Curso de Windows 2000 Avanzado

Fernando Ferrer

Tabla de contenidos

Lista de figuras

Lista de tablas

Capítulo 1. El sistema de nombres de dominio (DNS)

Tabla de contenidos

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*.

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 unívoca 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 padre 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 contener, 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 correspondiente 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.

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.

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 dividirla 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.

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.

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 informació sobre múltiples dominios.

DNS define dos tipos de servidores de nombres que mantienen informacion 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 “Transferencias 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.

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.

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, BIND (*Berkeley Intenet Name Domain*), se utiliza los nombres de archivo siguientes para almacenar los registros de cada zona:

- `Db.dominio`: zona de resolución directa.
- `Db.direccion`: zona de resolución inversa.
- `Db.cache`: sugerencias de servidores raíz.
- `Db.127.0.0.1`: resolución inversa de bucle cerrado.

Por el contrario, 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, en Windows 2000, la base de datos DNS puede integrarse con la base de datos de Active Directory, en cuyo caso dicha información participa de los mismos mecanismos de almacenamiento y replicación que el resto de información contenida en el Directorio Activo.

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.

El formato de cada registro de recursos es el siguiente:

```
Propietario     TTL     Clase     Tipo     RDATA
```

donde:

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

un nombre de host/dominio (completamente cualificado o no), el símbolo "@" (que representa el nombre de la zona que se está describiendo) o una cadena vacía (en cuyo caso equivale al propietario del registro de recursos 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.

A continuación se describen los principales tipos de registros de recursos: SOA, NS, A, PTR, CNAME, MX y SRV.

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.
- **Tipo**: "`SOA`".
- **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 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 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  pc0100.admon.com  hostmaster.admon.com.
                (
                  1      ; número de serie
                  3600   ; actualización 1 hora
                  600    ; reintentar 10 minutos
                  86400  ; caducar 1 día
                  60     ; TTL 1 minuto
                )
```

Registro de Recurso NS

El registro de recursos NS (*Name Server*) indica los servidores de nombres autorizados 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.
```

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
```

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 “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.
```

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:

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

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.
```

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:

- El campo `servicio` especifica el nombre de servicio: http, telnet, etc.
- El campo `protocolo` especifica el protocolo utilizado: TCP o UDP.
- `nombre` define el nombre de dominio al que hace referencia el registro de recurso SRV.
- Los campos `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.
```

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
```

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 (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 continuacion se describe cada tipo brevemente.

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.

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.

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 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.

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.

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.

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 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).

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.

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.

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.

Capítulo 2. Protección Local

Tabla de contenidos

Introducción

Como ya sabemos, el Directorio Activo (o *Active Directory*) es una estructura jerárquica que almacena información sobre objetos (o recursos) en dominios Windows 2000. El Directorio Activo permite organizar lógicamente estos recursos en sus respectivos dominios, de forma que resulte fácil tanto localizar como administrar esos recursos desde cualquier ordenador en cualquier dominio de la organización.

Sin embargo, antes de estar en condiciones de administrar eficazmente el Directorio Activo, es necesario adquirir una base en la administración local de recursos de Windows 2000. Esta base incluye el modelo de protección que incorpora este sistema, que incluye los conceptos de usuario, grupo (local), derecho y permiso. En los siguientes capítulos se amplía esta "administración local" a la administración de un dominio (o múltiples dominios) mediante el Directorio Activo.

Concepto de usuario

Como muchos otros sistemas operativos, Windows 2000 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 2000 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 2000 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 2000 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 2000 del mundo (son identificadores únicos). Windows 2000 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 2000, existen de entrada las cuentas de dos usuarios preinstalados (*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.

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. Un usuario puede pertenecer a tantos grupos como sea necesario, poseyendo implícitamente la *suma* de los permisos de todos ellos. Esta forma de administrar la protección del sistema es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales.

Considérese, 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 grupos, esta operación sería tan sencilla como cambiar al usuario de un grupo a otro. Por ello, en Windows 2000 se recomienda que los permisos se asignen en base a *grupos*, y no en base a usuarios individuales.

Al igual que existen cuentas preinstaladas, en todo sistema 2000 existen una serie de grupos preinstalados (*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 2000 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 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).
- Usuarios autentificados (*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 autentificados".

El modelo de protección

El modelo de protección de Windows 2000 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 2000 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 accion 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 2000. 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 ("Atributos de protección de los procesos"), los derechos que pueden establecerse en el sistema ("Derechos de usuario") y los atributos de protección que poseen los recursos ("Atributos de protección de los recursos"). La "Reglas de protección" establece las reglas concretas que definen el control de acceso de los procesos a los recursos.

Atributos de protección de los procesos

Cuando un usuario es autorizado a conectarse interactivamente a un sistema Windows 2000, el sistema construye para él una acreditación denominada *Security Access Token* o SAT. Esta acreditación contiene la información de protección del usuario, y Windows 2000 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:

a. **SID**. El identificador único del usuario.

b. **SID de sus grupos**. Lista de los SIDs de los grupos a los que pertenece el usuario.

c. **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 "Derechos de usuario").

Esta forma de construir la acreditación introduce ya una de las máximas de la protección de Windows 2000: el nivel de acceso de un usuario incluye implícitamente los niveles de los grupos a los que pertenece.

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 2000 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. Derechos más importantes en Windows 2000 presenta los derechos más destacados de cada tipo, junto con su descripción.

Tabla 2.1. Derechos más importantes en Windows 2000

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 *Plug and Play*.
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.).

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 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.

Otras directivas de seguridad

En Windows 2000, los derechos son un tipo de *directivas de seguridad*. En este sentido, Windows 2000

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*).

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

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.

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.

Claves públicas

> Este apartado permite administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

Atributos de protección de los recursos

En un sistema de archivos NTFS de Windows 2000, cada carpeta o archivo posee los siguientes atributos de protección:

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).

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 2000 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).

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 registro, 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 2000 se explican en la "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 2000: 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 2000). 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.

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, este posee por defecto permisos heredados (de la carpeta o unidad donde se ubica) y ningún permiso explícito.
- Cualquier usuario que posea control total sobre el archivo o carpeta (por defecto, su propietario) puede incluir nuevos permisos (positivos o negativos) en la lista de permisos explícita.
- El control sobre la herencia de permisos (i.e., qué objetos heredan y qué permisos se heredan) se realiza a dos niveles:
    a. Cada objeto (archivo o carpeta) tiene la potestad de decidir si desea o no heredar los permisos de su carpeta padre. Es decir, cada carpeta/archivo puede *desactivar* la herencia de su carpeta padre.
    b. Cuando se define un permiso explítito en una carpeta, se puede también decidir qué objetos por debajo van a heredarlo. En este caso, se puede decidir entre cualquier combinación de la propia carpeta, las subcarpetas y los archivos. La opción por defecto es todos, es decir, la carpeta y todas las 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 (o unidad) padre correspondiente a la nueva ubicación.
- Mover un archivo distingue dos casos: si movemos una carpeta o archivo a otra ubicación

dentro del mismo volúmen (partición) NTFS, se desactiva la herencia y se mantienen los permisos que tuviera como explíticos en la nueva ubicación. Si el volúmen 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).

Permisos estándar e individuales

Windows 2000 distingue entre los *permisos estándar* de carpetas (directorios) 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).

En la Tabla 2.2. Permisos estándar sobre carpetas y archivos en Windows 2000 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 2000 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 2000

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,

ARCHIVOS	
Nombre	**Significado**
	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 2000 muestra cuáles son los permisos individuales en Windows 2000, 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 2000

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`	plicado 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.

Nombre	Significado
Tomar posesión	Permite tomar posesión de la carpeta o archivo.

La Tabla 2.4. Correspondencia de permisos estándar a individuales en Windows 2000 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.

Tabla 2.4. Correspondencia de permisos estándar a individuales en Windows 2000

Permiso	C. Total	Modificar	Leer y Ej.	Listar	Leer	Escribir
Atravesar carpeta/ejecutar archivo	√	√	√	√		
Leer carpeta/Leer datos	√	√	√	√	√	
Leer atributos	√	√	√	√	√	
Leer atributos extendidos	√	√	√	√	√	
Crear ficheros/escribir datos	√	√				√
Crear carpetas/anexar datos	√	√				√
Escribir atributos	√	√				√
Escribir atributos extendidos	√	√				√
Borrar subcarpetas y archivos	√					
Borrar	√	√				
Leer permisos	√	√	√	√	√	√
Cambiar permisos	√					
Tomar posesión	√					

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 2000 son acumulativos: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SIDs de su acreditación (ver "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 2000 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:

a. 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.
b. 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.
c. 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 2000 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.

Capítulo 3. Administración de Dominios

Tabla de contenidos

Introducción

Este capítulo introduce los conceptos fundamentales sobre dominios Windows 2000, suficientes para poder unificar y centralizar la administración de conjuntos de sistemas Windows 2000 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 definirseen el mismo, la compartición de recursos entre sistemas de la organización y la delegación de tareas administrativas dentro de un dominio.

El Directorio Activo

Dominios Windows 2000 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 2000 utiliza el concepto de **directorio** para implementar dominios de sistemas Windows 2000.

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 2000. 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 2000 (Server) de nuestra red, convertimos a dichos ordenadores en los servidores del dominio, o más correctamente, en los denominados *Controladores de Dominio* (*Domain Controllers*). 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 incluye 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.

Estándares relacionados

A diferencia de su antecesor NT 4.0, Windows 2000 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.

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 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 2000 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 2000 se identifica unívocamente mediante un nombre DNS (por ejemplo, `miempresa.com`) y cada equipo basado en Windows 2000 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:

A. **Resolución de nombres**: DNS permite realizar la resolución de nombres al convertir los nombres de host a direcciones IP.

B. **Definición del espacio de nombres**: Directorio Activo utiliza las convenciones de nomenclatura de DNS para asignar nombre a los dominios.

C. **Búsqueda de los componentes físicos de AD**: para iniciar una sesión de red y realizar consultas en Directorio Activo, un equipo con Windows 2000 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.

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.

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 unívocamente 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 2000 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 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 políticas se aplican dentro del dominio y no a través de los dominios.
- **Delegar permisos administrativos**. En las redes que ejecutan Windows 2000, 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.

Modos de Dominio

Tras instalar el Directorio Activo y crear un dominio nuevo, ambos se ejecutan en modo mixto. Un dominio en modo mixto es compatible con controladores de dominio que ejecutan Windows 2000 y Windows NT. Si la red no dispone de ningún controlador de dominio NT (PDC) o cuando todos los controladores de dominio se hayan actualizado a Windows 2000, se puede convertir el dominio de modo mixto a modo nativo.

En un dominio en modo nativo, todos los controladores de dominio ejecutan Windows 2000. Sin embargo, no es necesario actualizar a Windows 2000 los servidores miembro y los clientes con NT Workstation o W9x antes de convertir un dominio a modo nativo.

Lo que sí es necesario subrayar es que parte de la funcionalidad del Directorio Activo Directory requiere que el dominio esté en modo nativo. Además, puede convertirse un dominio a modo nativo independientemente de los modos de otros dominios del bosque. El cambio de modo mixto a modo nativo es un proceso irreversible.

Múltiples dominios en la misma organización

Existen muchos casos en los que es interesante disponer de varios dominios de ordenadores Windows

2000 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 2000 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.

A. **Arbol**.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 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.

B. **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 el espacio de nombres, el bosque tiene un único dominio raíz, llamado el dominio raíz del bosque. Este será el primer dominio creado en el bosque

Añadir nuevos dominios a un bosque es fácil. Sin embargo, no se pueden mover dominios de Active Directory entre bosques. Solamente se podrán eliminar dominios de un bosque si este no tiene dominios hijo. Además, después de haber establecido el dominio raíz de un árbol, no se pueden añadir dominios con un nombre de nivel superior al bosque. Tampoco se puede crear un dominio padre de un dominio existente.

El implementar bosques y árboles de dominio permite mantener convenciones de nombres contiguos y discontiguos, lo cual puede ser útil en organizaciones con divisiones independendientes que quieren mantener sus propios nombres DNS.

En resumen, cuando promocionamos un servidor Windows 2000 a controlador de dominio (mediante el asistente dcpromo, tenemos que decidir una de las siguientes opciones de instalación:

1. DC adicional de un dominio existente o de 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 de un arbol de dominios ya creado), o bien el dominio principal (raíz) de un nuevo arbol de dominios.
3. En este segundo caso, el dominio raíz puede ser de un bosque existente o de un nuevo bosque.

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 un controlador de dominio de otro dominio. Estas relaciones permiten a los usuarios acceder a los recursos de otro dominio y a los administradores definir los derechos de usuario para los usuarios del otro dominio.

Todas las relaciones de confianza en un bosque basado en Windows 2000 son *bidireccionales y transitivas*:

a. **Bidireccionales**: cuando se crea un nuevo dominio hijo, este automáticamente confía en el dominio padre y viceversa.
b. **Transitivas**: si el dominio A y el dominio B (padre e hijo) confían el uno en el otro y además el dominio B y el dominio C (también padre e hijo) confían el uno en el otro, entonces el dominio A y el domino C confían mutuamente el uno en el otro de forma implícita, aunque no exista una relación de confianza directa entre ellos.

Hablando del bosque, podemos decir que una relación de confianza se crea automáticamente entre el dominio raíz del bosque y el dominio raíz de cada árbol de dominio añadido al bosque, lo que provoca que exista una confianza completa entre todos los dominios en un bosque de Active Directory.

Desde un punto de vista práctico, un único proceso de inicio de sesión (*logon*) le permite al sistema autentificar a un usuario o máquina en cualquier dominio del bosque. Por tanto, este proceso permite potencialmente a las cuentas de usuario y máquina acceder a los recursos en cualquier dominio del bosque.

Además de las confianzas transitivas y bidireccionales del bosque, que se generan automáticamente en el sistema operativo Windows 2000, se pueden crear explícitamente dos tipos diferentes de relaciones de confianza:

A. **Relación de confianza de acceso directo**: una relación de confianza de acceso directo, también denominada relación de confianza de vínculo cruzado, es una relación de confianza creada manualmente, que mejora la eficacia de los inicios de sesión remotos, acortando la ruta de confianza. Si los usuarios del dominio A necesitan frecuentemente tener acceso a los recursos

del dominio C, se podría crear un vínculo directo mediante una relación de confianza de acceso directo, de forma que se omita el dominio B en la ruta de confianza. Una relación de confianza de acceso directo tiene las siguientes características:

- se puede establecer entre cualesquiera dos dominios del mismo bosque.
- debe establecerse manualmente en cada dirección.
- debe ser transitiva.

B. **Relación de confianza externa**: una relación de confianza externa se crea manualmente entre dominios de Windows 2000 que pertenencen a bosques diferentes o entre un dominio de Windows 2000 y un dominio cuyo controlador de dominio ejecuta Windows NT 4.0. Las relaciones de confianza externas son unidireccionales e intransitivas, y deben establecerse manualmente en cada sentido para poder disponer de una relación de confianza externa bidireccional.

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 foma coherente. En el Directorio Activo, las unidades organizativas permiten:

a. **Conseguir una estructuración lógica** de los objetos del directorio, de acuerdo con la organización de la *empresa* (por departamentos o secciones, sedes, delegaciones geográficas, etc.). Entre otras ventajas, esta organización le permite al administrador del dominio una gestión más lógica de usuarios, grupos, equipos, etc., pero también le permite a cualquier usuario una búsqueda de los objetos más sencilla cuando explora el directorio buscando recursos (por ejemplo, se podría localizar fácilmente las impresoras compartidas del edificio central de la delegación de Alicante).

b. **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.

c. **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.

En muchos sentidos, el concepto de unidad organizativa se puede utilizar en Windows 2000 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 2000 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.

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.

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 2000 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.

Controladores de dominio

Un controlador de dominio (*Domain Controller*, DC) es un equipo donde se ejecuta Windows 2000 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:

A. **Partición de directorio de dominio**: contiene todos los objetos del directorio para este

dominio. Los datos del dominio en cada dominio se replican a cada controlador de domino en este dominio, pero no mas allá del dominio.

B. **Partición del directorio de esquema**: contiene todos los tipos de objetos y atributos que pueden ser creados en el 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.

C. **Partición de directorio de configuración**: contiene la topología de replicación y los metadatos. Por ejemplo, aplicaciones compatibles con Active Directory almacenan información en esta partición del directorio. Estos datos son comunes a todos los dominios en el bosque, y se replican a todos los controladores de dominio en el bosque.

Además de estas tres 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.

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

En Windows 2000, 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.

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.

Operaciones de Maestro Unico

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 dominio 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 2000 en modo mixto, pero todavía requieren un controlador principal de dominio (PDC), se asigna a un controlador de dominio específico basado en Windows 2000, 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.

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 2000. 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 2000, 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 2000, planteando en cada caso sus opciones de configuración y su utilidad dentro de la administración del dominio.

Usuarios globales

En el Capítulo 2. *Protección Local* se ha visto cómo pueden crearse cuentas de usuarios y grupos en Windows 2000, y cómo se utilizan ambas para:

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

Por lo tanto, según lo que sabemos hasta ahora, 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 2000, 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*). Em 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 utilizando 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 2000 (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.

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 2000 se definen tres clases de grupos de seguridad (o, de forma más precisa, se pueden definir grupos de tres *ámbitos* distintos):

Grupos locales del dominio

> En un dominio en modo mixto, pueden contener cuentas de usuario y grupo globales de cualquier dominio del bosque. En un dominio en modo nativo, 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 (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).

Grupos globales

> En un dominio en modo mixto, pueden contener cuentas de usuario globales del mismo dominio. En un dominio en modo nativo, 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.

Grupos universales

> Sólo están disponibles en dominios en modo 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 el Capítulo 2. *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 2000 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).

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.

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 directoio 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 unívocamente. Este identificador es análogo al SID de cada cuenta de usuario, y sólo lo conocen los DC s y el propio ordenador miembro. Es por tanto, un dato interno del sistema operativo, y ni siquiera el administrador puede cambiarlo.

Windows 2000 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. Estos protocolos se utilizan siempre que información relativa a aspectos de seguridad se intercambia entre máquinas 2000 pertenecientes a algún dominio y, en concreto, para autenticar usuarios (como se ha explicado arriba).

Unidades Organizativas

Como hemos visto en "Unidades Organizativas", las unidades organizativas son objetos del directorio que a su vez, pueden contener otros objetos. El uso fundamental de las OUs es organizar de forma lógica los objetos de un dominio, pudiendo además utilizarse para 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 específicas a la unidad.

Compartición de recursos entre sistemas Windws 2000

Cuando un sistema Windows 2000 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 2000. La compartición de otros recursos (tales como impresoras, por ejemplo) queda fuera del ámbito de este texto.

Permisos y derechos

Cualquier sistema Windows 2000 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 subcarpetas).

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 2000 denominado A, y desea conectarse a un recurso de red que exporta otro Windows 2000 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 A comparte.

Compartición dentro de un dominio

Cuando la compartición de recursos la realizan equipos que forman parte de un dominio Windows 2000, 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, 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.

Y segundo, cuando un sistema Windows 2000 se agrega a un dominio, los siguientes recursos se comparten de forma automática y por defecto (estas comparticiones no deben modificarse ni prohibirse):

- `letra_de_unidad$`. Por cada partición existente en el sistema Windows 2000 (`C:`, `D:`, etc.) se crea un recurso compartido denominado `C$`, `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 2000.

- `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 2000, 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: prohibe 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).

Mandatos Windows 2000 para compartir recursos

La compartición de recursos en Windows 2000 puede realizarse en línea de órdenes utilizando los mandatos **net share** y **net use**. La sintaxis de ambos mandatos es la siguiente:

a. 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
```

b. 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:[nombre_dominio\]nombre_usuario]
         [[/delete] | [/persistent:{yes | no}]]
net use nombre_dispositivo [/home[contraseña | *]]
         [/delete:{yes | no}]
net use  [/persistent:{yes | no}]
```

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 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.

Capítulo 4. Administración de Políticas de Grupo

Tabla de contenidos

Introducción

Este capítulo introduce una de las herramientas que incluye Windows 2000 para centralizar la administración y configuración de usuarios y equipos en un dominio: las *Políticas 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.

Objetos de Política de Grupo

En cada sistema Windows 2000, 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 2000.

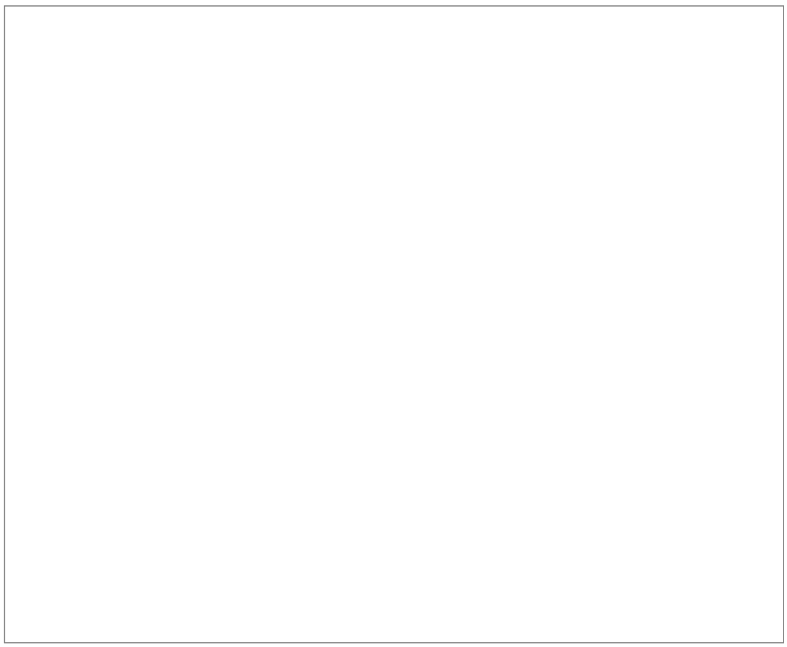
En concreto, las políticas se especifican mediante objetos de directorio denominados *Objetos de Política de Grupo* (*Group Policy Objects*), o simplemente GPOs. Un GPO es un objeto que incluye como atributos cada una de las políticas (también denominadas *directivas*) que puede establecerse en Windows 2000 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.

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 existen dos *nodos principales*, justo por debajo del nodo raíz, que separan las configuraciones para equipos y para usuarios:

a. 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.

b. 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.

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 la GPO, con el consiguiente retraso (no útil) en el inicio de sesión de dicho usuario.

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.

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 politica(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 vinculadas a unidades de segundo nivel, de tercer nivel, etc.

Este orden de aplicación decide la *prioridad* entre las 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 dos parámetros que pueden activarse independientemente sobre cada GPO:

a. **No reemplazar** (*No override*). Si una GPO tiene este parámetro activado, sus políticas no pueden ser sobrescritas por GPOs que se apliquen más tarde.
b. **Bloquear herencia de directivas** (*Block policy inheritance*). Cuando un GPO con este

parámetro activado se vincula a un contenedor, se desactiva la herencia de las políticas establecidas en contenedores superiores, *excepto* aquellas que corresponden a GPOs con el parámetro "No reemplazar".

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 las GPOs puede refinarse aún más utilizando grupos de seguridad.

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.

Filtrar el Ambito 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 autentificados*, 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 la 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.

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:

- 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:

A. **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.

B. **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 explicó en la Sección~ "Delegación de la administración".

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:

a. **Configuración de Software** (*Software Settings*). Contiene la configuración, bien del equipo o bien de usuario, de la instalación automática de software.

b. **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.

c. **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.

Plantillas administrativas

Este grupo contiene todas las configuraciones de políticas basadas en el registro de Windows 2000,

incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows 2000 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 2000, 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 2000, 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.

Configuraciones de seguridad

En este apartado se encuentra la configuración de muchos de los aspectos de seguridad que pueden establecerse en un sistema Windows 2000.

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~ "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~ "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.

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.

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 2000, 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.

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 últil 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.

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 Windows 2000 Professional.

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 delegación 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.
- **Miniminzar 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 desado.
- **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 usuario, 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 las GPOs, se recomienda limitarlo a las ocasiones en que sea estrictamente necesario.

Capítulo 5. El servicio DHCP en Windows 2000

Tabla de contenidos

El protocolo DCHP

DHCP (*Dynamic Host Configuration Protocol*) o Protocolo Dinámico de Configuración de Equipos no es un protocolo específico de Windows 2000, 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 proporciones 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 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 iniciarlo.

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 `DCHP Offer` proporcionando una dirección al cliente.
3. El cliente acepta la oferta respondiendo con un mensaje `DHCP Request`.
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.

Concepto de Ambito

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.

Administración de Ambitos

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.
- 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.

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 2000 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).

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 funciones como servidores de impresión, servidores web o encaminadores (*routers*).

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.

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

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 2000, 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 2000.

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 admininistración DHCP. Sólo los miembros del grupo "Administración de Empresas" (perteneciente al dominio raíz del bosque) tienen permisos suficientes para realizar esta acción.

DHCP y DNS

De manera predeterminada, la implementación de DHCP de Windows 2000 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 2000, es el cliente DHCP de Windows 2000 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.

Capítulo 6. El servicio Terminal Server

Tabla de contenidos

Introducción

Los denominados *Servicios de Terminal* (*Terminal Server*) constituyen un componente incluido en la familia de servidores Windows 2000: Windows 200 Server, Windows 2000 Advanced Server y Windows 2000 Datacenter Server. Los Servicios de Terminal proporcionan interfaz de usuario gráfica de Windows a dispositivos remotos a través de conexiones LAN, WAN o Internet. Todo el procesamiento de las aplicaciones se realiza en el servidor y solo los datos desde los dispositivos como el monitor, teclado etc., son transmitidos entre el servidor y el cliente de los servicios de Terminal.

Los Servicios de Terminal pueden ser habilitados en dos modos diferentes: Servidor de aplicaciones o Administración Remota. El modo Servidor de Aplicaciones permite a múltiples clientes remotos acceder simultáneamente a las aplicaciones Windows que se ejecutan en el servidor. Este es el modo de empleo tradicional del Servicio de Terminal.

El modo de Administración remota es una característica nueva de los Servicios de Terminal de Windows 2000. Está diseñada para proporcionar a los operadores y administradores acceso remoto a los servidores y controladores de dominio. El administrador tienen acceso a las herramientas gráficas del entorno Windows, incluso si no se está usando un ordenador basado en Windows para administrar el servidor.

El software cliente de los Servicios de Terminal para ordenadores basados en Windows de 16 o 32 bits se incluye con Windows 2000 Server.

El modo de administración remota no afecta al rendimiento del servidor. Hasta dos sesiones de administración remota están soportadas, además de sesión de la consola. No se se necesitan Licencias de Acceso al Cliente de Servicios de Terminal para utilizar la administración remota.

El modo de administración remota de los Servicios de Terminal ofrece las siguientes característica y ventajas:

- Administración gráfica de los servidores Windows 2000 desde cualquier cliente de Servicios de Terminal. Existen clientes disponibles para correr sobre Windows 3.11, Windows 9x, windows CE 2.11, Windows NT y Windows 2000.
- Posibilidad de actualizaciones remotas, reboots, y promociones de controladores de dominio.
- Acceso a servidores a través de conexiones bajo ancho de banda, con hasta 128 bits de cifrado (56 fuera de Estados Unidos)
- Instalación de aplicaciones de forma remota y ejecución de las mismas.
- La sesión de la consola no se ve afectada mientras tiene lugar la administración remota.
- No se ve afectado el rendimiento.
- No se necesitan licencias.
- Dos administradores remotos pueden compartir una sesión con propósitos de colaboración.

Funcionamiento

El servicio Terminal Server permite el acceso multiusuario al sistema operativo Windows 2000, de forma que varias personas puedan ejecutar sesiones simultáneamente en un mismo equipo.

El entorno multiusuario de los Servicios de Terminal Server consta de tres partes:

a. **Servidor de Servicios de Terminal Server**. El servidor administra los recurso informáticos para cada sesión de cliente y ofrece un entorno único a todos los usuarios que tienen iniciada una sesión. El servidor recibe y procesa todas las pulsaciones del teclado y las acciones del ratón que realiza el cliente remoto, y dirige al cliente apropiado todo el resultado que aparece en la pantalla tanto para el sistema operativo como para las aplicaciones.
b. **Cliente**. La sesión de Terminal se abrirá como una ventana en el escritorio del equipos cliente. Dentro de dicha ventana se ejecuta el escritorio remoto del servidor de Terminal. El equipo

cliente sólo necesita la cantidad mínima de software necesario para establecer una conexión con el servidor y presentar la interfaz de usuario.

c. **Protocolo de escritorio remoto**. El *Remote Desktop Protocol* o RDP permite la comunicación entre cliente y el servidor. Este protocolo está optimizado para mover elementos de la interfaz gráfica al cliente. RDP es un protocolo de la capa de aplicación que se basa en TCP/IP para transportarlo por la red. RDP se basa en el estándar T.120 de International Telecommunication Union (ITU) para conferencia multicanal.

Características y ventajas

Los Servicios de Terminal Server poseen ciertas características que ofrecen ventajas para la organización. A continuación se muestran unas y otras.

Acceso al escritorio y a aplicaciones

Es posible utilizar Terminal Server para extender a diversos clientes el sistema operativo Windows 2000 y las aplicaciones basadas en Windows. Las ventajas que supone ampliar el acceso pueden ser:

- Ejecutar aplicaciones Windows. Se puede poner a disposición de una amplia gama de clientes las aplicaciones basadas en Windows con sólo hacer algunas modificaciones. No es necesario volver a escribir las aplicaciones para que se ejecuten en distintos sistemas operativos y distinto hardware.
- Extender el uso de equipos obsoletos.

Mayor Seguridad y Fiabilidad

Puesto que los datos de las aplicaciones o de los usuarios nunca residen en el cliente, Servicios de Terminal Server permite aumentar el control de la seguridad. Además, proporciona compatibilidad con cifrado multinivel, que se podrá habilitar siempre que exista riesgo de que se produzca una interceptación no autorizada de la transmisión en el vínculo entre el servidor y el cliente. Hay tres niveles de cifrado: bajo, medio y alto. Todos estos niveles de cifrado emplean el cifrado estándar RSA RC4 (tecnología de cifrado de claves públicas).

Administración y Compatibilidad Mejoradas

Como ya hemos comentado, Servicios de Terminal Server dispone de varias características que resultan útiles para las tareas administrativas. Con el modo de Administración remota se pueden controlar los servidores Windows 2000 desde un único escritorio.

Existe otra característica denominada Control Remoto, mediante la cual los administradores pueden supervisar desde otra sesión de cliente las acciones llevadas a cabo por un usuario que tiene iniciada una sesión en Terminal Server. El control remoto permite observar o controlar activamente una sesión de cliente. Al hacerlo, las acciones del teclado y ratón se introducen directamente en la sesión de cliente. Una sesión de cliente no puede controlar de forma remota la consola del sistema. El control remoto resulta de utilidad para solucionar problemas de forma remota y cuando se enseña a los usuarios nuevas aplicaciones.

Distribución Centralizada de Aplicaciones

Los Servicios de Terminal Server puede ser utilizado para distribuir aplicaciones en un modo totalmente centrado en el servidor, donde las aplicaciones se ejecutan por completo, por tanto no se requiere hardware tan caro ya que el usuario puede usar meros terminales para acceder a las aplicaciones. Además y más importante, proporciona un fácil acceso a software nuevo o actualizado. Cuando los Servicios de Terminal Server se habilitan en un servidor Windows 2000, los administradores no tienen que instalar aplicaciones en cada equipo de la red. En su lugar, la aplicación se instala una vez en el servidor y los clientes tienen acceso automáticamente al paquete de software nuevo o actualizado.

Instalación de Servicios de Terminal Server

Para ejecutar los Servicios de Terminal Server, hay que instalar el programa servidor y el software de Cliente de Servicios de Terminal Server en los equipos cliente.

Los Servicios de Terminal Server se pueden instalar en el servidor durante la instalación de Windows 2000 server o puede instalarlos después junto con Licencias de Servicios de Terminal Server, mediante Agregar o quitar programas del Panel de Control.

Con esta última opción, puede seleccionar el Modo de servidor de aplicaciones o el Modo de administración remoto. Las dos diferencias principales, que ya hemos comentado, radican en que el Modo de administración remoto no existen requisitos de licencia y además sólo permite dos conexiones simultáneas.

Puede instalar Licencias de Servicios de Terminal Server con servicios de Terminal Server o bien instalarlo en otro equipo distinto. Al instalar Licencias de Servicios de Terminal Server, se especifica si el servidor el servidor de licencias atenderá al dominio o grupo de trabajo, o al bosque entero.

Cuando instalamos Servicios de Terminal Server, se agregan varios elementos al menú Herramientas administrativas, en función del servicio instalado:

- Creador de clientes de Servicios de terminal Server: permite crear los discos para instalar el software de cliente de Servicios de Terminal Server.
- Configuración de Servicios de Terminal Server: administra la configuración del protocolo y las opciones del servidor de Servicios de Terminal Server.
- Licencias de Servicios de Terminal Server: administra las licencias de acceso de cliente.
- Administrador de Servicios de Terminal Server: administra y supervisa sesiones y procesos en el servidor donde se ejecuta Servicios de Terminal Server.

Instalación del cliente de Servicios de Terminal Server

Existen dos métodos para instalar el cliente de Servicios de Terminal Server. Utilizar un conjunto de discos de instalación para instalarlo en el cliente, o utilizar una carpeta compartida para instalarlo a través de la red.

Creación de discos de instalación del cliente

Al instalar Servicios de Terminal Server, Windows 2000 incluye la herramienta administrativa Creador del Cliente de Servicios de Terminal Server, con la que puede crear los discos de instalación para el software del cliente. Una vez instalado el software en el cliente, éste podrá conectarse a un servidor en el que se ejecute Servicios de Terminal Server.

Para crear los discos de instalación del cliente, hay que seguir los siguientes pasos:

1. En el menú Herramientas administrativas, abrir Creador de cliente de Servicios de Terminal Server
2. Seleccionar el tipo de software Cliente de Servicios de Terminal Server que desea crear. Hay dos opciones: Serv. De Terminal Server para Windows de 16 bits (requiere 4 discos) y Serv. De Terminal Server para Windows de 32 bits (requiere 2 discos)
3. Introducir un disco en la unidad destino.
4. Después de copiar los archivos a los discos, cerrar el cuadro de diálogo Crear discos de instalación o hacer clic en Aceptar para crear más discos.

Instalación de software a través de la red

Los archivos de origen del Cliente de Servicios de Terminal Server se almacenan en la carpeta `%SYSTEMROOT%\system32\clients\tsclient`. La carpeta `Tsclient` contiene las subcarpetas `Net`, `Win16`, `Win32`. Para permitir que los usuarios tengan acceso al Cliente de Servicios de Terminal Server a través de la red y lo instalen en sus equipos, hay que compartir la carpeta `Tsclient`.

Acto seguido puede procederse a instalar el software cliente, siguiendo los pasos que se indican a continuación:

1. Conectar la unidad de red `\\servidor\Tsclient`.
2. Entrar en la carpeta `Win32`.
3. Ejecutar `Setup.exe`.
4. Se especifica y confirma el nombre de usuario y la organización.
5. Aceptar el contrato de licencia.
6. Aceptar la carpeta predeterminad donde irá a parar el software.
7. Especificar si deseamos instalar el software de cliente para todos los usuarios del equipo o sólo para el usuario actual.
8. El programa de instalación copiará los archivos apropiados de la carpeta compartida a la carpeta especificada del cliente.

Capítulo 7. El servicio DFS

Tabla de contenidos

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 que 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.

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 usuario 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 recursos 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 cuentan 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 2000 incluyen software de cliente DFS. Debe descargar e instalar este software en los equipos que ejecuten Microsoft Windows 95.

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.

Dentro de un árbol DFS, el administrador organiza los recursos compartidos, vínculos a recursos compartidos en los distintos servidores y vínculos a 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 2000 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.

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 2000 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_del_dominio\raiz_DFS
```

De este modo, el usuario no necesita recordar los nombres de los servidores donde están alojados realmente los recursos compartidos. Si creamos una raíz DFS de dominio, el usuario podrá localizar los recuros simplemente con el nombre del dominio y un nombre significativo a la raíz DFS.

Además, desde Windows 2000 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 UNCs 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 2000 escogerá el recurso al cual debe conectarse para dar acceso al usuario. Windows 2000 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.

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.

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.

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 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.

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 2000 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.

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 continuación 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".

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 2000, 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.

Sistema de Replicación de Archivos (FRS)

File Replication System, o FRS, es el sistema de replicación multimaestro de archivos y carpetas entre maquinas Windows 2000. El contenido de recursos NTFS puede así mantenerse redundante en múltiples servidores Windows 2000 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.

Funcionamiento de FRS

FRS se instala automáticamente en todos los servidores de Windows 2000. 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.

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.

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.

Capítulo 8. Servidores Web: Internet Information Server

Tabla de contenidos

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).

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 especifico 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 conteniendo modificadores de petición, información del cliente etc.. El servidor responde con una línea de estado que 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.

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.

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.

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 5.0 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.

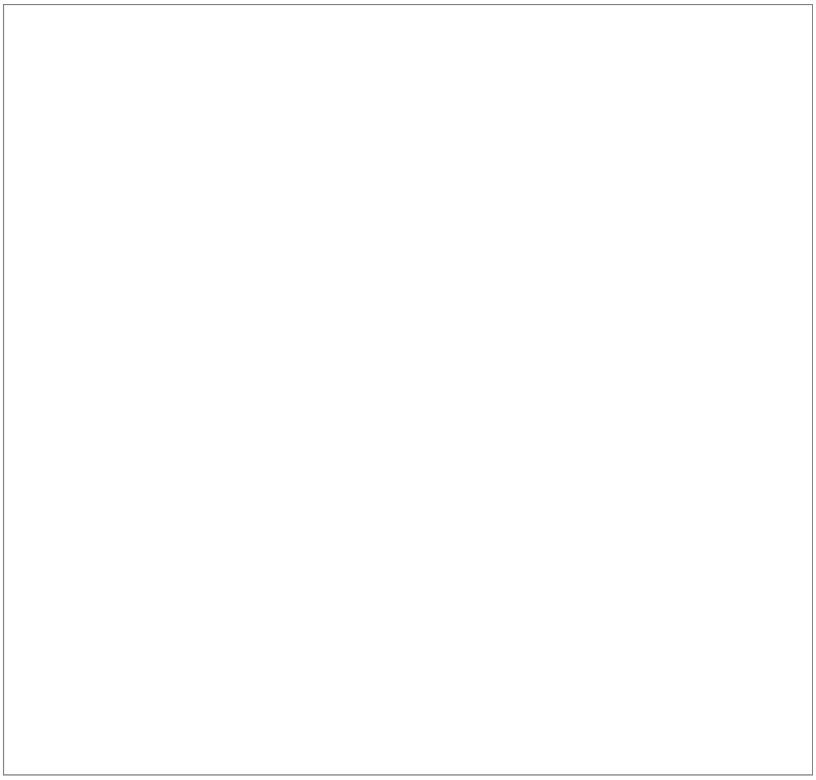
Además, la administración de la seguridad del servidor IIS es una tarea fácilmente ejecutable a base de asistentes para la seguridad. Se pueden definir permisos de acceso en directorios virtuales e incluso en archivos, de forma que el asistente actualizará los permisos NTFS para reflejar los cambios. Si se trabaja con entidades emisoras de certificados, es posible gestionar la lista de certificados de confianza (*CTL, Certificate Trust List*) con el asistente para CTL.

Instalación de IIS

Como cualquier otro software de Windows, la instalación de IIS 5.0 es tan sencilla como hacer un doble clic de ratón. Normalmente es uno de los componentes de Windows 2000 que viene seleccionado por defecto. Si no fuera así, en la propia instalación de Windows 2000 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 icono Agregar o Qitar 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



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 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 Interner snap-in

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 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.

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 item Permitir accesos anónimos a este sitio Web.

Figura 8.5. Directorio particular

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.

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 menu 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 lengueta, 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 2000 Profesional, existe una limitación de 10 conexiones. También podremos habilitar un regisro o log de los accesos y errores del sitio web.
- Operadores. Los operadores del sitio web son usuarios definidos en Windows 2000 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 un página concreta.
- Encabezados HTTP. Utilizaremos esta pestaña para configurar los valores que se eviarán al navegador en el encabezado de la página HTML.

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

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

Figura 8.10. Permisos del directorio virtual

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 5.0 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 proposito 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 2000 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, deberemos modificar las propiedades predeterminadas en la pestaña Seguridad de directorios.

Figura 8.11. Seguridad en directorios

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 5.0, 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.

- 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

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.

Figura 8.13. Restricciones de nombres de dominio y dirección IP

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 asi tener una copia del mismo. No hay que alarmarse debido a que IIS no ofrezca 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 icono 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 segridad, 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*

Programación Web en IIS 5.0

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 5.0 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.

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 consultador información del servidor.

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 VBasic 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.

Capítulo 9. Tutorial del lenguaje Python

Tabla de contenidos

"Hello World!"

El primer programa al que se enfrentará el desarrollador más avanzado cuando empieza con un nuevo lenguaje, será sin ninguna duda el famoso ¡ Hola Mundo !

```
>>> print 'Hello World!'
Hello World!
```

La sentencia **print** se utiliza en python para mostrar la salida por la pantalla. Aquellos que estén familiarizados con C, deben saber que funciona de forma parecida a la sentencia **printf()**.

Un apunte final, la sentencia **print** junto con el operador de formateo de cadenas (%) se comporta exactamente igual a la sentencia **printf()** de C.

```
>>> print "%s es el número %d!" % ("Python", 1)
Python es el número 1!
```

Entrada de Usuario. raw_input()

La forma más fácil de obtener la entrada de datos de un usuario por pantalla, es utilizando la sentencia **raw_input()**.

```
>>> user = raw_input('Introduce tu login: ')
Introduce tu login: root
>>> print 'Tu login es:', user
Tu login es: root
```

El ejemplo anterior espera que la entrada sea una cadena, pero si queremos introducir un valor numérico y que sea tratado como tal, habrá que convertirlo previamente.

```
>>> num = raw_input('Introduce un número: ')
Introduce un número: 1024
>>> print 'El doble del número es: %d' % (int(num) * 2)
El doble del número es: 2048
```

La función **int()** convierte la variable de tipo *string* en un entero.

Operadores

- **Operadores matemáticos**: + - * / % **
- **Operadores de comparación**: < <= > >= == != <>
- **Operadores lógicos**: and or not

Variables

Las reglas que rigen el comportamiento de las variables en Python son muy parecidas a las de otros lenguajes. Las variables son simples identificadores que deben empezar siembre por un carácter alfabético, en mayúsculas o minúsculas o el símbolo _ (guión bajo), seguidos de cualquier carácter alfanumérico.

Hay que recalcar que Python distingue entre mayúsculas y minúsculas.

Python es un lenguaje de tipos dinámicos, lo cual significa que no hay necesidad de declarar el tipo de una variable. El tipo se definirá en el momento de la asignación de la variable.

```
>>> contador = 0
>>> millas = 1000.0
>>> nombre = 'Fernando'
>>> contador = contador + 1
>>> kms = 1.609 * millas
>>> print '%f millas es lo mismo que %f km' % (millas, kms)
1000.000000 millas es lo mismo que 1609.000000 km
```

Números

Python soporta cuatro tipos numéricos:

1. Enteros con signo (*int*).
2. Enteros largos (*long*) que pueden ser representados también en octal o hexadecimal.
3. Reales en coma flotante (*float*)
4. Números complejos (*complex*)

Los tipos realmente interesantes en Python por las particularidades que comportan son el tipo *long* y el tipo *complex*.

El tipo long es superior al archiconocido long de C, ya que en Python no tiene límite de capacidad, solamente el que le imponga la memoria virtual del sistema. Sería más parecido a los números definidos en Java con la clase BigInteger.

En cuanto al soporte de números complejos, Python es el único lenguaje que nativamente soporta este tipo de datos.

Secuencias (*strings, listas y tuplas*)

Las secuencias son un tipo de datos cuyos elementos están ordenados y pueden ser accedidos vía un índice.

Todos los tipos de secuencias comparten el mismo modelo de acceso a sus elementos. Para acceder a un elemento en concreto se utiliza la siguiente nomenclatura *seq[i]*. Dada una variable de tipo secuencia denominada seq, accedemos al elemento que ocupa la posicion i. El esquema de numeración utilizado empieza en el 0 y finaliza en el valor que defina la longitud de la secuencia menos 1.

Varios elementos (substrings) pueden ser obtenidos a la vez utilizando el operador slice (trozo). La sintaxis para obtener un grupo de elementos es la siguiente:

```
secuencia[indice_inicial : indice_final]
```

Con esta sintaxis podemos obtener un trozo (slice) empezando en el elemento definido por el indice_inicial y terminando en el elemento anterior al definido por el indice_final.

```
>>> cadena='Hola Mundo!'
>>> print cadena[0:4]
Hola
```

Parece algo confuso pero la mejor forma de recordar como funciona el operador slice es pensar que los indices apuntan realmente entre los caracteres.

```
 +---+---+---+---+---+
 | H | e | l | p | A |
 +---+---+---+---+---+
 0   1   2   3   4   5
-5  -4  -3  -2  -1
```

En la siguiente tabla se muestra una lista de operadores que se pueden utilizar con todos los tipos de secuencias:

Tabla 9.1. Operadores de secuencias

secuencia[index]	elemento situado en el índice index de la secuencia
secuencia[ind1:ind2]	elementos desde el índice ind1 hasta el índice ind2
secuencia * n	la secuencia se repite n veces
secuencia1 + secuencia2	concatena las secuencias secuencia1 y secuencia2
objeto in secuencia	comprueba si objeto es un miembro de secuencia

objeto not in secuencia	comprueba si objeto no es un miembro de secuencia

La siguiente tabla muestra algunas de las funciones predefinidas que se pueden aplicar a las secuencias.

Tabla 9.2. Funciones Pre-Definidas

list (secuencia)	convierte la secuencia a un tipo lista
str (objeto)	convierte el objeto a un tipo string
tuple (secuencia)	convierte la secuencia a un tipo tupla
len (secuencia)	devuelve la longitud (numero de elementos) de la secuencia
max (secuencia)	devuelve el elemento mas grande de la secuencia
min (secuencia)	devuelve el elemento menor de la secuencia

Los diferentes tipos de secuencias se exponen a continuación.

Strings

Para Python, las cadenas (strings) son un conjunto contiguo de caracteres encerrados entre simples o dobles comillas.

```
>>> cadena='Hola Mundo!'
>>> print cadena
Hola Mundo!
```

Los strings son inmutables, no se puede alterar su valor a no ser que sean copiados a otro objeto string.

Los métodos y funciones aplicables al tipo de objeto string se encuentran definidos en el módulo string

```
>>> import string
>>> cadena.upper()
'HOLA MUNDO!'
```

La línea i**mport string** permite acceder a todos los métodos y atributos disponibles para un tipo de dato string, siendo la línea **cadena.upper()** la forma de invocar al método *upper* sobre el objeto string denominado *cadena*. Como resultado obtenemos el string en mayúsculas.

La siguiente tabla muestra algunos de los métodos disponibles en el módulo string:

Tabla 9.3. Métodos del módulo string

find(sub[, start[, end]])	devuelve el índice menor donde se encuentra el substring *sub* dentro del string
isalnum()	devuelve verdadero si todos los caracteres en el string son alfanuméricos y existe al menos uno.
isdigit()	devuelve verdadero si todos los caracteres en el string son dígitos y existe al menos uno.
lower()	devuelve una copia del string convertido a minúsculas.
split([sep [,maxsplit]])	devuelve una lista de elementos del string utilizando como separador *sep*.

Listas y Tuplas

Python posee varios tipos de datos para agrupar de una forma fácil diferentes valores. El tipo de dato más versátil es la lista. Una lista es una colección de elementos separados por comas y encerrados entre paréntesis. Los elementos de una lista no tienen porque ser del mismo tipo.

```
>>> lista = [ 1,'dos',3,'cuatro']
>>> print lista
[1, 'dos', 3, 'cuatro']
```

Como ocurría con el tipo de datos string, los índices de una lista empiezan en el 0, y pueden ser troceadas (sliced), concatenadas ...

```
>>> lista [0]
1
>>> lista [3]
'cuatro'
>>> lista [1:-1]
['dos', 3]
>>> lista + [5,'seis']
[1, 'dos', 3, 'cuatro', 5, 'seis']
```

A diferencia de los strings, que por definición eran inmutables, en una lista podemos cambiar el valor de un elemento individual.

```
>>> lista
[1, 'dos', 3, 'cuatro']
>>> lista [2] = 'tres'
>>> lista
[1, 'dos', 'tres', 'cuatro']
```

Es posible también crear listas anidadas (listas cuyos elementos pueden ser otras listas)

```
>>> lista1 = [2, 3]
>>> lista2 = [1, lista1, 4]
>>> len(lista2)
3
>>> lista2
[1, [2, 3], 4]
```

Diccionarios

El tipo de dato *diccionario* de Python es parecido al que se puede encontrar en otros lenguajes bajo el nombre de *Arrays Asociativos*. A diferencia de las secuencias donde los índices son números, los diccionarios están indexados por claves. Las claves solo podrán ser de algún tipo de dato inmutable (números y strings).

Un diccionario consiste por tanto en un conjunto de pares clave-valor, donde las claves son inmutables, mientras que los valores pueden ser de cualquier tipo.

Un diccionario se crea encerrando entre llaves ({}) una lista de pares clave-valor.

```
>>> usuario = {'login': 'fferrer', 'uid': 501 }
>>> usuario
```

```
{'login': 'fferrer', 'uid': 501}
>>> usuario ['login']
'fferrer'
>>> usuario ['uid']
501
```

Las operaciones habituales con diccionarios son la de almacenar y extraer algún valor con su correspondiente clave, pero también es posible eliminar algún elemento con la función **del()**.

A la hora de recorrer un diccionario será importante tener una lista de sus claves para poder acceder a los valores. El método **keys()** aplicado a un objeto de tipo diccionario, devolverá dicha lista.

```
>>> usuario
{'login': 'fferrer', 'uid': 501}
>>> usuario.keys()
['login', 'uid']
>>> del usuario ['uid']
>>> usuario
{'login': 'fferrer'}
```

En la siguiente tabla se exponen algunos de los principales métodos que se pueden usar con objetos del tipo diccionario.

Tabla 9.4. Métodos Pre-definidos de un diccionario

dict.clear()	elimina todos los elementos del diccionario *dict*
dict.get(clave, [default])	devuelve el valor de la clave o lo que definamos por defecto si la clave no se encuentra en el diccionario
dict.has_key(clave)	devuelve 1 si la clave se encuentra en el diccionario. En cualquier otro caso devuelve 0.
dict.items()	devuelve una lista de pares de tuplas clave-valor.
dict.keys()	devuelve una lista de claves
dict.values()	devuelve la lista de valores
dict.update(dict2)	añade los pares clave-valor del diccionario *dict2* al diccionario *dic*

Bloques de código

Una de las primeras cosas que sorprende cuando se empieza a utilizar Python es la forma en que este lenguaje delimita los bloques de código. No existen las llaves ({}) ni sentencias begin-end para encerrar el código, en su lugar un bloque de código viene delimitado por la identación.

```
>>> def f1 (a):
...     print a
...
>>> f1('Hola')
Hola
```

A parte de sorprender, lo que deja claro esta alternativa es que los programas en Python son legibles por

cualquiera, lo cual a la larga es muy cómodo.

Sentencia if

La sintaxis de la sentencia if es la siguiente:

```
if expression1:
     if_bloque
elif expression2:
     elif_bloque
else:
     else_bloque
```

La expresión debe devolver un valor distinto de cero o verdadero para que se ejecute el if.

Otra cosa que también puede sorprender es que no existe una sentencia **case**, pero vista la sintaxis de la sentencia **if**, anidando diferentes elif podemos conseguir el mismo resultado.

Bucle while

La sintaxis y funcionamiento del bucle while es similar a la de la sentencia if:

```
while expression:
      while_bloque
```

El bloque while se ejecutará indefinidamente hasta que la expresión sea 0 o falso. De nuevo resaltar la identación para definir el bloque de código.

Bucle for

La sentencia **for** de Python es diferente a la de otros lenguajes. Solamente itera sobre una lista de elementos de una secuencia. En otros lenguajes (c o Perl) se puede iterar sobre una progresion aritmetica también.

La sintaxis es la siguiente:

```
for elemento in secuencia:
      bloque_for
```

Un ejemplo concreto de utilización:

```
>>> for i in [1,2,3,4]:
...     print i
...
1
2
3
```

si queremos tener un bucle **for** que itere sobre una progresión aritmética, podemos utilizar la función range() que devuelve una lista de números:

```
>>> for i in range(1,5):
...     print i
...
1
2
3
4
```

Definición de funciones

La palabra clave **def** es utilizada para la definición de una función. Debe de ir seguida del nombre de la función y la lista de parámetros entre paréntesis. Python no distingue entre procedimientos y funciones. Si es una función, esta devolverá algún tipo de valor con la sentencia **return**.

```
def nombre_funcion (param1, param2 ...):
     bloque_funcion
```

Los parámetros de una función pueden tener valores por defecto, de forma que cuando se invoque a la función no tengamos que especificarlos todos. En este último caso habrá que nominar los parámetros, para saber cuales toman un valor y cuales su defecto.

```
>>> def tabla_mult(p1=1):
...     for i in range(11):
...             print i * p1
…
```

Módulos

Los módulos son el mecanismo que utiliza Python para organizar trozos de código que luego puedan ser reutilizables. Los módulos pueden contener código ejecutable, clases o funciones.

Cuando se crea un fichero fuente de Python, el nombre del módulo será el nombre del fichero pero sin la extensión *.py*. Una vez que el módulo ha sido creado, la forma de utilizar sus componentes es invocando la orden **import** *nombre_módulo*. Y para hacer uso de las funciones o clases definidas en el módulo una vez que este ha sido importado, se utiliza la sintaxis típica de **modulo.funcion()**

A continuación se presenta el programa inicial Hola Mundo! pero utilizando las funciones de salida del módulo **sys**.

```
>>> import sys
>>> sys.stdout.write('Hello World!\n')
Hello World!
```

Ficheros

El soporte de acceso a ficheros es uno de los componentes más importantes de cualquier lenguaje. En Python existe una función pre-definida denominada **open** que permite abrir un fichero.

```
handle = open( file_name, access_mode='r')
```

La variable `file_name` contiene el nombre del fichero que deseamos abrir, mientras que el parámetro *acces_mode* define el modo en que queremos abrir el fichero. Estos modos pueden ser **r**(*lectura*), **w**(*escritura*), **a**(*añadir*), **b**(*binario*), **r+**(*lectura/escritura*)

Para leer los contenidos del fichero tenemos varios métodos. **readline()** leerá una línea en cada invocación del método, mientras que **readlines()** leerá todo el fichero generando una lista de líneas.

```
file = open(filename, 'r')
allLines = file.readlines()
file.close()
for eachLine in allLines:
   print eachLine,
```

A continuación se presenta una tabla con los métodos más utilizados sobre ficheros:

Tabla 9.5. Métodos del objeto Fichero

file.close()	cierra el fichero
file.fileno()	devuelve un entero representando el descriptor de fichero
file.flush()	descarga el buffer interno al fichero
file.read (size=-1)	lee todos los bytes del fichero o los especificados en el parámetro size
file.readline()	lee una línea del fichero incluyendo un salto de línea \n
file.readlines()	lee todas las líneas del fichero en un lista
file.seek(off, whence)	se mueve a una posición dentro del fichero off bytes desde lo que marque la variable whence (0= principio de fichero, 1=posición actual, 2=final de fichero)
file.write(str)	escribe la cadena str al fichero
file.writelines(list)	escribe la lista de cadenas al fichero

Errores y excepciones

Los errores de sintaxis se detectan en el proceso de compilación, pero Python puede detectar errores durante la ejecución del programa. Cuando se produce un error de ejecución, Python genera (*raises*) una excepción.

Para añadir este tipo de detección de errores, denominado manejo de excepciones, hay que encerrar nuestro código entre las clausulas **try-except**. El bloque que define la sentencia try será el código de nuestro programa en si. El código que viene detrás de la clausula except será el código que se ejecuta si se produjo alguna excepción. La sintaxis es la siguiente.

```
try:
     bloque_de_código
except Error:
     acción_contra_el_error
```

Vimos al principio de este capítulo como solicitar del usuario que introduzca un número y convertirlo a entero, ya que la entrada estandar siempre era un string. ¿ Pero que pasa si el usuario introduce una cadena ? Una pequeña modificación a nuestro ejemplo manejando la excepcion nos ayudará.

```
>>> while True:
...     try:
...         x = int(raw_input("Introduce un número: "))
...         break
...     except ValueError:
...         print "Oops! No es un número válido. Intentalo de nuevo..."
...
```

Si hubieramos ejecutado simplemente la sentencia que nos pide introducir el número y este no es correcto, esta hubiera fallado abortando el programa.

```
>>> x = int(raw_input("Introduce un número: "))
Introduce un número: aaaa
Traceback (most recent call last):
  File "<stdin>", line 1, in ?
ValueError: invalid literal for int(): aaaa
```

Por tanto se ve claramente las posibilidades que tiene el manejo de excepciones para acotar firmemente nuestro programa.

Capítulo 10. Seguridad en Red

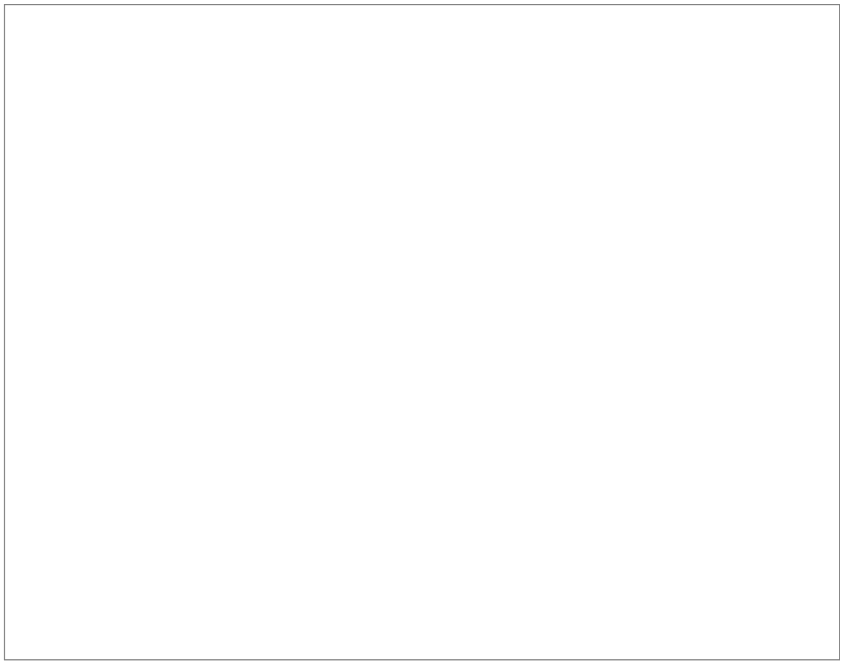
Tabla de contenidos

Filtrado TCP/IP

Windows 2000 posee capacidades de filtrado de paquetes TCP/IP de forma muy básica. Este componente de software le permite al administrador definir una política que permita o deniegue cierto tráfico IP hacia el host local para cada interfaz de red a un puerto en concreto.

Para acceder a las capacidades de filtrado TCP/IP, haga clic sobre **Mis Sitios de Red** con el botón derecho del ratón el cual abrirá la carpeta que contiene la lista de conexiones de red existentes. Sobre **conexión de área local** y con el botón derecho de nuevo elija **Propiedades**. En la ventana de *Propiedades* de *conexión de área local* haga doble clic con el ratón en **Protocolo Internet(TCP/IP)**, clic en **Avanzadas** y escoja la lengüeta **Opciones**. En **configuración opcional**, haga clic sobre **Filtrado TCP/IP**.

Figura 10.1. Filtrado TCP/IP



Como se puede observar la ventana de diálogo permite controlar que puertos TCP y UDP tienen permitido el tráfico.

Visto el escaso margen de maniobra que permite la herramienta, el administrador se ve tentado a

utilizar otras como puede ser el servicio RRAS (Routing and Remote Access) por sus capacidades de filtrado. El problema es que los filtros solo funcionan si el subsistema RRAS se está ejecutando. Por tanto si el servicio de enrutamiento está parado porque se ha cometido algun error o es vulnerable a algún ataque, el sistema se encontrará desprotegido.

La principal desventaja del Filtrado TCP/IP es que solo controla el tráfico entrante y además el administrador no puede permitir que ciertos hosts accedan a un servicio.

Si se quiere mayor flexibilidad y un control más al detalle, una opción sería una buena política de filtros IPSEC como ocurría con RRAS, IPSec tiene la desventaja de depender de un servicio en modo usuario denominado Agente de Políticas IPSec para poder funcionar. Sin embargo, es posible combinar el filtrado TCP/IP con la seguridad de IPSec.

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** (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 enrutadores, 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 2000 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.

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 correcta 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.

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.
- 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.

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 2000 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.

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 configuración 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 trónfico 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.

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 contener 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 especónficas.
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.
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 2000 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 2000 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.

Configuración de un servidor VPN

Cuando se configura una conexión entrante en un servidor de acceso remoto, hay que habilitar el puerto a través del que los clientes se van a conectar al servidor. El administrador puede habilitar puertos para conexiones VPN, conexiones por módem y conexiones directas por cable.

Si el el equipo no es servidor ni miembro de un dominio, las conexiones entrantes se configuran en Windows 2000 con el Asistente para conexión de red que se utiliza para las conexiones salientes.

Sin embargo, cuando el equipo es servidor y miembro de un dominio, para configurar conexiones entrantes tiene que utilizar la herramienta Enrutamiento y acceso remoto. El uso de esta herramienta puede ayudar a configurar redes privadas virtuales y conjuntos de módems en un servidor de acceso remoto.

El Asistente para la instalación del servidor de Enrutamiento y acceso remoto se utiliza para configurar tipos de servidores de acceso remoto comunes, como servidores de redes privadas virtuales.

Para configurar e iniciar un servidor de red privada virtual:

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 Conrigurar 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.

La primera vez que se inicia un servidor VPN, Windows 2000 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 Conrigurar.
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.

Apéndice A. Nota Legal