar la GPO para instalar software para una cuenta de usuario o de computadora. Esta tarea también incluye seleccionar el tipo de instalación que se requiere.
3. **Cambiar las características de la instalación del software.** Dependiendo de sus requisitos, Usted puede cambiar las características que fueron fijadas durante la instalación inicial del software.

### 3.4. Assigning Software vs. Publishing Software



**Los dos tipos de instalación son:** asignar software y publicar software.

Usando la asignación de software, Usted se asegura que el software esté siempre disponible para el usuario. Cuando éste inicie sesión, aparecerán ***Start*** menu shortcuts y desktop icons para el aplicativo. Por ejemplo, si el usuario abre un archivo que utiliza Microsoft Excel en una computadora que no tiene Excel, pero Excel ha sido asignado al usuario, Windows Installer instala Excel en la computadora cuando el usuario abre archivo. Además, el asignar software hace al software resilient. Si por cualquier razón el usuario quita el software, Windows Installer lo reinstalará la próxima vez que el usuario inicie sesión e inicie el aplicativo.

Usando la publicación de software, Usted se asegura que el software esté disponible para que los usuarios lo instalen en sus computadoras. Windows Installer no agrega shortcuts en el escritorio del usuario o en el ***Start*** menu, y no realiza entradas en registry local. Dado que los usuarios deciden instalar el published software, Usted puede publicar software solamente a los usuarios y no a las computadoras.

***Usted puede asignar y publicar software usando uno de los métodos de la tabla siguiente:***

| Método de instalación | Método 1 | Método 2 |
|---|---|---|
| Asignación | Configurando al usuario. Cuando Usted asigne software a un usuario, el software se anunciará en el escritorio del mismo cuando inicie sesión. La instalación no comenzará hasta que el usuario haga doble-click al inicio de la aplicación o a un archivo asociado con la aplicación. Este es un método llamado activación de documento. Si el usuario no activa el aplicativo, el software no es instalado. De esta forma, se ahorra espacio en el disco duro y tiempo. | Configurando la computadora. Cuando Usted asigne software a una computadora, ningun aviso ocurrirá. En su lugar, el software se instalará automáticamente cuando la computadora se encienda. Asignando software a una computadora Usted se asegura que ciertos aplicativos estén siempre disponibles en esa computadora, sin importar quién la utiliza. Usted no puede asignar software a una computadora que sea domain controller. |
| Publicación | Usando Add or Remove Programs. Un usuario puede abrir el Control Panel y hacer doble-click en Add or Remove Programs para exhibir los aplicativos disponibles. El usuario puede seleccionar un aplicativo y entonces hacer click en Add. | Usando la activación de documentos. Si usted publica un aplicativo en Active Directory las extenciones de nombre de archivo de los documentos soportados por la aplicación serán asociadas en el directorio. |

## 3.5. Práctica 7: ¿Cómo utilizar una GPO para instalar Software?

Después de crear un software distribution point, Usted deberá crear una GPO que instale esos aplicativos, y después linkear la GPO al contenedor que contenga los usuarios o computadoras en donde desee instalar el software.

**Importante:** No asignar ni publicar un Windows Installer package más de una vez en la misma GPO. Por ejemplo, si Usted asigna Microsoft Office XP a computadoras que son afectadas por una GPO, no deberá asignar ni publicar a los usuarios afectados por la misma GPO.

***Para utilizar una GPO para instalar software, tendrá que realizar los siguientes pasos:***

1. Crear o editar la GPO.
2. Bajo ***User Configuration*** o ***Computer Configuration*** (dependiendo si Usted está asignando el software a los usuarios o a las computadoras o publicándolo a los usuarios), expandir ***Software Settings***, hacer click derecho en ***Software Installation***, marcar ***New***, y después hacer click en ***Package***.
3. En el cuadro ***File Open***, hacer browse al software distribution point, usando el nombre Universal Naming Convention (UNC). Por ejemplo, **\\ServerName\ShareName**, seleccionar el archivo package y después hacer click en ***Open***.

4. En el cuadro ***Deploy Software***, seleccionar el método de instalación y después hacer click en ***OK***.

### 3.6. Práctica 8: ¿Cómo cambiar las opciones para la instalación de Software?

Un GPO puede contener varias configuraciones que afecten cómo un aplicativo es instalado, manejado y quitado. Usted puede definir las configuraciones por defecto global para los nuevos packages en la GPO, también puede cambiar algunas de estas configuraciones más adelante, editando las propiedades del package en la extensión de la instalación de software. Después de instalar un software package, recién podrá cambiar las características de la instalación que fueron fijadas durante la instalación inicial del software. Por ejemplo, Usted puede prevenir a usuarios la instalación del software package usando la activación de documento.

***Para configurar las opciones implícitas para la instalación del software, deberá realizar los siguientes pasos:***

1. Crear o editar la GPO.
2. Bajo ***User Configuration*** o ***Computer Configuration***, expandir ***Software Settings***, hacer click derecho en ***Software Installation*** y después en ***Properties***.
3. En la lengüeta ***General***, configurar las opciones siguientes de la instalación de software:

   - ***Default package location***
   - ***When adding new packages to user settings***
   - ***Installation user interface options***

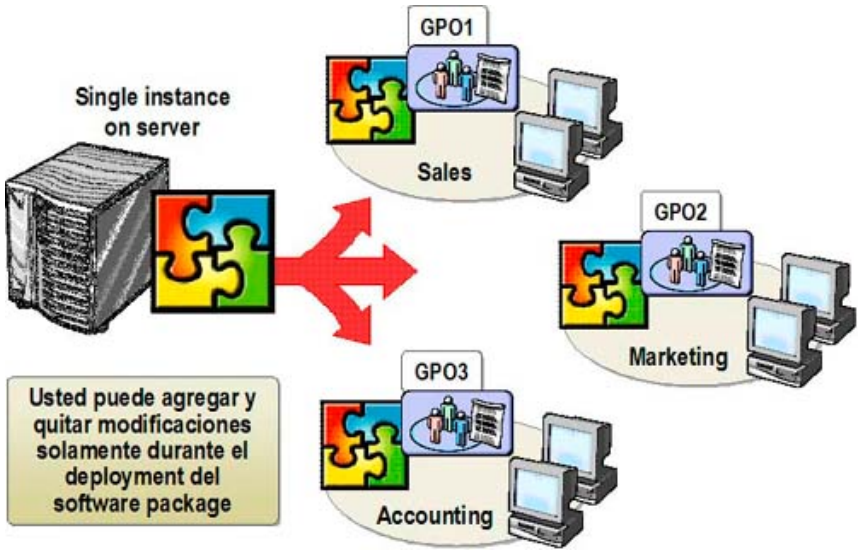
4. En la lengüeta ***Advanced***, seleccionar la opción ***Uninstall the application when they fall out of the scope of management***.

***Para cambiar las características de la instalación de software, deberá:***

1. En Software Installation, hacer click derecho en el package instalado, y después hacer click en ***Properties***.
2. En el cuadro ***Properties*** de la lengüeta ***Deployment***, cambiar las siguientes opciones:

   - ***Deployment type***
   - ***Deployment options***
   - ***Installation user interface options***

### 3.7. ¿Qué es la modificación de Software?



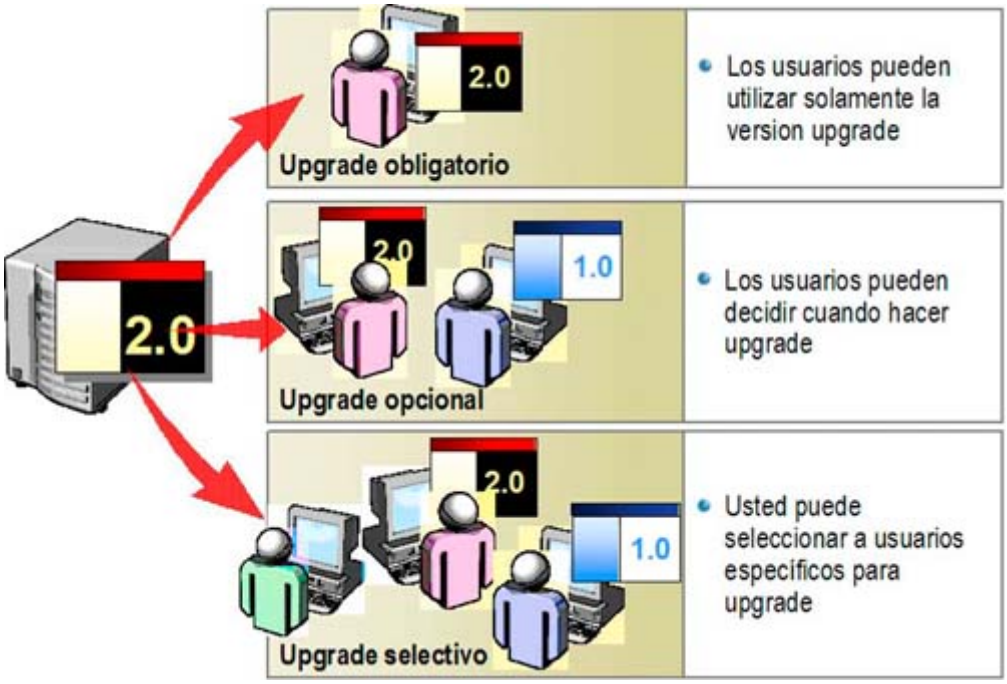

Las modificaciones se asocian a un Windows Installer package en la instalación anterior que utilice ese Windows Installer package para instalar o modificar el aplicativo.

Instalar varias configuraciones de un aplicativo, permite a diversos grupos en su organización utilizar un paquete de software de diversas maneras. Usted puede utilizar modificaciones de software o archivos ***.mst*** (también llamado ***archivos de transformación***) para instalar varias configuraciones de un aplicativo. Un archivo .mst es un custom software package que modifica cómo Windows Installer instala el ***.msi*** package asociado.

Windows Installer aplica modificaciones a packages en el orden que Usted especifique. Para guardar modificaciones en un archivo .mst, deberá correr el custom installation wizard y elegir el archivo .msi en el cual desea basar la transformación. Usted deberá determinar el orden en el cual aplicar las transformaciones a los archivos antes de asignar o publicar el aplicativo.

**Ejemplo:** Una organización grande, por ejemplo, puede querer instalar Microsoft Office XP, pero los requisitos por departamento para el Office suite varian extensamente en la organización. En lugar de configurar manualmente cada uno de los departamentos, Usted puede utilizar diferentes GPOs y archivos .mst en combinación con los archivos .msi por defecto, para que cada departamento instale varias configuraciones de Office XP. En este ejemplo, Usted puede correr el Office XP custom installation wizard del Office Resource Kit para crear el archivo de transformación.

### 3.8. Tipos de actualización de Software




Las tareas en una organización son dinámicas y variadas. Usted puede utilizar Group Policy para instalar y administrar software upgrades que cumplan con requisitos departamentales en su organización. Las actualizaciones implican típicamente cambios importantes al software y tienen nuevos números de versión. Generalmente, un número substancial de archivos cambia para una actualización.

***Varios acontecimientos en el ciclo de vida de un aplicativo pueden accionar la necesidad de una actualización, incluyendo lo siguiente:***

- Una nueva versión del software se lanza y contiene nuevas y mejoradas características.
- Parches y seguridad o realces funcionales se han hecho al software desde el lanzamiento pasado.
- Una organización decide utilizar un software de diversos vendedores.

***Hay tres tipos de actualizaciones:***

***Mandatory upgrades.*** Estas actualizaciones substituyen automáticamente una vieja versión del software con la nueva version. Por ejemplo, si los usuarios utilizan actualmente la versión del programa 1.0, se quita esta versión, y la versión del programa 2.0 se instala la próxima vez que la computadora se encienda o el usuario inicie sesión.

***Optional upgrades.*** Estas actualizaciones permiten que los usuarios decidan cuándo actualizar la nueva versión. Por ejemplo, los usuarios pueden determinar si desean actualizar a la versión 2.0 del software o continuar usando la versión 1.0.

***Selective upgrades.*** Si algunos usuarios requieren una actualizacion pero no otros, Usted puede crear GPOs múltiples para que se apliquen a los usuarios que requieran la actualización y crear los paquetes de software apropiados en ellas.

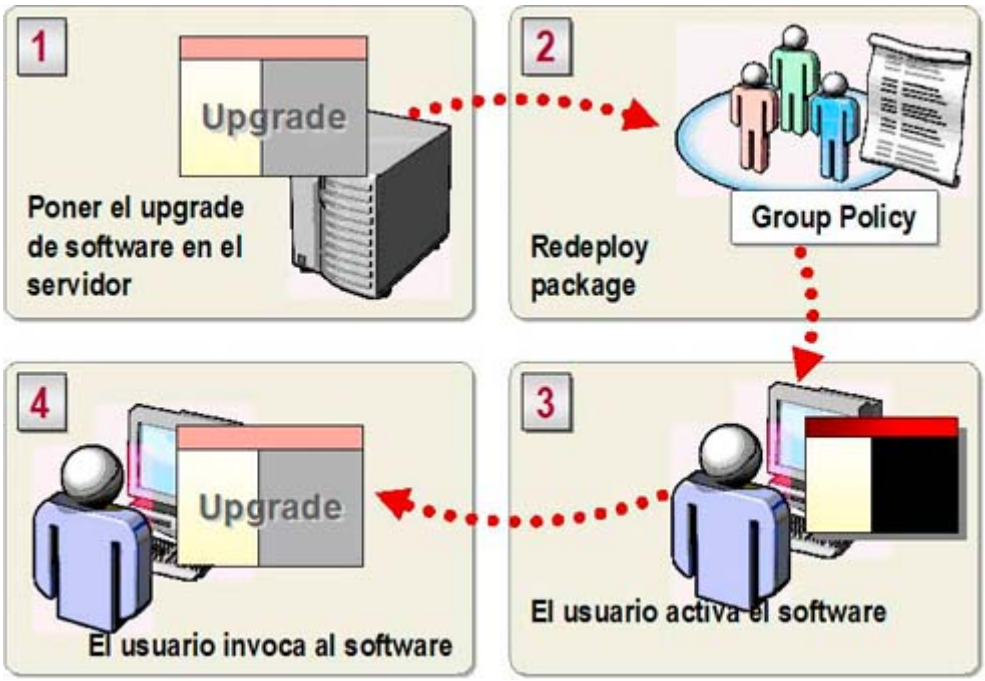
### 3.9. Práctica 9: ¿Cómo actualizar el Software instalado?

Usted utiliza la instalación de software para establecer el procedimiento de actualización de software a la versión actual.

***Para instalar una actualización, deberá:***

1. Instalar la versión siguiente del software.
2. Abrir Software Installation, hacer click derecho en la nueva versión, y después hacer click en ***Properties***.
3. En el cuadro ***Properties*** de la lengüeta ***Upgrades***, en la sección ***Packages that this package will upgrade***, hacer click en ***Add***, y despues seleccionar la versión anterior (actual) del software. Usted puede actualizar un aplicativo usando la GPO actual o seleccioando una GPO específica. Si ambas versiones del programa tienen un Windows Installer Package de forma nativa, este paso se realizará automáticamente.
4. Hacer Click en ***Package can upgrade over existing package o Uninstall the existing package, then install the upgrade package***, y despues hacer click en ***OK***.
5. Seleccionar el tipo de actualización:
   - Para realizar un mandatory upgrade, seleccionar el cuadro ***Required upgrade for existing packages***, y después hacer click en ***OK***.
   - Para realizar un optional upgrade, limpiar el cuadro ***Required upgrade for existing packages***, y después hacer click en ***OK***.

### 3.10. ¿Cómo funciona la reinstalación de Software?




***Redeployment*** es la aplicación de service packs y actualizaciones de software al software instalado. Usted puede instalar un package instalado forzando la reinstalación del software. La reinstalación puede ser necesaria si el software package instalado previamente es actualizado pero sigue teniendo la misma versión, o si hay problemas de interoperabilidad o virus que la reinstalación del software arregle.

Cuando Usted marca un archivo package para reinstalación, el software se anuncia a cada uno de los que se ha concedido el acceso al aplicativo, ya sea a través asignación o publicación. Entonces, dependiendo de cómo el package original haya sido instalado, uno de estos tres escenarios ocurrirá:

- Cuando usted asigne software a un usuario, el ***Start*** menu, los shortcuts de escritorio y la configuración de registry serán relevantes al software y actualizados la próxima vez que el usuario inicie sesión. La próxima vez que el usuario inicie el software, el service pack o actualización de software se aplicará automáticamente.

- Cuando usted asigne software a una computadora, el service pack o actualización de software se aplicará automáticamente la próxima vez que la computadora se encienda.

- Cuando Usted publique e instale software, el ***Start*** menu, los shortcuts de escritorio y la configuración de registry, serán relevante al software y actualizados la próxima vez que el usuario inicie sesión. La próxima vez que el usuario inicie el software, el service pack o actualización de software se aplicará automáticamente.

## 3.11. Práctica 10: ¿Cómo reinstalar Software?

Usted utiliza la instalación de software para establecer el procedimiento de reinstalación del mismo. Antes de reinstalar, asegúrese que el servicio incluya un nuevo archivo Windows Installer package (.msi ). De lo contrario, Usted no podrá reinstalar el software, porque solamente el nuevo archive package contiene las instrucciones para instalar los archivos nuevos que el service pack o actualización de software contiene.

***Para reinstalar un software, deberá:***

Obtener el service pack o actualización de software del vendedor del aplicativo y colocar los archivos en las carpetas apropiadas de instalación.

1. Editar la GPO que originalmente instaló el software.
2. Abrir Software Installation, hacer click derecho en el nombre del archive package, marcar ***All Tasks***, y después hacer click en ***Redeploy Application***.
3. En el cuadro de diálogo, hacer click en ***Yes***.

## 3.12. Métodos para quitar Software instalado


Puede ser necesario quitar el software si una versión no es soportada en adelante o si los usuarios no requieren más el software. Usted puede forzar el retiro del software o dar a los usuarios la opción de continuar, usando el viejo software.

**Hay dos métodos de remoción:**

***Forced removal.*** Usted puede forzar la remoción del software, lo cual automáticamente removerá el software de la computadora la próxima vez que la computadora se encienda o la próxima vez que un usuario inicie sesión, en caso de un Group Policy setting de usuario. El software se removerá antes que aparezca el escritorio del usuario.

***Optional removal.*** Usted puede quitar el software de la instalación del mismo sin forzar el retiro del software. El software no se quita realmente de las computadoras. El software no aparece más en ***Add or Remove Programs***, pero los usuarios pueden todavía utilizarlo. Si los usuarios remueven manualmente el software, no podrán reinstalarlo.

## 3.13. Práctica 11: ¿Cómo quitar Software instalado?

Cuando Usted utiliza Group Policy para instalar software, puede configurar la GPO para remover el software viejo, si no es más requerido por su organización. También quitar software viejo configurando la GPO que permite a los usuarios un optionally upgrade a un nuevo software package.

***Para quitar software instalado, deberá:***

1. Abrir la GPO que fue utilizada originalmente para instalar el software.
2. En Software Installation, hacer click derecho al nombre del package, marcar ***All Tasks***, y después hacer click en ***Remove***.
3. En el cuadro ***Remove Software***, hacer click a una de las siguientes opciones, y después hacer click en ***OK***.

- ***Immediately uninstall the software from users and computers.***

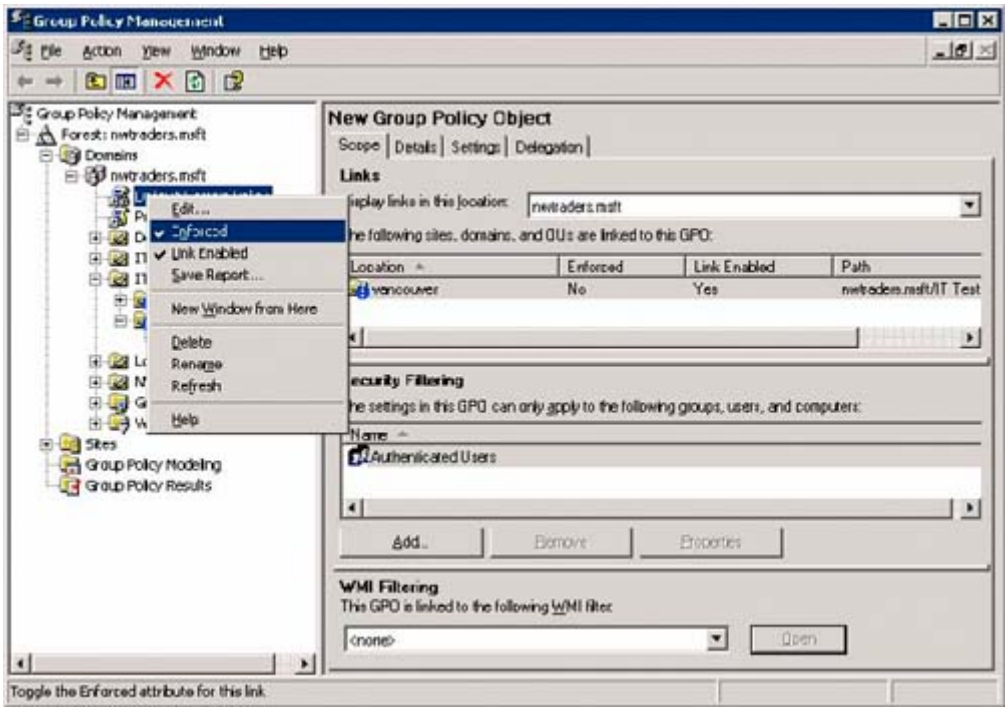
- ***Allow users to continue to use the software, but prevent new installations.***

**Nota:** Usted debe asegurarse que los usuarios reinicien sus computadoras si el cambio afecta a la computadora, o que inicien sesión nuevamente si el cambio afecta al usuario.

## 4. new! Group Policy Management Console (GPMC)

Conjuntamente con Microsoft® Windows Server. 2003, Microsoft está lanzando una nueva herramienta Group Policy Management que unifica la administracion de Group Policy. La Microsoft Group Policy Management Console (GPMC) proporciona una sola solución para manejar todas las areas relacionadas a Group Policy. Consiste en un nuevo Microsoft Management Console (MMC) snap-in y un sistema de interfases de scripting para la administración de Group Policy Management Console. La GPMC ayuda manejar una empresa con más eficacia.

### 4.1. ¿Qué es la Group Policy Management Console?




La Group Policy Management Console (GPMC) es una herramienta nueva para manejar Group Policy en Windows Server 2003.

***La GPMC:***

- Permite que usted maneje Group Policy para múltiples forests, dominios y organizational units a partir de una interfaz constante.
- Exhibe los links, herencia y delegación de Group Policy
- Muestra los contenedores a los cuales se aplican policy.
- Proporciona reportes HTML de las configuraciones.
- Proporciona las herramientas para mostrar el Resultant Set of Policies (RSoP) y experimentar con combinaciones propuestas de policies.

**Nota:** La GPMC no viene con Windows Server 2003. Usted puede descargarla de

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

## 4.2. GPMC Requisitos del Sistema

GPMC ayuda a manejar ambos dominios basados en Windows 2000 y Windows Server 2003 con Active Directory® service.

***En cualquier caso, la computadora en la cual corre GPMC debe funcionar con uno de los sistemas operativos siguientes:***

- Windows Server 2003.

- Windows XP Professional con Service Pack 1 (SP1) y Microsoft .NET Framework. Además, es requerido un hotfix post-SP1 (QFE Q326469). Este QFE actualiza su versión de gpedit.dll a version 5.1.2600.1186, la cual se requiere para GPMC. Este QFE se incluye con GPMC y la instalación de GPMC le pregunta sobre su instalación. Sin embargo, si el lenguaje de GPMC no concuerda con el lenguaje de su sistema operativo, GPMC no instalará el QFE y se necesitará obtener e instalar por separado este QFE, que será incluido en Windows XP Service Pack 2.

## 4.3. Instalación de GPMC

La instalación de GPMC es un proceso simple que implica la ejecución de un Windows Installer (.MSI) package. Los archivos necesarios serán instalados en la carpeta **%SystemRoot%\Program Files\GPMC**.

***Para ello:***

1. Hacer Doble-click en ***gpmc.msi*** package y en ***Next***.
2. Aceptar el End User License Agreement (EULA), y hacer click en ***Next***.
3. Hacer Click en ***Close*** para terminar la instalación.

Sobre la terminación de la instalación, la lengüeta Group Policy que aparecía en las páginas de propiedades de sites, dominios y organizational units (OUs) en el Active Directory snap-ins, es actualizada para proporcionar un acceso directo a la GPMC. La funcionalidad que existió previamente en la lengüeta original de Group Policy no estará más disponible; toda la funcionalidad para manejar Group Policy estará disponible a través de la GPMC.

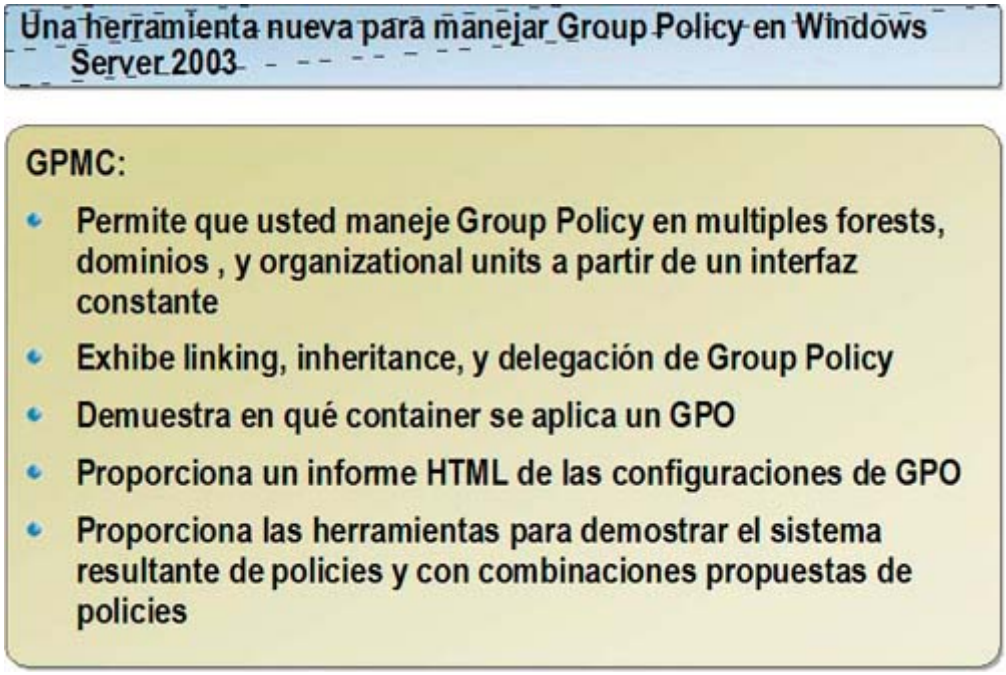
***Para abrir el GPMC snap-in directamente, utilizar alguno de los métodos siguientes:***

- Hacer Click en ***Start***, click ***Run***, ingresar ***GPMC.msc***, y después hacer click en ***OK***.
- Hacer Click en el acceso ***Group Policy Management*** en la carpeta ***Administrative Tools*** del Start Menu o en el Control Panel.
- Crear una consola custom MMC

1. Hacer Click en ***Start***, click ***Run***, ingresar ***MMC***, y después hacer click en ***OK***.
2. En el menu ***File***, hacer click en ***Add/Remove Snap-in,*** hacer click en ***Add***, seleccionar ***Group Policy Management***, hacer click en ***Add***, hacer click en ***Close***, y después hacer click en ***OK***.

- Para reparar o quitar GPMC, usar ***Add or Remove Programs*** en Control Panel. Alternativamente, correr el gpmc.msi package, seleccionr la opción apropiada, y hacer click en ***Finish***.

### 4.4. Group Policy Modeling y Group Policy Results




#### *Group Policy Modeling*

Windows Server 2003 tiene una nueva característica de gran alcance: Group Policy Management. Esta permite que el usuario simule la aplicación de policy que sería aplicada a los usuarios y a las computadoras antes aplicar realmente policies. Esta característica, es conocida como Resultant Set of Policy (RSoP). El Modo de planeamiento en Windows Server 2003, se integra en GPMC como Group Policy Modeling. Esto requiere un domain controller Windows Server 2003 en el forest porque la simulación es realizada por un servicio que está solamente presente en domain controllers Windows Server 2003.

Sin embargo, usando esta característica, Usted puede simular el resultant set of policy para cualquier computadora en el forest, incluyendo las que funcionan con Microsoft Windows® 2000.

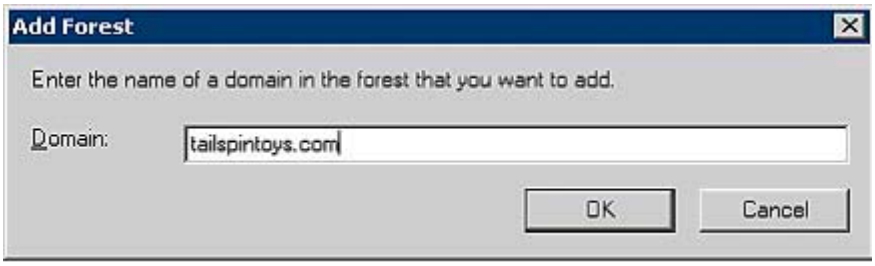
#### *Group Policy Results*

Esta característica permite que los administradores determinen el resultant set of policy que fue aplicada a una computadora específica y (opcionalmente) el usuario que inició sesión en esa computadora. Los datos que se presentan son similares a los datos de Group Policy Modeling. Sin embargo, son diferentes a Group Policy Modeling puesto que no son una simulación. Es el resultado real de resultant set of policy obtenido de la computadora destino. También difiere Group Policy Modeling, con los datos de Group Policy Results que se obtienen del cliente, y no se simula en el domain controller. El cliente debe correr Windows XP, Windows Server 2003 o superior. No es posible conseguir Group Policy Results para una computadora que corra Windows 2000 o anterior.

## 4.5. Administrando múltiples Forests

***Múltiples forests pueden ser agregados fácilmente a la consola. Para ello deberá:***

1. Hacer click derecho al nodo de la raíz ***Group Policy Management***, y seleccionar ***Add Forest...***




2. Especificar el nombre DNS o NetBIOS del dominio deseado en el forest que no se haya cargado en GPMC, y hacer click en ***OK***.

El forest especificado aparecerá como nodo secundario en la consola y será cargado en la consola con el dominio que fue incorporado en el cuadro ***Add Forest***.

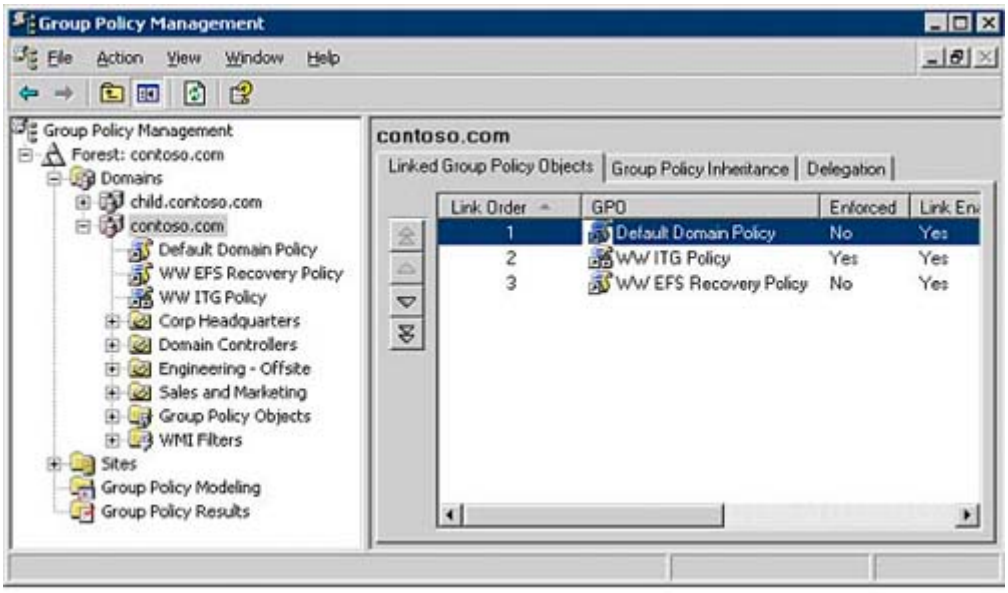
Para quitar un nodo de forest, simplemente haga click derecho en el nodo, y seleccione ***Remove***. Por defecto usted puede agregar solamente forest a la GPMC si hay 2-way trust con el forest del usuario que corre la GPMC.

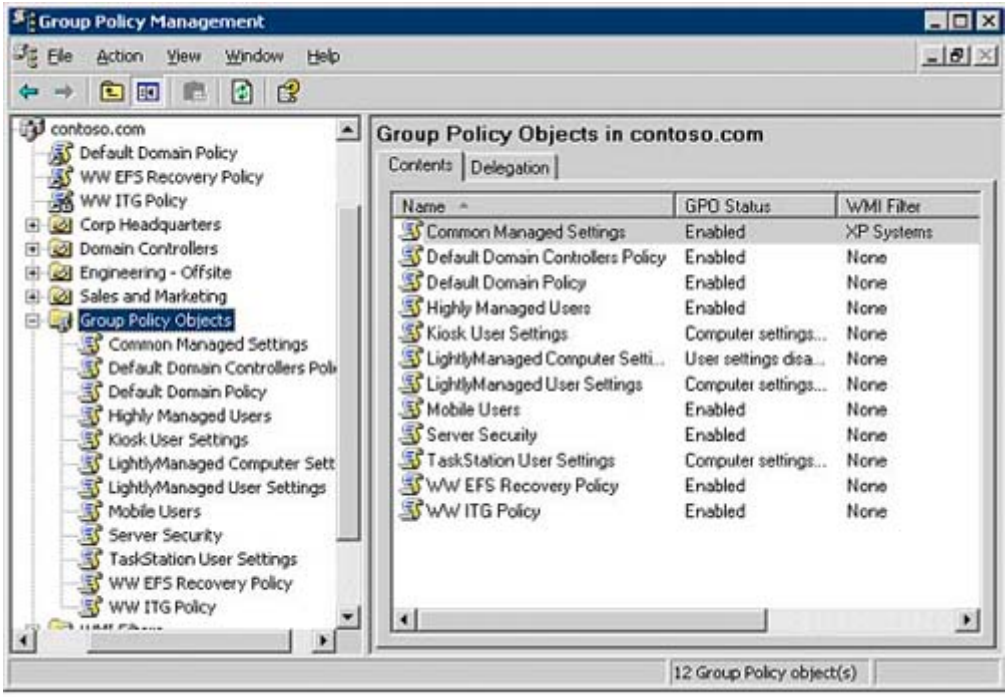
## 4.6. Contenido de Dominios

Dentro de cada dominio, GPMC proporciona una vista basada en policy de Active Directory y los componentes asociados a las Group Policy, por ejemplo, GPOs, WMI filters y GPO links. La visión en GPMC es similar a la visión en Active Directory Users and Computers MMC snap-in, que muestra la jerarquía de OU. Sin embargo, GPMC difiere de este snap-in porque en vez de mostrar usuarios, computadoras y grupos en OUs, exhibe las GPOs que están linkeadas a cada contnedor.

***Cada nodo de dominio en GPMC exhibe los puntos siguientes:***

- Todas las GPOs linkeadas al dominio.
- Todas las top-level OUs y una vista del árbol de OUs y GPOs linkeadas a cada una de las OUs.
- Los contenedores de ***Group Policy Objects*** muestran todas las GPOs en el dominio.
- El contenedor ***WMI Filters*** muestra todos los WMI Filters en el dominio.



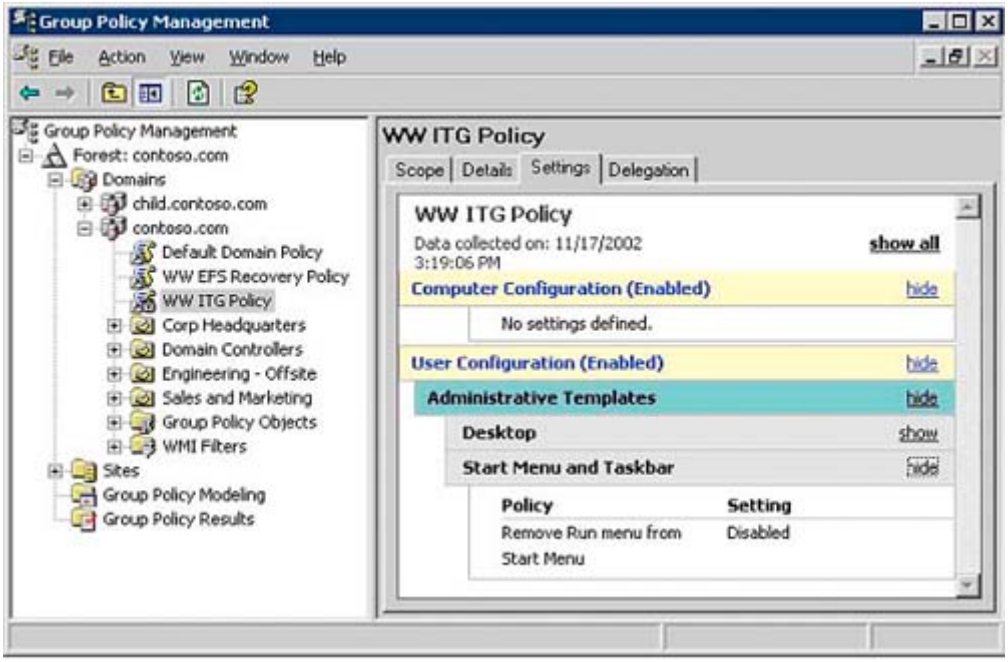




### 4.7. Reportes de configuración de GPO

La lengüeta de configuración de GPO o GPO link en GPMC, muestra un informe HTML que exhibe todas las configuraciones definidas en la GPO. Haciendo click en esta lengüeta se genera un informe de las configuraciones en la GPO. Este informe puede ser generado por cualquier usuario con acceso de lectura al GPO. Sin GPMC, usuarios que no tenían acceso de escritura a un GPO no podrán leer y revisar configuracion en esa GPO. Esto es porque el editor de Group Policy Object requiere que el usuario tenga permisos de lectura y escritura al abrir la GPO.

Los informes HTML también hacen fácil que el administrador tenga visión de todas las configuraciones que se contengan en un GPO de un vistazo. Seleccionando la opción ***Show All*** arriba del informe, éste se amplía completamente y se muestran todas las configuraciones.

Para ver o guardar un informe directamente en un browser Web, Usted debe utilizar Internet Explorer 6 o Netscape 7. Netscape 7 no soporta la funcionalidad que permita mostrar u ocultar datos en informes.




## 4.8. Operaciones con GPO

Las operaciones GPO se refieren a la capacidad de ***backup*** (export), ***restore***, ***import*** y copy de GPOs. Hacer backup de GPO consiste en hacer copia de los datos de GPO al sistema de archivos. Observar que la función ***Backup*** también sirve como la función de la exportación para GPOs.

El Restore de GPO toma un backup existente y recrea la GPO en el dominio. El propósito del restore es reajustar un GPO específico de nuevo al estado idéntico que tenia cuando fue realizado el backup. Por lo tanto, la operacion de restore no puede ser utilizada para transferir GPOs a través de dominios. Para esta operación debe utilizar la importación de GPO ó la operación de copy.

### 4.8.1. Backup

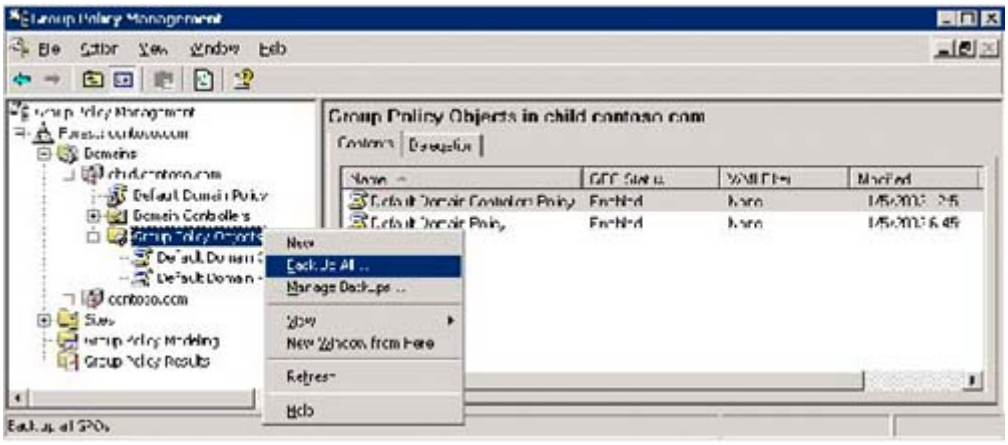
***El Backup de GPO pone una copia de todos los datos relevantes de GPO en una localización especificada del sistema de archivos. Los datos relevantes incluyen:***

- El GPO GUID y dominio.
- Configuraciones GPO.
- La Discretionary Access Control List (DACL) de la GPO.
- Los WMI filter link.

La operación de backup solamente hace backup de componentes de la GPO que están en Active Directory y en la estructura de archivo de GPO en SYSVOL. La operación no captura los datos almacenados fuera del GPO, por ejemplo WMI filters e IP Security policies. Éstos son objetos separados con su propio sistema de permisos y es posible que un administrador que realiza el backup o el restore, pueda no tener los permisos requeridos en esos otros objetos.

***Los administradores pueden hacer backup de una o más GPOs usando los métodos siguientes:***

- Hacer click derecho en la GPO bajo el nodo ***Group Policy objects*** y elegir ***Back up...*** del menú de contexto.
- Hacer click derecho en una o más GPOs en la lengüeta ***Contents*** del nodo ***Group Policy objects*** y elegir ***Back up...*** del menú de contexto. Esto hace backup de las GPO(s) seleccionadas.
- En el nodo ***Group Policy Objects***, hacer click derecho y elegir la opción ***Back Up All...*** Esto hace backup de todas las GPOs en el dominio.
- Use los GPO backup scripts. Usted puede escribir sus el propios scripts o puede utilizar la muestra de scripts incluida con GPMC en la carpeta GPMC\scripts . Hay dos scripts ***BackupGPO.wsf*** y ***BackupAllGPOs.wsf*** que se incluyen con GPMC, los cuales usted pueden utilizar para hacer backup de GPOs.




### 4.8.2. Restore

La operación de Restore de GPO restaura la GPO a un estado anterior y puede ser utilizada en los casos siguientes: se realiza backup a la GPO pero se ha removido desde entonces, o la GPO está viva y se desea volverla a un estado anterior.

***La operación de restore substituye los componentes siguientes de una GPO:***

- Configuraciones de GPO.
- ACLs en la GPO.
- Los WMI filter links.

***Usted puede realizar un restore de GPOs usando cualquiera de los métodos siguientes:***

- Para hacer restore una GPO existente, hacer click derecho a la GPO en el contenedor ***Group Policy objects*** y seleccionar ***Restore from Backup...*** Esto abre el ***Restore Group Policy Object Wizard***.

- Usar los GPO restore scripts. Usted puede escribir sus propios scripts o utilizar las muestras de scripts incluídas con GPMC en la carpeta **GPMC\scripts**
  Hay dos scripts ***RestoreGPO.wsf*** y ***RestoreAllGPOs.wsf***.

### 4.8.3. Import

La operación de importación transfiere configuración en una GPO existente de Active Directory, usando un backup de GPO en la localización del sistema de archivos como su fuente. Las operaciones de importación se pueden utilizar para transferir configuraciones a través de GPOs dentro del mismo dominio, a través de dominios en el mismo forest o en forest separados.

Las operaciones de importación son ideales para emigrar Group Policy a través de ambientes donde no hay confianza.

***Las operaciones de importación se pueden realizar usando cualquiera de los métodos siguientes:***

- Hacer click derecho en la GPO bajo el nodo Group Policy Objects y hacer click en Import Settings. Esto iniciará un wizard que lo guiará en el proceso de seleccionar el backup y opcionalmente especificando una tabla de migración si es apropiado.

- Usar uno de los scripts ***ImportGPO.wsf*** o ***ImportAllGPOs.wsf*** que se incluyen con GPMC.

### 4.8.4. Copy

1. Una operación de copia transfiere configuraciones usando una GPO existente en Active Directory como la fuente y crea un GPO nueva como su destino.

2. Una operación de copia se puede utilizar para transferir configuraciones a un GPO nuevo cualquiera en el mismo dominio, en otros dominios, en el mismo forest o en forest separados. Puesto que una operación de copia utiliza un GPO existente en Active Directory como origen, la confianza se requiere entre el origen y los dominios de la destino.

***Las operaciones de copia se pueden realizar usando cualquiera de los métodos siguientes:***

- Hacer click derecho en la GPO origin, elegir la copy y hacer click derecho en el contenedor ***Group Policy Object***s del dominio deseado de destino. Elegir la opción paste.

- Usar drag and drop para arrastrar la GPO origin al contenedor ***Group Policy Objects*** en el dominio destino.

- Usar el script ***CopyGPO.wsf*** command-line que se incluye con GPMC.

Para obtener mas información:

http://www.microsoft.com/windowsserver2003/gpmc/default.mspx
http://www.microsoft.com/windowsserver2003/gpmc/migrgpo.mspx
http://www.microsoft.com/grouppolicy
http://www.microsoft.com/technet/grouppolicy

# Capitulo 6
# Implementación y Administración de Terminal Server en Windows Server 2003.

Terminal Server, en Microsoft® Windows Server 2003, ofrece la experiencia de Windows® para diversificar hardware de escritorio mediante la emulación de terminales.

***As imismo soporta una amplia gama de clientes y mejora los ambientes de cómputo al:***

- Ampliar la familia Windows escalable, que da servicio a compañías que deseen implementar la solución de "cliente delgado" para ofrecer Windows de 32-bits a una gran variedad de dispositivos de hardware de escritorio heredados.

- Combinar el bajo costo de una terminal con los beneficios de un ambiente administrado, basado en Windows. También ofrece el mismo ambiente de bajo costo y administración central de un ***mainframe*** tradicional con terminales, pero añade la familiaridad, facilidad de uso y variedad de soporte para aplicaciones que ofrece una plataforma de sistema operativo Windows.

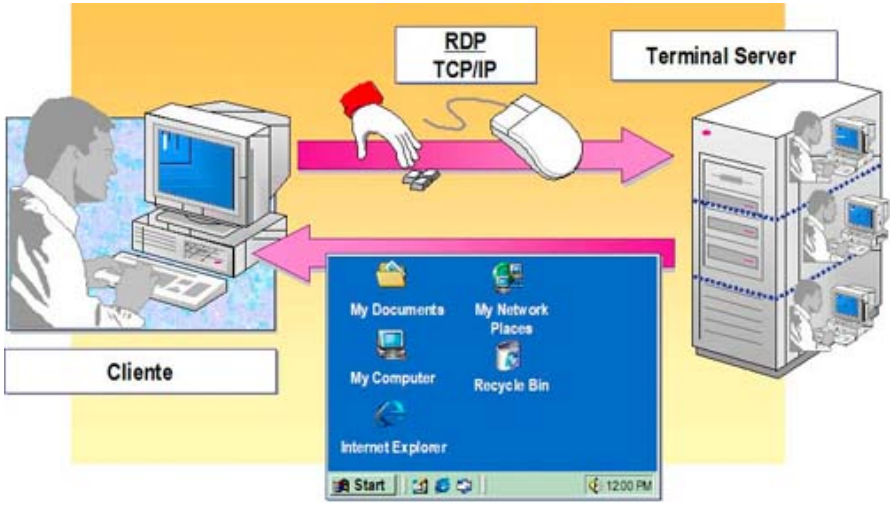
***Al finalizar este capitulo Usted tendrá la habilidad de:***

- Implementar Remote Desktop para administración
- Instalar Terminal Server
- Administrar un entorno Terminal Server

## 1. Introducción

Terminal Services permite el acceso de múltiples usuarios a Windows Server 2003, permitiendo que varias personas inicien sesiones en un servidor simultáneamente. Los administradores pueden instalar aplicaciones basadas en Windows del Terminal Server y ponerlas a disposición de todos los clientes que se conecten con el servidor. Aunque los usuarios pueden tener diversos hardware y sistemas operativos, la sesión Terminal que se abre en el escritorio del cliente conserva el mismo aspecto y funcionalidad para todos.

### 1.1. ¿Cómo funciona Terminal Services?




***Windows Server 2003 Terminal Server consiste en cuatro componentes:***

- ***Terminal Server:*** Este núcleo de servidor multi-usuario proporciona la capacidad de albergar varias sesiones simultáneas de clientes en Windows Server 2003 y en versiones futuras de Windows Server. Asimismo puede albergar en forma directa escritorios de cliente multi-usuario compatibles, que se ejecuten en una variedad de hardware. Las aplicaciones estándar basadas en Windows, si están escritas adecuadamente, no requieren ninguna modificación para ejecutarse en Terminal Server, y la vez se pueden utilizar todas las infraestructuras de administración y tecnologías estándar basadas en Windows server 2003 para administrar los escritorios cliente.

- ***Protocolo de escritorio remoto:*** Este Protocolo es un componente clave de Terminal Server y permite al cliente comunicarse con Terminal Server en una red. Se basa en el protocolo T.120 de la Unión Internacional de Telecomunicaciones (UIT), y es un protocolo de multi-canal que está ajustado para ambientes empresariales de ancho de banda elevado, y que dará soporte a tres niveles de encriptación.

- ***Cliente de Terminal Server:*** Es el software de cliente que presenta una interfaz Windows de 32 bits familiar, en una gran variedad de hardware de escritorio:

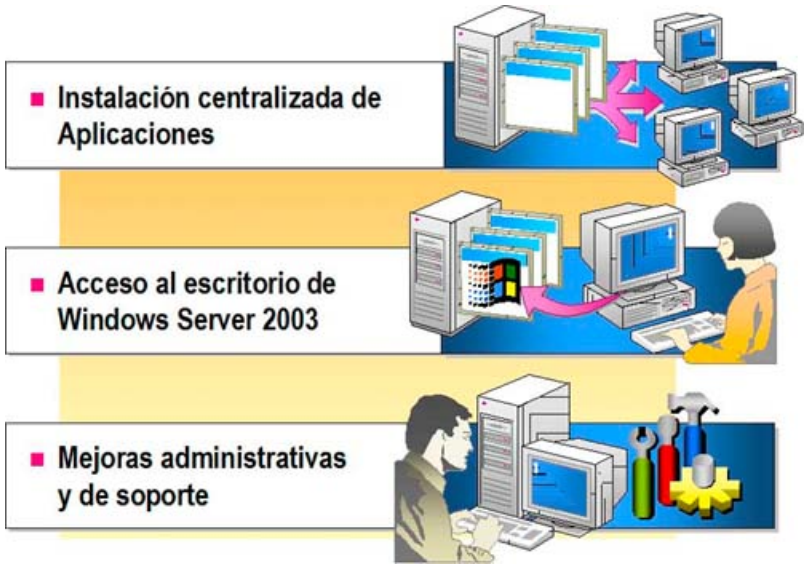
    - Nuevos dispositivos Terminal basados en Windows (incrustados).
    - Computadoras personales que ejecutan Windows 95, Windows 98 y Windows NT Workstation 3.51 o 4.0, Windows 2000 o XP Professional.
    - Computadoras personales que ejecutan Windows for Workgroups 3.11.

- Herramientas de administración: Además de todas las herramientas de administración familiares de Windows Server 2003, Terminal Server añade un administrador de licencias de Terminal Services, la configuración de Terminal Server (MMC) y herramientas de administración para Terminal Server y para sesiones de clientes. Asimismo, se han agregado dos nuevos objetos al Monitor de rendimiento, que son Sesión y Usuario, para permitir ajustarlos al servidor en un ambiente de usuarios múltiples.

### 1.2. Entornos de Usuario


Después de instalar el software de cliente, los usuarios acceden al Terminal Server abriendo Remote Desktop Connection Client del menú ***Programs/Accesories/ Communications.*** Cuando un usuario conecta e inicia sesión al Terminal Server, el escritorio de Windows Server 2003 aparece en el escritorio del cliente. Cuando un usuario inicia un programa, si el programa no está funcionando en forma local, es algo totalmente transparente.

### 1.3. Características y ventajas




Las características de Terminal Server proporcionan varias ventajas que una organización puede utilizar, como instalación, acceso y manejo de los aplicativos de negocio.

### Instalación Centralizada

Las organizaciones pueden instalar aplicaciones de negocios, puesto que el funcionamiento de los programas se realizará enteramente en el servidor. Terminal Server tiene el TCO más bajo para un solo dispositivo de aplicativo que funciona en una línea del aplicativo de negocio, por ejemplo, un sistema de reservas o un Call Center.

***Asimismo proporciona las siguientes ventajas:***

- ***Menos hardware costoso.*** Empleados que realizan sólo los trabajos que requieran el acceso a un programa de negocio y que se puedan equipar de terminales o computadoras menos costosas.

- ***Acceso fácil a software nuevo o actualizado.*** Cuando Terminal Server se habilita en Windows Server 2003, los administradores no tienen que instalar aplicaciones en cada computadora de escritorio. El aplicativo ya está instalado en el servidor y los clientes tienen acceso automático a la nueva o actualizada versión de software.

### Acceso al escritorio Windows Server 2003

Terminal Server puede extender Windows Server 2003 y aplicaciones basadas en Windows a una variedad de clientes.

***Al mismo tiempo, permite:***

- ***Ejecutar aplicaciones Windows.*** Terminal Server puede hacer disponibles aplicaciones Windows a una amplia gama de clientes. Estas aplicaciones basadas en Windows pueden funcionar en diversos sistemas, en el operativo o el hardware, con poca o ninguna modificación.

- ***Ampliar el uso de un equipo más viejo.*** Una organización puede implementar Terminal Server como tecnología transitoria para tender un puente sobre sistemas operativos viejos, con entornos de escritorio Windows Server 2003 y aplicaciones 32-bit basadas en Windows.

- ***Sustituir las terminales basados en texto.*** Dado que muchos terminales basados en Windows pueden soportar conectividad de emulación terminal en el mismo dispositivo, las organizaciones pueden sustituir terminales basadas en texto por terminales basadas en Windows. Estas últimas permiten a usuarios que trabajan con datos de sistemas, tener acceso a software más nuevo basado en Windows, como por ejemplo Microsoft Outlook.

- ***Seguridad y confiabilidad incrementadas.*** Debido a que ningún programa o datos de usuario residen en el cliente, Terminal Server puede proporcionar un ambiente más seguro para los datos sensibles. También proporciona soporte de encripción multinivel, el cual se permite que siempre haya riesgo de intercepción desautorizada de transmisión en la conexión entre el servidor y el cliente. Hay tres niveles de encripción disponibles: low, medium y high. Todos estos niveles usan el Standard Rivest-Shamir-Adleman (RSA) RC4 Encryption. Este es un estándar de encripción para los datos que se envían sobre redes públicas, como por ejemplo Internet.

### Administración y soporte mejorados

***Terminal Server tiene varias características que son útiles para la administración y tareas de soporte, las cuáles puede también ayudar a reducir los costos de administración y soporte:***

- ***Remote administration***. Remote Desktop Administration es una nueva característica en Terminal Server para Windows Server 2003. Está diseñado para proveer a operadores y administradores, el acceso remoto a servidores Microsoft BackOffice® y Domain Controllers. El administrador tiene acceso a las herramientas de interfaz gráficas que están disponibles en el ambiente Windows, incluso si no se está utilizando una computadora basada en Windows para administrar el servidor.

- ***Remote support.*** Los administradores pueden realizar soporte remoto para un usuario que inicia sesión al Terminal Server, siguiendo la sesión del cliente desde otra sesión de cliente. Los administradores o el personal de soporte pueden también realizar acciones de teclado y de mouse a nombre de un usuario, usando Remote Control. Remote Control puede ser útil para el entrenamiento o el soporte de usuarios en sistemas o aplicaciones nuevas.

## 1.4. Planificando la instalación


### 1.4.1. Identificando aplicaciones de Cliente

Antes de instalar Terminal Server, identifique las aplicaciones que Usted piensa instalar en el escritorio del cliente. La mayoría de los programas que funcionan correctamente en Windows Server 2003, se ejecutan también en Terminal Server.

#### Aplicaciones basadas en Windows

Los aplicativos que se instalan en un Terminal Server deben ser compatibles con Windows Server 2003. Si un programa no funciona en Windows Server 2003, no funcionará en el ambiente multiusuario de Terminal Server. Aplicaciones 32-bit funcionan más eficientemente que aplicaciones 16-bit, tomando ventaja completa del hardware y el sistema operativo 32-bit. Ejecutando aplicaciones 16-bit en Terminal Server se puede reducir el número de usuarios que el procesador soporte, tanto como un 40 por ciento, y aumentar la memoria requerida por un usuario, a un 50 por ciento.

#### Aplicaciones MS-DOS

Puesto que aplicaciones basadas en Microsoft MS-DOS® nunca fueron diseñadas para a ambientes de trabajo múltiples, ejecutar aplicaciones MS-DOS en Terminal Server puede retardar el funcionamiento del sistema con procesos ociosos. Si el funcionamiento del servidor se retarda perceptiblemente cuando los usuarios utilizan aplicaciones MS-DOS, se necesitará ajustar las configuraciones del sistema.

### 1.4.2. Identificando requisitos de Hardware del Cliente

Computadoras cliente que se conectan con un Terminal Server no requieren tener mucha energía de proceso, y por lo tanto, es muy fácil integrar Terminal Server en una red que tiene computadoras y equipos viejos.

**Terminal Server soporta las siguientes plataformas**

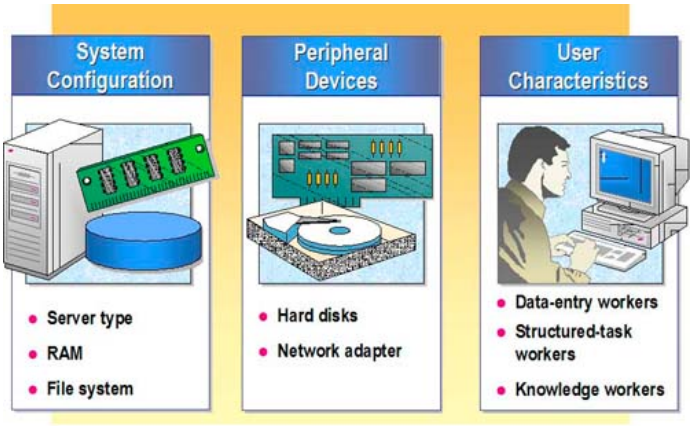
- Microsoft Windows 2000/XP/2003
- Microsoft Windows NT® versions 3.51 and 4.0
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows for Workgroups 3.11
- Microsoft Windows CE, Handheld PC Edition 3.0
- Windows CE, Handheld PC Professional Edition 3.0
- Windows-based Terminals

**Requisitos de Hardware**

La tabla siguiente describe los requisitos de hardware específicos de cliente para Terminal Server.

| Operating System | RAM | CPU | Video |
|---|---|---|---|
| Windows 2000 | 32 megabytes (MB) | Pentium | VGA |
| Windows NT versions 3.51 o 4.0 | 16 MB | 486 | VGA |
| Windows 98 | 16 MB | 486 | VGA |
| Windows 95 | 16 MB | 386 | VGA |
| Windows for Workgroups 3.11 | 16 MB | 386 | VGA |
| Windows CE, Handheld PC/PRO | Vendor | Vendor | Vendor |

### 1.4.3. Determinando la configuración del Server para el soporte de usuarios




Puesto que todo el proceso de aplicaciones ocurre en el servidor, el Terminal Server requiere normalmente más recursos de servidor que una computadora ejecutando Windows Server 2003. Asegurar que su servidor pueda acomodar su base de usuarios es crucial para determinar la manera en que el funcionamiento del servidor Terminal Server debe soportar a usuarios. En adición, es necesario considerar los factores siguientes: configuración del sistema, dispositivos periféricos y características de usuario.

#### Configuración del Sistema

***Antes de instalar Terminal Server, considere las siguientes recomendaciones:***

- ***Tipo de servidor.*** Se recomienda instalar Terminal Server en un Member Server y no en un Domain Controller. Instalar Terminal Server en un Domain Controller puede obstaculizar el funcionamiento del servidor debido a la memoria adicional, el tráfico de la red y el tiempo de procesador que requiere realizar las tareas de un Domain Controller en el dominio.

- ***RAM.*** Generalmente, un Terminal Server requiere un adicional de 4 a 10 MB of RAM para cada sesión terminal en administración, o más, en modo aplicación

- ***File system.*** Se recomienda instalar un Terminal Server en una partición formateada con NTFS File System, ya que éste proporciona la seguridad para los usuarios en un ambiente múltiple de sesión que tienen acceso a las mismas estructuras de datos.

#### Dispositivos Periféricos

***Los dispositivos periféricos pueden también afectar el funcionamiento del Terminal Server:***

- ***Discos duros.*** La velocidad de disco es crítica para el funcionamiento del Terminal Server. Small Computer System Interface (SCSI) disk drives, especialmente dispositivos compatibles con SCSI y Scsi-2 rápidos, tienen un rendimiento de procesamiento perceptiblemente mejor que otros tipos de discos. Esto es menos importante en los sistemas que no almacenan User Profiles y datos en el Terminal Server, pero sí afectará el tiempo de carga del programa inicial. Para un rendimiento más alto de disco, es importante considerar el uso de SCSI Redundant Array of Independent Disks (RAID) Controller. RAID Controller pone automáticamente los datos en discos múltiples para aumentar el rendimiento del disco y para mejorar la confiabilidad de los datos.

- ***Adaptador de red.*** El adaptador de red de alta-performance es recomendado, especialmente si los usuarios requieren acceso a datos que se almacenan en los servidores de red o ejecutan aplicaciones client/server. Usando adaptadores múltiples, se puede aumentar perceptiblemente el throughput de la red, y también se puede incrementar la seguridad del sistema en la separación del acceso de cliente de servicios back-end.

### Características de Usuario

Los patrones de uso de los usuarios de computadoras pueden tener un impacto significativo en el funcionamiento de Terminal Server.

***La prueba de funcionamiento de Microsoft clasifica a usuarios en las tres categorías siguientes:***

- ***Data-entry worker.*** Estos trabajadores funcionan típicamente con un solo aplicativo que utilizan para la entrada de datos (por ejemplo, aplicaciones de negocio escritos en Microsoft Visual Basic®).

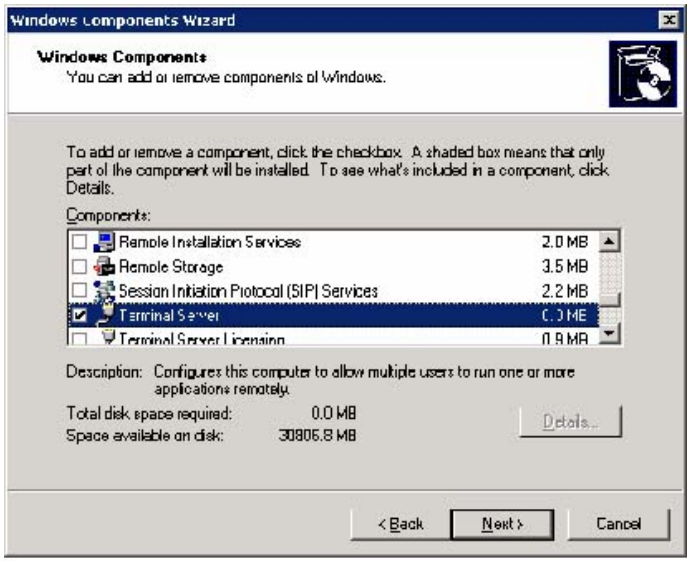
- ***Structured-Task worker.*** Estos trabajadores ejecutan uno o dos programas al mismo tiempo. Los usuarios típicos ejecutan los programas que exige el sistema informático no pesado (por ejemplo, un procesador de textos y un browser). Los programas se abren y cierran con frecuencia.

- ***Knowledge worker.*** Los trabajadores de conocimiento ejecutan tres o más programas simultáneamente, y generalmente dejan los programas abiertos. Knowledge workers también pueden ejecutar programas que exigen al sistema intensamente (por ejemplo, queries detalladas en grandes bases de datos).

## 1.5. Instalando Terminal Server

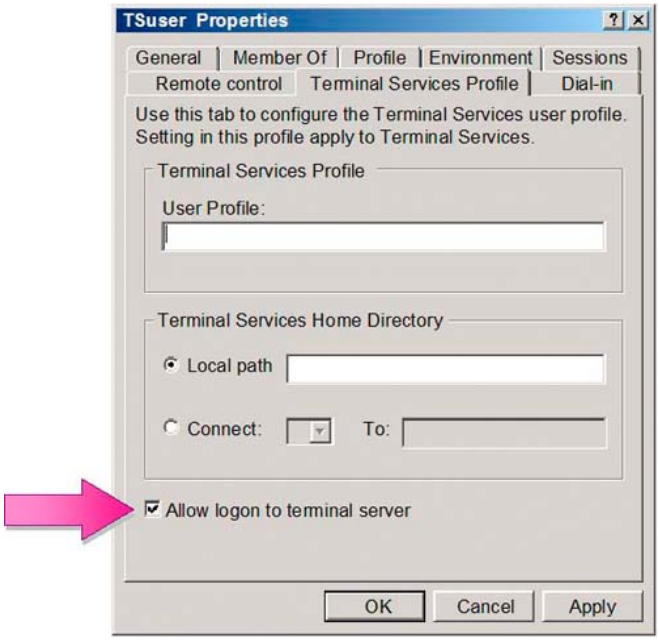
Para instalar Terminal Server, se debe habilitar el componente Terminal Server luego de la instalación, usando el Windows Components wizard. Usted puede habilitar Terminal Server de dos modos: con Terminal Application Server o Remote Desktop Administration. Este último no requiere licenciar y permite solamente tres conexiones. Terminal Server Licensing se puede instalar con Terminal Server o por sí mismo en una otra computadora. Cuando se instale Terminal Server Licensing, se deberá especificar si el servidor de licencias servirá al dominio, Workgroup o site.

Para habilitar Terminal Server (Application), el proceso se realiza mediante el Wizard de Windows Components. En cambio, para habilitar Remote Desktop Administration (Instalado por defecto) debe hacerlo desde las propiedades de System lengüeta "Remote" y seleccionar la opción "Allow users to connect remotely to this computer".




Terminal Server se habilita agregando el componente "Terminal Server" y usando Windows Components en ***Add/Remove Programs*** wizard.

### 1.6. Configurando Acceso de Usuario




Los usuarios que tienen cuentas en un Terminal Server se habilitan para iniciar sesión en el servidor por defecto.

Para inhabilitar el proceso de conexión para un usuario, se debe limpiar el cuadro ***Allow logon to Terminal Server*** en la lengüeta ***Terminal Services Profile*** del cuadro Properties para la cuenta del usuario, y luego hacer click en ***Apply***. En esta lengüeta, Usted también puede especificar home directories y user profiles para los usuarios.

### 1.7. new! Instalando Remote Desktop Connection

Remote Desktop Connection viene incluido en Windows XP y Windows Server 2003, pudiendo también ser instalado en otras computadoras por varios métodos.

- ***Utilizando herramientas***, por ejemplo Microsoft Systems Management Server o Windows 2000 Group Policy usando publish/assign del Windows Installer-based RDC (.msi).

- ***Compartiendo la carpeta*** %systemroot%\system32\clients\tsclient\win32 en Windows Server 2003. (Esto se puede hacer también con Windows 2000 Server.)

- ***Instalando directamente desde el CD de Windows XP o Windows Server 2003***, usando 'Perform Additional Tasks' del menu autoplay . (Esto no requiere la instalación del sistema operativo.)

- ***Descargando el Software RDC desde*** http://www.microsoft.com/windowsxp/remotedesktop/

### 1.7.1. new! Interfaz mejorada

Las sesiones remotas usando Remote Desktop Connection puden realizarse en high-color y full-screen con una barra de conexión para permitir la conmutación rápida entre la sesión remota y el escritorio local. La conexión remota se puede modificar para requisitos particulares y para satisfacer sus necesidades, con las opciones para pantalla, recursos locales, programas y experiencia. La configuración de la lengüeta experiencia permite que Usted elija su velocidad de conexión y opciones gráficas, por ejemplo themes o menu y window animation para optimizar la performance de conexiones con bajo ancho de banda.

### 1.7.2. new! Redirección de recursos del Client

La redirección de recursos está disponible para los clientes Windows Server 2003 o Windows XP Professional, y ofrece una variedad de tpo's de datos a redirigir. Para maximizar seguridad, cada tipo de redirección puede ser habilitado o inhabilitado por separado por el cliente o el servidor. También se exhibe un alerta de seguridad cuando se solicita una redirección del sistema de archivos, puerto o una Smart Card, habilitando al usuario para rechazar la redirección o incluso cancelar la conexión si lo desea.

Remote Desktop Connection habilita la regeneración de audio (por ejemplo notificaciones de "error" o "new mail", se pueden redireccionar al cliente). Combinaciones de teclas, como Alt-Tab y Control-Escape, son enviadas a la sesión remota por defecto, mientras que Control-Alt-Delete es mantenido siempre por la computadora del cliente para mantener la seguridad del servidor. Información Time Zone puede también redirigirse del servidor a los clientes, habilitando un servidor para manejar usuarios múltiples a través de diferentes Time Zones. Los programas con características de calendario pueden aprovechar la redirección de Time Zone.

- new! ***Redireccion de File System***

El copiado de archivos entre el cliente y el servidor es más fácil. Los discos del Cliente, locales y de red, ahora están disponibles dentro de la sesión del servidor. Los usuarios pueden tener acceso a sus propios discos locales y transferir los archivos entre el cliente y el servidor sin tener que salir de la sesión remota.

- new! ***Redireccion de puertos e impresoras***

Impresoras locales y de red instaladas en el cliente están disponibles en la sesión remota, con nombres sencillos. Los puertos seriales del cliente pueden ser montados de modo que el software en el servidor pueda tener acceso al hardware conectado. Clientes que reconocen Smart Cards-Windows 2000, Windows XP, y Windows CE .NET- pueden proporcionar credenciales de Smart Cards para el inicio de sesión a la sesión remota en Windows Server 2003.

### 1.8. Instalando aplicaciones en Terminal Server

Para hacer un aplicativo disponible para usuarios múltiples, una instalación del aplicativo debe copiar archivos de programa a una localización central en el servidor, en lugar del Home Directory de los usuarios.

**Nota:** a los fines de seguridad, se recomienda instalar los aplicativos en una partición NTFS.

***Hay dos métodos para instalar programas en un Terminal Server:***

- ***Usando Add/Remove Programs en el Control Panel o el comando Change User del Command prompt.*** El primero ejecuta automáticamente el comando Change User, que es el método preferido para instalar programas en un Terminal Server.

***Para instalar un programa usando Add/Remove Programs, deberá realizar los siguientes pasos:***

1. Iniciar sesión en el Terminal Server como administrador y cerrar todos los programas.
2. Hacer Click en ***Start, Settings*** y después en ***Control Panel***.
3. En Control Panel, hacer doble-click en ***Add/Remove Programs***.
4. Hacer Click en ***Add New Programs*** y después en ***CD o Floppy***.
5. Seleccionar el archivo de setup para el aplicativo, hacer doble-click en el ejecutable, y después hacer click en ***Next***.
6. En la página ***Change User Option***, verificar si está seleccionando ***All users begin with common application settings***.
7. Instalar el programa en el disco local según las instrucciones del programa de instalación.
8. Seguir las instrucciones en el wizard para finalizar la instalación.

- ***Usando el comando Change User, solamente cuando no se pueda instalar el aplicativo usando Add/Remove Programs.***

***Para instalar un programa usando el comando Change User, deberá realizar los siguientes pasos:***

1. Iniciar sesión en el Terminal Server como administrador y cerrar todos los programas.
2. En una ventana de línea de comandos, ingresar ***change user /install*** y después presionar ENTER.
1. Instalar el programa en el disco local según las instrucciones del programa de instalación.
2. En una ventana de línea de comandos, ingresar ***change user /execute*** cuando la instalación se complete.

Para obtener más información:

http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx

## 2. Administración Remota con Remote Desktop

***Remote Desktop para administración incluye las siguientes características y ventajas:***

- Administración gráfica de servidores Windows Server 2003 y Windows 2000 desde cualquier cliente Terminal Services. (Los clientes están disponibles para las computadoras que funcionen con Windows for Workgroups, Windows 95, Windows 98, Windows CE 2.11, Windows CE.NET, Windows NT®, Windows 2000, Windows XP Professional, y Macintosh OS-X.)
- Actualizaciones remotas, reinicio y promoción / desmonte de Domain Controllers.
- Acceso a los servidores, utilizando conexiones de bajo ancho de banda, hasta con 128-bit de encripción.
- Instalación y ejecución remota de aplicaciones, con el acceso rápido a los discos locales y a los medios (Por ejemplo, cuando se copian archivos grandes y virus scans).
- Posibilidad que dos administradores remotos puedan compartir una sesión para los propósitos de colaboración.
- Remote Desktop Protocol (RDP). Esto incluye la impresión local y de red, redirección de File System, mapeo del clipboard (cut, copy y paste), redirección de Smart Card, redirección de dispositivos serie, y soporte para cualquier programa de canal virtual RDP.

### 2.1. Integrando Terminal Services

El componente Terminal Services de la familia Windows Server 2003 se integra firmemente en el kernel y está disponible en cada instalación de Windows Server 2003. Habilitar Remote Desktop for Administration no requiere espacio de disco adicional y tiene un impacto mínimo en la performance. Solo se necesitan alrededor de 2 megabytes (MB) de la memoria del servidor, con un impacto insignificante en el uso de la CPU. La performance se afecta únicamente cuando se inicia una sesión remota, similar en costo a la consola.

Es por estas razones que Microsoft recomienda habilitar Remote Desktop for Administration en cada computadora y Domain Controller Windows Server 2003. Esto proporcionará flexibilidad y sensibilidad sustanciales en la administración de los servidores de una organización, sin importar su localización.

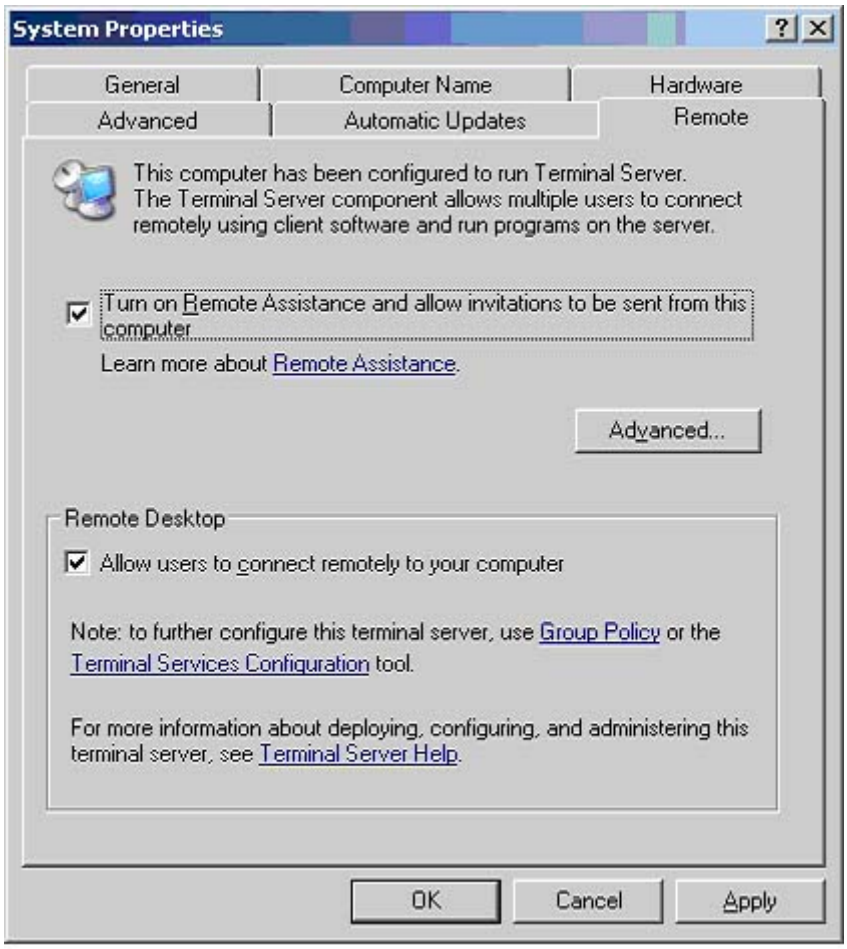
### 2.2. Práctica 1: Habilitando Remote Desktop for Administration

Terminal Server y Remote Desktop for Administration ahora se configuran por separado en Windows Server 2003, proporcionando opciones más flexibles para la administración.

**Remote Desktop for Administration**

Remote Desktop for Administration es instalado por defecto en Windows Server 2003, pero por razones de seguridad viene preconfigurado como deshabilitado. Se puede habilitar con ***System*** en el ***control panel***.

Además de las dos sesiones virtuales que están disponibles en Windows 2000 Terminal Services Remote Administration mode, un administrador puede también conectarse remotamente con la consola verdadera de un servidor, a través de Remote Desktop for Administration en Windows Server 2003. Herramientas que antes no funcionarían en una sesión virtual, porque ellas interactuaban con la 'session 0', ahora funcionan remotamente.




***Para habilitar Remote Desktop for Administration deberá:***

1. En el control panel, hacer doble-click en ***System***.
2. Hacer click en la lengüeta ***Remote***, y después seleccionar el cuadro ***Allow users to connect remotely to this computer***.
3. Hacer click en ***Apply*** y después en ***OK***.

***Para realizar una conexión al Servidor deberá:***

1. Iniciar sesión normalmente en otro equipo con Windows XP ó Windows Server 2003.
2. En ***Start, Run***, ingresar ***mstsc.exe*** y después presionar ***ENTER***.
3. En el cuadro ***Computer***, ingresar el nombre del servidor al cual desea conectarse y después presionar ***ENTER***.

***Para realizar una conexión a la consola deberá:***

1. Iniciar sesión normalmente en otro equipo con Windows XP ó Windows Server 2003.
2. En ***Start Run***, ingresar ***mstsc.exe /console /v:nombredelserver***, y después presionar ***ENTER***.
3. Verificar si luego de iniciar la sesión de consola el servidor al cual Usted se conectó, ha bloqueado la sesión activa.

**Recuerde:** Para realizar esta práctica debe tener al menos dos equipos, ya que es imposible conectar la consola dentro de la misma sesión.

Para obtener más información:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323353

## 2.3. Herramientas de Administración

A continuación, una muestra limitada de las herramientas de administración que pueden ayudarle a manejar sesiones remotas:

### Conectar con la consola

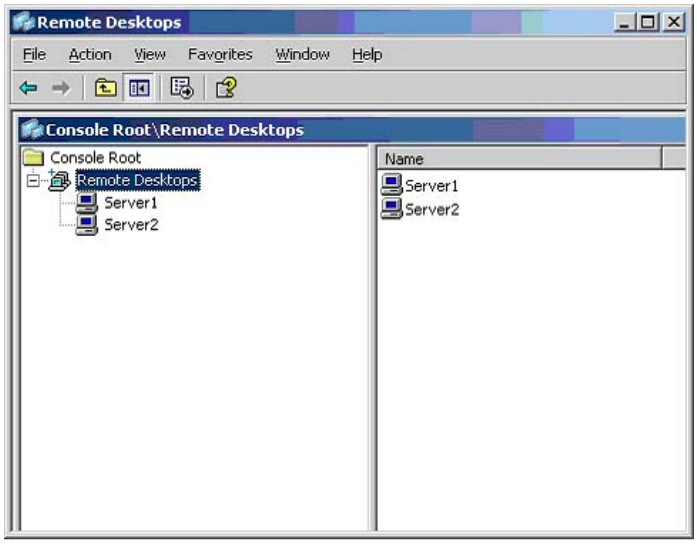
***Para conectar con la consola, los administradores pueden elegir uno de los métodos siguientes:***

- Utilizar Remote Desktop Microsoft Management Console (MMC) snap-in.
- Ejecutar el programa Remote Desktop Connection (mstsc.exe) con el switch /console.
- Crear páginas Remote Desktop Web Connection con la propiedad ConnectToServerConsole.

### Terminal Services Group Policy

Group Policy puede ser utilizado para administrar Terminal Services para las computadoras que ejecuten sistemas operativos Windows Server. Terminal Services Group Policies puede configurar conexión de Terminal Services, de User Policies y de Terminal Server Clusters, y administrar sesiones Terminal Services.

### Remote Desktops MMC




La consola Remote Desktops Microsoft Management Console (MMC) Snap-in habilita a administradores a configurar múltiples conexiones Terminal Services. Es útil también para manejar muchos servidores que ejecuten Windows Server 2003 Family o Windows 2000 Server.

Una exhibición navegable del árbol permite que los administradores vean, controlen y cambien rápidamente entre las sesiones múltiples de una sola ventana. Como con la herramienta Remote Desktop Connection, las computadoras remotas también se pueden configurar para ejecutar programas específicos sobre la conexión, y para redireccionar discos locales en la sesión remota. La información de logon y el área de pantalla del cliente se pueden configurar en el snap-in. Asimismo, los administradores pueden crear conexiones remotas a la sesión de consola de una computadora Windows Server Operating Systems.

### Terminal Services Manager

Esta utilidad, tsadmin.exe, se utiliza para administrar usuarios Terminal Services, sesiones y procesos en cualquier servidor de la red ejecutando Terminal Services. Usando esta herramienta, Usted puede conectar y desconectar, cerrar sesión, resetear y controlar remotamente sesiones. También puede utilizarla para conectarse con otros servidores en dominios confiados, manejar sesiones sobre un servidor remoto, enviar mensajes a los usuarios o cerrar sesiones y terminar procesos.

### Terminal Services Configuration

Esta utilidad, tscc.msc, se utiliza para cambiar la configuración de la encripción por defecto, y para configurar timeouts de reset y disconnect. Para configurar timeouts de reset y disconnect para cuentas individuales, se debe utilizar la lengüeta de las sesiones en el cuadro Account Properties del usuario. Muchas de las configuraciones se pueden fijar también con Terminal Services Group Policy o Windows Management Instrumentation. En ese caso, la configuración de Terminal Services se sobrescribe.

### Event Viewer

Use Event Viewer, eventvwr.msc, para buscar los acontecimientos que pudieron haber ocurrido como dialogos pop-up en la consola del servidor.

### Command-line Utilities

***Command-line utilities incluye lo siguiente:***

- ***Query User.*** Esta es una utilidad de línea de comando, quser, listas usuarios activos y desconectados.

- ***Disconnect.*** Esta utilidad de línea de comando, tsdiscon, desconecta la sesión. Un procedimiento análogo apaga el monitor mientras que deja funcionando de la computadora. Desconectar, es también accesible con Start/Shutdown. Para volver a conectar a la sesión, iníciela simplemente al servidor, otra vez con el mismo usuario desde Remote Desktop Connection.

## 3. Terminal Server como Servidor de Aplicaciones

El componente Terminal Services de Microsoft® Windows® Server 2003 se estructura en la fundación sólida proporcionada por Application Server Mode en Windows 2000 Terminal Services, e incluye las nuevas capacidades del cliente y del protocolo en Windows XP. Terminal Services le deja entregar vitrtualmente, aplicaciones basadas en Windows o el escritorio de Windows, a cualquier dispositivo, incluyendo los que no pueden ejecutar Windows.

Terminal Services en Windows Server 2003 puede mejorar las capacidades de instalación del software de una empresa para una variedad de escenarios, habilitando flexibilidad sustancial en infraestructura y administración de aplicativos. Cuando un usuario ejecuta un aplicativo en Terminal Server, la ejecución del aplicativo ocurre en el servidor, y solamente la información de teclado, mouse y display es trasmitida en la red. Cada usuario ve solamente su sesión individual, la cual es manejada en forma transparente por el sistema operativo del servidor, y es independiente de cualquier otra sesión de cliente.

### 3.1. Beneficios

Terminal Services en Windows Server 2003 proporciona tres importantes beneficios.

| Beneficio | Descripción |
|---|---|
| Instalación rápida y centralizada de aplicaciones. | Terminal Server es óptimo para instalar rápidamente aplicaciones basadas en Windows a través de la empresa, especialmente aplicaciones que se actualizan con frecuencia, que se utilizan con frecuencia o de administración difícil. |
| Acceso a datos utilizando conexiones de bajo ancho de banda | Terminal Server reduce considerablemente el ancho de banda requerido en la red para tener acceso a datos remotamente. Usando Terminal Server para ejecutar un aplicativo sobre conexiones de bajo ancho de banda, por ejemplo dial-up o Links WAN compartidos, resulta muy eficaz para tener acceso remotamente y manipular grandes cantidades de datos, dado que solamente se transmite la pantalla de datos, en lugar de los datos en sí mismos. |
| Windows dondequiera | Terminal Server ayuda a que los usuarios sean más productivos, permitiendo el acceso a los programas actuales en cualquier dispositivo. |

### 3.2. new! Características Adicionales de administración

***Las características siguientes mejoran la flexibilidad de Terminal Services en Windows Server 2003:***

***Group Policy.*** Group Policy puede ser utilizado para controlar las propiedades de Terminal Services. Esto habilita la configuración de grupos de servidores simultáneamente, incluyendo la configuración para las nuevas características, por ejemplo per-computer Terminal Services profile path, y deshabilitando el wallpaper mientras que está conectado remotamente.

***Windows Management Interface Provider.*** Un proveedor completo de Windows Management Instrumentation (WMI) habilita la configuración por medio de scripts de Terminal Services. Un número de alias de WMI son incluidos para proveer un simple front end de tareas frecuentes, usando WMI.

***Printer Management. La administración de impresoras se ha mejorado de las siguientes maneras:***

- El mapeo de Printer driver se ha realzado.
- Cuando un driver no machea con el cliente, es confiado un Driver Path que permite especificar otro standard printer drivers, el cual se agrega en los Terminal Servers.
- La corriente de la impresión se comprime para mejorar la performance en enlaces lentos entre un servidor y un cliente.

**Terminal Services Manager**

Terminal Services Manager mejorado, habilita una administración más fácil de grandes arrays de servers, reduciendo la enumeración automática del servidor. Esto da acceso directo a los servidores arbitrados por nombre, y provee una lista de servidores preferidos.

#### Terminal Server License Manager

El Terminal Server License Manager se ha mejorado dramáticamente para hacer más fácil activar un Terminal Server License Server, y asignarle las licencias.

#### Single Session Policy

Configurando Single Session Policy se permite al administrador limitar usuarios a una sola sesión, sin importar si está activo o no (lo mismo que a través de una granja de servidores).

#### Client Error Messages

Más de 40 nuevos mensajes de error de cliente hacen más fácil diagnosticar problemas de la conexión del cliente.

### 3.3. Mejoras en la Seguridad

El modelo de acceso a Terminal Server ahora se conforma mejor con los paradigmas de administración de Windows Server.

#### Remote Desktop Users Group

En vez de agregar a usuarios a una lista en Terminal Services Connection Configuration (TSCC) Program, Usted simplemente los hará miembros del grupo Remote Desktop Users (RDU). Por ejemplo, el administrador puede agregar el grupo "Everyone" al grupo RDU para permitir que todos tengan acceso al Terminal Server.

Usar un grupo verdadero de NT también significa que el acceso a Terminal Servers puede ser controlado a través Group Policy en grupos de servidores.

#### Security Policy Editor

Para configuraciones adicionales en Terminal Services, los derechos de usuario se pueden asignar a los usuarios o a los grupos individuales, usando el Security Policy Editor. Haciendo esto, Usted le da a los usuarios la habilidad de iniciar sesión al Terminal Server, sin tener que ser un miembro del grupo Remote Desktop Users descrito arriba.

#### 128-Bit Encryption

Por defecto, las conexiones a Terminal Servers se aseguran con 128-bit, bi-direccional RC4 encryption, cuando está utilizando un cliente que soporta 128-bit. (RDC es 128-bit por defecto). Es posible conectar clientes más viejos con encripción mas baja de 128-bit, a menos que se especifique que solamente los clientes high-encryption están habilitados.

#### Software Restriction Policies

Las políticas de restricción de software en Windows Server 2003 habilitan a los administradores a utilizar Group Policy para simplificar el locking down de Terminal Servers, solamente permitiendo que ciertos programas sean ejecutados por los usuarios especificados.

Para obtener mas información:

http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp

Esta característica de Windows sustituye la herramienta AppSec (Application Security), utilizada en versiones anteriores de Terminal Services.

### 3.4. Directorio de Sesión

Terminal Servers puede ser organizado en "granjas." Esta configuración permite clusters de load-balancing de computadoras para ofrecer a sus usuarios un servicio de fault-tolerant.

La nueva característica Session Directory en Terminal Services habilita a los usuarios a reconectar una sesión especifica desconectada dentro de la granja, dirigiéndose a un servidor cargado cuando se conectan.

El Session Directory puede utilizar el servicio Windows Load Balancing o un Load Balancer de terceras partes, y el servicio puede funcionar en cualquier computadora ejecutando Windows Server 2003. Sin embargo, los miembros de la granja de Terminal Server deben ejecutar Windows Server 2003, Enterprise Edition.

### 3.5. Práctica 2: Instalación de Terminal Server Application

Durante esta práctica Usted instalará un Terminal Server para ejecutar aplicaciones.

1. En el control panel, hacer doble-click en ***Add/Remove Programs***, y después en Windows Components.
2. Seleccionar ***Terminal Server***, y después hacer click en ***Next***.
3. Aceptar la configuración por defecto, y hacer click en ***Next***.
4. Al finalizar la instalación, hacer click en ***Finish***.

Para instalar aplicativos, siga las instrucciones en el punto 1.8 del capitulo. Recuerde que puede instalar, por ejemplo, Microsoft Office XP para instalar Microsoft Office 2000, requiriendo el Resource Kit de Office.

### 3.6. new! Windows System Resource Manager

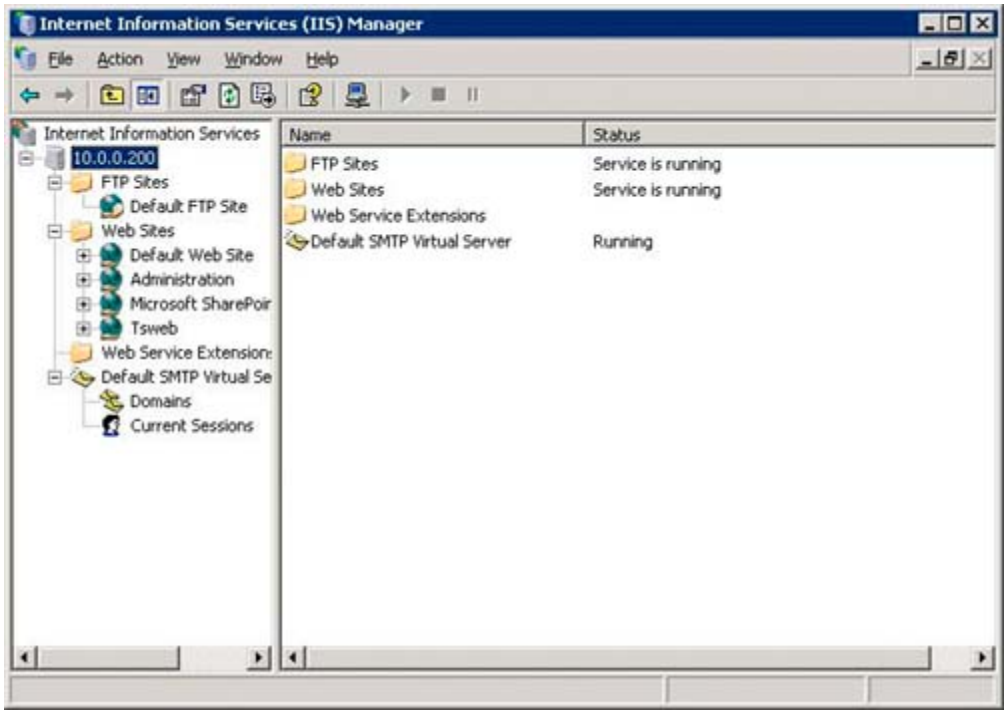
Windows Server 2003 introduce un nuevo producto, que no viene con el CD de Windows Server 2003. Esta herramienta es compatible solamente con las versiones Enterprise y Datacenter.

Windows System Resource Manager (WSRM), permite administrar recursos de hardware, por ejemplo memoria y procesador, asignándole a los usuarios los recursos preestablecidos. De esta forma, Usted puede evitar que un usuario consuma recursos por demás, ejecutando tareas innecesarias o procesos múltiples, sin limite de recursos. También puede asignar a los recursos un schedule de horarios, por ejemplo, asignar durante el día una cantidad de recursos limitada y en horarios nocturnos, un limite superior o sin limite según sea el caso.

Para obtener mas información y descarga:

http://www.microsoft.com/windowsserver2003/downloads/wsrm.mspx

# Capitulo 7
# Implementación y Configuración de IIS 6.0




***Durante este capítulo Usted irá asimilando conocimientos acerca de los servicios web, y al finalizar mismo tendrá la habilidad de:***

- Implementar Servicios Web
- Instalar IIS6
- Administrar un entorno de servicios Web

## 1. Introducción

Los Servicios de Microsoft Internet Information Server (IIS) 6.0 con Windows Server 2003 proporcionan capacidades de servidor Web integrado, confiable, escalable, seguro y administrable en una intranet, una extranet o en Internet. IIS 6.0 incorpora mejoras significativas en la arquitectura para cubrir las necesidades de los clientes alrededor del mundo.

### 1.1. Ventajas

IIS 6.0 y Windows Server 2003 introducen muchas características nuevas para la administración, disponibilidad, confiabilidad, seguridad, rendimiento y escalabilidad de los servidores de aplicaciones Web. IIS 6.0 también mejora el desarrollo de aplicaciones Web y la compatibilidad internacional. Juntos, IIS 6.0 y Windows Server 2003, proporcionan la solución para servidores Web más confiable, productiva, conectada e integrada.

| Ventaja | Descripción |
|---|---|
| ***Confiable y escalable*** | IIS 6.0 proporciona un entorno de servidor Web más inteligente y confiable para lograr la confiabilidad óptima. Este nuevo entorno incluye la supervisión del estado de las aplicaciones y el reciclaje automático de las mismas. Las características de confiabilidad aumentan la disponibilidad y acaban con el tiempo que los administradores dedican a reiniciar los servicios de Internet. IIS 6.0 está ajustado para proporcionar posibilidades de consolidación y escalabilidad optimizadas que sacan el máximo provecho de cada servidor Web. |
| ***Seguro y administrable*** | IIS 6.0 proporciona una seguridad y capacidad de administración significativamente mejoradas. Las mejoras de seguridad incluyen cambios tecnológicos y de procesamiento de solicitudes. Además, se ha mejorado la autenticación y la autorización. La instalación predeterminada de IIS 6.0 está completamente bloqueada, lo cual significa que la configuración se establece al máximo de seguridad de forma predeterminada. IIS 6.0 también proporciona capacidades de administración aumentadas, una administración mejorada con la metabase XML y nuevas herramientas de línea de comandos. |
| ***Desarrollo y compatibilidad internacional mejorados*** | Con Windows Server 2003 e IIS 6.0, los desarrolladores de aplicaciones se benefician con un único entorno de alojamiento de aplicaciones integrado, con una compatibilidad total con las características avanzadas y con la caché en modo de núcleo. Creado en IIS 6.0, Windows Server 2003 ofrece a los desarrolladores unos elevados niveles de funcionalidad adicional, incluyendo un desarrollo de aplicaciones rápido y una amplia selección de lenguajes. IIS 6.0 también ofrece compatibilidad internacional con los estándares Web más recientes. |

## 1.2. Mejoras y características nuevas

***Windows Server 2003 proporciona nuevas características y mejoras en tres áreas principales:***

- Confiabilidad y escalabilidad
- Seguridad y capacidad de administración
- Mejor desarrollo y compatibilidad internacional

### 1.2.1. Confiabilidad y escalabilidad

Windows Server 2003 proporciona las características siguientes para obtener una confiabilidad y una escalabilidad mejoradas.

| Característica | Descripción |
|---|---|
| ***Nueva arquitectura de procesamiento de solicitudes*** | Con la nueva arquitectura de procesamiento de solicitudes, IIS 6.0 detecta automáticamente las pérdidas de memoria, las infracciones de acceso y otros errores. Cuando se producen estas condiciones, la arquitectura subyacente proporciona una tolerancia a errores y la capacidad de reiniciar procesos cuando sea necesario. Mientras tanto, IIS 6.0 continúa poniendo las solicitudes en cola sin interrumpir la experiencia del usuario. |
| ***Detección de estado*** | IIS 6.0 es capaz de supervisar el estado de los procesos de trabajo, las aplicaciones y los sitios Web. Asimismo puede detectar el estado de los procesos de trabajo, como reciclar los procesos de trabajo en base a diversos factores, como el rendimiento, una planificación designada, el número de solicitudes y el consumo de memoria. También puede reciclar los procesos de trabajo bajo demanda. |
| ***Escalabilidad de los sitios*** | IIS 6.0 ha mejorado la forma en que el sistema operativo utiliza los recursos internos. Por ejemplo, IIS 6.0 no ubica previamente los recursos durante la inicialización. Se pueden alojar muchos más sitios en un único servidor que ejecute IIS 6.0 y un gran número de procesos de trabajo pueden estar activos de forma simultánea. El inicio y el cierre de un servidor son procesos más rápidos, en comparación con las versiones anteriores de IIS. Todas estas mejoras contribuyen a aumentar la escalabilidad de los sitios con IIS 6.0. |
| ***Nuevo controlador en modo de núcleo, HTTP.SYS*** | Windows Server 2003 introduce un nuevo controlador en modo de núcleo, HTTP.SYS, para el análisis y la caché de HTTP, proporcionando una escalabilidad y un rendimiento aumentados. IIS 6.0 se ha creado sobre HTTP.SYS y está ajustado específicamente para aumentar el rendimiento del servidor Web. Además, HTTP.SYS procesa directamente solicitudes en el núcleo, bajo determinadas circunstancias. |

### 1.2.2. new! Seguridad y capacidad de administración

Windows Server 2003 proporciona las características siguientes para obtener una seguridad y una escalabilidad mejoradas.

| Característica | Descripción |
|---|---|
| *Servidor bloqueado* | IIS 6.0 proporciona una seguridad significativamente mejorada. Para reducir la superficie de ataque de los sistemas, IIS 6.0 no se instala de forma predeterminada en Windows Server 2003; los administradores deben seleccionarlo e instalarlo de forma explícita. IIS 6.0 se entrega en un estado bloqueado y únicamente sirve el contenido estático. Mediante el uso del nodo de extensión de servicios Web, los administradores de sitios Web pueden habilitar o deshabilitar la funcionalidad de IIS en base a las necesidades individuales de la organización. |
| *Autorización* | IIS 6.0 extiende el uso de un nuevo marco de autorización que se proporciona con Windows Server 2003. Además, las aplicaciones Web pueden utilizar la autorización de direcciones URL, formando pareja con el Administrador de autorizaciones para controlar la obtención de acceso. La autorización delegada y restringida, proporciona ahora a los administradores de dominio, el control para delegar únicamente a servicios y equipos particulares. |
| *Metabase XML* | La metabase de texto de IIS 6.0, con formato XML, proporciona unas capacidades mejoradas de copia de seguridad y restauración para los servidores que experimentan errores críticos. También proporciona una recuperación de errores de la metabase y una solución de problemas mejorada. La modificación directa, mediante herramientas comunes de modificación de texto, proporciona la capacidad de administración mayor. |

### 1.2.3. new! Desarrollo y compatibilidad internacional mejorados

Windows Server 2003 proporciona las características siguientes para obtener un mejor desarrollo y compatibilidad internacional.

| Característica | Descripción |
|---|---|
| *Integración de IIS y ASP.NET* | Windows Server 2003 ofrece una experiencia mejorada para el desarrollador con la integración de IIS y Microsoft ASP.NET. Creadas a partir de IIS 6.0, las mejoras de Windows Server 2003 ofrecen a los desarrolladores unos elevados niveles de funcionalidad, como el desarrollo de aplicaciones rápido (RAD) y una amplia selección de lenguajes. En Windows Server 2003, la experiencia de utilizar ASP.NET y Microsoft .NET Framework se ha mejorado porque la arquitectura de procesamiento de solicitudes se integra con IIS 6.0. |
| *Información compartida a través de los límites geográficos* | La información compartida a través de los límites geográficos, en una gran variedad de idiomas, está ganado importancia en la economía global. En el pasado, la estructura no Unicode del protocolo HTTP limitaba a los desarrolladores al sistema de las páginas de códigos. Ahora, con las direcciones URL codificadas en UTF-8 (Formato de transformación de Unicode 8), el uso de Unicode ya es posible. Esta es una ventaja que proporciona la capacidad de admitir idiomas más complejos, como el chino. IIS 6.0 permite que los clientes obtengan acceso a las variables del servidor en Unicode. También agrega nuevas funciones de compatibilidad con el servidor que permiten a los desarrolladores obtener acceso a la representación en Unicode de una dirección URL, y con ello mejorar la compatibilidad internacional. |

Para obtener mas información:

http://www.microsoft.com/windowsserver2003/iis/default.mspx

## 2. IIS como servidor de aplicaciones

***El servidor de aplicaciones es un nuevo rol del servidor de productos Windows Server 2003, combinado con las siguientes tecnologías:***

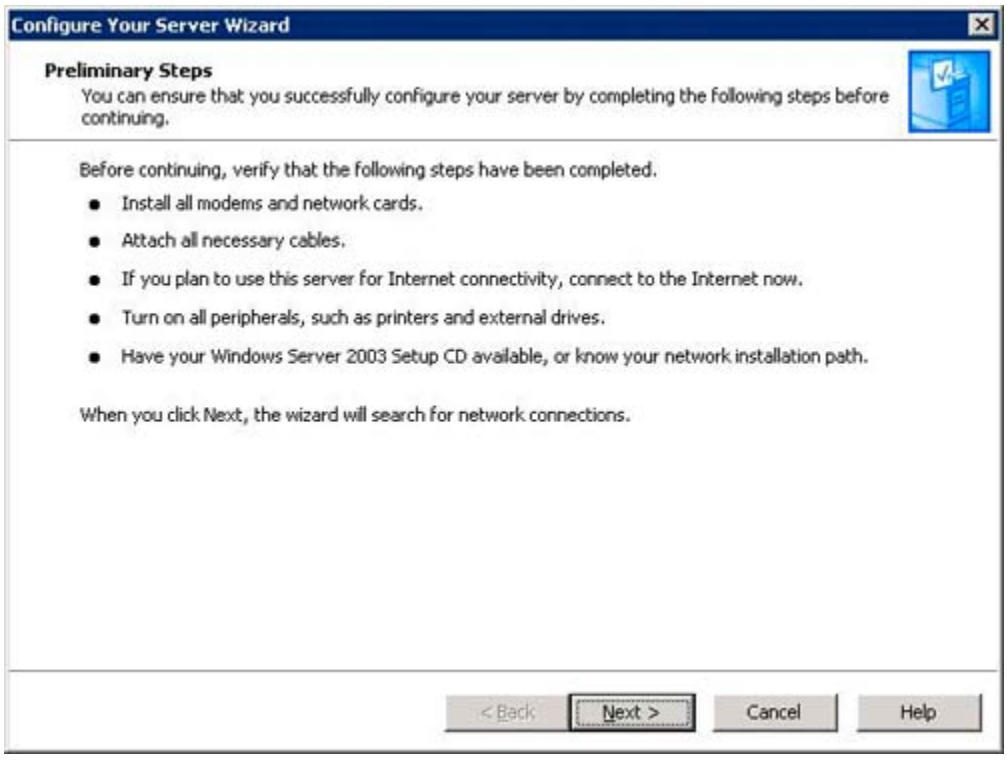
- Internet Information Services (IIS) 6.0
- Microsoft .NET Framework
- ASP.NET
- ASP
- UDDI Services
- COM+
- Microsoft Message Queuing (MSMQ)

El rol del servidor de aplicaciones combina estas tecnologías en una experiencia cohesiva, dando a los desarrolladores y administradores Web la habilidad de hospedar aplicaciones dinámicas, por ejemplo un aplicativo de base de datos Microsoft ASP.NET, sin la necesidad de instalar cualquier otro software en el servidor.

### Configuración del servidor de aplicaciones

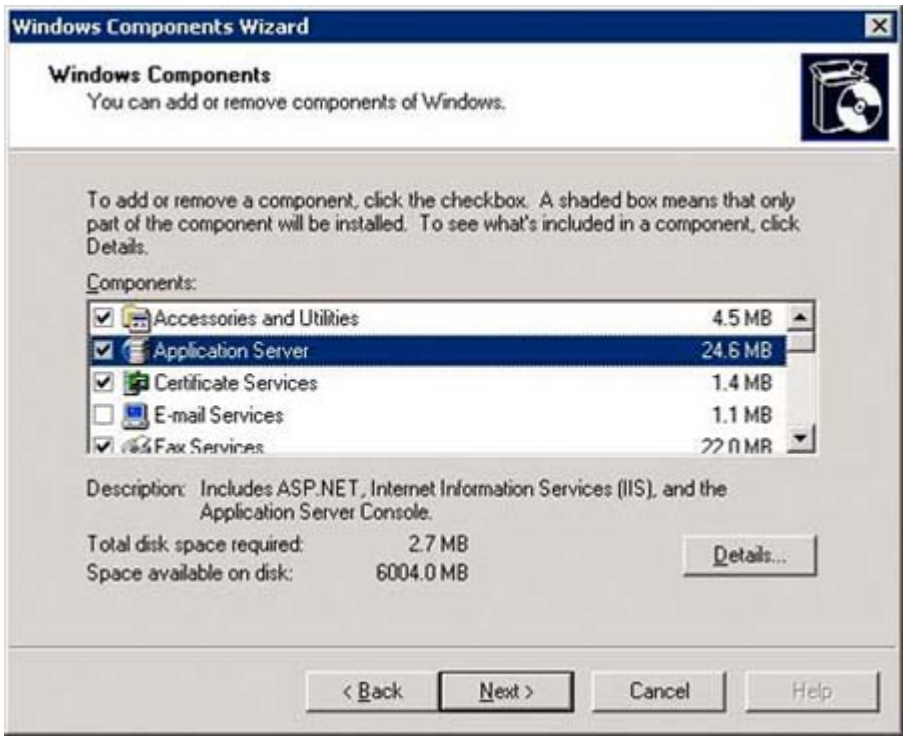
El servidor de aplicaciones es configurable en dos lugares de Windows Server 2003: en Configure Your Server wizard y en Add/Remove Components application.

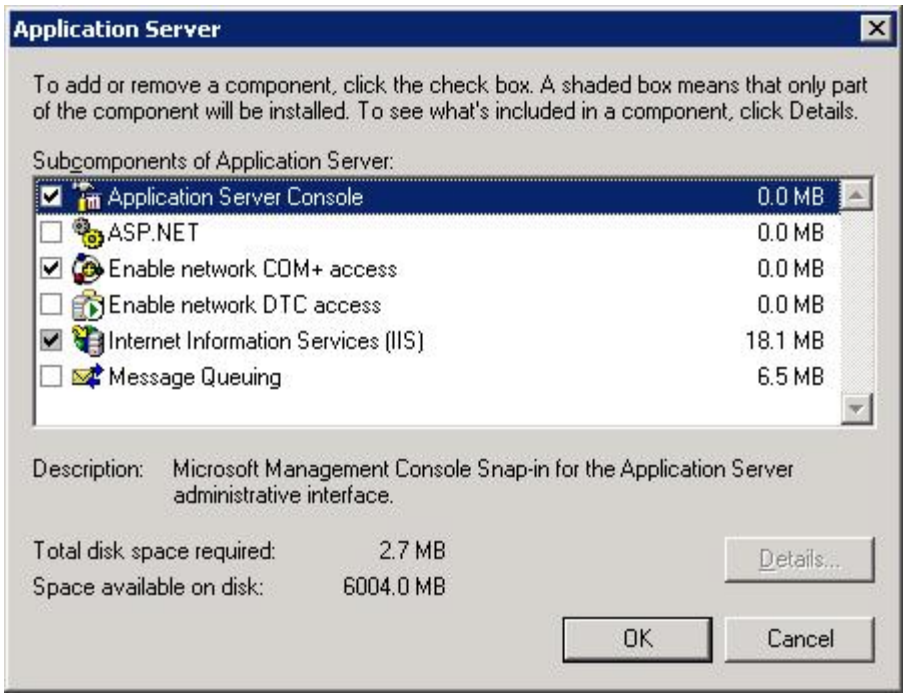
***Configure Your Server Wizard***

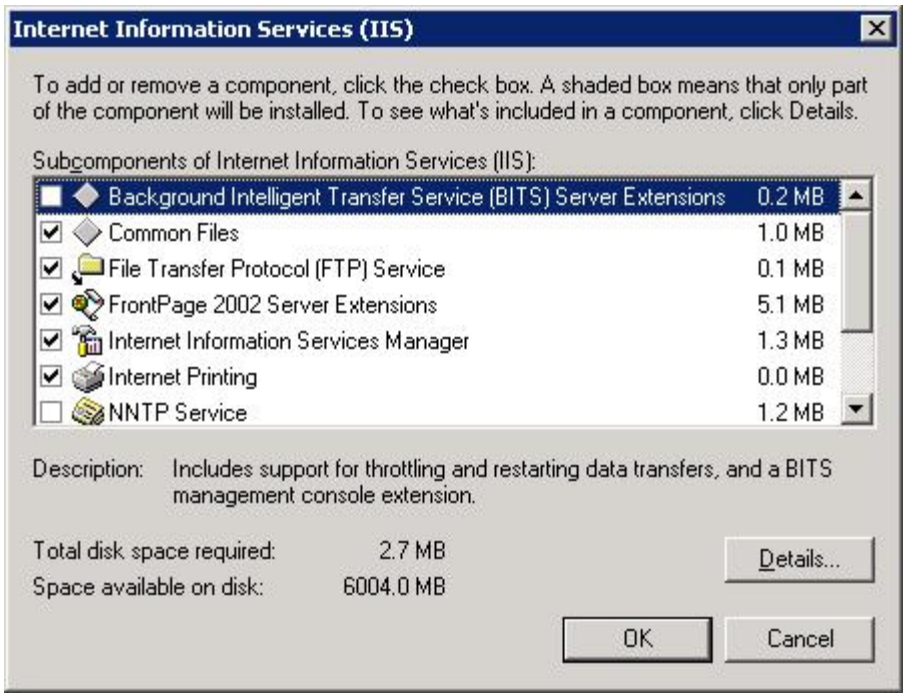



El Wizard Configure Your Server (CYS), es un punto central para configurar roles en Windows Server 2003, y ahora incluye el rol de servidor de aplicaciones. Para tener acceso al Wizard Configure Your Server, haga click en Add o Remove Roles del Wizard Manage Your Server. Este rol sustituye el rol existente del servidor Web. Después de instalar este nuevo rol, la página Manage Your Server, también incluirá una entrada para el nuevo rol.

*Add/Remove Components Application*






El servidor de aplicaciones también se incluye en Windows Server 2003 Add/Remove Components, como componente opcional top-level. Asimismo las aplicaciones del servidor que pertenecen al servidor de aplicaciones (IIS 6.0, ASP.NET, COM+, y MSMQ), pueden ser instaladas y configurar los componentes secundarios usando Add/Remove Components. Usando Add/Remove Components para configurar el servidor de aplicaciones, se obtiene un control mayor sobre los componentes secundarios específicos que serán instalados.

## 2.1. new! Arquitectura IIS 6.0 -Nueva arquitectura de procesamiento de Request

Los sitios Web y el código de aplicaciones están llegando a ser cada vez más complejos. Al mismo tiempo, los sitios dinámicos y los aplicativos Web pueden contener código imperfecto que se escape de la memoria o cause errores, como por ejemplo violaciones de acceso. Por lo tanto un servidor Web debe ser el encargado activo del ambiente runtime del aplicativo y automáticamente detectar y responder a los errores del aplicativo.

Cuando ocurre un error del aplicativo, el servidor necesitará ser fault-tolerant, significando que debe reciclar y recomenzar activamente el aplicativo culpable, mientras continúen haciendo cola las peticiones para el aplicativo, sin interrupción para el usuario. Es por ello que IIS 6.0 ofrece una nueva arquitectura fault-tolerant de procesamiento de request que ha sido diseñada para proporcionar este activo manejo del runtime y para alcanzar la confiabilidad y la escalabilidad dramáticamente crecientes, combinando un nuevo modelo de proceso aislado llamado Worker Process Isolation Mode. Este último posee grandes mejoras de funcionamiento, como por ejemplo Kernel Mode Queuing y Caching.

La versión anterior de IIS, IIS 5.0, fue diseñada para tener un proceso llamado Inetinfo.exe, que funcionaba como el proceso principal del servidor Web. En comparación, IIS 6.0 se ha rediseñado en dos nuevos componentes: el Kernel-Mode HTTP Protocol Stack (HTTP.sys) y el User-Mode Administration and Monitoring Component. Esta arquitectura permite que IIS 6.0 separe las operaciones del servidor Web de proceso del sitio Web y el código del aplicativo - sin sacrificar performance.

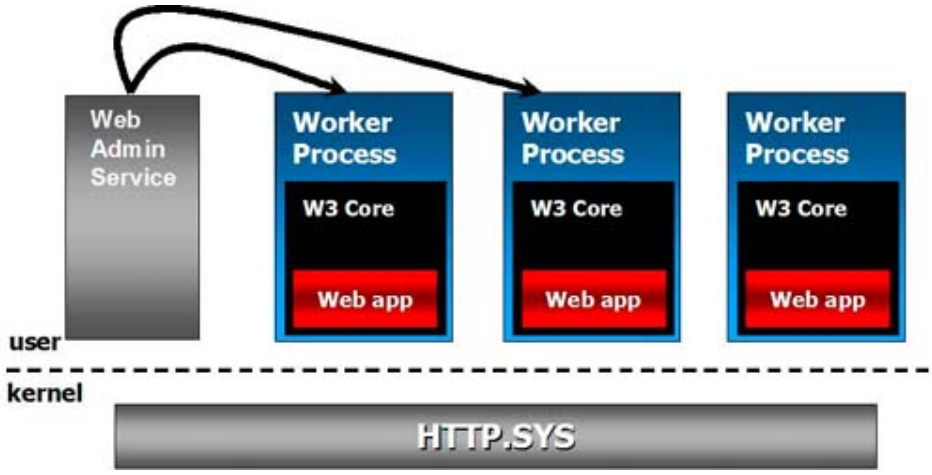
- new! ***HTTP.sys.*** El Kernel-Mode HTTP Protocol Stack, encola y parsea pedidos entrantes HTTP, y a la vez cachea y retorna el contenido del site y la aplicación. HTTP.sys no carga ningún código de aplicativo, simplemente parsea y rutea pedidos.

- new! ***WWW Service Administration and Monitoring Component.*** El User-Mode Configuration and Process Manager maneja operaciones del servidor y supervisa la ejecución del código del aplicativo. Como HTTP.sys, este componente no carga ni procesa ningún código de aplicativos.

Antes de discutir sobre estos componentes, es importante introducir dos nuevos conceptos de IIS 6.0: Application Pools y Worker Processes.

new! ***Los Application pools*** se utilizan para administrar Web sites y aplicaciones. Cada Application Pool corresponde a una cola de petición en HTTP.sys y al o los procesos de Windows que procesen estas peticiones. IIS 6.0 puede soportar hasta 2,000 Application Pools por servidor, y pueden haber múltiples Application Pools funcionando al mismo tiempo. Por ejemplo, un servidor departamental puede tener HR en un Application Pool y finance en otros Application Pool. Asimismo un Internet Service Provider (ISP) puede tener Web sites y aplicaciones de un cliente en un Application Pool, y Web sites de otro cliente en un Application Pool diferente. Application Pools se separan de otros por límites de proceso en Windows Server 2003. Por lo tanto, un aplicativo en un Application Pool no se afecta por aplicativos en otros Application Pools, y una petición del aplicativo no se puede rutear a otro Application Pool. Asimismo los aplicativos se pueden asignar fácilmente a otros Application Pool mientras que el servidor está funcionando.

new! ***Un Worker Process*** procesa pedidos de servicios de los sitios Web y aplicativos en un Application Pool. Todo el proceso de aplicativos Web, incluyendo la carga de ISAPI filters y extensiones, así como la autentificación y la autorización, es hecho por un nuevo WWW service DLL, el cual se carga en uno o más Worker Processes. El Worker Process ejecutable se llama W3wp.exe.




## 2.2. HTTP.sys

En IIS 6.0, HTTP.sys escucha peticiones y las encola apropiadamente. Cada cola de petición corresponde a un Application Pool. Dado que ningún código de aplicativo funciona en HTTP.sys, no puede ser afectado por faltas en código User-Mode, afectando normalmente el estado del Web Service. Si un aplicativo falla, HTTP.sys continúa aceptando y haciendo cola de nuevas peticiones en la cola apropiada hasta que uno de los siguientes eventos sucedan: el proceso se ha recomenzado y comienza a aceptar peticiones, no hay colas disponibles, no hay espacio en las colas o el servicio Web en sí mismo ha sido cerrado por el administrador. Puesto que HTTP.sys es un componente Kernel-Mode, la operación que hace es especialmente eficiente, permitiendo a la arquitectura de IIS 6.0 combinar el aislamiento de proceso con alto rendimiento al solicitar procesos.

Una vez que el servicio de WWW note el aplicativo fallado, comienza un nuevo Worker Process, si es que aún hay peticiones excepcionales que esperan para ser mantenidas en el Worker Process de un Application Pool.

Así, mientras puede haber una interrupción temporal en el proceso de la petición del User-Mode, un usuario no experimenta la falla porque las peticiones continúan siendo aceptadas y encoladas.

## 2.3. WWW Service Administration and Monitoring Component

El componente WWW Service Administration and Monitoring eleva una porción base del servicio WWW. Como HTTP.sys, ningún código del aplicativo funciona en el componente WWW Service Administration and Monitoring. Este componente tiene dos responsabilidades primarias: configuración de sistema y administración del Worker Process.

### Server Configuration

En el tiempo de la inicialización, la porción del Configuration Manager del servicio WWW utiliza la configuración en memoria de la metabase para inicializar la tabla de ruteo del Namespace de HTTP.sys. Cada entrada en la tabla de ruteo contiene la información que rutea las URLs entrantes al Application Pool que contiene el aplicativo asociado al URL. Estos pasos de pre-registro informan a HTTP.sys que hay un Application Pool para responder a las peticiones en una parte específica del Namespace, y ese HTTP.sys puede solicitar que un Worker Process se inicie para un Application Pool cuando llegue una petición.

## 2.4. Worker Process Management

En el rol de Worker Process Management, el componente WWW Service Administration and Monitoring es responsable de controlar el curso de vida del Worker Process que procesa las peticiones. Esto incluye la determinación de cuándo comenzar, reciclar o reiniciar un Worker Process, si es que no puede procesar más peticiones (se bloquea). Es también responsable de la supervisión de los Worker Processes y puede detectar cuando uno de ellos ha terminado inesperadamente.

## 2.5. Worker Process Isolation Mode

IIS 6.0 introduce un nuevo modo de aislamiento de aplicaciones para manejar el proceso de Web sites y aplicaciones: Worker Process Isolation Mode. Éste funciona en todo el código del aplicativo en un ambiente aislado. Los aplicativos se pueden aislar totalmente de uno a otro, donde un error del aplicativo no afecte a otro en un proceso diverso, usando Application Pools. Las peticiones se tiran directamente al Kernel en vez de tener un proceso User-Mode y rutear a otros procesos User-Mode. Primero, HTTP.sys rutea el sitio Web y las peticiones del aplicativo al correcto Application Pool. Luego, el Worker Processes que sirve al Application Pool envía los requests directamente a la cola del aplicativo en HTTP.sys. Este modelo elimina los saltos de proceso innecesarios encontrados al enviar una petición out-of-process DLLHost.exe (al igual que el caso en IIS 4.0 y 5.0), y aumenta la performance.

Worker Process Isolation Mode evita que un aplicativo o sitio pare otro. Además, separando aplicativos o sitios en Worker Processes separados, simplifica el número de tareas administrativas, por ejemplo, poner un site/application online o offline (independientemente de todos los otros site/applications corriendo en el sistema).

Para mas información acerca de IIS 6.0 con servidor de aplicaciones:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/iiswelcome.asp

## 3. Mejoras en la Seguridad

La seguridad ha sido siempre un aspecto importante de Internet Information Services. Sin embargo, en las versiones anteriores del producto (e.g. IIS 5.0 en Windows 2000 Server), el servidor no fue enviado en estado "locked down" por defecto. Muchos servicios innecesarios, por ejemplo Internet printing, estaban habilitados en la instalación.

Endurecer el sistema era un proceso manual y muchas organizaciones simplemente dejaron sus ajustes del servidor sin cambios. Esto condujo a una extensa vulnerabilidad al ataque, porque aunque cada servidor se podría hacer seguro, muchos administradores no realizaron lo que necesitaron o no tenían las herramientas para hacerlo.

Es por ello que Microsoft ha aumentado perceptiblemente su foco en seguridad desde el desarrollo de versiones anteriores de IIS. Por ejemplo, a principios de 2002 el trabajo de desarrollo de todos los ingenieros de Windows - más de 8.500 personas - fue puesto en asimiento mientras que la compañía condujo el entrenamiento intensivo de la seguridad. Una vez que el entrenamiento fuera terminado, los equipos de desarrollo analizaban la base del código de Windows, incluyendo HTTP.sys e IIS 6.0, para poner el nuevo conocimiento en ejecución. Esto representa una inversión sustancial para mejorar la seguridad de la plataforma de Windows. Además, durante la fase de diseño del producto, Microsoft condujo la amenaza extensa que modelaba para asegurarse que los desarrolladores del software de la compañía entendieran el tipo de ataques que el servidor pudo hacer frente en implementaciones del cliente. Asimismo los expertos de terceros han conducido las revisiones independientes de la seguridad del código.

### 3.1. new! Locked Down Server

Para reducir la superficie de ataque de la infraestructura Web, la instalación de Windows Server 2003 no instala IIS 6.0 por defecto. Los administradores deben seleccionar e instalar explícitamente IIS 6.0 en todos los productos Windows Server 2003, excepto en Windows Server 2003 Web Edition. Esto significa que ahora IIS 6.0 no tiene que ser desinstalado después que Windows haya sido instalado, si no que es necesario para el rol del servidor (por ejemplo si el servidor se instala para funcionar como a mail o database server). IIS 6.0 también será deshabilitado cuando un servidor sea migrado a Windows Server 2003, a menos que el IIS 5.0 Lockdown Tool esté instalado antes de la migración o se haya configurado una llave del registro. Además, IIS 6.0 es configurado por defecto en estado "locked down" cuando se instala. Después de la instalación, IIS 6.0 acepta solamente los pedidos de archivos estáticos hasta configurarlo para servir el contenido dinámico, y todos los time-outs y ajustes se fijan a los defectos agresivos de la seguridad. IIS 6.0 puede también ser deshabilitado usando Windows Server 2003 Group Policies.

### 3.2. new! Niveles múltiples de seguridad

La siguiente tabla resume los niveles múltiples de la seguridad disponible en IIS 6.0.

| Nivel de Seguridad de IIS 6.0 | Descripción |
|---|---|
| No instalado por defecto en Windows Server 2003 | Mucha seguridad está sobre la reducción de la superficie del ataque de su sistema. Por lo tanto, IIS 6.0 no es instalado por defecto en Windows Server 2003. Los administradores deben seleccionar e instalar explícitamente IIS 6.0. |
| Instala en estado locked down | La instalación por defecto de IIS 6.0 expone solamente funcionalidad mínima. Únicamente los archivos estáticos consiguen funcionalidad, mientras que otros (por ejemplo el ASP y ASP.NET) tendrán que ser permitidas explícitamente por el administrador. |
| Deshabilitación en upgrades | En Upgrades a Windows Server 2003 de servidores con IIS instalado, si el administrador no instaló y no corrió la herramienta Lockdown Tool o si configuró la llave del registro ***RetainW3SVCStatus*** en el servidor que es actualizado, entonces IIS 6.0 será instalado en estado deshabilitado. |
| Deshabilitación via | Con Windows Server 2003, los administradores del dominio pueden |

| | |
|---|---|
| Group Policy | prevenir a usuarios la instalación de IIS 6.0 en sus computadoras. |
| Cuenta de bajo privilegio IIS 6.0 | Worker Process corre en contexto low-privileged user por defecto. Esto reduce drásticamente el efecto de ataques potenciales. |
| ASP Seguro Todas las funciones | ASP built-in siempre corren con una cuenta low-privileged (anonymous user). |
| Extensiones de archivo reconocidas | Sirve solamente peticiones a los archivos que han reconocido extensiones de archivo y rechaza pedidos de extensiones no reconocidas. |
| Herramientas Command-line no accesibles a los usuarios Web | Los atacantes se aprovechan a menudo de herramientas command-line ejecutables vía Web server. En IIS 6.0, las herramientas command-line no pueden ser ejecutadas por el servidor Web. |
| Protección de escritura para el contenido | Una vez que los atacantes consiguen el acceso a un servidor, intentan desfigurar sitios Web. Para prevenir que usuarios anónimos Web sobrescriban el contenido del Web, éstos ataques pueden ser atenuados. |

## 3.3. new! Abriendo funcionalidad con IIS 6.0 Web Service Extensions

En un esfuerzo de reducir la superficie de ataque de su Web Server, IIS 6.0 sirve solamente el contenido estático después de una instalación por defecto. La funcionalidad programática proporcionada por Internet Server API (ISAPI) Extensions o Common Gateway Interfaces (CGI), debe ser habilitada manualmente por un administrador de IIS 6.0. ISAPI. CGI extenderá la funcionalidad de sus páginas Web, y por esta razón se referirá como Web Service Extensions. Por ejemplo, para correr Active Server Pages (ASP) en esta versión de IIS 6.0, el ISAPI pone ASP.DLL en ejecución, debiéndose habilitar específicamente como un Web Service Extension.

Usando las características de Web Service Extensions, los administradores del sitio Web pueden permitir o inhabilitar la funcionalidad de IIS 6.0 basada en las necesidades individuales de la organización. Esta funcionalidad global se hace cumplir a través del servidor entero.

## 3.4. new! Identidad configurable de Worker Process

Los aplicativos múltiples corriendo o los sitios en un servidor Web, ponen requisitos adicionales en el servidor. Si un ISP recibe a dos compañías en un servidor (que incluso pueden ser competidores), tiene que garantizar el funcionamiento de estos dos aplicativos aislados de uno. Principalmente, el ISP tiene que cerciorarse que un administrador malicioso para un aplicativo no pueda tener acceso a los datos del otro aplicativo. IIS 6.0 proporciona este nivel del aislamiento con la identidad configurable por Worker Process. Junto con otras características de aislamiento, como ancho de banda y uso de la CPU o reciclaje almacenado en la memoria, IIS 6.0 proporciona un ambiente a los aplicativos múltiples en un servidor para que se separen totalmente.

### 3.5. Mejoras SSL

***Hay tres mejoras principales en Secure Sockets Layer (SSL) de IIS 6.0. Estas son:***

- new! ***Performance.*** IIS 5.0 ya proporcionaba el más rápido software de implementación para SSL del mercado. Consecuentemente, el 50% de todos los sitios Web SSL corren en IIS 5.0. IIS 6.0 SSL es incluso más rápido. Microsoft ha mejorado la implementación de SSL para proveer más performance y escalabilidad.

- new! ***Remotable Certification Object.*** En IIS 5.0, los administradores no podían manejar certificados SSL remotamente porque el cryptographic service provider y certificate store no era remoto. Dado que los clientes manejan centenares o aún millares de servidores IIS con certificados SSL, necesitan una manera de manejar certificados remotamente. Es por eso que el CertObject ahora permite que los clientes realicen esto.

- new! ***Selectable CryptographicService Provider.*** Si se habilita SSL, la performance cae dramáticamente porque la CPU tiene que realizar muchas operaciones de criptografía intensiva. Sin embargo, ahora hay tarjetas aceleradoras basadas en hardware que permiten sacar los datos de estos cómputos criptográficos. Los Cryptographic Service Providers pueden entonces poner sus propios Crypto API providers en el sistema. Con IIS 6.0, es fácil seleccionar un Crypto API provider de terceras partes.

### 3.6. Autorización y autentificación

Si la autentificación contesta a la pregunta "¿Quién es usted?", entonces la autorización contestará a la pregunta "¿Qué puede usted hacer?". La autorización está para permitir o negar a un usuario que realice una cierta operación o tarea. Windows Server 2003 integra .NET Passport como mecanismo soportado para la autentificación de IIS 6.0. IIS 6.0 amplía el uso de un nuevo framework de autorización que viene con Windows Server 2003. Además, los aplicativos Web pueden utilizar la autorización del URL en tándem con Authorization Manager para controlar el acceso.

#### new! Integración de .NET Passport con IIS 6.0

La integración de .NET Passport con IIS 6.0 proporciona servicios de autentificación .NET Passport en el servidor Web base. .NET Passport 2.0 utiliza interfases de las aplicaciones proporcionadas por componentes estándares Passport, por ejemplo Secure Sockets Layer (SSL) Encryption, HTTP Redirects y cookies. Los administradores pueden poner sus sitios y aplicativos Web a disposición de la base .NET Passport entera, la cual abarca cerca de 150.000.000 usuarios, sin tener que ocuparse de la administración de cuentas públicas, por ejemplo la expiración o el aprovisionamiento de la contraseña.

Después que haya autenticado a un usuario, con el .NET Passport Unique ID (PUID) del usuario se podrá mapear a una cuenta en Microsoft Active Directory® - si tal aprovisionamiento se ha configurado para sus sitios Web. El token es creado por la Local Security Authority (LSA) para el usuario y el sistema de IIS 6.0 para la petición HTTP.

Para obtener mas información acerca de la seguridad en IIS 6.0:

http://www.microsoft.com/windowsserver2003/techinfo/overview/iisenhance.mspx

## 4. Práctica 1: Instalando IIS 6.0 en Windows Server 2003

Para poder realizar esta práctica Usted necesitará tener instalado Windows Server 2003.

***Para instalar IIS 6.0 en Windows Server 2003, deberá:***

1. Desde el control panel, hacer doble-click en ***Add/Remove Programs***.
2. Hacer click en ***Windows Components***.
3. Seleccionar ***Application Server***, y hacer click en ***Details***.
4. Seleccionar el cuadro ***Internet Information Services***.
5. Introducir el CD de Windows Server 2003, una vez que se le pida.
6. Realizar la comprobación, una vez finalizado el proceso de instalación.
7. Abrir el ***Internet Explorer***, y escribir **http://localhost**.
8. Verificar la aparición de la página de inicio de IIS 6.0.

Para obtener más información acerca de la instalación:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323384

http://support.microsoft.com/default.aspx?scid=kb;en-us;309506

# Capítulo 8
# Seguridad: Nuevas funcionalidades en Windows Server 2003

Durante este capítulo Usted irá asimilando conocimientos acerca de las mejoras de seguridad introducidas en Windows Server 2003.

***Al finalizar este capítulo podrá:***

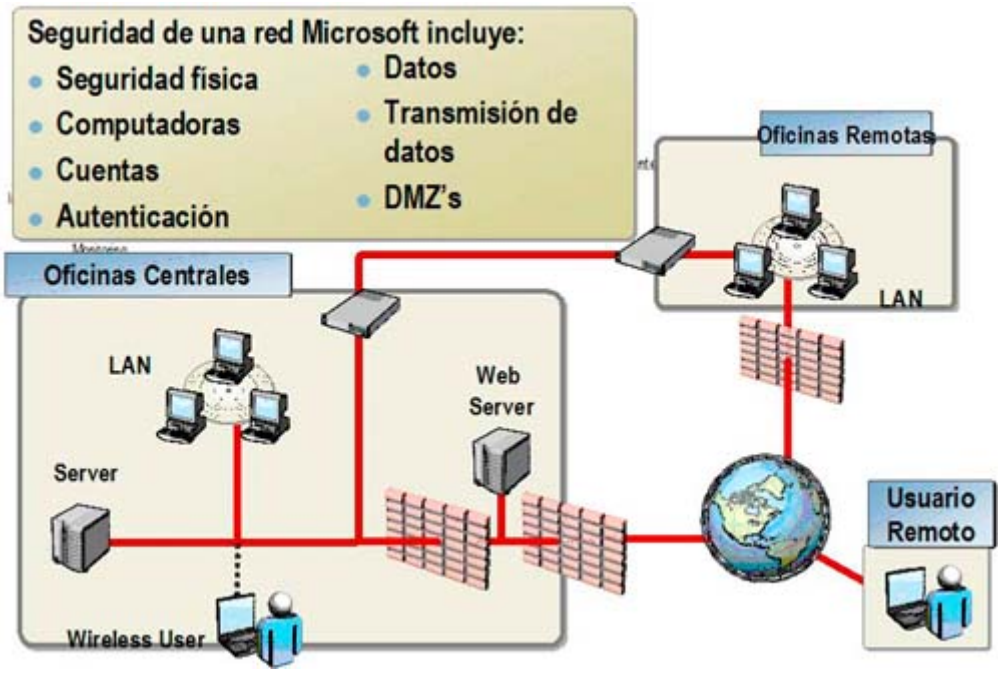
- Describir las funcionalidades de seguridad
- Implementar y verificar las funcionalidades de seguridad

**Nota:** Dada la cantidad de información acerca de temas referentes a seguridad y tratándose este capítulo de un resumen de las nuevas funcionalidades, sugerimos repasar los conocimientos adquiridos en Windows 2000, como así también las publicaciones de Technet.

Si Usted desea recibir el boletín de seguridad Microsoft, suscríbase al mismo mediante esta dirección, que además de ser gratuito, le será de mucha utilidad en sus tareas diarias.

http://register.microsoft.com/subscription/subscribeme.asp?id=166

## 1. Introducción




Las empresas han ampliado sus redes tradicionales de área local (LAN) mediante la combinación de sitios de Internet, intranets y extranets. Como resultado, una mayor seguridad de los sistemas resulta ahora más importante que nunca. Para proporcionar un entorno informático seguro, el sistema operativo Windows Server 2003 aporta muchas características nuevas e importantes de seguridad sobre aquellas incluidas originalmente en Windows 2000 Server.

### 1.1. Informática de confianza

Los virus existen y por ello que la seguridad del software es un reto constante. Para hacer frente a éstos, Microsoft ha convertido la informática de confianza en una iniciativa clave para todos sus productos. La informática de confianza es un marco para desarrollar dispositivos basados en equipos y software seguros y confiables, como los dispositivos y aparatos domésticos que utilizamos diariamente. Aunque en la actualidad no exista ninguna plataforma de informática de confianza, el nuevo diseño básico de Windows Server 2003 es un paso sólido hacia la conversión de este concepto en realidad.

### 1.2. Lenguaje común en tiempo de ejecución

El motor de software del lenguaje común en tiempo de ejecución es un elemento clave de Windows Server 2003 que mejora la confiabilidad y facilita un entorno informático seguro. Asimismo reduce el número de errores y los agujeros de seguridad causados por errores comunes de programación, posibilitando que existan menos vulnerabilidades que los atacantes puedan explotar.

El lenguaje común en tiempo de ejecución verifica que las aplicaciones puedan realizarse sin errores, y a la vez comprueba los permisos de seguridad adecuados, asegurando que el código realice exclusivamente las operaciones correctas. Esto se lleva a cabo comprobando aspectos como los siguientes: la ubicación desde la cual se ha descargado o instalado el código, si el código tiene una firma digital de un desarrollador de confianza, y si el código ha sido alterado desde su firma digital.

### 1.3. Ventajas

Windows Server 2003 proporcionará una plataforma más segura y económica para la realización de actividades empresariales.

| Ventaja | Descripción |
|---|---|
| ***Disminución de costos*** | Esto conlleva procesos de administración de seguridad simplificados, como las listas de control de acceso y el Administrador de credenciales. |
| ***Implementación de estándares abiertos*** | El protocolo IEEE 802.1X facilita la seguridad de las LAN inalámbricas ante el peligro de espionaje dentro del entorno empresarial. |
| ***Protección para equipos móviles y otros dispositivos nuevos*** | Las características de seguridad como el Sistema de archivos de cifrado (EFS), los servicios de certificado y la inscripción automática de tarjetas inteligentes, facilitan la seguridad de una amplia gama de dispositivos. El EFS es la tecnología básica para cifrar y descifrar archivos almacenados en volúmenes NTFS. Únicamente el usuario que cifra un archivo protegido puede abrirlo y trabajar con él. Los servicios de certificado son una parte del sistema operativo básico que permite que una empresa actúe como si fuera una entidad emisora de certificados (CA) y emita y administre certificados digitales. La inscripción automática de tarjetas inteligentes y las características de entidad de registro automático proporcionan seguridad a los usuarios empresariales, agregando otro nivel de autenticación. Esto se realiza de forma adicional a los procesos de seguridad simplificada, en organizaciones preocupadas por su seguridad. |

### 1.4. Mejoras y características nuevas

***La familia de Windows Server 2003 proporciona las siguientes características:***

- Una plataforma más segura para realizar actividades empresariales
- La mejor plataforma para la infraestructura de claves públicas
- Una extensión segura de sus actividades empresariales en Internet

***Una plataforma más segura para llevar a cabo actividades empresariales***

Windows Server 2003 proporciona muchas características nuevas y mejoradas que se combinan para crear una plataforma más segura para llevar a cabo actividades empresariales.

| Característica | Descripción |
|---|---|
| ***Servidor de seguridad de conexión a Internet*** | Windows Server 2003 proporciona seguridad de Internet mediante el uso de un servidor de seguridad basado en software, llamado Servidor de seguridad de conexión a Internet (ICF). El ICF proporciona protección a los equipos conectados directamente a Internet o a los equipos ubicados detrás de un equipo host de conexión compartida a Internet (ICS) y que ejecute un ICF. |
| ***Servidor IAS/RADIUS seguro*** | El Servidor de autenticación de Internet (IAS) es un Servidor de usuario de acceso telefónico de autenticación remota (RADIUS) que administra la autorización y la autenticación del usuario. También administra conexiones con la red mediante el uso de diversas tecnologías de conectividad, como el acceso telefónico, las redes privadas virtuales (VPN) y los servidores de seguridad. |
| ***Redes LAN Ethernet e inalámbricas seguras*** | Windows Server 2003 permite la autenticación y la autorización de usuarios y equipos que se conectan a redes LAN Ethernet e inalámbricas. Esto es posible por la compatibilidad de Windows Server 2003 con los protocolos IEEE 802.1X. (Los estándares IEEE 802 definen métodos para obtener acceso a redes LAN y controlarlas.) |
| ***Directivas de restricción de software*** | Windows Server 2003 permitirá que un administrador de sistemas utilice la exigencia de directivas o ejecución para prevenir que se lleven a cabo en un equipo programas ejecutables. Por ejemplo, aplicaciones específicas de ámbito corporativo pueden ver su ejecución restringida a menos que se ejecuten desde un directorio específico. Las directivas de restricción de software también pueden configurarse para prevenir la ejecución de código mal intencionado o infectado por virus. |
| ***Mejoras de la seguridad para servidores en redes LAN Ethernet e inalámbricas*** | Windows Server 2003 proporciona seguridad para redes LAN Ethernet e inalámbricas basadas en las especificaciones IEEE 802.11 y que sean compatibles con certificados públicos implementados mediante la inscripción automática o las tarjetas inteligentes. Estas mejoras en la seguridad permiten el control de la obtención de acceso a redes Ethernet en lugares públicos, como centros comerciales o aeropuertos. La autenticación de equipos también se admite en un entorno operativo de protocolo de autenticación extensible (EAP). |
| ***Seguridad aumentada para servidores Web*** | La seguridad de la información es un problema de vital importancia para las organizaciones de todo el mundo. Para aumentar la seguridad de los servidores Web, los Servicios de Internet Information Server 6.0 (IIS 6.0) se configuran para obtener la máxima seguridad. Su instalación predeterminada es el estado "bloqueado". Las características de seguridad avanzada de IIS 6.0 incluyen: servicios criptográficos que se pueden seleccionar, autenticación de síntesis avanzada y control configurable de la obtención de acceso a los procesos. Estas son sólo algunas de las tantas características de seguridad que le permitirán realizar negocios de forma segura en la Web. |
| ***Cifrado de la base de datos de archivos sin conexión*** | La opción para cifrar la base de datos de archivos sin conexión, ahora se encuentra disponible. Esto es una mejora sobre Windows 2000, donde los archivos de la caché no podían cifrarse. Esta característica es compatible con el cifrado y descifrado de toda la base de datos sin conexión. Se requieren privilegios administrativos para configurar la forma en que se cifrarán los archivos sin conexión. |
| ***Compatible con FIPS, modo de núcleo, módulo criptográfico*** | Este módulo criptográfico se ejecuta como un controlador en modo de núcleo e implementa algoritmos criptográficos aprobados por el Estándar Federal de Procesamiento de Información (FIPS). Entre estos algoritmos cabe incluir: SHA-1, DES, 3DES y un generador de número aleatorio aprobado. El módulo criptográfico, compatible con FIPS de modo de núcleo, permite que las organizaciones gubernamentales implementen Seguridad de Protocolo |

| | |
|---|---|
| | Internet (IPSec) compatible con FIPS 140-1. Para ello deberán utilizar:<br>• Servidor y cliente de VPN L2TP (Protocolo de túnel de capa 2)/IPSec.<br>• Túneles L2TP/IPSec para conexiones VPN entre puertas de enlace.<br>• Túneles IPSec para conexiones VPN entre puertas de enlace.<br>• Tráfico de red de extremo a extremo, cifrado mediante IPSec, entre cliente y servidor, y de servidor a servidor. |
| ***Nuevo paquete de seguridad de síntesis*** | El nuevo paquete de seguridad de síntesis es compatible con el protocolo de autenticación de síntesis, junto con RFC 2617 y RFC 2222. Estos protocolos son compatibles con Microsoft Internet Information Server (IIS) y el servicio Active Directory®.<br>Mejoras en la seguridad de los sistemas Se han realizado importantes mejoras para garantizar una seguridad general de los sistemas, incluyendo:<br>• Mejoras del rendimiento en un 35 por ciento, al utilizar la capa de sockets segura (SSL).<br>• IIS no se instala de forma predeterminada. Para implementar IIS, primero debe instalarsemediante la opción Agregar o quitar programas del Panel de control. Capacidad de comprobación del búfer de Microsoft Visual Studio®. (Los piratas informáticos utilizan habitualmente las saturaciones del búfer para explotar un sistema.) |
| ***Administrador de credenciales*** | El administrador de credenciales de Windows Server 2003 proporcionará un almacén seguro para las credenciales del usuario, incluyendo contraseñas y certificados X.509. Estas credenciales proporcionan una experiencia sólida de inicios de sesión únicos para los usuarios, incluidos los usuarios móviles. Una API de Win32® se encuentra disponible para permitir que las aplicaciones basadas en cliente o en servidor obtengan credenciales del usuario. |
| ***Mejoras en la autenticación de clientes SSL*** | En Windows Server 2003, la caché de sesión SSL puede compartirse mediante múltiples procesos. Esto reduce el número de veces que un usuario tiene que volver a autenticarse en las aplicaciones, y asimismo reduce los ciclos de CPU en el servidor de aplicaciones. |

### *La mejor plataforma para la infraestructura de claves públicas*

Windows Server 2003 facilitará la implementación de una infraestructura de claves públicas, junto con tecnologías asociadas como las tarjetas inteligentes.

| Característica | Descripción |
|---|---|
| *Renovación automática e inscripción automática de certificados* | Estas nuevas características importantes reducen de forma drástica la cantidad de recursos necesarios para administrar certificados X.509. Windows Server 2003 posibilita la inscripción e implementación automática de certificados para los usuarios. Asimismo cuando el certificado caduque, podrá renovarse en forma automática. La renovación automática e inscripción automática de certificados facilita la implementación más rápida de tarjetas inteligentes y mejora la seguridad de las conexiones inalámbricas (IEEE 802.1X) mediante la caducidad y renovación automática de certificados. |
| *Compatibilidad de Windows Installer con la firma digital* | La compatibilidad con la firma digital permite que los paquetes y contenedores externos de Windows Installer se firmen digitalmente. Esto proporciona a los administradores de tecnologías de la información, unos paquetes de Windows Installer más seguros, resultando de suma importancia si el paquete se envía a través de Internet. |
| *Mejoras en las listas de revocación de certificados (CRL)* | El servidor de certificados incluido en Windows Server 2003 ahora es compatible con las CRL delta. Una CRL hace que la publicación de certificados X.509 revocados sea más eficaz, y facilita que un usuario pueda recuperar un certificado nuevo. Y como ahora se puede especificar la ubicación en la cual se encuentra almacenada la CRL, resulta más fácil moverla para albergar las necesidades de seguridad y empresariales específicas. |

### *Extensión segura de las actividades empresariales en Internet*

Una empresa necesita establecer una forma segura de comunicarse con sus empleados, clientes y asociados que no se encuentren dentro de su intranet. Windows Server 2003 facilitará este aspecto, ampliando de forma segura la obtención de acceso a la red para personas y otras empresas que necesitan trabajar con datos o recursos del usuario.

| Característica | Descripción |
|---|---|
| *Integración con Passport* | Puede asignarse una identidad de Passport a una identidad de Active Directory en Windows Server 2003. Por ejemplo, la asociación de una identidad de Passport con una identidad de Active Directory permite que una empresa asociada pueda ser autorizada para obtener acceso a los recursos a través de IIS, en lugar de tener que iniciar sesión directamente en una red de Windows. La integración con Passport proporcionará una experiencia de inicio de sesión única, mediante el uso de IIS. |
| *Relaciones de confianza entre bosques* | Si trabaja con un asociado o una empresa que ha implementado un bosque de Active Directory, puede utilizar Windows Server 2003 para configurar una relación de confianza entre los bosques del asociado o la empresa y sus propios bosques. Esto le permite confiar de forma explícita en algunos usuarios, en grupos o en todos, los que pertenezcan a otro bosque. También tiene la capacidad de establecer permisos en base a los usuarios o grupos que residen en el otro bosque. Las relaciones de confianza entre bosques facilitan la dirección de negocios con otras empresas mediante Active Directory. |

## 2. Personal Firewall (ICF)


El Internet Connection Firewall (ICF) es una nueva característica en Windows Server 2003, que le permite proteger su conexión a Internet. Utilizando esta herramienta Usted puede determinar qué servicios estarán disponibles desde Internet hacia el Servidor corriendo Windows Server 2003 y qué servicios estarán disponibles desde su servidor hacia Internet. Esta nueva característica le permite proteger sus conexiones, ya sean las que utilizan adaptadores de red como así también las que utilizan conexiones telefónicas.

**Nota:** Usted puede utilizar ICF para proteger conexiones exclusivamente en el servidor corriendo Windows Server 2003. Si necesitase habilitar acceso a Internet seguro para clientes internos deberá analizar una implementación de Internet Security and Acceleration Server 2000 (ISA Server).

***Para obtener mas información acerca de ICF:***

http://support.microsoft.com/default.aspx?scid=kb;en-us;317530

### 2.1. Práctica 1: Habilitando ICF

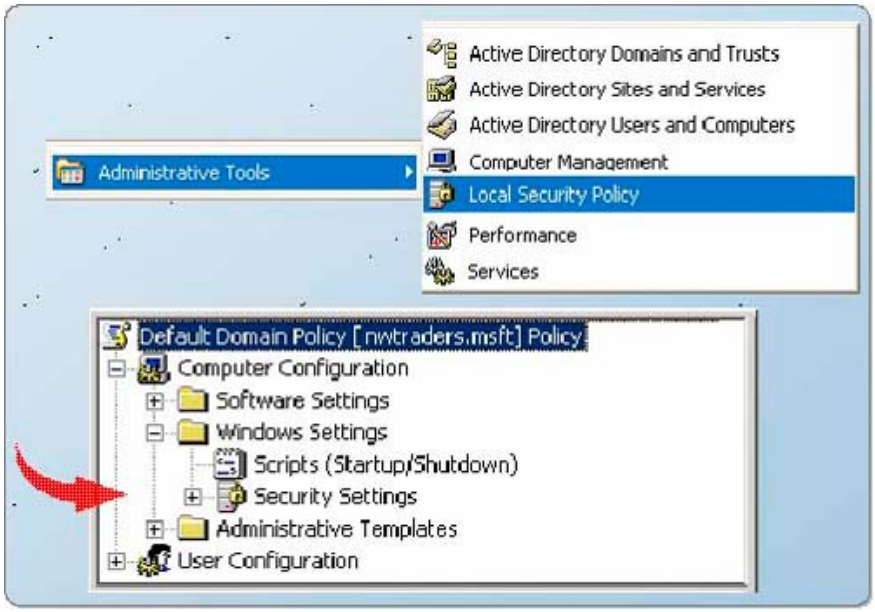
***Para realizar esta práctica Usted deberá tener dos instalaciones de Windows Server 2003.***

1. Desde el menú ***Start***, hacer click en ***Network Connections***.
2. Seleccionar el adaptador de red, hacer click derecho y después hacer click en ***Properties***.
3. Hacer click en la lengüeta ***Advanced***.
4. Marcar el cuadro ***Internet Connection Firewall***.
5. Hacer click en ***OK***.

***Para comprobar la configuración:***

- Desde la computadora B, intentar una conexión del tipo **\\nombredeserver**
- Verificar si la conexión pudo realizarse.

## 3. Usando Security Templates para asegurar Computadoras




Usted puede usar Security Templates para crear y alterar Security Policies que cumplan con las necesidades de su compañía. Security Policies se puede implementar de diferentes maneras. El método que Usted usará dependerá del tamaño y las necesidades de seguridad de la organización. De esta manera, llas organizaciones pequeñas, que no poseen una implementación de Active Directory, tendrán que configurar la seguridad manualmente, mientras que las organizaciones grandes requerirán niveles de seguridad altos. Para ello Usted puede considerar el uso de Group Policy Objects (GPOS) para instalar políticas de seguridad.

### 3.1. ¿Qué es un Security Policy?

Los Security Policies son una combinación de configuraciones de seguridad que afectan la seguridad de una computadora. Usted puede usar Security Policy para establecer: Account Policies y Local Policies en la computadora local y en Active Directory.

Los siguientes Security Templates son una colección de configuraciones de seguridad predeterminadas. Usted puede usar el Security Templates Snap-in para modificar los Templates predefinidos o crear nuevos Templates que cumplan con sus necesidades. Luego, en la creación o modificación, se podrán utilizar las siguientes herramientas para aplicar las configuraciones de seguridad: Security Configuration and Analysis Snap-in, la herramienta de línea de comando Secedit o Local Security Policy / Group Policy para importar y exportar Security Templates.

**Windows Server 2003 provee los siguientes Templates predefinidos:**

***Default Security (Setup Security.inf)***

Este Template es creado durante la instalación del sistema operativo y representa la configuración básica aplicada durante la instalación, incluyendo permisos de archivos para el Root del System Drive.

### *Domain Controller Security (DC security.inf)*

Este Template es creado cuando un Server es promovido a Domain Controller. Contiene configuraciones de seguridad necesarias sobre archivos, registry y servicios. Usted puede aplicar este Template usando Security Configuration and Analysis Snap-in o con la herramienta Secedit.

### *Compatible (Compatws.inf)*

Este Template aplica configuraciones de seguridad necesarias para todas aquellas aplicaciones que no estén certificadas por el Windows Logo Program.

### *Secure (Secure*.inf)*

Este Template aplica configuraciones de seguridad con alto nivel, afectando la compatibilidad de aplicaciones. Por ejemplo, Stronger Password, Lockout, y configuraciones de auditoria.

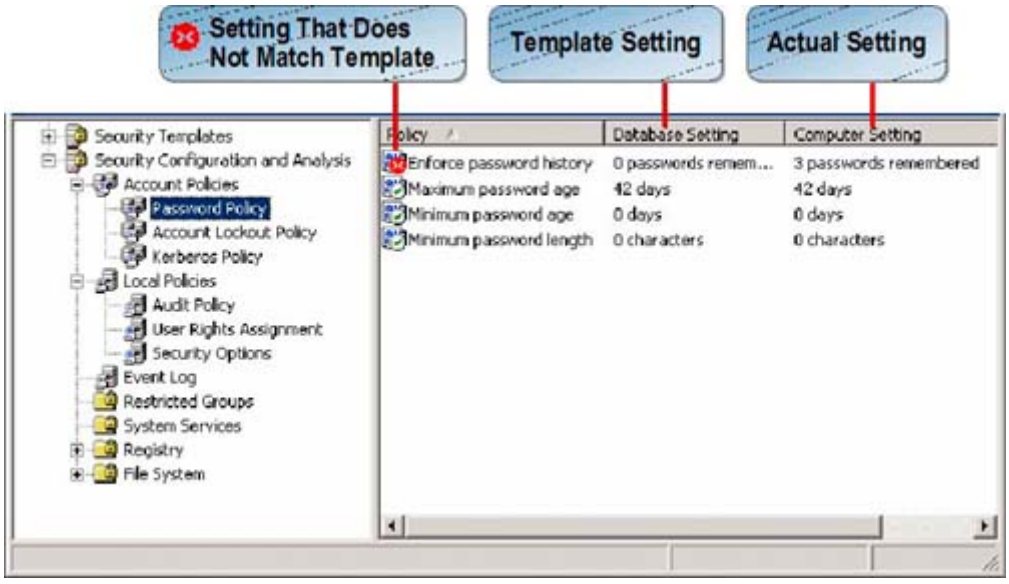
### *Highly Secure (Hicec*.inf)*

Este Template aplica las configuraciones de seguridad más elevadas posibles. Para ello impone restricciones sobre los niveles de encripción y el firmado de paquetes de datos sobre canales seguros y entre clientes y servidores sobre los paquetes Server Message Block (SMB).

Para más información acerca de ***secedit***

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/secedit_cmds.asp?frame=true

## 3.2. ¿Qué es la herramienta Security Configuration and Analysis?




La herramienta Security Configuration and Analysis compara la configuración de seguridad entre la computadora local a una configuración alterna que es importada del template (archivo .inf ) y la almacenada en una base de datos separada (archivo .sdb). Cuando el análisis se completa, Usted puede analizar los ajustes de la seguridad en árbol de la consola para ver los resultados. Las discrepancias están marcadas con una bandera roja, las consistencias están marcadas con una marca verde y los ajustes que no están marcados con una bandera roja o una marca verde, no se configuran en la base de datos.

***Después de analizar los resultados usando la herramienta Security Configuration and Analysis, Usted puede realizar varias tareas, incluyendo:***

- Eliminar las discrepancias configurando los ajustes en la base de datos a los ajustes actuales de la computadora. Para configurar ajustes de la base de datos, haga doble-click en la configuración del panel de detalles.

- Importar otro template, combinando sus ajustes y sobrescribiendo ajustes donde hay un conflicto. Para importar otro template, haga click derecho en ***Security Configuration and Analysis***, y después haga click en ***Import Template***.

- Exportar los ajustes actuales de la base de datos a un template. Para exportar otro template, haga click derecho en ***Security Configuration and Analysis***, y después haga click en ***Export Template***.

***Para mas información acerca de Security Tools:***

***Security Configuration Manager:***

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/SEconcepts_SCM.asp

**Best Practices for Security Configuration and Analysis.**

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SCMbp.asp

***Informacion adicional sobre seguridad:***

**Introducción Técnica a seguridad.**

http://www.microsoft.com/windowsserver2003/techinfo/overview/security.mspx

**Guía de seguridad en Windows Server 2003.**

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2003/W2003HG/SGCH00.asp

**IPsec en Windows Server 2003.**

http://support.microsoft.com/default.aspx?scid=kb;en-us;323342

http://support.microsoft.com/default.aspx?scid=kb;en-us;324269

**Public Key Encryption**

http://support.microsoft.com/default.aspx?scid=kb;en-us;281557

http://support.microsoft.com/default.aspx?scid=kb;en-us;290760