

Universidad Politécnica de Valencia
Departamento de Sistemas Informáticos y Computación



Administración avanzada de Windows Server 2003

por
Fernando Ferrer García
Andrés Terrasa Barrena

Curso Académico 2007/2008
Valencia, 9 de junio de 2008

Administración avanzada de Windows Server 2003

Índice

1. El Sistema de Nombres de Dominio (DNS)	1
1.1. Funcionamiento de DNS	3
1.1.1. El espacio de nombres de dominio	3
1.1.2. El espacio de nombres de dominio en Internet	4
1.1.3. Delegación	4
1.1.4. Servidores de nombres y zonas	5
1.1.5. Resolución de nombres	6
1.2. Configuración de DNS	7
1.2.1. Registros de Recursos (RR)	7
1.2.2. Definición de la delegación	12
1.2.3. Tipos de zonas	12
1.2.4. Transferencias de zona	14
1.2.5. Actualizaciones dinámicas	15
2. Protección local en Windows 2003	17
2.1. Concepto de usuario	19
2.2. Grupos de Usuarios	20
2.3. El modelo de protección	22
2.4. Atributos de protección de los procesos	22
2.5. Derechos de usuario	23
2.5.1. Otras directivas de seguridad	24
2.6. Atributos de protección de los recursos	25
2.6.1. Asociación de permisos a recursos	26
2.6.2. Permisos estándar e individuales	27
2.6.3. Modificación de atributos de protección	30
2.7. Reglas de protección	31
3. Administración de dominios Windows 2003	33
3.1. Introducción	35
3.2. El Directorio Activo	35
3.2.1. Dominios Windows 2003 y el Directorio Activo	35
3.2.2. Estándares relacionados	36
3.2.3. El Directorio Activo y DNS	37
3.2.4. Estructura lógica	38
3.2.5. Estructura física	46
3.3. Objetos que administra un dominio	50
3.3.1. Usuarios globales	50
3.3.2. Grupos	51
3.3.3. Equipos	53
3.3.4. Unidades Organizativas	54
3.4. Compartición de recursos	54

3.4.1. Permisos y derechos	54
3.4.2. Compartición dentro de un dominio	55
3.4.3. Mandatos Windows 2003 para compartir recursos	56
3.5. Delegación de la administración	57
4. Administración de Políticas de Grupo	59
4.1. Introducción	61
4.2. Objeto de Política de Grupo (GPO)	61
4.3. Aplicación de Políticas de Grupo	63
4.4. Políticas de Grupo y grupos de seguridad	65
4.4.1. Filtrar el ámbito de aplicación de un GPO	65
4.4.2. Delegar la administración de un GPO	65
4.5. Principales políticas incluidas en un GPO	66
4.5.1. Plantillas administrativas	67
4.5.2. Configuraciones de seguridad	68
4.5.3. Instalación de software	68
4.5.4. Guiones (Scripts)	69
4.5.5. Redirección de carpetas	70
4.5.6. Otras políticas	70
4.6. Recomendaciones de uso	70
5. Servicios del sistema	73
5.1. Introducción	75
5.2. Servicios	75
5.2.1. Tipo de inicio de un servicio	76
5.2.2. Dependencias entre servicios	77
5.2.3. Recuperación de un servicio	77
5.3. Solucionando problemas	79
6. El servicio DHCP en Windows 2003	81
6.1. El protocolo DCHP	83
6.2. Concesión y renovación	84
6.3. Concepto de ámbito	86
6.3.1. Administración de ámbitos	86
6.3.2. Intervalos de exclusión	87
6.3.3. Reservas	88
6.3.4. Eliminación de concesiones	89
6.4. Administración de opciones DHCP	89
6.5. Autorización de un servidor DHCP	90
6.6. DHCP y DNS	91
7. Seguridad IP y VPN's	93
7.1. IPSEC	95
7.1.1. Ataques a la seguridad	96
7.1.2. Características de seguridad de IPSEC	97
7.1.3. Componentes de IPSEC	98
7.1.4. Configuración de directivas de IPSEC	99

7.1.5. Componentes de las reglas de seguridad	101
7.2. Fundamentos de las VPN's	103
7.2.1. Autenticación	103
7.2.2. Tunneling	104
7.2.3. Cifrado	104
7.3. Configuración de un servidor VPN	105
8. Internet Information Server	109
8.1. Introducción	111
8.1.1. HTTP: Hyper Text Transfer Protocol.	111
8.1.2. URI: Uniform Resource Identifiers.	112
8.1.3. HTML: HyperText Markup Language.	112
8.2. Características de IIS	113
8.3. Instalación de IIS	114
8.4. Administración de sitios Web	114
8.4.1. Creación de un sitio Web	115
8.4.2. Configuración de un sitio Web	119
8.4.3. Directorios Virtuales	120
8.4.4. Seguridad de un sitio Web	122
8.4.5. Copia de seguridad y restauración de la configuración	125
8.5. Programación Web en IIS 6	126
8.5.1. ASP y Python	126
9. Administración de discos	129
9.1. Geometría de los discos duros	131
9.1.1. Límites a la geometría de los discos IDE	131
9.1.2. Problemas causados por límites a la geometría IDE	134
9.1.3. Particiones del disco	135
9.2. La consola de administración de discos	137
9.2.1. Configuración de la consola	137
9.2.2. Discos básicos y dinámicos	138
9.2.3. Creación de particiones	139
9.2.4. Creación de volúmenes	142
9.3. Utilidades	145
9.3.1. Diskpart	145
9.4. Sistemas de ficheros	147
9.5. Cuotas de disco	148
9.5.1. Habilitar cuotas	148
9.5.2. Definición de cuotas individuales	149
9.6. Copias de seguridad	150
9.6.1. Carpetas y ficheros	150
9.6.2. Estado del sistema	151
10. El servicio DFS	153
10.1. Introducción	155
10.2. Tipos y características de DFS	156

10.3. Funcionamiento de DFS	157
10.3.1. Acceso a los recursos de un DFS	158
10.3.2. Replicación de DFS basado en dominio	160
10.3.3. Seguridad de DFS	160
10.4. Configuración de una raíz DFS	160
10.4.1. Configuración de una raíz DFS independiente	161
10.4.2. Configuración de una raíz DFS de dominio	161
10.5. Configuración de los vínculos DFS	162
10.6. Sistema de Replicación de Archivos (FRS)	163
10.6.1. Funcionamiento de FRS	163
10.6.2. Replicación de réplicas DFS	164
11. Recuperación ante desastres	165
11.1. El proceso de arranque de Windows 2003	167
11.1.1. La secuencia de arranque	167
11.1.2. La carga del sistema operativo	167
11.2. Solución de problemas en el proceso de arranque	168
11.2.1. Reparación de una instalación con los discos de arranque de Windows 2003	168
11.2.2. Menú de opciones avanzado	169
11.2.3. Creación de un disco de arranque	171
11.2.4. La consola de recuperación	172
11.3. Linux al rescate	175
11.4. Service Packs. Windows Updates	177
A. Nota Legal	179

Lista de figuras

4.1. Herramienta de configuración de un GPO	62
5.1. Utilidad Servicios de Windows 2003	75
5.2. Ficha Propiedades de un servicio	76
5.3. Interdependencias de servicios	77
5.4. Acciones de recuperación de un servicio	78
5.5. HKLM\SYSTEM\CurrentControlSet\Services	79
8.1. Asistente para componentes de Windows	114
8.2. Administrador de servicios de Interner snap-in	115
8.3. Descripción del sitio web	116
8.4. Dirección IP y configuración del puerto	117
8.5. Directorio particular	117
8.6. Permisos de acceso al sitio web	118
8.7. Propiedades Sitio web	119
8.8. Alias del directorio virtual	121
8.9. Ubicación del directorio	121
8.10. Permisos del directorio virtual	122
8.11. Seguridad en directorios	123
8.12. Métodos de autenticación	124
8.13. Restricciones de nombres de dominio y dirección IP	125

Lista de tablas

2.1. Principales derechos de usuario en Windows 2003	24
2.2. Permisos estándar sobre carpetas y archivos en Windows 2003	28
2.3. Permisos individuales en Windows 2003	29
2.4. Correspondencia entre permisos estándar e individuales en Windows 2003	30
4.1. Principales políticas que afectan el comportamiento de los scripts	69
9.1. Principales tipos de particiones	136

1

El Sistema de Nombres de Dominio (DNS)

Indice

1.1. Funcionamiento de DNS	3
1.1.1. El espacio de nombres de dominio	3
1.1.2. El espacio de nombres de dominio en Internet	4
1.1.3. Delegación	4
1.1.4. Servidores de nombres y zonas	5
1.1.5. Resolución de nombres	6
1.2. Configuración de DNS	7
1.2.1. Registros de Recursos (RR)	7
1.2.2. Definición de la delegación	12
1.2.3. Tipos de zonas	12
1.2.4. Transferencias de zona	14
1.2.5. Actualizaciones dinámicas	15

1.1. Funcionamiento de DNS

El *Domain Name System* (DNS) o Sistema de Nombres de Dominio permite a los usuarios de una red TCP/IP utilizar nombres jerárquicos y descriptivos para localizar fácilmente ordenadores (*hosts*) y otros recursos en dicha red, evitando de esta manera tener que recordar la dirección IP de cada ordenador al que se desea acceder. En esencia, DNS es una base de datos distribuida que contiene asociaciones de nombres simbólicos (de hosts) a direcciones IP. El hecho de que sea distribuida permite delegar el control sobre diferentes segmentos de la base de datos a distintas organizaciones, pero siempre de forma que los datos de cada segmento están disponibles en toda la red, a través de un esquema cliente-servidor.

Los programas denominados servidores de nombres (*name servers*) constituyen la parte servidora del esquema cliente-servidor. Los servidores de nombres contienen información sobre algunos segmentos de la base de datos y los ponen a disposición de los clientes, llamados solucionadores o *resolvers*.

1.1.1. El espacio de nombres de dominio

La base de datos distribuida de DNS está indexada por nombres de dominio. Cada nombre de dominio es esencialmente una trayectoria en un árbol invertido denominado *espacio de nombres de dominio*. La estructura jerárquica del árbol es similar a la estructura del sistema de ficheros UNIX. El árbol tiene una única raíz en el nivel superior llamada raíz (*root*). Cada nodo del árbol puede ramificarse en cualquier número de nodos de nivel inferior. La profundidad del árbol está limitada a 127 niveles.

Cada nodo en el árbol se identifica mediante una etiqueta no nula que puede contener hasta 63 caracteres, excepto el nodo raíz, identificado mediante una etiqueta nula. El nombre de dominio completo de cualquier nodo está formado por la secuencia de etiquetas que forman la trayectoria desde dicho nodo hasta la raíz, separando cada etiqueta de la siguiente mediante un punto. De esta forma, el nombre del nodo especifica de forma única su localización en la jerarquía. A este nombre de dominio completo o absoluto se le conoce como *nombre de dominio completamente cualificado* o *Fully Qualified Domain Name* (FQDN). Al ser nula la etiqueta que identifica el nodo raíz, el FQDN de cualquier nodo del árbol siempre acaba con un punto. La única restricción que se impone en el árbol de nombres es que los nodos hijos del mismo parent tengan etiquetas diferentes.

En el esquema jerárquico de nombres DNS, se denomina *dominio* a cualquier subárbol del espacio de nombres de dominio. De esta forma, cada dominio puede tener, a su vez, otros dominios. Generalmente, los hosts están representados por las hojas del árbol, aunque es posible nombrar a un host con una etiqueta correspon-

1.1.2. El espacio de nombres de dominio en Internet

diente a un nodo intermedio del árbol (en este caso, tendríamos un dominio y un nodo que se llaman igual).

La información sobre los nombres de dominio DNS se guarda mediante los denominados *registros de recursos* en los servidores DNS de la red. Concretamente, cada servidor DNS contiene los registros de recursos necesarios para responder a las consultas sobre la parte del espacio de nombres en la que tiene autoridad.

1.1.2. El espacio de nombres de dominio en Internet

El estándar DNS no impone muchas reglas sobre las etiquetas de los nombres de dominio, ni tampoco asocia un significado determinado a las etiquetas de un determinado nivel del espacio de nombres. Cuando manejamos una parte de este espacio, podemos decidir el significado y la sintaxis de nuestros nombres de dominio. Sin embargo, en el espacio de nombres Internet existente, se ha impuesto una estructura de nombres bien definida, especialmente en los dominios de primer nivel.

Los dominios originales de primer nivel dividían originalmente el espacio de nombres de Internet en siete dominios: com, edu, gov, mil, net, org, e int. Posteriormente, para acomodar el crecimiento y la internacionalización de Internet, se reservaron nuevos dominios de primer nivel que hacían referencia a países individuales.

Actualmente, los dominios originales se denominan *dominios de primer nivel genéricos* y han surgido nuevos nombres que se ajustan a los tiempos que corren.

1.1.3. Delegación

Es importante resaltar que el objetivo principal del diseño del sistema de nombres de dominio fue su administración descentralizada. Este objetivo se consigue a través de la *delegación*. La delegación de dominios funciona de forma parecida a la delegación de tareas en una organización. Un responsable de proyecto divide el proyecto en pequeñas tareas y asigna (delega) la responsabilidad de las mismas a diferentes empleados.

De la misma forma, una organización que administra un dominio puede dividirlo en subdominios. Cada subdominio puede ser delegado a diferentes organizaciones, lo cual implica que esa organización será responsable de mantener los datos (registros de recursos) de ese subdominio. Esa organización puede libremente cambiar los datos e incluso volver a dividir el dominio delegado en subdominios y delegarlos. El dominio padre solamente contiene enlaces a los responsables del subdominio delegado, de forma que pueda hacer referencia a ellos cuando se le planteen consultas sobre nombres en dicho subdominio delegado.

1.1.4. Servidores de nombres y zonas

Realmente, la subdivisión de un dominio en subdominios y la delegación de dichos subdominios son cosas distintas. En primer lugar, un dominio que tenga capacidad de autogestión (autoridad), siempre puede decidir subdividirse en diferentes subdominios, manteniendo él en principio la autoridad sobre todos ellos. Posteriormente, la organización que gestiona el dominio puede decidir además delegar la autoridad de algunos (o todos) sus subdominios en otras organizaciones. La delegación es una acción que siempre decide el dominio padre, y éste puede revocarla cuando desee, volviendo a retomar la autoridad sobre el subdominio que había delegado.

1.1.4. Servidores de nombres y zonas

Como se ha dicho anteriormente, los programas que almacenan información sobre el espacio de nombres de dominio se denominan servidores de nombres. En virtud de la delegación mencionada anteriormente, cada servidor de nombres posee generalmente información completa sobre una *parte contigua* del espacio de nombres (generalmente un dominio, potencialmente dividido en subdominios). Dicha parte del espacio se denomina *zona*, y se dice que el servidor de nombres tiene *autoridad* sobre ella. En realidad, un mismo servidor de nombres puede tener autoridad sobre múltiples zonas, y obtiene la información que describe la zona (los registros de recursos) o bien de un fichero local o bien de otro servidor de nombres.

Entender la diferencia entre una zona y un dominio es importante. Todos los dominios de primer nivel, y la mayoría de dominios de segundo nivel, se dividen en unidades más pequeñas y manejables gracias a la delegación. Estas unidades se denominan zonas y contienen una serie de registros almacenados en un servidor. Sin embargo, las zonas no son dominios. Un dominio es un subárbol del espacio de nombres, mientras que una zona es una parte del espacio de nombres DNS que se almacena generalmente en un fichero y que puede contener información sobre múltiples dominios.

DNS define dos tipos de servidores de nombres que mantienen información sobre el espacio de nombres: primarios (*maestros*) y secundarios (*esclavos*). Un servidor de nombres primario para una zona lee los datos de la zona desde un fichero que él mantiene. Un servidor de nombres secundario para una zona obtiene los datos de la zona desde otro servidor de nombres que es autoritario para la zona, llamado servidor maestro. Normalmente el servidor maestro es el servidor primario de la zona, pero esto no es un requisito ya que un servidor secundario puede cargar los datos desde otro secundario.

Cuando un servidor de nombres secundario se inicia, éste se pone en contacto con su servidor maestro y, si es necesario, inicia una transferencia de zona, es decir, una actualización de su información sobre la zona (ver Sección 1.2.4, “Transferencias

1.1.5. Resolución de nombres

de zona"). Además, periódicamente el servidor secundario contacta con el servidor maestro para ver si los datos de zona han cambiado. Tanto el servidor primario como el secundario poseen autoridad sobre la zona. Definir servidores secundarios proporciona tolerancia a errores y reduce la carga en el servidor primario de la zona.

1.1.5. Resolución de nombres

Los clientes DNS utilizan bibliotecas llamadas "solucionadores" (*resolvers*) que efectúan las consultas DNS a los servidores en nombre del cliente.

Los servidores de nombres son los expertos en obtener información del espacio de nombres de dominio. Es decir, no solamente responden los datos referentes a las zonas sobre los que tienen autoridad, sino que pueden también buscar información a través del espacio de nombres de dominio para encontrar datos sobre los que no son autoritarios. A este proceso se le denomina *resolución de nombres*. Por ese motivo, existen servidores de nombres que no mantienen información sobre ninguna zona, y únicamente sirven para responder consultas de los clientes (*resolvers*) sobre cualquier dominio. Este tipo de servidores DNS se denomina *cache only*.

Ya que el espacio de nombres está estructurado como un árbol invertido, un servidor de nombres necesita únicamente los nombres de dominio y las direcciones de los servidores de nombres raíz para encontrar cualquier punto en el árbol. Los servidores raíz conocen dónde se encuentran los servidores de nombres con autoridad para los dominios de primer nivel. De hecho, la mayoría de servidores raíz son autoritarios para los dominios de primer nivel genéricos.

Cuando se solicita una consulta a cualquier nombre de dominio, los servidores raíz pueden al menos proporcionar los nombres y direcciones de los servidores de nombres autoritarios para el dominio de primer nivel al que pertenece el nombre de dominio buscado. Y los servidores de nombres de primer nivel pueden proporcionar la lista de servidores de nombres autoritarios para el dominio de segundo nivel al que pertenece el nombre de dominio buscado. De esta forma, cada servidor de nombres consultado va proporcionando la información más próxima a la respuesta buscada, o proporciona la propia respuesta.

Como conclusión hay que resaltar la importancia que tienen los servidores de nombres raíz en el proceso de resolución. Por esta razón, el sistema de nombres de dominio proporciona mecanismos de caché para ayudar a reducir la carga que supondría el proceso de resolución sobre los servidores raíz. Si todos los servidores raíz de Internet fallaran por un largo período de tiempo, toda la resolución en Internet fallaría. Para protegerse, Internet posee 13 servidores de nombres raíz repartidos por diferentes partes de la Red.

1.2. Configuración de DNS

Los estándares de DNS no especifican la estructura de datos interna en que deben almacenarse los registros de recursos (registros de la base de datos DNS), y por tanto existen varias implementaciones que son diferentes en este sentido. Por regla general, los servidores guardan la información sobre las zonas en ficheros en texto plano sin formato. Los nombres de los archivos son arbitrarios y se especifican en la configuración del servidor DNS.

Por ejemplo, en la implementación habitual de DNS en el mundo UNIX, denominada BIND (*Berkeley Internet Name Domain*), se utiliza los nombres de archivo siguientes para almacenar los registros de cada zona:

- Db.nombre_de_zona: zona de resolución directa.
- Db.identificador_de_red: zona de resolución inversa.
- Db.cache: sugerencias de servidores raíz.
- Db.127.0.0.1: resolución inversa de bucle cerrado.

Sin embargo, la configuración predeterminada del servidor DNS de Microsoft Windows 2000 no utiliza los mismos nombres de archivo que BIND, sino que usa la nomenclatura nombre_zona.dns. Por otra parte, Windows 2000 permite que la base de datos DNS se integre en la base de datos del Directorio Activo, en cuyo caso dicha información participa de los mismos mecanismos de almacenamiento y replicación que el resto de información contenida en dicho servicio de directorio.

1.2.1. Registros de Recursos (RR)

Para resolver nombres, los servidores consultan sus zonas. Las zonas contienen *registros de recursos* que constituyen la información de recursos asociada al dominio DNS. Por ejemplo, ciertos registros de recursos asignan nombres descriptivos a direcciones IP, otros establecen quienes son los servidores de nombres de la zona, etc.

El formato de cada registro de recursos es el siguiente:

Propietario	TTL	Clase	Tipo	RDATA
-------------	-----	-------	------	-------

donde:

- **Propietario:** nombre de *host* (ordenador) o del dominio DNS al que pertenece este recurso. Puede contener:

1.2.1. Registros de Recursos (RR)

1. un nombre de host o de dominio, completamente cualificados o no (cualquier nombre que no acaba en un punto se considera *relativo* a la zona que se está describiendo),
 2. el símbolo "@" (que representa el nombre de la zona que se está describiendo), o
 3. una cadena vacía (en cuyo caso equivale al propietario del registro de recursos inmediatamente anterior).
- **TTL**(*Time To Live*): Tiempo de vida, generalmente expresado en segundos, que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla. Este campo es opcional. También se puede expresar mediante letras indicando días (d), horas (h), minutos (m) y segundos (s). Por ejemplo: "2h30m".
 - **Clase**: define la familia de protocolos en uso. Suele ser siempre "IN", que representa Internet.
 - **Tipo**: identifica el tipo de registro.
 - **RDATA** : los datos del registro de recursos.

Las siguientes secciones describen los principales tipos de registros de recursos: SOA, NS, A, PTR, CNAME, MX y SRV.

1.2.1.1. Registro de Recurso SOA

Cada zona contiene un registro de recursos denominado Inicio de Autoridad o SOA (*Start Of Authority*) al comienzo de la zona. Los registros SOA incluyen los siguientes campos (sólo se incluyen los que poseen un significado específico para el tipo de registro):

- **Propietario**: nombre de dominio de la zona.
- **Persona responsable**: contiene la dirección de correo electrónico del responsable de la zona. En esta dirección de correo, se utiliza un punto en el lugar del habitual símbolo "@".
- **Número de serie**: muestra el número de versión de la zona, es decir, un número que sirve de referencia a los servidores secundarios de la zona para saber cuándo deben proceder a una actualización de su base de datos de la zona (o *transferencia de zona*). Cuando el número de serie del servidor secundario sea *menor* que el número del maestro, esto significa que el maestro ha cambiado la zona, y por tanto el secundario debe solicitar al maestro una transferencia de zona. Por tanto, este

1.2.1. Registros de Recursos (RR)

número debe ser incrementado (manualmente) por el administrador de la zona cada vez que realiza un cambio en algún registro de la zona (en el servidor maestro).

- **Actualización:** muestra cada cuánto tiempo un servidor secundario debe ponerse en contacto con el maestro para comprobar si ha habido cambios en la zona.
- **Reintentos:** define el tiempo que el servidor secundario, después de enviar una solicitud de transferencia de zona, espera para obtener una respuesta del servidor maestro antes de volverlo a intentar.
- **Caducidad:** define el tiempo que el servidor secundario de la zona, después de la transferencia de zona anterior, responderá a las consultas de la zona antes de descartar la suya propia como no válida.
- **TTL mínimo:** este campo especifica el tiempo de validez (o de vida) de las respuestas "negativas" que realiza el servidor. Una respuesta negativa significa que el servidor contesta que un registro no existe en la zona.

Hasta la versión 8.2 de BIND, este campo establecía el tiempo de vida por defecto de todos los registros de la zona que no tuvieran un campo TTL específico. A partir de esta versión, esto último se consigue con una *directiva* que debe situarse al principio del fichero de la zona. Esta directiva se especifica así:

```
$TTL tiempo
```

Por ejemplo, un tiempo de vida por defecto de 30 minutos se establecería así:

```
$TTL 30m
```

Un ejemplo de registro SOA sería el siguiente:

```
admon.com. IN SOA pc0100.admon.com hostmaster.admon.com.  
(  
    1           ; número de serie  
    3600        ; actualización 1 hora  
    600         ; reintentar 10 minutos  
    86400       ; caducar 1 día  
    60          ; TTL (negativo) 1 minuto  
)
```

1.2.1.2. Registro de Recurso NS

El registro de recursos NS (*Name Server*) indica los servidores de nombres autoriza-

1.2.1. Registros de Recursos (RR)

dos para la zona. Cada zona debe contener registros indicando tanto los servidores principales como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

Por otra parte, estos registros también se utilizan para indicar quiénes son los servidores de nombres con autoridad en subdominios delegados, por lo que la zona contendrá al menos un registro NS por cada subdominio que haya delegado.

Ejemplos de registros NS serían los siguientes:

```
admon.com.           IN   NS   pc0100.admon.com.  
valencia.admon.com. IN   NS   pc0102.valencia.admon.com.
```

1.2.1.3. Registro de Recurso A

El tipo de registro de recursos A (*Address*) asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre de host dado.

Un ejemplo de registro A que asignaría la dirección IP 158.42.178.1 al nombre de dominio pc0101.valencia.admon.com., sería el siguiente:

```
pc0101.valencia.admon.com.     IN   A   158.42.178.1
```

1.2.1.4. Registro de Recurso PTR

El registro de recursos PTR (*PointeR*) o puntero, realiza la acción contraria al registro de tipo A, es decir, asigna un nombre de dominio completamente cualificado a una dirección IP. Este tipo de recursos se utilizan en la denominada *resolución inversa*, descrita en Sección 1.1.4, “Servidores de nombres y zonas”.

Un ejemplo de registro PTR que asignaría el nombre pc0101.valencia.admon.com. a la dirección IP 158.42.178.1 sería el siguiente:

```
1.178.42.158.in-addr.arpa.    IN   PTR   pc0101.admon.valencia.com.
```

1.2.1.5. Registro de Recurso CNAME

El registro de nombre canónico (CNAME, *Canonical NAME*) crea un alias (un sinónimo) para el nombre de dominio especificado.

Un ejemplo de registro CNAME que asignaría el alias controlador al nombre de dominio pc0102.valencia.admon.com, sería el siguiente:

1.2.1. Registros de Recursos (RR)

```
controlador.valencia.admon.com.  
IN      CNAME    pc0101.valencia.admon.com.
```

1.2.1.6. Registro de Recurso MX

El registro de recurso de intercambio de correo (MX, *Mail eXchange*) especifica un servidor de intercambio de correo para un nombre de dominio. Puesto que un mismo dominio puede contener diferentes servidores de correo, el registro MX puede indicar un valor numérico que permite especificar el orden en que los clientes deben intentar contactar con dichos servidores de correo.

Un ejemplo de registro de recurso MX que define al servidor pc0100 como el servidor de correo del dominio admon.com, sería el siguiente:

```
admon.com.      IN      MX      0      pc0100.admon.com.
```

1.2.1.7. Registro de Recurso SRV

Con registros MX se puede especificar varios servidores de correo en un dominio DNS. De esta forma, cuando un proveedor de servicio de envío de correo necesite enviar correo electrónico a un host en el dominio, podrá encontrar la ubicación de un servidor de intercambio de correo. Sin embargo, esta no es la forma de resolver los servidores que proporcionan otros servicios de red como WWW o FTP.

Los registros de recurso de servicio (SRV, *SeRVice*) permiten especificar de forma genérica la ubicación de los servidores para un servicio, protocolo y dominio DNS determinados.

El formato de un registro SRV es el siguiente:

```
servicio.protocolo.nombre TTL clase SRV  
prioridad peso puerto destino
```

donde:

- **Servicio:** especifica el nombre de servicio: http, telnet, etc.
- **Protocolo:** especifica el protocolo utilizado: TCP o UDP.
- **Nombre:** define el nombre de dominio al que hace referencia el registro de recurso SRV.

1.2.2. Definición de la delegación

- **TTL** y **clase** ha sido definidos anteriormente.
- **Prioridad**: especifica el orden en que los clientes se pondrán en contacto con los servidores: los clientes intentarán ponerse en contacto primero con el host que tenga el valor de prioridad más bajo, luego con el siguiente y así sucesivamente.
- **Peso**: es un mecanismo de equilibrio de carga.
- **Puerto**: muestra el puerto del servicio en el host.
- **Destino**: muestra el nombre de dominio completo para la máquina compatible con ese servicio.

Un ejemplo de registros SRV para los servidores Web del dominio `admon.com.`, sería:

```
http.tcp.admon.com. IN SRV 0 0 80 www1.admon.com.  
http.tcp.admon.com. IN SRV 10 0 80 www2.admon.com.
```

1.2.2. Definición de la delegación

Para que una zona especifique que uno de sus subdominios está delegado en una zona diferente, es necesario agregar un *registro de delegación* y, generalmente, el denominado "registro de pegado" (*glue record*). El registro de delegación es un registro NS en la zona principal (padre) que define el servidor de nombres autorizado para la zona delegada. El registro de pegado es un registro tipo A para el servidor de nombres autorizado para la zona delegada, y es necesario cuando el servidor de nombres autorizado para la zona delegada también es un miembro de ese dominio (delegado).

Por ejemplo, si la zona `admon.com` deseara delegar la autoridad a su subdominio `valencia.admon.com`, se deberían agregar los siguientes registros al archivo de configuración correspondiente de la zona `admon.com`:

```
valencia.admon.com. IN NS pc0102.valencia.admon.com.  
pc0102.valencia.admon.com. IN A 158.42.178.2
```

1.2.3. Tipos de zonas

Aunque distintas implementaciones de DNS difieren en cómo configurar las zonas, generalmente existe un fichero que indica sobre qué zonas tiene autoridad el servidor, indicando para cada una el fichero que contiene la información de dicha zona

1.2.3. Tipos de zonas

(si el servidor es primario para la zona), o la dirección del servidor maestro a quien preguntar por ella (si es secundario).

En general, existen tres tipos distintos de zonas: zonas de búsqueda directa, zonas de búsqueda inversa y zonas de "sugerencia raíz". Un servidor DNS puede tener autoridad sobre varias zonas directas e inversas, y necesita poseer información sobre las "sugerencias raíz" si desea responder a sus clientes sobre registros de zonas sobre las que no posee autoridad. A continuación se describe cada tipo brevemente.

1.2.3.1. Zona de búsqueda directa

Las zonas de búsqueda directa contienen la información necesaria para resolver nombres en el dominio DNS. Deben incluir, al menos, registros SOA y NS, y pueden incluir cualquier otro tipo de registros de recurso, excepto el registro de recursos PTR.

1.2.3.2. Zona de búsqueda inversa

Las zonas de búsqueda inversa contienen información necesaria para realizar las búsquedas inversas. La mayor parte de las consultas proporcionan un nombre y solicitan la dirección IP que corresponde a ese nombre. Este tipo de consulta es el descrito en la zona de resolución directa.

Pero existen ocasiones en que un cliente ya tiene la dirección IP de un equipo y desea determinar el nombre DNS de ese equipo. Esto es importante para los programas que implementan la seguridad basándose en el FQDN que se conecta y también se utiliza para la solución de problemas de red TCP/IP.

Si el único medio de resolver una búsqueda inversa es realizar una búsqueda detallada de todos los dominios en el espacio de nombres DNS, la búsqueda de consulta inversa sería demasiado exhaustiva como para realizarla de forma práctica.

Para solucionar este problema se creó un dominio DNS especial para realizar búsquedas "inversas", denominado `in-addr.arpa.`. Este dominio utiliza un orden inverso de números en la notación decimal de las direcciones IP. Con esta disposición se puede delegar la autoridad de miembros inferiores del dominio `in-addr.arpa.` a las distintas organizaciones, a medida que se les asigna identificadores de red de clase A, B o C.

1.2.3.3. Sugerencias de los servidores del Dominio Raíz

El archivo de "sugerencias raíz" (*root hint*), denominado también archivo de sugerencias de caché, contiene la información de host necesaria para resolver nombres fuera

1.2.4. Transferencias de zona

de los dominios en los que el servidor posee autoridad. En concreto, este archivo contiene los nombres y las direcciones IP de los servidores DNS del dominio punto (.) o raíz.

1.2.4. Transferencias de zona

En aquellas zonas en las que existen diferentes servidores de nombres con autoridad (uno principal o maestro y uno o varios secundarios o esclavos), cada vez que se realizan cambios en la zona del servidor maestro, estos cambios deben replicarse a todos los servidores secundarios de esa zona. Esta acción se lleva a cabo mediante un mecanismo denominado transferencia de zona. Existen dos tipos de transferencia de zonas: completa e incremental.

1.2.4.1. Transferencia completa de zona

En una transferencia completa de zona, el servidor maestro para una zona transmite toda la base de datos de zona al servidor secundario para esa zona.

Los servidores secundarios siguen los siguientes pasos a la hora de realizar una transferencia de zona:

1. El servidor secundario para la zona espera el tiempo especificado en el campo Actualizar del registro SOA y luego le pregunta al servidor maestro por su registro SOA.
2. El servidor maestro responde con su registro SOA.
3. El servidor secundario para la zona compara el número de serie devuelto con su propio número y si este es mayor que el suyo, solicita una transferencia de zona completa.
4. El servidor maestro envía la base de datos de la zona completa al servidor secundario.

Si el servidor maestro no responde, el servidor secundario lo seguirá intentando después del intervalo especificado en el campo Reintentos del registro SOA. Si todavía no hay respuesta después del intervalo que se especifica en el campo Caduca desde la última transferencia de zona, este descarta su zona.

1.2.4.2. Transferencia incremental de zona

Las transferencias completas de zona pueden consumir gran ancho de banda de la red. Para poder solucionar este problema se define la transferencia incremental de

1.2.5. Actualizaciones dinámicas

zona, en la cual sólo debe transferirse la parte modificada de una zona.

La transferencia incremental de zona funciona de forma muy similar a la transferencia completa. En este caso, el servidor secundario para la zona comprueba el número de serie del registro SOA del maestro con el suyo, para determinar si debe iniciar una transferencia de zona, la cual en este caso sería incremental (sólo de los cambios realizados).

1.2.4.3. Notificación DNS

Con este proceso se pretende que el servidor maestro para la zona notifique los cambios a ciertos servidores secundarios y de esta manera los secundarios podrán comprobar si necesitan iniciar una transferencia de zona. De esta forma se mejora la coherencia de los datos mantenida por todos los servidores secundarios.

1.2.5. Actualizaciones dinámicas

Originalmente, DNS se diseñó para que solamente admitiera cambios estáticos. De esta forma, sólo el administrador del sistema DNS podía agregar, quitar o modificar los registros de recursos, realizando cambios manuales sobre los ficheros de configuración correspondientes.

El sistema de actualizaciones dinámicas, permite que el servidor principal para la zona pueda configurarse de forma que acepte actualizaciones de recursos enviadas desde otros equipos (habitualmente, sus clientes DNS). Este es el sistema preferido en el caso de Windows 2000, aunque muchos administradores de DNS lo desaconsejan por razones de seguridad.

Por ejemplo, el servidor maestro puede admitir (e incluir en su configuración) actualizaciones de registros A y PTR de las estaciones de trabajo de su dominio, que le envían esa información cuando arrancan. También sería posible recibir estas actualizaciones de un servidor DHCP, una vez ha proporcionado la configuración IP a un cliente.

2

Protección local en Windows 2003

Índice

2.1. Concepto de usuario	19
2.2. Grupos de Usuarios	20
2.3. El modelo de protección	22
2.4. Atributos de protección de los procesos	22
2.5. Derechos de usuario	23
2.5.1. Otras directivas de seguridad	24
2.6. Atributos de protección de los recursos	25
2.6.1. Asociación de permisos a recursos	26
2.6.2. Permisos estándar e individuales	27
2.6.3. Modificación de atributos de protección	30
2.7. Reglas de protección	31

2.1. Concepto de usuario

Como muchos otros sistemas operativos, Windows 2003 permite tener un riguroso control de las personas que pueden entrar en el sistema y de las acciones que dichas personas están autorizadas a ejecutar.

Windows 2003 denomina *usuario* a cada persona que puede entrar en el sistema. Para poder controlar la entrada y las acciones de cada usuario utiliza básicamente el concepto de *cuenta de usuario* (*user account*). Una cuenta de usuario almacena toda la información que el sistema guarda acerca de cada usuario. De entre los numerosos datos que Windows 2003 almacena en cada cuenta de usuario, los más importantes son los siguientes:

- **Nombre de usuario.** Es el nombre mediante el cual el usuario *se identifica* en el sistema. Cada usuario ha de tener un nombre de usuario distinto para que la identificación sea unívoca.
- **Nombre completo.** Es el nombre completo del usuario.
- **Contraseña.** Palabra cifrada que permite *autenticar* el nombre de usuario. En Windows 2003 la contraseña distingue entre mayúsculas y minúsculas. Sólo los usuarios que se identifican y autentican positivamente pueden ser *autorizados* a conectarse al sistema.
- **Directorio de conexión.** Es el lugar donde (en principio) residirán los archivos personales del usuario. El directorio de conexión de cada usuario es privado: ningún otro usuario puede entrar en él, a menos que su propietario conceda los permisos adecuados.
- **Horas de conexión.** Se puede controlar a qué horas un usuario puede conectarse para trabajar en el sistema. Inclusive se puede especificar un horario distinto para cada día de la semana.
- **Activada.** Esta característica permite inhabilitar temporalmente una cuenta. Una cuenta desactivada sigue existiendo, pero no puede ser utilizada para acceder al sistema, ni siquiera conociendo su contraseña.

Existe un dato especial que se asocia a cada cuenta, pero que a diferencia de todos los expuestos arriba, no puede ser especificado manualmente cuando se da de alta la cuenta. Se trata del **identificador seguro** (*Secure Identifier*, o SID). Este identificador es interno y el sistema lo genera automáticamente cuando se crea una nueva cuenta. Además, los SIDs se generan de tal forma que se asegura que no pueden

existir dos iguales en todas las instalaciones de Windows 2003 del mundo (son identificadores únicos). Windows 2003 utiliza siempre el SID (y no el nombre de usuario) para controlar si un usuario tiene o no permisos suficientes para llevar a cabo cualquiera de sus acciones. La ventaja de este modelo es que el SID es un dato completamente interno del sistema operativo, es decir, ningún usuario puede establecerlo en ningún sitio (ni siquiera el administrador del sistema). Por tanto, nadie puede obtener un mayor grado de privilegio intentando *suplantar* la identidad de otro usuario.

Cuando en un equipo se instala Windows 2003, existen de entrada las cuentas de dos usuarios integrados (*built-in users*): el Administrador y el Invitado. El primero es un usuario especial, el único que en principio posee lo que se denominan derechos administrativos en el sistema. Es decir, tiene la potestad de administrar el sistema en todos aquellos aspectos en que éste es configurable: usuarios, grupos de usuarios, contraseñas, recursos, derechos, etc. La cuenta de Administrador no puede ser borrada ni desactivada. Por su parte, la cuenta de Invitado es la que utilizan normalmente aquellas personas que no tienen un usuario propio para acceder al sistema. Habitualmente esta cuenta no tiene contraseña asignada, puesto que se supone que el nivel de privilegios asociado a ella es mínimo. En cualquier caso, el Administrador puede desactivarla si lo considera oportuno.

2.2. Grupos de Usuarios

La información de seguridad almacenada en una cuenta de usuario es suficiente para establecer el grado libertad (o de otro modo, las restricciones) que cada usuario debe poseer en el sistema. Sin embargo, resultaría muchas veces tedioso para el administrador determinar dichas restricciones usuario por usuario, especialmente en sistemas con un elevado número de ellos. El concepto de *grupo de usuarios* permite agrupar de forma lógica a los usuarios de un sistema, y establecer permisos y restricciones a todo el grupo de una vez. De forma análoga a las cuentas de usuario, una cuenta de grupo posee un nombre y un identificador interno o SID, además de una lista de los usuarios que pertenecen a dicho grupo.

La administración de la protección del sistema mediante grupos de usuarios es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales, ya que un usuario puede pertenecer a tantos grupos como sea necesario, obteniendo implícitamente la *suma* de los permisos asignados a todos ellos. Considerese, por ejemplo, que en una empresa un sistema es utilizado por empleados de distinto rango, y que cada rango posee un distinto nivel de privilegios. Supongamos que se desea cambiar de rango a un empleado, debido a un ascenso, por ejemplo. Si la seguridad estuviera basada en usuarios individuales, cambiar los privilegios de este usuario adecuadamente supondría modificar sus privilegios en cada lugar del sistema en que estos debieran cambiar (con el consiguiente trabajo, y el riesgo de olvidar alguno). Por el contrario, con la administración de seguridad basada en gru-

2.2. Grupos de Usuarios

pos, esta operación sería tan sencilla como cambiar al usuario de un grupo a otro. Por ello, en Windows 2003 se recomienda que los permisos se asignen en base a *grupos*, y no en base a usuarios individuales.

Al igual que existen usuarios integrados, en todo sistema 2003 existen una serie de grupos integrados (*built-in groups*): Administradores, Operadores de Copia, Usuarios Avanzados, Usuarios, e Invitados. El grupo Administradores recoge a todos aquellos usuarios que deban poseer derechos administrativos completos. Inicialmente posee un solo usuario, el Administrador. De igual forma, el grupo Invitados posee al Invitado como único miembro. Los otros tres grupos están vacíos inicialmente. Su uso es el siguiente:

- **Usuarios.** Son los usuarios normales del sistema. Tienen permisos para conectarse al sistema interactivamente y a través de la red.
- **Operadores de copia.** Estos usuarios pueden hacer (y restaurar) una copia de todo el sistema.
- **Usuarios avanzados.** Son usuarios con una cierta capacidad administrativa. Se les permite cambiar la hora del sistema, crear cuentas de usuario y grupos, compartir ficheros e impresoras, etc.

El Administrador, al ir creando las cuentas de los usuarios, puede hacer que cada una pertenezca al grupo (o grupos) que estime conveniente. Asimismo, puede crear nuevos grupos que refinen esta estructura inicial, conforme a las necesidades particulares de la organización donde se ubique el sistema.

Finalmente, Windows 2003 define una serie de grupos especiales, cuyos (usuarios) miembros no se establecen de forma manual, sino que son determinados de forma dinámica y automática por el sistema. Estos grupos se denominan genéricamente identidades especiales (*special identities*) y se utilizan normalmente para facilitar la labor de establecer la protección del sistema. De entre estos grupos, destacan:

- **Usuarios Interactivos (Interactive).** Este grupo representa a todos aquellos usuarios que tienen el derecho de iniciar una sesión local en la máquina.
- **Usuarios de Red (Network).** Bajo este nombre se agrupa a todos aquellos usuarios que tienen el derecho de acceder al equipo desde la red.
- **Todos (Everyone).** Agrupa a todos los usuarios que el sistema conoce. Puede agrupar a usuarios existentes localmente y de otros sistemas (conectados a través de la red). A partir de Windows 2003, este grupo no incluye las conexiones anónimas.

nimas (sin aportar usuario y contraseña).

- **Usuarios autenticados** (*Authenticated Users*). Agrupa a todos los usuarios que poseen una cuenta propia para conectarse al sistema. Por tanto, aquellos usuarios que se hayan conectado al sistema utilizando la cuenta de "invitado" pertenecen a "Todos" pero no a "Usuarios autenticados".

2.3. El modelo de protección

El modelo de protección de Windows 2003 establece la forma en que el sistema lleva a cabo el *control de acceso* de cada usuario y grupo de usuarios. En otras palabras, es el modelo que sigue el sistema para establecer las acciones que un usuario (o grupo) está autorizado a llevar a cabo. Este modelo está basado en la definición y contrastación de ciertos *atributos de protección* que se asignan a los procesos de usuario por un lado, y al sistema y sus recursos por otro. En el caso del sistema y sus recursos, Windows 2003 define dos conceptos distintos y complementarios: el concepto de *derecho* y el concepto de *permiso*, respectivamente.

Un *derecho* o *privilegio* de usuario (*user right*) es un atributo de un usuario (o grupo) que le permite realizar una acción que afecta al sistema en su conjunto (y no a un objeto o recurso en concreto). Existe un conjunto fijo y predefinido de derechos en Windows 2003. Para determinar qué usuarios poseen qué derechos, cada derecho posee una lista donde se especifican los grupos/usuarios que tienen concedido este derecho.

Un *permiso* (*permission*) es una característica de cada *recurso* (carpeta, archivo, impresora, etc.) del sistema, que concede o deniega el acceso al mismo a un usuario/grupo concreto. Cada recurso del sistema posee una lista en la que se establece qué usuarios/grupos pueden acceder a dicho recurso, y también qué tipo de acceso puede hacer cada uno (lectura, modificación, ejecución, borrado, etc.).

En los apartados siguientes se detallan los atributos de protección de los procesos de usuario (Sección 2.4, “Atributos de protección de los procesos”), los derechos que pueden establecerse en el sistema (Sección 2.5, “Derechos de usuario”) y los atributos de protección que poseen los recursos (Sección 2.6, “Atributos de protección de los recursos”). La Sección 2.7, “Reglas de protección” establece las reglas concretas que definen el control de acceso de los procesos a los recursos.

2.4. Atributos de protección de los procesos

Cuando un usuario es autorizado a conectarse interactivamente a un sistema Windows 2003, el sistema construye para él una acreditación denominada *Security Ac-*

cess Token o SAT. Esta acreditación contiene la información de protección del usuario, y Windows 2003 la incluye en los procesos que crea para dicho usuario. De esta forma, los *atributos de protección* del usuario están presentes en cada proceso del usuario, y se utilizan para controlar los accesos que el proceso realiza a los recursos del sistema en nombre de dicho usuario.

En concreto, el SAT contiene los siguientes atributos de protección:

1. **SID.** El identificador único del usuario.
2. **SIDs de sus grupos.** Lista de los SIDs de los grupos a los que pertenece el usuario.
3. **Derechos.** Lista de derechos del usuario. Esta lista se construye mediante la inclusión de todos los derechos que el usuario tiene otorgados por sí mismo o por los grupos a los que pertenece (ver Sección 2.5, “Derechos de usuario”).

Esta forma de construir la acreditación introduce ya una de las máximas de la protección de Windows 2003: el nivel de acceso de un usuario incluye implícitamente los niveles de los grupos a los que pertenece.

2.5. Derechos de usuario

Un *derecho* es un atributo de un usuario o grupo de usuarios que le confiere la posibilidad de realizar una acción concreta sobre el sistema en conjunto (no sobre un recurso concreto). Como hemos visto, la lista de derechos de cada usuario se añade explícitamente a la acreditación (SAT) que el sistema construye cuando el usuario se conecta al sistema. Esta lista incluye los derechos que el usuario tiene concedidos a título individual más los que tienen concedidos todos los grupos a los que el usuario pertenece.

Windows 2003 distingue entre dos tipos de derechos: los *derechos de conexión (logon rights)* y los *privilegios (privileges)*. Los primeros establecen las diferentes formas en que un usuario puede conectarse al sistema (de forma interactiva, a través de la red, etc.), mientras que los segundos hacen referencia a ciertas acciones predefinidas que el usuario puede realizar una vez conectado al sistema. La Tabla 2.1, “Principales derechos de usuario en Windows 2003” presenta los derechos más destacados de cada tipo, junto con su descripción.

Es importante hacer notar lo siguiente: cuando existe un conflicto entre lo que concede o deniega un permiso y lo que concede o deniega un derecho, este último tiene prioridad. Por ejemplo: los miembros del grupo Operadores de Copia poseen el derecho de realizar una copia de seguridad de todos los archivos del sistema. Es

2.5.1. Otras directivas de seguridad

posible (y muy probable) que existan archivos sobre los que no tengan ningún tipo de permiso. Sin embargo, al ser el derecho más prioritario, podrán realizar la copia sin problemas. De igual forma, el administrador tiene el derecho de tomar posesión de cualquier archivo, inclusive de aquellos archivos sobre los que no tenga ningún permiso. Es decir, como regla general, los derechos y privilegios siempre prevalecen ante los permisos particulares de un objeto, en caso de que haya conflicto.

Tabla 2.1. Principales derechos de usuario en Windows 2003

DERECHOS DE CONEXIÓN	
Nombre	Significado
Acceder a este equipo desde la red	Permite/impide al usuario conectar con el ordenador desde otro ordenador a través de la red.
Inicio de sesión local	Permite/impide al usuario iniciar una sesión local en el ordenador, desde el teclado del mismo.
PRIVILEGIOS	
Nombre	Significado
Añadir estaciones al dominio	Permite al usuario añadir ordenadores al dominio actual.
Hacer copias de seguridad	Permite al usuario hacer copias de seguridad de archivos y carpetas.
Restaurar copias de seguridad	Permite al usuario restaurar copias de seguridad de archivos y carpetas.
Atravesar carpetas	Permite al usuario acceder a archivos a los que tiene permisos a través de una ruta de directorios en los que puede no tener ningún permiso.
Cambiar la hora del sistema	Permite al usuario modificar la hora interna del ordenador.
Instalar manejadores de dispositivo	Permite al usuario instalar y desinstalar manejadores de dispositivos <i>Plug and Play</i> .
Apagar el sistema	Permite al usuario apagar el ordenador local.
Tomar posesión de archivos y otros objetos	Permite al usuario tomar posesión (hacerse propietario) de cualquier objeto con atributos de seguridad del sistema (archivos, carpetas, objetos del Directorio Activo, etc.).

2.5.1. Otras directivas de seguridad

En Windows 2003, los derechos son un tipo de *directivas de seguridad*. En este sentido, Windows 2003 ha agrupado un conjunto de reglas de seguridad que en versiones anteriores de NT estaban dispersas en distintas herramientas administrativas, y las ha incorporado a una consola de administración única denominada *directivas de seguridad local*).

2.6. Atributos de protección de los recursos

Dentro de esta herramienta de administración podemos establecer, entre otras, los siguientes tipos de reglas de seguridad para el equipo local:

1. **Cuentas.** En este apartado podemos establecer cuál es la *política de cuentas* o de contraseñas que sigue el equipo para sus usuarios locales. Dentro de este apartado se pueden distinguir reglas en tres epígrafes: *Contraseñas*, *Bloqueo* y *Kerberos*. Entre ellas, las dos primeras hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión local.
2. **Directiva local.** Dentro de este apartado se encuentra, por una parte, la *Auditoría* del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, inicios de sesión local). Por otra parte, este apartado incluye los *derechos y privilegios* que acabamos de explicar.
3. **Claves públicas.** Este apartado permite administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

2.6. Atributos de protección de los recursos

En un sistema de archivos NTFS de Windows 2003, cada carpeta o archivo posee los siguientes atributos de protección:

1. **SID del propietario.** Inicialmente, el propietario es siempre el usuario que ha creado el archivo o carpeta, aunque este atributo puede ser luego modificado (esto se explica más adelante).
2. **Lista de control de acceso de protección.** Esta lista incluye los *permisos* que los usuarios tienen sobre el archivo o carpeta. La lista puede contener un número indefinido de entradas, de forma que cada una de ellas concede o deniega un conjunto concreto de permisos a un usuario o grupo conocido por el sistema. Por tanto, Windows 2003 permite definir multitud de niveles de acceso a cada objeto del sistema de archivos, cada uno de los cuales puede ser *positivo* (se otorga un permiso) o *negativo* (se deniega un permiso).
3. **Lista de control de acceso de seguridad.** Esta segunda lista se utiliza para definir qué acciones sobre un archivo o carpeta tiene que *auditar* el sistema. El proceso de auditoría supone la anotación en el *registro del sistema* de las acciones que los usuarios realizan sobre archivos o carpetas (las entradas de este regis-

2.6.1. Asociación de permisos a recursos

tro, denominado registro de seguridad, pueden consultarse más tarde mediante la herramienta administrativa Visor de Sucesos). El sistema sólo audita las acciones especificadas (de los usuarios o grupos especificados) en la lista de seguridad de cada archivo o carpeta. Esta lista está inicialmente vacía en todos los objetos del sistema de archivos.

La lista de control de acceso de protección se divide realmente en dos listas, cada una de ellas denominada *Discretionary Access Control List* (lista de control de acceso discrecional) o DACL. Cada elemento de una DACL se denomina *Access Control Entry* (entrada de control de acceso) o ACE. Cada entrada liga a un SID de usuario o grupo con la concesión o denegación de un permiso concreto (o conjunto de permisos), tal como se ha descrito arriba. Los diferentes permisos que se pueden asignar a usuarios o grupos en Windows 2003 se explican en la Sección 2.6.2, “Permisos estándar e individuales”.

El hecho de que cada archivo o carpeta tenga dos DACL en vez de una tiene que ver con el mecanismo de la *herencia de permisos* que ha incorporado Windows 2003: cada archivo o carpeta puede heredar implícitamente los permisos establecidos para la carpeta que lo contiene y puede además definir permisos propios (denominados explícitos en la jerga de Windows 2003). Es decir, que cada archivo o carpeta puede poseer potencialmente una *DACL heredada* y una *DACL explícita* (aunque no está obligado a ello, como veremos). De esta forma, si una cierta carpeta define permisos explícitos, éstos (junto con sus permisos heredados) serán a su vez los permisos heredados de sus subcarpetas y archivos (y así sucesivamente). El mecanismo de herencia de permisos es dinámico, queriendo decir que la modificación un permiso explícito de una carpeta se refleja en el correspondiente permiso heredado de sus subcarpetas y archivos.

2.6.1. Asociación de permisos a recursos

La asociación de permisos a archivos y carpetas sigue una serie de reglas:

- Cuando se crea un **nuevo** archivo o carpeta, éste no posee ningún permiso explícito y adquiere como permisos heredados los permisos heredados y explícitos de su carpeta padre.
- Si se desea añadir permisos sobre un archivo o carpeta, éstos se añaden siempre a la lista de permisos explícitos. De igual forma, sólo se puede modificar o eliminar *individualmente* un permiso si éste es explícito.
- El control sobre la **herencia** de permisos (i.e., qué recursos heredan y qué permisos se heredan) se puede realizar a dos niveles de forma independiente:

2.6.2. Permisos estándar e individuales

1. Cada carpeta o archivo tiene la potestad de decidir si desea o no heredar los permisos de su carpeta padre (herencia "*desde arriba*"). Es decir, en cada recurso se puede *desactivar* la herencia, con lo que los permisos definidos por encima del recurso en la jerarquía de archivos no se le aplican. Desactivar la herencia no es una acción irreversible: la herencia puede volver a activarse más tarde si se desea, sin que ello modifique los permisos explícitos que pueda tener el recurso.
2. Cada permiso lleva asociada una regla que indica qué recursos van a poder heredarlo (herencia "*hacia abajo*"). Esta regla sólo interviene cuando se asocia un permiso a una carpeta, puesto que sólo las carpetas poseen recursos dentro de ellas (subcarpetas y archivos) que puedan heredar el permiso. Por tanto, cuando en una carpeta se define un permiso explícito, su regla de la herencia puede utilizarse para restringir qué recursos por debajo de dicha carpeta van a poder heredarlo.

Concretamente, la regla permite establecer que el permiso sea aplicable: (a) sólo en la propia carpeta, (b) sólo en las subcarpetas, (c) sólo en los archivos, o cualquier combinación entre estas tres opciones. La regla por defecto al crear un nuevo permiso explícito es que dicho permiso sea heredable por la carpeta y todas sus subcarpetas y archivos.

- **Copiar** un archivo o carpeta a otra ubicación se considera una creación, y por tanto el archivo copiado recibe una lista de permisos explícitos vacía y se activa la herencia de la carpeta padre correspondiente a la nueva ubicación.
- **Mover** un archivo distingue dos casos: si movemos una carpeta o archivo a otra ubicación dentro del mismo volumen (partición) NTFS, se desactiva la herencia y se mantienen los permisos que tuviera como explícitos en la nueva ubicación. Si el volumen destino es distinto, entonces se actúa como en una copia (sólo se tienen los permisos heredados de la carpeta padre correspondiente a la nueva ubicación).

2.6.2. Permisos estándar e individuales

Windows 2003 distingue entre los *permisos estándar* de carpetas y los de archivos. Como ocurría en versiones previas de Windows NT, los permisos estándar son combinaciones predefinidas de *permisos individuales*, que son aquellos que controlan cada una de las acciones individuales que se pueden realizar sobre carpetas y archivos. La existencia de estas combinaciones predefinidas es el resultado de una agrupación "lógica" de los permisos individuales para facilitar la labor del administrador (y de cada usuario cuando administra los permisos de sus archivos). Por este motivo, los permisos estándar se conocen también como "plantillas de permisos".

2.6.2. Permisos estándar e individuales

En la Tabla 2.2, “Permisos estándar sobre carpetas y archivos en Windows 2003” se muestran los permisos estándar de carpetas y archivos junto con su significado cualitativo. La descripción de las tablas hacen referencia a las acciones que cada permiso concede, pero no olvidemos que en Windows 2003 cada permiso puede ser positivo o negativo, es decir, que realmente cada permiso *permite* o *deniega* la acción correspondiente. Como puede verse en ambas tablas, muchos de los permisos estándar se definen de forma *incremental*, de forma que unos incluyen y ofrece un nivel de acceso superior que los anteriores. La herencia de permisos se establece de forma natural: las carpetas heredan directamente los permisos estándar establecidos en la carpeta padre, mientras que los archivos heredan cualquier permiso excepto el de Listar (sólo definido para carpetas).

Tabla 2.2. Permisos estándar sobre carpetas y archivos en Windows 2003

CARPETAS	
Nombre	Significado
Listar	Permite listar la carpeta: ver los archivos y subcarpetas que contiene.
Leer	Permite ver el contenido de los archivos y subcarpetas, así como su propietario, permisos y atributos (sistema, sólo lectura, oculto, etc.).
Escribir	Permite crear nuevos archivos y subcarpetas. Permite modificar los atributos de la propia carpeta, así como ver su propietario, permisos y atributos.
Leer y Ejecutar	Permite moverse por la jerarquía de subcarpetas a partir de la carpeta, incluso si no se tienen permisos sobre ellas. Además, incluye todos los permisos de Leer y de Listar.
Modificar	Permite eliminar la carpeta más todos los permisos de Escribir y de Leer y Ejecutar.
Control Total	Permite cambiar permisos, tomar posesión y eliminar subcarpetas y archivos (aun no teniendo permisos sobre ellos), así como todos los permisos anteriores.

ARCHIVOS	
Nombre	Significado
Leer	Permite ver el contenido del archivo, así como su propietario, permisos y atributos (sistema, sólo lectura, oculto, etc.).
Escribir	Permite sobreescribir el archivo, modificar sus atributos y ver su propietario, permisos y atributos.
Leer y Ejecutar	Permite ejecutar el archivo más todos los permisos de Leer.
Modificar	Permite modificar y eliminar el archivo más todos los permisos de Escribir y de Leer y Ejecutar.
Control Total	Permite cambiar permisos y tomar posesión del archivo, más todos los permisos anteriores.

Cuando la asignación de permisos que queremos realizar no se ajusta al comportamiento de ninguno de los permisos estándar, debemos entonces ir directamente a asignar permisos individuales. La Tabla 2.3, “Permisos individuales en Windows

2.6.2. Permisos estándar e individuales

2003" muestra cuáles son los permisos individuales en Windows 2003, junto con su significado concreto. También en este caso debe entenderse que cada permiso puede ser concedido de forma positiva o negativa.

Tabla 2.3. Permisos individuales en Windows 2003

Nombre	Significado
Atravesar carpeta/ejecutar archivo	Aplicado a una carpeta, permite moverse por subcarpetas en las que puede que no se tenga permiso de acceso. Aplicado a un archivo, permite su ejecución.
Leer carpeta/Leer datos	Aplicado a una carpeta, permite ver los nombres de sus ficheros y subcarpetas. Aplicado a un archivo, permite leer su contenido.
Leer atributos	Permite ver los atributos del fichero/carpeta, tales como oculto o sólo lectura, definidos en NTFS.
Leer atributos extendidos	Permite ver los atributos extendidos del archivo o carpeta. (Estos atributos están definidos por los programas y pueden variar).
Crear ficheros/escribir datos	Aplicado a una carpetas, permite crear archivo en ella. Aplicado a un archivo, permite modificar y sobreescribir su contenido.
Crear carpetas/anexar datos	Aplicado a una carpeta, permite crear subcarpetas en ella. Aplicado a un archivo, permite añadir datos al mismo.
Escribir atributos	Permite modificar los atributos de un archivo o carpeta.
Escribir atributos extendidos	Permite modificar los atributos extendidos de un archivo o carpeta.
Borrar subcarpetas y archivos	Sólo se puede aplicar a una carpeta, y permite borrar archivos o subcarpetas de la misma, aun no teniendo permiso de borrado en dichos objetos.
Borrar	Permite eliminar la carpeta o archivo.
Leer permisos	Permite leer los permisos de la carpeta o archivo.
Cambiar permisos	Permite modificar los permisos de la carpeta o archivo.
Tomar posesión	Permite tomar posesión de la carpeta o archivo.

Finalmente, la Tabla 2.4, "Correspondencia entre permisos estándar e individuales en Windows 2003" pone de manifiesto el subconjunto de los permisos individuales forman cada uno de los permisos estándar mencionados anteriormente. Como curiosidad, puede verse que los permisos individuales correspondientes a **Listar** y **Leer** y **Ejecutar** son los mismos. En realidad, lo que les distingue es cómo se heredan: el primero sólo es heredado por carpetas, mientras que el segundo es heredado por carpetas y archivos.

2.6.3. Modificación de atributos de protección

Tabla 2.4. Correspondencia entre permisos estándar e individuales en Windows 2003

Permiso	C.Total	Modif.	L.y Ej.	Listar	Leer	Escribir
Atravesar carpeta/ ejecutar archivo	+	+	+	+		
Leer carpeta/Leer datos	+	+	+	+	+	
Leer atributos	+	+	+	+	+	
Leer atributos ex- tendidos	+	+	+	+	+	
Crear ficheros/es- cribir datos	+	+				+
Crear carpetas/ane- xar datos	+	+				+
Escribir atributos	+	+				+
Escribir atributos extendidos	+	+				+
Borrar subcarpetas y archivos	+					
Borrar	+	+				
Leer permisos	+	+	+	+	+	+
Cambiar permisos	+					
Tomar posesión	+					

2.6.3. Modificación de atributos de protección

Las reglas que plantea Windows 2003 para controlar quién puede modificar los atributos de protección de un recurso están completamente integradas en su modelo de protección, basado en los *permisos* y los *derechos* del usuario implicado en la modificación. Este modelo es diferente del que plantean los sistemas UNIX, cuyas reglas en este sentido son independientes de los permisos que posea el propio recurso.

En concreto, las reglas que dictan quién puede modificar los diferentes atributos de protección de los recursos (archivos y carpetas) son:

1. **Propietario.** Cualquier usuario que posea el permiso individual Tomar posesión(incluido dentro de Control Total) sobre un recurso concreto, puede pasar a ser su nuevo propietario.

Asimismo, cualquier usuario que tenga concedido el derecho Tomar posesión de archivos y otros objetos puede convertirse en propietario de *cualquier* recurso del sistema. Por defecto, este derecho solamente lo tiene concedido el grupo Administradores.

Finalmente, Windows 2003 ha introducido otra posibilidad: el derecho de usuario Restaurar archivos y carpetas lleva asociado la posibilidad de *asignar* la posesión de cualquier archivo y carpeta del sistema a cualquier usuario, sin tener que tomar posesión en nombre propio. Por defecto, sólo los grupos Administradores y Operadores de copia tienen este derecho concedido.

2. **Lista de control de acceso de protección.** Cualquier usuario que posea el permiso individual Cambiar Permisos (incluido dentro de Control Total) sobre un recurso concreto, puede modificar sus permisos. De forma independiente, el *propietario* de un recurso siempre puede cambiar los permisos del mismo.

Las acciones concretas que se incluyen en el cambio de permisos sobre un recurso son: (a) la activación/desactivación de la herencia de permisos y (b) la edición (creación, modificación y eliminación) de permisos explícitos.

3. **Lista de control de acceso de seguridad.** Se aplican las mismas reglas que en el caso anterior.

Después de haber visto el modelo de protección y de cambio de atributos, es interesante analizar la diferencia de los modelos de Windows 2003 y UNIX respecto a la figura del Administrador/root. En el mundo UNIX, root no tiene ninguna restricción en sus acciones en el sistema. En Windows 2003, por el contrario, al Administrador se le aplican las mismas reglas que al resto de usuarios: si dicho usuario no posee permisos sobre un recurso, no podrá acceder al mismo. Si podrá, no obstante, tomar posesión del recurso (gracias al *derecho* que tiene concedido) y, una vez sea su propietario, añadirse permisos que le permitan cualquier acceso. El modelo de Windows 2003 se basa, por tanto, en definir la protección como un conjunto de reglas (permisos, derechos) y conceder a cada usuario aquellas necesarias para que desempeñe su función. El Administrador tiene concedidas más reglas que el resto de usuarios, pero aún así el sistema sigue verificándolas para cada acción que realiza en el sistema. Se recomienda al lector reflexionar sobre este hecho y su repercusión en el modelo de protección.

2.7. Reglas de protección

Las principales reglas que controlan la comprobación de permisos a carpetas y archivos son las siguientes:

- Una única acción de un proceso puede involucrar varias acciones individuales

sobre varios archivos y/o carpetas. En ese caso, el sistema verifica si el proceso tiene o no permisos para todas ellas. Si le falta algún permiso, la acción se rechaza con un mensaje de error genérico de falta de permisos.

- Los permisos en Windows 2003 son acumulativos: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SIDs de su acreditación (ver Sección 2.4, “Atributos de protección de los procesos”), es decir, los permisos del usuario y de todos los grupos a los que pertenece.
- La ausencia un cierto permiso sobre un objeto supone implícitamente la imposibilidad de realizar la acción correspondiente sobre el objeto.
- Si se produce un conflicto en la comprobación de los permisos, los permisos negativos tienen prioridad sobre los positivos, y los permisos explícitos tienen prioridad sobre los heredados.

Estas reglas son más fáciles de recordar si se conoce el algoritmo que sigue Windows 2003 para conceder o denegar una acción concreta sobre un archivo o directorio concreto. Para ello, el sistema explora secuencialmente las entradas de las DACLs de protección de dicho objeto hasta que se cumple alguna de las condiciones siguientes:

1. Cada permiso involucrado en la acción solicitada está concedido explícitamente al SID del usuario o de algún grupo al que el usuario pertenece. En ese caso, se permite la acción.
2. Alguno de los permisos involucrados está explícitamente denegado para el SID del usuario o para alguno de sus grupos. En este caso, se deniega la acción.
3. La lista (DACL) ha sido explorada completamente y no se ha encontrado una entrada (ni positiva ni negativa) correspondiente a alguno de los permisos involucrados en la acción para el SID del usuario o sus grupos. En este caso, se deniega la acción.

Este algoritmo realmente produce el comportamiento descrito por las reglas anteriores debido al orden en que Windows 2003 establece las entradas de las DACLs de cada objeto. Este orden es siempre el siguiente: permisos negativos explícitos, permisos positivos explícitos, permisos negativos heredados y permisos positivos heredados.

3

Administración de dominios Windows 2003

Índice

3.1. Introducción	35
3.2. El Directorio Activo	35
3.2.1. Dominios Windows 2003 y el Directorio Activo	35
3.2.2. Estándares relacionados	36
3.2.3. El Directorio Activo y DNS	37
3.2.4. Estructura lógica	38
3.2.5. Estructura física	46
3.3. Objetos que administra un dominio	50
3.3.1. Usuarios globales	50
3.3.2. Grupos	51
3.3.3. Equipos	53
3.3.4. Unidades Organizativas	54
3.4. Compartición de recursos	54
3.4.1. Permisos y derechos	54
3.4.2. Compartición dentro de un dominio	55
3.4.3. Mandatos Windows 2003 para compartir recursos	56
3.5. Delegación de la administración	57

3.1. Introducción

Este capítulo introduce los conceptos fundamentales sobre dominios Windows 2003, suficientes para poder unificar y centralizar la administración de conjuntos de sistemas Windows 2003 en organizaciones de cualquier tamaño.

En concreto, se explicarán los conceptos fundamentales que soportan el Directorio Activo (*Active Directory*), así como la administración del mismo, incluyendo los principales objetos que pueden definirse en el mismo, la compartición de recursos entre sistemas de la organización y la delegación de tareas administrativas dentro de un dominio.

3.2. El Directorio Activo

3.2.1. Dominios Windows 2003 y el Directorio Activo

Hoy en día, los ordenadores existentes en cualquier organización se encuentran formando parte de redes de ordenadores, de forma que pueden intercambiar información. Desde el punto de vista de la administración de sistemas, la mejor forma de aprovechar esta característica es la creación de un *dominio* de sistemas, en donde la información administrativa y de seguridad se encuentra *centralizada* en uno o varios servidores, facilitando así la labor del administrador. Windows 2003 utiliza el concepto de **directorio** para implementar dominios de sistemas Windows 2003.

En el ámbito de las redes de ordenadores, el concepto de *directorio* (o almacén de datos) es una estructura jerárquica que almacena información sobre objetos en la red, normalmente implementada como una base de datos optimizada para operaciones de lectura y que soporta búsquedas de grandes datos de información y con capacidades de exploración.

Active Directory es el servicio de directorio de una red de Windows 2003. Este servicio de directorio es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y *administrar* centralizadamente el acceso a los recursos de la red.

Como veremos, al instalar el Directorio Activo en uno o varios sistemas Windows 2003 (Server) de nuestra red, convertimos a dichos ordenadores en los servidores del dominio, o más correctamente, en los denominados *Controladores de Dominio* (*Domain Controllers*) o simplemente "DCs". El resto de los equipos de la red pueden convertirse entonces en los *clientes* de dicho servicio de directorio, con lo que reciben toda la información almacenada en los controladores. Esta información inclu-

3.2.2. Estándares relacionados

ye no sólo las cuentas de usuario, grupo, equipo, etc., sino también los perfiles de usuario y equipo, directivas de seguridad, servicios de red, etc. El Directorio Activo se convierte así en la herramienta fundamental de administración de toda la organización.

Una de las ventajas fundamentales del Directorio Activo es que separa la estructura *lógica* de la organización (dominios) de la estructura *física* (topología de red). Ello permite, por una parte, independizar la estructuración de dominios de la organización de la topología de la(s) red(es) que interconectan los sistemas; y, por otra parte, permite administrar la estructura física explícitamente cuando es necesario, de forma independiente de la administración de los dominios. Más adelante en este capítulo se exponen ambas estructuras detalladamente.

3.2.2. Estándares relacionados

A diferencia de su antecesor NT 4.0, Windows 2003 proporciona compatibilidad con un buen número de protocolos y estándares existentes, ofreciendo interfaces de programación de aplicaciones que facilitan la comunicación con otros servicios de directorio. Entre ellos, podemos destacar los siguientes:

- DHCP (*Dynamic Host Configuration Protocol*). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de direcciones de red.
- DNS (*Domain Name System*). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.
- SNTP (*Simple Network Time Protocol*). Protocolo simple de tiempo de red, que permite disponer de un servicio de tiempo distribuido.
- LDAP (*Lightweight Directory Access Protocol*). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden y modifican la información existente en el directorio.
- Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas..
- Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

De entre todos ellos, es imprescindible que el administrador conozca en detalle la relación entre el Directorio Activo y DNS. A continuación se exponen los aspectos fundamentales de esta relación.

3.2.3. El Directorio Activo y DNS

El Directorio Activo y DNS son espacios de nombres. Podemos entender un espacio de nombres como un área delimitada en la cual un nombre puede ser resuelto. La resolución de nombres es el proceso de traducción de un nombre en un objeto o información que lo representa. Por ejemplo, el sistema de ficheros NTFS puede ser considerado un espacio de nombres en el cual un fichero puede ser resuelto en el fichero propiamente dicho.

DNS es el sistema de nombres de facto para redes basadas en el protocolo TCP/IP y el servicio de nombres que se usa para localizar equipos en Internet. Windows 2003 utiliza DNS para localizar equipos y controladores de dominio. Una estación de trabajo o servidor miembro busca un controlador de dominio preguntando a DNS.

Cada dominio de Windows 2003 se identifica únicamente mediante un nombre DNS (por ejemplo, `miempresa.com`) y cada equipo basado en Windows 2003 que forma parte de un dominio tiene un nombre DNS cuyo sufijo es precisamente el nombre DNS de dicho dominio (siguiendo con el ejemplo, `pc0100.miempresa.com`). De esta forma vemos que dominios y equipos se representan como objetos en Active Directory y como nodos en DNS. Por tanto resulta fácil confundir ambos espacios de nombres ya que comparten idénticos nombres de dominio. La diferencia es que aunque comparten la misma estructura, almacenan información diferente: DNS almacena zonas y registros de recursos y el Directorio Activo guarda dominios y objetos de dominio.

Como conclusión diremos que Directorio Activo *utiliza* DNS, para tres funciones principales:

1. **Resolución de nombres:** DNS permite realizar la resolución de nombres al convertir los nombres de host a direcciones IP.
2. **Definición del espacio de nombres:** Directorio Activo utiliza las convenciones de nomenclatura de DNS para asignar nombre a los dominios.
3. **Búsqueda de los componentes físicos de AD:** para iniciar una sesión de red y realizar consultas en Directorio Activo, un equipo con Windows 2003 debe encontrar primero un controlador de dominio o servidor de catálogo global para procesar la autenticación de inicio de sesión o la consulta. La base de datos DNS almacena información acerca de qué equipos realizan estas funciones para que se pueda atender la solicitud adecuadamente. En concreto, esto se lleva a cabo mediante registros de recursos SRV que especifican el servidor (o servidores) del dominio que proporcionan los servicios de directorio correspondientes.

3.2.4. Estructura lógica

La estructura lógica del Directorio Activo se centra en la administración de los *recursos* de la red organizativa, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes. Como veremos, la estructura lógica de la organización se basa en el concepto de *dominio*, o unidad mínima de directorio, que internamente contiene información sobre los recursos (usuarios, grupos, directivas, etc.) disponibles para los ordenadores que forman parte de dicho dominio. Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de *unidades organizativas*, que permiten una administración independiente sin la necesidad de crear múltiples dominios. Sin embargo, si la organización desea estructurarse en varios dominios, también puede hacerlo, mediante los conceptos de *árbol* y *bosque*; ambos son jerarquías de dominios a distintos niveles, en función de si los dominios comparten o no un espacio de nombres común. A continuación se presentan todos estos conceptos de forma más detallada.

3.2.4.1. Dominios

La unidad central de la estructura lógica del Directorio Activo es el dominio. Un dominio es un conjunto de equipos que comparten una base de datos de directorio común. Dentro de una organización, el Directorio Activo se compone de uno o más dominios, cada uno de ellos soportado, al menos, por un controlador de dominio. Como hemos visto, cada dominio se identifica únicamente por un nombre de dominio DNS, que debe ser el sufijo DNS principal de todos los ordenadores miembros del dominio, incluyendo el o los controladores.

El uso de dominios permite conseguir los siguientes objetivos:

- **Delimitar la seguridad.** Un dominio Windows 2003 define un límite de seguridad. Las directivas de seguridad, los derechos administrativos y las listas de control de acceso (*Access Control Lists*, ACLs) no se comparten entre los dominios. Active Directory puede incluir uno o más dominios, teniendo cada uno sus propias directivas de seguridad.
- **Replicar información.** Un dominio es una partición del directorio, las cuales son unidades de replicación. Cada dominio almacena solo la información sobre los objetos localizados en este dominio. Active Directory utiliza un modelo de replicación con varios maestros. Todos los controladores de dominio del dominio pueden recibir cambios realizados sobre los objetos, y pueden replicar estos cambios a todos los controladores de dominio en el dominio.
- **Aplicar Políticas (o Directivas) de Grupo.** Un dominio define un posible ámbito para las políticas. Al aplicar un objeto de política de grupo (GPO) al dominio, este establece como los recursos del dominio se configuran y se usan. Estas políti-

3.2.4. Estructura lógica

cas se aplican dentro del dominio y no a través de los dominios.

- **Delegar permisos administrativos.** En las redes que ejecutan Windows 2003, se puede delegar a medida la autoridad administrativa tanto para unidades organizativas (OUs) individuales como a dominios individuales, lo cual reduce el número de administradores necesarios con amplios permisos administrativos. Ya que un dominio representa un límite de seguridad, los permisos administrativos se limitan al dominio.

3.2.4.2. Múltiples dominios en la misma organización

Existen muchos casos en los que es interesante disponer de varios dominios de ordenadores Windows 2003 en la misma organización (distribución geográfica o departamental, distintas empresas, etc.). El Directorio Activo permite almacenar y organizar la información de directorio de varios dominios de forma que, aunque la administración de cada uno sea independiente, dicha información esté disponible para todos los dominios.

Según los estándares de nombres DNS, los dominios de Active Directory se crean dentro de una estructura de árbol invertida, con la raíz en la parte superior. Además, esta jerarquía de dominios de Windows 2003 se basa en relaciones de confianza, es decir, los dominios se vinculan por relaciones de confianza entre dominios.

Cuando se instala el primer controlador de dominio en la organización se crea lo que se denomina el *dominio raíz* del bosque, el cual contiene la configuración y el esquema del bosque (compartido por todos los dominios de la organización). Más adelante, podemos agregar dominios como subdominios de dicha raíz (**árbol de dominios**) o bien crear otros dominios "hermanos" de la raíz (**bosque de dominios**), debajo del cual podemos crear subdominios, y así sucesivamente.

Árbol Un árbol es un conjunto de uno o más dominios que comparten un espacio de nombres contiguo. Si existe más de un dominio, estos se disponen en estructuras de árbol jerárquicas.

El primer dominio creado es el dominio raíz del primer árbol. Cuando se agrega un dominio a un árbol existente este pasa a ser un dominio secundario (o hijo). Un dominio inmediatamente por arriba de otro dominio en el mismo árbol de dominio es su padre. Todos los dominios que tengan un dominio raíz común se dice que forman un espacio de nombres contiguo.

Los dominios secundarios (hijos) pueden representar entidades geográficas (valencia, madrid, barcelona), entidades administrativas dentro

3.2.4. Estructura lógica

de la organización (departamento de ventas, departamento de desarrollo ...), u otras delimitaciones específicas de una organización, según sus necesidades.

Los dominios que forman un árbol se enlazan mediante relaciones de confianza bidireccionales y transitivas. La relación padre-hijo entre dominios en un árbol de dominio es simplemente una relación de confianza. Los administradores de un dominio padre no son automáticamente administradores del dominio hijo y el conjunto de políticas de un dominio padre no se aplican automáticamente a los dominios hijo.

Por ejemplo, en la Universidad Politécnica de Valencia cuyo dominio actual de Active Directory es `upv.es` se crean dos nuevos departamentos: DSIC y DISCA. Con el fin de permitir la administración de los dominios por parte de los técnicos de los respectivos departamentos, se decide agregar dos nuevos dominios a su árbol de dominios existente en lugar de crear dos unidades organizativas en el dominio existente. Los dominios resultantes, `dsic.upv.es` y `disca.upv.es` forman un espacio de nombres contiguo, cuya raíz es `upv.es`. El administrador del dominio padre (`upv.es`) puede conceder permisos para recursos a cuentas de cualquiera de los tres dominios del árbol, pero por defecto no los puede administrar.

Bosque	Un bosque es un grupo de árboles que no comparten un espacio de nombres contiguo, conectados a través de relaciones de confianza bidireccionales y transitivas. Un dominio único constituye un árbol de un dominio, y un árbol único constituye un bosque de un árbol. Los árboles de un bosque aunque no forman un espacio de nombres común, es decir, están basados en diferentes nombres de dominio raíz de DNS, comparten una configuración, un esquema de directorio común y el denominado catálogo global.
---------------	--

Es importante destacar que, aunque los diferentes árboles de un bosque no comparten un espacio de nombres contiguo, el bosque tiene siempre un único dominio raíz, llamado precisamente *dominio raíz del bosque*; dicho dominio raíz será siempre el primer dominio creado por la organización.

Añadir nuevos dominios a un bosque es fácil. Sin embargo, existen ciertas limitaciones que hemos de tener en cuenta al respecto:

- No se pueden mover dominios de Active Directory entre bosques.
- Solamente se podrán eliminar dominios de un bosque si este no tiene

3.2.4. Estructura lógica

dominios hijo.

- Después de haber establecido el dominio raíz de un árbol, no se pueden añadir dominios con un nombre de nivel superior al bosque.
- No se puede crear un dominio padre de un dominio existente.

En general, la implementación de bosques y árboles de dominio permite mantener convenciones de nombres tanto contiguos como discontinuos, lo cual puede ser útil en organizaciones con divisiones independientes que quieren mantener sus propios nombres DNS.

Finalmente, debemos relacionar estos conceptos con el procedimiento para **crear un dominio**. Esto se hace mediante la ejecución de un asistente denominado **dcromo** en el sistema Windows 2003 Server que queramos *promocionar* a controlador de dominio. En concreto, este asistente nos permite elegir entre las siguientes opciones de instalación:

1. DC adicional de un dominio existente o DC para un dominio nuevo (creación de un dominio).
2. En el segundo caso, el dominio (nuevo) puede ser un dominio secundario de otro dominio existente (es decir, un subdominio en un árbol de dominios ya creado), o bien el dominio principal (raíz) de un nuevo árbol de dominios.
3. En este segundo caso, el dominio raíz puede ser de un bosque existente (agregamos una raíz nueva a un bosque) o de un nuevo bosque (creación del bosque). Por tanto, el primer dominio que creemos en una organización siempre será un dominio nuevo de un árbol nuevo de un bosque nuevo.

3.2.4.3. Niveles funcionales

La funcionalidad de los dominios de Windows 2003 es diferente de la que tenían sistemas anteriores de la misma familia (Windows NT4 y Windows 2000). Tanto Windows 2000 como Windows 2003 pueden configurarse en diferentes *niveles funcionales* ("modos de dominio" en Windows 2000) para que puedan ser compatibles con sistemas anteriores.

En concreto, Windows Server 2003 soporta cuatro niveles funcionales *de dominio* y tres niveles funcionales *de bosque*, explicados a continuación.

Un *dominio* Windows 2003 puede estar en cuatro niveles funcionales:

1. **Windows 2000 mixto.** Este es el nivel funcional por defecto cuando se crea un nuevo dominio (o cuando se actualiza de un sistema anterior). En este nivel, los DCs de Windows 2003 son compatibles dentro del mismo dominio con DCs Windows NT4 y Windows 2000. Por este motivo, un conjunto significativo de opciones de configuración no están disponibles (como por ejemplo el anidamiento de grupos, el cambio de ámbito de grupo y los grupos universales).
2. **Windows 2000 nativo.** En este nivel funcional, los DCs de Windows 2003 son compatibles dentro del mismo dominio con DCs que ejecuten Windows 2000 pero no Windows NT4. Se tiene una funcionalidad completa del Directorio Activo a nivel de Windows 2000, aunque se excluyen las nuevas opciones que Windows 2003 ha introducido en los dominios (entre las cuales destaca la posibilidad de cambiar de nombre a un DC sin necesidad de despromocionarlo previamente).
3. **Windows Server 2003 provisional.** En este nivel funcional, los DCs de Windows 2003 son compatibles dentro del mismo dominio con DCs que ejecuten Windows NT4 pero no Windows 2000. Se trata de un nivel funcional reservado únicamente para migraciones directas de NT4 a Windows 2003, y se supone que es completamente transitorio.
4. **Windows Server 2003.** En este nivel funcional, los DCs de Windows 2003 son compatibles únicamente entre sí (sólo puede configurarse si todos los DCs del dominio son Windows Server 2003). Este nivel ofrece la funcionalidad completa de dominios, incluyendo todas las características definidas en Windows 2000 más las nuevas incluidas en Windows Server 2003.

Por otro lado, un *bosque de dominios* Windows 2003 puede estar en tres niveles funcionales:

- **Windows 2000.** Este es el nivel por defecto al crear un nuevo bosque (o actualizar desde un sistema anterior). En este nivel funcional, los DCs de Windows 2003 son compatibles dentro del bosque con DCs que ejecuten Windows 2000 o Windows NT4. Se tiene una funcionalidad completa del bosque a nivel de Windows 2000, aunque se excluyen las nuevas opciones que Windows 2003 ha introducido a este nivel (incluyendo mejoras en la replicación, las relaciones de confianza entre bosques y la posibilidad de renombrar dominios en lugar de eliminarlos y volverlos a crear).
- **Windows Server 2003 provisional.** En este nivel funcional, los DCs de Windows 2003 son compatibles dentro del bosque con DCs que ejecuten Windows NT4 pero no Windows 2000. Se trata de un nivel funcional reservado únicamente para la migración directa de NT4 a Windows 2003 en el primer dominio del bosque, y

3.2.4. Estructura lógica

se supone que es completamente transitorio.

- **Windows Server 2003.** En este nivel funcional, los DCs de Windows 2003 son compatibles únicamente entre sí (sólo puede configurarse si todos los DCs *del bosque* son Windows Server 2003). Este nivel ofrece la funcionalidad completa para los bosques, incluyendo todas las características definidas en Windows 2000 más las nuevas incluidas en Windows Server 2003.

Por tanto, por defecto al crear un nuevo bosque, éste se sitúa en el nivel funcional "Windows 2000", y al crear un nuevo dominio, éste se sitúa en el nivel funcional "Windows 2000 mixto", manteniendo, en ambos casos, la compatibilidad completa con sistemas anteriores.

Tanto a nivel de dominio como de bosque, la transición entre niveles funcionales sólo es posible *elevando* el nivel actual, es decir, pasando a un nivel con mayor funcionalidad (a excepción de los niveles provisionales, reservados para casos poco frecuentes). La elevación de nivel funcional es, por tanto, un paso irreversible, y sólo debe hacerse cuando se está seguro de que no van a añadirse sistemas anteriores como DCs al dominio, o al bosque. La elevación del nivel funcional de dominio o de bosque se realiza desde la herramienta "Dominios y Confianzas de Active Directory".

3.2.4.4. Relaciones de confianza

Una relación de confianza es una relación establecida entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por los DCs de otro dominio. Estas relaciones permiten a los usuarios acceder a los recursos de otro dominio y a los administradores definir los permisos y derechos de usuario para los usuarios del otro dominio.

Windows Server 2003 soporta varios tipos de relaciones de confianza, que veremos posteriormente. Al margen de su uso, los diferentes tipos de relaciones se diferencian en función de tres rasgos característicos:

- **Método de creación:** algunos tipos de relaciones de confianza se crean de forma automática (implícita) y otros de forma manual (explícita).
- **Dirección:** algunos tipos de relaciones son unidireccionales y otros bidireccionales. Si la relación es unidireccional, los usuarios del dominio A (de confianza) pueden utilizar los recursos del dominio B (que confía), pero no al revés. En una relación bidireccional, ambas acciones son posibles.
- **Transitividad:** algunos tipos de relaciones son transitivas y otras no. Una rela-

3.2.4. Estructura lógica

ción de confianza transitiva es aquella que permite que si un dominio A confía en otro B, y éste confía en un tercero C, entonces de forma automática, A confía en C. En las relaciones no transitivas, la confianza entre A y C tendría que añadirse explícitamente.

Después de ver las características de las relaciones de confianza, se explican a continuación los tipos de relaciones de confianza válidos en dominios y bosques Windows Server 2003:

- **Confianza raíz de árbol.** Esta relación se establece de forma automática entre los dominios raíz del mismo bosque. Es bidireccional y transitiva.
- **Confianza principal-secundario.** Esta relación se establece de forma automática entre un dominio dado y cada uno de sus subdominios (o dominios secundarios). Es bidireccional y transitiva.
- **Confianza de acceso directo.** Este tipo de relación debe establecerse de forma manual, y tiene como objetivo mejorar la eficiencia en los inicios de sesión remotos. Si los usuarios de un dominio A necesitan acceder frecuentemente a los recursos de un dominio B, y ambos dominios se encuentran "lejos" entre sí (con muchos dominios intermedios), la confianza permite una relación directa que acorta el tiempo necesario para la autentificación de los usuarios. Es transitiva y unidireccional (si se necesita en ambos sentidos, deben crearse dos relaciones de confianza).
- **Confianza externa .** Este tipo de relación se crea manualmente y permite a usuarios de un dominio Windows 2003 acceder a recursos ubicados en dominios de otro bosque, o bien dominios Windows NT4. Es unidireccional e intransitiva.
- **Confianza de bosque .** Este tipo de relación debe crearse de forma manual entre los dominios raíz de dos bosques distintos, y permite a los usuarios de cualquier dominio de un bosque acceder a los recursos de cualquier dominio del otro bosque. Es unidireccional y sólo es transitiva entre dos bosques. Este tipo de relaciones sólo están disponibles si ambos bosques se sitúan en el nivel funcional "Windows Server 2003".
- **Confianza de territorio .** Este tipo de relación debe crearse de forma manual entre un dominio Windows 2003 y un territorio (*realm*) Kerberos (versión 5) que no sea Windows, y permite interoperabilidad entre ambos. Es unidireccional y puede ser transitiva o no.

Por tanto, las relaciones de confianza automáticas (implícitas) se crean por defec-

to al ir añadiendo dominios al bosque, y mantienen relacionados todos esos dominios de forma bidireccional y transitiva. El efecto de estas relaciones es que de forma automática, los usuarios de cualquier dominio del bosque son conocidos (y pueden acceder a los recursos) en todos los dominios de dicho bosque. Las relaciones de confianza manuales (explícitas) están reservadas para casos en donde se busca mejorar la eficiencia o permitir interactuar con otros bosques o con dominios que no son Windows 2003.

3.2.4.5. Unidades Organizativas

Una Unidad Organizativa (*Organizational Unit, OU*) es un objeto del Directorio Activo que puede contener a otros objetos del directorio. Es decir, es un *contenedor* de otros objetos, de forma análoga a una carpeta o directorio en un sistema de archivos tradicional. En concreto, dentro de una unidad de este tipo pueden crearse cuentas de usuario, de grupo, de equipo, de recurso compartido, de impresora compartida, etc., además de *otras* unidades organizativas. Es decir, mediante unidades organizativas podemos crear una *jerarquía* de objetos en el directorio (lo cual se asemeja otra vez a un sistema de archivos típico de Windows). Los objetos ubicados dentro de una unidad organizativa pueden moverse más tarde a otra, si fuera necesario. Sin embargo, un objeto no puede *copiarse*: cada objeto es único en el directorio, y su existencia es independiente de la unidad organizativa a la que pertenece.

Por tanto, el objetivo de las unidades organizativas es *estructurar* u organizar el conjunto de los objetos del directorio, agrupándolos de forma coherente. En el Directorio Activo, las unidades organizativas permiten:

1. **Delegar la administración.** Cada unidad organizativa puede administrarse de forma independiente. En concreto, se puede otorgar la administración total o parcial de una unidad organizativa a un usuario o grupo de usuarios cualquiera. Esto permite *delegar* la administración de subconjuntos estancos del dominio a ciertos usuarios que posean el nivel de responsabilidad adecuada.
2. **Establecer de forma centralizada comportamientos distintos a usuarios y equipos.** A cada unidad organizativa pueden vincularse políticas de grupo, que aplican comportamientos (generalmente en forma de restricciones) a los usuarios y equipos cuyas cuentas se ubican en dicha unidad. De esta forma, podemos aplicar restricciones distintas a subconjuntos de usuarios y equipos del dominio, en función exclusivamente de la unidad organizativa donde se ubican. Por ejemplo, podemos limitar a los usuarios del departamento de contabilidad para que sólo puedan utilizar ciertas aplicaciones, pero que esto no se aplique a los usuarios del departamento de informática.

3.2.5. Estructura física

En muchos sentidos, el concepto de unidad organizativa se puede utilizar en Windows 2003 de la misma forma que se entendía el concepto de dominio en versiones anteriores de Windows NT, es decir, conjunto de usuarios, equipos y recursos administrados independientemente. En realidad, en Windows 2003 el concepto de dominio viene más bien asociado a la distribución de los sitios (topología de red) y a la implementación de DNS que exista (o quiera crearse) en la empresa.

De este modo, en muchas organizaciones de pequeño o medio tamaño resulta más adecuado implementar un modelo de dominio único con múltiples unidades organizativas que un modelo de múltiples dominios. Si es necesario, cada unidad puede administrarse independientemente, con uno o varios administradores delegados y comportamientos (políticas) diferentes.

3.2.5. Estructura física

En Active Directory, la estructura lógica está separada de la estructura física. La estructura lógica se utiliza para organizar los recursos de red mientras que la estructura física se utiliza para configurar y administrar el tráfico de red. En concreto, la estructura física de Active Directory se compone de sitios y controladores de dominio.

La estructura física de Active Directory define dónde y cuándo se producen el tráfico de replicación y de inicio de sesión. Una buena comprensión de los componentes físicos de Active Directory permite optimizar el tráfico de red y el proceso de inicio de sesión, así como solventar problemas de replicación.

3.2.5.1. Sitios

Un sitio es una combinación de una o varias subredes IP que están conectadas por un vínculo de alta velocidad. Definir sitios permite configurar la topología de replicación y acceso a Active Directory de forma que Windows 2003 utilice los vínculos y programas más efectivos para el tráfico de inicio de sesión y replicación.

Normalmente los sitios se crean por dos razones principalmente:

- Para optimizar el tráfico de replicación.
- Para permitir que los usuarios se conecten a un controlador de dominio mediante una conexión confiable de alta velocidad.

Es decir, los sitios definen la estructura física de la red, mientras que los dominios definen la estructura lógica de la organización.

3.2.5.2. Controladores de dominio

Un controlador de dominio (*Domain Controller, DC*) es un equipo donde se ejecuta Windows 2003 Server y que almacena una replica del directorio. Los controladores de dominio ejecutan el servicio KDC, que es responsable de autenticar inicios de sesión de usuario.

La información almacenada en cada controlador de dominio se divide en tres categorías (particiones): dominio, esquema y datos de configuración. Estas particiones del directorio son las unidades de replicación:

1. **Partición del directorio de esquema:** contiene todos los tipos de objetos y atributos que pueden ser creados en Active Directory. Estos datos son comunes a todos los dominios en el bosque. Por tanto los datos del esquema se replican a todos los controladores de dominio del bosque.
2. **Partición de directorio de configuración:** contiene la estructura de los dominios y la topología de replicación. Estos datos son comunes a todos los dominios en el bosque, y se replican a todos los controladores de dominio en el bosque.
3. **Partición de directorio de dominio:** contiene todos los objetos del directorio para este dominio. Dichos datos se replican a todos los controladores de ese dominio, pero no a otros dominios.
4. **Partición de directorio de aplicaciones:** contiene datos específicos de aplicación. Estos datos pueden ser de cualquier tipo excepto *principales de seguridad* (usuarios, grupos y equipos). En este caso, se tiene un control fino sobre el ámbito de la replicación y la ubicación de las réplicas. Este tipo de partición es nuevo de Windows Server 2003.

Además de estas cuatro particiones de directorio de escritura, existe una cuarta categoría de información almacenada en un controlador de dominio: el catálogo global. Un catálogo global es un controlador de dominio que almacena las particiones de directorio de escritura, así como copias parciales de sólo lectura de todas las demás particiones de directorio de dominio del bosque.

3.2.5.3. Funciones de los controladores de dominio

Las versiones anteriores de Windows NT Server usaban múltiples controladores de dominio y sólo se permitía que uno de ellos actualizase la base de datos del directorio. Este esquema de maestro único exigía que todos los cambios se replicasen desde

3.2.5. Estructura física

el controlador de dominio principal (*Primary Domain Controller*, PDC) a los controladores de dominio secundarios o de reserva (*Backup Domain Controllers*, BDCs).

En Windows 2003, todos los controladores de dominio admiten cambios, y estos cambios se replican a todos los controladores de dominio. Las operaciones de administración de usuarios, grupos y equipos son operaciones típicas de múltiples maestros. Sin embargo no es práctico que algunos cambios se realicen en múltiples maestros debido al tráfico de replicación y a los posibles conflictos en las operaciones básicas. Por estas razones, las funciones especiales, como la de servidor de catálogo global y operaciones de maestro único, se asignan sólo a determinados controladores de dominio. A continuación veremos estas funciones.

3.2.5.4. Servidor de catálogo global

El *catálogo global* es un depósito de información que contiene un subconjunto de atributos para todos los objetos de Active Directory (partición de directorio de dominio). Los atributos que se almacenan en el catálogo global son los que se utilizan con más frecuencia en las consultas. El catálogo global contiene la información necesaria para determinar la ubicación de cualquier objeto del directorio.

Un servidor de catálogo global es un controlador de dominio que almacena una copia del catálogo y procesa las consultas al mismo. El primer controlador de dominio que se crea en Active Directory es un servidor de catálogo global. Se pueden configurar controladores de dominio adicionales para que sean servidores de catálogo global con el fin de equilibrar el tráfico de autenticación de inicios de sesión y la transferencia de consultas.

El catálogo global cumple dos funciones importantes en el directorio:

- Permite que un usuario inicie una sesión en la red mediante el suministro de la información de pertenencia a grupos universales a un controlador de dominio cuando inicia un proceso de sesión.
- Permite que un usuario busque información de directorio en todo el bosque, independiente de la ubicación de los datos.

3.2.5.5. Operaciones de maestro único

Un maestro de operaciones es un controlador de dominio al que se le ha asignado una o varias funciones de maestro único en un dominio o bosque de Active Directory. Los controladores de dominio a los que se les asignan estas funciones realizan operaciones que no pueden ocurrir simultáneamente en otros controladores de do-

minio de la red. La propiedad de estas operaciones de maestro único puede ser transferida a otros controladores de dominio.

Todos los bosques de Active Directory deben tener controladores de dominio que cumplan dos de las cinco funciones de operaciones de maestro único. Las funciones para todo el bosque son:

- **Maestro de esquema.** El controlador de dominio maestro de esquema controla todas las actualizaciones y modificaciones del esquema. Para actualizar el esquema de un bosque, debe tener acceso al maestro de esquema.
- **Maestro de nombres de dominio.** El controlador de dominio maestro de esquema controla las operaciones de agregar o quitar dominios del bosque, asegurando que los nombres de dominio sean únicos en el bosque.

Todos los dominios de Active Directory deben tener controladores de dominio que cumplan tres de las cinco funciones de operaciones de maestro único:

- **Maestro de identificadores relativos (RID).** El controlador de dominio maestro de identificadores relativos (RID) asigna secuencias de identificadores relativos a cada uno de los distintos controladores de su dominio.

Cuando un controlador de dominio crea un objeto de usuario, grupo o equipo, asigna al objeto un identificador de seguridad único (SID). Este identificador está formado por un identificador de seguridad de dominio, que es el mismo para todos los que se crean en el dominio, y un identificador relativo que es único para cada identificador de seguridad que se crea en el dominio.

- **Emulador de controlador de dominio principal (PDC).** Para mantener la compatibilidad con servidores basados en Windows NT que puedan funcionar como controladores de dominio de reserva (BDC) en dominios de Windows 2003 en modo mixto, pero todavía requieren un controlador principal de dominio (PDC), se asigna a un controlador de dominio específico basado en Windows 2003, la función de emular a un PDC. A este controlador de dominio lo ven los servidores basados en NT como un PDC.
- **Maestro de infraestructuras.** Cuando los objetos se mueven o se eliminan, un controlador de dominio de cada dominio, el maestro de infraestructura, es el responsable de actualizar los identificadores de seguridad y nombres completos en las referencias de objetos de dominio cruzado de ese dominio.

3.3. Objetos que administra un dominio

El Directorio Activo, tal como se ha visto en capítulos anteriores, es en realidad una base de datos jerárquica de *objetos*, que representan las entidades que pueden administrarse en una red de ordenadores, o, más correctamente en nuestro caso, en un *dominio* de sistemas Windows 2003. Esta base de datos de objetos de administración es compartida, para consulta, por todos los ordenadores miembros del dominio y, para modificación, por todos los controladores del dominio (o DC, *Domain Controllers*).

Por tanto, en Windows 2003, la gestión de un dominio puede realizarse de forma centralizada, administrando únicamente el Directorio Activo. En este contexto, "administrar" significa crear y configurar adecuadamente los objetos del directorio que representan a las entidades o *recursos* que existen en el dominio (recursos como usuarios, grupos, equipos, etc.).

Este apartado expone con detalle los principales tipos de objetos que pueden crearse en el Directorio Activo de Windows 2003, planteando en cada caso sus opciones de configuración y su utilidad dentro de la administración del dominio.

3.3.1. Usuarios globales

En la administración de sistemas Windows 2003 independientes (administración local), se crean en los sistemas cuentas de usuario y de grupo que sirven para:

1. identificar y autenticar a las personas (usuarios) que deben poder acceder al sistema, y
2. administrar los permisos y derechos que permitirán aplicar el control de acceso adecuado a dichos usuarios en el sistema.

Por lo tanto, utilizando únicamente protección local, si una persona debe trabajar en varios ordenadores, necesita poseer una cuenta de usuario en cada uno de ellos. A continuación explicaremos una alternativa a esto.

En un dominio Windows 2003, cualquier servidor que actúa como DC puede crear cuentas de *usuario global*. En este caso, el término "global" debe interpretarse como *global al dominio*. Los datos de una cuenta de usuario global se almacenan en el Directorio Activo y por tanto son conocidos por todos los ordenadores del dominio (en realidad, por todos los ordenadores de *bosque*). En otras palabras, no es que se cree una cuenta para ese usuario en cada ordenador miembro, sino que existe una *única* cuenta (con un único SID) que es visible en todos los ordenadores del dominio. En este caso, cuando una persona se conecta a cualquiera de dichos ordenadores uti-

3.3.2. Grupos

lizando para ello su cuenta de usuario global, el ordenador en cuestión realiza una consulta al Directorio Activo (i.e., a alguno de los DCs) para que se validen las credenciales del usuario. El resultado de la validación es enviado al ordenador miembro (y de éste al usuario), concediendo o rechazando la conexión.

Los ordenadores miembros de un dominio que no sean DCs, además de conocer a los usuarios globales del dominio, pueden crear también sus propios usuarios *locales*. En este caso, estos usuarios son únicamente visibles en el ordenador en el que han sido creados. Cuando una persona desea entrar en el sistema utilizando una cuenta local, dicha cuenta se valida contra la base de datos local de ese ordenador. Además, es importante resaltar que a dicho usuario local no se le pueden asignar permisos sobre recursos que residan en otro sistema Windows 2003 (puesto que allí no existe). Por el contrario, a un usuario global se le pueden conceder permisos sobre cualquier recurso (archivo, directorio, impresora, etc.) de cualquier ordenador miembro del dominio, puesto que es visible (y posee el mismo SID) en todos ellos.

3.3.2. Grupos

De forma análoga a los usuarios globales, existen *grupos* que son almacenados en el Directorio Activo y que por tanto son visibles desde todos los ordenadores del dominio (y, en algunos casos, también de otros dominios del bosque). En el directorio pueden crearse dos tipos de grupos: grupos de distribución y grupos de seguridad. Los primeros se utilizan exclusivamente para crear listas de distribución de correo electrónico, mientras que los segundos son los que se utilizan con fines administrativos. Por este motivo, a partir de ahora nos referiremos exclusivamente a los grupos de seguridad.

En concreto, en dominios Windows 2003 se definen tres clases de grupos de seguridad (o, de forma más precisa, se pueden definir grupos de tres *ámbitos* distintos):

1. **Grupos locales del dominio.** En un dominio en nivel funcional Windows 2000 mixto, pueden contener cuentas de usuario y grupo globales de cualquier dominio del bosque. En un dominio en nivel Windows 2000 nativo o Windows Server 2003, pueden contener, además, grupos universales y otros grupos locales del dominio. Sólo son visibles en el dominio en que se crean, y suelen utilizarse para conceder permisos y derechos en cualquiera de los ordenadores del dominio (nótese que en modo mixto, sólo son visibles por los DCs del dominio, y por tanto sólo se pueden utilizar para administrar permisos y derechos en esos ordenadores).
2. **Grupos globales.** En un dominio en nivel funcional Windows 2000 mixto, pueden contener cuentas de usuario globales del mismo dominio. En un dominio

3.3.2. Grupos

en nivel Windows 2000 nativo o Windows Server 2003, pueden contener, además, otros grupos globales del mismo dominio. Son visibles en todos los dominios del bosque, y suelen utilizarse para clasificar a los usuarios en función de las labores que realizan.

3. **Grupos universales.** Sólo están disponibles en dominios en nivel funcional Windows 2000 nativo o Windows Server 2003 nativo. Pueden contener cuentas de usuario y grupos globales, así como otros grupos universales, de cualquier dominio del bosque. Son visibles en todo el bosque.

En un ordenador miembro de un dominio también se pueden definir grupos locales. Los grupos locales pueden estar formados por cuentas de usuario locales y usuarios y grupos globales de cualquier dominio del bosque (en modo mixto) y además por grupos universales (en modo nativo). Un grupo local no puede ser miembro de otro grupo local. Los grupos locales pueden utilizarse para conceder permisos y derechos en el equipo en que son creados.

Por tanto, la administración de la protección en cada ordenador del dominio puede realizarse mediante grupos locales del dominio o grupos locales del equipo en que reside el recurso a administrar. Por tanto, la recomendación que se hacía en la protección local respecto a la asignación de permisos en base a grupos locales sigue siendo válida. En el caso más general, la regla que recomienda Windows 2003 es la siguiente:

1. Asignar usuarios globales a grupos globales, según las labores que desempeñen en la organización.
2. Incluir (usuarios y/o) grupos globales en grupos locales (del equipo o del dominio) según el nivel de acceso que vayan a tener.
3. Asignar permisos y derechos únicamente a estos grupos locales (del equipo o del dominio).

La utilización de grupos universales tiene sentido sólo cuando un mismo conjunto de usuarios (y/o grupos) de varios dominios deben recibir permisos/derechos en varios dominios simultáneamente. En Windows 2000, el uso de este tipo de grupo estaba muy desaconsejado, por dos motivos: primero, porque estos grupos y sus miembros deben replicarse en todos los catálogos globales del bosque, y segundo, porque cualquier inicio de sesión de un usuario debe consultar a un catálogo global para determinar la pertenencia de dicho usuario a posibles grupos universales. Windows 2003 ha suavizado el primero de los problemas, mejorando la eficiencia de esa replicación (sólo si el bosque está en nivel funcional Windows Server 2003), de for-

3.3.3. Equipos

ma que su uso no está ahora tan desaconsejado como lo estaba en Windows 2000. En cualquier caso, el uso de un grupo universal siempre puede simularse con la combinación adecuada de grupos globales y locales del dominio. Se recomienda al lector reflexionar sobre cómo podría hacerse.

En relación con esto, es importante saber que cuando un ordenador pasa a ser miembro de un dominio, el grupo global **Administradores del dominio** se incluye automáticamente en el grupo local **Administradores** de dicho ordenador. De igual forma, el grupo global **Usuarios del dominio** se incluye dentro del grupo local **Usuarios**. De esta forma, los administradores y usuarios normales del dominio tienen en cada miembro los mismos derechos y permisos que los que tengan ya definidos los administradores y usuarios locales, respectivamente. El administrador local puede, si lo desea, invalidar esta acción automática, extrayendo posteriormente los grupos globales de los locales.

3.3.3. Equipos

Como hemos visto, en el Directorio Activo de un dominio se conserva toda la información relativa a cuentas de usuarios y grupos globales. Esta misma base de datos de directorio recoge también una *cuenta de equipo* por cada uno de los ordenadores miembro de un dominio.

Entre otras informaciones, en cada una de estas cuentas se almacena el nombre del ordenador, así como un identificador único y privado que lo identifica únicamente. Este identificador es análogo al SID de cada cuenta de usuario o grupo, y sólo lo conocen los DCs y el propio ordenador miembro. Es por tanto, un dato interno del sistema operativo, y ni siquiera el administrador puede cambiarlo. Es precisamente este dato, propio de las cuentas de usuario, grupo y equipo, lo que permite asignar permisos y derechos en los sistemas a estos tres tipos de cuentas. Por este motivo, se denominan *principales de seguridad (security principals)*. Por tanto, la asignación de derechos y permisos (NTFS) a cuentas de equipo es posible, pero se limita a situaciones muy poco frecuentes y está fuera del ámbito de este texto.

Windows 2003 puede utilizar distintos protocolos de comunicaciones seguros entre los ordenadores miembro de un dominio y los DCs. Entre ellos los más importantes son NTLM (el protocolo utilizado por versiones anteriores de Windows NT, que se mantiene por compatibilidad hacia atrás) y Kerberos V5. Kerberos presenta numerosas ventajas respecto a NTLM, pero sólo es viable en la práctica si todas las máquinas del dominio son Windows 2000, Windows XP o Windows Server 2003. Estos protocolos se utilizan siempre que información relativa a aspectos de seguridad se intercambia entre sistemas pertenecientes a algún dominio y, en concreto, para autenticar usuarios (como se ha explicado arriba).

3.3.4. Unidades Organizativas

Como hemos visto en Sección 3.2.4.5, “Unidades Organizativas”, las unidades organizativas son objetos del directorio que a su vez, pueden contener otros objetos. El uso fundamental de las OUs es delegar la administración de sus objetos a otros usuarios distintos del administrador del dominio, y personalizar el comportamiento de los usuarios y/o equipos mediante la aplicación de directivas de grupo (GPOs) específicas a la unidad.

3.4. Compartición de recursos

Cuando un sistema Windows 2003 participa en una red (grupo de trabajo o dominio), puede compartir sus recursos con el resto de ordenadores. En este contexto, sólo vamos a considerar como recursos a compartir las *carpetas* o directorios que existen en un sistema Windows. La compartición de otros recursos (tales como impresoras, por ejemplo) queda fuera del ámbito de este texto.

3.4.1. Permisos y derechos

Cualquier sistema Windows 2003 puede compartir carpetas, tanto si es un servidor como si es una estación de trabajo. Para poder compartir una carpeta basta con desplegar su menú contextual desde una ventana o desde el explorador de archivos, y seleccionar Compartir.... En la ventana asociada a esta opción se determina el nombre que tendrá el recurso (que no tiene por qué coincidir con el nombre de la propia carpeta), así como qué usuarios van a poder acceder al mismo. En relación con esto, existe una gran diferencia entre que el directorio resida en una partición FAT y que resida en una NTFS.

Si la carpeta reside en una partición FAT, este filtro de acceso será el único que determine los usuarios que van a poder acceder al contenido de la carpeta, puesto que no es posible determinar permisos sobre la misma o sus archivos. Es decir, el filtro sólo se establece para poder acceder al recurso. Si un usuario tiene permisos suficientes para conectarse a un recurso, tendrá acceso sobre todos los archivos y subcarpetas del recurso. Concretamente, el tipo de acceso sobre todos ellos será el que le permita el permiso sobre el recurso (Lectura, Escritura o Control Total).

Por el contrario, si la carpeta se encuentra en una partición NTFS, ésta tendrá unos permisos establecidos (así como sus subcarpetas y archivos), al margen de estar o no compartida. En este caso también es posible establecer permisos desde la ventana de Compartir..., pero entonces sólo los usuarios que puedan pasar *ambos* filtros podrán acceder a la carpeta compartida y a su contenido. En este caso se recomienda dejar Control Total sobre Todos en los permisos asociados al recurso (opción por defecto), y controlar quién (y cómo) puede acceder al recurso y a su contenido mediante los permisos asociados a dicha carpeta (y a sus archivos y sub-

3.4.2. Compartición dentro de un dominio

carpetas). Sin embargo, esta no es la opción por defecto en Windows Server 2003 (aunque sí lo era en Windows 2000), que sólo concede inicialmente el permiso de lectura al grupo Todos al compartir una carpeta.

Esta recomendación es muy útil, si tenemos en cuenta que de esta forma para cada carpeta (y archivo) del sistema no utilizamos dos grupos de permisos sino uno solo, independientemente de que la carpeta sea o no compartida. Este forma de trabajar obliga al administrador a asociar los permisos correctos a cada objeto del sistema (aunque no esté compartido), pero por otra parte se unifica la visión de la seguridad de los archivos, con lo que a la larga resulta más segura y más sencilla.

Cuando compartimos recursos a otros usuarios en la red (especialmente en un dominio) hay que tener en cuenta no sólo los permisos del recurso y su contenido, sino también los *derechos* del ordenador que comparte el recurso. En concreto, si un usuario ha iniciado una sesión interactiva en un ordenador Windows 2003 denominado A, y desea conectarse a un recurso de red que exporta otro Windows 2003 denominado B, además de poseer suficientes permisos (sobre el recurso, sobre el propio carpeta y sobre su contenido), tiene que tener concedido en B el derecho *Acceder a este equipo desde la red*. De lo contrario, dicho usuario ni siquiera podrá obtener la lista de los recursos que el ordenador B comparte.

3.4.2. Compartición dentro de un dominio

Cuando la compartición de recursos la realizan equipos que forman parte de un dominio Windows 2003, existen consideraciones que el administración debe conocer.

Primero, una vez se ha compartido físicamente una carpeta en la red (según el procedimiento descrito arriba), el administrador del dominio puede además *publicar* este recurso en el directorio. Para ello debe crear un nuevo objeto, en la unidad organizativa adecuada, de tipo *Recurso compartido*. A este objeto se le debe asociar un nombre simbólico y el nombre de recurso de red que representa (de la forma \\equipo\recurso). Es importante tener en cuenta que cuando se publica el recurso de esta forma, no se comprueba si realmente existe o no, por lo que es responsabilidad del administrador el haberlo compartido y que su nombre coincida con el de la publicación. Una vez publicado, el recurso puede localizarse mediante búsquedas en el Directorio Activo, como el resto de objetos del mismo. Windows Server 2003 ha introducido otra forma de publicación: entre las opciones de la pestaña "Compartir" del explorador de archivos, puede publicarse dicha compartición en el directorio, simplemente asignándole un nombre simbólico. Si se publica de esta forma, el proceso crea automáticamente el objeto que representa la carpeta compartida en el directorio.

Y segundo, cuando un sistema Windows 2003 se agrega a un dominio, los siguientes recursos se comparten de forma automática y por defecto (estas comparti-

3.4.3. Mandatos Windows 2003 para compartir recursos

ciones no deben modificarse ni prohibirse):

- letra_de_unidad\$. Por cada partición existente en el sistema Windows 2003 (C:, D:, etc.) se crea un recurso compartido denominado C\$, D\$, etc. Los administradores del dominio, así como los operadores de copia del domino, pueden conectarse por defecto a estas unidades.
- ADMIN\$. Es un recurso utilizado por el propio sistema durante la administración remota de un ordenador Windows 2003.
- IPC\$. Recurso que agrupa los tubos (colas de mensajes) utilizados por los programas para comunicarse entre ellos. Se utiliza durante la administración remota de un ordenador Windows 2003, y cuando se observa los recursos que comparte.
- NETLOGON. Recurso que exporta un DC para proporcionar a los ordenadores miembros del dominio el servicio de validación de cuentas globales a través de la red (*Net Logon service*).
- SYSVOL. Recurso que exporta cada DC de un dominio. Contiene información del Directorio Activo (por ejemplo, de directivas de grupo) que debe replicarse en todos los DCs del dominio.

En relación con los nombres de estos recursos, es interesante saber que añadir el carácter "\$" al final de cualquier nombre de recurso tiene un efecto específico: prohíbe que dicho recurso se visualice dentro de la lista de recursos que una máquina exporta al resto. Es decir, convierte un recurso en "invisible" para al resto del mundo. En este caso, un usuario remoto sólo podrá conectarse al recurso si conoce su nombre de antemano (y tiene suficientes permisos, obviamente).

3.4.3. Mandatos Windows 2003 para compartir recursos

La compartición de recursos en Windows 2003 puede realizarse en línea de órdenes utilizando los mandatos **net share** y **net use**. La sintaxis de ambos mandatos es la siguiente:

1. Mandato **net share**: Crea, elimina o muestra recursos compartidos.

```
net share
net share recurso_compartido
net share recurso_compartido=unidad:ruta_de_acceso
    [/users:número | /unlimited] [/remark:"texto"]
net share recurso_compartido [/users:número | unlimited]
    [/remark:"texto"]
net share {recurso_compartido | unidad:ruta_de_acceso} /delete
```

2. Mandato **net use**: Conecta o desconecta un equipo de un recurso compartido o muestra información acerca de las conexiones del equipo. También controla las conexiones de red persistentes.

```
net use [nombre_dispositivo]
[\\nombre_equipo\recurso_compartido[\volumen]]
[contraseña | *] [/user:[nombreDominio\]nombre_usuario]
[[/delete] | [/persistent:{yes | no}]]
net use nombre_dispositivo [/home[contraseña | *]]
    [/delete:{yes | no}]
net use [/persistent:{yes | no}]
```

3.5. Delegación de la administración

Para delegar, total o parcialmente, la administración de una unidad organizativa existe un asistente (*wizard*) que aparece cuando se selecciona la acción **Delegar el control...** en el menú contextual de la unidad organizativa. Este asistente pregunta básicamente los dos aspectos propios de la delegación: *a quién* se delega y *qué* se delega. La primera pregunta se contesta o bien con un usuario o con un grupo (se recomienda un grupo). Para responder a la segunda pregunta, se puede elegir una tarea *predefinida* a delegar (de entre una lista de tareas frecuentes), o bien podemos optar por construir una tarea personalizada. En este último caso, tenemos que especificar la tarea mediante un conjunto de permisos sobre un cierto tipo de objetos del directorio. Esto se explica a continuación.

Internamente, los derechos de administración (o control) sobre un dominio o unidad organizativa funcionan de forma muy similar a los permisos sobre una carpeta o archivo: existe una DACL propia y otra heredada, que contienen como entradas aquellos usuarios/grupos que tienen concedida (o denegada) una cierta acción sobre la unidad organizativa o sobre su contenido. En este caso, las acciones son las propias de la administración de objetos en el directorio (control total, creación de objetos, modificación de objetos, consulta de objetos, etc.), donde los "objetos" son las entidades que pueden ser creados dentro de la unidad: usuarios, grupos, unidades organizativas, recursos, impresoras, etc.

En resumen, la delegación de control sobre una unidad organizativa puede hacerse de forma completa (ofreciendo el *Control Total* sobre la unidad) o de forma parcial (permitiendo la lectura, modificación y/o borrado de los objetos de la misma). Hay que tener en cuenta que en el caso de la delegación parcial, el número de posibilidades es inmenso: por una parte, se incluye la posibilidad de establecer el

3.5. Delegación de la administración

permiso sobre cada *atributo* de cada tipo de objeto posible; por otra parte, se puede establecer a qué unidades se va a aplicar la regla (sólo en esa unidad organizativa, en todas las que se sitúan por debajo, en parte de ellas, etc.). Por tanto, para una delegación parcial se recomienda el uso del asistente, ya que su lista de delegación de tareas más frecuentes (como por ejemplo "Crear, borrar y administrar cuentas de usuario" o "Restablecer contraseñas en cuentas de usuario") resulta muy útil. Sin embargo, cuando la delegación que buscamos no se encuentra en la lista, tendremos que diseñar una a medida, asignando los permisos oportunos sobre los objetos del directorio que sean necesarios.

4

Administración de Políticas de Grupo

Índice

4.1. Introducción	61
4.2. Objeto de Política de Grupo (GPO)	61
4.3. Aplicación de Políticas de Grupo	63
4.4. Políticas de Grupo y grupos de seguridad	65
4.4.1. Filtrar el ámbito de aplicación de un GPO	65
4.4.2. Delegar la administración de un GPO	65
4.5. Principales políticas incluidas en un GPO	66
4.5.1. Plantillas administrativas	67
4.5.2. Configuraciones de seguridad	68
4.5.3. Instalación de software	68
4.5.4. Guiones (Scripts)	69
4.5.5. Redirección de carpetas	70
4.5.6. Otras políticas	70
4.6. Recomendaciones de uso	70

4.1. Introducción

Este capítulo introduce una de las herramientas que incluye Windows Server 2003 para centralizar la administración y configuración de usuarios y equipos en un dominio: las *Políticas o Directivas de Grupo* (*Group Policies*). Las políticas de grupo permiten establecer de forma centralizada múltiples aspectos de la configuración que reciben los usuarios cuando se conectan a una máquina del dominio. Estos aspectos incluyen, entre otros, configuraciones del registro, políticas de seguridad, instalación automática de software, ejecución de *scripts*, redirección de carpetas locales a recursos de red, etc.

4.2. Objeto de Política de Grupo (GPO)

En cada sistema Windows Server 2003, forme parte o no de un dominio, existe una *política local* que el administrador puede editar según su criterio para ajustar el comportamiento de dicho equipo. Lógicamente, cuando hay muchos equipos que administrar, resultaría incómodo tener que establecer este comportamiento uno por uno. Por este motivo, las políticas de grupo se han integrado dentro de la administración del Directorio Activo como una herramienta de configuración centralizada en dominios Windows 2003.

En concreto, las políticas se especifican mediante objetos de directorio denominados *Objetos de Política de Grupo* (*Group Policy Objects*), o simplemente GPOs. Un GPO es un objeto que incluye como atributos cada una de las políticas (también denominadas *directivas*) que puede establecerse en Windows Server 2003 para equipos y usuarios. Los GPOs se crean y posteriormente se *vinculan* a distintos *contenedores* del Directorio Activo (sitios, dominios y unidades organizativas), de forma que los usuarios y equipos que se ubican dentro de estos contenedores reciben los parámetros de configuración establecidos en dichos GPOs. De esta forma, y utilizando sólo el Directorio Activo, cada equipo y cada usuario del dominio puede recibir una configuración apropiada según el tipo de tarea que debe desempeñar. De entre los contenedores que existen por defecto al crear un dominio, el que representa al dominio y la unidad organizativa *Domain Controllers* ya tienen creados y vinculados sendos GPOs, con un conjunto mínimo de configuraciones. Al resto de unidades organizativas (*Builtin*, *Users* y *Computers*) no se les pueden asociar GPOs. Por lo tanto, para poder implementar un esquema de GPOs en un dominio es necesario crear primero una estructura adecuada de unidades organizativas, y distribuir en ellas los objetos usuario/equipo.

Dentro de cada GPO, las políticas se organizan jerárquicamente en un *árbol temático* que permite una distribución lógica de las mismas (ver Figura 4.1, “Herramienta de configuración de un GPO”). En este árbol de políticas, justo debajo del nodo raíz,

4.2. Objeto de Política de Grupo (GPO)

existen dos *nodos principales* que separan las configuraciones para equipos y para usuarios:

1. La **configuración del equipo** agrupan todos aquellos parámetros de configuración que pueden establecerse a nivel de equipo. Cuando un GPO afecta a un equipo, todas aquellas políticas de equipo del GPO que el administrador haya configurado se aplicarán al equipo cada vez que se inicie.
2. Las **configuración de usuario** agrupan los parámetros de configuración que pueden establecerse a nivel de usuario. Cuando un GPO afecta a un usuario, todas aquellas políticas de usuario del GPO que el administrador haya configurado se aplicarán cuando dicho usuario inicie una sesión local (en cualquier equipo del dominio).

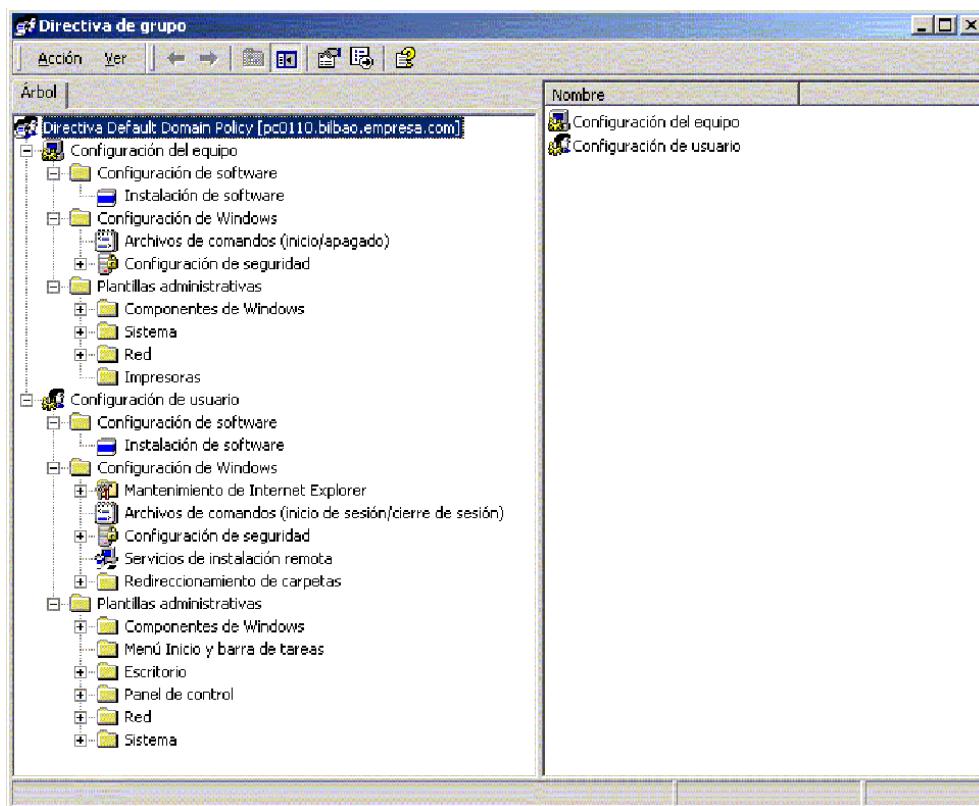


Figura 4.1. Herramienta de configuración de un GPO

Además de esa aplicación inicial de las políticas (en el inicio de los equipos y en el inicio de sesión de los usuarios), éstas se reevalúan automáticamente bajo demanda del administrador y, además, de forma periódica. Por defecto, la reevaluación periódica se produce cada 90 minutos, con un retraso aleatorio de hasta 30 minutos.

4.3. Aplicación de Políticas de Grupo

Por último, en cada GPO, el administrador puede *deshabilitar* selectivamente las políticas de equipo y/o de usuario, lo cual evita que se procesen y puedan aplicarse. Esto resulta útil en aquellos casos en los que en un GPO sólo se configuran políticas de uno de ambos tipos. Supongamos, por ejemplo, que en un GPO se han configurado únicamente ciertas políticas de equipo (y ninguna de usuario). Si el administrador no deshabilita la parte de políticas de usuario, el sistema las seguirá procesando (aunque no las aplicará, al no estar configuradas) para cada usuario al que afecte el GPO, con el consiguiente retraso (no útil) en el inicio de sesión de dicho usuario.

4.3. Aplicación de Políticas de Grupo

A partir de lo expuesto en el apartado anterior, se puede deducir lo siguiente respecto a cómo se aplican las políticas de grupo:

- Un mismo GPO puede contener indistintamente parámetros o políticas) de configuración que deben aplicarse a equipo y a usuarios.
- Cada GPO se vincula a un contenedor del directorio activo (un sitio, un dominio o una unidad organizativa), afectando implícitamente a todos los objetos que residen en él:
 - Los equipos se verán afectados por las políticas de equipo del GPO.
 - Los usuarios se verán afectados por las política de usuario del GPO.
 - Los sub-contenedores *heredarán* el GPO completo.

Es decir, los GPOs vinculados a un *sitio* son heredados por su *dominio*. Estos GPOs, más los vinculados al dominio, son heredados por las *unidades organizativas* de primer nivel establecidas en el dominio. Todos ellos, más los vinculados a estas unidades organizativas, son heredados por las unidades de segundo nivel ubicadas dentro de aquellas, y así sucesivamente.

- Existe una relación "muchos a muchos" entre contenedores y GPOs: un mismo GPO puede vincularse a múltiples contenedores y un contenedor puede tener vinculados múltiples GPOs.

En resumen, las políticas de grupo son *heredables* y *acumulativas*. Eso quiere decir que, desde el punto de vista de un equipo o de un usuario concretos, la lista de GPOs que les afecta depende de su ubicación en Directorio Activo: esta lista incluye *todos* los GPOs vinculados a los contenedores por los que hay que pasar para llegar desde el sitio (y dominio) hasta la unidad organizativa concreta donde ese equipo o usuario se ubica.

4.3. Aplicación de Políticas de Grupo

Puesto que cada GPO incorpora los mismos (posibles) parámetros de configuración, es posible que se produzcan conflictos entre los distintos GPOs que afectan a un usuario/equipo. Resulta necesario que exista un orden de aplicación concreto y conocido, de forma que se sepa finalmente qué política(s) afectarán a cada usuario y equipo. Este orden es el siguiente:

1. Se aplica la política de grupo local del equipo (denominada *Local Group Policy Object*, o LGPO).
2. Se aplican los GPOs vinculados a sitios.
3. Se aplican los GPOs vinculados a dominios.
4. Se aplican los GPOs vinculados a unidades organizativas de primer nivel. En su caso, posteriormente se aplicarían GPOs vinculados a unidades de segundo nivel, de tercer nivel, etc.

Este orden de aplicación decide la *prioridad* entre los GPOs, puesto que una política que se aplica más tarde prevalece sobre otras establecidas anteriormente (las *sobreescribe*). De forma análoga a lo establecido para permisos en el sistema de archivos NTFS, podríamos decir que las políticas explícitas de un contenedor tienen prioridad (se aplican más tarde) sobre las políticas heredadas de contenedores superiores. Este comportamiento puede ser refinado mediante los siguientes dos parámetros:

1. **Forzado** (*Enforced*). Este parámetro puede activarse independientemente a cada vínculo de un GPO. En particular, si el vínculo de un GPO a un contenedor tiene este parámetro activado, sus políticas no pueden ser sobreescritas por GPOs que se apliquen posteriormente (a subcontenedores de dicho contenedor).
2. **Bloquear herencia de directivas** (*Block policy inheritance*). Este parámetro pertenece a los contenedores del Directorio Activo. En particular, si un *contenedor* tiene este parámetro activado, se desactiva la herencia de las políticas establecidas en contenedores superiores, *excepto* aquellas que corresponden a GPOs vinculados con el parámetro "Forzado".

El comportamiento que se acaba de describir afecta a todos los equipos y a todos los usuarios del dominio en función, exclusivamente, de su ubicación dentro del Directorio Activo. En el caso de las políticas de usuario, este comportamiento y la propia administración de los GPOs puede refinarse aún más utilizando grupos de seguridad.

4.4. Políticas de Grupo y grupos de seguridad

Como todos los objetos del Directorio Activo, los GPOs poseen listas de control de acceso (o DACLs). En general, estas DACLs establecen qué usuarios y grupos pueden leer, escribir, administrar, etc., dichos objetos. En el caso concreto de los GPOs, esta asociación de permisos a *grupos de usuarios* (o grupos de seguridad) permite filtrar el ámbito de aplicación de un GPO y delegar su administración.

4.4.1. Filtrar el ámbito de aplicación de un GPO

Uno de los permisos de cada GPO es "Aplicar directiva de grupos" (o, simplemente, *Aplicar*). Por defecto, este permiso lo tienen concedido el grupo *Usuarios autenticados*, que incluye en la práctica a todos los usuarios del dominio. Por tanto, la política afecta a todos los usuarios cuyas cuentas se ubiquen dentro del contenedor al que se vincula el GPO.

Si este comportamiento no es el que se desea, se puede eliminar este permiso y concederlo a otro(s) grupo(s) más restringidos, o bien mantener este permiso y añadir permisos negativos a otros grupos. Hay que tener en cuenta varias cosas a este respecto:

- Si denegamos el permiso *Aplicar* a un grupo, impediremos que sus políticas afecten a cualquiera de sus miembros, aunque pertenezca a otros grupos que tengan este permiso concedido.
- El permiso *Aplicar* debe asignarse conjuntamente con el permiso *Leer*, ya que si no, el GPO no se aplica al grupo correspondiente. Si asignamos *Aplicar* a grupos más restringidos que el de Usuarios Autentificados, es recomendable que hagamos lo mismo con el permiso *Leer*, puesto que el GPO se *procesa* para todos los usuarios que poseen este permiso, aunque sólo se *aplica* a los que poseen además el *Aplicar*.
- Existe un caso en el que no se puede seguir esta recomendación: si la política no debe aplicarse al grupo de administradores, éstos no deben tener concedido el permiso *Aplicar*. Sin embargo, no es posible eliminar el permiso *Leer* a estos usuarios porque entonces no podrían administrar el GPO.

4.4.2. Delegar la administración de un GPO

Cualquier usuario o grupo que tenga concedido el permiso de Control Total sobre un GPO puede administrarlo. Por defecto, en este caso se encuentran:

4.5. Principales políticas incluidas en un GPO

- el grupo Administración de Empresas,
- el grupo Administradores del Dominio,
- el creador del GPO (*Creator Owner*),
- y el sistema (*System*).

A pesar de que estos grupos no tienen concedido el permiso "Aplicar a", los administradores también reciben por defecto la política, puesto que forman parte del grupo Usuarios Autentificados.

Es posible delegar la administración de GPOs a otros usuarios y grupos. En realidad, la administración de un GPO consta de dos actividades distintas y complementarias, que pueden delegarse independientemente:

1. **Creación de un GPO.** La creación de un GPO es una actividad previa (e independiente) a su vinculación a un contenedor del directorio. Unicamente los administradores de empresa y dominio y aquellos usuarios o grupos miembros del grupo *Group Policy Creator Owners* pueden crear nuevos objetos de este tipo. Por tanto, el administrador puede delegar esta acción haciendo que un cierto usuario o grupo pertenezca a este grupo de creadores de GPOs.
2. **Vinculación de un GPO a un contenedor.** Esta acción se controla mediante permisos específicos del *contenedor* (sitio, dominio o unidad organizativa), y puede delegarse mediante una de las tareas de delegación predefinidas denominada *Manage Group Policy links*. El procedimiento para realizar este tipo de delegaciones se encuentra en la Sección 3.5, "Delegación de la administración".

4.5. Principales políticas incluidas en un GPO

Como se ha visto en previamente, cada GPO consta de un árbol de políticas, subdividido en su nivel más alto en dos subárboles denominados *Configuración de equipo* y *Configuración de usuario*. La jerarquía de políticas en cada uno de ellos se subdivide en tres grupos:

1. **Configuración de Software** (*Software Settings*). Contiene la configuración, bien del equipo o bien de usuario, de la instalación automática de software.
2. **Configuración de Windows** (*Windows Settings*). Contiene la configuración de ciertos parámetros de Windows, como parámetros de seguridad o *scripts*, para

el equipo o para el usuario.

3. **Plantillas Administrativas** (*Administrative Templates*). Contiene las políticas y configuraciones que se guardan en el registro de Windows, para el equipo o para el usuario.

Es decir, en muchos casos, la misma política existe en ambos subárboles (equipo y usuario), aunque generalmente en cada caso con significados y parámetros distintos. Por ejemplo, bajo *Configuración del Equipo--Configuración de Windows--Scripts* podemos encontrar los *scripts* que deben ejecutarse cada vez que el equipo se inicia o detiene, mientras que bajo *Configuración de Usuario--Configuración de Windows--Scripts* se encuentran los *scripts* que deben ejecutarse cada vez que el usuario inicia o finaliza una sesión local.

A continuación se exponen los grupos de políticas más importantes que pueden configurarse mediante un GPO, independientemente de su ubicación concreta dentro de la jerarquía.

4.5.1. Plantillas administrativas

Este grupo contiene todas las configuraciones de políticas basadas en el registro de Windows 2003, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows Server 2003 y de algunas aplicaciones que utilizan estas políticas.

Estas políticas han sido rediseñadas respecto a sus homólogas en Windows NT 4.0, que tenían un serio inconveniente: una vez se habían aplicado, su efecto era *permanente* porque modificaban los valores del registro en su ubicación original, perdiéndose el valor anterior. Por ello, al eliminar la política no se desactivaban y la única forma de hacerlo era estableciendo políticas contrarias o editando el registro manualmente. En Windows Server 2003, las políticas que afectan el registro se almacenan en un lugar del registro dedicado exclusivamente a las Políticas de Grupo. Esto significa que dejan de tener efecto (y se recupera el valor por defecto original del registro) si el GPO que las estableció deja de estar en uso. En la terminología de Windows Server 2003, las nuevas políticas se denominan *políticas verdaderas (true policies)*, mientras que las que no cumplen con esta nueva filosofía se denominan *preferencias (Group policy preferences)*, y su uso está claramente desaconsejado. Por defecto, todas las políticas que pueden seleccionarse bajo el apartado de Plantillas Administrativas de un GPO son verdaderas.

4.5.2. Configuraciones de seguridad

En este apartado se encuentra la configuración de muchos de los aspectos de seguridad que pueden establecerse en un sistema Windows Server 2003.

En concreto, y centrándonos en los aspectos de seguridad a nivel de equipo, podemos destacar los siguientes (de entre muchos más):

1. **Políticas de Cuentas.** Se pueden configurar todos los aspectos sobre el plan de cuentas que se vieron en la Sección 2.5.1, “Otras directivas de seguridad”, tales como caducidad de contraseñas, bloqueo de cuentas, configuración de Kerberos, etc.
2. **Políticas Locales.** Bajo este apartado se encuentran las configuraciones que corresponden a la denominada “Directiva local” de la Sección 2.5.1, “Otras directivas de seguridad”, es decir, la configuración de la auditoría, la asignación de derechos y privilegios de usuario y las opciones de seguridad.
3. **Registro de Eventos.** Aquí se controla el registro de eventos en los registros de aplicación, seguridad y sistema, que posteriormente pueden visualizarse con la herramienta Visor de Sucesos.

4.5.3. Instalación de software

Mediante este apartado se puede *asignar* y/o *publicar* aplicaciones a equipos o a usuarios en el dominio:

1. **Asignar** una aplicación significa que los usuarios que la necesitan la tienen disponible en su escritorio sin necesidad de que un administrador la instale. Cuando se asigna una aplicación a un usuario o equipo, se crea una entrada para ella en el menú de inicio y se configura el registro adecuadamente. La primera vez que el usuario ejecuta la aplicación, ésta es automáticamente instalada en el equipo cliente.
2. **Publicar** una aplicación a un equipo o usuario le da la oportunidad al usuario de instalar dicha aplicación bajo demanda (a voluntad), pero no se realiza ninguna acción automática en el equipo (no se modifica el menú de inicio ni el registro). La lista de aplicaciones publicadas para un usuario aparecen en el Panel de Control, bajo la herramienta de *Añadir/Eliminar Programas*, desde donde pueden ser instaladas.

4.5.4. Guiones (Scripts)

Bajo este apartado, se pueden asignar *scripts* a equipos o usuarios. En concreto, existen cuatro tipos de *scripts* principales:

1. **Inicio** (equipo). Se ejecuta cada vez que el equipo arranca.
2. **Apagado** (equipo). Se ejecuta cada vez que el equipo va a detenerse.
3. **Inicio de sesión** (usuario). Se ejecuta cada vez que el usuario inicia una sesión interactiva (local) en un equipo.
4. **Cierre de sesión** (usuario). Se ejecuta cada vez que el usuario se finaliza una sesión interactiva en un equipo.

En todos esos casos, los *scripts* pueden implementarse en cualquiera de los lenguajes que entiende el soporte de *scripts* independiente del lenguaje de Windows Server 2003, o *Windows Scripting Host*. Actualmente existe soporte para Visual Basic Scripting Edition, Java Script, PERL y los tradicionales archivos por lotes MS-DOS. Es posible que en el futuro se incluya soporte para otros lenguajes como Tcl-Tk o Python.

El comportamiento de los *scripts* puede perfilarse mediante algunas políticas que se sitúan en el apartado de Plantillas Administrativas. En la tabla a continuación se muestran algunas que resulta útil conocer.

Tabla 4.1. Principales políticas que afectan el comportamiento de los *scripts*

Config. del Equipo--Plantillas Administrativas--Sistema--Inicio de Sesión	
Política	Significado
Ejecutar secuencia de comandos de inicio de sesión de forma síncrona.	Si esta política está activada, Windows 2000 espera a que se hayan procesado los <i>scripts</i> de inicio antes de iniciar el escritorio. Esta opción también existe para el usuario, pero la establecida aquí tiene preferencia.
Ejecutar archivos de comandos de inicio de forma asíncrona.	Por defecto, los <i>scripts</i> de inicio de equipo se ejecutan ocultos y de forma síncrona (el sistema operativo no termina de arrancar hasta que se han procesado completamente). Esta política permite cambiar este comportamiento por defecto.
Ejecutar archivos de comandos de inicio visibles.	Si está habilitada, los <i>scripts</i> de inicio del sistema se ejecutan visibles en una ventana de órdenes.
Ejecutar archivos de comandos de apagado visibles.	Esta es la política equivalente a la anterior para los <i>scripts</i> de detención del equipo.
Tiempo de espera máximo para secuencias de comandos de directivas de grupo.	El tiempo máximo de espera para los <i>scripts</i> (en el caso de que se queden suspendidos, por ejemplo) es de 600 segundos. Mediante esta política se puede cambiar este intervalo, hasta un máximo de 32000 segundos.

4.5.5. Redirección de carpetas

Config. de Usuario--Plantillas Administrativas--Sistema--Inicio/Cierre de Sesión	
Política	Significado
Ejecutar secuencia de comandos de inicio de sesión de forma síncrona.	Si esta política está activada, Windows Server espera a que se hayan procesado los <i>scripts</i> de inicio antes de iniciar el escritorio.
Ejecutar archivos de comandos de inicio de sesión visibles.	Si está habilitada, los <i>scripts</i> de inicio de sesión del usuario se ejecutan visibles en una ventana de órdenes.
Ejecutar archivos de comandos de cierre de sesión visibles	Esta es la política equivalente a la anterior para los <i>scripts</i> de fin de sesión del usuario.

4.5.5. Redirección de carpetas

Este grupo de políticas permite redirigir la ubicación local predefinida de ciertas carpetas particulares de cada usuario (como "Mis Documentos" o el menú de inicio) a otra ubicación, bien sea en la misma máquina o en una unidad de red.

Un ejemplo útil de redirección sería que la carpeta "Mis documentos" apuntara a un directorio personal de cada usuario en la red, como por ejemplo el recurso \\servidor\home\%username%. Esta aproximación resulta más útil que conectarle a dicho usuario ese recurso a una unidad de red, puesto que muchas aplicaciones abren automáticamente la carpeta "Mis documentos" para buscar los archivos personales de ese usuario. Para que dicha redirección funcione correctamente, es necesario que el usuario que recibe la redirección sea el propietario de la carpeta compartida.

4.5.6. Otras políticas

Existen muchas otras políticas que quedan fuera del contexto del presente capítulo. Entre ellas, podemos destacar el **Mantenimiento de Internet Explorer**, que controla la apariencia y la configuración personal de este navegador de web para cada usuario, y los **Servicios de Instalación Remota**, que permiten configurar automáticamente las opciones de instalación de clientes Windows (Windows 2000 Professional, Windows XP).

4.6. Recomendaciones de uso

Todo administrador debería tener en cuenta una serie de reglas básicas que permiten simplificar el diseño y la administración de las Políticas de Grupo. A continuación se exponen las más relevantes:

- **Administración de GPOs.** Un adecuado diseño de la administración y delega-

ción de GPOs es crucial en empresas medianas y grandes, en las que generalmente los dominios se encuentran muy jerarquizados en unidades organizativas. Este diseño debe realizarse en función de la organización y el reparto de labores administrativas que exista en la empresa.

- **Separar usuarios y equipos en unidades organizativas diferentes.** Esta decisión de diseño simplifica la aplicación de GPOs, ya que al diseñarlas sólo hay que tener en cuenta la configuración de usuarios o de equipos. Por otra parte, este diseño facilita que las labores de administrar equipos y administrar usuarios puedan repartirse entre grupos de administradores distintos. Finalmente, también es beneficioso respecto al tiempo dedicado a procesar las políticas de grupo, puesto que pueden deshabilitarse las políticas (de equipo o de usuario) que no se hayan configurado.
- **Organización homogénea de unidades organizativas.** La organización de las unidades organizativas (primero geográfica y luego funcional, o al revés) debe partir de la organización de la empresa y debe ser consistente con ella. Si se sobrediseña esta estructura, resultará más difícil aplicar correctamente las políticas de grupo a equipos y usuarios.
- **Minimizar los GPOs asociados a usuarios o equipos.** El tiempo de inicio de un equipo y el tiempo de inicio de sesión de un usuario se incrementan conforme más GPOs se aplican a dicho equipo o usuario. Resulta por tanto más interesante intentar conseguir las configuraciones adecuadas con el menor número posible de GPOs.
- **Minimizar el uso de "No reemplazar" y de "Bloquear la herencia".** Estas dos propiedades de un GPO resultan interesantes en ciertos escenarios, aunque su abuso puede complicar mucho la comprensión por parte del administrador de qué políticas están afectando realmente a equipos y usuarios. Lógicamente, esto dificulta la capacidad del administrador de resolver situaciones en las que el efecto de las políticas no es el deseado.
- **Evitar asignaciones de GPOs entre dominios.** Aunque es técnicamente posible vincular a un contenedor de un dominio un GPO creado en *otro* dominio, esta práctica está desaconsejada. El motivo es que los GPOs están almacenados en sus dominios respectivos y al utilizarlos desde otros dominios, el tiempo para su proceso se incrementa.
- **Utilizar el proceso *Loopback* sólo cuando sea necesario.** Aunque esta opción queda fuera de los objetivos de este capítulo, se explicará brevemente a continuación. En algunas ocasiones muy concretas, puede resultar conveniente para ciertos equipos en un dominio que sólo se apliquen las políticas de equipo que les afecten. En otras palabras, conseguir que *nunca* se apliquen las políticas de usu-

4.6. Recomendaciones de uso

rio, independientemente del usuario que inicie una sesión local en dichos equipos. Esto puede conseguirse mediante la denominada Política de Grupo "de bucle inverso" o *Loopback*, que puede configurarse en la política Configuración del Equipo--Plantillas Administrativas--Sistema--Directivas de Grupo--Utilizar modo de proceso de bucle inverso de directivas de grupo.. Puesto que esta opción se aleja bastante del funcionamiento normal de los GPOs, se recomienda limitarlo a las ocasiones en que sea estrictamente necesario.

5

Servicios del sistema

Indice

5.1. Introducción	75
5.2. Servicios	75
5.2.1. Tipo de inicio de un servicio	76
5.2.2. Dependencias entre servicios	77
5.2.3. Recuperación de un servicio	77
5.3. Solucionando problemas	79

5.1. Introducción

Un servicio es un programa que está ejecutándose indefinidamente para atender a peticiones de otros programas o del usuario. Como ocurría con Windows NT, Windows 2003 también utiliza los servicios. Por defecto W2003, ejecuta automáticamente muchos servicios (necesarios o no) que consumen más memoria que la necesaria para las funciones que está desempeñando el sistema. Si nunca vas a utilizar el Servicio de Fax o el Programador de Tareas, por qué tienen que estar ejecutándose y consumiendo memoria.

5.2. Servicios

Para poder acceder a todos los servicios disponibles en un sistema Windows 2003, se debe de iniciar sesión como administrador. Para ejecutar la utilidad Servicios, hay que seleccionar *Inicio->Programas->Herramientas Administrativas->Servicios*.

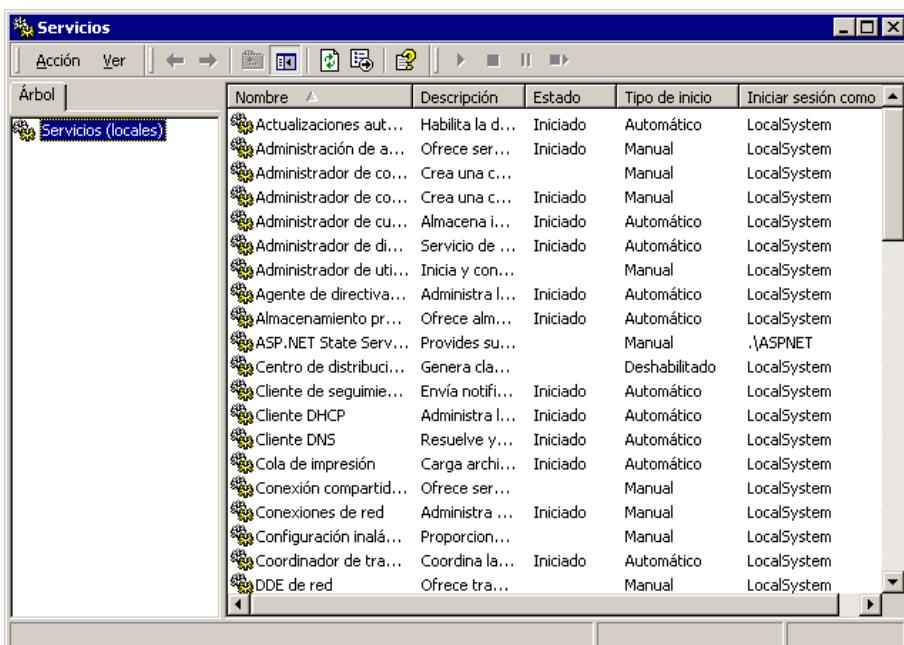


Figura 5.1. Utilidad Servicios de Windows 2003

Esta utilidad muestra todos los servicios disponibles en el sistema. Sobre todo hay que fijarse en la columna **Tipo de Inicio**, ya que este atributo define cuando se arrancará el servicio. Existen tres opciones a la hora de arrancar un servicio, que serán vistas más adelante en este capítulo.

5.2.1. Tipo de inicio de un servicio

5.2.1. Tipo de inicio de un servicio

Existen tres opciones a la hora de elegir el tipo de inicio de un servicio que esté disponible en el sistema:

1. **Automático:** el servicio se inicia automáticamente mientras se carga el sistema operativo (Windows 2003). Esta opción puede incrementar el tiempo de inicio del sistema, así como el consumo de recursos, mientras que el servicio igual no es necesario.
2. **Manual:** el servicio no se inicia de forma predeterminada tras la carga del sistema operativo, en cambio pude ser iniciado - manualmente - en cualquier instante.
3. **Deshabilitado:** esta opción en el tipo de inicio de un servicio, obliga al administrador a tener que habilitarlo antes de poder ejecutarlo.

Para poder cambiar el tipo de inicio de un servicio hay que editar las *Propiedades* de servicio respectivo. Para hacer esto, basta con apretar el botón derecho de nuestro ratón sobre el servicio en cuestión y seleccionar Propiedades.

Una vista de la ficha propiedades se muestra a continuación:

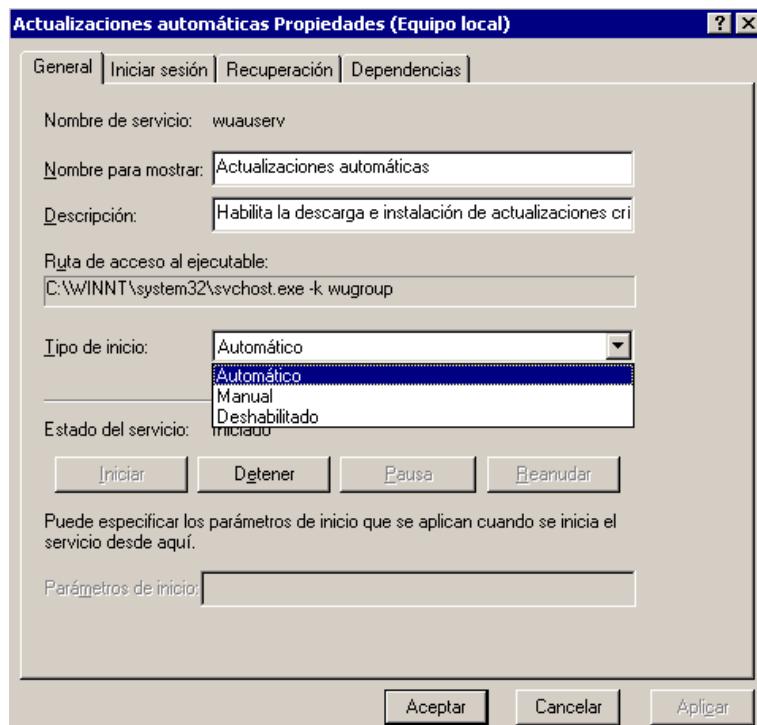


Figura 5.2. Ficha Propiedades de un servicio

5.2.2. Dependencias entre servicios

En el menú desplegable Tipo de Inicio, se elige como se ha de iniciar el servicio en el arranque: *Automático*, *Manual* o *Deshabilitado*. Una vez elegido el tipo de inicio, seleccionamos *Aplicar* para que los cambios surtan efecto. A veces es preferible dejar un servicio con un tipo de inicio *Manual* que deshabilitarlo.

5.2.2. Dependencias entre servicios

Las relaciones de dependencia entre los servicios implican que a la hora de parar servicios, todos aquellos que dependan de él se verán afectados también y así sucesivamente, corriendo el peligro de dejar el sistema en un estado no utilizable.

Para saber que servicios dependen de que otros, en la ficha de *Propiedades* del servicio, elige la lengüeta *Dependencias*.

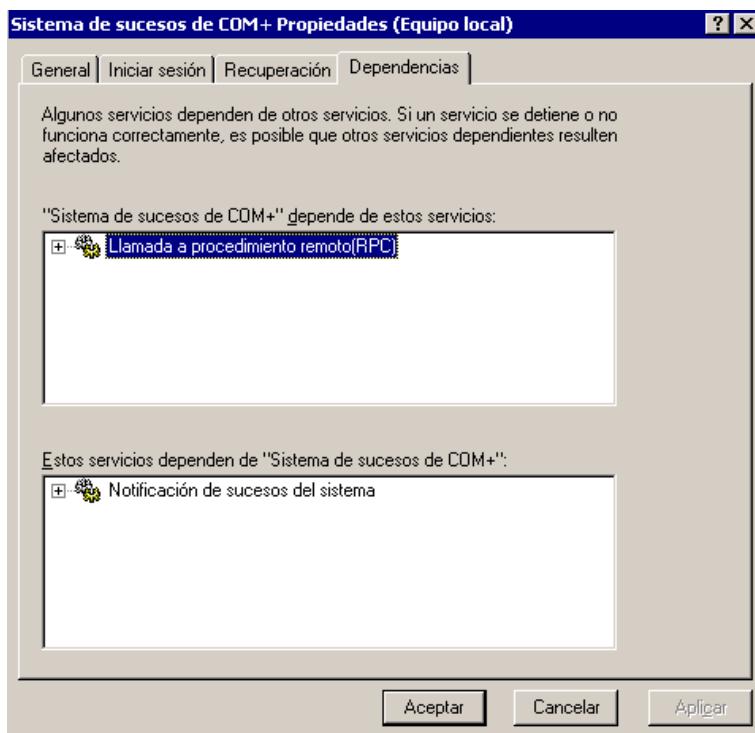


Figura 5.3. Interdependencias de servicios

Esta vista muestra en el panel superior los servicios de los que depende el servicio seleccionado, y en el panel inferior se muestran los servicios dependientes de él.

5.2.3. Recuperación de un servicio

También se pueden personalizar las opciones de **Recuperación** de un servicio ante

5.2.3. Recuperación de un servicio

un fallo o parada del servicio. En otras palabras, que hacer cuando falla un servicio.

De nuevo en la ficha *Propiedades* eligiendo la lengüeta *Recuperación* podemos definir dicho comportamiento.

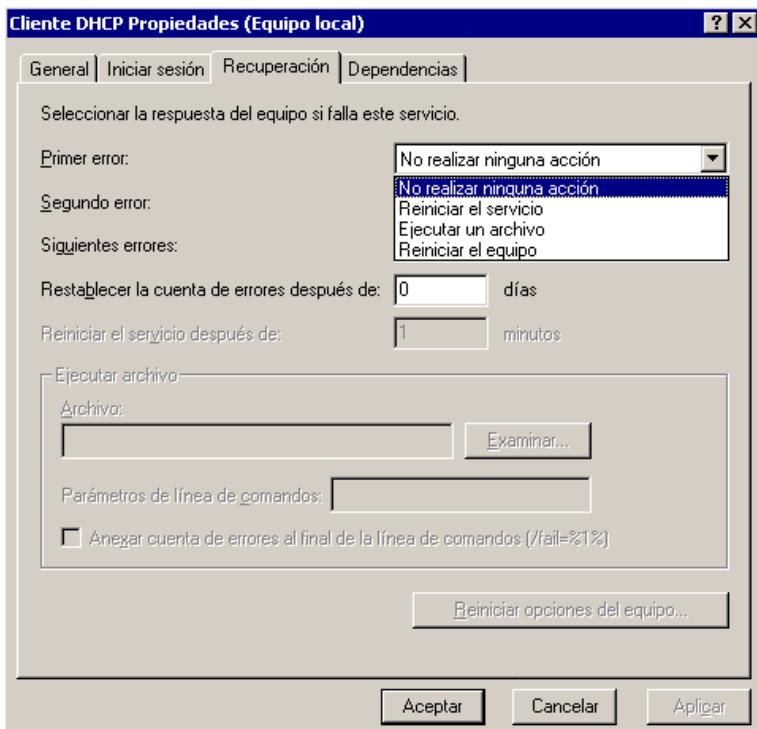


Figura 5.4. Acciones de recuperación de un servicio

Las acciones posibles a tomar son:

- **No realizar ninguna acción**
- **Reiniciar el servicio:** el sistema intentará reiniciar el servicio si este falló. Se puede definir el periodo de tiempo en minutos en que lo volverá a intentar
- **Ejecutar un archivo:** tenemos la posibilidad de ejecutar un archivo de comandos para tomar de una forma más granular las acciones adecuadas.
- **Reiniciar el equipo:** si es un servicio importante y no hay forma de levantarla, ya se sabe, botonazo ;-)

5.3. Solucionando problemas

Puede suceder que al haber deshabilitado un servicio que era necesario para la carga del sistema operativo Windows 2003 o para el buen funcionamiento del sistema, nos encontramos con la desagradable situación de que la utilidad de Servicios no nos permite devolver el estado a un servicio concreto. Una opción para arreglar esto es editar la subclave del registro `HKLM\SYSTEM\CurrentControlSet\Services`

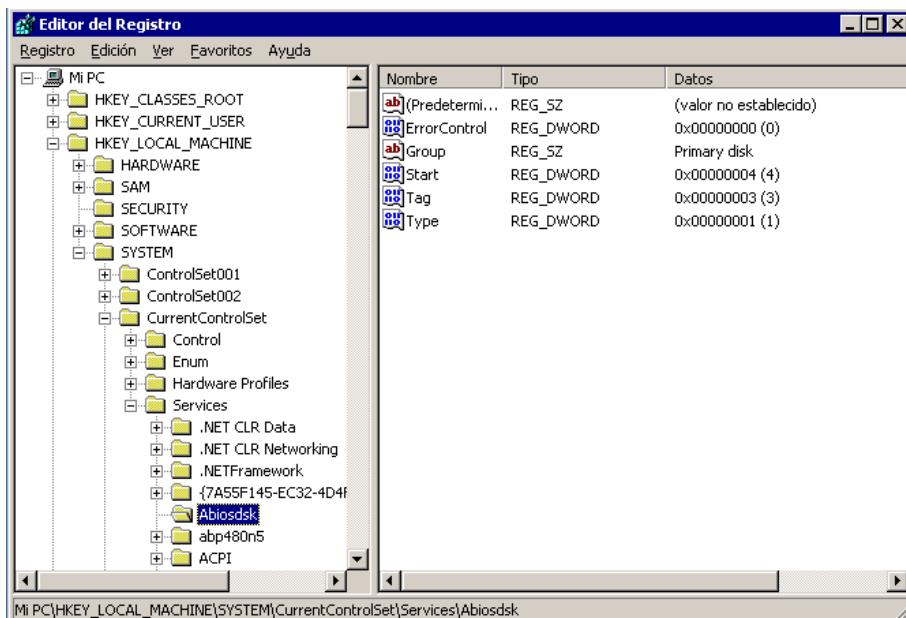


Figura 5.5. `HKLM\SYSTEM\CurrentControlSet\Services`

Es aquí donde se almacena el valor de tipo de inicio para cada servicio. Lo que hay que hacer es seleccionar el servicio apropiado y en el panel de la derecha cambiar el valor de la clave `Start` de tipo. Un valor DWORD hexadecimal o decimal determina el tipo de inicio del servicio. Los valores posibles de esta clave son:

1. Un valor **2** significa un tipo de inicio *Automático*
2. Un valor **3** significa un tipo de inicio *Manual*.
3. Un valor **4** significa que el servicio está *deshabilitado*.

6

El servicio DHCP en Windows 2003

Índice

6.1. El protocolo DCHP	83
6.2. Concesión y renovación	84
6.3. Concepto de ámbito	86
6.3.1. Administración de ámbitos	86
6.3.2. Intervalos de exclusión	87
6.3.3. Reservas	88
6.3.4. Eliminación de concesiones	89
6.4. Administración de opciones DHCP	89
6.5. Autorización de un servidor DHCP	90
6.6. DHCP y DNS	91

6.1. El protocolo DHCP

DHCP (*Dynamic Host Configuration Protocol*) o Protocolo Dinámico de Configuración de Equipos no es un protocolo específico de Windows 2003, sino que se trata de un estándar para cualquier tipo de sistema conectado a una red TCP/IP.

La función básica de este protocolo es evitar que el administrador tenga que configurar manualmente las características propias del protocolo TCP/IP en cada equipo. Para ello, existe en la red un sistema especial, denominado *servidor DHCP*, que es capaz de asignar la configuración TCP/IP al resto de máquinas presentes en la red, o *clientes DHCP*, cuando estos arrancan.

Entre los datos que más habitualmente proporciona el servidor a los clientes se incluyen:

- Una dirección IP por cada tarjeta de red o NIC (*Network Interface Card*) que posea el cliente.
- La máscara de subred.
- La puerta de enlace o *gateway*.
- Otros parámetros adicionales, como el sufijo del dominio DNS, o la dirección IP del servidor DNS.

En una red pueden convivir equipos que sean clientes DHCP con otros cuya configuración se haya establecido manualmente. Aquellos que estén configurados como clientes DHCP necesitarán encontrar en la red local un servidor DHCP para que les proporcione los parámetros TCP/IP.

Cuando un cliente arranca por primera vez, lanza por la red un mensaje de difusión (*broadcast*, solicitando una dirección IP. Si en la red existe un solo servidor DHCP, cuando este reciba el mensaje contestará al cliente asociándole una dirección IP junto con el resto de parámetros de configuración. En concreto, el servidor DHCP puede estar configurado para asignar al cliente una dirección IP cualquiera de las que tenga disponibles, o bien para asignarle una dirección en concreto (o dirección reservada), en función de la dirección física de la tarjeta ethernet del cliente. En ambos casos, una vez el cliente recibe el mensaje del servidor, ya tiene una configuración IP con la que poder acceder a la red de forma normal.

Si en la red hay más de un servidor DHCP, es posible que dos o más servidores escuchen la petición y la contesten. Entonces, el primer mensaje que recibe el cliente es aceptado y el resto son rechazados. Es muy importante resaltar que cuando hay

6.2. Concesión y renovación

varios servidores DHCP en una misma red local, estos no se comunican entre ellos para saber qué direcciones IP debe asignar cada uno. Es responsabilidad de los administradores que sus configuraciones sean independientes y consistentes.

En otras palabras, cuando en una misma red TCP/IP existe más de un servidor DHCP, es imprescindible que estén configurados de manera que no puedan asignar la misma dirección IP a dos ordenadores distintos. Para ello basta que los rangos de direcciones IP que puedan proporcionar no tengan direcciones comunes, o, si las tienen, que estas sean direcciones reservadas.

En cualquiera de los casos anteriores, desde el punto de vista del cliente los parámetros que ha recibido se consideran una *concesión*, es decir, son válidos durante un cierto tiempo. Cada vez que el cliente arranca, o bien cuando se alcanza el límite de la concesión (*lease time*) el cliente tiene que solicitar su renovación.

El protocolo DHCP es especialmente útil cuando el parque de equipos de una organización se distribuye en varias subredes físicas, y además los equipos cambian de ubicación (de subred) con cierta frecuencia. En este caso, cambiar el equipo de sitio no supone nunca reconfigurar manualmente sus parámetros de red, sino simplemente conectarlo a la nueva red e iniciararlo.

6.2. Concesión y renovación

Un cliente DHCP obtiene una concesión para una dirección IP de un servidor DHCP. Antes que se acabe el tiempo de la concesión, el servidor DHCP debe renovar la concesión al cliente o bien este deberá obtener una nueva concesión. Las concesiones se guardan en la base de datos del servidor DHCP aproximadamente un día después de que se agote su tiempo. Este periodo de gracia protege la concesión del cliente en caso de que este y el servidor se encuentren en diferentes zonas horarias, de que sus relojes internos no estén sincronizados o en caso de que el cliente esté fuera de la red cuando caduca el tiempo de la concesión.

La primera vez que se inicia un cliente DHCP e intenta unirse a una red, se realiza automáticamente un proceso de inicialización para obtener una concesión de un servidor DHCP:

1. El cliente DHCP solicita una dirección IP difundiendo un mensaje DHCP *Discover*.
2. El servidor responde con un mensaje DHCP *Offer* proporcionando una dirección al cliente.
3. El cliente acepta la oferta respondiendo con un mensaje DHCP *Request*.

6.3. Concepto de ámbito

4. El servidor envía un mensaje DHCP Ack indicando que aprueba la concesión.
5. Cuando el cliente recibe la confirmación entonces configura sus propiedades TCP/IP usando la información de la respuesta DHCP.

Si ningún servidor DHCP responde a la solicitud del cliente (DHCP Discover), entonces el cliente autoconfigura una dirección IP para su interfaz. En raras ocasiones un servidor DHCP puede devolver una confirmación negativa al cliente. Esto suele ocurrir si el cliente solicita una dirección no válida o duplicada. Si un cliente recibe una confirmación negativa (DHCP Nack), entonces deberá comenzar el proceso de concesión.

Cuando se inicia un cliente que ya tenía concedida una dirección IP previamente, este debe comprobar si dicha dirección sigue siendo válida. Para ello, difunde un mensaje DHCP Request en vez de un mensaje DHCP Discover. El mensaje DHCP Request contiene una petición para la dirección IP que se le asignó previamente. Si el cliente puede usar la dirección IP solicitada, el servidor responde con un mensaje DHCP Ack. Si el cliente no pudiera utilizarla porque ya no es válida, porque la esté usando otro cliente o porque el cliente se ha desplazado físicamente a otra subred, entonces el servidor responde con un mensaje DHCP Nack, obligando al cliente a reiniciar el proceso de concesión. Si el cliente no consigue localizar un servidor DHCP durante el proceso de renovación, entonces éste intenta hacer un ping al gateway predeterminado que se lista en la concesión actual, procediendo de la siguiente forma:

- Si tiene éxito, el cliente DHCP supone que todavía se encuentra en la red en la que obtuvo la concesión actual y la seguirá usando. En segundo plano, el cliente intentará renovar la concesión actual cuando se agote el 50% del tiempo de la concesión asignada.
- Si falló el ping, el cliente supone que se desplazó a otra red y autoconfigura su dirección IP, intentando cada 5 minutos localizar un servidor DHCP y obtener una concesión.

La información de TCP/IP que se concede al cliente, deberá ser renovada por éste de forma predeterminada cuando se haya agotado el 50% del tiempo de concesión. Para renovar su concesión, un cliente DHCP envía un mensaje DHCP Request al servidor del cual se obtuvo la concesión. El servidor renueva automáticamente la concesión respondiendo con un mensaje DHCP Ack. Este mensaje contiene la nueva concesión, así como cualquier parámetro de opción DHCP. Esto asegura que el cliente DHCP puede actualizar su configuración TCP/IP si el administrador de la red actualiza cualquier configuración en el servidor DHCP.

6.3. Concepto de ámbito

En el contexto de DHCP, un *ámbito* (*scope*) se define como una agrupación administrativa de direcciones IP que posee una serie de parámetros de configuración comunes y que se utiliza para asignar direcciones IP a clientes DHCP situados en una misma red física.

Es decir, para que un servidor DHCP pueda asignar direcciones IP a sus potenciales clientes, es necesario que defina al menos un ámbito en cada red física en la que haya clientes que atender. El administrador debe establecer para dicho ámbito sus parámetros de configuración, tales como el rango de direcciones IP que puede asignar, las direcciones excluidas, la máscara de red, el límite de tiempo que los equipos pueden disfrutar de la concesión, etc.

En cualquier caso, para que un servidor DHCP pueda atender varias redes físicas distintas interconectadas, es necesario que esté conectado a dichas redes, o bien que los encaminadores utilizados tengan la capacidad de encaminar los mensajes del protocolo DHCP entre dichas redes. De no ser así, es necesario utilizar un servidor DHCP distinto en cada red, o bien instalar el servicio de reenvío de DHCP en algún host el cual está configurado para escuchar los mensajes de difusión utilizados por el protocolo DHCP y redirigirlos a un servidor DHCP específico. De esta manera se evita la necesidad de tener que instalar dos servidores DHCP en cada segmento de red.

En cada ámbito sólo se admite un rango consecutivo de direcciones IP. Si todas las direcciones de dicho rango no deben de ser asignadas, es posible definir subrangos (o direcciones individuales) que deban ser excluidos.

6.3.1. Administración de ámbitos

Es necesario definir y activar al menos un ámbito en el servidor para que los clientes DHCP puedan recibir la configuración dinámica de TCP/IP. Como hemos definido, un ámbito es una colección administrativa de direcciones IP y de parámetros de configuración TCP/IP que se encuentran disponibles para la concesión a los clientes DHCP.

Un ámbito tiene las siguientes propiedades:

- Un nombre de ámbito.
- Rango de direcciones IP a ofertar.
- Máscara de subred (única para todo el ámbito).
- Valores de duración de concesión.

6.3.2. Intervalos de exclusión

- Opcionalmente, otros datos de TCP/IP comunes para el ámbito, tales como sufijo DNS, servidor(es) DNS, etc. Estos se denominan genéricamente "opciones DHCP".

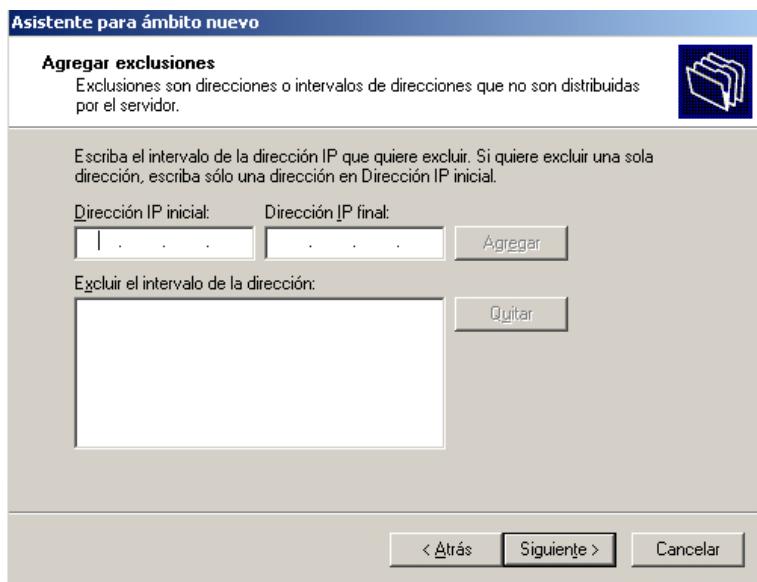
Cada subred puede tener un único ámbito DHCP con un solo intervalo continuo de direcciones IP. Si se desea ofrecer varios grupos de direcciones en el mismo ámbito (o en una sola subred), es necesario definir primero el ámbito y luego establecer intervalo(s) de exclusión.



6.3.2. Intervalos de exclusión

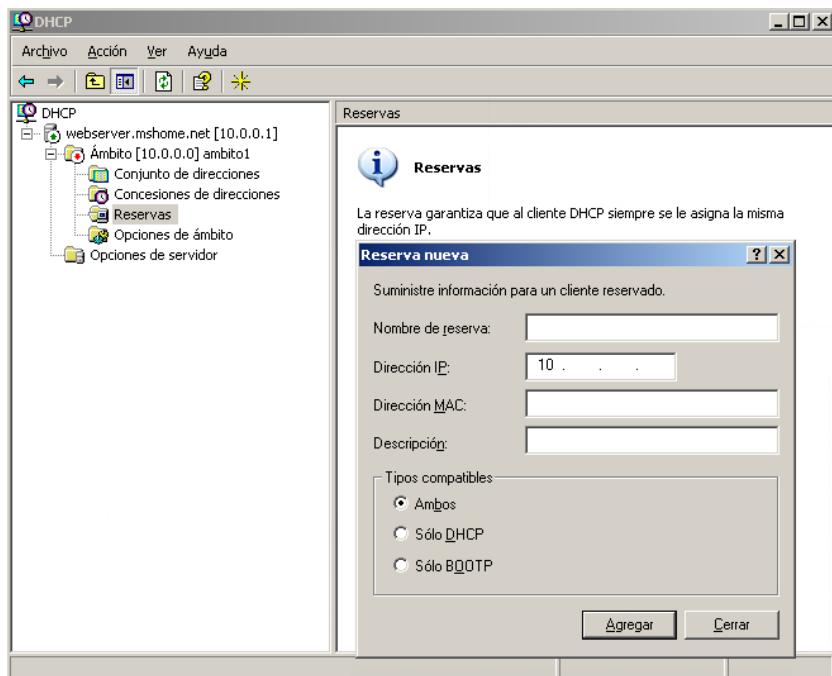
Cuando se crea un nuevo ámbito, deberían excluirse del intervalo las direcciones de equipos configurados estáticamente, de forma que esas direcciones no puedan ofrecerse a los clientes. Como Windows 2003 Server necesita que el equipo que ejecuta el servicio DHCP tenga configurada estáticamente su dirección IP, hay que asegurarse que la dirección IP del equipo servidor esté excluida de las posibles ofertadas (y, lógicamente, que éste no sea cliente DHCP).

6.3.3. Reservas



6.3.3. Reservas

Un administrador de red puede reservar direcciones IP para la asignación de concesiones permanentes a equipos y dispositivos específicos de la red. Las reservas se encargan de asegurar que un dispositivo hardware específico siempre pueda usar la misma dirección IP. Se recomienda hacer reservas para clientes DHCP que funcionen como servidores de impresión, servidores web o encaminadores (*routers*).



6.3.4. Eliminación de concesiones

Hay ocasiones en las que es necesario modificar un ámbito para eliminar la concesión de un cliente DHCP, normalmente porque ésta entra en conflicto con un intervalo de exclusión de una dirección IP o una dirección reservada.

La acción de eliminar una concesión tiene el mismo efecto que si se agotara el tiempo de concesión del cliente, es decir, la próxima vez que se inicie el sistema del cliente éste deberá repetir el proceso de solicitud de concesión. Sin embargo, no existe ninguna forma de evitar que el cliente obtenga una nueva concesión para la misma dirección IP. Para evitar esto se debe conseguir que la dirección deje de estar disponible antes de que el cliente pueda solicitar otra concesión, quitándola del ámbito mediante una reserva o una exclusión.

6.4. Administración de opciones DHCP

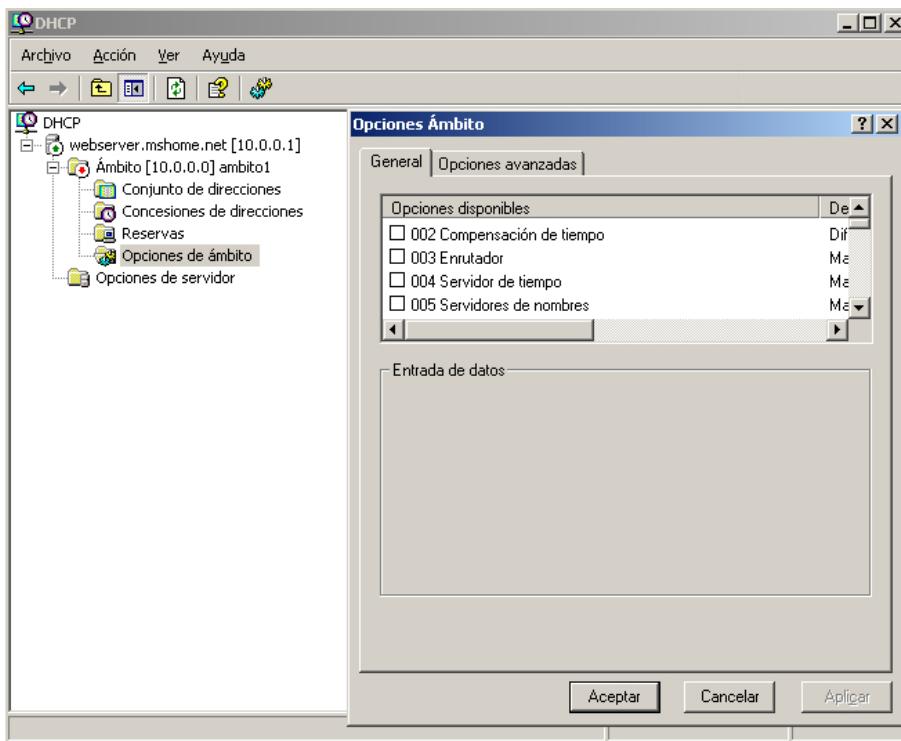
Las opciones DHCP que el servidor proporciona a los clientes junto con el resto de propiedades TCP/IP (dirección, máscara, etc.) pueden configurarse en el servidor a diferentes niveles. En concreto, existen cuatro niveles donde dichas opciones se pueden configurar:

- a. **Opciones globales predeterminadas:** las opciones configuradas a este nivel se aplican globalmente a todos los ámbitos, clases y clientes. Las opciones globales activas se aplican siempre, a menos que sean ignoradas o modificadas por un ámbito, clase o cliente en concreto.
- b. **Opciones de ámbito:** las opciones configuradas para un ámbito se aplican a cualquier cliente que obtenga una concesión en dicho ámbito, siempre y cuando no sean ignoradas o modificadas por opciones de clase o específicas de cliente.
- c. **Opciones de clase:** se aplican a cualquier cliente que especifique el valor concreto de identificador de clase DHCP cuando obtiene una concesión de ámbito. Los tipos de opción de clase activa se aplican siempre a todos los equipos que se configuran como miembros en una opción de clase DHCP especificada, a menos que las ignore o modifique la configuración específica de cliente reservada.
- d. **Opciones de cliente reservado:** se aplican a cualquier equipo que tenga una reserva en el ámbito para su dirección IP. Cuando los tipos de opción de cliente reservado sean activos, las configuraciones para estos tipos de opciones ignorarán el resto de los posibles valores predeterminados.

De la explicación anterior se deduce que, en caso de que se produzca un conflicto entre los valores especificados para una opción DHCP en distintos niveles, el valor

6.5. Autorización de un servidor DHCP

del nivel más específico siempre tiene preferencia sobre el menos específico.

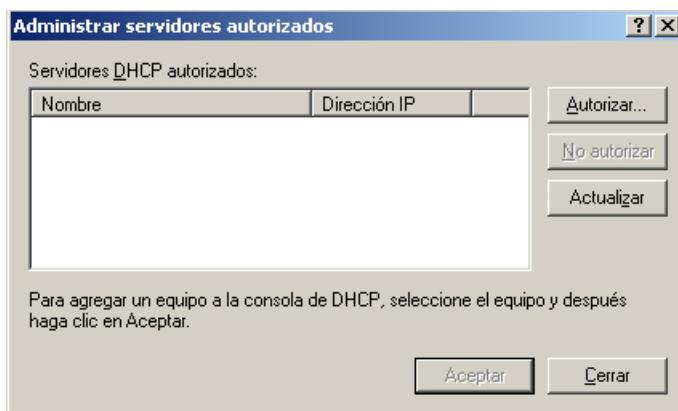


6.5. Autorización de un servidor DHCP

En las implementaciones anteriores de DHCP (de Microsoft), cualquier usuario podía crear un servidor DHCP en la red, lo que podía ocasionar conflictos en las asignaciones de direcciones IP. En Windows 2003, Active Directory debe autorizar a un servidor DHCP para que dicho servidor pueda emitir concesiones para los clientes DHCP. Como resultado, los administradores de redes tienen mayor control sobre las asignaciones de concesiones IP en una red de Windows 2003.

Cuando un servidor DHCP se inicia, entra en contacto con Active Directory para determinar si se encuentra en la lista de los servidores que están actualmente autorizados para operar en la red. Si el servidor DHCP está autorizado, se iniciará correctamente el servicio, si no lo está, el servidor DHCP anotará un error en el registro del sistema y no responderá a los clientes.

La autorización de un servidor DHCP se realiza en la acción "Autorización de Servidores" de la consola de administración DHCP. Sólo los miembros del grupo "Administración de Empresas" (perteneciente al dominio raíz del bosque) tienen permisos suficientes para realizar esta acción.



6.6. DHCP y DNS

De manera predeterminada, la implementación de DHCP de Windows 2003 está configurada para permitir la actualización dinámica de los servidores de nombres DNS que sean compatibles con el protocolo de actualización dinámica. Por tanto, DHCP actualiza automáticamente los registros PTR con las direcciones IP asignadas a los equipos cliente. Esta característica reduce considerablemente el trabajo administrativo necesario para mantener los servidores DNS.

La configuración de DHCP para permitir la actualización dinámica de los servidores DNS se realiza en la ficha DNS del cuadro de diálogo Propiedades del servidor DHCP. Están disponibles las siguientes opciones:

- Actualizar automáticamente la información del cliente DHCP en DNS.
- Descartar las búsquedas directas al caducar la concesión.
- Habilitar actualizaciones para clientes DNS que no sean compatibles con actualizaciones dinámicas.

Sin embargo, cuando se utiliza un servidor DHCP de Microsoft Windows NT 4.0 con clientes Windows 2003, es el cliente DHCP de Windows 2003 quien tiene que actualizar los registros A y PTR en el servidor DNS. Exactamente igual ocurre cuando un cliente configurado de forma estática actualiza dinámicamente los registros A y PTR cada vez que se inicia, o cuando se modifica su dirección IP o su nombre de dominio.

7

Seguridad IP y VPN's

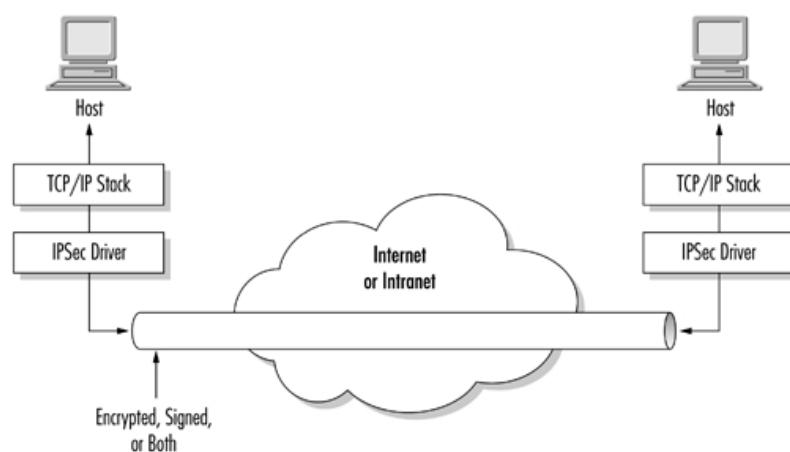
Indice

7.1. IPSEC	95
7.1.1. Ataques a la seguridad	96
7.1.2. Características de seguridad de IPSec	97
7.1.3. Componentes de IPSec	98
7.1.4. Configuración de directivas de IPSec	99
7.1.5. Componentes de las reglas de seguridad	101
7.2. Fundamentos de las VPN's	103
7.2.1. Autenticación	103
7.2.2. Tunneling	104
7.2.3. Cifrado	104
7.3. Configuración de un servidor VPN	105

7.1. IPSEC

Las redes se diseñan normalmente para impedir el acceso no autorizado a datos confidenciales desde fuera de la intranet de la empresa mediante el cifrado de la información que viaja a través de líneas de comunicación públicas. Sin embargo, la mayor parte de las redes manejan las comunicaciones entre los hosts de la red interna como texto sin formato. Con acceso físico a la red y un analizador de protocolos, un usuario no autorizado puede obtener fácilmente datos privados.

IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.



IPSec aumenta la seguridad de los datos de la red mediante:

- La autenticación mutua de los equipos antes del intercambio de datos. IPSec puede utilizar Kerberos V5 para la autenticación de los usuarios.
- El establecimiento de una asociación de seguridad entre los dos equipos. IPSec se puede implementar para proteger las comunicaciones entre usuarios remotos y redes, entre redes e, incluso, entre equipos cliente dentro de una red de área local (LAN).
- El cifrado de los datos intercambiados mediante **Cifrado de datos estándar**

7.1.1. Ataques a la seguridad

(DES, Data Encryption Standard), triple DES (3DES) o DES de 40 bits. IPSec usa formatos de paquete IP estándar en la autenticación o el cifrado de los datos. Por tanto, los dispositivos de red intermedios, como los enruteadores, no pueden distinguir los paquetes de IPSec de los paquetes IP normales.

El protocolo también proporciona las ventajas siguientes:

- Compatibilidad con la infraestructura de claves públicas. También acepta el uso de certificados de claves públicas para la autenticación, con el fin de permitir relaciones de confianza y proteger la comunicación con hosts que no pertenezcan a un dominio Windows 2003 en el que se confía.
- Compatibilidad con claves compartidas. Si la autenticación mediante Kerberos V5 o certificados de claves públicas no es posible, se puede configurar una clave compartida (una contraseña secreta compartida) para proporcionar autenticación y confianza entre equipos.
- Transparencia de IPSec para los usuarios y las aplicaciones. Como IPSec opera al nivel de red, los usuarios y las aplicaciones no interactúan con IPSec.
- Administración centralizada y flexible de directivas mediante Directiva de grupo. Cuando cada equipo inicia una sesión en el dominio, el equipo recibe automáticamente su directiva de seguridad, lo que evita tener que configurar cada equipo individualmente. Sin embargo, si un equipo tiene requisitos exclusivos o es independiente, se puede asignar una directiva de forma local.
- Estándar abierto del sector. IPSec proporciona una alternativa de estándar industrial abierto ante las tecnologías de cifrado IP patentadas. Los administradores de la red aprovechan la interoperabilidad resultante.

7.1.1. Ataques a la seguridad

A continuación se presenta una lista parcial de los ataques a las redes más comunes:

- Rastreo. Un rastreador de red es una aplicación o un dispositivo que puede supervisar y leer los paquetes de la red. Si los paquetes no están cifrados, un rastreador de red obtiene una vista completa de los datos del paquete. El Monitor de red de Microsoft es un ejemplo de rastreador de red.
- Modificación de datos. Un atacante podría modificar un mensaje en tránsito y enviar datos falsos, que podrían impedir al destinatario recibir la información co-

7.1.2. Características de seguridad de IPSec

rrecta o permitir al atacante conseguir la información protegida.

- Contraseñas. El atacante podría usar una contraseña o clave robadas, o intentar averiguar la contraseña si es fácil.
- Suplantación de direcciones. El atacante usa programas especiales para construir paquetes IP que parecen provenir de direcciones válidas de la red de confianza.
- Nivel de aplicación. Este ataque va dirigido a servidores de aplicaciones al explotar las debilidades del sistema operativo y de las aplicaciones del servidor.
- Intermediario. En este tipo de ataque, alguien entre los dos equipos comunicantes está supervisando activamente, capturando y controlando los datos de forma desapercibida (por ejemplo, el atacante puede estar cambiando el encaminamiento de un intercambio de datos).
- Denegación de servicio. El objetivo de este ataque es impedir el uso normal de equipos o recursos de la red. Por ejemplo, cuando las cuentas de correo electrónico se ven desbordadas con mensajes no solicitados.

7.1.2. Características de seguridad de IPSec

Las siguientes características de IPSec afrontan todos estos métodos de ataque:

- Protocolo Carga de seguridad de encapsulación (ESP, Encapsulating Security Payload). ESP proporciona privacidad a los datos mediante el cifrado de los paquetes IP.
- Claves basadas en criptografía. Las claves cifradas, que se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito. Se utiliza material de claves diferente para cada segmento del esquema de protección global y se puede generar nuevo material de claves con la frecuencia especificada en la directiva de IPSec.
- Administración automática de claves. La claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques. IPSec usa el protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar dinámicamente claves cifradas entre los equipos que se comunican.

7.1.3. Componentes de IPSec

- Negociación de seguridad automática. IPSec usa *ISAKMP* para negociar de forma dinámica un conjunto de requisitos de seguridad mutuos entre los equipos que se comunican. No es necesario que los equipos tengan directivas idénticas, sólo una directiva configurada con las opciones de negociación necesarias para establecer un conjunto de requisitos con otro equipo.
- Seguridad a nivel de red. IPSec existe en el nivel de red, proporcionando seguridad automática a todas las aplicaciones.
- Autenticación mutua. IPSec permite el intercambio y la comprobación de identidades sin exponer la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicar con la protección de IPSec. Pueden estar en cualquier dominio de confianza de la empresa. La comunicación se cifra, lo que dificulta la identificación e interpretación de la información.
- Filtrado de paquetes IP. Este proceso de filtrado habilita, permite o bloquea las comunicaciones según sea necesario mediante la especificación de intervalos de direcciones, protocolos o, incluso, puertos de protocolo específicos.

7.1.3. Componentes de IPSec

En el proceso de autenticación y cifrado de IPSec intervienen varios componentes. Su conocimiento y el de los procesos en que consiste la comunicación IPSec le ayudará a encontrar soluciones a los problemas de implementación.

El proceso de negociación y filtrado

Cuando un equipo configurado con una directiva de IPSec intenta comunicar con otro equipo, comienza el proceso siguiente:

1. Las directivas de IPSec se entregan al controlador de IPSec y el intercambio de clave ISAKMP/Oakley a través de directivas locales o configuraciones de Directiva de grupo desde Active Directory.
2. ISAKMP supervisa las negociaciones entre los hosts y proporciona claves que se usan con algoritmos de seguridad.
3. El controlador de IPSec supervisa, filtra y protege el tráfico entre el nivel de transporte y el nivel de red.

Directivas de seguridad de IP

Las directivas son las reglas de seguridad que definen el nivel de seguridad deseado, el algoritmo de hash, el algoritmo de cifrado y la longitud de la clave. Estas reglas también definen las direcciones, protocolos, nombres DNS, subredes o tipos de conexión a los que se aplica la configuración de seguridad. Las directivas de IPSec se pueden configurar de acuerdo con los requisitos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global. Windows 2003 proporciona Administración de directiva de seguridad de IP para crear y administrar directivas de IPSec localmente o a través de Directiva de grupo. Se proporcionan directivas predefinidas (predeterminadas) para configuraciones de seguridad de grupo y locales. Se pueden modificar para cumplir requisitos específicos. Una vez definida una directiva, tiene que asignarse. De forma predeterminada, no hay directivas asignadas.

ISAKMP y directivas de seguridad

Durante la configuración de IPSec, se crea una directiva en la interfaz. Sin embargo, IPSec crea las dos siguientes directivas de negociación de seguridad en segundo plano:

- La primera negociación incluye autenticación de identidad de usuario para los dos hosts que se van a comunicar y el intercambio de las claves de la sesión para proteger los datos. ISAKMP administra esta primera negociación, que se puede llamar directiva de negociación.
- La segunda negociación sigue al intercambio de las claves. Los dos hosts tienen que acordar la configuración de seguridad que van a utilizar para proteger su comunicación sobre IP. A la directiva que define las reglas de esta negociación se le llama directiva de seguridad.

7.1.4. Configuración de directivas de IPSec

Las directivas de IPSec locales se crean y configuran mediante Directiva de seguridad local. Use Directiva de seguridad del dominio para crear y configurar directivas de IPSec para todo el dominio. También puede agregar el complemento Administración de directivas de seguridad de IP a una consola MMC.

Se pueden definir varias directivas, pero sólo una se asigna a un equipo al mismo tiempo. Para asignar una directiva, en Directiva de seguridad local o la consola de Directiva de grupo apropiada, haga clic con el botón secundario del mouse en la directiva de IPSec y, a continuación, haga clic en Asignar. Recuerde que la configura-

7.1.4. Configuración de directivas de IPSec

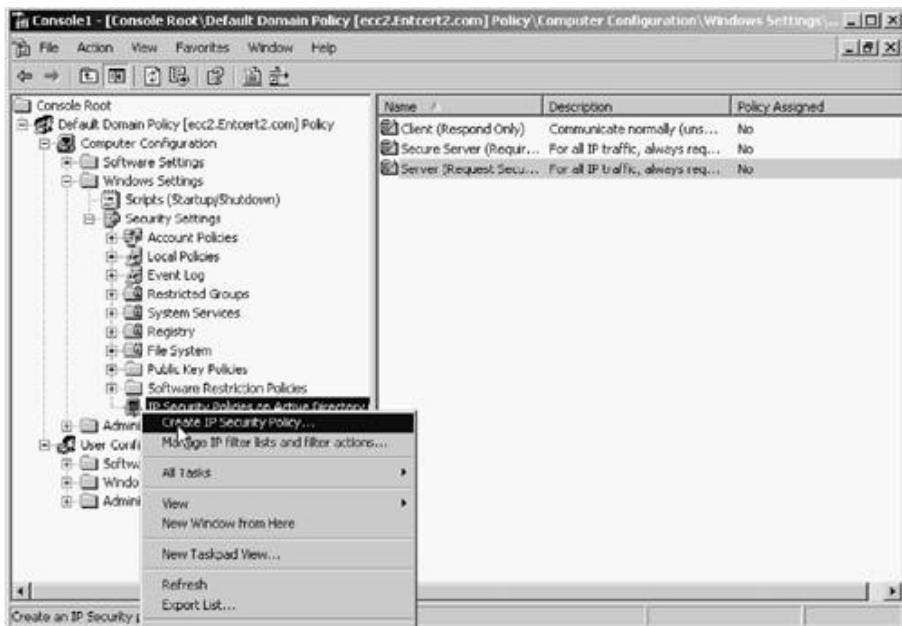
ción del dominio sobrescribe la configuración local.

Directiva de grupo presenta tres entradas de directiva predefinidas:

- La directiva Cliente (sólo responder) permite comunicaciones en texto sin formato, pero responderán a solicitudes de IPSec e intentarán negociar la seguridad. Esta directiva permite la comunicación efectiva en texto sin formato pero intentarán negociar la seguridad si se efectúa una solicitud de seguridad.
- La directiva Servidor (seguridad de petición) permite que los equipos reciban tráfico desde los clientes en texto sin formato y respondan a solicitudes de IPSec. Cada conexión que se inicia intenta negociar la seguridad. Para todas las respuestas que el equipo pueda tener, solicita Seguridad IP con el destino (en general, para todo el tráfico saliente). La directiva Seguridad de petición se reduce de forma predeterminada a texto sin formato si el destino no responde para admitir equipos no habilitados para IPSec. Este comportamiento se puede deshabilitar cuando se hacen pruebas. Esta directiva permite la comunicación efectiva en texto legible pero siempre intenta negociar la seguridad cuando se inicia una conexión.
- La directiva Servidor seguro (requiere seguridad) obliga a la seguridad en todo el tráfico IP entrante y saliente. Requiere que los equipos de destino sean de confianza y que el tráfico se proteja con IPSec. Permite que el equipo responda a solicitudes de IPSec. Esta directiva no permite la comunicación en texto legible.

Para modificar una directiva, haga clic con el botón secundario del mouse en la directiva y, a continuación, haga clic en Propiedades. Para crear una directiva, haga clic con el botón secundario del mouse en el nodo Directivas de seguridad IP, haga clic en Crear directiva de seguridad IP y, a continuación, complete el Asistente para directiva de seguridad de IP.

7.1.5. Componentes de las reglas de seguridad



7.1.5. Componentes de las reglas de seguridad

Las reglas gobiernan cómo y cuándo se invoca una directiva de IPSec. Una regla proporciona la capacidad para iniciar y controlar una comunicación segura en función del origen, el destino y el tipo de tráfico IP. Cada directiva de IPSec puede tener una o varias reglas; una o todas ellas pueden estar activas de forma simultánea. Se proporcionan reglas predeterminadas que se adaptan a una amplia gama de comunicaciones entre cliente y servidor. Para satisfacer los requisitos de una red, puede crear reglas nuevas o modificar las predeterminadas.

Componentes de las reglas

Una regla se compone de 6 elementos:

1. Lista de filtros IP. Define qué tráfico se va a proteger con esta regla. Puede utilizar los filtros predeterminados o crear filtros específicos de directiva para ciertos tipos de tráfico IP o para subredes específicas.
2. Acciones de filtrado. Enumera las acciones de seguridad que se tomarán cuando el tráfico cumple los criterios de un filtro. La acción especifica si el tráfico se bloquea, se permite o si se negocia la seguridad de la conexión. Se pueden especificar una o varias acciones de filtrado negociadas. Las acciones de filtrado aparecen en una lista en la que el primer método tiene preferencia. Si dicha acción de filtrado no se puede negociar, se intenta la acción de filtrado siguiente.

7.1.5. Componentes de las reglas de seguridad

3. **Métodos de seguridad.** Especifica cómo los equipos que se comunican tienen que proteger el intercambio de datos. Puede utilizar los métodos predefinidos Medio y Alto, o definir métodos de seguridad personalizados.
4. **Configuración de túneles.** En algunas situaciones, como entre encaminadores que sólo están conectados por Internet, debe considerar habilitar el modo de túnel en IPSec. El extremo final del túnel es el equipo del túnel más próximo al destino del tráfico IP, como se especifica en la lista del filtro asociado. Para definir un túnel IPSec tiene que haber dos reglas, una para cada sentido.
5. **Métodos de autenticación.** El método de autenticación define cómo cada usuario se va a asegurar de que el otro equipo o el otro usuario son realmente quienes dicen ser. Windows 2003 acepta tres Métodos de autenticación:
 - Kerberos. El protocolo de seguridad Kerberos V5 es la tecnología de autenticación predeterminada. Este método se puede usar en cualquier cliente que ejecute el protocolo Kerberos V5 (sean o no clientes de Windows) que sean miembros de un dominio de confianza.
 - Certificados. Este método requiere que se haya configurado al menos una entidad emisora de certificados (CA, Certificate Authority). Windows 2003 acepta certificados X.509 Versión 3, incluidos los generados por entidades emisoras de certificados comerciales.
 - Clave previamente compartida. Es una clave secreta, compartida, que dos usuarios acuerdan de antemano y que configuran manualmente antes de usarla.

Cada regla puede estar configurada con uno o varios Métodos de autenticación. Cada método de autenticación configurado aparece en una lista según el orden de preferencia. Si el primer método no se puede usar, se intenta el siguiente.

6. **Tipos de conexión.** Permite que el administrador de la red elija si la regla se aplica a todas las conexiones de la red, a la red de área local o a las conexiones de acceso remoto.

Para modificar las propiedades de la regla, haga clic en ella en el cuadro de diálogo Propiedades de una directiva de IPSec y, a continuación, haga clic en Modificar. Para modificar la lista de filtros IP y acciones predeterminadas, haga clic con el botón secundario del mouse en Directivas de seguridad IP y, a continuación, haga clic en Administrar listas de filtros IP y acciones de filtrado.

Regla de respuesta predeterminada

La regla de respuesta predeterminada se usa para asegurar que el equipo responde a solicitudes de comunicación segura. Si una directiva activa no tiene definida una regla para que un equipo solicite una comunicación segura, se aplicará la regla de respuesta predeterminada y se negociará la seguridad. Esta regla se encuentra en todas las directivas definidas, pero puede que no esté activa. Cuando crea una nueva directiva, el asistente presenta la opción de usar la regla de respuesta predeterminada. Si la regla de respuesta predeterminada esté activada, el asistente permite que el administrador establezca el método de autenticación de la regla.

7.2. Fundamentos de las VPN's

Las VPN's son uno de los servicios sobre el que mas se habla por parte de los administradores de entornos Windows Server 2003, pero a su vez uno de los peor entendidos. El servicio de VPN ha sido soportado por Microsoft desde la aparición de Windows NT. En Windows Server 2003, el software que implementa este servicio se denomina RRAS (Enrutamiento y Acceso Remoto). Una VPN habilita a dos ordenadores o redes poder comunicarse de forma privada a través de una red pública o compartida como es Internet. Una VPN proporciona seguridad y fiabilidad a través de una conexión insegura como es una red pública. Una VPN está compuesta básicamente de tres tecnologías que cuando se utilizan juntas, forman una conexión segura. Estas tecnologías son: Autenticación, *Tunneling* y Encriptación.

7.2.1. Autenticación

El principal objetivo de la autenticación en una VPN es poseer un método que asegure que el cliente y el servidor son quien dicen ser antes de que la conexión VPN sea establecida. Antes de crear el tunel se tiene que producir una autenticación con éxito para que los datos se puedan transmitir, pero el tipo de autenticación utilizada dependerá de los clientes y por tanto la seguridad se verá afectada.

Existen diferentes métodos que pueden ser utilizados para establecer la VPN. Por defecto RRAS utilizará la autenticación MS-CHAP y MS-CHAPv2. La lista completa de métodos de autenticación sería:

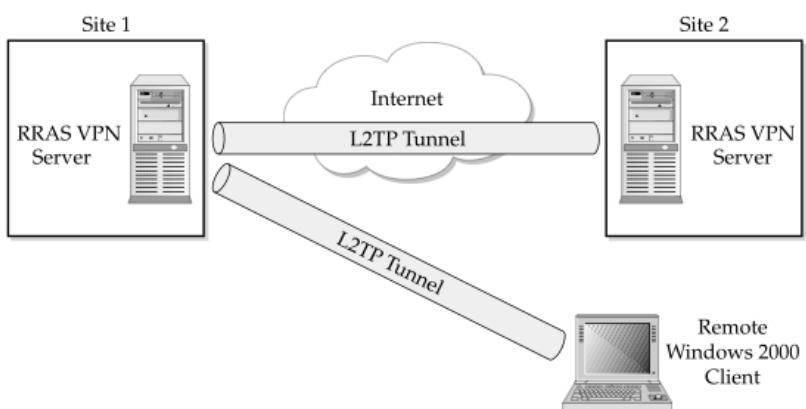
- Extensible Authentication Protocol (EAP).
- Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2)
- Microsoft Challenge Handshake Authentication Protocol (MSCHAP)

7.2.2. Tunneling

- Challenge Handshake Authentication Protocol (CHAP)
- Shiva Password Authentication Protocol (SPAP)
- Password Authentication Protocol (PAP)
- Acceso sin autenticación

7.2.2. Tunneling

El *Tunneling* se utiliza para encapsular diferentes protocolos de red (TCP/IP, Apple-Talk, NetBEUI) dentro de un paquete IP que pueda viajar a través de Internet. Antes de que el tunel sea creado, se debe verificar que los dos extremos son quien dicen ser. Una vez establecido el proceso de autenticación, se crea el tunel y se envia información entre los extremos como se muestra en la figura.



Los dos protocolos utilizados para crear túneles en Windows Server 2003 son PPTP y L2TP. Este último es más avanzado que el protocolo PPTP y además utiliza IPSEC como mecanismo de autenticacion y encriptación. L2TP está solamente disponible en las versiones de RRAS de Windows Server 2003 y Windows 2000 y solamente Windows XP lo soporta.

7.2.3. Cifrado

El último componente importante de una conexión VPN es la encriptación. Se adopta como medida adicional para proteger los datos que se envían a través del tunel. Los datos son cifrados antes de ser enviados por el tunel para reducir el riesgo de que alguien pueda romper el tunel. Windows Server 2003 soporta dos tecnologías de cifrado:

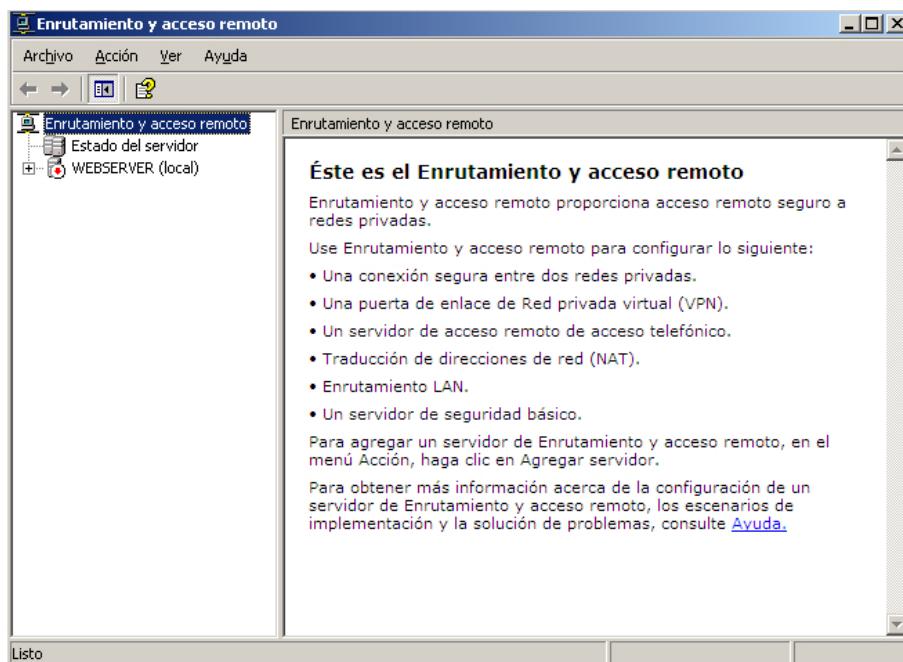
7.3. Configuración de un servidor VPN

- Microsoft Point-to-Point Encryption (MPPE). Este método puede cifrar los datos en conexiones VPN establecidas con el protocolo PPTP. MPPE soporta esquemas de cifrado estandar de 40 y 56 bits y cifrado fuerte de 128 bits (solo disponible en USA y Canada). Para utilizar MPPE se deben emplear los protocolos de autenticación MSCHAP o MSCHAPv2.
- IPSEC. Este conjunto de protocolos, proporciona como sabemos, tanto autenticación como cifrado en las conexiones VPN que utilizan L2TP. Sin embargo, L2TP también utiliza métodos de autenticación como EAP y MSCHAP. IPSEC utiliza esquemas de cifrado como DES o 3DES

7.3. Configuración de un servidor VPN

El servicio de Enrutamiento y Acceso remoto viene instalado por defecto en Windows Server 2003. Para poder utilizarlo hay que habilitarlo, esto quiere decir que aunque esté instalado no está consumiendo recursos de ningún tipo.

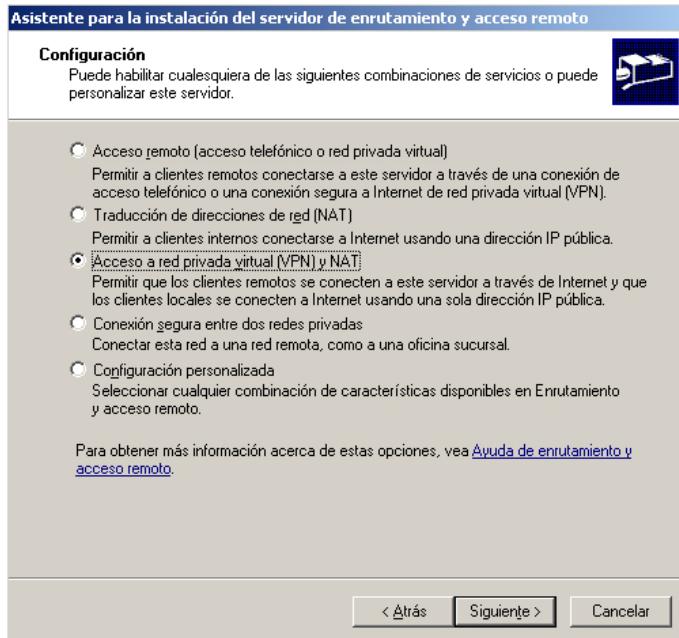
El Asistente para la instalación del servidor de Enrutamiento y acceso remoto permite configurar 4 tipos de servidores de acceso remoto comunes, como es el caso de servidores de redes privadas virtuales, y un quinto servidor personalizado.



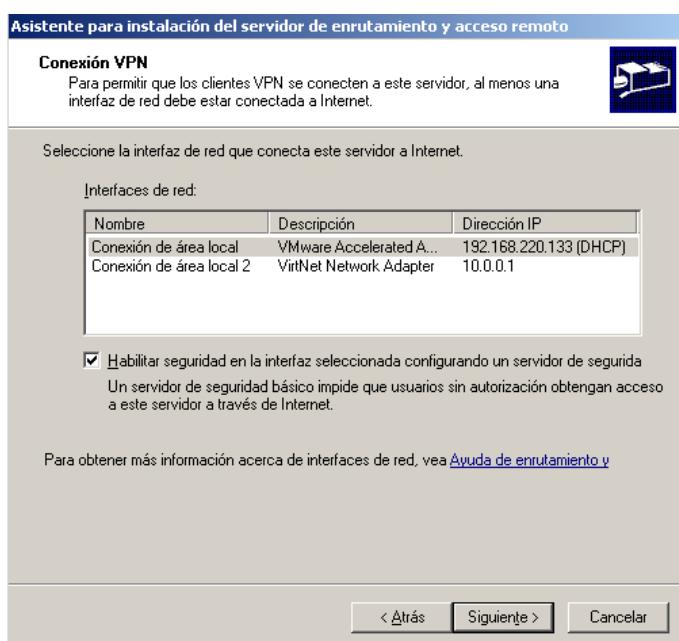
Para configurar e iniciar un servidor de red privada virtual que tambien soporte NAT (Network Address Translation):

7.3. Configuración de un servidor VPN

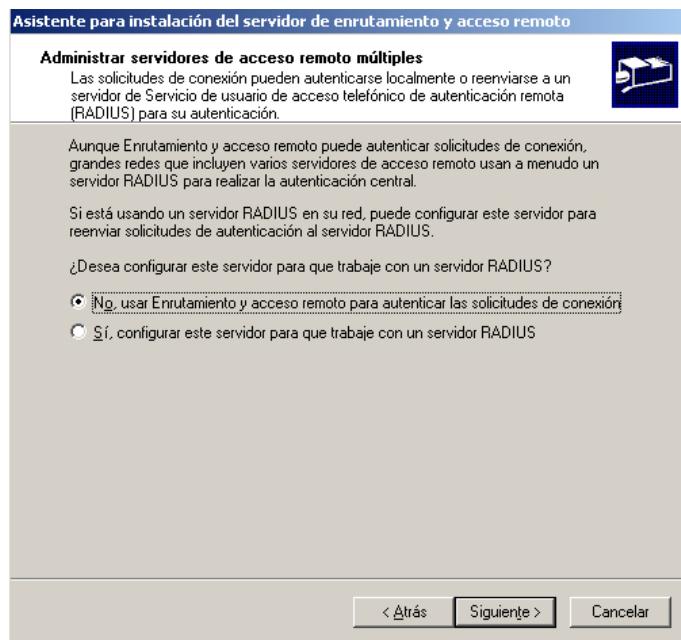
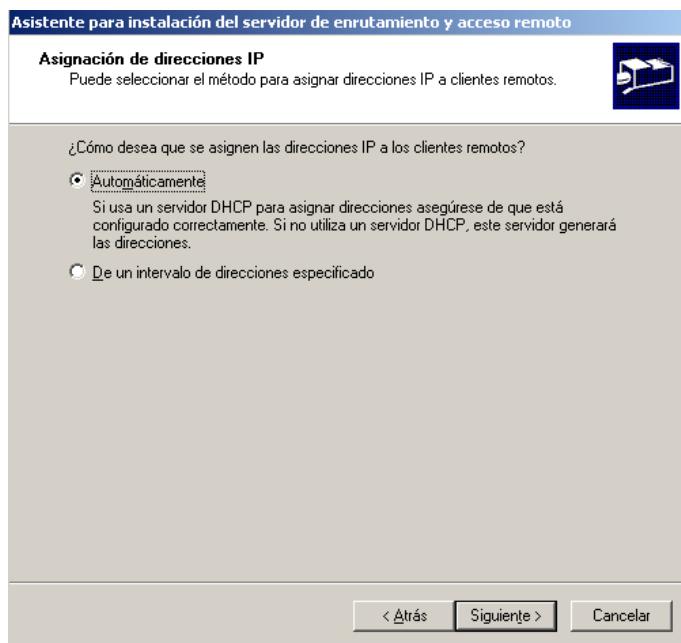
1. En el menú Herramientas administrativas, abra Enrutamiento y acceso remoto, haga clic con el botón secundario del mouse en el nombre del servidor y, después, haga clic en Configurar y habilitar el enrutamiento y el acceso remoto.
2. Complete el Asistente para instalación de enrutamiento y acceso remoto.



3. Configure las directivas de acceso remoto, la autenticación y las opciones de cifrado.

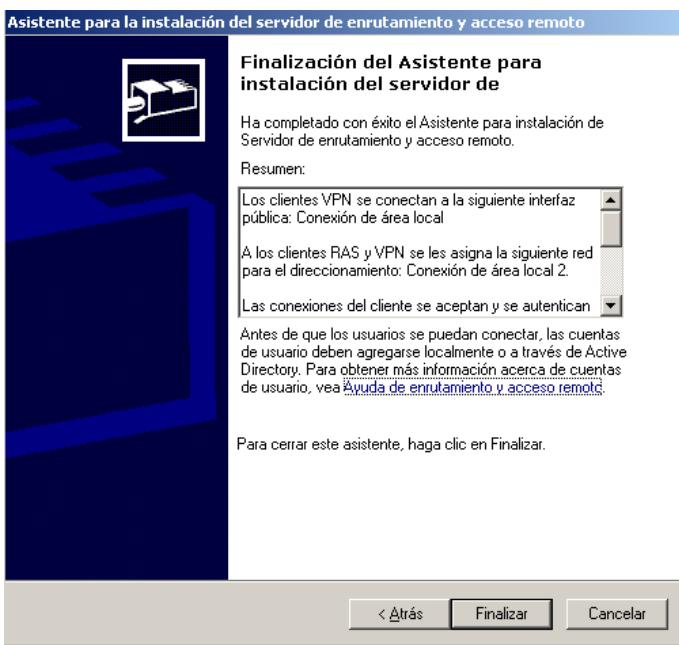


7.3. Configuración de un servidor VPN



Una vez se ha configurado el servicio RRAS, aparecerá una ventana como la siguiente, indicando las opciones que hemos definido en nuestro servidor. En este instante, clientes remotos se podrán conectar y establecer una VPN con nuestro servidor a través de una red pública como Internet.

7.3. Configuración de un servidor VPN



La primera vez que se inicia un servidor VPN, Windows 2003 crea automáticamente 128 puertos PPTP y 128 puertos L2TP. El número de puertos virtuales disponibles para un servidor VPN no está limitado por el hardware físico. Puede aumentarlo o reducirlo al número apropiado para el ancho de banda disponible en el servidor.

Para configurar los puertos VPN, siga los pasos siguientes en el servidor:

1. En Enrutamiento y acceso remoto, abra el cuadro de diálogo Propiedades de Puertos.
2. En el cuadro de diálogo Propiedades de Puertos, seleccione un dispositivo (para los puertos VPN, son Minipuerto WAN (PPTP) y Minipuerto WAN (L2TP) y haga clic en Configurar.
3. En el cuadro de diálogo Configurar dispositivo, active la casilla de verificación Conexiones de acceso remoto (sólo de entrada) para habilitar las conexiones VPN entrantes.
4. Opcionalmente puede aumentar o reducir el número de puertos virtuales disponibles en el servidor.
5. Haga clic en Aceptar en los cuadros de diálogo Configurar dispositivos y Propiedades de Puertos.

8

Internet Information Server

Indice

8.1. Introducción	111
8.1.1. HTTP: Hyper Text Transfer Protocol.	111
8.1.2. URI: Uniform Resource Identifiers.	112
8.1.3. HTML: HyperText Markup Language.	112
8.2. Características de IIS	113
8.3. Instalación de IIS	114
8.4. Administración de sitios Web	114
8.4.1. Creación de un sitio Web	115
8.4.2. Configuración de un sitio Web	119
8.4.3. Directorios Virtuales	120
8.4.4. Seguridad de un sitio Web	122
8.4.5. Copia de seguridad y restauración de la configuración	125
8.5. Programación Web en IIS 6	126
8.5.1. ASP y Python	126

8.1. Introducción

Con el auge de Internet, muchos son los servicios ofertados a los numerosos clientes que tienen acceso a ella. Entre ellos destaca el correo electrónico o mail y los servidores de Web.

El World Wide Web (Web) es una red de recursos de información. El Web cuenta con tres mecanismos para hacer que estos recursos estén disponibles para el mayor número posible de clientes:

1. Un esquema de nominación uniforme para localizar los recursos en la Web (URI's).
2. La pila de protocolos necesarios para acceder a los recursos definidos a través de la Web (HTTP).
3. El hipertexto para una fácil navegación por los recursos (HTML).

8.1.1. HTTP: Hyper Text Transfer Protocol.

El protocolo de transferencia de hipertexto (HTTP) es un protocolo del nivel de aplicación para sistemas de información hipermedia y distribuidos. Además, es un protocolo orientado a objetos y sin estado.

HTTP viene siendo usado en Internet desde 1990. En este momento la versión de protocolo utilizada es la 1.1.

Con estas palabras comienza el documento RFC2616 que define la especificación del protocolo mas usado en Internet. El protocolo HTTP permite comunicar a ordenadores que sirven información (servidores web) en un determinado formato (HTML: HiperText Markup Language) con ordenadores que consultan dicha información (clientes).

Por supuesto que existe un software específico para cada función. El software cliente recibe el nombre de navegador (Explorer, Netscape, Amaya, Lynx ...) y el software servidor se denomina también servidor web.

HTTP es un protocolo de petición - respuesta. Un cliente envía una petición al servidor en la forma definida por el método solicitado, una URI y la versión de protocolo, seguido de un mensaje del estilo MIME contenido modificadores de petición, información del cliente etc.. El servidor responde con una línea de estado que

8.1.2. URI: Uniform Resource Identifiers.

incluye la confirmación de la versión del protocolo y un código de error o de éxito seguido por información del servidor y la información solicitada, terminándose acto seguido la comunicación.

8.1.2. URI: Uniform Resource Identifiers.

La forma de acceder a los recursos que ofrecen los servidores Web, es especificando en el navegador una URI (Identificador Uniforme de Recursos).

Para el protocolo HTTP un URI es un string formateado que identifica por medio de un nombre, o una localización, un recurso en la red. Una URI bajo el punto de vista del protocolo HTTP puede ser representada de forma absoluta o relativa, dependiendo del contexto en donde se la use.

Ambas formas se diferencian en el hecho de que las URI's absolutas empiezan siempre por un nombre de protocolo seguido por dos puntos ':'.

Básicamente las URI's constan de tres partes:

1. El esquema de nominación del mecanismo utilizado para acceder al recurso.
2. El nombre de la máquina que alberga el recurso.
3. El nombre del recurso propiamente dicho, dado como un path.

`http : // host [: puerto] [path absoluto] [? consulta]`

Si el puerto no se especifica, se asume el puerto 80 por defecto.

8.1.3. HTML: HyperText Markup Language.

HTML es una aplicación SGML (Standard Generalized Markup Language) conforme al standard internacional ISO 8879 y es reconocido como el lenguaje de publicación estándar en el World Wide Web.

SGML es un lenguaje para describir lenguajes de marcas, utilizados particularmente en el intercambio de información electrónica, gestión de documentos y publicación de los mismos. HTML es un ejemplo de lenguaje definido en SGML.

HTML fue originariamente concebido como un lenguaje de intercambio de documentos científicos y técnicos por Tim Berners-Lee mientras trabajaba en el CERN y popularizado por el navegador Mosaic desarrollado en NCSA.

HTML proporciona los medios para:

- Publicar online documentos con cabeceras, texto, tablas, listas, fotos etc ...
- Obtener información en línea vía enlaces de hipertexto con un solo clic del ratón.
- Diseñar formularios para realizar transacciones con servicios remotos, que nos permitan búsqueda de información, realizar reservas, comprar productos.
- Incluir hojas de cálculo, video-clips, sonidos y otras aplicaciones directamente en los documentos.

8.2. Características de IIS

Microsoft ha mejorado sustancialmente su software estrella en el campo de los servicios Web. Los avances vienen motivados sobre todo por la seguridad y el rendimiento, aunque todavía adolece de algunos agujeros de seguridad.

Las características agregadas en seguridad se aprovechan de las últimas tecnologías de cifrado y métodos de autenticación mediante certificados de cliente y servidor. Una de las formas que tiene IIS de asegurar los datos es mediante SSL (*Secure Sockets Layer*). Esto proporciona un método para transferir datos entre el cliente y el servidor de forma segura, permitiendo también que el servidor pueda comprobar al cliente antes de que inicie una sesión de usuario.

Otra característica nueva es la autenticación implícita que permite a los administradores autenticar a los usuarios de forma segura a través de servidores de seguridad y proxy.

IIS 6 también es capaz de impedir que aquellos usuarios con direcciones IP conocidas obtengan acceso no autorizado al servidor, permitiendo especificar la información apropiada en una lista de restricciones.

Volviendo de nuevo a la seguridad, IIS tiene integrado el protocolo Kerberos v5 (como le ocurre al sistema operativo). El almacenamiento de certificados se integra ahora con el almacenamiento CryptoAPI de Windows. Se puede utilizar el administrador de certificados de Windows para hacer una copia de seguridad, guardar y configurar los certificados.

Además, la administración de la seguridad del servidor IIS es una tarea fácilmente ejecutable a base de asistentes para la seguridad. Se pueden definir permisos de acceso en directorios virtuales e incluso en archivos, de forma que el asistente actualizará los permisos NTFS para reflejar los cambios. Si se trabaja con entidades emiso-

8.3. Instalación de IIS

tras de certificados, es posible gestionar la lista de certificados de confianza (CTL, *Certificate Trust List*) con el asistente para CTL.

8.3. Instalación de IIS

Como cualquier otro software de Windows, la instalación de IIS 6 es tan sencilla como hacer un doble clic de ratón. Normalmente es uno de los componentes de Windows 2003 que viene seleccionado por defecto. Si no fuera así, en la propia instalación de Windows 2003 se puede seleccionar bajo el epígrafe *Componentes de Windows*.

Si se desea instalar manualmente habría que ir al *Panel de Control->Añadir o Quitar Programas* y hacer clic sobre el ícono *Agregar o Quitar componentes de Windows*. Una vez lanzado el *Asistente para Componentes de Windows*, seleccionar de la lista *Servicios de Internet Information Server*.

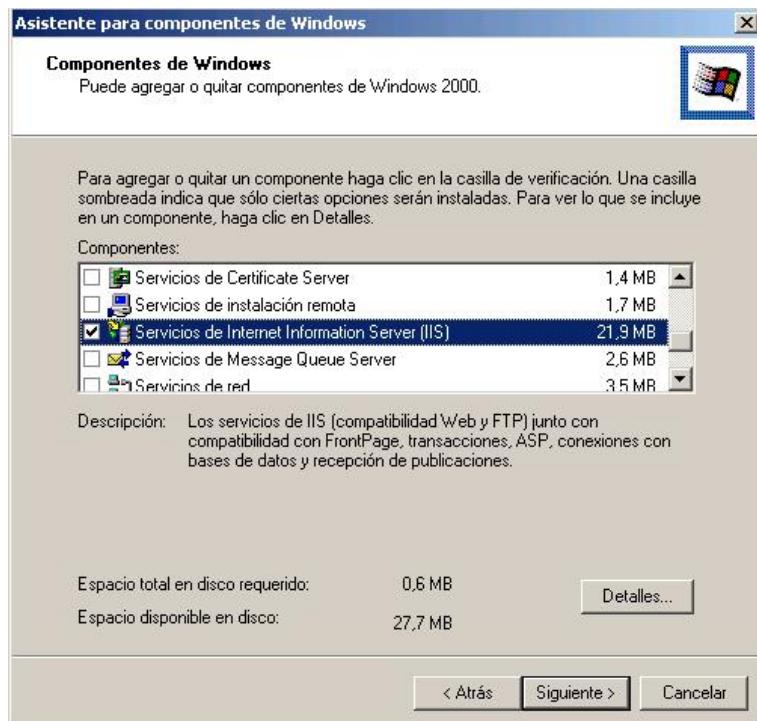


Figura 8.1. Asistente para componentes de Windows

8.4. Administración de sitios Web

En este punto, nos centraremos en las tareas de administración del servidor Web y Ftp de IIS, aunque IIS puede realizar las funciones de servidor SMTP (*Send Mail*

8.4.1. Creación de un sitio Web

Transfer Protocol) y de servidor NNTP (o servidor de noticias).

La herramienta recomendable de administración del software IIS será el snap-in de la MMC (Microsoft Management Console) o Administrador de servicios de Internet.

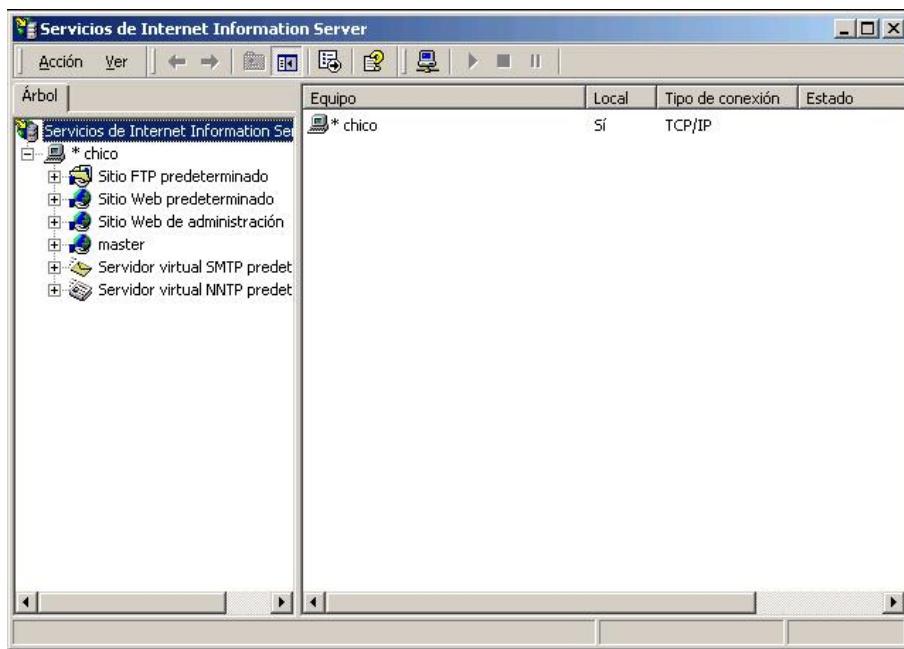


Figura 8.2. Administrador de servicios de Internet snap-in

8.4.1. Creación de un sitio Web

Internet Information Server incluye un sitio web, un sitio FTP, un sitio SMTP y un sitio NNTP configurados por defecto. Esto no significa que deba limitarse a un único sitio; se pueden crear sitios virtuales en el mismo equipo

Los sitios web están almacenados en directorios según una estructura lógica. Existen dos tipos de directorios: directorios principales y directorios virtuales.

- *Directorio principal:* En el caso del sitio web predeterminado suele ser el directorio *c:\InetPub\wwwroot*. En este directorio colgarán nuestras páginas web.
- *Directorio virtual:* se utiliza cuando el sitio web está distribuido entre varios directorios, unidades o equipos.

El primer paso para crear varios sitios web en su servidor consistirá en configurar

8.4.1. Creación de un sitio Web

los directorios principales predeterminados. Estos directorios pueden residir en el disco local o en una unidad de red. Bastará utilizar el explorador de Windows para crear una nueva carpeta.

A continuación, se iniciará el Administrador de servicios de Internet. En el menú *Acción*, seleccione *Nuevo sitio web*, para iniciar el *Asistente para crear un sitio web*. Haga clic en *Siguiente* para pasar a la pantalla de introducción de datos. El primer cuadro de diálogo nos pedirá una descripción del sitio, la cual lo identificará en la MMC.

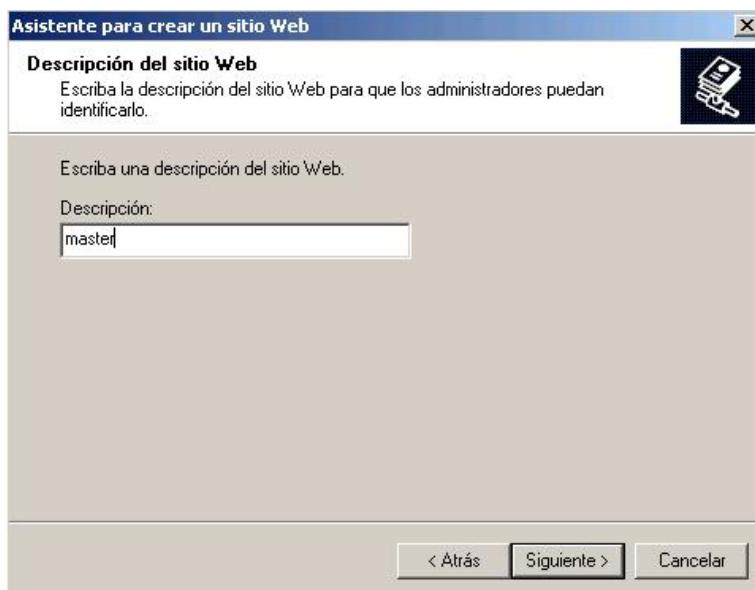


Figura 8.3. Descripción del sitio web

A continuación, aparecerá el cuadro de diálogo *Dirección IP y configuración de puerto*. En esta sección, también podemos definir el nombre de encabezado de host que nos permitirá crear un sitio virtual. Eso si, habrá que tener en cuenta que tendremos que añadir esa información a un servidor DNS (normalmente con una directiva CNAME) o en nuestro caso añadiendo la correspondiente entrada al fichero hosts.

8.4.1. Creación de un sitio Web

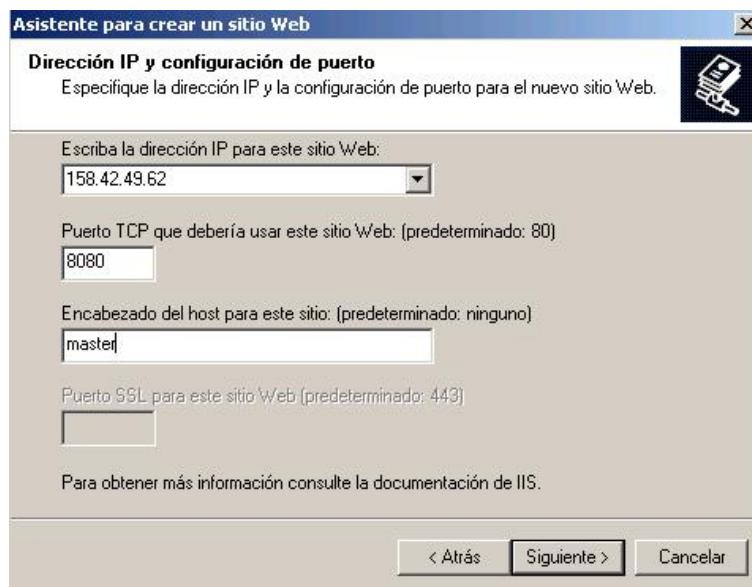


Figura 8.4. Dirección IP y configuración del puerto

El siguiente paso es definir el *Directorio particular*, donde escribiremos la ruta de acceso a la carpeta que hemos creado anteriormente. Si queremos que todo el mundo (sin autenticación previa) acceda a nuestro sitio web, dejaremos definido el ítem *Permitir accesos anónimos a este sitio Web*.

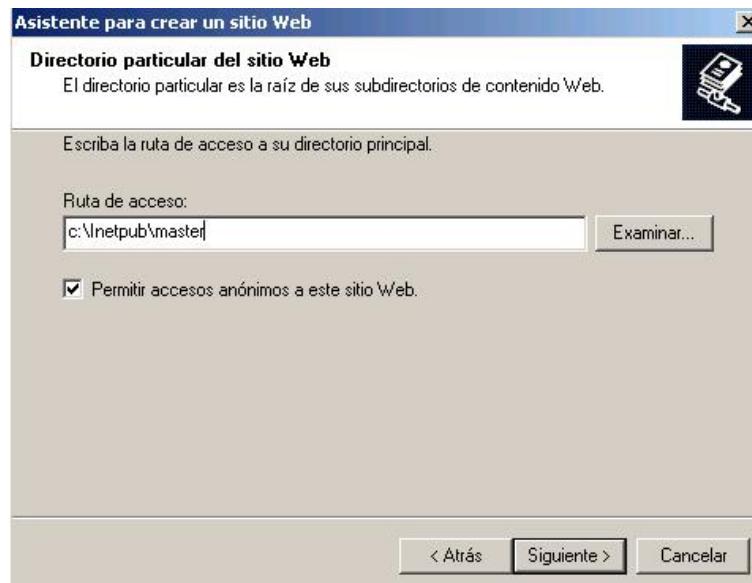


Figura 8.5. Directorio particular

8.4.2. Configuración de un sitio Web

Una vez definido el *Directorio particular*, aparecerá el cuadro de diálogo *Permisos de acceso al sitio web*.

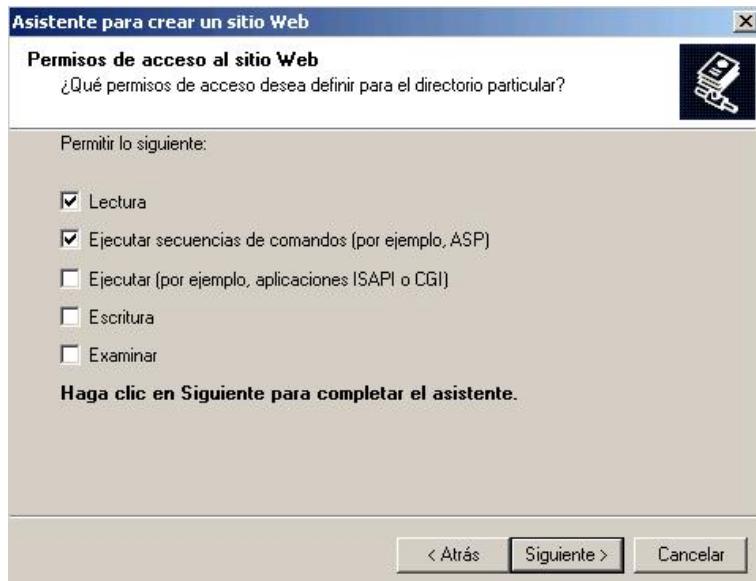


Figura 8.6. Permisos de acceso al sitio web

Esta pestaña nos permitirá definir los permisos adecuados para que los clientes tengan acceso a este sitio web:

- *Lectura*. Permite que los clientes vean páginas de este sitio.
- *Ejecutar secuencias de comandos*. Permite que los clientes soliciten páginas con código ASP y que se ejecute dicho código.
- *Ejecutar*. Esta opción permite la ejecución de aplicaciones CGI o ISAPI en este sitio.
- *Escritura*. Si se activa esta opción, los clientes podrán cargar, eliminar o transferir archivos a este directorio.
- *Examinar*. Permite que los clientes examinen el contenido de los directorios

Si hemos seguido los pasos anteriores en MMC tendremos una nueva entrada cuyo nombre se corresponderá con la descripción del sitio y por tanto habremos creado un nuevo sitio web.

8.4.2. Configuración de un sitio Web

8.4.2. Configuración de un sitio Web

Cada sitio web tiene asociadas una serie de propiedades que definen su comportamiento. Por tanto, el administrador es libre de cambiar este comportamiento modificando sus propiedades. Estas propiedades se pueden modificar a través de las páginas de propiedades, y pueden referirse al sitio, al directorio o a un fichero en cuestión.

La página de propiedades de un sitio web se obtiene en la MMC pulsando el botón derecho sobre el sitio web anteriormente definido y eligiendo el menú propiedades.

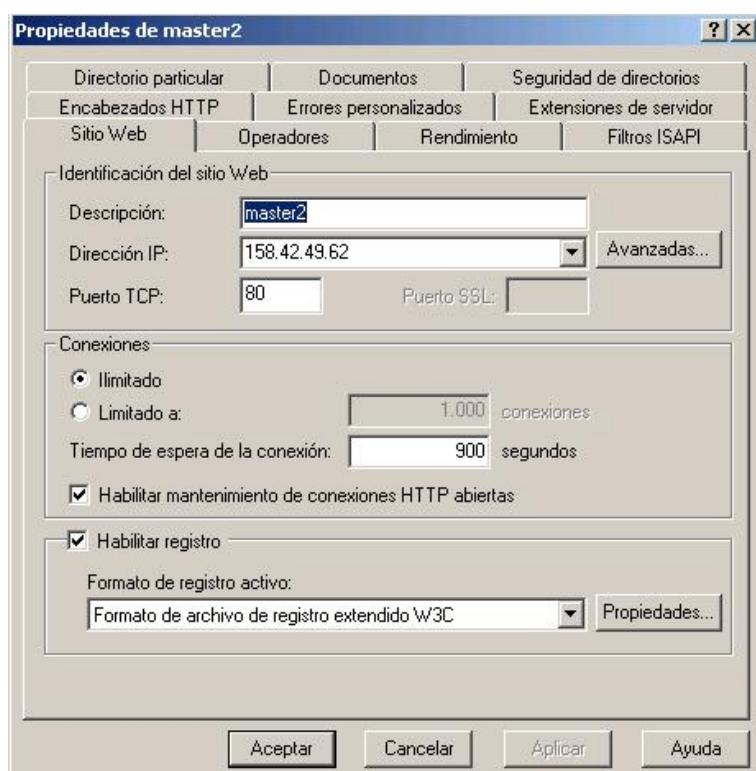


Figura 8.7. Propiedades Sitio web

Muchas de las propiedades que podemos definir aquí ya las hemos visto a la hora de definir el nuevo sitio web. Nos centraremos en este momento en aquellas que creemos son importantes para un buen funcionamiento del servidor.

- *Sitio Web.* En esta pestaña, además de definir la identificación del sitio web, podemos definir el número de conexiones que aceptará nuestro servidor web. En el caso de estar ejecutando IIS sobre Windows XP Profesional, existe una limitación

8.4.3. Directorios Virtuales

de 10 conexiones. También podremos habilitar un registro o log de los accesos y errores del sitio web.

- *Operadores.* Los operadores del sitio web son usuarios definidos en Windows 2003 que poseen permisos para alterar la configuración y el funcionamiento del servidor Web. Aquí añadiremos aquellos usuarios que deseamos administren el sitio web.
- *Rendimiento.* En esta pestaña podremos ajustar una serie de parámetros que influirán en el rendimiento del sitio web. Los parámetros que se configuran para cada sitio, prevalecen sobre los definidos en el servidor
- *Documentos.* Aquí definiremos el documento predeterminado que se mostrará si se invoca este sitio directamente sin indicar una página concreta.
- *Encabezados HTTP.* Utilizaremos esta pestaña para configurar los valores que se enviarán al navegador en el encabezado de la página HTML.

8.4.3. Directorios Virtuales

Los directorios virtuales son directorios lógicos, que pertenecerán a la estructura de directorios que puede percibir el usuario que se conecta a nuestro servidor, pero que se corresponde con directorios físicos que se encuentran en ubicaciones distintas del directorio principal del servidor.

Los directorios virtuales se crean definiendo un alias que hace referencia a un directorio físico, de forma que cuando se navega por el servidor web el usuario verá dicho directorio como si fuese un directorio que cuelga directamente del directorio principal del servidor.

Para crear un directorio virtual, seleccionaremos el sitio web deseado y con el botón derecho elegiremos *Nuevo* y a continuación *Directorio Virtual*, para lanzar el asistente de creación de directorios virtuales. Lo primero que nos solicitará será el nombre del alias que le queremos dar al directorio

8.4.3. Directorios Virtuales

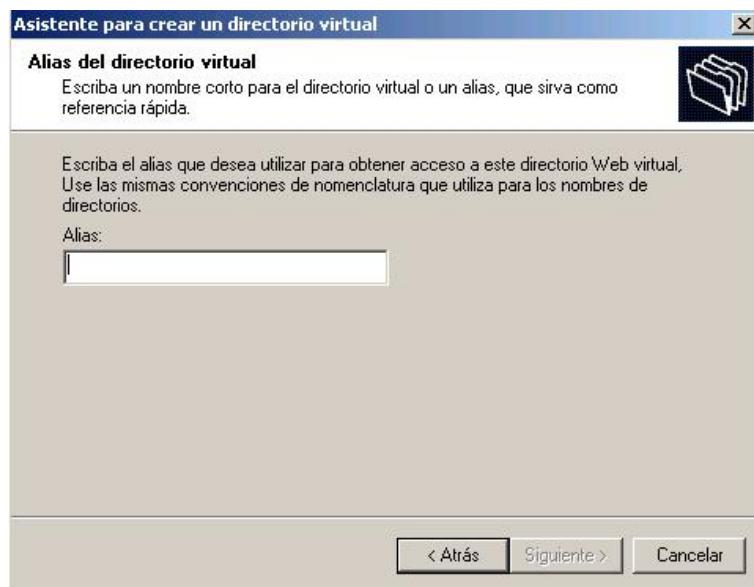


Figura 8.8. Alias del directorio virtual

Y a continuación nos pedirá la ubicación física del directorio, es decir su trayectoria y los permisos que queremos que posea.



Figura 8.9. Ubicación del directorio

8.4.4. Seguridad de un sitio Web

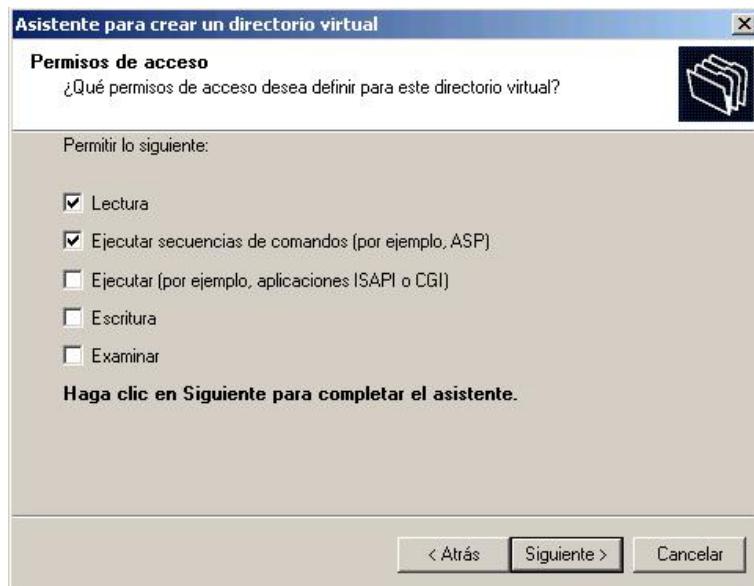


Figura 8.10. Permisos del directorio virtual

8.4.4. Seguridad de un sitio Web

Realmente, los mayores esfuerzos de Microsoft a la hora de lanzar esta nueva versión de IIS se han centrado en la seguridad. Dejando a un lado los agujeros de seguridad que caracterizan a este software (pero sin olvidarse de ellos), IIS 6 incorpora nuevas y muy buenas funcionalidades referentes a la autenticación y la seguridad.

Normalmente, el acceso a un servidor web (acceso a sus recursos) se lleva a cabo de forma anónima o más bien bajo la apariencia de un usuario que se crea con tal propósito en el momento de la instalación de IIS. Este usuario se denomina *IUSR_nombreservidor*.

Pero será conveniente limitar el acceso a ciertas zonas del servidor que contienen información privilegiada o simplemente información preparada para un usuario o máquina concreta, ya que IIS utiliza las características de seguridad de Windows 2003 y el sistema de ficheros NTFS para fijar la política de seguridad del sitio web.

Si queremos restringir el acceso a nuestro sitio web o a partes del mismo, debemos modificar las propiedades predeterminadas en la pestaña *Seguridad de directorios*.

8.4.4. Seguridad de un sitio Web

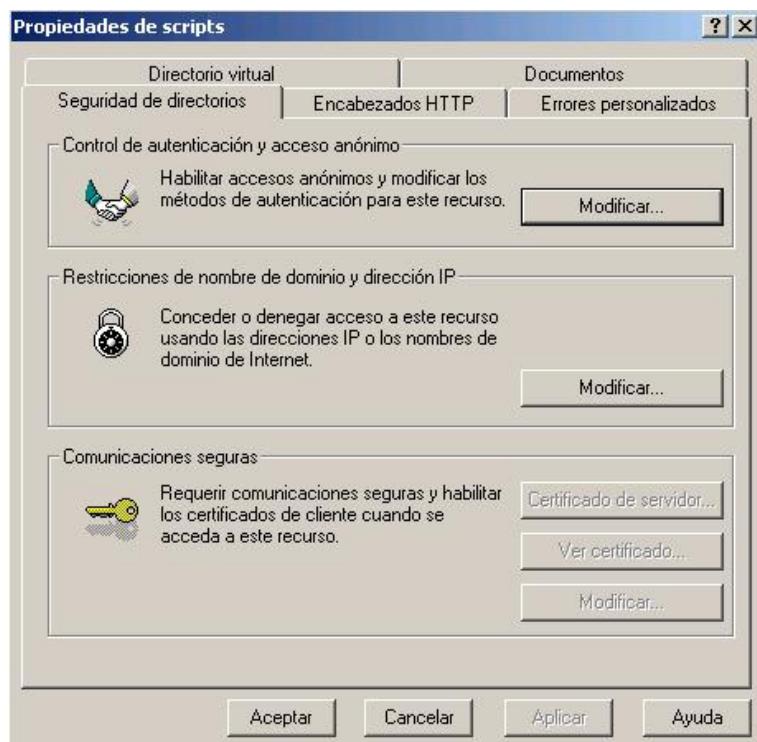


Figura 8.11. Seguridad en directorios

8.4.4.1. Control de autenticación y acceso anónimo

Si lo que deseamos es proteger una zona del servidor según el usuario que solicita el recurso, emplearemos esta propiedad, la cual nos permite definir tres métodos de autenticación

- *Autenticación básica* La autenticación básica es un método estándar, soportado por la mayoría de navegadores, que solicita al cliente un usuario y un password. El problema radica en que esa información crítica de seguridad viaja por la red sin cifrar.
- *Autenticación de texto implícita* La autenticación de texto implícita, una nueva característica de IIS 6, ofrece las mismas características que la autenticación básica, pero incluye una forma diferente de transmitir las credenciales de autenticación. Las credenciales de autenticación pasan por un proceso unidireccional, frecuentemente llamado hashing. El resultado de este proceso se denomina hash o código resultado del mensaje y no es factible descifrarlo. Es decir, no se puede descifrar el texto original a partir del hash.

8.4.4. Seguridad de un sitio Web

- *Autenticación de Windows integrada* La autenticación de Windows integrada (anteriormente llamada NTLM o Autenticación Desafío/Respuesta de Windows NT) es un método seguro de autenticación, ya que no se envía a través de la red el nombre de usuario ni la contraseña. Al habilitar la autenticación de Windows integrada, el explorador del usuario demuestra que conoce la contraseña mediante un intercambio criptográfico con el servidor Web, en el que interviene el hashing.

En la siguiente figura se muestran como seleccionar y definir las propiedades de los diferentes métodos de autenticación.

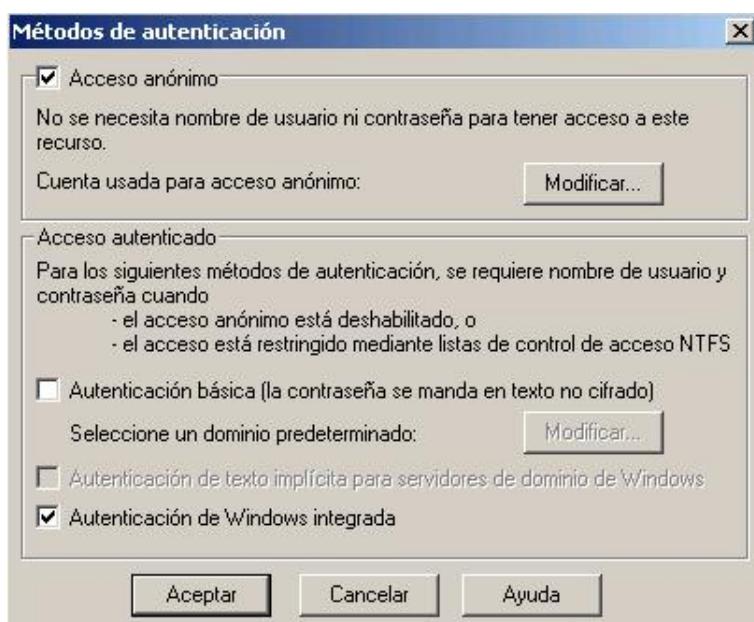


Figura 8.12. Métodos de autenticación

8.4.4.2. Restricciones de dominio y dirección IP

Si lo que interesa al administrador del sitio web es limitar el acceso por equipo, sabemos que todas las máquinas en una red como Internet vienen definidas por su dirección IP, por tanto podremos establecer una lista o rango de direcciones o nombres de dominio que tengan el acceso garantizado.

8.4.5. Copia de seguridad y restauración de la configuración



Figura 8.13. Restricciones de nombres de dominio y dirección IP

8.4.5. Copia de seguridad y restauración de la configuración

Una de las grandes ventajas de IIS (para algunos administradores) es su configuración gráfica, debido a su interfaz intuitiva y de fácil uso. Pero no sería práctico, sino pudieramos salvar la información de configuración para poder restaurarla después.

Siempre he pensado que lo mejor es un fichero de configuración tipo texto, donde poder ir modificando variables y así tener una copia del mismo. No hay que alarmarse debido a que IIS no ofrece esta característica ya que si que soporta salvar la configuración en un formato propio de Windows para posteriormente restaurarla de forma sencilla.

Los pasos a realizar para hacer una copia de seguridad de la configuración actual serían los siguientes:

- En el complemento, *Administración de servicios de Internet*, se selecciona el ícono del equipo para resaltarlo en el panel izquierdo.
- En el menú *Acción*, elija la opción *Realizar o restaurar copia de seguridad de la configuración*.
- Hacer clic en el botón *Realizar copia de seguridad*, que mostrará un cuadro de diálogo *Realizar copia de seguridad* que le permitirá definir el archivo de copia de seguridad.

De forma predeterminada, el archivo de copia de seguridad se almacena en el directorio *c:\winnt\system32\inetsrv\Metaback*

8.5. Programación Web en IIS 6

Un sitio web no se nutre solamente de contenidos estáticos. La verdadera naturaleza de la Web es la posibilidad de ofrecer contenidos dinámicos ya sea consultando a una Base de Datos o a cualquier otro medio de almacenamiento.

Como casi todos los servidores Web disponibles en el mercado, IIS 6 ofrece una gran gama de posibilidades de programación, pudiendo optar el desarrollador por distintos lenguajes y tecnologías.

Entre las diferentes tecnologías disponibles en IIS, podemos desarrollar contenidos dinámicos utilizando *ASP* (*Active Server Pages*), *aplicaciones ISAPI* (*Internet Server Application Programming Interface*) o *aplicaciones CGI* (*Common Gateway Interface*).

La elección del lenguaje es particular en cada programador y adaptable a las circunstancias que pueda requerir la aplicación. Nosotros, en los siguientes apartados vamos a ahondar en el desarrollo de un lenguaje como Python y como se integra con IIS.

8.5.1. ASP y Python

ASP es una tecnología de Microsoft que permite ejecutar secuencias de comandos en el servidor para crear y ejecutar aplicaciones dinámicas e interactivas de servidor Web. Con ASP puede combinar páginas HTML, secuencias de comandos y componentes COM para crear páginas Web interactivas o dinámicas.

ASP está implementado como un conjunto de objetos con características predefinidas para el fácil y rápido acceso a los servicios proporcionados por el servidor web. ASP expone siete objetos que pasamos a detallar ahora:

- *Application*: este objeto representa la aplicación ASP bajo la cual se ejecuta el script. Una aplicación ASP es una colección de ficheros ASP que comparten cierto estado e información.
- *ObjectContext*: este objeto expone el mecanismo transaccional que existe tras ASP.
- *Request*: representa los valores del navegador cliente que han sido pasados al servidor cuando se estableció la conexión.
- *ASPError*: contiene información sobre la condición de error.
- *Response*: este objeto envia la salida al cliente.
- *Server*: representa el servidor ASP, permitiendo al programador consultar información del servidor.

8.5.1. ASP y Python

Con esta tecnología no es necesario ningún requerimiento en el cliente, solo se necesita en el servidor indicar que hacer con esas características. Normalmente, un lenguaje de *scripting* se instala y se utiliza en el servidor para programar ASP.

Python se instala con ActivePython y es capaz de funcionar como lenguaje de scripting otorgando el poder de Python al entorno ASP. Solamente se necesita aprender el modelo de objetos de ASP y como trabaja PERL con objetos.

Para ejecutar correctamente la secuencia de comandos dentro de un fichero ASP, debemos especificar que lenguaje de scripting debe utilizar ASP para interpretarlos. Esto se consigue introduciendo como primera línea en el fichero asp la siguiente secuencia:

```
<%@ Language=Python %>
```

Una vez definido el lenguaje, las secuencias de comandos irán delimitados por <% %>. Un sencillo ejemplo de página ASP utilizando como lenguaje Python sería el siguiente:

```
<%@Language=Python%>
<HTML> <TITLE> Python ASP Test </TITLE> <%
for i in range(1,5): Response.Write("<FONT SIZE=$i
COLOR=#000000>") Response.Write("Hello World!
</FONT> <BR>" ) %> </HTML>
```

A destacar el empleo de objetos en Python, utilizando la misma sintaxis que VB Basic *Response.Write*

Response almacena el objeto *Response* del modelo de objetos ASP, responsable de enviar datos del servidor al cliente (Cookies ...), mientras que *Write*, define un método de dicho objeto.

Estos ficheros ASP habría que ubicarlos en un directorio (particular o virtual), que tuviera permisos de acceso *Ejecutar secuencias de comandos*, para que fuera posible su ejecución.

9

Administración de discos

Índice

9.1.	Geometría de los discos duros	131
9.1.1.	Límites a la geometría de los discos IDE	131
9.1.2.	Problemas causados por límites a la geometría IDE	134
9.1.3.	Particiones del disco	135
9.2.	La consola de administración de discos	137
9.2.1.	Configuración de la consola	137
9.2.2.	Discos básicos y dinámicos	138
9.2.3.	Creación de particiones	139
9.2.4.	Creación de volúmenes	142
9.3.	Utilidades	145
9.3.1.	Diskpart	145
9.4.	Sistemas de ficheros	147
9.5.	Cuotas de disco	148
9.5.1.	Habilitar cuotas	148
9.5.2.	Definición de cuotas individuales	149
9.6.	Copias de seguridad	150
9.6.1.	Carpetas y ficheros	150
9.6.2.	Estado del sistema	151

9.1. Geometría de los discos duros

Los discos duros son el medio de almacenamiento masivo y permanente por excelencia en los ordenadores. Existen dos grandes grupos de discos en función de su interfaz con el ordenador, IDE y SCSI. En esencia, ambos grupos son equivalentes, salvo en aspectos de rendimiento, fiabilidad y precio. Difieren, eso sí, en las limitaciones que el software de sistemas ha impuesto de forma artificial a los discos IDE en el mundo de los PCs. Un disco almacena su información en uno o más platos, disponiendo de una cabeza lectora para cada una de las dos caras del plato (aunque en algunas ocasiones una cara no es utilizada). Cada cara está dividida en varios anillos concéntricos, denominados pistas. Esta división es debida a que el plato gira sobre su eje, y la cabeza lectora se desplaza longitudinalmente hacia o desde el eje. A su vez, cada pista está subdividida en sectores, todos ellos de igual capacidad, 512 bytes en la gran mayoría de los casos. Todos los platos de un disco están unidos y también lo están entre si las cabezas lectoras. El conjunto de pistas que se encuentran bajo todas las cabezas lectoras recibe el nombre de cilindro. Resumiendo, la capacidad de un disco puede describirse indicando su número de cilindros, cabezales y sectores por pista. Por ejemplo, un disco con 4096 cilindros, 16 cabezales y 63 sectores por pista alberga un total de:

$$4096 \times 16 \times 63 = 4.128.768 \text{ sectores de 512 bytes}$$

$$2.113.929.216 \text{ bytes}$$

$$2.064.384 \text{ Kbytes}$$

$$2.016 \text{ Mbytes} =$$

$$1'96875 \text{ Gbytes.}$$

Hay que tener en cuenta que el fabricante del disco dirá que su disco tiene 2^{30} Gbytes. Los fabricantes de discos asumen que un Gbyte equivale a mil millones de bytes, no a 2^{30} bytes. Por cierto, los nuevos estándares dan la razón a los fabricantes, y nos indican que deberíamos utilizar los nuevos términos Kibbytes, Mibbytes, Gibbytes para expresar las correspondientes potencias de 2. Sin embargo, en este documento no vamos a utilizar este estándar.

9.1.1. Límites a la geometría de los discos IDE

Existen diferentes límites a la geometría descrita que han sido impuestos (artificialmente) por el hardware o el software. Los tres más importantes se explican a continuación, seguidos de un apartado que comenta cómo se han superado hasta la fecha.

9.1.1.1. La especificación ATA

Según la especificación establecida por los fabricantes de discos duros, la forma de indicar al controlador del disco qué sector deseamos acceder es mediante su número de cilindro, de cabezal y de sector. La especificación también establece un número máximo de bits para cada valor, lo cual condiciona el número más grande de cilindros, cabezales y sectores que podemos direccionar. Este máximo número de bits es, para cada valor, el siguiente:

- Para el número de cilindro : 16 bits.
- Para el número de cabezal : 4 bits.
- Para el número de sector: 8 bits.

Por tanto, según la especificación ATA, un disco duro puede direccionar, como mucho:

65536 cilindros * 16 cabezales * 256 sectores por pista.

Si multiplicamos este número máximo de sectores por 512 bytes, el resultado es de 127'5 Gbytes, es decir, el tamaño teórico máximo de disco duro de la especificación ATA.

En el momento de escribir estas líneas, este límite está prácticamente a punto de alcanzarse, dado que ya se venden discos IDE de 100Gb de capacidad.

9.1.1.2. Las rutinas de disco clásicas de la BIOS

Algunos sistemas operativos antiguos para PC, como por ejemplo MSDOS, utilizan la BIOS como la forma natural de acceder a los discos, entre otros dispositivos. Es el mismo caso que muchos de los cargadores de los sistemas operativos actuales. En estos casos, el sistema operativo informa a la BIOS de qué número de sector desea acceder, y la BIOS traduce esta petición al controlador del disco, según la especificación ATA presentada anteriormente.

En este caso, la propia BIOS presenta al sistema operativo una interfaz de funciones en la que tiene también un número de bits reservados para direccionar el cilindro, cabezal y sector. La cantidad máxima de bits que las funciones "clásicas" de acceso reservaban para cada valor son las siguientes:

- Para el número de cilindro : 10 bits.

9.1.1. Límites a la geometría de los discos IDE

- Para el número de cabezal : 8 bits.
- Para el número de sector: 6 bits.

Por tanto, utilizando las rutinas tradicionales de la BIOS, un disco duro puede direccionar, como mucho:

1024 cilindros * 256 cabezales * 63 sectores por pista

El hecho de que el número de sectores por pista sea de 63 en vez de 64 proviene del hecho de que, según el mecanismo tradicional de direccionamiento de los discos (denominado CHS^{footnote{Su nombre viene del acrónimo inglés *Cylinder-Head-Sector*, los sectores se numeran desde 1 en vez de numerarlos desde 0.}}

Multiplicando esta cantidad de sectores por 512 bytes, el valor resultante es de 7'84 Gbytes, que es el tamaño máximo de disco duro que reconocen esas BIOS tradicionales. Incluso en BIOS más modernas, que incorporan otras funciones de acceso, esa limitación sigue existiendo para el software que utiliza aquellas funciones clásicas para acceder al disco. Este es el caso, por ejemplo, del ancestral sistema DOS y, hasta hace poco tiempo, también de LILO, el cargador por excelencia del sistema operativo Linux.

9.1.1.3. La limitación conjunta de las dos anteriores

En un primer momento, la limitación real no fue la anterior, sino la limitación combinada de las dos anteriores. Es decir, puesto que los discos duros no pueden tener más de 16 cabezales (porque así lo han decidido los fabricantes), la limitación de la BIOS aún se restringía más, dando como resultado los siguientes números:

- Para el número de cilindro : 10 bits.
- Para el número de cabezal : 4 bits.
- Para el número de sector: 6 bits.

Es decir:

1024 cilindros * 16 cabezales * 63 sectores por pista.

Multiplicando por 512 bytes, esta cantidad de sectores permitía un total de 1'048 Mbytes}, una cantidad supuestamente inalcanzable en los años de los primeros sistemas para PC, pero que apenas 15 años después resultó claramente insuficiente.

9.1.1.4. Superando las limitaciones

La aparición de discos de más de 504 Mb, con más de 1024 cilindros, causó serios problemas, ya que millones de ordenadores con DOS instalado no podían utilizarlos directamente.

La forma de salvar esta primera limitación consistió en aprovechar que la BIOS permitía un número mayor de cabezales que la especificación ATA, aunque menos cilindros. Por tanto, el objetivo consistía en implementar a nivel de BIOS una traducción que, manteniendo inalterable el número máximo de sectores del disco, ofreciera al sistema operativo un número superior (ficticio) de cabezales (hasta 256) y un número proporcionalmente inferior de cilindros (hasta 1024). Internamente la BIOS realiza la traducción de ese número de sector virtual al número de sector real.

En este sentido, el modo de direccionamiento LBA (o Logical Block Addressing) resulta particularmente interesante. En este modo de direccionamiento, el controlador del disco ofrece a los niveles superiores la visión de que el disco está formado por un vector lineal de sectores. Por tanto, los tres valores que identifican un sector en el disco (cilindro, cabezal y sector) se especifican como un único número entre 0 y el número máximo de sector. A nivel de la especificación ATA, el número de sector sería un número de 28 bits ($16 + 4 + 8$). Al aparecer discos que permitían direccionamiento LBA, las BIOS fueron modificadas para utilizar también este modo y sus 24 bits de direccionamiento ($10 + 8 + 6$) se utilizaron para especificar un número lineal entre 0 y 2^{24} , que luego la BIOS pasa directamente al controlador del disco, permitiendo llegar naturalmente hasta el máximo de 7'84 Gb.

Finalmente, esa barrera de los 7'84 Gb se ha superado incluyendo nuevas funciones en las BIOS, con una especificación LBA que utiliza un número mayor de bits. De esta forma se puede llegar hasta el máximo de la especificación ATA.

9.1.2. Problemas causados por límites a la geometría IDE

Estas limitaciones en los discos típicos para PC han ocasionado limitaciones en algunos sistemas operativos. A continuación se revisan los sistemas más populares:

1. DOS, Windows 3.x, Windows 95, Windows NT 3.x. DOS utiliza las rutinas clásicas de la BIOS para acceder al disco. Por tanto, DOS no puede utilizar más de 1024 cilindros. El modo LBA es imprescindible y el tamaño máximo de disco soportado, tal como se ha explicado anteriormente, es de 7'84 Gbytes. Los sistemas Windows que aparecieron a continuación heredaron esta restricción de DOS por motivos de compatibilidad.
2. Windows 95 OSR2, Windows 98, Windows ME. No tienen ningún problema.

9.1.3. Particiones del disco

No utilizan las rutinas clásicas de la BIOS y por tanto pueden utilizar más de 1024 cilindros.

3. Windows NT 4.0. Este sistema tiene soporte para discos grandes desde su aparición. No obstante, el proceso de instalación de NT está basado en DOS, con lo cual, la partición donde reside NT debe estar antes de la barrera de los 1024 cilindros.

En resumen, en nuestros días apenas nos estamos librando de las restricciones que impuso el diseño original de la BIOS. Sólo en las últimas versiones de los sistemas operativos para PC, esas limitaciones no suponen un problema de instalación o de uso.

9.1.3. Particiones del disco

En el primer sector de un disco duro reside el denominado MBR (o Master Boot Record). En estos 512 bytes residen el código inicial de carga del sistema operativo, la tabla de particiones primarias y la firma del disco.

El código de carga más frecuente es el que define el sistema operativo DOS, el cual se encarga de buscar la partición de arranque, cargar en memoria el primer sector de dicha partición y cederle el control. Éste es el método utilizado por todos los sistemas operativos de Microsoft. Este código de carga puede recuperarse (reinstalarse) con el mandato DOS FDISK /MBR, el cual deja intacta la tabla de particiones.

Otros códigos de carga bastante utilizados son los cargadores que vienen con el sistema operativo Linux: LILO y GRUB. En realidad, el código que se ubica en el MBR es el correspondiente a la primera fase del proceso de arranque. Estos cargadores son más complejos y flexibles que el código de carga de DOS, y utilizan la información que reside en el directorio /boot de Linux para determinar qué sistema operativo debe cargarse.

El código de carga se utiliza tan sólo en el disco principal del sistema (es decir, el disco maestro del interfaz IDE primario). Hay BIOS que permiten arrancar de otros discos duros, pero generalmente aparecen numerosos problemas al utilizar esta opción.

La tabla de particiones está formada por cuatro entradas, donde cada una de ellas describe una potencial partición primaria. Los detalles de cada entrada son algo oscuros, y su utilización varía sensiblemente de un sistema operativo a otro. No obstante, simplificando un poco, cada entrada indica, para la partición que describe, la siguiente información:

9.1.3. Particiones del disco

1. El sector del disco donde comienza.
2. Su tamaño.
3. Si es una partición de arranque (activa).
4. Su tipo.

DOS, Windows 3.x y Windows 95 representan el inicio de la partición utilizando la tripleta <cilindro,cabezal,sector>, con lo cual el tamaño máximo de una partición es de 7'84 Gbytes (debido a la limitación de los 1024 cilindros). El resto de sistemas representan el inicio de la partición indicando cuál es el sector lógico donde comienza (viendo al disco como un vector de sectores lógicos). Estos sistemas utilizan una palabra de 32 bits, lo que permite 2^{32} sectores, equivalente a 2 Tbytes (2×1024 Gbytes). En este caso, aún estamos algo lejos de disponer de discos de estas características.

El indicador de partición de arranque es utilizado tan sólo por el código de carga de DOS. Linux ignora por completo esta información.

Existen numerosos tipos de particiones, en función de su utilización o de su organización interna (establecida por el sistema operativo que la defina). Existe una convención que establece el identificador de cada tipo de partición como un número concreto en hexadecimal. La siguiente tabla expone los tipos de particiones más habituales.

Tabla 9.1. Principales tipos de particiones

Tipo	Uso	Limitación
0	Partición vacía	
5	Partición extendida	1024 cilindros (7'84GB)
6	DOS FAT 16	2 GB
7	OS2 o NTFS	2TB
b	Windows 95 FAT 32	2TB
f	Extendida Windows 95	2TB
80	Old Minix	-
82	Linux Swap	-
83	Linux Native	2TB

Una partición extendida es un contenedor para otras particiones, a las cuales se les denomina particiones lógicas. Sólo una de las particiones primarias puede declararse como extendida. La representación de las unidades lógicas se realiza utilizando una lista enlazada que reside dentro de la partición extendida, por lo que no hay

límite en cuanto al número de particiones lógicas que se pueden crear. La partición extendida convencional ha tenido que ser cambiada por la nueva partición extendida Windows 95, ya que la primera no puede abarcar discos mayores de 7'84 Gbytes.

9.2. La consola de administración de discos

La herramienta típica para manejar discos y particiones en el entorno windows, siempre ha sido *FDISK*. Cuando el sistema posee múltiples discos, esta utilidad suele traer muchos quebraderos de cabeza al administrador.

En el proceso de instalación de un sistema windows 2003, se solicita la creación, borrado y formateado de particiones, como paso previo a la definición de un sistema de ficheros. La utilidad encargada de ello se denomina *DISKPART* (ver sección...).

Una vez arrancado el sistema la consola de administración de discos, será la principal utilidad para manejar los discos físicos y lógicos de nuestra máquina. La Consola de Administración de Discos puede ser utilizada por usuarios miembros del grupo Administradores. Esta herramienta se utiliza tanto para configurar nuevos discos, como para administrar la tolerancia a fallos de los mismos.

Para ejecutar la Consola de Administración de Discos, sigue los siguientes pasos:

1. En el menú Inicio, selecciona Programas.
2. En Programas, selecciona Herramientas Administrativas.
3. En Herramientas Administrativas, selecciona Administración de Equipo.

9.2.1. Configuración de la consola

La Consola es una herramienta altamente configurable. Muestra de una forma visual el tamaño y el tipo de las particiones para poder identificarlas fácilmente.

La Consola de Administración de Discos tiene dos paneles configurados por defecto para mostrar en el superior la lista de dispositivos extraíbles, discos, cd-rom, mientras que el inferior muestra una vista gráfica y coloreada de las particones, conjuntos espejo, seccionados etc ...

Para poder personalizar la Consola de Administración de Discos, sigue los siguientes pasos:

9.2.2. Discos básicos y dinámicos

1. En el menú, seleccionar Ver.
2. Desde aquí se puede seleccionar lo que queremos ver, tanto en el panel superior como en el inferior. Las elecciones pueden ser las siguientes:
 - Lista de discos: muestra todos los dispositivos en forma de lista.
 - Lista de Volúmenes: es la vista por defecto en el panel superior.
 - Vista Gráfica: vista por defecto en el panel inferior.

9.2.2. Discos básicos y dinámicos

En Windows 2003 disponemos de dos tipos de almacenamiento:

1. Básico:

Discos orientados a particiones, que es el sistema tradicional del PC. El disco puede contener particiones primarias y extendidas, y dentro de estas últimas volúmenes lógicos. Todos los sistemas anteriores a Windows 2003 pueden ver este tipo de disco.

2. Dinámico:

Se trata de una novedad de Windows 2003 para dar soporte a sistemas tolerantes a fallos mediante el uso de varios discos. Los discos no se organizan en particiones sino en volúmenes, superando esta nueva organización las restricciones tradicionales del sistema de particiones del PC. Con el almacenamiento dinámico, los cambios en los discos surten efecto en el sistema sin necesidad de reiniciar el equipo. Por el contrario, no pueden contener particiones y por tanto no son accesibles desde versiones anteriores de Windows ni desde MS-DOS.

Se administran con el servicio LDM (Logic Disk Manager) y el controlador dmio.sys.

Todos los discos dinámicos forman parte del grupo de discos de la máquina. La información de los discos dinámicos se encuentra guardada en un espacio reservado en los propios discos, y no en el registro como en la versión anterior de Windows NT. De este modo, si se lleva el disco a otra máquina, la máquina destino sabe que ese disco estaba en otra máquina y podrá acceder a la información pues los metadatos están en el mismo disco. En la máquina origen, se reconoce la falta del disco pues en el resto de discos dinámicos se tiene la infor-

9.2.3. Creación de particiones

mación referente a este disco.

No obstante, Windows 2003 es compatible con los conjuntos de volúmenes de Windows NT. Dispone del controlador FTDISK de modo que reconoce los conjuntos de volúmenes que NT creaba sobre particiones en discos básicos.

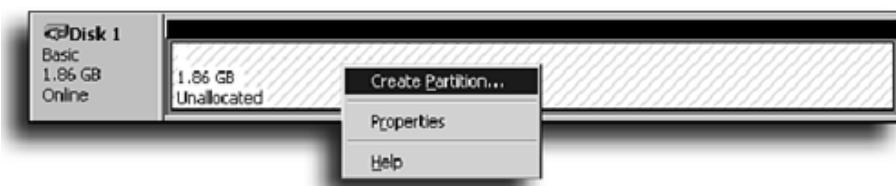
Visto lo anterior, cuando se quiera destinar un nuevo disco en el sistema para crear particiones y unidades lógicas se utilizará en modo básico. Si se desea crear un sistema tolerante a fallos, se inicializará el disco en modo dinámico.

Un disco puede pasar de dinámico a básico y viceversa, pero cuando el disco contiene datos, se deben tener en cuenta ciertas restricciones que se detallan en el apartado Actualización de discos básicos a dinámicos, más adelante en este capítulo.

9.2.3. Creación de particiones

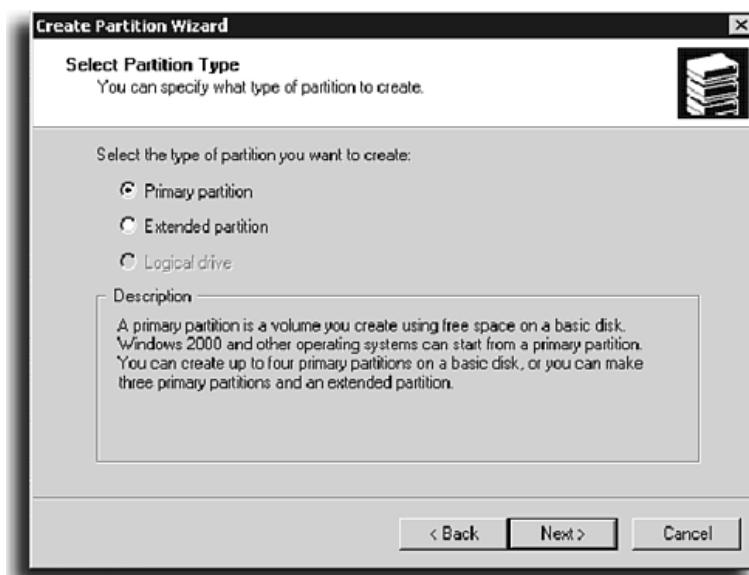
Antes de crear una partición se necesita saber que tipo de partición queremos: primaria, extendida o lógica. Los pasos necesarios para poder crear una partición se detallan a continuación:

1. Abrir la Consola de Administración de Discos.
2. Selecciona el disco sobre el que crear la partición y que dispone de espacio libre.
3. Con el botón derecho del ratón, selecciona Crear Partición.

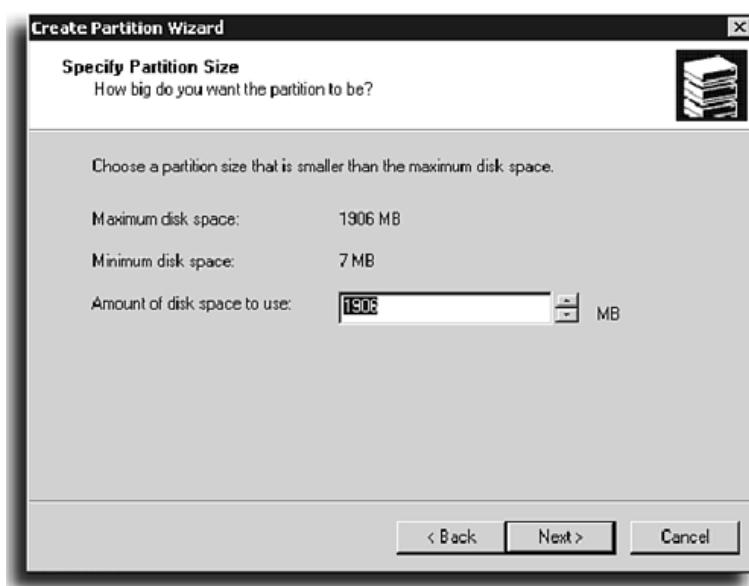


4. En el cuadro de dialogo que aparece, selecciona el tipo de partición (primaria, extendida, lógica). Si es sobre un espacio libre las únicas opciones que nos aparecerán son primaria y extendida. Si es sobre una partición extendida, solo aparecerá tipo de partición lógica.

9.2.3. Creación de particiones



5. A continuación se selecciona el tamaño de la partición.



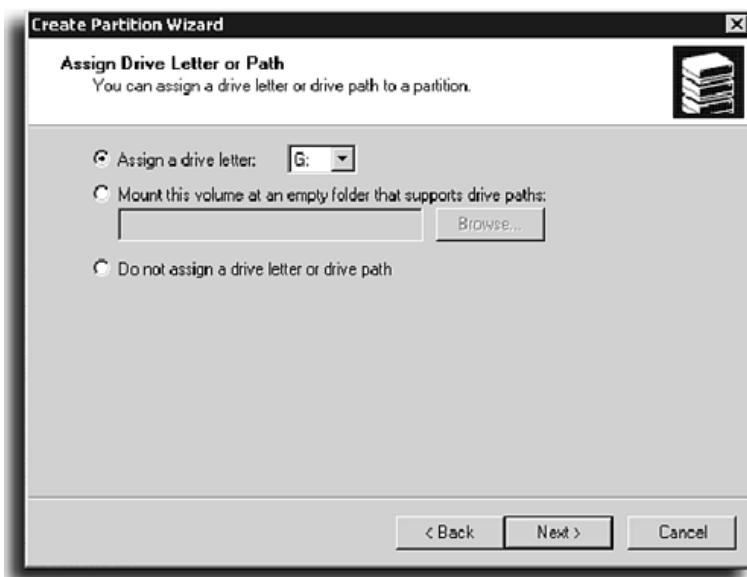
6. El siguiente paso sería asignar a la partición un punto de montaje (letra de unidad o Path). Windows 2003 trata a los volúmenes como unidades de almacenamiento que pueden o no encontrarse en el espacio de nombres del almacenamiento del sistema. Para que los volúmenes sean accesibles, se han de montar en el espacio de nombres. Los puntos de montaje son estáticos, es decir, una vez asignado, el volumen mantiene su ruta de acceso.

Una letra de unidad hace accesible la partición al modo tradicional de MS-

9.2.3. Creación de particiones

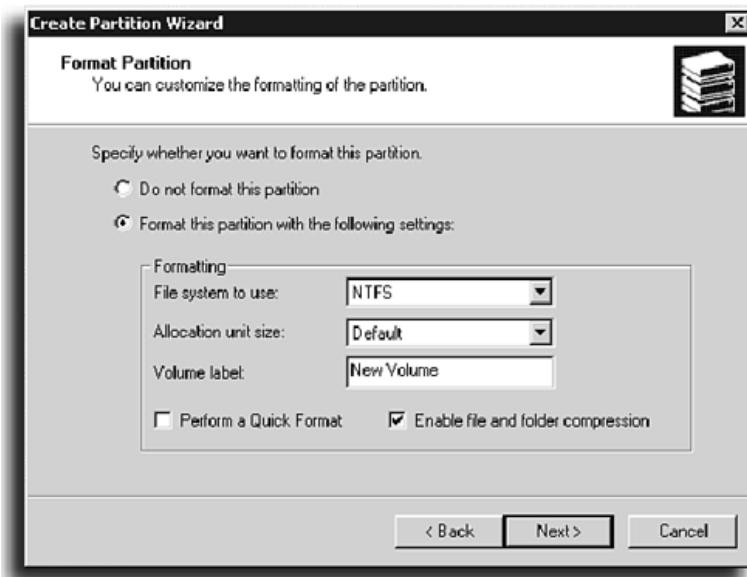
DOS. Todos los datos del volúmen se encuentran accesibles partiendo de la letra que se ha asignado. Windows 2003 permite asignar 26 letras, de las que la A y la B están reservadas para unidades de disquete, y de la C a Z al resto. Las letras de las particiones del sistema o de arranque no pueden ser modificadas. Además, solo puede asignarse una letra.

Asignando al volumen un punto de montaje en una carpeta vacía de otro volúmen ya montado, el volúmen se hace accesible a partir de esa carpeta. Los volúmenes pueden montarse en cualquier carpeta de un volúmen formateado con NTFS de Windows 2003, de un disco tanto básico como dinámico. La unidad montada puede estar formateada con cualquier sistema de archivos soportado por Windows 2003.



7. El último paso consistirá en decidir que sistema de ficheros (formato) queremos asignar a la partición a crear. También está la posibilidad de no formatearla en este instante.

9.2.4. Creación de volúmenes



Este proceso al final mostrará un sumario de las acciones que se van a llevar a cabo. Hacer notar que si se decide formatear la partición, este proceso se realizará en un segundo plano.

9.2.4. Creación de volúmenes

Los volúmenes aparecen en Windows 2003 gracias a la nueva gestión de los discos. Solo están disponibles en discos dinámicos, y dan posibilidad de disponer de tolerancia a fallos. Un volumen de disco es una porción de disco duro que funciona como si se tratase de un disco físico independiente. El volumen puede estar formado por una sola porción de un disco duro o por varias porciones del mismo disco o varias porciones de varios discos duros.

Los volúmenes de Windows 2003 pueden ser de varios tipos:

- Simple: Único tipo posible si solo disponemos de un disco en modo dinámico.
- Distribuido
- Seccionado.
- De espejo.
- RAID-5

9.2.4.1. Volumen simple

Se trata de un volumen formado por una o varias porciones del mismo disco. Solo pueden crearse en discos dinámicos y se pueden reflejar, aunque no soportan más opciones de tolerancia a fallos. Los volúmenes simples son lo mas parecido a las particiones en los discos básicos.

Los volúmenes simples pueden extenderse añadiendo porciones del mismo disco o de otros discos, pero no se puede reducir su tamaño una vez extendido ni eliminar porciones que se añadieron, sólo se podrá eliminar el volumen completo. Un volumen simple puede extenderse por otros discos hasta ocupar un máximo de 32 discos dinámicos.

9.2.4.2. Volumen distribuido

Se trata de un volumen formado por varias porciones de varios discos. Sólo pueden crearse en discos dinámicos y no soportan opciones de tolerancia a fallos.

Los volúmenes distribuidos se pueden extender añadiendo porciones del mismo disco. Al extender un volumen distribuido, ocurrirá igual que en los simples, que no se podrá desasignar espacio. Se corresponden con los conjuntos de volúmenes de Windows NT.

9.2.4.3. Volumen seccionado

Volumen que esta formado por un conjunto de porciones o bandas de igual tamaño (64 Kbytes) de varios discos, hasta un máximo de 32 discos. La información se reparte entre las bandas de los distintos discos. El reparto de información es equitativo y alternativo, ocupando de este modo todas las bandas o porciones de los discos integrantes. Como resultado, el rendimiento de E/S es mas alto.

Los discos no tienen por qué ser del mismo tamaño, pues lo que es igual son las bandas que se crean en los discos. Además, no pueden variar de tamaño una vez creados.

Estos volúmenes sólo pueden crearse en discos dinámicos y no ofrecen tolerancia a errores si no todo lo contrario. Si uno de los discos, o una banda, tuviese errores, el volumen completo falla y la información se pierde. Se corresponde con lo que en Windows NT se conocía como conjunto de bandas (RAID 0). La fiabilidad de este sistema es siempre menor que la fiabilidad del disco menos fiable.

Los volúmenes seccionados son el sistema de almacenamiento que ofrece el mejor rendimiento de todos los tipos de volúmenes de Windows 2003, tanto en escritu-

9.2.4. Creación de volúmenes

ra como lectura, por lo que se puede escoger por su rendimiento.

9.2.4.4. Volumen reflejado

Volúmen tolerante a fallos que utiliza un segundo espacio de almacenamiento físico de igual tamaño donde duplica toda la información del volumen. Aunque el tamaño utilizado en los dos discos es el mismo, los discos no tienen porqué tener el mismo tamaño físico, ni en número de cilindros, etc...

Las dos copias siempre deben encontrarse en dos discos distintos, y preferentemente en controladoras de disco distintas, a este mecanismo se le denomina duplicación. Si uno de los discos fallase, el sistema se repondrá utilizando la copia. Esto es recomendable, por ejemplo, para el volumen del sistema. Además, desde el disco de reparación de emergencia, se puede arrancar de una copia en espejo. Como inconveniente, el espacio útil de disco se reduce en un 50%.

Sólo pueden crearse en discos dinámicos. Se corresponde con lo que en Windows NT era el conjunto de espejos (RAID-1). Son más lentos a la hora de escribir, puesto que se han de realizar las escrituras por duplicado. Esto puede mitigarse con la duplexación.

Para reflejar el volúmen, es necesario que en el sistema exista al menos otro disco en modo dinámico, además del que queremos reflejar. En ese momento, pulsando con el botón derecho sobre el volúmen, el sistema ofrece la posibilidad de reflejarlo utilizando espacio no asignado de alguno de los discos.

Para eliminar un volumen reflejado tenemos dos opciones:

- Romper el espejo: Esta opción descompone el volumen reflejado dividiéndola en dos volúmenes independientes. Como resultado tenemos dos volúmenes idénticos en tamaño y con la misma información en ambos, pero ya no están reflejados.
- Quitar un espejo: Esta opción libera una de las dos copias integrantes del espejo, dejando el espacio que ocupaba tal copia como no asignado. La otra copia sigue funcionando, pero ahora no está reflejada.

9.2.4.5. Volumen RAID-5

Volúmen formado por bandas o porciones de tres o más discos duros, hasta 32 discos. En estos volúmenes, a los datos se les añade un información de paridad que servirá de código de detección y corrección de posibles errores. Los datos y la paridad se escribe de forma alterna entre el conjunto de bandas del volúmen.

La banda de paridad se calcula utilizando una función OREX del resto de bandas de datos.

Los volúmenes de RAID5 son tolerantes a fallos. Si un disco o una banda contiene errores, Windows 2003 puede reconstruir la información perdida a partir de los datos que quedan en las otras bandas junto con la paridad. El sistema puede por tanto soportar la pérdida de un disco sin pérdida de datos, ya que el volumen continua en línea.. No obstante, a partir del momento de la recuperación, el sistema es propenso a fallos hasta que se cambia el disco averiado o se rompe el RAID. En una operación de lectura, solo se lee la banda donde se encuentran los datos. Solo es necesario leer una banda para saber si existe o no error. Si el sistema detecta un error en la banda que ha leído o un error en el disco, leerá el resto de bandas de datos y la banda de paridad, con lo que podrá reconstruir la banda dañada. Si el error se produce en la banda de la paridad no es necesaria la reconstrucción.

No toda la capacidad de un volumen RAID5 está disponible para guardar datos, puesto que siempre una de las bandas se destina a guardar los datos de paridad. El tamaño disponible dependerá del número de discos que componen el RAID5, como siempre se destina una banda a la paridad, al incrementar el número de discos del RAID5 aumenta el espacio de almacenamiento útil disponible. En la figura se puede observar una configuración RAID5 con 3 discos. En cada disco, se utilizan porciones del mismo tamaño (20 Mbytes) . El tamaño total del volumen es de 40 Mbytes, y no 60 Mbytes, pues una de las bandas se destina a paridad.

Si el volumen estuviese formado por 4 discos y también con 20Mbytes por banda, el tamaño de disco disponible hubiese aumentado hasta 60Mbytes, pues se seguirán ocupando 20Mbytes para la paridad. Los volúmenes RAID5 sólo pueden crearse en discos dinámicos y no pueden reflejarse ni extenderse. Además, no se puede instalar el sistema en un volumen RAID5.

Los volúmenes RAID5 consumen mas memoria del sistema. Su uso es para información importante que en la medida de lo posible no sea muy cambiante, pues el rendimiento en escrituras es peor.

9.3. Utilidades

9.3.1. Diskpart

Diskpart es una utilidad que proporciona Microsoft para realizar la gestión de discos desde la línea de comandos. Soporta, mediante comandos o mediante el paso de un script de comandos, operaciones sobre los discos del sistema.

```
diskpart [ /s script ]
```

9.3.1. Diskpart

Los comandos de diskpart funcionan sobre: un disco, una partición,un volúmen

Los comandos emitidos se realizan sobre el foco , que es un objeto de uno de los tipos anteriores seleccionado mediante el comando Select. Por tanto, este es el primer comando que se debe utilizar para determinar donde se realizaran los comandos siguientes.

La sintaxis de Select es la siguiente:

```
Select [ volume | partition | disk ] [ = numero]
```

Todos los comandos requieren la selección del foco, a excepción de:

- List [disk | volume | partition] :Lista los discos, volúmenes y particiones.
- Help: Visualiza la ayuda de la herramienta.
- Rem: Introducir comentarios en los scripts de diskpart.
- Exit: Salir de la consola.
- Rescan: Fuerza a volver a buscar discos en el sistema.

El resto de comandos que admite diskpart es siempre sobre el foco, de entre ellos podemos destacar:

- Active: Hacer activa la partición foco.
- Assign [letter=letra | mount=ruta] [noerr]: Asignarle un punto de montaje.
- Remove [letter=letra | mount=ruta | all] [noerr]: Eliminarle un punto de montaje.
- Create: Crear una partición en el disco foco.
- Delete: Eliminar la partición foco.
- Extend [size=n] [noerr]: Extender el volumen foco.
- Add: Agregar un espejo al volumen simple foco.
- Break: Dividir o Romper el espejo del volumen foco.
- Convert: Para pasar de modo dinámico a básico.

Los códigos de error que puede dar diskpart son:

- 0: "Sin errores. Toda la secuencia de comandos se ejecutó sin errores."
- 1: "Excepción fatal. Puede haber un problema grave."
- 2: "Argumentos incorrectos especificados en una línea de comandos de Diskpart."
- 3: "DiskPart no pudo abrir la secuencia de comandos o el archivo de salida especificados."
- 4: "Uno de los servicios que utiliza DiskPart ha devuelto un error."
- 5: "Error en la sintaxis de un comando. Error en la secuencia de comandos porque un objeto se seleccionó incorrectamente o su uso no era válido en dicho comando."

9.4. Sistemas de ficheros

Cuando apareció Windows NT 3.1 en 1993, Microsoft utilizó las capacidades avanzadas del sistema de ficheros HPFS (High Performance File System) previamente utilizado en Microsoft/IBM OS/2, para crear el sistema de ficheros NTFS. La parte principal del modelo de seguridad que ofrece W2003 está basada en NTFS. Aunque los recursos compartidos se pueden configurar en W2003 sin tener en cuenta el sistema de ficheros subyacente, solo con NTFS se pueden asignar permisos a ficheros individuales.

Aunque W2003 soporta varios sistemas de ficheros (FAT,FAT16,FAT32,NTFS), NTFS es el sistema preferido ya que permite utilizar todas las características de seguridad avanzadas.

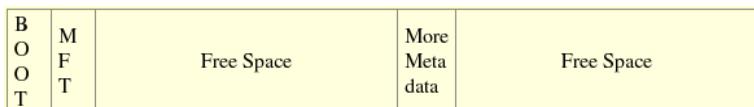
Aviso

W2003 no utiliza NTFS para formatear un floppy disk, debido a la cantidad de información necesaria para crear el sistema de ficheros y que excedería la capacidad de un disquete

Un volumen NTFS almacena la información sobre descriptores de ficheros en una tabla de ficheros maestra (MFT), la cual es asu vez un fichero. A parte de varios registros que contienen información sobre la propia MFT, esta contiene un registro por cada fichero y directorio del sistema La MFT también contiene un fichero de log. Se mantiene en el propio sistema de ficheros una copia de la MFT. Enlaces a la MFT

9.5. Cuotas de disco

y su copia están almacenados en el sector de inicio del disco. Una copia del sector de inicio se almacena en el centro del disco. Al mantener tanta información replicada, la recuperación de los datos de un sistema de ficheros NTFS es mucho más fácil. La estructura de un sistema NTFS se puede apreciar en la siguiente imagen:

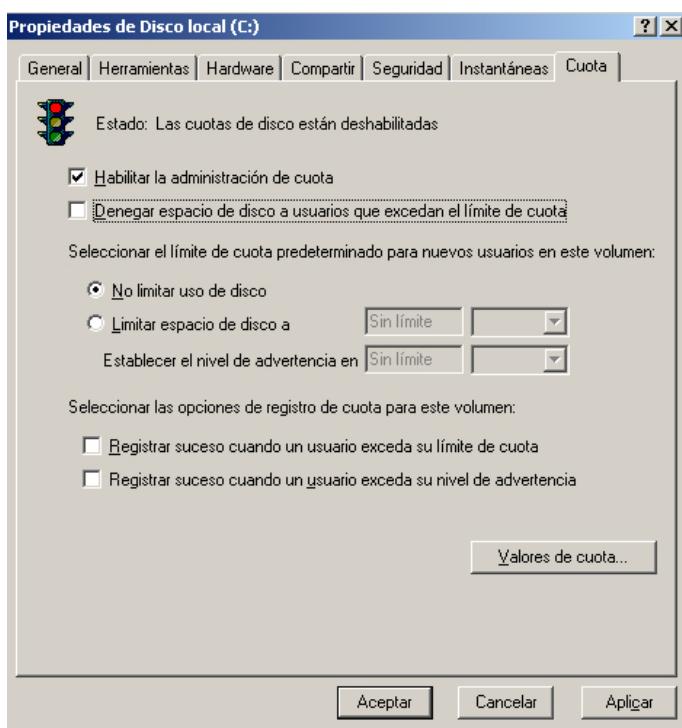


9.5. Cuotas de disco

Cuando se trabaja con cuotas de disco, se puede empezar definiendo una cuota por defecto para cada volumen y luego ir ajustando individualmente las cuotas de usuario según se necesiten. Definiendo una pequeña cuota por defecto y luego ajustándola según las necesidades es la forma más eficiente de abordar el problema de las cuotas.

9.5.1. Habilitar cuotas

Para empezar a trabajar con cuotas de disco en Windows Server 2003 hay que habilitar el soporte de cuotas sobre un volumen. Si presionamos el botón derecho del ratón sobre el volumen y accedemos a Propiedades, la pestaña Cuotas nos permitirá definir todas las opciones posibles.



9.5.2. Definición de cuotas individuales

Seleccionaremos **Denegar espacio de disco a usuarios ...** si queremos prevenir que el usuario pueda escribir en el disco cuando alcance su cuota. En caso contrario, los usuarios serán advertidos de que llegan al límite de la cuota.

El administrador puede definir dos valores para las cuotas:

1. **Limitar espacio de disco a:**

Define la cantidad de espacio en disco que un usuario tiene permitido utilizar.

2. **Establecer el nivel de advertencia en:**

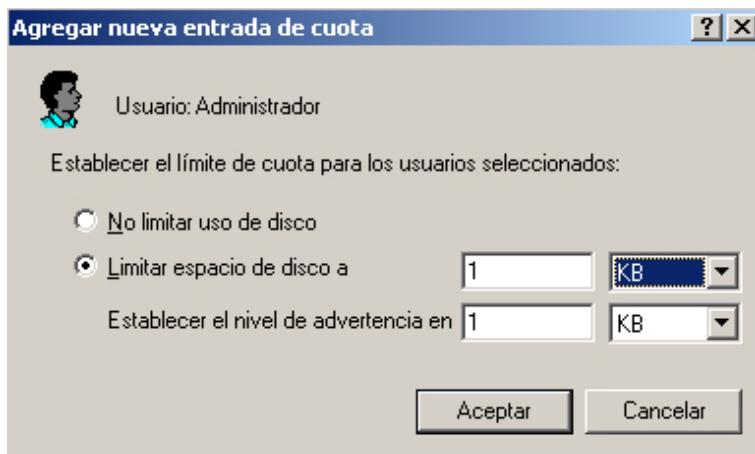
Cuando se alcance este límite, el sistema avisará al usuario de que está cerca de alcanzar la cuota de disco asignada.

Estas dos opciones permiten introducir un número y la unidad de medida asociada a las cuotas. Estas unidades de medida que se muestran en el desplegable, se generan dinámicamente según la capacidad del volúmen.

En esta misma pestaña, tenemos la posibilidad de registrar eventos de cuotas, bien cuando se alcanza la cuota o cuando se produce la advertencia.

9.5.2. Definición de cuotas individuales

Tenemos la capacidad de definir cuotas por usuario, habilitandole para que exceda el límite por defecto definido para el volúmen. También podemos definir usuarios que no tengan ningún límite de cuotas.



9.6. Copias de seguridad

La herramienta de copia de seguridad que viene instalada en la familia de servidores Windows 2003 proporciona al administrador las utilidades necesarias para copiar todos los datos importantes del sistema o el sistema entero. Con esta nueva versión, el administrador puede respaldar su sistema en un fichero en otro disco, en un recurso de red y por supuesto en cinta. La herramienta es fácil de usar y configurable, proporcionando wizards que guiarán al administrador en la complicada tarea de respaldar el sistema.

Algunas de las características de ntbackup son más útiles bajo windows 2003 Server, ya que permite copiar partes del Directorio Activo, por ejemplo. O también es posible habilitar el Servicio de almacenamiento remoto que permite planificar las copias de seguridad de una pequeña red de area local. Entre las funciones básicas de ntbackup están:

- Creación del disco de reparación de emergencia
- Hacer copias del estado del sistema: registro, ficheros de arranque y bases de datos del Servicio de Certificados.

Como pasa con la mayoría de herramientas de Windows 2003, el usuario debe de tener los privilegios necesarios para usarla. Para poder copiar y restaurar cualquier fichero o carpeta del sistema local el usuario debe pertenecer al grupo Administradores o al grupo Operadores de Copia de Seguridad. Si no eres miembro de uno de estos grupos, deberás tener al menos los privilegios de **Back up files and directories** o **Restore files and directories**

9.6.1. Carpetas y ficheros

Para arrancar la aplicación, desde una consola MS-DOS, ejecuta ntbackup y sigue las siguientes instrucciones:

- Para hacer una copia de seguridad del sistema, elige Backup Wizard y sigue las instrucciones de la pantalla.
- Para restaurar el sistema tenemos otro wizard

El administrador a la hora de hacer backups, tendría que tener en cuenta que:

- Como miembro del grupo Administradores u Operadores de Copia, puedes co-

piar todos los ficheros y carpetas aunque solo tengas permiso de lectura sobre ellas. Cuando los restauras en el mismo sistema o en otro, ntbackup mantiene los permisos originales y por tanto solo serás capaz de leer aquellos ficheros sobre los que tengas permiso.

- Ntbackup copia también los ficheros encriptados. El programa los almacena encriptados en cinta oen el medio apropiado. Por tanto no se puede utilizar ntbac-kup para desencriptar los ficheros por perdida de la clave.

Ntbackup no copia todos los ficheros de cada carpeta; la utilidad mantiene en el registro una lista de ficheros y carpetas a excluir. Las siguientes claves del registro **FilesNotToBackup** y **FilesNotToRestore** localizadas en **HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore** es donde ntbackup almacena dicha información. Cada una contiene valores del tipo REG_MULTI_SZ cuyos contenidos indican un fichero o una carpeta a excluir. De forma similar ntbac-kup tiene definiciones similares de que claves del registro que no tiene que hacer respaldo. (**KeysNotToRestore**)

9.6.2. Estado del sistema

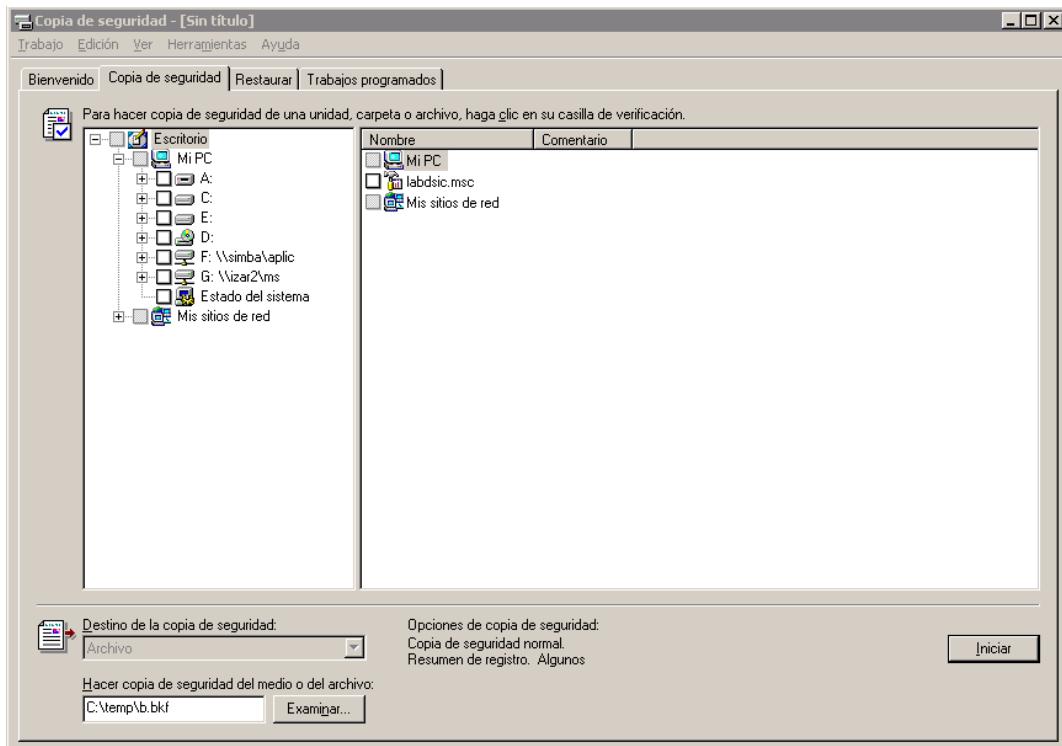
Windows Backup coloca el registro y otros datos del sistema juntos, denominando al conjunto **Datos del Estado del Sistema**. Estos datos incluyen el registro, la base de datos de clases COM+ y ficheros de arranque. El proceso de copia y restauración del *Estado del sistema* es tratado como una única operación. Sin embargo, se puede restaurar el estado del sistema en un sitio alternativo y luego copiar partes de el manualmente.

Here are the different ways to back up System State data: A continuación se presenta una lista de los diferentes procedimientos para copiar el estado del sistema:

- Para copiar el estado del sistema como parte de un backup normal, hay que seleccionar Estado del Sistema en la lengüeta de Copia de Seguridad.
- Para copiar una serie de ficheros, incluyendo el Estado del Sistema, hay que hacer click en *Hacer copia de seguridad de archivos, unidades o datos de red seleccionados* en el Wizard y después seleccionar Estado del Sistema en la lengüeta Copia de Seguridad.
- Para copiar todos los ficheros, incluyendo el Estado del Sistema, hacer click en *Hacer Copiar de Seguridad de todo el contenido de mi equipo*
- Para copiar solo el Estado del Sistema, haga click sobre *Hacer copia de seguridad sólo de los datos del sistema*

9.6.2. Estado del sistema

A continuación se muestra una imagen de la utilidad ntbackup:



10

El servicio DFS

Índice

10.1. Introducción	155
10.2. Tipos y características de DFS	156
10.3. Funcionamiento de DFS	157
10.3.1. Acceso a los recursos de un DFS	158
10.3.2. Replicación de DFS basado en dominio	160
10.3.3. Seguridad de DFS	160
10.4. Configuración de una raíz DFS	160
10.4.1. Configuración de una raíz DFS independiente	161
10.4.2. Configuración de una raíz DFS de dominio	161
10.5. Configuración de los vínculos DFS	162
10.6. Sistema de Replicación de Archivos (FRS)	163
10.6.1. Funcionamiento de FRS	163
10.6.2. Replicación de réplicas DFS	164

10.1. Introducción

El Sistema de archivos distribuidos o DFS (*Distributed File System*) es un componente de red del servidor que facilita la forma de encontrar y manejar datos en la red. DFS agrupa ficheros que están en diferentes ordenadores en un espacio de nombres único.

DFS facilita la construcción de una única vista jerárquica de múltiples servidores de archivos. En vez de ver una red física compuesta por decenas de servidores de ficheros, cada uno con una estructura de directorios separada, los usuarios verán unos pocos directorios lógicos que incluyen todos los servidores y carpetas compartidas. Cada carpeta compartida aparecerá en el lugar lógico que le corresponde en el directorio, sin importar en qué servidor se encuentra.

DFS es, para los servidores y las carpetas compartidas, lo que los sistemas de ficheros es para los discos duros. Los sistemas de ficheros proporcionan un acceso nominado uniforme al conjunto de sectores del disco; DFS proporciona una convención de nominación uniforme para los servidores, carpetas compartidas y ficheros. De esta forma, DFS hace posible organizar los servidores de archivos y sus recursos compartidos en una estructura jerárquica, haciendo más fácil para una gran organización administrar y usar sus recursos de información.

Históricamente, con la convención de nombres universal (*Universal Name Convention, UNC*), un usuario o aplicación debía de especificar el servidor y el recurso compartido, seguido de la ruta a partir del recurso hasta llegar al fichero, para poder acceder a dicho fichero. Es decir, un UNC tiene la forma siguiente:

```
\servidor\recurso_compartido\ruta\...\archivo
```

Aunque en general los nombres UNC se pueden utilizar directamente, la forma más habitual de acceder a ficheros compartidos por otros equipos es realizar como paso previo la asignación del recurso (carpeta) compartida a una letra de unidad local (que queda redireccionada a dicho recurso \\servidor\recurso_compartido). Posteriormente, el usuario se desplaza a partir de dicha unidad redireccionada a los datos a los que desea tener acceso. Por ejemplo:

```
net use x: \\servidor\carpeta_compartida  
copy x:\ruta\....\archivo directorio
```

Mientras las redes continúan creciendo en tamaño y las organizaciones empiezan a usar el almacenamiento del que disponen, tanto interna como externamente, para

tales fines como son las intranets, la asignación de una única letra de unidad a medios de red compartidos resulta eficaz. Además, a pesar de poder usar directamente nombres UNC, los usuarios pueden verse desbordados por el número creciente de lugares de donde deben obtener datos.

DFS soluciona estos problemas vinculando servidores de archivos y recursos compartidos a un espacio de nombres sencillo y descriptivo. Dado que DFS asigna el almacenamiento físico como una representación lógica, la ventaja es que la ubicación física de los datos se hace transparente para los usuarios y las aplicaciones.

10.2. Tipos y características de DFS

Como hemos visto, en un entorno de red, los usuarios pueden tener dificultades para mantenerse al corriente de las ubicaciones físicas de los recursos compartidos. Cuando se utiliza DFS, sin embargo, las estructuras de la red y del sistema de archivos se hacen transparentes para los usuarios. Esto permite al administrador centralizar y optimizar el acceso a los recursos en función de una estructura con un único árbol. DFS proporciona una estructura de árbol lógico para los recursos del sistema de archivos que pueden estar en cualquier lugar de la red. Como el árbol de DFS es un punto de referencia único, los usuarios pueden tener acceso fácilmente a los recursos de la red cualquiera que sea su ubicación real. DFS también permite a los administradores administrar varias carpetas compartidas desde una única ubicación.

Se pueden configurar dos tipos de DFS:

- A. **DFS independiente.** Almacena la topología de DFS en el registro del equipo local donde se crea. Este tipo de DFS no proporciona tolerancia a errores si se produce un error en el equipo donde se almacenan las carpetas compartidas o la topología DFS, puesto que se almacena en una sola máquina. Cada equipo puede alojar solo un árbol DFS como máximo.
- B. **DFS de dominio.** Almacena la topología de DFS en Active Directory. Este tipo de DFS señala a varias carpetas compartidas idénticas, lo que proporciona tolerancia a errores. Además, admite el Sistema de nombres de dominio, varios niveles y la replicación de archivos.

Como conclusión, podemos decir que para compartir los recursos de archivo en toda la red, DFS:

- **Organiza los recursos en una estructura de árbol.** Un recurso compartido de DFS utiliza una estructura de árbol que contiene un nodo raíz y vínculos. Para

crear un recurso compartido DFS, primero debe crear una raíz DFS. Cada raíz DFS puede tener varios vínculos por debajo, cada uno de los cuales señala a una carpeta compartida. Los vínculos de la raíz DFS representan carpetas compartidas que pueden encontrarse físicamente en diferentes servidores.

- **Facilita la exploración de la red.** Un usuario que recorre un árbol administrado por DFS no necesita conocer el nombre del servidor donde está compartida la carpeta. Esto simplifica el acceso a la red, ya que los usuarios no necesitan encontrar el servidor donde se encuentra un determinado recurso de red. Tras conectar con la raíz DFS, los usuarios podrán buscar y tener acceso a todos los recursos situados por debajo de la raíz, con independencia de la ubicación o el nombre del servidor.
- **Facilita la administración de la red.** DFS de dominio también simplifica la administración de la red. Si se produce un error en un servidor, un administrador puede mover un vínculo de un servidor a otro sin que los usuarios se den cuenta del cambio. Para mover un vínculo basta con modificar la carpeta DFS para que haga referencia a la ubicación de las carpetas compartidas en el nuevo servidor. Los usuarios siguen utilizando la misma ruta DFS que señala el vínculo.
- **Conserva los permisos de red.** Un usuario puede tener acceso a una carpeta compartida a través de DFS, siempre y cuando tenga el permiso necesario de acceso a la carpeta compartida.

Sólo los equipos cliente con software de cliente DFS pueden tener acceso a los recursos de DFS. Los equipos que corren bajo Windows 98, Windows NT 4.0 o Windows 2003 incluyen software de cliente DFS. Debe descargar e instalar este software en los equipos que ejecuten Microsoft Windows 95.

10.3. Funcionamiento de DFS

Un recurso compartido de DFS utiliza una estructura de árbol. Para crear un recurso compartido DFS, primero debe crear una raíz DFS. La raíz en sí es un recurso compartido que se encuentra en lo mas alto del árbol DFS y que sirve de punto de inicio para alojar:

- **Carpetas compartidas.**
- **Vínculos a recursos compartido**, que se trata de una referencia a una carpeta compartida SMB, NetWare, NFS , NCP u otra raíz DFS. Se componen de una etiqueta, que es el nombre visible en el árbol DFS y la referencia al recurso de red vinculado.

10.3.1. Acceso a los recursos de un DFS

Dentro de un árbol DFS, el administrador organiza los recursos compartidos, vínculos a recursos compartidos en los distintos servidores y vínculos en otros árboles DFS. Por tanto, podemos crear estructuras más complejas que nos permitirá organizar todos nuestros recursos en un único espacio de nombres uniforme, independizando la forma de acceder a los recursos de la forma en que hemos distribuido éstos entre los servidores.

Toda la información de recursos definida a partir de la raíz de un sistema DFS comparten el espacio de nombres DFS, que es lo que verán los usuarios. Este espacio de nombres tiene una limitación en el tamaño de ruta hacia cualquier archivo en 260 caracteres y otra en el número máximo de carpetas compartidas y vínculos DFS que se pueden crear por raíz, que es de 1000.

Cuando el árbol DFS es de dominio, puede tener varias réplicas de la raíz, aunque en un servidor sólo puede haber una réplica de la misma raíz. Windows 2003 acepta hasta 256 miembros de una replica del árbol DFS. El conjunto de raíces del árbol DFS contienen la misma información, pero dotan al sistema de tolerancia a fallos y de reparto de carga equilibrado entre los servidores integrantes. Toda la información de la topología se almacena en el directorio y los mecanismos de replicación de éste se encargan de mantener replicada la topología en todos los servidores raíz de DFS.

Los cambios en la topología son visibles en el momento de aplicar sin necesidad de detener el servicio.

10.3.1. Acceso a los recursos de un DFS

El acceso a una archivo o carpeta dentro del espacio de nombres de DFS se realiza del mismo modo que a un recurso UNC. Por tanto, los clientes NT 4.0 y Windows 9x pueden acceder a él de la forma:

```
\servidor\recurso
```

siendo **recurso** el nombre del recurso compartido raíz del árbol DFS y **servidor** el nombre del ordenador que ofrece tal recurso.

Desde clientes Windows 2003 o Windows anteriores actualizados con el software de acceso a DFS, se puede también acceder a los árboles DFS de dominio mediante el UNC:

```
\nombre_delDominio\raiz_DFS
```

De este modo, el usuario no necesita recordar los nombres de los servidores don-

10.3.1. Acceso a los recursos de un DFS

de están alojados realmente los recursos compartidos. Si creamos una raíz DFS de dominio, el usuario podrá localizar los recursos simplemente con el nombre del dominio y un nombre significativo a la raíz DFS.

Además, desde Windows 2003 y NT 4.0, se puede utilizar:

- **net use "profundo"**, que consiste en poder asignar letra de unidad a una ruta dentro del espacio de nombres del árbol DFS.
- **Vínculos a volúmenes** NetWare, NFS o NCP. Desde el resto de clientes, estos vínculos aparecen como carpetas vacías.

Internamente, cuando el usuario necesita acceso a los recursos del DFS, el cliente DFS hace una consulta a los servidores para obtener una estructura de datos que almacena la topología del DFS y que se denomina PKT (*Partition Knowledge Table*). Esta tabla almacena información sobre los recursos del DFS del tipo:

- Ruta DFS de recurso. Por ejemplo, el siguiente:

```
\upv.es\raiz_dfs\ms\aplicaciones
```

- UNC o UNC's del recurso. Como, por ejemplo:

```
\izar2\aplicaciones e \izar3\aplicaciones
```

- Sistema operativo de la máquina servidora.
- Tiempo de vida de la entrada PKT.

Con esta información y la dirección IP del cliente, el software cliente DFS de Windows 2003 escogerá el recurso al cual debe conectarse para dar acceso al usuario. Windows 2003 garantiza que se realiza equilibrio de la carga si un recurso se encuentra replicado en varios servidores y que el acceso se realizará sobre la réplica más accesible, desde el punto de vista de la configuración de sitios del directorio.

Para acelerar el acceso, los clientes almacenan en caché las partes de la PKT a medida que el usuario va recorriendo la estructura del espacio DFS. Por este motivo, se introduce un campo de validez de la PKT.

10.3.2. Replicación de DFS basado en dominio

La replicación de DFS consta de dos partes:

- a. **Replicación de la topología DFS.** La información de la topología se encuentra en el directorio activo y por tanto esta sujeta a la replicación de éste. Esto implica que durante un tiempo, diferentes controladores pueden ver una topología distinta hasta que los cambios realizados en algún controlador leguen a replicarse en él.

El tiempo de replicación puede ser considerable debido a que cada vínculo ocupa alrededor de 400 bytes en la PKT. Dependiendo del árbol en concreto, esto puede traducirse en varias decenas de kilo-bytes a replicar.

- b. **Replicación del contenido DFS.** Pueden configurarse múltiples copias de una carpeta compartida con, o sin, replicación de contenido. Se puede encargar al servicio de replicación de archivos, en adelante FRS (*File Replication Service*) la sincronización de las copias o bien realizar copias manuales. Si el recurso no se actualiza a menudo puede considerarse realizar a mano la sincronización.

10.3.3. Seguridad de DFS

Al espacio de nombres de DFS no se pueden aplicar ACLs. Cuando un usuario accede a un vínculo en concreto del DFS, se aplicarán las ACLs definidas para ese recurso en el servidor. Cuando un usuario intenta acceder a una carpeta intermedia donde no tenga permisos, ésta aparecerá vacía para él. Esto implica que el resto de la jerarquía no será visible aunque en niveles inferiores si tuviese permisos.

Si se realiza a mano la sincronización de réplicas de los vínculos, se ha de asegurar que el almacenamiento destino tenga los mismos permisos. Si la replicación es por FRS, las ACLs también se copian en las réplicas.

Por lo que respecta a la administración, el administrador del dominio puede administrar la topología del DFS, pero la administración de las ACLs de los recursos a los que se vincula queda condicionada a los permisos de administración que pueda tener en dichos recursos.

10.4. Configuración de una raíz DFS

El primer paso para configurar un recurso compartido de DFS es crear una raíz DFS. Las raíces DFS se pueden crear sobre particiones FAT o NTFS. Como siempre, hay

10.4.1. Configuración de una raíz DFS independiente

que tener en cuenta que el sistema de archivos FAT no ofrece las ventajas de seguridad (permisos) del sistema NTFS.

Cuando se crea una raíz DFS, se tiene la opción de establecer una raíz independiente o una raíz de dominio. A continuación se explican ambas.

10.4.1. Configuración de una raíz DFS independiente

Una raíz independiente se encuentra físicamente en el servidor al que los usuarios se conectan inicialmente. Para crear una raíz DFS independiente, en Herramientas administrativas abra la consola del Sistema de archivos distribuido e inicie el Asistente para crear nueva raíz DFS. Las opciones del asistente son las siguientes:

- Seleccionar el tipo de raíz DFS: en este caso, independiente.
- Especificar el servidor huésped para la raíz DFS: el punto de conexión inicial, o el servidor *host*, para todos los recursos contenidos en el árbol DFS. Se puede crear una raíz DFS en cualquier equipo que corra bajo Windows 2003 Server.
- Especificar el recurso compartido de raíz DFS: una carpeta compartida para albergar la raíz DFS.
- Nombre de la raíz DFS: un nombre descriptivo para la raíz DFS.

10.4.2. Configuración de una raíz DFS de dominio

Una raíz DFS de dominio debe estar alojada en un servidor miembro del dominio. Active Directory almacena la topología de cada árbol DFS y replica la topología en todos los servidores raíz DFS participantes. Como los cambios realizados en un árbol DFS se sincronizan automáticamente con Active Directory, siempre puede restaurar la topología de un árbol DFS si la raíz DFS está fuera de conexión por cualquier motivo.

Se puede implementar la tolerancia a fallos los archivos contenidos en el árbol DFS mediante la asignación de réplicas a un vínculo DFS. Un conjunto de recursos replicados puede atender a cualquier nodo del árbol DFS. Si por cualquier motivo se produce un error en la conexión de un cliente a una réplica, el cliente DFS intentará automáticamente conectarse a otra réplica. El cliente DFS recorre todas las réplicas hasta que encuentra una disponible.

Para crear una raíz DFS de dominio, utilice la consola del Sistema de archivos distribuido y desde ahí, inicie el Asistente para crear nueva raíz DFS. A continua-

ción se describen las opciones que se pueden configurar:

- Selección del tipo de raíz DFS: en este caso, raíz DFS de dominio.
- Selección del dominio huésped para la raíz DFS: el dominio *host* del árbol DFS. Un dominio puede alojar varias raíces DFS.
- Especificar el servidor huésped para la raíz DFS: el punto de conexión inicial, o el servidor *host*, para todos los recursos contenidos en el árbol DFS.
- Especificar el recurso compartido de raíz DFS: una carpeta compartida para albergar la raíz DFS. Puede elegirse una carpeta compartida existente o crearse una nueva.
- Nombre de la raíz DFS: un nombre descriptivo para la raíz DFS.

Para crear una segunda raíz DFS de dominio, hay que abrir la consola del Sistema de archivos distribuidos, hacer clic con el botón secundario del ratón en el dominio y después hacer clic en "Nuevo miembro duplicado de raíz". Las únicas opciones que hay para crear una segunda raíz son "Especifique el servidor para albergar DFS" y "Seleccione el recurso compartido para el volumen de la raíz DFS".

10.5. Configuración de los vínculos DFS

Se pueden agregar recursos compartidos DFS en la raíz o en cualquier otro nodo de rama del árbol. Si el recurso en cuestión no es de Windows 2003, el recurso compartido se agregará como una hoja, que no puede tener un vínculo por debajo de ella.

Una vez que haya creado una raíz DFS, puede crear vínculos DFS que señalen a las carpetas compartidas. Para crear un vínculo DFS, deben seguirse los pasos citados a continuación:

1. En la consola Sistema de archivos distribuido, hacer clic en la raíz DFS a la que agregará un vínculo.
2. En el menú Acción, hacer clic en Nuevo vínculo DFS.
3. En el cuadro de diálogo Crear un nuevo vínculo DFS, se pueden configurar las opciones:
 - Nombre de vínculo: el nombre que los usuarios verán cuando se conecten a DFS.

- Enviar el usuario a esta carpeta compartida: el nombre UNC de la ubicación real de la carpeta compartida a la que se refiere el vínculo.
- Comentario.
- Los clientes mantienen en caché esta referencia durante x segundos: es el intervalo de tiempo durante el que los clientes mantendrán en caché una referencia a un vínculo DFS. Una vez caducada la referencia, el cliente tienen que volver a consultar al servidor DFS para conocer la ubicación del vínculo.

Una vez creado el vínculo, este aparecerá bajo el volumen de la raíz DFS en la consola del Sistema de archivos distribuidos.

10.6. Sistema de Replicación de Archivos (FRS)

File Replication System, o FRS, es el sistema de replicación multamaestro de archivos y carpetas entre máquinas Windows 2003. El contenido de recursos NTFS puede así mantenerse redundante en múltiples servidores Windows 2003 de forma automática. Entre las distintas réplicas del recurso, no existen relaciones maestro-esclavo, sino que cuando una archivo se modifica y se cierra en una réplica, los cambios se actualizan en el resto.

El sistema dispone un calendario configurable para marcar el momento de replicar la información de una carpeta ubicada en varias máquinas, permitiendo la copia del archivo, su información, atributos y ACLs.

10.6.1. Funcionamiento de FRS

FRS se instala automáticamente en todos los servidores de Windows 2003. En los DC de dominio, se inicia de forma automática y en los servidores independientes (miembro) se configura con arranque manual.

Cada archivo configurado para replicar tiene asociado:

- Número de secuencia de actualización (*Update Sequence Number, USN*). Cada vez que se modifica un archivo y se cierra, este número se incrementa en una unidad y se notifica del cambio al resto de miembros de la réplica.
- Fecha de suceso: denota cuando se cerró el archivo o cuando se replicó por última vez.

10.6.2. Replicación de réplicas DFS

Cada miembro de una réplica decide si actualizar o no el archivo en su réplica en función del momento de actualización y del USN del archivo. Si la réplica local tiene una fecha de suceso 30 minutos más antigua que la del archivo notificado, la réplica local se actualiza. Si la diferencia es menor de 30 minutos, se atenderá al numero de secuencia para saber cual de las dos copias es mas reciente. Si la copia local es mas reciente no se actualizará.

Este mecanismo se basa en la filosofía de que el último que escribe gana.

10.6.2. Replicación de réplicas DFS

La replicación de réplicas DFS permite mantener sincronizado el conjunto de réplicas de una raíz o de un vínculo del DFS de dominio. La replicación no es posible en un DFS independiente.

Desde la consola de administración del DFS, se puede configurar la replicación de la información entre las réplicas DFS.

Aunque la réplica es multimaestro, la primera vez FRS asigna al primer servidor de la réplica el papel de maestro inicial, de modo que toda la información de la carpeta se replicará de este hacia el resto de servidores miembros de la réplica. Después de esta réplica inicial, los cambios en cualquier réplica se actualizan en el resto.

Para poder configurar la replicación FRS de una carpeta es necesario que:

- el sistema de archivos sea NTFS 5.0.
- todas las replicas de DFS tengan instalado RFS.
- los servidores estén en el mismo dominio o en dominios en los que se tenga permisos.

11

Recuperación ante desastres

Índice

11.1. El proceso de arranque de Windows 2003	167
11.1.1. La secuencia de arranque	167
11.1.2. La carga del sistema operativo	167
11.2. Solución de problemas en el proceso de arranque	168
11.2.1. Reparación de una instalación con los discos de arranque de Windows 2003	168
11.2.2. Menú de opciones avanzado	169
11.2.3. Creación de un disco de arranque	171
11.2.4. La consola de recuperación	172
11.3. Linux al rescate	175
11.4. Service Packs. Windows Updates	177

11.1. El proceso de arranque de Windows 2003

Si se llega a conocer bien las fases del proceso de arranque es posible que muchos de los problemas que se presentan por un fallo en el arranque puedan ser solucionados en menos tiempo. El proceso de arranque de un sistema operativo es algo complejo en el que intervienen múltiples factores.

Lo primero que sucede tras encender el ordenador es el autochequeo del mismo. Las comprobaciones que se realizan pretenden detectar problemas con los dispositivos hardware conectados. De esta forma, se realiza una comprobación de la memoria, de los dispositivos de entrada y salida como ratón o teclado; comprobación de las unidades de disco, comprobación de unidades SCSI si existen, provocando además el arranque de la BIOS de estos dispositivos. Cualquier error o problema que surja durante este proceso se debe a un fallo del hardware instalado o a un fallo de configuración de la CMOS.

11.1.1. La secuencia de arranque

Después del autochequeo, el sistema debe localizar el dispositivo de arranque y cargar el sector de arranque maestro o Master Boot Record (MBR) en memoria. En el MBR se almacena el programa encargado de arrancar el sistema con un sistema operativo u otro. Por tanto, tras realizar la carga del MBR en memoria, se ejecuta el programa almacenado en el mismo.

El programa del MBR busca la partición de arranque o Partition Boot Record (PBR) para localizar la partición activa. Tras localizarla, el sector de arranque de dicha partición es cargado en memoria. En este sector de arranque se indica el programa encargado de realizar la carga del sistema operativo, que en el caso de Windows 2003 Server es el fichero Ntldr.exe, el cual debe encontrarse en el directorio raíz de la partición de arranque de Windows 2003.

El proceso de instalación de Windows 2003 Server se encarga de configurar el sector de arranque, así como de colocar el fichero Ntldr.exe en lugar apropiado. Este fichero posee los atributos de Oculto y Sistema. Por tanto, parece importante mantener una copia de este fichero y será necesario incluirlo en el disquete de arranque de Windows 2003.

11.1.2. La carga del sistema operativo

Después de los pasos anteriores comienza la carga del sistema operativo propiamente dicho. La secuencia de arranque se encarga ahora de obtener información sobre el hardware del sistema, así como los manejadores (drivers) asociados a los dispositi-

vos.

El programa Ntldr.exe cambia el procesador del modo real al modo de 32 bits, ya que Ntldr es una aplicación de 32 bits. La primera tarea que realiza el programa Ntldr consiste en cargar el minicontrolador del sistema de archivos. Este paso es necesario para la localización y la carga de Windows 2003. A continuación lee el fichero Boot.ini, mostrando los diferentes sistemas operativos con los que se puede arrancar. Si el sistema operativo elegido es distinto de 2003, Ntldr carga y ejecuta Bootsec.dos, parándose el proceso de arranque de Windows 2003. Si el sistema operativo seleccionado es 2003, el programa Ntldr ejecuta Ntdetect.exe, encargado de buscar el hardware del equipo, devolviendo una lista con el hardware encontrado a Ntldr para que sea incluido en el registro.

Por último Ntldr carga Ntoskrnl.exe, Hal.dll y la clave "System" del Registro que permite a Ntldr cargar los manejadores configurados para ser iniciados en el proceso de arranque. Tras ello, Ntldr cede el control a Ntoskrnl.exe terminando el proceso de arranque para comenzar la carga del sistema operativo.

11.2. Solución de problemas en el proceso de arranque

Como hemos visto, son muchos los elementos que intervienen en el proceso de arranque de Windows 2003, elevando así las posibilidades de fallos durante este proceso.

Windows 2003 incorpora diversos medios para corregir los posibles errores en el proceso de arranque. Entre las soluciones a estos problemas vamos a destacar tres:

1. Reparación de una instalación con los discos de instalación de Windows 2003.
2. El menu de opciones avanzado.
3. Creación de un disquete de arranque.

11.2.1. Reparación de una instalación con los discos de arranque de Windows 2003

Si el error se produce debido a un fallo o un error en alguno de los ficheros de Windows 2003, es posible recuperarlo utilizando los discos de instalación de Windows 2003.

Se introduce el primero de los disquetes iniciando el proceso de instalación de Windows 2003. Durante dicho proceso aparece un menú preguntando si se desea

11.2.2. Menú de opciones avanzado

instalar 2003 o reparar una instalación existente. Al elegir esta opción, aparece un nuevo menú preguntando si deseamos reparar los ficheros de 2003 o la base de datos de usuario. Será necesario introducir el Cd-rom de 2003 y el programa de instalación se encargará de revisar los ficheros de la instalación de 2003 y reparar aquellos que se hayan modificado.

11.2.2. Menú de opciones avanzado

Siempre es conveniente conocer el nuevo menú avanzado que posee Windows Server 2003 a la hora de resolver problemas en el arranque. A este menú se llega apretando F8 y presenta las siguientes opciones al administrador:

- Modo Seguro.
- Modo Seguro con funciones de Red.
- Modo Seguro con simbolo de sistema.
- Habilitar el registro de inicio.
- Habilitar modo VGA.
- Ultima Configuración buena Conocida.
- Modo de Restauración de SD.
- Modo de Depuración
- Iniciar Windows Normalmente.
- Reiniciar.
- Regresar al menú de opciones del SO.

11.2.2.1. Modo seguro

Lo mejor del Modo Seguro es que te permite acceder a todos los discos sin tener en cuenta el sistema de ficheros que posea. Si este arranque funciona, el administrador puede realizar cambios en la configuración para corregir el problema. Por ejemplo, es habitual utilizar este modo para desinstalar un nuevo driver que no funcionó adecuadamente. Las siguientes opciones están disponibles en este modo:

11.2.2. Menú de opciones avanzado

1. Modo Seguro:

Carga solamente los ficheros y drivers necesarios para levantar y ejecutar el sistema operativo: ratón, monitor, teclado, almacenamiento, video, y servicios del sistema por defecto.

2. Modo Seguro con Red:

Añade soporte de Red, pero no funciona con tarjetas PCMCIA.

3. Modo Seguro con símbolo del sistema:

Levanta el sistema en modo texto (consola). Utilizaremos esta opción si tenemos problemas con explorer.exe (la shell gráfica de Windows). Se pueden realizar todo tipo de tareas en modo comando, incluso abrir aplicaciones gráficas si se conoce el comando.

11.2.2.2. Habilitar el registro de inicio

Esta opción le dice al sistema operativo Windows Server 2003 que cree un fichero de registro (%SystemRoot%\Ntbtlog.txt). El fichero muestra una lista de todos los drivers que se cargan y los que no.

11.2.2.3. Habilitar modo VGA

Esta opción inicia Windows Server 2003 utilizando el driver básico de VGA. Esta opción es útil después de haber instalado un nuevo driver de video para la tarjeta gráfica y este no funcionó como esperábamos. El driver de video VGA es el mismo que se utiliza cuando arrancamos Windows Server 2003 con cualquiera de los *Modos Seguros*.

11.2.2.4. Última configuración buena conocida

Se trata de una copia en el registro que contiene la información de la última configuración buena conocida, con la cual el sistema arrancó sin problemas.

En la clave HKEY_LOCAL_MACHINE\SYSTEM del Registro de Windows 2003 aparecen distintos conjuntos de configuraciones denominados ControlSet. El primero se denomina CurrentControlSet que contiene la configuración actual del sistema. Existen otros conjuntos con un número de orden ControlSet001, ControlSet002, etc., los cuales representan distintas configuraciones almacenadas.

Cuando el sistema arranca utiliza una configuración por defecto que es copiada a

11.2.3. Creación de un disco de arranque

la clave CurrentControlSet. Además si el proceso de inicio de sesión (Logon) ha ido bien, la configuración actual (CurrentControlSet) se copia de forma automática a la clave que contiene la última configuración buena conocida.

La forma de saber cuál es la clave por defecto y cuál es la última buena conocida es mediante los valores almacenados en la clave Select que se encuentra al mismo nivel de las claves de conjuntos de configuraciones. Dentro de esta clave aparecen los valores Current para la configuración actual, Default para la configuración por defecto, Failed que indica el número de clave que contiene una configuración que ha fallado y LastKnownGood que contiene el número de la clave con la última configuración buena conocida.

Es importante tener en cuenta que esta opción no repara ficheros dañados sino que no realiza la carga de los últimos drivers añadidos que pueden ser los que están provocando el error. Por tanto tiene que tenerse en cuenta que al utilizar la última configuración buena conocida para el arranque, cualquier modificación realizada en la configuración durante el último arranque del sistema se perderá.

11.2.2.5. Modo de restauración de SD (sólo en controladores de dominio)

Esta opción solo está disponible en Controladores de Dominio y se encarga de restaurar el estado del sistema de un DC, el cual incluye %SystemRoot\$\Sysvol (donde se encuentran los ficheros públicos del dominio que son replicados entre los diferentes Controladores) y el directorio Activo.

11.2.2.6. Modo de depuración

Esta opción se utiliza para arrancar Windows Server 2003 y enviar información de depuración a otro ordenador a través de un cable serie. Esto puede ser útil si el administrador necesita monitorizar el proceso de arranque desde otro ordenador.

11.2.3. Creación de un disco de arranque

Lo primero que debe realizarse para crear un disco de arranque de Windows 2003 es formatear el disco desde el propio Windows 2003, de esta forma se asegura que se introduce en el sector de arranque del disco información necesaria para que se arranque utilizando el Ntldr.

Una vez formateado el disco, deben copiarse en el mismo los ficheros necesarios para el arranque como son Ntldr, Ntdetect y Boot.ini; resulta necesario además Ntbootd si tenemos dispositivos SCSI y Bootsec.dos para arrancar otros sistemas; el

resto de ficheros involucrados en el arranque del sistema se tomarán del disco duro.

11.2.4. La consola de recuperación

Microsoft ha incluido en Windows 2003 (W2003) una gran cantidad de funciones y herramientas largamente esperadas. Pero de todos es sabido que, con independencia de las ventajas que estas nuevas herramientas puedan reportar tanto a administradores como a usuarios, toda instalación de una nueva versión de un sistema operativo conlleva, al menos, una desventaja ciertamente importante: que se vuelven obsoletas muchas de las técnicas y herramientas que, a diario, han utilizado y desarrollado los administradores de redes para el mantenimiento del sistema operativo. Pensemos en la recuperación del sistema.

Si nuestra empresa depende de W2003, deberemos saber cómo reparar los sistemas W2003 en el supuesto de que éstos fallen. Es cierto que Microsoft ha mejorado notablemente la fiabilidad y recuperabilidad de W2003, pero también es cierto que las cosas pueden torcerse y que, de hecho, se tuercen con cierta frecuencia. Por ello, y con el fin de estar preparados para lo que pueda suceder, Microsoft ha incluido en W2003 una serie de herramientas nuevas que nos permitirán realizar las tareas más fácilmente.

Microsoft ha conseguido eliminar, por fin, las diferencias en el terreno de la recuperabilidad antes mencionadas al incluir en W2003 las utilidades que han logrado situarlo a un mismo nivel que los sistemas Windows 9x. Además de las mejoras internas en la fiabilidad que han hecho de W2003 un sistema menos proclive a los bloqueos, Microsoft ha incluido varias características nuevas de recuperación que facilitan la reparación de los sistemas W2003 que presenten problemas de inicio. W2003 permite, por ejemplo, iniciar el sistema en varios modos seguros (es decir, a prueba de fallos) de forma muy similar a Windows 9x. Y, al igual que Windows 9x, W2003 ofrece durante el inicio varias opciones adicionales que permiten desactivar ciertas funciones del sistema operativo con el fin de poder iniciar el sistema correctamente. Para acceder a la mayoría de estas opciones, hay que pulsar F8 cuando se abra el menú del cargador de sistemas operativos de W2003 durante el inicio.

Entre estas nuevas características, existe un nuevo modo de inicio denominado Consola de recuperación (Recovery Console o RC). La Consola de recuperación es un intérprete de comandos que permite iniciar los equipos basados en NTFS para realizar las tareas de recuperación del sistema. Esta utilidad, tan pronto como se instala, permite iniciar el sistema abriendo una sesión especial de consola reducida de W2003 que permite acceder a todas las particiones de disco FAT16, FAT32 y NTFS del sistema, así como a un conjunto básico de mandatos y utilidades para la realización de tareas de recuperación.

11.2.4. La consola de recuperación

Para utilizar la Consola de recuperación en un sistema W2003, primero hay que instalarla, para lo que es preciso ejecutar el programa de instalación de W2003 (es decir, winnt32.exe) con el parámetro /cmdcons (por ejemplo, D:\i386\winnt32 /cmdcons). A continuación, W2003 mostrará en pantalla un mensaje advirtiendo que se va a instalar la Consola de recuperación y preguntando si se desea continuar con la operación. Tan pronto como se hace clic en «Yes» (Sí), el sistema copia los archivos necesarios (que, normalmente, no llegan a los 6 MB) en una carpeta oculta denominada \cmdcons, que reside en el directorio raíz de la unidad de inicio del sistema (por ejemplo, C:\cmdcons). La próxima vez que se inicie el sistema, el menú del cargador de sistemas operativos de W2003 ya incluirá la nueva opción «Microsoft Windows 2003 Recovery Console» (Consola de recuperación de Microsoft Windows 2003).

Cuando se selecciona esta opción de inicio, W2003 permite, durante un brevísimo espacio de tiempo, pulsar la tecla F6 para cargar un controlador RAID (Redundant Array of Inexpensive Disks o Array redundante de discos de bajo coste) o SCSI de otro fabricante. (Esta opción es necesaria si la Consola de recuperación no es capaz de detectar correctamente la configuración del controlador de disco.) A continuación, el sistema pasa a modo texto y solicita al administrador que especifique la instalación de W2003 en la que desea iniciar una sesión. Esta característica permite utilizar la Consola de recuperación para recuperar las distintas instalaciones de sistema operativo de un sistema multiinicio. Una vez que se haya seleccionado la instalación a la que se desea acceder, el sistema pedirá al administrador que suministre la contraseña de administrador para dicha instalación. (Dicha contraseña es la contraseña de la cuenta de administrador local, no la de la cuenta de administrador de dominio, en el caso de que exista un dominio).

Además de poder instalar una copia de la Consola de recuperación en el disco duro de cada uno de los sistemas esenciales, también es posible iniciar esta utilidad mediante la opción de reparación del programa de instalación de W2003. De este modo, también se podrá acceder a la consola tras ejecutarse el programa de instalación de W2003 desde CD-ROM o desde disquetes de 3,5 pulgadas. Esta posibilidad resulta muy útil cuando se tienen problemas con un sistema W2003 en el que la instalación de la Consola de recuperación se encuentra dañada o en el que nunca se ha instalado dicha utilidad.

La Consola de recuperación resulta especialmente útil cuando no hay forma de iniciar W2003 y es preciso acceder con urgencia al sistema de archivos para diagnosticar y solucionar el problema. Como dicha herramienta permite acceder directamente al sistema de archivos e incluye numerosas utilidades y mandatos de bajo nivel, los administradores pueden hacer la mayoría de tareas de recuperación de un sistema.

Puede resultar complejo para el administrador tener que utilizar la línea de co-

mandos, pero las posibilidades que otorga deben de hacer entender, que la RC era una herramienta que hacia falta en las instalaciones de NT. Es importante identificar las causas probables de los problemas de inicio de un sistema antes de que se produzcan, así como conocer las medidas que deben tomarse para resolverlos. Una lista con las causas más frecuentes de los fallos de inicio de W2003 y NT debidos a problemas con el software, se detalla a continuación:

- Se ha dañado o eliminado un archivo esencial del sistema (por ejemplo, los archivos de secciones del Registro o los archivos ntoskrnl.exe, ntdetect.com, hal.dll o boot.ini).
- Se ha instalado un servicio o controlador incompatible o defectuoso, o se ha dañado o eliminado un servicio o controlador esencial.
- Se han producido daños en el disco o en el sistema de archivos, incluidos los daños en las estructuras de directorios, el MBR (Master Boot Record o Registro de inicio principal) y el sector de inicio de W2003 o NT.
- El Registro contiene datos no válidos (es decir, el Registro se encuentra físicamente intacto pero contiene datos erróneos desde el punto de vista lógico, como un valor fuera de rango como valor del Registro correspondiente a un servicio o controlador).
- Son incorrectos o excesivamente restrictivos los permisos de la carpeta \%systemroot% (por ejemplo, C:\winnt).

La Consola de recuperación también permite resolver los problemas causados por los daños subyacentes que existan en el disco o en el sistema de archivos. De hecho, esta utilidad incluye varios mandatos que permiten reparar discos dañados desde fuera de W2003. Uno de estos mandatos es «Chkdsk», que es muy similar al mandato de Windows 9x y DOS que lleva el mismo nombre. Otros dos mandatos muy útiles a la hora de reparar un disco son «Fixmbr» y «Fixboot». «Fixmbr», al igual que el mandato «Fdisk /mbr» de Windows 9x, sustituye el MBR del disco principal del sistema por una copia en buen estado, lo que permite resolver todos aquellos problemas en los que el MBR hubiera resultado dañado o infectado por un virus. Igualmente útil es el mandato «Fixboot», que permite reparar el sector de inicio de W2003 en el supuesto de que hubiera resultado dañado o sobrescrito durante la instalación de otro sistema operativo (eventualidad que conlleva la pérdida del menú del cargador de sistemas operativos de W2003). Otra herramienta muy útil que incluye la Consola de recuperación es Diskpart, una utilidad de administración de discos similar a la incluida en el programa de instalación de W2003. Diskpart permite efectuar tareas básicas de administración de discos tales como la creación y eliminación de particiones.

La Consola de recuperación también incluye otros mandatos que pueden resultar muy útiles, como «Listsvc», «Enable» y «Disable», que permiten generar una lista de los servicios y controladores del sistema, activarlos y desactivarlos, respectivamente. Esta serie de comandos es vital cuando el problema de inicio del sistema se debe a la existencia de un servicio o controlador defectuoso. Basta con iniciar una sesión en la Consola de recuperación, desactivar el servicio o controlador que esté dando problemas y, por último, reiniciar el sistema, por lo que no es preciso efectuar ninguna modificación ni restauración del Registro.

Como la Consola de recuperación muestra las carpetas de instalación tanto de W2003 como de NT en los sistemas de inicio dual, es posible que a los usuarios de tales sistemas les resulte útil esta herramienta para la recuperación de instalaciones NT fallidas. Aun cuando se advierte en varios artículos de Microsoft que no se debe seguir esta práctica, lo cierto es que no se ofrece ninguna explicación que justifique dicha advertencia. Como la mayoría de los mandatos de esta utilidad guardan relación con el sistema de archivos, funcionan perfectamente en volúmenes NTFS5 compartidos entre W2003 y NT. (Es preciso recordar, no obstante, que hay que instalar Service Pack 4 —SP4—, o una versión posterior de este paquete de servicios, en NT con el fin de que este sistema operativo sea compatible con NTFS5).

Hay que hacer constar algunos defectos e inconvenientes que presenta la Consola de recuperación. Una limitación bastante importante es la de que no se puede instalar en un volumen espejo/RAID1 «basado en software» (es decir, un volumen que se haya creado mediante el Administrador de discos de NT o el Administrador de discos lógicos de W2003, no una controladora RAID de hardware). Por lo que se refiere a los requisitos de configuración de las particiones, las reglas que se siguen para la instalación de la Consola de recuperación son similares a las que se siguen para la instalación de W2003. Al igual que en las instalaciones normales y corrientes de sistemas operativos, este problema se puede sortear eliminando el espejo, instalando la Consola de recuperación y volviendo a restablecer el espejo.

Como conclusión podemos destacar que el uso de la Consola de Recuperación no va a sustituir a todas las herramientas que comúnmente viene utilizando un administrador, pero si que aglutina las capacidades necesarias para que sea una herramienta de cabecera.

11.3. Linux al rescate

Puede resultar complicado entender que otro sistema operativo pueda resultar de ayuda a la hora de resolver problemas en un sistema W2003, y más si cabe si este SO se llama Linux. Sabido es la batalla emprendida por Microsoft para desprestigiar a Linux.

Sin embargo a un administrador cuyo objetivo es devolver su sistema a un estado óptimo en el menor tiempo posible, solo debe preocuparle que herramientas me pueden sacar del apuro.

Linux es un clon de Unix, desarrollado bajo la licencia GPL, que permite utilizar, modificar y distribuir, los fuentes de Linux. Linux soporta varios sistemas de ficheros, entre ellos toda la gama que soporta W2003 (FAT,FAT16,FAT32,NTFS). Por tanto, es fácil arrancar nuestra máquina con un disquete que contenga un mínimo sistema Linux y poder acceder a la partición que contiene nuestro Windows 2003 (algo parecido a la Consola de Recuperación de W2003). Por tanto, un administrador con los suficientes conocimientos podría editar el Registro, manipular la SAM o modificar el sistema de ficheros NTFS. Pero las cosas no tienen que ser tan complicadas. Existen utilidades ya preparadas que nos permiten realizar estas tareas. Nosotros nos vamos a centrar en el trabajo realizado por un desarrollador desinteresado que ha construido un disquete que arranca un sistema Linux con soporte SCSI y que permite editar el registro, habilitar y deshabilitar cuentas, así como cambiar el password del administrador.

La utilidad en cuestión es de libre distribución y se denomina Petter Nordahl-Hagen's Offline NT Password & Registry Editor. Esta utilidad permite, como hemos comentado, cambiar el password de cualquier usuario que tenga una cuenta local válida en el sistema W2003, modificando la contraseña encriptada del fichero SAM del Registro. No se necesita conocer la contraseña anterior para definir una nueva. La utilidad funciona fuera de línea, es decir, necesitamos reiniciar el sistema y arrancar desde disquete o CD-ROM. El disquete incluye el soporte necesario para acceder a particiones NTFS y una serie de scripts que nos facilitan la tarea. Además, detectará y permitirá desbloquear cuentas deshabilitadas o bloqueadas.

El único problema que se puede presentar en sistemas XP o W2003 con Service Pack instalado, es que si el usuario utilizó EFS para cifrar sus ficheros, estos no podrán ser leídos a no ser que recuerde la contraseña antigua.

El autor dispone de un disquete de arranque que automatiza todo este proceso. Lo único que hay que hacer es bajarse la imagen del disquete y generarla bien con **rawrite.exe** si estamos en un entorno MS-DOS o con el comando **dd** si estamos en Linux. El sitio Web donde podemos encontrar toda la información referente a esta utilidad es la siguiente <http://home.eunet.no/~pnordahl/ntpasswd/>

Como referencia comentar que existe la posibilidad de cambiar la contraseña del administrador de un dominio Windows 2003, siguiendo el truco que se comenta en la siguiente página web <http://www.jms1.net/nt-unlock.html>

11.4. Service Packs. Windows Updates

No cabe duda que todo software por muy testeado que esté, siempre es susceptible de mejorarse o de esconder agujeros imprevistos ante situaciones imprevistas. Por tanto, todo administrador de sistemas W2003, debe seguir una política activa de actualizaciones, lo cual implica una constante formación así como aplicar todos los parches habidos y por haber.

Microsoft publica periódicamente los denominados Hot-fixes para evitar agujeros de seguridad en sus sistemas. No siempre con la celeridad que sería de agradecer. Cuando existe un cúmulo de actualizaciones importante, suele publicar un Service Pack para arreglar los diferentes servicios que tenga instalado el sistema.

Actualmente la instalación de un Service Pack solo modifica el software que tenga instalado la máquina, pero nos seguimos viendo obligados a reinstalarlo si el servicio se ha instalado posteriormente.

Microsoft proporciona un sistema de actualización en línea vía web muy útil pero poco práctico si tenemos que actualizar cientos de estaciones y servidores. Para ello Microsoft Software Update Services (SUS) proporciona la forma más rápida y segura de actualizar una red montando un servidor de actualizaciones propio. La instalación y configuración de este servicio escapa a los objetivos del curso, pero toda la información disponible se puede encontrar en la siguiente dirección <http://www.microsoft.com/windowsserversystem/sus/default.mspx>

A

Nota Legal

Se concede permiso para copiar, distribuir y/o modificar este documento bajo los términos de la GNU Free Documentation License, Version 1.2 o posterior, publicada por la Free Software Foundation, siendo secciones invariantes este apéndice que contiene la nota legal. Se considera texto de portada el siguiente:

Administración Avanzada de Windows Server 2003

por Fernando Ferrer García y Andrés Terrasa Barrena

Copyright (c) 2002 Fernando Ferrer

Copyright (c) 2003-07 Fernando Ferrer y Andrés Terrasa

Versión 2.0, abril 2007

Este documento puede ser copiado y distribuido en cualquier medio con o sin fines comerciales, siempre que la licencia GNU Free Documentation License (FDL) [<http://www.gnu.org/copyleft/fdl.html>], las notas de copyright y esta nota legal diciendo que la GNU FDL se aplica al documento se reproduzcan en todas las copias y que no se añada ninguna otra condición a las de la GNU FDL.