3

Protección local en Windows Server 2008

Indice

3.1. Concepto de usuario

Como muchos otros sistemas operativos, Windows Server 2008 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 Server 2008 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 Server 2008 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 Server 2008 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 Server 2008 del mundo (son identificadores únicos). Windows Server 2008 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 Server 2008, existen de entrada las cuentas de dos usuarios integrados (*built-in users*): el Administrador y el Invitado. El primero es un usuario especial, el único que en principio posee lo que se denominan derechos administrativos en el sistema. Es decir, tiene la potestad de administrar el sistema en todos aquellos aspectos en que éste es configurable: usuarios, grupos de usuarios, contraseñas, recursos, derechos, etc. La cuenta de Administrador no puede ser borrada ni desactivada. Por su parte, la cuenta de Invitado es la que utilizan normalmente aquellas personas que no tienen un usuario propio para acceder al sistema. Habitualmente esta cuenta no tiene contraseña asignada, puesto que se supone que el nivel de privilegios asociado a ella es mínimo. En cualquier caso, el Administrador puede desactivarla si lo considera oportuno.

3.2. Grupos de Usuarios

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

La administración de la protección del sistema mediante grupos de usuarios es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales, ya que un usuario puede pertenecer a tantos grupos como sea necesario, obteniendo implícitamente la *suma* de los permisos asignados a todos ellos. 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 gru-

pos, esta operación sería tan sencilla como cambiar al usuario de un grupo a otro. Por ello, en Windows Server 2008 se recomienda que los permisos se asignen en base a *grupos*, y no en base a usuarios individuales.

Al igual que existen usuarios integrados, en todo sistema Server 2008 existen una serie de grupos integrados (*built-in groups*): Administradores, Operadores de Copia, Usuarios Avanzados, Usuarios, e Invitados. El grupo Administradores recoge a todos aquellos usuarios que deban poseer derechos administrativos completos. Inicialmente posee un solo usuario, el Administrador. De igual forma, el grupo Invitados posee al Invitado como único miembro. Los otros tres grupos están vacíos inicialmente. Su uso es el siguiente:

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

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

Finalmente, Windows Server 2008 define una serie de grupos especiales, cuyos (usuarios) miembros no se establecen de forma manual, sino que son determinados de forma dinámica y automática por el sistema. Estos grupos se denominan genéricamente identidades especiales (*special identities*) y se utilizan normalmente para facilitar la labor de establecer la protección del sistema. De entre estos grupos, destacan:

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

nes anónimas (sin aportar usuario y contraseña).

- **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".

3.3. El modelo de protección

El modelo de protección de Windows Server 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 Server 2008 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 Server 2008. Para determinar qué usuarios poseen qué derechos, cada derecho posee una lista donde se especifican los grupos/usuarios que tienen concedido este derecho.

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

En los apartados siguientes se detallan los atributos de protección de los procesos de usuario (Sección 3.4, “Atributos de protección de los procesos”), los derechos que pueden establecerse en el sistema (Sección 3.5, “Derechos de usuario”) y los atributos de protección que poseen los recursos (Sección 3.6, “Atributos de protección de los recursos”). La Sección 3.7, “Reglas de protección” establece las reglas concretas que definen el control de acceso de los procesos a los recursos.

3.4. Atributos de protección de los procesos

Cuando un usuario es autorizado a conectarse interactivamente a un sistema Windows Server 2008, el sistema construye para él una acreditación denominada *Secu-*

rity Access Token o SAT. Esta acreditación contiene la información de protección del usuario, y Windows Server 2008 la incluye en los procesos que crea para dicho usuario. De esta forma, los *atributos de protección* del usuario están presentes en cada proceso del usuario, y se utilizan para controlar los accesos que el proceso realiza a los recursos del sistema en nombre de dicho usuario.

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

1. **SID**. El identificador único del usuario.
2. **SIDs de sus grupos**. Lista de los SIDs de los grupos a los que pertenece el usuario.
3. **Derechos**. Lista de derechos del usuario. Esta lista se construye mediante la inclusión de todos los derechos que el usuario tiene otorgados por sí mismo o por los grupos a los que pertenece (ver Sección 3.5, "Derechos de usuario").

Esta forma de construir la acreditación introduce ya una de las máximas de la protección de Windows Server 2008: el nivel de acceso de un usuario incluye implícitamente los niveles de los grupos a los que pertenece.

3.5. Derechos de usuario

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

Windows Server 2008 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 3.1, "Principales derechos de usuario en Windows Server 2008" presenta los derechos más destacados de cada tipo, junto con su descripción.

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

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

Tabla 3.1. Principales derechos de usuario en Windows Server 2008

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.).

3.5.1. Otras directivas de seguridad

En Windows Server 2008, los derechos son un tipo de *directivas de seguridad*. En este sentido, Windows Server 2008 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:

1. **Cuentas**. En este apartado podemos establecer cuál es la *política de cuentas* o de contraseñas que sigue el equipo para sus usuarios locales. Dentro de este apartado se pueden distinguir reglas en tres epígrafes: *Contraseñas*, *Bloqueo* y *Kerberos*. Entre ellas, las dos primeras hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión local.

2. **Directiva local**. Dentro de este apartado se encuentra, por una parte, la *Auditoría* del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, inicios de sesión local). Por otra parte, este apartado incluye los *derechos y privilegios* que acabamos de explicar.

3. **Claves públicas**. Este apartado permite administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

3.6. Atributos de protección de los recursos

En un sistema de archivos NTFS de Windows Server 2008, cada carpeta o archivo posee los siguientes atributos de protección:

1. **SID del propietario**. Inicialmente, el propietario es siempre el usuario que ha creado el archivo o carpeta, aunque este atributo puede ser luego modificado (esto se explica más adelante).

2. **Lista de control de acceso de protección**. Esta lista incluye los *permisos* que los usuarios tienen sobre el archivo o carpeta. La lista puede contener un número indefinido de entradas, de forma que cada una de ellas concede o deniega un conjunto concreto de permisos a un usuario o grupo conocido por el sistema. Por tanto, Windows Server 2008 permite definir multitud de niveles de acceso a cada objeto del sistema de archivos, cada uno de los cuales puede ser *positivo* (se otorga un permiso) o *negativo* (se deniega un permiso).

3. **Lista de control de acceso de seguridad**. Esta segunda lista se utiliza para definir qué acciones sobre un archivo o carpeta tiene que *auditar* el sistema. El proceso de auditoría supone la anotación en el *registro del sistema* de las acciones que los usuarios realizan sobre archivos o carpetas (las entradas de este regis-

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

La lista de control de acceso de protección se divide realmente en dos listas, cada una de ellas denominada *Discretionary Access Control List* (lista de control de acceso discrecional) o DACL. Cada elemento de una DACL se denomina *Access Control Entry* (entrada de control de acceso) o ACE. Cada entrada liga a un SID de usuario o grupo con la concesión o denegación de un permiso concreto (o conjunto de permisos), tal como se ha descrito arriba. Los diferentes permisos que se pueden asignar a usuarios o grupos en Windows Server 2008 se explican en la Sección 3.6.2, "Permisos estándar e individuales".

El hecho de que cada archivo o carpeta tenga dos DACL en vez de una tiene que ver con el mecanismo de la *herencia de permisos* que incorpora Windows Server 2008: 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 Server). 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.

3.6.1. Asociación de permisos a recursos

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

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

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

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

- **Copiar** un archivo o carpeta a otra ubicación se considera una creación, y por tanto el archivo copiado recibe una lista de permisos explícitos vacía y se activa la herencia de la carpeta padre correspondiente a la nueva ubicación.

- **Mover** un archivo distingue dos casos: si movemos una carpeta o archivo a otra ubicación dentro del mismo 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).

3.6.2. Permisos estándar e individuales

Windows Server 2008 distingue entre los *permisos estándar* de carpetas y los de archivos. Como ocurría en versiones previas de Windows NT, los permisos estándar son combinaciones predefinidas de *permisos individuales*, que son aquellos que controlan cada una de las acciones individuales que se pueden realizar sobre carpetas y archivos. La existencia de estas combinaciones predefinidas es el resultado de una agrupación "lógica" de los permisos individuales para facilitar la labor del administrador (y de cada usuario cuando administra los permisos de sus archivos). Por este motivo, los permisos estándar se conocen también como "plantillas de permisos".

En la Tabla 3.2, "Permisos estándar sobre carpetas y archivos en Windows Server 2008" 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 Server 2008 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 3.2. Permisos estándar sobre carpetas y archivos en Windows Server 2008

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

Cuando la asignación de permisos que queremos realizar no se ajusta al comportamiento de ninguno de los permisos estándar, debemos entonces ir directamente a asignar permisos individuales. La Tabla 3.3, "Permisos individuales en Windows

Server 2008" muestra cuáles son los permisos individuales en Windows Server 2008, junto con su significado concreto. También en este caso debe entenderse que cada permiso puede ser concedido de forma positiva o negativa.

Tabla 3.3. Permisos individuales en Windows Server 2008

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

Finalmente, la Tabla 3.4, "Correspondencia entre permisos estándar e individuales en Windows Server 2008" 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 3.4. Correspondencia entre permisos estándar e individuales en Windows Server 2008

Permiso	C.Total	Modif.	L.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	+					

3.6.3. Modificación de atributos de protección

Las reglas que plantea Windows Server 2008 para controlar quién puede modificar los atributos de protección de un recurso están completamente integradas en su modelo de protección, basado en los *permisos* y los *derechos* del usuario implicado en la modificación. Este modelo es diferente del que plantean los sistemas UNIX, cuyas reglas en este sentido son independientes de los permisos que posea el propio recurso.

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

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

   Asimismo, cualquier usuario que tenga concedido el derecho `Tomar posesión de archivos y otros objetos` puede convertirse en propietario de

cualquier recurso del sistema. Por defecto, este derecho solamente lo tiene concedido el grupo `Administradores`.

Finalmente, Windows Server 2008 ha introducido otra posibilidad: el derecho de usuario `Restaurar archivos y carpetas` lleva asociado la posibilidad de *asignar* la posesión de cualquier archivo y carpeta del sistema a cualquier usuario, sin tener que tomar posesión en nombre propio. Por defecto, sólo los grupos `Administradores` y `Operadores de copia` tienen este derecho concedido.

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

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

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

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

3.7. Reglas de protección

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

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

- Los permisos en Windows Server 2008 son acumulativos: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SIDs de su acreditación (ver Sección 3.4, "Atributos de protección de los procesos"), es decir, los permisos del usuario y de todos los grupos a los que pertenece.

- La ausencia un cierto permiso sobre un objeto supone implícitamente la imposibilidad de realizar la acción correspondiente sobre el objeto.

- Si se produce un conflicto en la comprobación de los permisos, los permisos negativos tienen prioridad sobre los positivos, y los permisos explícitos tienen prioridad sobre los heredados.

Estas reglas son más fáciles de recordar si se conoce el algoritmo que sigue Windows Server 2008 para conceder o denegar una acción concreta sobre un archivo o directorio concreto. Para ello, el sistema explora secuencialmente las entradas de las DACLs de protección de dicho objeto hasta que se cumple alguna de las condiciones siguientes:

1. Cada permiso involucrado en la acción solicitada está concedido explícitamente al SID del usuario o de algún grupo al que el usuario pertenece. En ese caso, se permite la acción.

2. Alguno de los permisos involucrados está explícitamente denegado para el SID del usuario o para alguno de sus grupos. En este caso, se deniega la acción.

3. La lista (DACL) ha sido explorada completamente y no se ha encontrado una entrada (ni positiva ni negativa) correspondiente a alguno de los permisos involucrados en la acción para el SID del usuario o sus grupos. En este caso, se deniega la acción.

Este algoritmo realmente produce el comportamiento descrito por las reglas anteriores debido al orden en que Windows Server 2008 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.