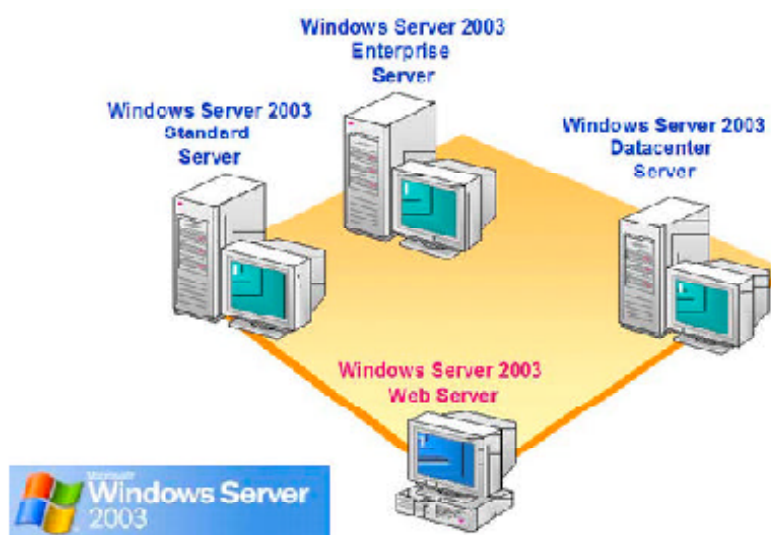




Universidad Nacional del Nordeste
Facultad de Ciencias Exactas, Naturales y Agrimensura

MONOGRAFIA

WINDOWS 2003 SERVER



Maria de los Angeles Ibarra - L.U.: 30505

Director: Mgter. David Luis la Red Martínez

Licenciatura en Sistemas de Información
Corrientes - Argentina

2003

Índice General

1	Introducción a Windows Server 2003	1
1.1	Nuevas Características	2
1.1.1	Automated System Recovery	2
1.1.2	Snapshot Infraestructura (Replica from Media DS)	2
1.1.3	Volume Shadow Copy	3
1.1.4	Encrypted File System (EFS)	3
1.1.5	Driver Rollback	3
1.1.6	Active Directory	3
1.1.7	Reboot Reason Collector “Event Tracker”	5
1.1.8	“Remote Installation Services” RIS	5
1.1.9	IIS 6.0 - Internet Information Services 6.0	5
1.1.10	Versiones	7
1.1.11	Requerimientos	7
1.2	Funcionalidades	9
1.2.1	Domain controller (Active Directory)	9
1.2.2	File Server	9
1.2.3	Print Server	9
1.2.4	DNS Server	10
1.2.5	Application Server	10
1.2.6	Terminal Server	10
1.2.7	La Herramienta Manage Your Server	11
2	Instalación y Migración	12
2.1	introducción a la Instalación de Windows Server 2003	12
2.2	Seleccionando File System	13
2.2.1	NTFS	13
2.2.2	FAT y FAT32	13
2.3	Modelo de Licenciamiento	14
2.4	Determinación de Pertenencia a Workgroup o Dominio	15

2.4.1	Dominio	15
2.4.2	Workgroup	16
2.5	Instalando desde Compact Disc	16
2.5.1	Funcionamiento del Programa de Instalación	17
2.5.2	Iniciando el Wizard de Instalación de Windows Server 2003	17
2.5.3	Instalación de Componentes para Networking	19
2.5.4	Fin de la Instalación	19
2.6	Instalando desde la Red	19
2.7	Usando Remote Instalation Services (RIS)	20
2.8	Usando System Preparation Tool (sysprep)	22
2.9	Migración desde Windows NT 4.0	23
2.9.1	Migración de Member Servers	23
2.9.2	Migración de Dominios	24
2.10	Migración desde Windows 2000	25
2.10.1	Migración de Member Servers Windows 2000	25
2.10.2	Migración de Dominios	26
3	Instalación y Configuración	28
3.1	DHCP - Dynamic Host Configuration Protocol	28
3.1.1	Direccionamiento de Direcciones IP mediante DHCP	29
3.1.2	Funcionamiento del Proceso DHCP Lease Generation	30
3.1.3	Funcionamiento del Proceso DHCP Lease Renewal	31
3.1.4	Stand-alone DHCP Server	33
3.1.5	Los DHCP Scopes	34
3.1.6	Las opciones de DHCP	35
3.1.7	DHCP Relay Agent	35
3.2	Descripción de Domain Name System	37
3.2.1	Domain Namespace	37
3.2.2	Query DNS	38
3.2.3	Funcionamiento del Caching de DNS Server	39
3.2.4	Mantenimiento y Almacenamiento de los Datos DNS	39
3.2.5	Resource Records y Record Types	41
3.2.6	Creación de Zonas de Búsqueda Estándar	42
3.2.7	Configuración de Zonas Estándar	43
3.2.8	Proceso de transferencia de zona	44
3.2.9	Introducción a las actualizaciones dinámicas	45
3.3	Descripción de WINS	47
3.3.1	Estudio de los Registros de la Base de Datos WINS	48

3.3.2	Estudio de la Información de Registro de WINS	48
3.3.3	Replicación de WINS	49
3.3.4	Funcionamiento de la Replicación Push	50
3.3.5	Funcionamiento de la Replicación Pull	50
3.3.6	Mantenimiento	50
3.3.7	Procesos de Resolución de Nombres e Integración WINS / DNS	51
3.3.8	Resolución de Nombres NetBIOS	52
3.3.9	Introducción a la Integración WINS y DNS	53
4	Active Directory Service	54
4.1	Introducción a Active Directory Services	54
4.1.1	La Funcionalidad	55
4.1.2	Estructura Lógica de Active Directory	55
4.1.3	Estructura Física de Active Directory	57
4.1.4	Los Operations Masters	58
4.1.5	Transferencia de Operations Master Roles	60
4.2	Servicio de Directorio	60
4.2.1	Capacidades de Active Directory	61
4.2.2	El Schema	61
4.2.3	El Global Catalog	62
4.2.4	Los Distinguished y Relative Distinguished Names	63
4.2.5	Active Directory Snap-ins y Herramientas	64
4.3	Instalación de Active Directory	65
4.3.1	Requisitos para Instalar Active Directory	65
4.3.2	El Proceso de Instalación de Active Directory	66
4.3.3	Renombrar un Domain Controller	68
4.4	Las zonas DNS Active Directory Integrated	69
4.4.1	Zonas Active Directory Integrated	69
4.4.2	Funcionalidad de Forest y Domain	70
4.4.3	Habilitación de nuevas características en Windows Server 2003	71
4.5	Funcionamiento de los Trusts entre Forests	72
4.5.1	Acceso a un Recurso	72
4.5.2	Replicación en Active Directory	73
4.5.3	Linked Multivalued Attributes	74
4.5.4	Generación Automática de la Topología de Replicación	75
4.5.5	Creación y Configuración de Sites	75
4.6	Backup de Active Directory	76
4.6.1	Restauración de Active Directory	77

5	Group Policy	79
5.1	Los User y Computer Configuration Settings	79
5.2	Herramientas Usadas para Crear GPOs	81
5.2.1	Creación de un Grup Policy	82
5.2.2	Herencia de Permisos de Group Policy en Active Directory	84
5.2.3	Conflicto de GPOs	84
5.2.4	Bloqueo de Deployment de GPO	85
5.2.5	Configuración de Group Policy Enforcement	86
5.2.6	Filtrado de Deployment de GPO	86
5.3	Administración del entorno de usuario	87
5.3.1	Group Policy Settings Enable o Disable	87
5.3.2	Scripts de Group Policy Settings	88
5.3.3	Folder Redirection	89
5.3.4	Carpetas Redireccionadas	89
5.3.5	Configuraciones Requeridas para Configurar Folder Re- direction	90
5.3.6	Los Gpupdate y los Gpresult	90
5.4	Administración de instalación de Software	91
5.4.1	Instalación del Software y el Proceso de Mantenimiento	91
5.4.2	Windows Installer	92
5.4.3	Descripción del Proceso de Software Deployment	93
5.4.4	Assigning Software vs. Publishing Software	93
5.4.5	Instalación de un Software a Traves de un GPO.	94
5.4.6	Cambio de Opciones para la Instalación de Software	95
5.4.7	Modificación de un Software	96
5.4.8	Tipos de Actualizaciones de Software	96
5.4.9	Utilización del Software Instalado	97
5.4.10	Funcionamiento de la Reinstalación de Software	98
5.4.11	Reinstalación de Software	99
5.4.12	Métodos para Quitar Software Instalado	99
5.5	Group Policy Management Console	100
5.5.1	GPMC Requisitos del Sistema	101
5.5.2	Instalación de GPMC	101
5.5.3	Group Policy Modeling y Group Policy Results	102
5.5.4	Administrando Múltiples Forests	103
5.5.5	Contenido de Dominios	103
5.5.6	Reportes de Configuración de GPO	104
5.5.7	Operaciones con GPO	104
6	Implementación y Administración	108

6.1	Funcionamiento	108
6.1.1	Entornos de Usuario	109
6.1.2	Características y Ventajas	110
6.1.3	Planificando la Instalación	112
6.1.4	Instalando Terminal Server	115
6.1.5	Configuración de Acceso de Usuario	115
6.1.6	Instalación de Remote Desktop Connection	115
6.1.7	Instalación de Aplicaciones en Terminal Server	117
6.2	Administración Remota con Remote Desktop	117
6.2.1	Integrando Terminal Services	118
6.2.2	Habilitación de Remote Desktop para Administración	119
6.2.3	Herramientas de Administración	120
6.3	Terminal Server como Servidor de Aplicaciones	122
6.3.1	Beneficios	122
6.3.2	Características Adicionales de administración	123
6.3.3	Mejoras en la Seguridad	124
6.3.4	Directorio de Sesión	125
6.3.5	Windows System Resource Manager	125
7	Implementación y Configuración de IIS 6.0	127
7.1	Ventajas	127
7.1.1	Características Nuevas y Mejoras	128
7.2	IIS como Servidor de Aplicaciones	131
7.2.1	Arquitectura IIS 6.0 -Nueva Arquitectura de Procesamiento de Request	132
7.2.2	HTTP.sys	134
7.2.3	WWW Service Administration and Monitoring Component	135
7.2.4	Worker Process Management	135
7.2.5	Worker Process Isolation Mode	136
7.3	Mejoras en la Seguridad	136
7.3.1	Abriendo Funcionalidad con IIS 6.0 Web Service Extensions	139
7.3.2	Identidad Configurable de Worker Process	139
7.3.3	Mejoras SSL	140
7.3.4	Autorización y Autenticación	141
8	Seguridad	142
8.1	Introducción a la Seguridad	142
8.1.1	Informática de Confianza	142

8.1.2	Lenguaje Común en Tiempo de Ejecución	143
8.1.3	Ventajas	143
8.1.4	Mejoras y Características Nuevas	144
8.2	Personal Firewall (ICF)	149
8.3	Security Templates	150
8.3.1	Security Policy	150
8.3.2	Security Configuration and Analysis	151

Bibliografía	153
---------------------	------------

Índice de Materias	154
---------------------------	------------

Índice de Figuras

1.1	Modelo Cliente Servidor.	6
2.1	Requisitos para Unirse a un Dominio o un Workgrup.	16
2.2	Funcionamiento del RIS.	21
2.3	Migración a Windows NT 4.0.	23
3.1	Funcionamiento del Proceso DHCP.	30
3.2	Funcionamiento del DHCP Relay Agent.	36
3.3	Esquema de un Domain Nemespace.	38
3.4	Proceso de Resolución de Nombres de HOST en un Cliente. . .	53
4.1	Proceso de Transferencia.	60
7.1	Descripción Gráfica del Worker Process.	134

Índice de Tablas

1.1	Funcionalidades.	8
1.2	Requerimiento del Sistema	8

Capítulo 1

Introducción a Windows Server 2003

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.

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 [7, SHAPIRO].

1.1 Nuevas Características

A continuación se detallarán las nuevas características incorporadas en Windows Server 2003 [4, JONES].

1.1.1 Automated System Recovery

Esta nueva herramienta permite recuperar el sistema operativo a su estado anterior. Utiliza un Diskette con información de la configuración y un set de backup. Cuando se quiera iniciar el proceso de Recovery se deberá tener los elementos antes mencionados y el Cd-Rom de instalación de Windows Server 2003.

Para este proceso, se necesitará del 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.

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.

1.1.2 Snapshot Infraestructura (Replica from Media DS)

Esta nueva característica puede 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 se podrá instalar el Controlador de Dominio en la Locación B a partir de un Backup del Controlador existente en la Locación A.

1.1.3 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. Para ello utiliza un cache en disco para el almacenamiento de versiones de archivos, que luego se pueden recuperar cuando sea necesario desde esa copia.

1.1.4 Encrypted File System (EFS)

La nueva funcionalidad del EFS en Windows Server 2003 permite realizar una encriptación 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 encriptación que utiliza EFS es una combinación de dos métodos, encriptación Asimétrica y Public Key Infrastructure (PKI).

1.1.5 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.

1.1.6 Active Directory

Las nuevas funcionalidades del Servicio de Directorio que trae Windows Server 2003 son las siguientes:

- *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 brinda 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 Políticas y hacer soporte para drag-and-drop en la herramienta. También incluye la funcionalidad de Backup, Restore y copia de Políticas, y trae una herramienta de Reportes para analizar la utilización de Políticas.
- *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 sign-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.
- *Políticas de Restricción de Software:* por medio de estas Políticas 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 de máximo 5000. A partir de Window 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).

1.1.7 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 primer Logon, el motivo del desperfecto para almacenarlo.

1.1.8 “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.

En la figura 1.1 de la página 6 se puede observar el Modelo Cliente Servidor.

1.1.9 IIS 6.0 - Internet Information Services 6.0

Este componente del sistema operativo presenta significativos cambios en relación con 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.



Figura 1.1: Modelo Cliente Servidor.

- *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 incrementar 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 di-

námicas deshabilitadas. Todo esto hace de IIS 6.0 el Web Server más seguro.

1.1.10 Versiones

Windows Sever 2003 presenta cuatro versiones con una serie de funcionalidades que se detallaran a continuación:

- **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
- **ESTANDARD 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.
- **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.
- **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.

A continuación se detalla como la funcionalidad varía de versión a versión, es por ello que se deberá tener en cuenta las necesidades al momento de la elección del sistema operativo:

1.1.11 Requerimientos

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

-	Server	Web Server	Enterprise Server	Datacenter
CPU /RAM	2CPU 4GB	2CPU 2GB	8 CPU 32 GB (x86) 64 GB (64-Bit)	8-64 CPU 64GB (x86) 512 GB (64-Bit)
Características	Nuevas Características: NLBS Personal Firewall	Puede Correr: IIS 6.0 NLBS DNS, DHCP, WINS Limitaciones: No DC Promo No Aplicaciones No TS App Mode	All Features From Standard Plus: 8-node Clustering 64 bit Version	All Features from Enterprise Plus: Datacenter Program Datacenter HCL Maintenance Multi-instance support

Tabla 1.1: Funcionalidades.

Requerimiento	Standard	Enterprise	Datacenter	Web
Velocidad Recomendada	550 MHz	733 MHz	733 MHz	550 MHz
RAM Recomendada	256 MB	256 MB	1 GB	256 MB
Soporte Multiprocesador (SMP)	Hasta 4	Hasta 8	8 Mín. 64 Máx.	Hasta 2
Espacio en Disco	1.5 GB	1.5 GB p/Arq. x86 2.0 GB P/Arq. Itanium	1.5 GB p/Arq. x86 2.0 GB p/Arq. Itanium	1.5 GB

Tabla 1.2: Requerimiento del Sistema

1.2 Funcionalidades

Los servidores desempeñan muchos papeles en el ambiente cliente - servidor de una red. Algunos servidores se configuran para proporcionar la autenticación 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. Se espera que el administrador del sistema sepa los tipos primarios de servidores y qué funciones realizan en su red [5, HONEYCUTT].

1.2.1 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, autenticación y búsquedas del directorio. Cuando se instala Active Directory en una computadora que corre Windows Server 2003, la computadora se convierte en Controlador de dominio (Domain Controller). En una red Windows Server 2003, todos los servidores en el dominio que no sean Domain Controllers se llaman Member Servers. Los servidores no asociados a un dominio se llaman workgroup Servers.

1.2.2 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.

1.2.3 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.

1.2.4 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.

1.2.5 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 se planea hacer hosting de Web y Sitios File Transfer Protocol (FTP) con IIS, configure el Server como Application Server.

1.2.6 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, se 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, excepto archivos, y utilizar los recursos de la red de una posición remota, como si éstos recursos fueran instalados en su propia computador

1.2.7 La Herramienta Manage Your Server

Cuando Windows Server 2003 es instalado y un usuario realiza el logon por primera vez, la herramienta Manage Your Server corre automáticamente. Esta herramienta es utilizada para agregar o para quitar Roles a Servers. Cuando se agrega 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, se 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

2.1 introducción a la Instalación de Windows Server 2003

La instalación y configuración de Windows Server 2003 es similar a la versión anterior aunque presenta una serie de mejoras [9, MINASI].

- *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.
- *Comprobación de compatibilidad:* el Asistente permite a los usuarios realizar una prueba de compatibilidad detallada en sus PCs. También mediante la herramienta “Application Compatibility Toolkit” se puede comprobar la compatibilidad de aplicaciones.

2.2 Seleccionando File System

Una vez que se haya creado la partición donde se planea instalar Windows Server 2003, la instalación permitirá que seleccione el sistema de archivos para darle formato. Windows Server 2003 soporta sistema de archivos NTFS y FAT16/FAT32.

2.2.1 NTFS

Para su utilización se 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.
- Encriptación de archivos. NTFS permite transparentar encripte, 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.

2.2.2 FAT y FAT32

Normalmente se utiliza 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 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 Modelo de Licenciamiento para Windows Server 2003

Existen una serie de elementos del modelo de licenciamiento Windows Server 2003 que no han cambiado, como ser:

- 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 “autenticado”
- 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” (nteriormente 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.

Los cambios realizados fueron los siguientes:

- 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). Al tener dos tipos de CAL’s, permite utilizar el modelo más conveniente para su organización.

Los cambios realizados son los siguientes:

- 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. Al tener dos tipos de CAL's, se podrá utilizar el modelo mas conveniente para la organización

2.4 Determinación de Pertenencia a Workgroup o Dominio

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

2.4.1 Dominio

Durante la instalación se puede agregar la computadora a un dominio existente como member server, para lo cual se 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. La cuenta puede ser creada antes de la instalación o, si posee de privilegios administrativos en el dominio, puedeser creada 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

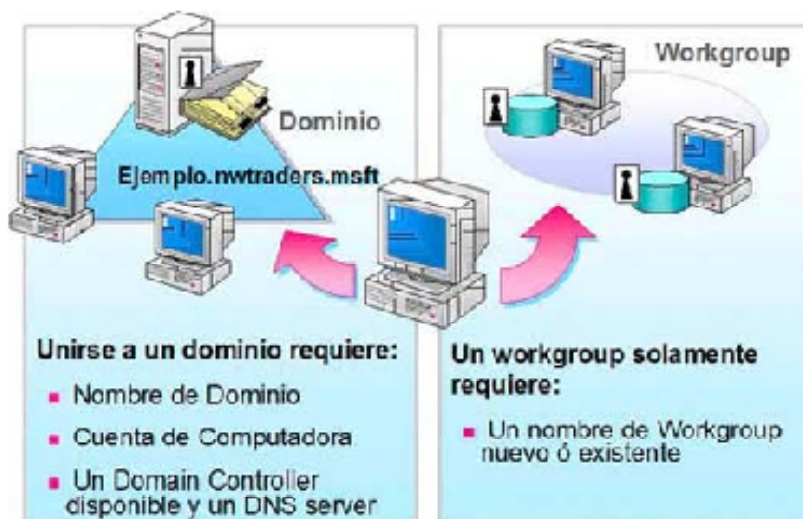


Figura 2.1: Requisitos para Unirse a un Dominio o un Workgroup.

2.4.2 Workgroup

Se 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 se asigne puede ser el nombre de un workgroup existente o de un workgroup nuevo que se cree durante la instalación.

En la figura 2.1 de la página 16 se hace referencia en forma grafica de los requisitos básicos necesarios para unirse ya se a un dominio o un workgroup.

2.5 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.

2.5.1 Funcionamiento del Programa de Instalación

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. 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.

2.5.2 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.

A continuación se describen las opciones que están disponibles en el Wizard.

CertificateServices: Permite crear y solicitar certificados digitales para la autenticación X.509. Los certificados proporcionan medios comprobables de identificar a usuarios en redes no-seguras, tales como Internet.

Fax Services: Permite enviar y recibir faxes desde su computadora.

Indexing Service: Permite hacer búsquedas dinámicas con texto completo de los datos que se almacenan en la computadora o la red.

Message Queuing: Soporta aplicaciones que envían mensajes a las colas. También permite comunicar aplicaciones a través de redes heterogéneas y con computadoras que pueden estar temporalmente fuera de línea.

Remote Installation Services: Permite la instalación remota de Windows XP Professional, Windows 2000 y Windows Server 2003 sobre una conexión de red.

Remote Storage: Permite que el usuario utilice las librerías de cintas como extensiones de volúmenes NTFS, moviendo datos automáticamente y desde medios de cinta.

Terminal Server: Configura la computadora para permitir que los usuarios múltiples utilicen una o más aplicaciones remotamente. Asimismo está disponible durante la instalación, por ejemplo RIS y Servidor de Aplicación.

Terminal Server Licensing: Configura el servidor como Terminal Services License Server y eso proporciona licencias del cliente.

Update Root Certificates: Descarga automáticamente la lista más actual de root certificates desde Windows Update, si fuese necesario.

Windows Media Services: Permite hacer stream de contenido multimedia para usuarios.

Después de realizar la selección de componentes opcionales, Wizard permite ajustar la fecha y hora, lo que es crítico para opciones de réplica de base de datos en Windows Server 2003.

2.5.3 Instalación de Componentes para Networking

Una vez que Winzard recopila información de su computadora, procede a guiar al usuario a través de la instalación de componentes para networking. Este segmento del proceso de instalación comienza con la detección de las tarjetas de red. Después de configurar los adaptadores de red, la instalación localiza el server corriendo el servicio de DHCP Server en la 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.

2.5.4 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 se especificó anteriormente.
- Guarda la configuración al disco duro local.
- Quita archivos temporales y reinicia la computadora.

2.6 Instalando desde la Red

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.

Los pasos para la instalación son similares a la versión anterior, 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.

2.7 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, se 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, se 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 se planea instalar en la computadora del cliente.
3. Las imágenes que se almacenan en el RIS server.

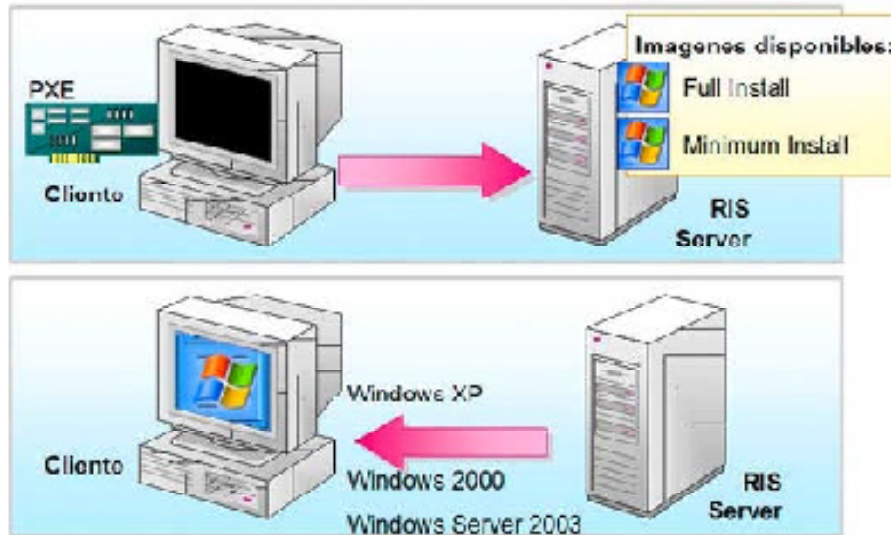


Figura 2.2: Funcionamiento del RIS.

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.

Los requisitos para RIS Server son los siguientes:

- Active Directory.
- DHP Server.
- DNS Server.

En la figura 2.2 de la página 21 se hace mención al funcionamiento del Servicio de Instalación Remoto.

2.8 Usando System Preparation Tool (sysprep)

Cuando se quiera instalar 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 Server 2003, y copiando esa imagen sobre las computadoras múltiples de destino, de esta manera se ahorra tiempo en deployment de Windows Server 2003.

Para instalar 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.

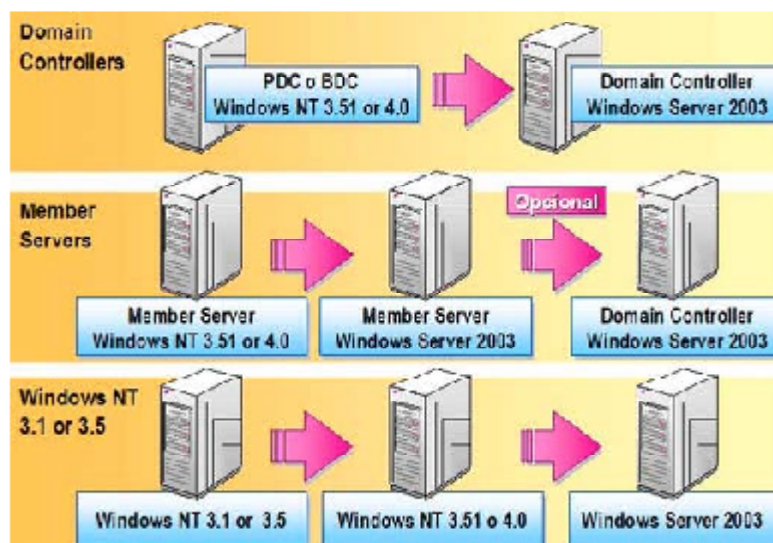


Figura 2.3: Migración a Windows NT 4.0.

2.9 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.

La figura 2.3 de la página 23 nos da una idea gráfica de la migración desde Windows NT 4.0.

2.9.1 Migración de Member Servers

Antes de migrar a Windows Server 2003, es importante que se realice un backup de los archivos críticos para asegurar que sus datos sean preservados si el proceso falla. Para preservar los archivos críticos y configuraciones se debe 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 esto se debe introducir el CD-ROM de Windows Server 2003 y comenzar el proceso de instalación. Este proceso es similar a una instalación nueva. Si se lo realiza desde la red se debe ejecutar Winnt32.exe.

Se podría presentar el caso que la partición de sistema no tenga espacio para el proceso de migración. No obstante, el mismo disco posee espacio adicional para obtener información sobre cómo expandir esa partición.

Al finalizar el proceso el server que se tenía pasará a ser un Windows Server 2003 Member Server.

2.9.2 Migración de Dominios

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

Migración In-Place: este proceso determina las acciones necesarias para conservar la estructura anterior. Por lo tanto si se tenía 4 dominios Windows NT 4.0, al finalizar se 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. Es importante instalar un nuevo BDC, retirarlo de la red, promover a PDC e instalar Windows Server 2003 en esa computadora.
- A continuación se debe poner nuevamente en la red esa computadora y despromuever en PDC productivo a BDC.
- Luego migrar todos los BDC del Dominio.

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

Reestructuración de Dominio: este proceso determina las acciones necesarias para reestructurar la estructura anterior (consolidación de Dominios). Por lo tanto si se tenía 4 dominios Windows NT 4.0, al finalizar se 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.

2.10 Migración desde Windows 2000

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

2.10.1 Migración de Member Servers Windows 2000

Antes de que se migre a Windows Server 2003, es importante que se haga un back up de archivos críticos para asegurar que los datos sean preservados en el caso que el proceso falle. Las siguientes tareas sirven para preservar los 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, se debe intrducir el CD-ROM de Windows Server 2003 y comenzar el proceso de instalación. Este proceso es similar a una instalación nueva, si se lo realiza desde la red se debe ejecutar Winnt32.exe.

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

Al finalizar el proceso el server que se tenía pasará a ser un Windows Server 2003 Member Server.

2.10.2 Migración de Dominios

El upgrade de Active Directory puede ser gradual y realizado sin interrupción de las operaciones. Si se 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 se 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, es necesario asegurarse de que el dominio está preparado.

Existen dos herramientas command-line que ayudan en la migración de Domain Controller:

- Winnt32. Permite comprobar la compatibilidad de upgrade del server.
- Adprep. Se lo debe usar en el Schema Operations Master para preparar el forest.

Se debe tener 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 se 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 / forestprep` 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.

Capítulo 3

Instalación y Configuración de Servicios DHCP, DNS y WINS

3.1 DHCP - Dynamic Host Configuration Protocol

DynamicHostConfigurationProtocol(DHCP) es un estándar IP para simplificar la administración de la configuración del IP del cliente. El estándar DHCP permite utilizar 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.

La utilización de 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.

Configuración manual de TCP/IP

Cuando se 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.

Configuración automática TCP/IP

Cuando se 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 se necesita realizar un cambio en la configuración IP de varios clientes, se podrá realizarlo una vez en el DHCP Server, para que el DHCP actualice automáticamente la configuración del cliente reflejando el cambio.

3.1.1 Direccionamiento de Direcciones IP mediante DHCP

DHCP permite manejar la asignación de IP de una localización central, y por lo tanto se 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.

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.

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.

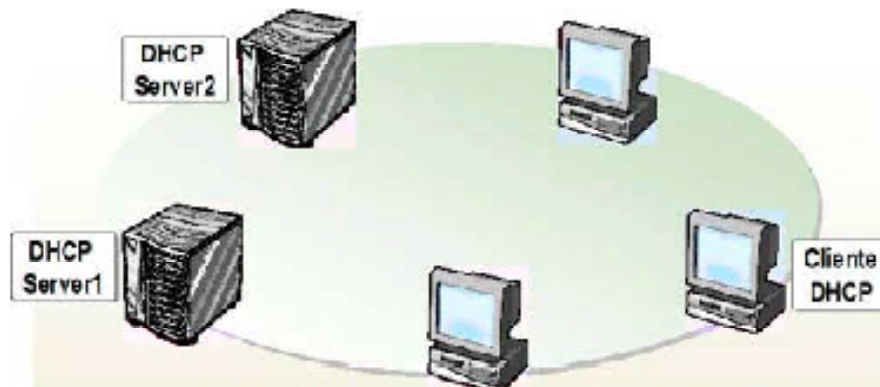


Figura 3.1: Funcionamiento del Proceso DHCP.

3.1.2 Funcionamiento del Proceso DHCP Lease Generation

La figura 3.1 de la página 30 muestra sintéticamente como el proceso DHCP funciona.

A continuación se describe con más detenimiento los pasos que se deben seguir:

El cliente DHCP envía un broadcast, 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 no lo logra.

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.

3.1.3 Funcionamiento del Proceso DHCP Lease Renewal

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.

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 DHCPRE-

LEASE al DHCP Server para liberar la configuración IP y para cancelar el lease restante.

El proceso “Lease Renewal” puede ser automático o manual:

- *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.

- *Proceso manual Lease Renewal:*

Si necesita actualizar la configuración DHCP inmediatamente, se 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.).

La autorización de DHCP es el proceso de registrar el servicio DHCP Server en un dominio Active Directory Service, 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.

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 se está configurando un DHCP Server, la autorización debe ocurrir como parte del dominio Active Directory. Si no se 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.

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.

3.1.4 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 servicio 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 DHCP Server continuará funcionando si recibe un DHCPACK de otro DHCP Server que no sea miembro de Active Directory.

3.1.5 Los DHCP Scopes

Un scope es un rango de direcciones válidas IP que están disponibles para asignar a computadoras cliente en una subred en particular. Se 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. Se 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.

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 Gateway.
- Scope name: Identificador para propósitos administrativos.
- Exclusion range: El rango de direcciones IP en el scope excluidas para la asignación.

Cada subred 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.

También es importante saber que es una reserva DHCP; una reserva es una dirección IP permanente asignada a un cliente específico. Se puede reservar una dirección IP permanente a un dispositivo en la red. La reserva se realiza a la dirección MAC del dispositivo.

3.1.6 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.

Las Opciones más comunes de DHCP son las siguientes:

- *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 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.

3.1.7 DHCP Relay Agent

El DHCP Relay Agent es una computadora o router configurado para escuchar broadcast DHCP/BOOTP de clientes DHCP y reenviar esos mensajes a los DHCP 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 con-

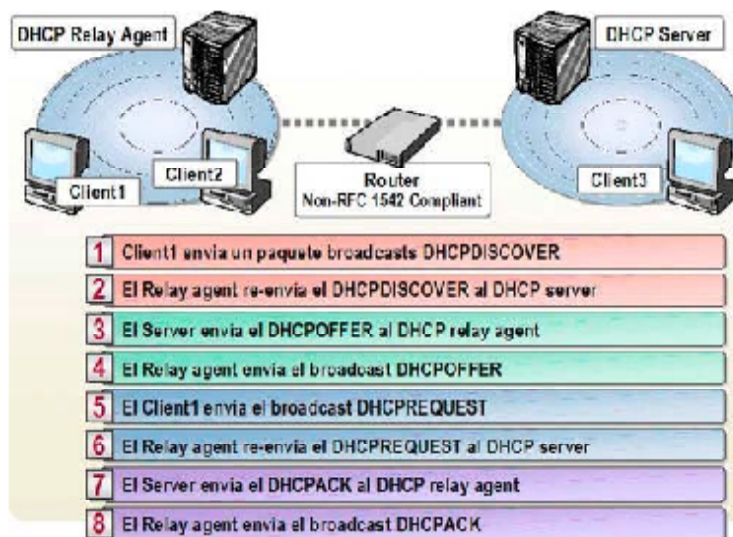


Figura 3.2: Funcionamiento del DHCP Relay Agent.

figurados específicamente para dejarlos pasar. Por lo tanto, sin configuración adicional, los DHCP Servers solo proveen direcciones IP a clientes en su sub-set local. Para que se pueda asignar direcciones a clientes en otros segmentos, deberá configurar la red para que los DHCP broadcasts puedan llegar desde el cliente al DHCP Server. Esto se puede hacer de dos maneras:

- configurando los routers que conectan las subnets para dejar pasar DHCP broadcasts,
- o configurando DHCP Relay Agents. Windows Server 2003 soporta el servicio Routing and Remote Access configurado para funcionar como DHCP Relay Agent.

En la figura 3.2 de la página 36 se describe gráficamente como 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.

3.2 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.

3.2.1 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.

La figura 3.3 de la página 38 muestra el esquema del Domain Namespace.

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.

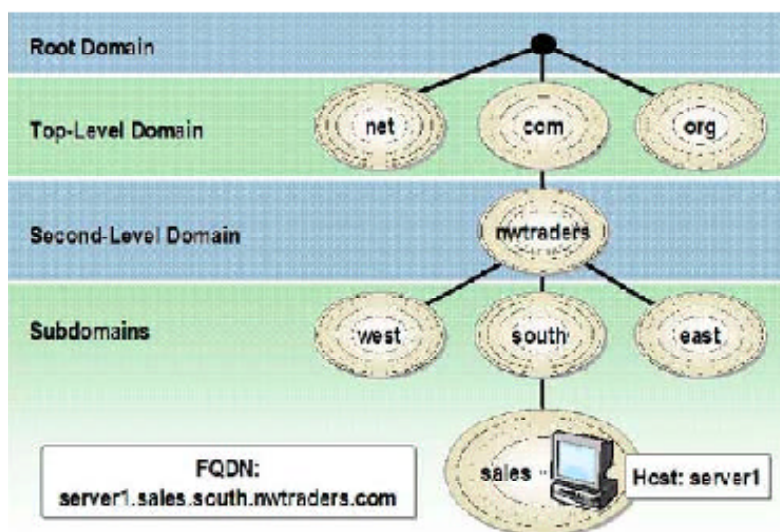


Figura 3.3: Esquema de un Domain Namespace.

3.2.2 Query DNS

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

El Query Recursiva funciona de la siguiente manera:

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, la respuesta es un error, indicando que no puede resolver el nombre.

El Query Interactiva funciona de la siguiente manera:

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 Iterativa.

3.2.3 Funcionamiento del Caching de DNS Server

Caching es el proceso temporal de almacenar la información reciente, 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.

3.2.4 Mantenimiento y Almacenamiento de 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, se deben comprender claramente 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.

Es importante recordar que 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.

Identificación de tipos de zonas

A continuación 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.

3.2.5 Resource Records y Record Types

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.

3.2.6 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.

Creación de una zona de búsqueda directa

Para crear una zona de búsqueda directa, se debe hacer click en Búsqueda directa en la página Zona de búsqueda directa o inversa del Asistente para zona nueva. El asistente sirve de 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.

Creación de una zona de búsqueda inversa

Para crear una zona de búsqueda inversa, se debe hacer click en Búsqueda inversa en la página Zona de búsqueda directa o inversa del Asistente para zona nueva. El asistente proporciona una guía de 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.

3.2.7 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.

Es importante recordar que para crear una zona secundaria estándar, debe crear primero una zona principal estándar.

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, se debe escribir la dirección IP del Master Server en el cuadro Dirección IP y hacer click en Agregar.

3.2.8 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.

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.

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.

3.2.9 Introducción a las actualizaciones dinámicas

Se puede realizar la configuración de 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.

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.

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:

- 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.
- El servidor DHCP devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
- El cliente envía al servidor DNS una solicitud de actualización DNS de su propio registro de búsqueda directa, el registro de recursos A (dirección).
- 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.

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:

- 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.
- El servidor devuelve al cliente un mensaje de confirmación DHCP, en el que se otorga una concesión de dirección IP.
- El servidor DHCP envía al servidor DNS actualizaciones de los registros de recursos A y PTR del cliente.

Configuración del DNS Server para permitir actualizaciones dinámicas

Para configurar un servidor DNS de modo que permita actualizaciones dinámicas, se debe abrir 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?, corresponde hacer click en Yes.

3.3 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 también lo usará para llevar a cabo consultas 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.

3.3.1 Estudio de los Registros de la Base de Datos WINS

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

Para abrir la base de datos WINS se deberá:

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

3.3.2 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.

3.3.3 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.

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.

3.3.4 Funcionamiento de la Replicación Push

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:

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

3.3.5 Funcionamiento de la Replicación Pull

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:

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

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

3.3.6 Mantenimiento

Backup

Se deben realizar tareas de mantenimiento en períodos de tiempo específico. Para ayudar en esta tarea, el WINS Server puede ser configurado para realizar los backups automáticamente. Se debe tener 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 [1, WILLIAMS].

Para especificar el directorio de backup de WINS deberá:

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

El WINS Server realizará un backup automáticamente cada 24 horas.

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 se deberá 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.

3.3.7 Procesos de Resolución de Nombres e Integración WINS / DNS

Resolución de nombres de host

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

- 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.
- 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.
- 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.
- 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.
- 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.
- Por último tendrá que consultar el archivo local HOST 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.

La figura 3.4 de la página 53 responde gráficamente al proceso de resolución de nombres de HOST en un cliente.

3.3.8 Resolución de Nombres NetBIOS

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

- 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.
- 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.

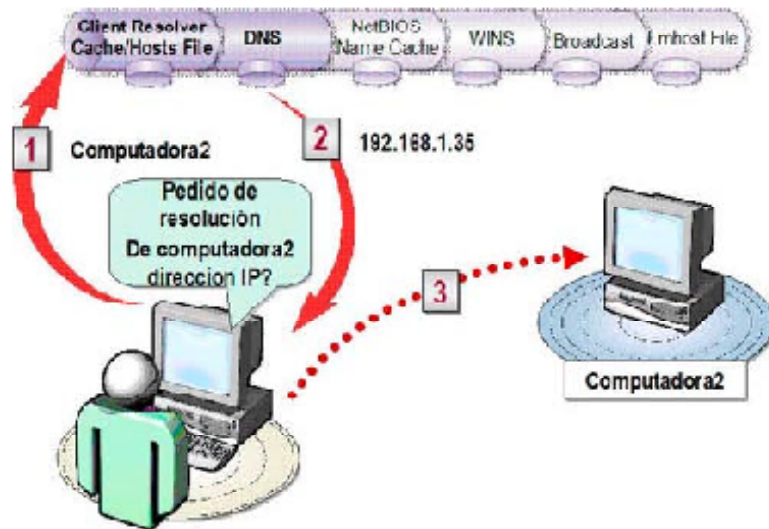


Figura 3.4: Proceso de Resolución de Nombres de HOST en un Cliente.

- 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.
- Por último tendrá que consultar el archivo local LMHOST 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.

3.3.9 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.

Se puede configurar DNS integrado con WINS Servers.

Capítulo 4

Active Directory Service

4.1 Introducción a Active Directory Services

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, es necesario comprender el funcionamiento y la estructura de Active Directory.

Active Directory proporciona 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 [8, KING].

4.1.1 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.

4.1.2 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, se 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*: Se 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. También se puede 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:
 1. Un límite administrativo para los objetos.
 2. Medios de administrar la seguridad para los recursos compartidos.
 3. 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.

4.1.3 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, se 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 continua de Active Directory, cada domain debe tener más de un Domain Controller.
- *Active Directory site*: Los sites son grupos de computadoras conectadas. Cuando se 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. Se crean 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 topología 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.

4.1.4 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.

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, se 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.

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 específico.

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, compu-

tadoras, 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.

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, de 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.

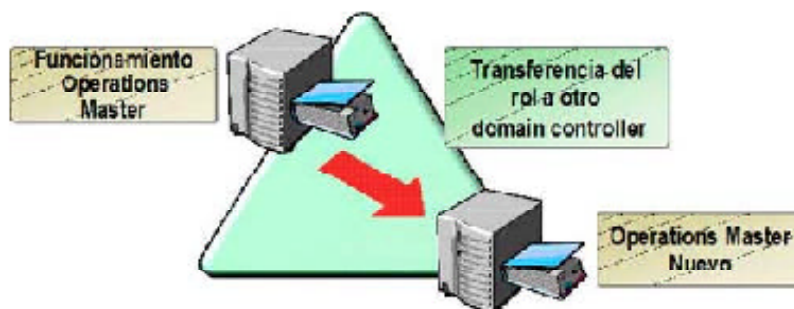


Figura 4.1: Proceso de Transferencia.

4.1.5 Transferencia de Operations Master Roles

Las Operations Master Roles deben ser colocados 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 se 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.

La figura 4.1 de la página 60 describe el proceso de transferencia gráficamente.

4.2 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.

4.2.1 Capacidades de Active Directory

Permite a usuarios y aplicaciones tener acceso a la información sobre objetos: Esta información se almacena en forma de valores atributos. Se 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.

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.

4.2.2 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.

Se 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.

Sobre Domain Controllers Windows Server 2003, se 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.

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.

4.2.3 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 atributos que 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 se busca un objeto y se 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. Se 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.

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.

Para poder utilizar esta nueva característica de Windows Server 2003, se debe 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.

4.2.4 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.

Los domain components de los Distinguished Name están basados en Do-

main Name System (DNS).

4.2.5 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.

A continuación se describen los snap-ins administrativos comunes para administración de Active Directory.

- *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.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. También resulta conveniente describir la herramientas de command-line para utilizar cuando se quiera administrar Active Directory.
- *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. Se 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.
- *Dsrn*: 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.

4.3 Instalación de Active Directory

4.3.1 Requisitos para Instalar Active Directory

Antes de instalar Active Directory, se debe comprobar que la computadora esté 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.

Los requisitos para la instalación de Active Directory son los siguientes:

- 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 y con sistema de archivos. 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.

- *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, se 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 se 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.

4.3.2 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.
 - Domain DNS Zone Partition.

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.
- **Configura pertenencia al site apropiado para el Domain Controller.** Si la IP del servidor que se 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 se 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 Objects.
- **Aplica el password para la cuenta del administrador.** Se utiliza la cuenta para iniciar el Domain Controller en Directory Services Restore Mode

4.3.3 Renombrar un Domain Controller

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

Cuando se renombra un Domain Controller, se debe 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, se deben realizar los siguientes pasos:

1. En Control Panel, hacer doble-click en System.
2. En el cuadro System Properties, en Computer Name, hacer click en 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.

Se 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.

Para mover un Domain Controller a otro domain, se debe primero degradar el Domain Controller y entonces promoverlo en el nuevo dominio.

4.4 Las zonas DNS Active Directory Integrated

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.

4.4.1 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. Se 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.

Las Zonas Active Directory Integrated ofrecen las siguientes ventajas:

Multimaster replication: Cuandose realiza la configuración de 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), 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, se pueden 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.

4.4.2 Funcionalidad de Forest y Domain

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.

La funcionalidad del 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. Se 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. Se 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. Se lo puede utilizar 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.

- Windows 2003 Interim. Este nivel es un nivel funcional especial que soporta Domain Controllers Windows NT 4.0 y Windows Server 2003.

La funcionalidad 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

4.4.3 Habilitación de nuevas características en Windows Server 2003

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. se 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. Se debe ser Enterprise Administrator para elevar el nivel funcional del forest.

En ocasiones se hace necesario elevar el nivel funcional del forest y del dominio a Windows Server 2003 habilita ciertas características, por ejemplo, forest trusts, que no está disponible en otros niveles funcionales. Se puede elevar la funcionalidad del forest y del dominio usando Active Directory Domains and Trusts.

4.5 Funcionamiento de los Trusts entre Forests

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 trusted 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.

4.5.1 Acceso a 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.

Es importante recordar 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.

4.5.2 Replicación en Active Directory

Un punto importante de la replicación en Active Directory es la 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*: Retrasa 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 los 15 segundos 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

4.5.3 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 sobrescribir 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.

4.5.4 Generación Automática de la Topología de Replicación

Cuando se agregan 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.

4.5.5 Creación y Configuración de Sites

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

En Active Directory, los sites ayudan a definir la estructura física de una red. Una o más subnets TCP/IP en un 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.

Los 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 los 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.

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.

4.6 Backup de Active Directory

Hacer backup de Active Directory es esencial para mantener la base de datos de Active Directory. Se puede hacer backup de Active Directory usando una graphical user interface (GUI) y herramientas command-line tools, que provee Windows Server 2003 [10, MORIMOTO].

Con frecuencia se 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, se 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 se 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.

4.6.1 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.

- **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.

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

Capítulo 5

Implementación, Administración y Monitoreo de Group Policy

Group Policy otorga control de administración sobre los usuarios y las computadoras de la 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 se definió. También se puede aplicar configuraciones de Group Policy a través de una organización entera o a grupos específicos de usuarios y de computadoras [6, IVENS].

5.1 Los User y Computer Configuration Settings

Se 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 Configuration, 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.

5.2 Herramientas Usadas para Crear GPOs

- Active Directory User: se 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: 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, se puede:

- Hacer Back up y restore de GPOs.
- Copiar e importar GPOs.

- Usar filtros Windows Management Instrumentation (WMI).
- Generar reportes de GPO y RSoP.
- Buscar para GPOs.

Group Policy Management vs. default Group Policy tools

Antes de Group Policy Management, se 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, aún se 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, se 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, todavía se 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.

5.2.1 Creación de un Grup Policy

Se deben utilizar 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, se deben realizar los siguientes pasos:

- 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.

- 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.

Es importante antes que nada saber con claridad el significado de 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, se puede centralizar la administración y el deploy de GPOs a muchos dominios u organizational units.

Cuando se 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, se 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 se 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.

5.2.2 Herencia de 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.

Se puede también tener GPOs múltiples linkeadas a 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.

5.2.3 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, organizational 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 sobrescribe 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, se 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*: Esta opción se utiliza para prevenir que contenedores child eliminen una GPO 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.

5.2.4 Bloqueo de Deployment de GPO

Usted puede prevenir en un contenedor child la herencia de cualquier GPO 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 se desea asegurar 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.

5.2.5 Configuración de Group Policy Enforcement

Para configurar enforcement de GPO link deberá:

1. En Group Policy Management de la consola, expandir el forest con el link en el cual se 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.
1. Hacer click derecho en el GPO link y después hacer click en Enforced para permitir o inhabilitar el enforcement.

5.2.6 Filtrado de Deployment 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 se desea. Usando la característica de filtrado, se puede determinar qué configuraciones se aplican a los usuarios y a las computadoras en el contenedor específico.

Se 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. 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

5.3 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. Se manejan los ambientes de usuario para estar seguro de que los mismos tengan lo necesario para realizar sus trabajos. De esta manera, no podrán corromper o configurar incorrectamente sus ambientes.

5.3.1 Group Policy Settings Enable o Disable

Si se 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, no se necesita inhabilitar el policy setting Prohibit access to the Control Panel, a menos que previamente haya aplicado un policy setting habilitándolo. En esta situación, se debe fijar 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. Se 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 se permite un policy setting, estará consintiendo la acción del policy setting. Por ejemplo, para revocar a alguien acceso al Control Panel, se puede permitir 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 se 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, se 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. A veces se puede necesitar seleccionar un grupo o una computadora si el policy setting necesita volver a dirigir al usuario a una cierta información. Otras veces, para permitir proxy settings, se 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.

5.3.2 Scripts de Group Policy Settings

Se 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. Se 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, se 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. Se 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.

5.3.3 Folder Redirection

Cuando se 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.
- 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, se puede utilizar Group Policy para configurar disk quotas, limitando la cantidad de espacio que es tomado por los usuarios.

5.3.4 Carpetas Redireccionadas

Se puede redireccionar las carpetas My Documents, Application Data, Desktop y Start Menu. Una organización debe 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.

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

- My Documents.
- Application Data.
- Desktop.
- Start Menu.

5.3.5 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.

Folder Redirection tiene las siguientes opciones básicas:

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 redireccionadas. 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.

5.3.6 Los Gpupdate y los Gpresult

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. Se puede correr gpupdate para

probar una Group Policy setting o aplicar inmediatamente un Group Policy setting.

Debido a que se 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. Se puede utilizar *gpresult* para ver qué configuraciones de la GPO son efectivas y localizar problemas en la aplicación.

5.4 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, se puede asegurar que los programas que los usuarios requirieran para realizar sus trabajos, estén disponibles siempre y donde sea necesario.

5.4.1 Instalación del Software y el Proceso de Mantenimiento

En Windows Server 2003, permite 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, se puede manejar varias fases de la instalación del software sin instalar software en cada computadora individualmente.

La siguiente lista describe cada fase en la instalación del software y proceso de mantenimiento:

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. Se 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.

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.

Maintenance: El software se actualiza con una nueva versión o reinstalando el software con un service pack o un software update. De esta manera, estará automáticamente actualizado o reinstalado cuando la computadora se encienda o cuando el usuario inicie el programa.

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 sesión.

5.4.2 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.
- Windows Installer package.

Las ventajas de usar tecnología 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.

5.4.3 Descripción del Proceso de Software Deployment

Cuando se instala software, se está especificando cómo se instalan los aplicativos y cómo se mantienen los mismos en su organización.

Para instalar nuevo Software, utilizando Group Policy, se deberá:

- *Crear un software distribution point:* Esta carpeta compartida en el 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.
- *Utilizar la GPO para instalar software:* Se 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.
- *Cambiar las características de la instalación del software:* Dependiendo de sus requisitos, se puede cambiar las características que fueron fijadas durante la instalación inicial del software.

5.4.4 Assigning Software vs. Publishing Software

Los dos tipos de instalación son: asignar software y publicar software.

Usando la asignación de software, se esta aseguro 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, 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 deben instalar el published software, se puede publicar software solamente a los usuarios y no a las computadoras.

5.4.5 Instalación de un Software a Traves de un GPO.

Después de crear un software distribution point, se 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.

Es importante recordar que asignar ni publicar un Windows Installer package más de una vez en la misma GPO.

Para utilizar una GPO para instalar software, se tendrá que realizar los siguientes pasos:

1. Crear o editar la GPO.
2. Bajo User Configuration o Computer Configuration (dependiendo de si se esta realizando la asignación del 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.

5.4.6 Cambio de Opciones para la Instalación de Software

Un GPO puede contener varias configuraciones que afecten cómo un aplicativo es instalado, manejado y quitado. Se puede definir las configuraciones por defecto global para los nuevos packages en la GPO, también se 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 se podrá cambiar las características de la instalación que fueron fijadas durante la instalación inicial del software.

Para configurar las opciones implícitas para la instalación del software, se 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

1. 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, es necesario realizar los siguientes pasos:

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.

5.4.7 Modificación de un 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 la organización utilizar un paquete de software de diversas maneras. Se 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 se le 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. se deberá determinar el orden en el cual aplicar las transformaciones a los archivos antes de asignar o publicar el aplicativo.

5.4.8 Tipos de Actualizaciones de Software

Las tareas en una organización son dinámicas y variadas. Se 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 versión. 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 actualización pero no otros, se puede crear GPOs múltiples para que se apliquen a los usuarios que requieran la actualización y crear los paquetes de software apropiados en ellas.

5.4.9 Utilización del Software Instalado

Se utiliza la instalación de software para establecer el procedimiento de actualización de software a la versión actual.

Para instalar una actualización, se 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 después seleccionar la versión anterior (actual) del software. Se puede actualizar un aplicativo usando la GPO actual o seleccionando 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 después 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.

5.4.10 Funcionamiento de la Reinstalación de Software

Redeployment es la aplicación de service packs y actualizaciones de software al software instalado. Se 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 se 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 se asigne software a una computadora, el service pack o actualización de software se aplicará automáticamente la próxima vez que la computadora se encienda.
- Cuando se 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.

5.4.11 Reinstalación de Software

Se utiliza la instalación de software para establecer el procedimiento de reinstalación del mismo. Antes de reinstalar, uno se debe asegurar que el servicio incluya un nuevo archivo Windows Installer package (.msi). De lo contrario, no se 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.

5.4.12 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. Se 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: Se 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: Se puede quitar el software de la instalación del mismo sin forzar el retiro físico 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.

5.5 Group Policy Management Console

Conjuntamente con Microsoft Windows Server. 2003, se está lanzando una nueva herramienta Group Policy Management que unifica la administración de Group Policy. La Microsoft Group Policy Management Console (GPMC) proporciona una sola solución para manejar todas las áreas 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. La GPMC ayuda a manejar una empresa con más eficacia.

En pocas palabras se podría decir que es una herramienta nueva para manejar Group Policy en Windows Server 2003.

La GPMC:

- Permite el manejo de 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 combinaciones propuestas de policies.

5.5.1 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.

5.5.2 Instalación de GPMC

La instalación de GPMC es un proceso simple que implica la ejecución de un Windows Installer (.MSI) package.

Para ello:

- Hacer Doble-click en gpmc.msi package y en Next.
- Aceptar el End User License Agreement (EULA), y hacer click en Next.
- 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
- Para reparar o quitar GPMC, usar Add or Remove Programs en Control Panel. Alternativamente, correr el

gpmc.msi package, seleccionar la opción apropiada, y hacer click en Finish.

5.5.3 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, se 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.

5.5.4 Administrando Múltiples Forests

Múltiples forests pueden ser agregados fácilmente a la consola. Para ello se 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 se puede agregar solamente forest a la GPMC si hay 2-way trust con el forest del usuario que corre la GPMC.

5.5.5 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 contenedor.

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.

5.5.6 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 configuración 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.

5.5.7 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 tenía cuando era realizado el backup. Por lo tanto, la operación 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.

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 cualquiera 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.

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 perose 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.

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 cualquiera de los scripts ImportGPO.wsf o ImportAllGPOs.wsf que se incluyen con GPMC.

Copy

Una operación de copia transfiere configuraciones usando una GPO existente en Active Directory como la fuente y crea un GPO nueva como su destino.

Además en esta operación 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 Objects 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.

Capítulo 6

Implementación y Administración de Terminal Server en Windows Server 2003

Terminal Services permite el acceso de múltiples usuarios a Windows Server 2003, permitiendo que varias personas inicien sesiones en una sola computadora 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 [3, RUSSEL].

6.1 Funcionamiento

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 basados o no en Windows. 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 presentación remota: 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.

6.1.1 Entornos de Usuario

Después de instalar el software de cliente, los usuarios acceden al Terminal Server abriendo Remote Desktop Connection Client del menú Programs/Accessories/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.

6.1.2 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 im-

plementar 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 encriptación multinivel, el cual se permite que siempre haya riesgo de interceptación desautorizada de transmisión en la conexión entre el servidor y el cliente. Hay tres niveles de encriptación disponibles: low, medium y high. Todos estos niveles usan el Standard Rivest-Shamir-Adleman (RSA) RC4 Encryption. Este es un estándar de encriptación 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 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.

6.1.3 Planificando la Instalación

Identificando aplicaciones de Cliente

Antes de instalar Terminal Server, identifique las aplicaciones que 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 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.

La computadoras de 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.

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 por usuario que una computadora ejecutando Windows Server 2003. Asegurar que su servidor pueda acomodar su base de usuario 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.

Antes de instalar Terminal Server, es necesario considerar 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.
- 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.

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 simula 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).

6.1.4 Instalando Terminal Server

Para instalar Terminal Server, se debe habilitar el componente Terminal Server luego de la instalación, usando el Windows Components wizard. Se 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.

6.1.5 Configuración de 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, también se puede especificar home directories y user profiles para los usuarios.

6.1.6 Instalación de 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 Windo-

ws 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.)

INTERFAZ MEJORADA

Las sesiones remotas usando Remote Desktop Connection pueden 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 experiencia permite que se 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.

REDIRECCION DE RECURSOS DEL CLIENTE

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.

Redirección 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.

Redirección 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.

6.1.7 Instalación de 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.

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.
- Usando el comando Change User, solamente cuando no se pueda instalar el aplicativo usando Add/Remove Programs.

6.2 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 es-

tán 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 encriptación.
- 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.

6.2.1 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.

6.2.2 Habilitación de Remote Desktop para Administración

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.

6.2.3 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, se 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 encriptación 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.

6.3 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 virtualmente, 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 transmitida 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.

6.3.1 Beneficios

Terminal Services en Windows Server 2003 proporciona tres importantes beneficios.

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.

6.3.2 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 realizado.
- 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.

6.3.3 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, simplemente se 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, se 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 encriptación 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.

6.3.4 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.

6.3.5 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, se puede evitar que un usuario

consume recursos por demás, ejecutando tareas innecesarias o procesos múltiples, sin límite de recursos. También se 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 límite superior o sin límite según sea el caso.

Capítulo 7

Implementación y Configuración de IIS 6.0

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.

7.1 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.

A continuación se detallan algunas de las ventajas que proporcionan IIS 6.0 y Windows Server 2003:

Confiable y escalable

IIS 6.0 proporciona un entorno de servidor Web más inteligente y confiable

CAPÍTULO 7. IMPLEMENTACIÓN Y CONFIGURACIÓN DE IIS 6.0128

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.

7.1.1 Características Nuevas y Mejoras

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.

Confiabilidad y escalabilidad

CAPÍTULO 7. IMPLEMENTACIÓN Y CONFIGURACIÓN DE IIS 6.0129

Windows Server 2003 proporciona las características siguientes para obtener una confiabilidad y una escalabilidad mejoradas.

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.

Seguridad y capacidad de administración

CAPÍTULO 7. IMPLEMENTACIÓN Y CONFIGURACIÓN DE IIS 6.0130

Windows Server 2003 proporciona las características siguientes para obtener una seguridad y una escalabilidad mejoradas.

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.

Desarrollo y compatibilidad internacional mejorados

Windows Server 2003 proporciona las características siguientes para obtener un mejor desarrollo y compatibilidad internacional.

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 ganando 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.

7.2 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

CAPÍTULO 7. IMPLEMENTACIÓN Y CONFIGURACIÓN DE IIS 6.0132

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.

7.2.1 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.

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.

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.

Para poder discutir acerca de estos componentes, sería útil introducir dos nuevos conceptos de IIS 6.0:

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. Asi-

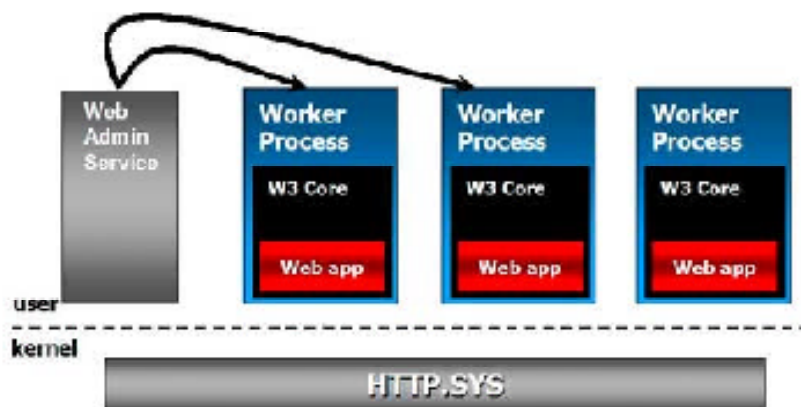


Figura 7.1: Descripción Gráfica del Worker Process.

mismo los aplicativos se pueden asignar fácilmente a otros Application Pool mientras que el servidor está funcionando.

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 autenticación 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.

En la figura 7.1 de la pagina 134 se describe gráficamente el funcionamiento de esta herramienta.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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).

7.3 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.

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.

Niveles múltiples de seguridad

- *No instalado por defecto en Windows Server 2003*

Mucha seguridad está sobre la reducción de la superficie del ataque de su

CAPÍTULO 7. IMPLEMENTACIÓN Y CONFIGURACIÓN DE IIS 6.0138

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 Group Policy*

Con Windows Server 2003, los administradores del dominio pueden 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.

7.3.1 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.

7.3.2 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.

7.3.3 Mejoras SSL

Hay tres mejoras principales en Secure Sockets Layer (SSL) de IIS 6.0. Estas son:

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.

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.

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.

7.3.4 Autorización y Autenticación

Si la autenticación 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 autenticación 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.

Integración de .NET Passport con IIS 6.0

La integración de .NET Passport con IIS 6.0 proporciona servicios de autenticación .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.

Capítulo 8

Seguridad: Nuevas funcionalidades en Windows Server 2003

8.1 Introducción a la Seguridad en Windows Server 2003

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 [2, BOSWELL].

8.1.1 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.

8.1.2 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.

8.1.3 Ventajas

Windows Server 2003 proporcionará una plataforma más segura y económica para la realización de actividades empresariales.

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.

8.1.4 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.

Windows Server 2003 proporciona muchas características nuevas y mejoradas que se combinan para crear una plataforma más segura para llevar a cabo actividades empresariales.

- *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:

- Servidor y cliente de VPN L2TP (Protocolo de túnel de capa 2)/IPSec.
 - Túneles L2TP/IPSec para conexiones VPN entre puertas de enlace.
 - Túneles IPSec para conexiones VPN entre puertas de enlace.
 - 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.

Mejoras en la seguridad de los sistemas Se han realizado importantes mejoras para garantizar una seguridad general de los sistemas, incluyendo:

- Mejoras del rendimiento en un 35 por ciento, al utilizar la capa de sockets segura (SSL).
- IIS no se instala de forma predeterminada. Para implementar IIS, primero debe instalarse mediante 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.

Windows Server 2003 facilitará la implementación de una infraestructura de claves públicas, junto con tecnologías asociadas como las tarjetas inteligentes.

- *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.

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.

- *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.

8.2 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 se 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.

Es importante recordar que se 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).

8.3 Usando Security Templates para Asegurar Computadoras

Se puede utilizar 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 se utilice dependerá del tamaño y las necesidades de seguridad de la organización. De esta manera, las 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 Se puede considerar el uso de Group Policy Objects (GPOS) para instalar políticas de seguridad.

8.3.1 Security Policy

Los Security Policies son una combinación de configuraciones de seguridad que afectan la seguridad de una computadora. Se 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.

Se 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. Se 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 auditoría.

Highly Secure (Hiccc*.inf)

Este Template aplica las configuraciones de seguridad más elevadas posibles. Para ello impone restricciones sobre los niveles de encriptación y el firmado de paquetes de datos sobre canales seguros y entre clientes y servidores sobre los paquetes Server Message Block (SMB).

8.3.2 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, se 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, se 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.

Bibliografía

- [1] Mark Walla Bob Williams. *The Ultimate Windows Server 2003 Systems Administrators Guide*. Addison and Wesley Professional, USA, 2003.
- [2] William Boswell. *Inside Windows Server 2003*. Addison and Wesley Professional, USA, 2003.
- [3] Jason Gerend Charlie Russel, Sharon Crawford. *Micrifoft Server 2003 Administrators Companion*. Microsoft Press, USA, 2003.
- [4] Mark Rouse Don Jones. *Micrifoft Server 2003 Delta Guide*. Que Publishing, USA, 2003.
- [5] Jerry Honeycutt. *Introducing Microsoft Windows Server 2003*. Microsoft Press, USA, 2003.
- [6] Kathy Ivens. *The Complete Reference: Windows Server 2003*. McGraw-Hill and Osborne Media, USA, 2003.
- [7] Brian Patterson Marcin Policht Scott Leathers Jeffrey Shapiro, Jim Boiyce. *Windows Server 2003 Bible*. John Wiley, USA, 2003.
- [8] Robert R. King. *Mastering Active Directory for Windows Server 2003*. Sybex, Incorporated, USA, 2003.
- [9] Michele Beveridge C. A. Callahan Lisa Justice Mark Minasi, Christa Anderson. *Mastering Windows Server 2003*. Sybex, Incorporated, USA, 2003.
- [10] Omar Droubi MichaelÑoel Rand Morimoto, Kenton Gardinier. *Micrifoft Windows Server 2003 Unleashed*. Sams Publishing, USA, 2003.

Índice de Materias

- Active Directory
 - Estructura Física, 57
 - Estructura Lógica, 55
 - Funcionalidad, 55
 - Introducción, 54
- DHCP
 - Direccionamiento, 29
 - Introducción, 28
- Funcionamiento DHCP
 - Lease Generation, 30
 - Lease Renewal, 31
- Group Policy
 - Conflicto, 84
 - Creación, 82
 - Herramientas, 81
 - Management Console
 - Instalación, 101
- Implementación IIS 6.0
 - Ventajas, 127
- Implementación IIS 6.0
 - Arquitectura, 132
 - Mejoras, 136
- Remote Desktop
 - Administración Remota, 117
 - Herramientas de Administración, 120
- Security Templates
 - Security Configuration, 151
 - Security Policy, 150
- Terminal Server
 - Funcionamiento, 108
 - Características, 110
 - Entorno de Usuario, 109
 - Instalación, 112
- WINDOWS 2000
 - Migración de
 - Dominios, 26
 - Members Server, 25
- WINDOWS 2003 SERVER
 - Características, 144
 - Funcionalidades, 142
 - Mejoras, 144
 - Personal Firewall, 149
 - Seguridad, 143
- WINDOWS NT 4.0
 - Migración de
 - Dominio, 24
 - Member Servers, 23
- WINDOWS SERVER
 - Características, 2
 - Funcionalidades, 9
 - Instalación y Migración, 12
 - introducción, 1
- Workgroup
 - Dominio, 15