CF GRADO SUPERIOR

CICLOS FORMATIVOS

R.D. 1538/2006

Administración de Sistemas Operativos

JULIO GÓMEZ LÓPEZ
OSCAR DAVID GÓMEZ LÓPEZ

Ra-Ma®

www.ra-ma.es/cf

Administración de Sistemas Operativos

JULIO GÓMEZ LÓPEZ
OSCAR DAVID GÓMEZ LÓPEZ

[redacted]

Ra-Ma®

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS
© Julio Gómez López, Oscar David Gómez López
© De la edición: Ra-Ma 2011

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. RA-MA ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

RA-MA es marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, RA-MA Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de RA-MA; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica.

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: **www.ra-ma.es** y **www.ra-ma.com**
ISBN: 978-84-9964-091-4
Depósito Legal: M-24.445-2011
Maquetación: Antonio García Tomé
Diseño de Portada: Antonio García Tomé
Filmación e Impresión: Closas-Orcoyen, S.L.
Impreso en España

Índice

INTRODUCCIÓN **9**

BLOQUE I. TEORÍA **11**

CAPÍTULO 1. ASPECTOS BÁSICOS **13**
1.1 TAREAS DEL ADMINISTRADOR 14
1.2 HARDWARE DEL SERVIDOR 15
1.2.1 CPD 15
1.2.2 Sistema de Rack 17
1.2.3 Servidores 18
1.2.4 Sistemas RAID 21
1.3 SOFTWARE DEL SERVIDOR 24
RESUMEN DEL CAPÍTULO 25
EJERCICIOS PROPUESTOS 26
TEST DE CONOCIMIENTOS 26

CAPÍTULO 2. INTEGRACIÓN DE SISTEMAS **27**
2.1 INTRODUCCIÓN 28
2.2 ESQUEMAS BÁSICOS DE RED 28
2.2.1 Esquema de red básico 29
2.2.2 Esquema de red con una zona neutra 30
2.3 INTEGRACIÓN DE SISTEMAS 34
2.3.1 Red 35
2.3.2 Datos 35
2.3.3 Servicios 36
2.4 SUPUESTO PRÁCTICO 38
2.4.1 Descripción 38
2.4.2 Diseño del sistema 39
RESUMEN DEL CAPÍTULO 43
EJERCICIOS PROPUESTOS 43
TEST DE CONOCIMIENTOS 44

BLOQUE II. WINDOWS 2008 ..... **45**

CAPÍTULO 3. INSTALACIÓN Y CONFIGURACIÓN **47**
3.1 PREPARACIÓN DEL SISTEMA 48
3.1.1 Primeros pasos 49
3.1.2 Instalación 50
3.2 AGREGAR O QUITAR FUNCIONES Y CARACTERÍSTICAS DEL SERVIDOR 53

RESUMEN DEL CAPÍTULO 55
EJERCICIOS PROPUESTOS 55
TEST DE CONOCIMIENTOS 55

CAPÍTULO 4. PUESTA EN MARCHA DEL SISTEMA 57
4.1 ADMINISTRACIÓN DE USUARIOS 58
4.1.1 Usuarios 58
4.1.2 El administrador de usuarios 59
4.1.3 Directivas de seguridad local 64
4.2 SISTEMA DE FICHEROS 67
4.2.1 Administrador de discos 67
4.2.2 Cuotas de disco 70
4.3 PERMISOS 72

RESUMEN DEL CAPÍTULO 74
EJERCICIOS PROPUESTOS 74
TEST DE CONOCIMIENTOS 75

CAPÍTULO 5. ADMINISTRACIÓN BÁSICA DEL SISTEMA 77
5.1 ARRANQUE Y PARADA 78
5.1.1 Configuración del gestor de arranque del SO 78
5.1.2 Servicios del sistema 79
5.1.3 Procesos 81
5.1.4 Programación de tareas 82
5.1.5 Proceso de parada del sistema 83
5.2 MONITORIZACIÓN DEL SISTEMA 85
5.2.1 Monitor de confiabilidad y rendimiento 85
5.2.2 Visor de eventos 89
5.3 COPIAS DE SEGURIDAD 91
5.3.1 Realizar una copia de seguridad 93
5.3.2 Recuperar una copia de seguridad 95
5.3.3 Configurar opciones de rendimiento 96

RESUMEN DEL CAPÍTULO 98
EJERCICIOS PROPUESTOS 98
TEST DE CONOCIMIENTOS 98

CAPÍTULO 6. ADMINISTRACIÓN DE LA RED 99
6.1 ESQUEMA BÁSICO DE RED 100
6.1.1 Configuración de la red 101
6.1.2 Enrutamiento 104
6.1.3 Firewall de Windows 105
6.1.4 DHCP 108
6.2 TERMINAL SERVER 113
6.2.1 Escritorio remoto 113
6.2.2 Servidor de aplicaciones 114
6.2.3 Cliente de Terminal Server 117

6.3 WINDOWS SERVER UPDATE SERVICES 120
6.3.1 Instalación 120
6.3.2 Cliente 121
6.3.3 Administración 122
RESUMEN DEL CAPÍTULO 126
EJERCICIOS PROPUESTOS 126
TEST DE CONOCIMIENTOS 126

CAPÍTULO 7. SERVIDORES DE IMPRESIÓN Y DE ARCHIVOS 127
7.1 COMPARTIR ARCHIVOS E IMPRESORAS 128
7.1.1 Compartir una carpeta 128
7.1.2 Acceso a un recurso compartido 129
7.1.3 Administrar recursos compartidos 130
7.1.4 Instantáneas 131
7.1.5 Sistemas de archivos distribuidos 133
7.2 SERVIDORES DE IMPRESIÓN 138
7.2.1 Compartir impresora 138
7.2.2 Servidor de impresión y documentos 141
7.2.3 Cliente 142
RESUMEN DEL CAPÍTULO 143
EJERCICIOS PROPUESTOS 144
TEST DE CONOCIMIENTOS 144

CAPÍTULO 8. DIRECTORIO ACTIVO 145
8.1 INTRODUCCIÓN 146
8.2 INSTALACIÓN DEL CONTROLADOR DE DOMINIO 148
8.2.1 Tareas previas 148
8.2.2 Instalación 149
8.3 ADMINISTRACIÓN DEL DIRECTORIO ACTIVO 152
8.3.1 Herramientas administrativas 152
8.3.2 Administración básica de objetos 152
8.4 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO 156
8.4.1 Directivas de seguridad 156
8.4.2 Directivas de grupo local 158
8.4.3 Administración de Directivas de Grupo 159
RESUMEN DEL CAPÍTULO 161
EJERCICIOS PROPUESTOS 162
TEST DE CONOCIMIENTOS 162

BLOQUE III. GNU/LINUX 163

CAPÍTULO 9. INSTALACIÓN Y CONFIGURACIÓN 165
9.1 INTRODUCCIÓN 166
9.1.1 Distribuciones 166
9.1.2 Licencias de software 168

9.2 INSTALACIÓN 169
9.2.1 Ubuntu 170
9.2.2 Fedora 177
9.3 X-WINDOWS 184
9.4 PRIMEROS PASOS 186
9.4.1 Intérprete de comandos 186
9.4.2 Estructura de directorios 190
9.4.3 Instalar y quitar componentes 191
9.4.4 Webmin 198

RESUMEN DEL CAPÍTULO 200
EJERCICIOS PROPUESTOS 200
TEST DE CONOCIMIENTOS 200

CAPÍTULO 10. PUESTA EN MARCHA DEL SISTEMA 201
10.1 ADMINISTRACIÓN DE USUARIOS 202
10.1.1 Intérprete de comandos 202
10.1.2 Ficheros utilizados 204
10.1.3 Configuración con asistentes 206
10.2 SISTEMA DE FICHEROS 208
10.2.1 Particionamiento 208
10.2.2 Sistemas RAID 213
10.2.3 Monitorización 215
10.2.4 Cuotas de disco 215
10.3 PERMISOS 219
10.3.1 Establecer los permisos 220
10.3.2 Establecer el usuario y grupo propietario 220

RESUMEN DEL CAPÍTULO 221
EJERCICIOS PROPUESTOS 222
TEST DE CONOCIMIENTOS 222

CAPÍTULO 11. ADMINISTRACIÓN BÁSICA DEL SISTEMA 223
11.1 ARRANQUE Y PARADA 224
11.1.1 Gestor de arranque 224
11.1.2 Proceso de arranque y parada del sistema 229
11.1.3 Servicios del sistema 231
11.1.4 Procesos 235
11.1.5 Programación de tareas 236
11.1.6 Reinicio y parada del sistema 237
11.2 MONITORIZACIÓN DEL SISTEMA 238
11.2.1 Herramientas básicas 238
11.2.2 Directorio /proc 240
11.2.3 Archivos de registro (syslog) 240
11.3 COPIAS DE SEGURIDAD 242
11.3.1 Comandos básicos 243
11.3.2 Herramientas gráficas 247

RESUMEN DEL CAPÍTULO 249
EJERCICIOS PROPUESTOS 250
TEST DE CONOCIMIENTOS 250

CAPÍTULO 12. PROGRAMACIÓN SHELL 251
12.1 CONCEPTOS BÁSICOS 252
12.1.1 Variables 252
12.1.2 Paso de parámetros 252
12.2 ENTRADA Y SALIDA DE DATOS 253
12.2.1 E/S por consola 253
12.2.2 Redirección de la E/S 254
12.2.3 Filtrado de textos 254
12.3 OPERACIONES ARITMÉTICOLÓGICAS 256
12.3.1 expr 256
12.3.2 test 257
12.4 ESTRUCTURAS DE CONTROL 258
12.4.1 Condición simple (if) 258
12.4.2 Condiciones múltiples (case) 259
12.4.3 Bucle for 259
12.4.4 Bucle while 260
12.5 FUNCIONES 260

RESUMEN DEL CAPÍTULO 262
EJERCICIOS PROPUESTOS 262
TEST DE CONOCIMIENTOS 262

CAPÍTULO 13. ADMINISTRACIÓN DE LA RED 263
13.1 ESQUEMA BÁSICO DE RED 265
13.1.1 Configuración de la red 265
13.1.2 Iptables 271
13.1.3 DHCP 276
13.2 ACCESO REMOTO AL SISTEMA 280
13.2.1 SSH 280
13.2.2 VNC 285

RESUMEN DEL CAPÍTULO 289
EJERCICIOS PROPUESTOS 289
TEST DE CONOCIMIENTOS 290

CAPÍTULO 14. SERVIDORES DE IMPRESIÓN Y DE ARCHIVOS 291
14.1 COMPARTIR ARCHIVOS E IMPRESORAS (SAMBA) 292
14.1.1 Instalación 292
14.1.2 Configuración 293
14.1.3 Cliente 300
14.2 NFS 304
14.2.1 Configuración del servidor 304
14.2.2 Configuración del cliente 305

RESUMEN DEL CAPÍTULO 306
EJERCICIOS PROPUESTOS 307
TEST DE CONOCIMIENTOS 307

CAPÍTULO 15. LDAP 309
15.1 INTRODUCCIÓN 310
15.2 OPENLDAP 310
15.2.1 Instalación 311
15.2.2 Configuración 311
15.3 HERRAMIENTAS Y UTILIDADES 317
15.3.1 Herramientas de cliente 317
15.3.2 Configuración del servidor 319
15.3.3 Herramientas gráficas 320
RESUMEN DEL CAPÍTULO 326
EJERCICIOS PROPUESTOS 326
TEST DE CONOCIMIENTOS 326

MATERIAL ADICIONAL 327

ÍNDICE ALFABÉTICO 329

Introducción

Este libro surge con el propósito de acercar al lector a los aspectos más importantes que encierra la **Administración de Sistemas Operativos** ante la creciente demanda de personal cualificado. Con tal propósito, puede servir de apoyo también para estudiantes del **Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red** y las titulaciones de Grado de Informática.

A lo largo del libro se estudian los aspectos fundamentales relacionados con la Administración de los Sistemas Operativos más utilizados en pequeñas y medianas empresas: Windows 2008 R2 y GNU/Linux. En concreto, aprenderá a utilizar las dos distribuciones GNU/Linux más utilizadas: Ubuntu Server y Fedora.

Los contenidos se han dividido en tres bloques. En el primer bloque se estudian los aspectos generales de la administración de sistemas donde se describe el hardware, el software de un servidor y la integración de sistemas. Los dos siguientes bloques se dedican a estudiar los aspectos específicos de cada sistema operativo. Así, el segundo bloque se dedica al estudio de Windows 2008 R2 y el tercer bloque se centra en los sistemas GNU/Linux. Entre otros aspectos, aprenderá a instalar y configurar el sistema operativo, gestionar las cuentas de los usuarios, administrar la red, administrar sus servicios, etc.

Para todo aquel que use este libro en el entorno de la enseñanza (Ciclos Formativos o Universidad), se ofrecen varias posibilidades: utilizar los conocimientos aquí expuestos para inculcar aspectos genéricos en la administración de sistemas operativos o simplemente centrarse en la administración de servidores Windows 2008 R2 y GNU/Linux. La extensión de los contenidos aquí incluidos hace imposible su desarrollo completo en la mayoría de los casos.

Ra-Ma pone a disposición de los profesores una guía didáctica para el desarrollo del tema que incluye las soluciones a los ejercicios expuestos en el texto. Puede solicitarlo a *editorial@ra-ma.com*, acreditándose como docente y siempre que el libro sea utilizado como texto base para impartir las clases.

TEORÍA

CAPÍTULOS

1. ASPECTOS BÁSICOS
2. INTEGRACIÓN DE SISTEMAS

1 Aspectos básicos

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer la importancia de la administración de sistemas.
- ✓ Conocer las diferentes tareas que realiza el administrador del sistema.
- ✓ Ver los elementos y estructura de un sistema informático.
- ✓ Conocer los diferentes tipos de sistemas RAID.
- ✓ Seleccionar las características hardware del servidor más adecuadas.
- ✓ Conocer los diferentes sistemas operativos para servidores.

En la actualidad, y cada vez más, las empresas precisan de sistemas informáticos que resultan fundamentales para su modelo de negocio. Se ha convertido en una escena habitual el que una organización trabaje y produzca en base a los servidores y datos de los que dispone, y que el éxito final de la misma dependa de los servicios informatizados que ofrece. Las tecnologías de la información se han convertido, con el paso de los años, en un elemento clave para la competitividad de las organizaciones.

El administrador del sistema es el responsable de que el sistema informático funcione correctamente y de modo seguro. Para ello, el administrador es una persona muy preparada que posee amplios conocimientos en sistemas operativos, redes, programación y, cómo no, de seguridad informática.

En esta unidad se van a ver los conceptos más importantes relacionados con la administración de sistemas: las diferentes tareas que realiza un administrador, el hardware del servidor y el software del servidor.

1.1 TAREAS DEL ADMINISTRADOR

Un sistema informático precisa de una planificación, configuración y atención continuada para garantizar que el sistema es fiable, eficiente y seguro. El sistema informático debe tener una o más personas designadas como administradores para gestionarlo y ver su rendimiento. El administrador del sistema tiene la responsabilidad de asegurar su adecuado funcionamiento, de saber a quién poder llamar si no se pueden resolver los problemas internamente, y de saber cómo proporcionar recursos hardware y software a los usuarios.

Las tareas y responsabilidades de los administradores de sistemas varían dependiendo del tamaño del sistema informático. En sistemas grandes las tareas de administración pueden dividirse entre varias personas. Por otro lado algunos sistemas pequeños tan solo necesitan un administrador.

El administrador del sistema cumple un papel muy importante en la empresa, ya que debe garantizar el correcto funcionamiento del sistema informático. Además, dada la responsabilidad y el tipo de información con el que trabaja, el administrador se convierte en una persona de confianza dentro de la empresa.

La descripción exacta del trabajo del administrador del sistema depende frecuentemente de cada organización. Un administrador del sistema puede encontrarse envuelto en una amplia variedad de actividades, desde establecer normas para instalar software a configurar los *routers*. Sin embargo, hay una serie de tareas que todos los administradores tienen que gestionar:

- **Instalación y configuración de software**. Instalar y configurar el sistema operativo, servicios y aplicaciones necesarios para que el servidor trabaje de forma correcta.
- **Instalación y configuración de hardware**. Instalar, configurar dispositivos como impresoras, terminales, módems, unidades de cinta, etc.
- **Instalación y configuración la red**. Instalar, configurar y realizar un mantenimiento de la red para permitir que los equipos se comuniquen correctamente.
- **Administración de usuarios**. Dar de alta o baja usuarios, modificar sus características y privilegios, etc.
- **Formación y asesoramiento de los usuarios**. Proporcionar directa o indirectamente formación a los usuarios de modo que puedan utilizar el sistema de forma efectiva y eficiente.
- **Inicio y apagado del sistema**. Iniciar y apagar el sistema de un modo ordenado para evitar inconsistencias en el sistema de ficheros.

- **Registro de los cambios del sistema**. Registrar cualquier actividad significativa relacionada con al sistema.
- **Realización de copias de seguridad**. Establecer una correcta política de seguridad que permita restablecer el sistema en cualquier momento.
- **Seguridad del sistema**. Evitar que los usuarios interfieran unos con otros a través de acciones accidentales o deliberadas, así como las posibles intrusiones.

ACTIVIDADES 1.1

- Busca en Internet ofertas de trabajo para administradores de sistemas y determina cuál es el perfil más demandado.
- A partir de las ofertas de trabajo encontradas, realiza una pequeña comparativa entre las demandas de administradores de sistemas Windows y GNU/Linux.

1.2 HARDWARE DEL SERVIDOR

En la actualidad, los administradores de sistemas se enfrentan a muchos retos a la hora de instalar un nuevo servidor, independientemente del sistema operativo y las aplicaciones que van a ejecutarse. Los administradores deben tener en cuenta el mayor número de factores posible antes de llevar a cabo cualquier instalación para asegurarse que el equipo ha sido configurado de acuerdo a las necesidades de los usuarios y a las aplicaciones instaladas en el servidor. Estos consejos evitarán tener que reconfigurar sus equipos nada más haber realizado la instalación por no cumplirse las expectativas previstas.

Entender los componentes básicos del hardware del servidor es esencial a la hora de planificar su primera instalación, reinstalación o actualización. A continuación se van a ver los aspectos más importantes que hay que tener en cuenta a la hora de elegir el hardware más importante para el servidor.

1.2.1 CPD

El CPD o Centro de Proceso de Datos suele ser uno de los lugares más importantes y seguros de una empresa ya que en él se encuentran todos los servidores de la empresa.

Figura 1.1. CPD

Un CPD suele tener las siguientes características:

- **Control de acceso**. Se suele controlar el acceso al CPD para no permitir accesos no autorizados. El control de acceso se puede realizar desde las tradicionales cerraduras de seguridad hasta las más avanzadas medidas biométricas.
- **Armarios**. El CPD suele contar de diversos armarios en *rack* donde se alojan los diferentes servidores, *routers*, sistemas de alimentación, etc.
- **Sistema de alimentación**. Su objetivo es estabilizar la tensión que llega a los equipos eliminando cualquier distorsión en la misma y alimentar el sistema en el caso de una caída del suministro eléctrico. Los CPD suelen contar con Sistemas de Alimentación Interrumpida (SAI), generadores de electricidad e incluso varias líneas eléctricas de proveedores diferentes.
- **Ventilación**. La ventilación y la temperatura es un elemento muy importante en los CPD. Lo normal es que la temperatura oscile entre 21 y 23 grados centígrados. Para mejorar la refrigeración de los servidores se suelen disponer de tal manera que los armarios forman los denominados "pasillos fríos" y "pasillos calientes", mejorando la circulación del aire con el consiguiente ahorro en energía.
- **Cableado**. Lo normal es que todo el cableado del CPD suela discurrir por un falso suelo para así facilitar las instalaciones. Es importante disponer de líneas redundantes para la alimentación eléctrica y las conexiones de datos del CPD.
- **Sistema antiincendios**. Lógicamente, el CPD cuenta con un sistema propio de detección del fuego y de extinción. No se debe a que el CPD suponga en sí mismo una posible fuente de incendios, sino más bien al valor de la información almacenada y al considerable daño que supondría para el negocio una pérdida de la misma.

El sistema de extinción no se puede realizar por agua ni polvo ya que dañaría completamente los equipos y se realiza con dióxido de carbono u otros gases con agentes de extinción. El objetivo de estos gases es "secuestrar" el oxígeno del CPD ya que sin oxígeno no existe fuego.

Figura 1.2.Sistema de extinción de un CPD

ACTIVIDADES 1.2

- Busca en Internet información sobre las características de un CPD de alguna empresa.

1.2.2 SISTEMA DE RACK

Un *rack* es el mejor lugar para colocar los servidores, ya que tras la instalación de dichos servidores, el conjunto ocupa el **menor espacio posible**, con la **mejor organización, ventilación y accesibilidad** para operar en ellos fácilmente en cualquier momento.

Un *rack* no es más que una estantería o armario generalmente de unos 1,8 metros de altura y 48 cm de ancho, donde los servidores pueden apilarse uno encima de otro. Las unidades estándar para definir las dimensiones de un *rack* son pulgadas para el ancho y "U" (unidades de *rack*) para el alto. Usualmente la anchura de los *racks* pueden ser 19" de ancho, mientras que la gran mayoría de *racks* disponen de una altura de 42U (una unidad de *rack* corresponde a 44,45 mm).

Así por ejemplo, tal y como se muestra en la Figura 1.3, un servidor puede ocupar 1 U ó 2 U en un *rack*, o tal vez "4 U *half" rack*.

Por tanto, si desea que los equipos dispongan de la mejor ventilación, accesibilidad, organización, etc., se recomienda sin duda alguna colocarlo adecuadamente en un *rack*.

Figura 1.3. *Rack*

ACTIVIDADES 1.3

- Realiza un presupuesto de un armario *Rack* 19".

1.2.3 SERVIDORES

El servidor es el centro del sistema y, por tanto, el punto más importante. Aunque puede configurar cualquier ordenador para que actúe como servidor, lo mejor es utilizar un hardware específico que esté preparado para trabajar de forma ininterrumpida.

El primer elemento que debe tener en cuenta es el formato del servidor. Tal y como puede verse en la Figura 1.4, existen varios formatos de servidores:

- **Torre**. Es el formato normal de un ordenador y el menos aconsejado para su instalación en un CPD.
- **Blade**. Son servidores integrados al máximo para utilizarse de forma conjunta en un *ChasisBlade*. Este tipo de servidores se utiliza en sistemas que exigen prestaciones muy altas.

- **Rack**. Es el formato más utilizado de servidor y su diseño está optimizado para poder almacenarlo en armarios *Rack* 19". El tamaño del servidor se mide por el número de U que ocupa en el servidor. Los tamaños más habituales son 1 U (o formato pizza), 2 U y 4 U.

Figura 1.4. *Tipos de servidores: Torre, Blade y Rack*

Un aspecto realmente importante, y al que en determinadas ocasiones no se le presta la atención suficiente, corresponde a la **redundancia de fuentes de alimentación**. La mejor forma de conseguir redundancia eléctrica consiste en conectar un sistema eléctrico a la primera fuente de alimentación y otro sistema eléctrico independiente a la segunda fuente de alimentación. Esto permite que en caso de fallo eléctrico en cualquiera de las líneas eléctricas, o en cualquiera de las fuentes de alimentación, el sistema pueda seguir en funcionamiento. Sin embargo, si no es posible disponer de dos puntos eléctricos independientes, el disponer de redundancia de fuentes de alimentación al menos garantiza cierta tranquilidad ante el fallo de una de éstas.

Hoy en día la mayoría de los servidores de media/alta gama dispone de fuentes de alimentación redundantes que se pueden cambiar en caliente. En la Figura 1.5 puede ver un ejemplo de dos fuentes de alimentación redundantes y en la Figura 1.6 puede ver un servidor con fuentes de alimentación redundantes.

Figura 1.5. *Fuente de alimentación redundante*

Figura 1.6. *Servidor con fuente de alimentación redundante*

Otro elemento característico de los servidores es la ventilación. Los servidores suelen estar dotados de un sistema de ventilación que permite que el servidor no se caliente. Lo normal es que los servidores estén dotados de un gran número de ventiladores intercambiables en caliente. En la Figura 1.7 puede verse el interior del servidor DELL R805 donde se puede apreciar en primer plano el sistema de ventilación.

Figura 1.7. *Interior de un servidor Dell R805*

Por último, y quizás lo más importante, son las prestaciones de procesamiento del servidor. Para dimensionar bien el servidor hay que tener muy en cuenta la utilización que se le va a dar. Aunque no se va a entrar en velocidades, cantidad de memoria, etc., por ser aspectos que cambian mucho en el tiempo, hay que tener en cuenta numerosos aspectos, entre los que se destacan:

- **Procesador**. Velocidad del procesador, arquitectura, número de núcleos y número de procesadores.
- **RAM**. Cantidad de memoria RAM, tipo de memoria, velocidad, etc.
- **Sistema de ficheros**. Capacidad, velocidad de transferencia, tecnología, etc.

ACTIVIDADES 1.4

- Accede a las páginas web de HP o DELL y realiza un presupuesto de un servidor de gama baja y de gama alta en *rack*.

1.2.4 SISTEMAS RAID

A la hora de seleccionar el tipo de subsistemas de disco, hay muchos aspectos importantes que deben tenerse en cuenta ¿qué tipo de discos debería usar? Si utiliza RAID, ¿qué nivel debería usar? Los distintos niveles de RAID tienen distintas características de rendimiento y, por este motivo, tiene que tener muy claro cómo quiere que funcione su servidor. ¿Dónde necesita la mejor capacidad de rendimiento de un RAID? ¿En lectura o en escritura?

RAID es un acrónimo de *Redundant Array of Independent Disk*. Un *array* de RAID es un grupo de discos que actúan colectivamente como un único sistema de almacenamiento, que, en la mayoría de los casos, soporta el fallo de uno de los discos sin perder información de modo que puedan operar con independencia.

Los niveles más importantes de los sistemas RAID son los siguientes:

- **RAID 0**. Disco con bandas sin tolerancia al error. El nivel 0 de RAID no es redundante, así que no se corresponde exactamente al acrónimo. En el nivel 0, la información está dividida en diversas unidades, obteniéndose como resultado una unidad mayor. Por ejemplo, si dispone de 2 discos duros de 2 TB se obtiene como resultado una unidad de 4 TB. La capacidad de procesamiento del RAID es muy buena, tanto en operaciones de escritura como de lectura, pero si falla una de las unidades, se pierde toda la información del *array*.

Figura 1.8. RAID 0

- **JBOD** (*Just a Bunch Of Drives*). Este modelo es como el nivel RAID 0 y lo que hace es combinar múltiples discos duros físicos en un solo disco virtual. Al igual que ocurre en el nivel RAID 0 si se rompe un disco duro se perderán los datos del sistema.
- **RAID 1** o disco espejo. El nivel 1 de RAID proporciona redundancia al duplicar todos los datos de una unidad a otra. El rendimiento de un *array* de nivel 1 es un poco mejor que cuando se tiene una única unidad, y además, si cualquiera de ellas falla, no se perderán los datos. El mayor aumento del rendimiento tiene lugar en lecturas y escrituras secuenciales. Es un buen sistema redundante de nivel de entrada porque solamente son necesarias dos unidades. Sin embargo, como una de ellas se usa para almacenar la información duplicada, el coste por megabyte es elevado.

Figura 1.9. RAID 1

- **RAID 0+1**. Reflejo de discos con bandas. El nivel RAID 0+1 proporciona redundancia y rendimiento al replicar dos conjuntos de bandas de RAID 0. Los controladores actuales de RAID proporcionan automáticamente rendimiento y redundancia mediante el duplicado de bandas de discos; para ello, debe utilizar un número par de cuatro o más discos.

Figura 1.10. RAID 0+1

- **RAID 5**. Discos de información independientes con bloques de paridad distribuidos. El problema de los sistemas RAID de nivel 0 es que se pierde un 50% de la capacidad del disco duro. En el nivel 5 en vez de duplicar completamente los datos del disco duro se utilizan los bits de paridad para que en caso de que se rompa un disco duro poder reconstruir la información del mismo. En este caso, los bits de paridad ocupan mucho menos espacio que duplicar un disco duro entero. En concreto, los bits de paridad ocupan 1 disco duro del volumen. De esta forma si dispone de RAID nivel 5 con 6 discos duros entonces al utilizar un disco para la paridad se pierde 1/6 (16%) del volumen para datos. Dada su robustez y nivel de aprovechamiento de los discos que forman el raid, el nivel 5 es el más utilizado de todos.

Figura 1.11. RAID 5

De esta forma, si utiliza un sistema RAID 1, 0+1 ó 5, en el caso de que se rompa un disco duro tiene la tranquilidad de que no se van a perder los datos. Una vez que se rompa un disco duro la tarea del administrador es reemplazar el disco duro para que el RAID se reconstruya.

Pero si desea una mayor tranquilidad puede utilizar un disco en espera (*Hot Spare*). Al utilizar un disco duro en espera, si se rompe un disco duro, la controladora RAID pasa a utilizarlo automáticamente sin necesidad de la intervención del administrador del sistema.

Al configurar el sistema de ficheros hay que tener en cuenta que es recomendable que el sistema operativo, los datos y los registros y ficheros de actividad (logs) se encuentren en sistemas de almacenamiento diferentes. De esta forma no solo mejora el rendimiento del sistema sino que además reduce el riesgo ante un problema de seguridad.

En la Tabla 1.1 puede ver las configuraciones recomendadas para utilizar en servidores de gama baja-media y alta.

Tabla 1.1. Configuraciones RAID recomendadas

	Servidor de gama	
Sistema de ficheros	**baja-media**	**alta**
Sistema operativo	1 HDD	Raid 1 ó 0+1
Datos	1 HDD, Raid 1 ó 0+1	Raid 5
Registro y ficheros de actividad (logs)	1 HDD	Raid 1 ó 0+1

ACTIVIDADES 1.5

- Analiza las características de tu ordenador para ver si permite utilizar unidades RAID hardware.
- Realiza un presupuesto para que un ordenador utilice un sistema RAID hardware. Indica las diferentes alterativas que existen.
- Calcula el espacio de disco disponible si creas un RAID 5 utilizando 6 discos duros de 1 TB, ¿y si utilizas un RAID 0?

1.3 SOFTWARE DEL SERVIDOR

Principalmente existen dos grandes alternativas a la hora de elegir un sistema operativo: los basados en UNIX (o su homólogo Linux) o Windows. Mientras que Linux es un sistema operativo abierto en el que participa de forma directa un amplio abanico de la comunidad informática, Windows es un producto comercial propiedad de Microsoft. La elección de una de estas dos alternativas no está libre de controversia: unos son admiradores del sistema Windows y otros son grandes detractores de él.

En la Tabla 1.2 se muestran los sistemas operativos más utilizados como cliente o servidor. Hay que señalar que mientras que los sistemas Windows tienen un uso específico (p.e. Windows 7 se utiliza como cliente, Windows Server 2008 como servidor) los sistemas GNU/Linux pueden como cliente o servidor.

Tabla 1.2. Sistemas operativos más utilizados

	Cliente	Servidor
Basados en Windows	Windows XP Windows Vista Windows 7	Windows Server 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Basados en GNU/Linux	Cualquier distribución GNU/Linux	Cualquier distribución GNU/Linux
Otros sistemas	React OS Chrome OS	MAC OS X Server

La comunidad informática considera que Linux es un sistema operativo mucho más estable y seguro que Windows. Linux es abierto, por lo que se conocen sus fuentes y esto facilita el descubrimiento de errores (y su solución). A pesar de eso, hay que destacar el hecho de que los sistemas operativos Windows son analizados en busca de fallos, por miles o quizás millones de personas. Posiblemente si Linux fuera tan analizado, tendría tantos o más fallos que Windows.

La popularidad es una moneda de dos caras para todos aquellos que utilicen las tecnologías Microsoft. Por un lado, podrá obtener los beneficios de un soporte más consolidado y robusto a nivel mundial y una aceptación prácticamente universal de los usuarios. Por otro lado, el monopolio dominante de Windows se está convirtiendo en el blanco

preferido por miles de *hackers* que desarrollan ataques cada vez más sofisticados y, posteriormente, los desencadenan a escala global.

Bien configurados, los servidores Windows pueden ser tan seguros como cualquier sistema operativo basado en UNIX, Linux o cualquier otro sistema operativo. Un antiguo dicho en seguridad afirma "*el conductor tiene más responsabilidad que el coche*".

A lo largo del libro van a ver las características más importantes de los sistemas Windows 2008 R2 Server y GNU/Linux, así como su instalación, configuración y administración.

ACTIVIDADES 1.6

- Busca y localiza la página web de cinco distribuciones GNU/Linux.
- Realiza una línea temporal de las versiones de Windows que han aparecido en el mercado.

RESUMEN DEL CAPÍTULO

En este primer capítulo se han visto la importancia del administrador del sistema y las tareas que realiza.

Se han descrito los elementos hardware de un sistema informático (CPD, *rack*, servidores...) haciendo especial hincapié en el tipo de servidores y los diferentes formatos de sistemas RAID.

También se han descrito las características más importantes de los sistemas operativos.

EJERCICIOS PROPUESTOS

- **1.** Enumera las tareas más importantes que realiza un administrador de sistemas.
- **2.** Comenta brevemente los elementos más importantes de un CPD.
- **3.** Enumera los elementos de seguridad que tiene un CPD.
- **4.** Realiza una tabla comparativa en la que indicas las ventajas y desventajas de cada sistema RAID.

TEST DE CONOCIMIENTOS

1 Indique la característica que no posee un CPD.

a) Control de acceso.
b) Sistemas de alimentación ininterrumpidos.
c) Cableado a la vista.
d) Sistema antiincendios.

2 ¿Qué es un *rack*?

a) Un conjunto de servidores con un mismo objetivo.
b) Un armario/estantería para la instalación de servidores.
c) Cada uno de los servidores ubicados en el CPD.
d) Cada pasillo para la insta.

3 ¿Cuál es el objetivo principal de un sistema RAID?

a) Almacenar información de forma redundante.
b) Aumentar el rendimiento en el almacenamiento de la información.
c) Mantener un mayor nivel de seguridad.
d) Tolerancia de fallos en uno de los discos sin perder información.

4 ¿Qué sistema RAID no utilizarías si quieres evitar perder la información cuando se rompa un disco duro?

a) RAID 1.
b) RAID 0+1.
c) RAID 0.
d) RAID 5.

2 Integración de sistemas

OBJETIVOS DEL CAPÍTULO

- ✓ Ver los diferentes tipos de esquema de red.
- ✓ Seleccionar el esquema de red más adecuado.
- ✓ Conocer los diferentes tipos de integración de sistemas.
- ✓ Conocer los servicios más importantes que permiten la integración de sistemas.
- ✓ Planificar, diseñar e implementar el sistema informático de una empresa.

2.1 INTRODUCCIÓN

En la actualidad es muy frecuente tener redes heterogéneas en las que conviven diferentes sistemas operativos tanto a nivel de cliente como de servidor. A nivel de servidor puede encontrar sistemas basados en Windows Server (2003, 2008 ó 2008 R2) y sistemas GNU/Linux. A nivel de cliente puede encontrar una extensa variedad de equipos con Windows XP, Windows Vista, Windows 7, Chrome OS, sistemas GNU/Linux, etc.

Tanto los sistemas operativos Windows y Linux tienen ventajas y/o desventajas que hacen que no exista el sistema ideal, ya que su utilización va estrechamente ligada al uso que se va a realizar. Por ejemplo, si quiere utilizar un equipo como cliente para un uso general (p.e. navegar por Internet, ofimática, ejecutar una aplicación empresarial) lo mejor es utilizar un sistema cliente basado en Windows (p.e. Windows 7). Si por el contrario necesita montar un servidor de red la mejor elección será utilizar un sistema GNU/Linux (p.e. Ubuntu).

Lógicamente, una tarea importante del administrador de sistemas es que los diferentes equipos de la red puedan comunicarse correctamente, compartir información, recursos, etc.

El objetivo de esta unidad es aprender a diseñar correctamente el sistema informático de una empresa (red, clientes y servidores) para aprovechar las ventajas de los diferentes sistemas operativos. Para ello, primero se van a ver los esquemas de red más utilizados para, posteriormente, ver como permitir la integración entre cualquier sistema de la red.

2.2 ESQUEMAS BÁSICOS DE RED

Uno de los aspectos más importantes a la hora de crear y configurar una red es diseñar y planificar correctamente la arquitectura de red. Una arquitectura de red es el diseño de la red en el que se emplean unos determinados componentes, cuya finalidad es la de canalizar, permitir o denegar el tráfico con los elementos apropiados.

Existen varias arquitecturas de red, desde la más sencilla, que utiliza simplemente un *router*, hasta otras más complejas, basadas en varios *routers*, *proxys* y redes perimetrales (o zonas neutras).

Antes de entrar en detalle con las arquitecturas existentes de cortafuegos, se van a describir tres elementos básicos que intervienen en ella:

- **Router**. Equipo que permite o deniega las comunicaciones entre dos o más redes. Al ser el intermediario entre varias redes debe estar especialmente protegido ya que puede ser objeto de un ataque. Un *router* puede ser un dispositivo específico o un servidor que actúe como *router*.
- **Red interna**. Es la red interna de la empresa y, por lo tanto, es donde se encuentran los equipos y servidores internos. Dependiendo del nivel de seguridad que necesite la red interna se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra.
- **Red perimetral o zona neutra**. Red añadida entre dos redes para proporcionar mayor protección a una de ellas. En esta red suelen estar ubicados los servidores de la empresa. Su principal objetivo es que ante una posible intrusión en unos de los servidores, se aísle la intrusión y no se permita el acceso a la red interna de la empresa.

A continuación se va a ver el esquema de red básico que se puede utilizar cuando desea crear una red interna pero no hay servidores que ofrezcan servicios a Internet. En el caso de tener servidores públicos entonces se recomienda tener una zona neutra.

A partir del esquema de red con una zona neutra se pueden realizar todas las modificaciones que estime oportunas dependiendo de la seguridad que quiera tener en la red interna, si quiere más zonas neutras, varias conexiones a Internet, etc. En este caso lo importante es adaptar el esquema de red a las necesidades de la empresa.

ACTIVIDADES 2.1

- Describe brevemente qué es un *router* neutro.
- Busca información en Internet sobre un *router* neutro (precio, características, etc.).

2.2.1 ESQUEMA DE RED BÁSICO

Es la configuración más simple y consiste en el empleo de un *router* para comunicar la red interna de la empresa con Internet (véase la Figura 2.1). Como el *router* es el encargado de comunicar ambas redes es ideal para permitir o denegar el tráfico.

Esta arquitectura de red, aunque es la más sencilla de configurar es la más insegura de todas ya que toda la seguridad reside en un único punto: el *router*. En caso de que se produzca un fallo de seguridad en el *router* el atacante tendrá acceso a toda la red interna.

Figura 2.1. *Arquitectura de router de selección*

Otro aspecto muy importante es que si desea tener un servidor que ofrezca servicios a Internet hay que ubicarlo en la red interna. Es peligroso poner el servidor en la red interna ya que el *router* permite el tráfico al servidor y, en el caso de que se produzca un fallo de seguridad el atacante tiene acceso completo a la red interna. Para solucionar este problema se añade una nueva red a la empresa que se denomina *zona neutra* o *zona desmilitarizada*.

2.2.2 ESQUEMA DE RED CON UNA ZONA NEUTRA

Éste esquema de red es considerado como el esquema base cuando quiere ofrecer servicios a Internet manteniendo un nivel adecuado de seguridad en la red interna. Como puede ver en la Figura 2.2 esta arquitectura utiliza dos *routers* que permiten crear un perímetro de seguridad (red perimetral o zona neutra), en la que se pueden ubicar los servidores accesibles desde el exterior, protegiendo así a la red local de los atacantes externos.

Figura 2.2. *Esquema de red com una zona neutra y una red interna*

Al tener dos redes independientes se puede indicar a través de los *routers* el tráfico que se permite entre Internet y la zona neutra, o el tráfico entre la zona neutra y la red interna. Lo normal es que el *router* exterior este configurado para permitir el acceso desde Internet a los servidores de la zona neutra, especificando los puertos utilizados, mientras que el *router* interior permite únicamente el tráfico saliente de la red interna al exterior. De esta forma si se produce un fallo de seguridad y se accede a los servidores de la zona neutra el atacante nunca podrá tener acceso a la red interna de la empresa.

A partir del esquema de red con una red interna y una zona neutra (véase la Figura 2.2) puede realizar las modificaciones que estime oportunas para adaptarlo a sus necesidades. A continuación, a modo del ejemplo, se muestran algunas de las configuraciones más utilizadas:

- **Esquema de red con una zona neutra y una red interna utilizando un único router**. Aunque lo recomendable es utilizar dos *routers* para separar las redes también puede crear el esquema de red con único *router* (Figura 2.3). En este caso el *router* tiene tres interfaces de red que le permiten crear la red interna, la zona neutra y conectarse a Internet. Aunque este esquema no es tan fiable como el anterior resulta más aconsejable utilizar que el modelo básico que no tiene ninguna zona neutra.

Figura 2.3. *Esquema de red con una zona neutra y una red interna utilizando un único router*

- **Esquema de red con una zona neutra y varias redes internas**. En los esquemas de red anteriores se ha creado una única red interna y por lo tanto todos los equipos y servidores internos están en la misma red dificultando así su seguridad. En el caso de que se tengan equipos con diferentes tipos de seguridad o servidores internos, resulta aconsejable crear varias redes internas para mejorar así la seguridad de la red. En la Figura 2.4 se puede ver un esquema de red que tiene dos redes internas.

Figura 2.4. *Esquema de red con una zona neutra y una red interna utilizando um único router*

- **Esquema de red con varias zonas neutras**. En el caso de que la empresa necesite dar servicios bien diferenciados por el exterior puede optar por tener dos zonas neutras o incluso dos salidas diferentes a Internet. Por ejemplo, en el esquema de red de la Figura 2.5 tiene dos zonas neutras y dos salidas a Internet. En este caso una de las zonas neutras se puede utilizar para ubicar los servidores públicos (p.e. servidor web, FTP) y la otra zona neutra se puede utilizar para que los clientes se conecten por VPN a la red interna de la empresa. De esta forma, los clientes en la VPN estarán en una zona neutra que se encuentra aislada de la red de servidores públicos y la red interna.

Figura 2.5. *Esquema de red con dos zonas neutras y una red interna*

ACTIVIDADES 2.2

- Realiza una tabla en la que indiques las direcciones privadas de clase A, B y C.

2.3 INTEGRACIÓN DE SISTEMAS

En una red es muy frecuente encontrar equipos cliente y servidor tanto en Windows como en GNU/Linux. En la Figura 2.6 puede ver un ejemplo de un esquema de red básico con los siguientes elementos: un *router* que utiliza GNU/Linux, un servidor en Windows Server 2008 R2 y varios equipos clientes que utilizan Windows (p.e. Windows 7) o GNU/Linux (p.e. Fedora).

Figura 2.6. *Esquema básico de red*

Para permitir que los diferentes equipos trabajen correctamente entre sí se deben cumplir los siguientes niveles de integración:

- **Red**. Los equipos pueden comunicarse entre sí.
- **Datos**. Los equipos pueden compartir datos entre sí garantizando el acceso, la disponibilidad y seguridad de la información.
- **Servicios**. Los equipos pueden acceder a los servicios que ofrecen otros equipos como por ejemplo, desde un equipo Windows puede acceder a un servidor GNU/Linux para poder administrarlos.

2.3.1 RED

Para que una red funcione correctamente como mínimo debe disponer de los siguientes servicios:

- **Enrutamiento**. Permite a un servidor actuar como *router* para permitir la comunicación entre dos o más redes.
- **Servidor DHCP**. Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando un portátil se conecta a una red obtiene su configuración IP a través de un servidor DHCP.
- **Servidor DNS**. Permite mantener una equivalencia entre un nombre y su dirección IP. Por ejemplo, el nombre *www.adminso.es* equivale a 150.214.150.30.

Aunque estos tres servicios pueden configurarse tanto en un servidor Windows Server 2008 como en un servidor GNU/Linux, lo recomendable es instalar los diferentes servicios en un servidor GNU/Linux porque permite un mejor rendimiento y seguridad.

2.3.2 DATOS

Sin duda alguna los datos son el recurso más importante de la empresa. Para garantizar una correcta integración de los sistemas es totalmente necesario permitir que los equipos Windows y GNU/Linux puedan compartir información entre sí.

Los servicios más utilizados para compartir datos son:

- **Samba**. Permite compartir archivos e impresoras entre sistemas Windows y GNU/Linux.
- **NFS** (*Network File System*). Está especialmente diseñado para compartir archivos entre sistemas GNU/Linux aunque en la última versión de Windows Server (Windows 2008 R2) permite acceder a sistemas NFS.

Puede configurar un servidor para utilizarlo como sistema de almacenamiento en red o utilizar directamente una unidad NAS (*Network Attached Storage*). La ventaja de utilizar una unidad NAS es que es un dispositivo dedicado, especialmente diseñado para compartir información y permite la utilización de unidades RAID para mejorar el rendimiento y la seguridad de los datos. En la Figura 2.7 puede ver una unidad NAS de uso doméstico y en la Figura 2.8 puede ver una unidad de uso empresarial.

Figura 2.7. *LinkSys NAS-200 con 2 HD 750Gb*

Figura 2.8. SERVIDOR NAS HP

Puede configurar una unidad de almacenamiento en red utilizando distribuciones Linux como FreeNAS, NASLite y Openfiler, además de distribuciones LiveCD que pueden incluso instalarse en memorias USB.

Otra forma de compartir datos es utilizar los sistemas de ficheros distribuidos. Los sistemas de ficheros distribuidos permiten acceder de forma transparente a los datos que se almacena en varios servidores. De esta forma, es posible tener varios servidores (p.e. uno en Almería y otro en Madrid) que compartan entre la misma carpeta y que de forma automática se repliquen los datos entre los diferentes servidores. Este método es especialmente útil cuando quiere que los clientes, ubicados en localizaciones físicas diferentes, accedan a los datos de una forma rápida.

ACTIVIDADES 2.3

- Busca en Internet información sobre un sistema NAS doméstico y otro empresarial.
- Examina y comparar las características y servicios que ofrece las unidades NAS que has encontrado.

2.3.3 SERVICIOS

Los servicios de red permiten dotar de una determinada funcionalidad a la red de una empresa. Por ejemplo, el servicio SSH permite conectarse de forma remota a un servidor GNU/Linux desde otro equipo GNU/Linux o Windows.

A continuación se van a ver los servicios más utilizados en el entorno empresarial:

- **Acceso remoto**. Los servicios que permiten acceder de forma remota a un equipo a través de la red se clasifican en dos categorías:

- **Acceso remoto en modo terminal**. Para acceder a un servidor GNU/Linux en modo terminal es posible utilizar los servicios Telnet (*TELecommunication NETwork*) y SSH (*Secure SHell*). Actualmente el servicio SSH es el más utilizado ya que garantiza la seguridad de las comunicaciones mientras que el servicio Telnet no se utiliza por ser inseguro.
- **Acceso remoto en modo gráfico**. Para acceder en modo gráfico a un servidor puede utilizar el servicio VNC (Windows y GNU/Linux) o el servicio de Escritorio remoto (únicamente para sistemas Windows).

- **Directorio Activo**. En un entorno de red normal, un usuario puede iniciar sesión en la red con un nombre de usuario y una contraseña (p.e. *mperez*). Asumiendo que tiene los permisos necesarios, *mperez* puede conectarse a un equipo y acceder a sus ficheros o los servicios que proporciona.

  Cuando existe un único servidor y pocos usuarios este modelo resulta útil. Pero en el caso de tener muchos usuarios o equipos este modelo es inviable ya que resulta muy difícil administrar el sistema. Por ejemplo, si desea cambiar la contraseña de un usuario tiene que hacerlo en todos los equipos.

  Si el sistema informático cuenta con unos cientos e incluso miles de usuarios, no cuesta ver lo difícil que puede ser el mantenimiento del sistema. A medida que el número de usuarios y equipos en una red crece los servicios de Directorio Activo (o dominio) se vuelven esenciales.

  Un dominio consiste en una agrupación de máquinas y usuarios. Cuando un usuario se conecta a la red, debe seleccionar el dominio al que quiere entrar e introducir sus datos de usuario. Al ser autenticado en un dominio, el usuario tiene disponibles todos los recursos dados de alta en dicho dominio sin tener que autenticarse en cada uno de los servidores que formen parte de dicho dominio. La gestión de un dominio se realiza de forma centralizada, ya que toda la información se encuentra en una base de datos almacenada en el Controlador de Dominio (DC).

- **Otros servicios**:
  - **Servidores de impresión**. Los servidores de impresión permiten compartir impresoras entre diferentes clientes. Además, a través del servidor de impresión puede monitorizar el estado de la impresora, la cola de impresión, administrar los trabajos, etc.
  - **Actualización centralizada de sistemas**. Resulta de vital importancia tener correctamente actualizados tanto los equipos clientes de una empresa; especialmente los sistemas Windows. Cuando en la empresa tiene pocos equipos resulta fácil mantenerlos actualizados manualmente o a través de la herramienta *Windows Update*. Pero cuando la empresa dispone de cientos o incluso miles de equipos, este método resulta demasiado costoso.

    Existen herramientas como *Windows Server Update Services* que permiten a los administradores de red especificar las actualizaciones de Microsoft que se deben instalar en los diferentes equipos de la red.
  - **Monitorización centralizada de sistemas**. La monitorización de sistemas es la encargada de supervisar continuamente los diferentes recursos y servicios de la empresa para garantizar el nivel de disponibilidad requerido y, en caso de un posible fallo, alertar a los administradores para que lo solucionen.

    Existen una gran variedad de herramientas básicas de monitorización que permiten comprobar de forma individual que un recurso o servicio del sistema se encuentra disponible, pero dado el gran número de equipos de una empresa (servidores, *routers*, puntos de acceso, etc.) resulta de vital importancia poder monitorizar dichos recursos de forma remota y centralizada.

    Para monitorizar de forma centralizada los diferentes equipos de una red, una de las mejores opciones es utilizar en un equipo GNU/Linux el servicio *Nagios* y *Centreon*.

2.4 SUPUESTO PRÁCTICO

Para poner a prueba los conocimientos adquiridos a lo largo del libro, se propone la realización de un supuesto práctico que va a unificar en un proyecto todos los conceptos, procedimiento y actitudes que debe aprender.

El objetivo del supuesto práctico es simular una situación real que puede encontrar en su próximo futuro laboral. Para realizar el supuesto práctico se deben realizar las siguientes fases:

- **Descripción del problema planteado**.
- **Diseño del sistema**. En esta fase se describe el diseño del sistema que se va a implementar. Para realizar el diseño hay que indicar el esquema de red que se va a utilizar así como una pequeña descripción con las características más importantes que va a tener cada equipo de la red (hardware, SO, servicios, configuración...).
- **Implementación**. Se describen los pasos realizados para poner el sistema en marcha.
- **Prueba**. Se describen los pasos realizados para comprobar el correcto funcionamiento del sistema.

A continuación se muestra la descripción del problema plateado así como la fase de diseño del mismo. Durante el desarrollo del libro se estudia todo lo necesario para la implementación y prueba del proyecto. Por lo tanto, una vez que haya realizado todas las prácticas del libro es recomendable que implementes el supuesto práctico o cualquier variación del mismo.

2.4.1 DESCRIPCIÓN

Una empresa de servicios ha solicitado el diseño y la puesta en marcha de un sistema informático que debe cumplir las siguientes características:

- Todos los equipos de la empresa estarán dentro de una red interna que tiene acceso a Internet y en la que se permite que los empleados conecten sus portátiles.
- Todos los usuarios de la empresa pueden utilizar cualquier ordenador de la empresa utilizando siempre su mismo nombre de usuario y contraseña.
- En la empresa existen tres tipos de usuarios: jefes, empleados y contabilidad. Los jefes son los dueños de la empresa y por lo tanto, pueden acceder a todos los recursos del sistema. El personal de contabilidad es el encargado de realizar todas las tareas de administración y contabilidad de la empresa. Y por último, los empleados utilizan una aplicación que permite gestionar las compras/ventas de la empresa.
- Los usuarios de la empresa tienen acceso a las carpetas compartidas con los permisos de acceso que se muestran en la Tabla 2.1.

Tabla 2.1. Recursos compartidos y permisos

Recurso	Empleados	Contabilidad	Jefes
/TPV	R/W	R/W	R/W
/proyectos			R/W
/presupuestos		R/W	R/W

- En las carpetas compartidas, los empleados solo pueden almacenar un máximo de 500 MB de datos.
- Hay que garantizar la seguridad del sistema. Especialmente hay que evitar la pérdida de información (p.e. ante la rotura de un disco duro).
- La empresa tiene varias impresoras que pueden utilizar todos los usuarios de la empresa libremente.
- Y, finalmente, el administrador del sistema tiene que tener acceso remoto a todos los servidores de la empresa.

2.4.2 DISEÑO DEL SISTEMA

Para realizar el diseño del sistema a implementar lo primero que hay que hacer es seleccionar el esquema de red más apropiado.

Tal y como se ha visto el apartado 2.2. (*Esquemas básicos de red*), existen diferentes esquemas de que se pueden adaptar a las necesidades de la empresa. Como punto de partida, se pueden utilizar los esquemas de red que se muestran en la Figura 2.9.

El esquema de red de la Figura 2.9a, es el más sencillo de implementar y se puede utilizar en el caso que de no utilizar servidores que ofrezcan servicios en Internet. En el caso de utilizar servidores públicos, es mejor crear una zona neutra por lo que se utiliza el esquema de la Figura 2.9b.

Figura 2.9. *a) Esquema de red básico; b) Esquema de red con zona neutra*

Como en el supuesto práctico no es necesario disponer de servidores públicos (p.e. servidor web, servidor FTP) se va a utilizar como punto de partida el esquema de la Figura 2.9a.

A continuación se va proceder a analizar cada uno de los requisitos para poder diseñar el sistema:

- **Requisito 1**. Para cumplir el requisito es necesario configurar un servidor que actúe como *router* y permita el acceso de la red interna a Internet. Como puede ver en la Figura 2.10 se va a crear la red interna 10.0.0.0/24. El *router* tiene una red pública, cuya configuración depende del proveedor de Internet de la empresa, y una red privada con la IP 10.0.0.1. Y los clientes de la red utilizan como puerta de enlace la dirección IP del *router* y un servidor de nombres público (p.e. 8.8.8.8 que es de Google).

  Para permitir que los empleados puedan configurar su portátil y tener acceso a la red de forma automática se va utilizar el servidor DHCP que se instala en el servidor.

  El servidor que actúa como *router* puede utilizar el sistema operativo Windows como GNU/Linux. En el esquema de red se va a utilizar GNU/Linux por ser un sistema operativo más preparado para gestionar los servicios de red.

Figura 2.10. *Esquema de red*

- **Requisito 2**. Como los empleados pueden utilizar cualquier equipo cliente de la empresa, es necesario utilizar un servicio de domino para centralizar toda la información. Como el servicio de dominio es un servicio crítico se va a utilizar otro servidor que puede ser en Windows o en GNU/Linux. Si se utiliza GNU/Linux entonces se utiliza LDAP y si es en Windows entonces se utiliza el servicio de Directorio Activo. Aunque en el libro se estudian los dos servicios de directorio, se va a utilizar un servidor Windows con el Directorio Activo por integrarse mejor con los clientes que están en Windows.

  Tal y como se puede ver en la Figura 2.11 se ha añadido un equipo que va a actuar como controlador de dominio. Además, los equipos clientes se dan de alta en el dominio y utilizan como servidor de nombres el equipo que actúa como directorio activo.

Figura 2.11. Esquema de red con Directorio Activo

- **Requisito 3**. Se crean los grupos *jefes, empleados y contabilidad* en el dominio. Además, para poder realizar pruebas se crean varios usuarios en cada grupo.
- **Requisito 4**. Para compartir datos entre equipos Windows se utiliza el servicio *SAMBA* si el servidor utiliza GNU/Linux o el servicio *Compartir archivos e impresoras* si el servidor utiliza Windows. Como es importante proteger los datos de la empresa se van a almacenar en el servidor de Directorio Activo ya que si se almacenan en el servidor que actúa como *router* están más accesibles ante un posible ataque.

- **Requisito 5**. Para limitar el uso de espacio de disco a los usuarios hay que activar las cuotas de usuario en el disco duro donde se almacenan las carpetas compartidas.
- **Requisito 6**. Para cumplir el requisito es necesario que se guarde toda la información de la empresa (carpetas compartidas) en un sistema RAID 1 o disco en espejo. Para cumplir este requisito el servidor debe tener, al menos, un disco duro para el sistema operativo y dos discos duros configurados en RAID 1 para los datos.
- **Requisito 7**. Se instala y se comparte la impresora en el servidor de Windows.
- **Requisito 8**. Para que los administradores del sistema puedan acceder a los servidores de forma remota es necesario utilizar el servicio SSH en el *router* y el servicio *Escritorio remoto* en el servidor Windows.

A modo de resumen, en la Tabla 2.2 se muestran la características hardware y servicios que tiene cada servidor.

Tabla 2.2. Configuración y características de los servidores

	Hardware	Características
Router	2 tarjetas de red 1 HDD	SO: GNU/Linux Servicios: • Enrutamiento • DHCP • SSH
Dominio	1 HDD para el SO 2 HDD en RAID 1 para los datos. 1 tarjeta de red	SO: Windows 2008 R2 Servicios: • Directorio Activo • DNS • Compartir archivos e impresoras • Cuota de disco • Escritorio remoto

ACTIVIDADES 2.4

- Una vez que finalice todo el libro, realiza la implementación del supuesto práctico.

RESUMEN DEL CAPÍTULO

En este capítulo se ha aprendido a integrar los diferentes sistemas GNU/Linux y Windows.

Se han descrito los diferentes esquemas de red y se ha explicado cómo adaptar el esquema de red a nuestras necesidades.

También se han descrito los diferentes niveles de integración de sistemas así como los servicios que se utilizan en cada caso.

Por último, se ha realizado un supuesto práctico en el que se ha planificado y diseñado un sistema informático a partir de unos requisitos dados.

EJERCICIOS PROPUESTOS

- **1.** Enumera y realiza una breve descripción de los elementos más importantes de una red (p.e. *router*, *switch*, cableado).
- **2.** Realiza el diseño del sistema informático de una empresa que conozcas. Pon especial cuidado en el esquema de red y en las caracterizas hardware que tiene cada servidor.
- **3.** Realiza un esquema en el que indiques para cada nivel de integración los servicios que intervienen.
- **4.** Enumera y describe brevemente todos los servicios comentados en el capítulo.

TEST DE CONOCIMIENTOS

1 Una zona neutra es:
a) Una red donde se ubican los servidores públicos.
b) Una red donde se ubican los servidores privados.
c) Una red que permite mejorar la seguridad de la empresa.
d) Todas las anteriores son correctas.

2 ¿Qué servicio no se utiliza para compartir datos entre equipos?
a) Samba.
b) Compartir archivos e impresoras.
c) SSH.
d) NFS.

3 ¿Qué servicio no permite el acceso remoto a un sistema?
a) Terminal Server.
b) VNC.
c) SSH.
d) NAS.

4 Un sistema de almacenamiento a través de la red accesible por servidores y ordenadores es:
a) Un sistema RAID.
b) Una unidad NAS.
c) El protocolo SMB.
d) Un disco duro.

WINDOWS 2008

CAPÍTULOS

3. INSTALACIÓN Y CONFIGURACIÓN
4. PUESTA EN MARCHA DEL SISTEMA
5. ADMINISTRACIÓN BÁSICA DEL SISTEMA
6. ADMINISTRACIÓN DE LA RED
7. SERVIDORES DE IMPRESIÓN Y DE ARCHIVOS
8. DIRECTORIO ACTIVO

3 Instalación y configuración

OBJETIVOS DEL CAPÍTULO

- ✓ Ver las características más importantes de Windows 2008 R2.
- ✓ Planificar la instalación del sistema.
- ✓ Instalar correctamente el sistema.
- ✓ Personalizar los roles y características del servidor.

3.1 PREPARACIÓN DEL SISTEMA

La instalación de un sistema operativo era hasta hace unos años una tarea difícil, manual y había que conocer perfectamente todos los dispositivos de hardware en la plataforma donde se iba a instalar. Ahora, por ejemplo, Windows 2008 R2 se suministra con un entorno de instalación amigable y fácil de usar, detectando e instalando casi todo lo que se refiere a hardware.

Figura 3.1. *Logo de Windows 2008 R2*

Antes de iniciar la instalación, lo primero que hay que hacer es conocer los requisitos que hacen falta para instalar el sistema operativo para que su rendimiento sea eficaz y rápido. Para ello hay que hacerse las siguientes preguntas: ¿cuánta memoria necesito?, ¿qué dispositivos de hardware hacen falta?, ¿detectará el sistema operativo esos dispositivos?, ¿cuánto disco duro hace falta?

En la Tabla 3.1, puede ver los requisitos mínimos para poder utilizar Windows 2008 R2 Server.

Tabla 3.1. Tabla de requerimientos de Windows Server 2008 R2

	Mínimo (según Microsoft)	Mínimo recomendado
Procesador	1.4 Ghz	>2 Ghz
Memoria	512 Mb	>1 Gb
Disco duro	32 Gb	50 Gb

Es muy importante planificar cuidadosamente cómo se va a gestionar el espacio del disco duro (o sistema de ficheros). Suele ser aconsejable crear varias particiones, utilizar sistemas RAID, etc.

Una vez que se ha decidido que el equipo albergará Windows 2008 R2 se inicia el proceso de instalación que se realiza en las siguientes fases: *Primeros pasos*, *instalación* y *finalización de la instalación.*

Para realizar el curso puedes descargar de la Web de Microsoft una versión de evaluación de Windows 2008 R2.

ACTIVIDADES 3.1

- Visite la web de Microsoft la página del Windows 2008 R2.
- Descarge Windows 2008 R2 de la web de Microsoft o de MSDN *Academic*.
- Prepare un equipo o máquina virtual con un disco duro de al menos 20 GB, 1 GB de RAM y una tarjeta de red.

3.1.1 PRIMEROS PASOS

Para iniciar la instalación debe realizar los siguientes pasos:

1 Inicie el equipo con el CD/DVD de Windows 2008 R2. Si el equipo no muestra el menú de arranque puede entrar en la BIOS del equipo y configurarla para que arranque el sistema directamente desde el CD.

2 Al iniciar el proceso de instalación, lo primero que hace es reconocer el hardware del equipo (teclado, tarjetas de vídeo, tarjetas de sonido, etc.). Seguidamente debe seleccionar la configuración regional y el idioma del teclado (véase la Figura 3.2).

Figura 3.2. *Instalación de Windows 2008 Server*

3 Seleccione la versión del sistema operativo que desea instalar (*Standard*, *Enterprise* o *Datacenter*) y acepte los términos de la licencia.

4 A continuación indique el tipo de instalación que desea realizar. Existen dos posibilidades: *Actualización* y *Personalizada*. En el tipo de instalación *Actualización* se actualizará Windows y se conservan los archivos, la configuración y los programas actuales de los que dispongamos. Por el contrario, en la instalación de tipo *Personalizada* se instala un nuevo Windows limpio, seleccionando en qué partición ubicarlo y pudiendo realizar cambios en las particiones y discos.

Por ejemplo, en la Figura 3.3 puede observar la elección de la partición de instalación para Windows tras haber elegido una instalación personalizada. Completados estos pasos, se inicia la segunda fase en la que se instala el sistema.

Figura 3.3. *Elección de disco y partición para Windows 2008 Server*

3.1.2 INSTALACIÓN

Una vez que el sistema ha recopilado toda la información necesaria se inicia el proceso de instalación que se compone de las siguientes fases:

- ✓ Copia los archivos necesarios para la instalación.
- ✓ Expande los archivos, realizando el grueso de la instalación.
- ✓ Instala características por defecto.
- ✓ Instala actualizaciones.

Finalmente una vez completados los pasos anteriores (que puede ver en la Figura 3.4) el sistema se reinicia para completar la instalación y configurar de manera automática el sistema.

Figura 3.4. *Pasos de instalación de Windows 2008*

3.1.2.1 Finalización de la instalación y configuración

Tras reiniciarse el sistema en varias ocasiones, finaliza la instalación de Windows 2008 R2. En el último reinicio el sistema detecta de forma automática las interfaces de red y las configura. Una vez realizadas, automáticamente, las configuraciones adicionales finaliza todo el proceso pidiendo al usuario la introducción de contraseña para el usuario *Administrador* (ver Figura 3.5).

Figura 3.5. *Contraseña del Administrador*

La contraseña del Administrador es muy importante y hay que tenerla siempre a mano, ya que su pérdida puede provocar no tener acceso al servidor. Después, el sistema aplica la configuración de usuario y carga el escritorio por primera vez.

Al acceder al sistema, se muestra una ventana de bienvenida que permite acceso directo a las principales actividades y configuraciones que puede realizar al principio (ver Figura 3.6), muchas de ellas para reconfigurar pasos configurados automáticamente por el instalador y otras que clásicamente eran incluidas en el proceso de instalación de Windows. Por ejemplo, entre estas tareas de configuración inicial puede encontrar:

- **Proporcionar información del equipo**: zona de uso horario, configurar conexiones de red, nombre completo del equipo, grupo de trabajo...
- **Actualizar el servidor**: habilitar comentarios y actualizaciones automáticas, descargar e instalar actualizaciones...
- **Personalización del servidor**: agregar roles (servidor web IIS, servidor DNS, servicios de impresión, de archivo...), agregar características (servidor Telnet, SMTP, servicio WLAN, servicios simples TCP/IP), habilitar escritorio remoto, configurar el *firewall* de Windows...

Figura 3.6. *Tareas de configuración inicial*

Una vez instalado correctamente el sistema operativo, es muy importante actualizar correctamente el sistema utilizando Windows Update.

ACTIVIDADES 3.2

- Instale Windows 2008 R2 en una única partición del sistema.
- Una vez realizada la instalación, inicie sesión como *Administrador*, examina el sistema y apaga el ordenador.
- Accede al menú *Programas y Herramientas Administrativas* para ver las diferentes aplicaciones y herramientas que tiene el sistema.
- Accede al *Administrador de dispositivos* y examina el hardware que tiene el equipo. Si hay algún dispositivo que no lo ha reconocido el sistema operativo, busca e instala el *driver* del dispositivo.

3.2 AGREGAR O QUITAR FUNCIONES Y CARACTERÍSTICAS DEL SERVIDOR

Windows permite agregar o quitar funciones (o roles) del servidor a través de la herramienta administrativa *Administrador del Servidor* (véase Figura 3.7). En esta herramienta dispone del menú *Roles*, en el que puede ver los roles que actualmente estén instaladas e iniciar asistentes para agregar o quitar roles.

Figura 3.7. *Funciones y características de Windows en el Administrador del Servidor*

Dentro del menú de programas "Herramientas administrativas" se encuentran las diferentes herramientas que permiten administrar el servidor.

Para iniciar alguno de estos asistentes y agregar o quitar alguna función pulse en el enlace *Agregar roles* o *Quitar roles*, dependiendo de lo que quiera hacer. Una vez que el asistente se ha iniciado, puede observar la lista de roles disponibles para su instalación (véase Figura 3.8). Al pulsar en un rol se muestra su descripción e información básica. Seleccione la función de la lista que quiere agregar o quitar y pulse el botón *Siguiente* para iniciar el proceso de instalación/desinstalación. En primer lugar se muestra la información adicional sobre las funciones seleccionadas en el paso anterior, para después confirmar las acciones y llevarlas a cabo.

Figura 3.8. *Agregar / Quitar funciones de Windows*

De igual forma que pueden agregar o quitar funciones del servidor, existe la posibilidad de agregar o quitar características como se puede observar en la Figura 3.9.

Figura 3.9. *Agregar / Quitar características de Windows*

ACTIVIDADES 3.3

- Utiliza el asistente "*Agregar/Quitar características de Windows*" para añadir una nueva característica al sistema.
- Actualiza el sistema.

RESUMEN DEL CAPÍTULO

En este capítulo se ha descrito cómo realizar la instalación de Windows 2008 R2.
Se han indicado los diferentes sistemas de archivos que se pueden utilizar en la instalación.
Se ha explicado como administrar los roles y las características del sistema.

EJERCICIOS PROPUESTOS

1. Realiza un listado de las diferentes roles que se pueden instalar en el servidor.

2. Explica brevemente la estructura de directorios de los sistemas Windows.

TEST DE CONOCIMIENTOS

1 Indique la fase que no se realiza durante el proceso de instalación de Windows Server 2008 R2:
- a) Instalar actualizaciones.
- b) Expandir los archivos, realizando el grueso de la instalación.
- c) Analizar las características de nuestro servidor.
- d) Instalar características por defecto.

2 Windows permite agregar o quitar funciones (o roles) del servidor a través de la herramienta administrativa:
- a) Administrador del Servidor.
- b) Administrador de recursos.
- c) Administrador de funciones.
- d) Es falso, no existe ninguna.

3 Indique la memoria RAM recomendada para instalar Windows Server 2008 R2:
- a) 256 MB.
- b) 512 MB.
- c) 1 GB.
- d) 2 GB.

4 Indique el rol de servidor que no pertenece a Windows Server 2008:
- a) Servidor DNS.
- b) Directorio Activo.
- c) Servidor VNC.
- d) Servidor DHCP.

4 Puesta en marcha del sistema

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer los diferentes tipos de usuario y grupos del sistema.
- ✓ Administrar los usuarios del sistema.
- ✓ Configurar las directivas de seguridad para proteger el sistema.
- ✓ Administrar los volúmenes del sistema.
- ✓ Administrar las cuotas de disco de los usuarios.
- ✓ Establecer los permisos adecuados en el sistema de ficheros.

4.1 ADMINISTRACIÓN DE USUARIOS

Las cuentas de usuario son una parte muy importante de la estructura de la seguridad de Windows ya que controlan el acceso a uno o varios ordenadores. Son la clave para conceder a los usuarios autorizados el acceso a los componentes dentro del entorno de Windows. Si se implantan correctamente, las cuentas proporcionan una forma cómoda y segura para permitir que los usuarios accedan a los recursos del sistema o de la red.

La administración de usuarios se realiza de dos formas diferentes dependiendo si el servidor es o no es un controlador de dominio:

- **El administrador de usuarios**. Administra la seguridad de las estaciones de trabajo y servidores miembro o servidores autónomos (no controladores del dominio).
- **El administrador de usuarios para dominios**. Administra la seguridad en el controlador principal o de reserva del dominio (controlador de dominio).

Las características de seguridad proporcionadas por el administrador de usuarios consisten en la creación de cuentas de usuarios y de grupo, la asignación de derechos de usuario y el establecimiento de relaciones de confianza entre diferentes dominios.

4.1.1 USUARIOS

Una cuenta de usuario contiene toda la información que define a ese usuario en particular dentro del entorno de Windows. Todo lo que se necesita es asociarle un identificador de seguridad de usuario (SID). La seguridad de las cuentas de usuario puede incluir un nombre único de usuario, una contraseña y los permisos que el usuario tiene para utilizar el sistema y acceder a los recursos. Cada usuario del sistema posee una cuenta de usuario y una contraseña asociada para su uso individual.

Las cuentas de usuario pueden definirse en una máquina local o en el dominio. Las cuentas definidas en la máquina local solo pueden utilizarse en esa máquina, mientras que las cuentas definidas en el dominio pueden utilizarse en cualquier máquina que pertenezca a ese dominio o en algún dominio de confianza.

Windows 2008 proporciona dos cuentas de usuario predefinidas:

- **Administrador**. La cuenta administrador posee control total sobre las operaciones y la seguridad del sistema completo. Cualquiera que pueda iniciar una sesión como administrador posee control total sobre la administración del sistema completo. Esto es un punto muy importante debido a que la cuenta Administrador y sus equivalentes deben ser totalmente de confianza.

  La cuenta Administrador está pensada para el individuo que administra la configuración del sistema. Un mal uso de la cuenta puede ser desastroso debido a los derechos y permisos asociados.

- **Invitado**. Está pensada para los usuarios que se conecten muy ocasionalmente al sistema. Sin embargo, se recomienda que nunca se use la cuenta Invitado, sino que se creen cuentas temporales que proporcionen unos controles de responsabilidad y auditoria mejores. Por defecto, la cuenta está desactivada y configurada como miembro del grupo local Invitados. Posee una contraseña vacía y no se puede cambiar su perfil por el perfil de usuario predeterminado.

Es recomendable utilizar la cuenta del administrador solamente para tareas administrativas.

4.1.2 EL ADMINISTRADOR DE USUARIOS

El administrador de usuarios permite gestionar de una manera fácil los usuarios y los grupos de usuarios en Windows 2008. Para utilizar el administrador de usuarios en el menú de inicio pulse el botón derecho del ratón sobre el *Equipo*, seleccione *Administrar* y luego *Usuarios y grupos locales* que se encuentra en la categoría *Configuración* del *Administrador del Servidor* (véase la Figura 4.1). Otra forma de acceder a la administración de usuarios y grupos locales es a través de la herramienta *Administración de equipos*, dentro de la categoría *Herramientas del sistema*.

Figura 4.1. *Usuarios y grupos locales en Administrador del Servidor / Configuración*

Si utilizas un Directorio Activo, para administrar los usuarios deberás utilizar la herramienta "Administración de usuarios y equipos del directorio activo" (véase el Capítulo 8).

4.1.2.1 Crear una cuenta de usuario

Para crear una nueva cuenta de usuario hay que hacer los siguientes pasos:

1 Seleccione el menú *Usuarios* de la barra de menús (en *Usuarios y grupos locales*) y dentro de este menú seleccione la opción *Usuario nuevo...* haciendo clic con el botón derecho.

2 En la ventana que aparece (véase la Figura 4.2) debe indicar los datos de la nueva cuenta de usuario, siendo el único campo obligatorio el referente al nombre de usuario. El resto de los campos que aparecen son: *nombre de usuario*, *nombre completo*, *descripción*, *contraseña* y *confirmar contraseña*.

Figura 4.2. *Dar de alta un usuario*

Además de estos campos, el cuadro de diálogo *Usuario nuevo* contiene una serie de casillas de verificación referentes a la contraseña y a la disponibilidad de la cuenta. Estas casillas y su significado son las siguientes: *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*, *El usuario no puede cambiar la contraseña*, *La contraseña nunca caduca* y *Cuenta deshabilitada*.

ACTIVIDADES 4.1

- Examina los usuarios y grupos que tiene el sistema por defecto.
- Crea un nuevo usuario y dalo de alta en el grupo *Administradores*.
- Accede al sistema con el usuario anterior.
- Habilite la cuenta de invitado del sistema.

4.1.2.2 Propiedades de un usuario

Para ver las propiedades de un usuario pulse dos veces sobre el usuario y aparecerá la ventana *Propiedades* (véase la Figura 4.3). El número de pestañas que aparece en la ventana *Propiedades* varía dependiendo de los servicios que tenga instalados en el sistema.

Figura 4.3. *Usuarios (propiedades de un usuario)*

A continuación se van a ver las pestañas más utilizadas: *General*, *Miembro de* y *Perfil*.

La pestaña *General* muestra la información suministrada a la hora de crear un nuevo usuario.

En la pestaña *Miembro de* aparece el listado de grupos al que pertenece el usuario. Para modificar los grupos a los que pertenece un usuario utilice los botones *Agregar* o *Quitar*. Si pulsa *Agregar* aparece un cuadro de diálogo (ver Figura 4.4) que permite escribir los nombres de los grupos a los pertenecerá el usuario. Si no se acuerda de los nombres de los grupos puede verlos pulsando el botón *Avanzadas*.

Figura 4.4. *Gestión de grupos*

En la pestaña *Perfil* (véase la Figura 4.5) puede establecer el perfil y el directorio particular de un usuario.

Figura 4.5. *Pestaña "Perfil" de la carpeta "Propiedades de usuario"*

A la hora de definir la *Carpeta particular* para un usuario, el administrador debe tener en cuenta si la ubicación del directorio es local o no. Si es local, entonces ese directorio únicamente será visto cuando el usuario se conecte desde la máquina en la que se ha definido, mientras que si utiliza un directorio de red, éste será visible independientemente de dónde se establezca la conexión.

Para definir estos directorios, basta con escribir el camino completo junto con el nombre de éste en el cuadro de texto apropiado, que será el cuadro titulado *Ruta de acceso local*. En el caso de tratarse de un directorio compartido debe seleccionarse la opción *Conectar a*; además, debe indicar la letra de la unidad en la que quiere asignar el directorio y en el cuadro de texto escribir la dirección (*Nombre_máquina**nombre_recurso_compatido*\).

ACTIVIDADES 4.2

- Crea una cuenta de usuario.
- Deshabilita la cuenta de usuario creada en el paso anterior.
- Accede al sistema con el usuario creado para ver lo que ocurre.
- Da de alta los usuarios *jefe1*, *empleado1* y *empleado2*.
- Crea el grupo de usuarios *empleados*.
- Añade al grupo *empleados* los usuarios *empleado1* y *empleado2*.

4.1.2.3 Comandos

Aunque lo normal es utilizar el entorno gráfico, también puede administrar los usuarios del sistema utilizando el *Símbolo del sistema*. En la Tabla 4.1 se muestran los comandos más utilizados.

Tabla 4.1. Comandos para la administración de usuarios

Comando	Ejemplo	Descripción
net user	net user	Muestra los usuarios del sistema (véase la Figura 4.6).
net user <login> <pass> /add	net user encarni hola00== /add	Añade un usuario con una determinada contraseña.
net user <login> <pass>	net user encarni hola00==	Cambia la contraseña del usuario.
net user <login> /del	net user encarni /del	Borra un usuario.
net localgroup <grupo> <usuario> /add	net localgroup Administradores encarni /add	Añade un usuario dentro del grupo.

Figura 4.6. net user

Si deseas conocer más opciones consulta la ayuda ejecutando:

```
C:\> net help user
```

ACTIVIDADES 4.3

- Crea la cuenta de usuario *prueba* por comandos.
- Inicie sesión con el usuario *prueba*.
- Elimine por comandos el usuario *prueba*.

4.1.3 DIRECTIVAS DE SEGURIDAD LOCAL

Uno de los puntos más importantes de un sistema es la fortaleza de las contraseñas de los usuarios. Si un usuario que tiene muchos privilegios utiliza como contraseña "*hola*", entonces el sistema corre un grave peligro. Quizás la organización tenga una seguridad casi perfecta, pero una contraseña débil puede suponer revelar los secretos de la organización, su uso para iniciar un ataque por denegación de servicio o incluso sabotear la red. Salvo que se utilicen métodos de autenticación de varios factores para todos los usuarios en la red (p.e. huella dactilar, tarjeta), debe implementar las opciones de seguridad de contraseña.

Dentro de *Inicio, Herramientas administrativas* puede ejecutar la herramienta *Directivas de seguridad local* para establecer los requisitos que deben cumplir las contraseñas de los usuarios (véase Figura 4.7).

Figura 4.7. *Configuración de seguridad local*

Existen tres tipos de directivas de cuentas: las directivas de contraseñas, las directivas de bloqueo de cuentas, y las directivas Kerberos.

Las directivas de contraseña permiten indicar cómo es la contraseña de los usuarios. Las directivas de las contraseñas que puede establecer son las siguientes:

- **Forzar el historial de las contraseñas**. Permite obligar a los usuarios a que no repitan las últimas contraseñas utilizadas anteriormente.
- **Vigencia máxima y mínima de la contraseña**. Permite establecer el tiempo máximo de la contraseña (vigencia máxima) y el tiempo mínimo que debe tener el usuario la contraseña (vigencia mínima). Al finalizar el período de vigencia de la contraseña el sistema le obliga al usuario a que cambie su contraseña.
- **Longitud mínima de la contraseña**. Determina el número mínimo de caracteres que un usuario debe utilizar en su contraseña. Cuanto más larga la contraseña, más difícil será comprometerla. No obstante, uno de

los efectos colaterales de exigir contraseñas largas es que los usuarios utilizan contraseñas fáciles de averiguar o que las escriban en algún lugar.

- **Las contraseñas deben cumplir los requerimientos de complejidad**. Si activa esta opción se exige que todas las contraseñas tengan, al menos, seis caracteres de longitud y que incluyan caracteres de tres de estas cuatro categorías: letras mayúsculas, letras minúsculas, números o símbolos.

  Además, la contraseña no puede contener ni el nombre de cuenta del usuario ni parte del nombre completo del usuario en más de dos caracteres consecutivos. También puede utilizar otros caracteres ACSII en las contraseñas como ½ (Alt + 233). Además, si la organización tiene sus propios requisitos de seguridad de las contraseñas, podrá crear un filtro de contraseñas personalizado e instalarlo en cada controlador del dominio. El fichero que proporciona el filtro integrado es *passfilt.dll*.

- **Almacenar contraseñas usando cifrado reversible para todos los usuarios del dominio**. Activar esta opción debilita significativamente la seguridad de las contraseñas y solo se debe hacerlo si es totalmente necesario.

Tabla 4.2. Configuración predeterminada de directiva de contraseña

Configuración	Valor predeterminado	Intervalo
Exigir historial de contraseñas	Se recuerdan 24 contraseñas en controladores de dominio, 0 en servidores independientes	0 a 24
Vigencia máxima de la contraseña	42 días	0 a 998
Vigencia mínima de la contraseña	1 día en controladores de dominio, 0 en servidores independientes	0 a 998
Longitud mínima de la contraseña	7 caracteres en controladores de dominio, 0 en servidores independientes	0 a 14
Las contraseñas deben cumplir los requerimientos de complejidad	Habilitado en controladores de dominio, Deshabilitado en servidores independientes	Habilitado o deshabilitado
Almacenar contraseñas haciendo uso de cifrado reversible para todos los usuarios del dominio	Deshabilitado	Habilitado o deshabilitado

Es recomendable que establezca una política de seguridad que permita que las contraseñas tengan una longitud mínima de 8 caracteres y que cumplan los requerimientos de complejidad.

También puede definir **directivas de bloqueo de cuentas** para todo el dominio o para cuentas locales en equipos individuales mediante las directivas de seguridad. En la Tabla 4.3 puede ver la configuración predeterminada de bloqueo de cuentas.

Tabla 4.3. Configuración predeterminada de bloqueo de cuenta

Configuración	Valor predeterminado	Intervalo
Duración del bloqueo de cuenta	No se puede aplicar	1 - 99.999 minutos (Un valor de 0 nunca reestablecerá el número de intentos erróneos realizados en un determinado intento de inicio de sesión).
Umbral de bloqueo de cuenta	0 intentos de inicio de sesión incorrectos (deshabilitado)	0 a 999 intentos.
Reestablecer el bloqueo de cuenta después de	No se puede aplicar	1 - 99.999 minutos (Un valor de 0 necesitará que un administrador desbloquee la cuenta).

Las **directivas locales** del equipo permiten indicar qué puede hacer el equipo y quién lo puede hacer. Por ejemplo, con las directivas locales puede establecer quién puede apagar el ordenador, quién puede utilizar la unidad CD-ROM, etc.

Figura 4.8. Directivas locales

ACTIVIDADES 4.4

- Modifique las directivas de seguridad local para que las contraseñas de los usuarios tengan una longitud de 10 caracteres y tengan una vigencia de 30 días.

4.2 SISTEMA DE FICHEROS

Con el *Administrador de discos* puede administrar fácilmente el almacenamiento en disco para proporcionar a sus usuarios un sistema de ficheros flexible, rápido y seguro.

4.2.1 ADMINISTRADOR DE DISCOS

La herramienta *Administración de discos*, que se muestra en la Figura 4.9, es la herramienta para administrar el subsistema de disco, lo que incluye cualquier unidad extraíble, tales como unidades USB, disco duro, etc. Se puede utilizar para administrar particiones o volúmenes, para asignar letras de unidad, formatear, etc.

Figura 4.9. *Administración de discos de Windows 2008*

El administrador de discos distingue dos tipos de discos: discos dinámicos o discos básicos. El modo de utilización de cada tipo de disco duro es diferente, mientras que los discos duros dinámicos permiten la utilización de volúmenes (p.e. discos espejo), los discos básicos se utilizan de la forma tradicional mediante particiones.

De forma predeterminada, todos los discos son básicos. Para convertir un disco en dinámico, seleccione el disco duro, pulse el botón derecho y seleccione la opción *Convertir en disco dinámico*. De forma análoga, si quiere convertir un disco de dinámico a básico seleccione el disco, pulse el botón derecho y seleccione la opción *Convertir en disco básico*.

El tipo de disco duro, básico o dinámico, lo puede ver junto a la descripción del disco duro (véase la Figura 4.9).

Aunque inicialmente el sistema realiza la distinción entre discos duros básicos y dinámicos a partir de Windows 2008, ambos se utilizan de forma idéntica permitiendo únicamente la creación de volúmenes.

Para crear un volumen seleccione una unidad de disco dinámica, pulse el botón derecho, y seleccione el tipo de volumen que desea crear y aparece el asistente que le guía durante todo el proceso. Los tipos de volúmenes existentes son:

- **Volumen simple**. Un volumen simple se compone por espacio libre de un único disco dinámico (disco normal).
- **Volumen distribuido (RAID 0)**. Un volumen distribuido se forma a partir de la capacidad de varios discos dinámicos. Cree un disco distribuido para crear volúmenes de gran tamaño.
- **Volumen seccionado**. Un volumen seccionado almacena datos en bandas de dos o más discos dinámicos. Un volumen seccionado proporciona un acceso más rápido a sus datos que un volumen simple y distribuido. La diferencia con el anterior tipo es que si utiliza un volumen seccionado las operaciones de lectura y escritura, se realizarán en paralelo en los discos duros que componen la banda.
- **Volumen reflejado (RAID 1)**. Un volumen reflejado o disco espejo duplica sus datos en dos discos dinámicos. De esta forma si se rompe un volumen se conservan los datos en la otra unidad.
- **RAID 5**. Para crear un volumen en RAID 5 necesita tener, como mínimo, tres discos duros. El nivel RAID 5 proporciona un nivel de rendimiento superior al nivel 1 (volumen reflejado).

Una vez seleccionado el tipo de volumen, seleccione los discos duros dinámicos que quiere utilizar (véase la Figura 4.10), y pulse *Siguiente*. Asigne la letra de la unidad o ruta de acceso y pulse *Siguiente*. Seleccione el tipo de formato que quiere utilizar, y pulse *Siguiente* para finalizar el proceso (antes se muestra un resumen de las opciones elegidas).

Figura 4.10. *Selección de discos en el Asistente para crear volúmenes*

Una vez finalizado el proceso de formateo del sistema de ficheros, el administrador de discos muestra el estado de las unidades (véase Figura 4.11). En la figura puede ver como se ha creado un disco espejo a partir de dos unidades de disco.

Figura 4.11. Asistente para crear volúmenes

Si quiere seguridad en su sistema debe utilizar el sistema de ficheros NTFS. Aunque lo más lógico es elegirlo durante la instalación, en cualquier momento puede realizar la conversión de FAT a NTFS usando el comando *convert* de la siguiente forma:

```
C:\> convert unidad: /fs:ntfs
```

La herramienta "Desfragmentación" permite mejorar la velocidad del sistema ficheros y la herramienta "Comprobación de errores" permite reparar cualquier error en el sistema de ficheros.

ACTIVIDADES 4.5

- Apague el equipo e instale dos nuevos discos duros.
- Crea un sistema RAID 1 con los dos nuevos discos duros.
- Asígnale al sistema RAID la etiqueta *Datos*.

4.2.2 CUOTAS DE DISCO

Las cuotas de disco permiten realizan un seguimiento y controlar el uso del espacio de disco de los volúmenes. Los administradores suelen utilizan las cuotas de usuario para:

- Evitar que se utilice más espacio de disco y registrar un suceso cuando un usuario sobrepase un límite de espacio de disco especificado.
- Registrar un suceso cuando un usuario sobrepase un nivel de advertencia de espacio de disco especificado.

Para habilitar la cuota de disco en un volumen, vaya a *Equipo*, seleccione la unidad, pulse el botón derecho, elija *Propiedades* y abra la pestaña *Cuota* -o bien desde la herramienta de *Administración de discos*-. Tal y como muestra la Figura 4.12, cuando habilite cuotas de disco puede configurar dos valores: el límite de la cuota de disco y el nivel de advertencia de la cuota de disco. El límite especifica la cantidad de espacio de disco que puede utilizar un usuario. El nivel de advertencia especifica el punto en el que el usuario se acerca al límite de cuota. Por ejemplo, puede configurar un límite de cuota de disco de 100 MB y un nivel de advertencia de cuota de disco de 90 MB. En este caso, el usuario no puede almacenar más de 100 MB de ficheros en el volumen y si el usuario almacena más de 90 MB se puede hacer que el sistema de cuotas de disco registre un suceso de sistema.

Figura 4.12. *Administrador de las cuotas de disco*

Puede especificar que los usuarios tengan la posibilidad de superar su límite de cuota. Puede ser útil habilitar cuotas y no limitar el uso del espacio de disco cuando no se desea denegar a los usuarios el acceso a un volumen, pero sí realizar un seguimiento del uso del espacio de disco por parte de cada usuario. También puede especificar si debe registrarse o no un suceso cuando los usuarios superen su nivel de advertencia de cuota o su límite de cuota.

A partir del momento en el que habilite cuotas de disco para un volumen, se realiza automáticamente un seguimiento del uso cuantitativo del volumen que hagan los nuevos usuarios.

Para ver el listado de todos los usuarios que utilizan el sistema pulse en el botón *Valores de cuota* que se encuentra dentro de la pestaña *Cuota*. El ejemplo de la Figura 4.13 muestra como el usuario *Maria* ha excedido el límite establecido (100 MB), mientras que el usuario *Jperez* está por debajo del límite.

Figura 4.13. *Administrador de las cuotas de disco (Estado de las cuotas de usuario)*

Para utilizar las cuotas el formato del disco duro tiene que ser NTFS.

ACTIVIDADES 4.6

- Active las cuotas de disco, en el disco duro de datos, para que los usuarios *empleado1* y *empleado2* tengan un espacio de 10 MB de espacio en disco.
- Accede al sistema con el usuario *empleado1* y copia datos en el disco duro de datos para intentar superar la cuota de disco. ¿Qué ocurre?
- Accede al sistema como administrador y examina el estado de la cuota del usuario.

4.3 PERMISOS

Los sistemas Windows ofrecen una gran libertad para establecer los permisos de acceso a un sistema de ficheros o carpeta ya que permite establecer los permisos para cualquier usuario o grupo de usuarios.

Los permisos que se pueden establecer para un usuario o grupo son: *Control Total*, *Modificar*, *Lectura y ejecución*, *Mostrar el contenido de la carpeta*, *Lectura*, *Escritura* y *Permisos especiales*. Lo mejor es clasificar los permisos en dos grupos: *Lectura* y *Escritura*. Los permisos de *Lectura* son *Lectura y ejecución*, *Mostrar el contenido de la carpeta* y *Lectura*. Y los permisos de *Escritura* son todos aquellos que implican poder cambiar el contenido de la carpeta o archivo. Si desea permitir en un recurso la escritura lo mejor es activar el permiso *Control Total*.

Para ver los permisos de acceso a un recurso (p.e. carpeta o disco duro) hay que seleccionar la carpeta, pulse el botón derecho y seleccione *Propiedades*. Tal y como puede ver en la Figura 4.14, en la pestaña *Seguridad* se muestran los permisos de la carpeta. En la parte superior se muestra el listado de los usuarios y grupos. Si selecciona un usuario o grupo en la parte inferior se muestran sus permisos.

Figura 4.14. *Permisos de una carpeta*

Un aspecto importante que hay que tener en cuenta es que los permisos se pueden establecer directamente a la carpeta o ser heredados de una carpeta superior. Por ejemplo, en la Figura 4.14 puede ver que los *Usuarios* tienen permisos de lectura en la carpeta *e:\Documentos*. Como los permisos aparecen sombreados, los permisos se heredados de la carpeta superior que en este caso es *E:*. Si desea cambiar estos permisos puede cambiarlos directamente en *E:*. Pero si desea en algún momento "romper" la herencia entonces tiene que pulsar el botón *Opciones Avanzadas* y en la ventana que aparece en la Figura 4.15 desactive la casilla *Incluir todos los permisos heredables del objeto primario de este objetivo* y automáticamente el sistema preguntará si desea copiar o eliminar los permisos del objeto superior.

Figura 4.15. *Permisos - Configuración avanzada*

Para modificar los permisos pulse el botón *Editar* y en la ventana que aparece en la Figura 4.16 puede añadir los usuarios o grupos a los que quiere establecerle los permisos de acceso.

Figura 4.16. *Permisos de una carpeta*

ACTIVIDADES 4.7

- Crea dentro del disco duro de datos la carpeta *Proyectos*.
- Establece los permisos de la carpeta *Proyectos* para que el usuario *jefe1* tenga control total, y el grupo *empleados* solo tenga acceso de lectura y el resto de usuarios no tenga ningún permiso.
- Accede al sistema con los usuarios *jefe1* y *empleado1* y comprueba que se han establecido correctamente los permisos.

RESUMEN DEL CAPÍTULO

En este capítulo ha aprendido a realizar la administración de los usuarios y grupos del sistema.

Se ha explicado a administrar el sistema de ficheros para crear los diferentes tipos de volúmenes de disco.

Además, se ha explicado a activar y administrar las cuotas de disco para limitar y monitorizar el espacio de disco duro que utilizan los usuarios en el sistema.

Por último, ha aprendido a establecer los permisos a los usuarios en el sistema de ficheros.

EJERCICIOS PROPUESTOS

- **1.** ¿Se puede cambiar el nombre de usuario *Administrador* para que sea *Admin*?
- **2.** ¿En qué carpeta se guardan los datos de los usuarios? ¿Qué contenido tiene la carpeta?
- **3.** ¿Indique las ventajas más importantes de formatear un disco duro en NTFS o FAT?
- **4.** ¿Cómo puede ver el estado de funcionamiento de un sistema RAID?
- **5.** ¿Se pude establecer la cuota de disco a un grupo de usuarios?
- **6.** Dentro del mismo disco duro, ¿se pueden establecer cuotas de usuario para las carpetas de forma diferente? (p.e. *D:/datos* que no tenga cuota y que la carpeta *D:/programas* tenga una cuota de 100 MB).
- **7.** Si un usuario excede su cuota de usuario, ¿cómo puede modificar su cuota?

TEST DE CONOCIMIENTOS

1 Indique la acción que realiza el comando *net user*:
a) Permite añadir un usuario.
b) Elimina a todos los usuarios del sistema.
c) Muestra a los usuarios del sistema.
d) Muestra los grupos y usuarios del sistema.

2 Indique la opción que no pertenece a las directivas de contraseña:
a) Forzar el historial de las contraseñas.
b) Almacenar contraseñas usando cifrado reversible para todos los usuarios del dominio.
c) Dos usuarios no pueden tener la misma contraseña.
d) Longitud mínima de la contraseña.

3 Indique el sistema de ficheros recomendable para instalar Windows 2008:
a) Ext2.
b) Fat.
c) Fat32.
d) NTFS.

4 Indique la respuesta correcta sobre la herencia de un directorio:
a) Permite que un archivo o carpeta tenga los mismos permisos que su directorio padre.
b) Permite que todos los hijos de un directorio padre no hereden sus permisos.
c) Obliga a que un directorio tenga los mismos permisos que sus hijos.
d) Permite cambiar el directorio padre de un archivo.

5 Administración básica del sistema

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer las diferentes fases y elementos que intervienen en el arranque del sistema.
- ✓ Distinguir entre los conceptos *servicio* y *proceso*.
- ✓ Administrar los servicios y procesos del sistema.
- ✓ Realizar la planificación de tareas del sistema.
- ✓ Conocer y utilizar las diferentes herramientas de monitorización.
- ✓ Conocer los diferentes elementos para monitorizar el sistema.
- ✓ Realizar, programar y restaurar las copias de seguridad.

5.1 ARRANQUE Y PARADA

5.1.1 CONFIGURACIÓN DEL GESTOR DE ARRANQUE DEL SO

Hay varias formas de indicar al gestor de arranque: el programa *osloader* es un sistema operativo para utilizar al iniciar el sistema.

Para configurar el gestor de arranque, en el menú de *Inicio*, seleccione *Equipo*, pulsar el botón derecho seleccione *Propiedades* y ejecute *Configuración avanzada del sistema*. En la sección *Inicio y recuperación* pulse el botón *Configuración*. En la ventana que se muestra en la Figura 5.1 puede especificar el sistema operativo que se inicia por defecto y el tiempo de espera que se muestra en el menú de inicio

Figura 5.1. *Inicio y recuperación de nuestro sistema*

Además, también permite indicar la acción que debe realizar el sistema operativo ante un fallo grave.

Otra forma de administrar el gestor de arranque es ejecutando la herramienta *msconfig* (véase la Figura 5.2).

Figura 5.2. *msconfig / Arranque*

ACTIVIDADES 5.1

- Ejecute *msconfig* y determine los programas que se inician al arrancar el sistema.

5.1.2 SERVICIOS DEL SISTEMA

Los servicios son aplicaciones que se ejecutan independientemente del usuario. Normalmente se asocia los servicios solo a servicios de red (Web, FTP, etc.), pero los servicios proporcionan una gran funcionalidad al sistema operativo (p.e. monitores del sistema, administración de actualizaciones). Para ejecutar el administrador de servicios vaya a *Inicio*, *Herramientas administrativas* y ejecute *Servicios* (ver Figura 5.3).

Figura 5.3. *Administrador de servicios*

Para ver las propiedades de un servicio haga doble clic con el ratón sobre el servicio deseado (véase la Figura 5.4). En la ficha *General*, bajo *Tipo de inicio* puede seleccionar el modo de inicio del servicio: manual, automático, automático (inicio retrasado) o deshabilitado. Si lo desea, puede modificar el estado actual del servicio pulsando los botones: *Iniciar*, *Detener*, *Pausar* o *Reanudar*.

Figura 5.4. *Administrador de servicios (propiedades de un servicio)*

En Windows, muchos servicios se instalan de forma predeterminada con el sistema operativo. Es conveniente evaluar cada servicio para determinar si es necesario. Deshabilite cualquier servicio que no necesite, con el fin de minimizar las posibles vías de ataque de su equipo y optimizar el rendimiento del equipo.

Es importante que solo ejecute los servicios necesarios para el correcto funcionamiento de su sistema.

Si quieres administrar los servicios del sistema por comandos puedes ejecutar el comando:

```
C:\> net service
```

ACTIVIDADES 5.2

- Examine los servicios que se encuentran ejecutándose en el sistema.
- Utilice el administrador de servicios y configure el servicio que quieras para que ante el primer y segundo fallo se reinicie el servicio, y en el tercer fallo se reinicie el servidor.
- Utilice el comando *net service* para ver los servicios que se encuentran activos en el sistema.

5.1.3 PROCESOS

Los procesos son programas en ejecución por parte del usuario o del sistema. En el caso de que lo ejecute el sistema entonces son servicios.

Para administrar los procesos del sistema hay que utilizar el *Administrador de tareas de Windows*. Para ejecutar el administrador de tareas pulse las teclas CTRL + ALT + SUPR o sobre la barra de herramientas pulse el botón derecho del ratón y seleccione *Administrador de tareas*.

Tal y como puede ver en la Figura 5.5, en la pestaña *Procesos* puede ver todos los procesos que se ejecutan en el sistema. Para cada proceso puede ver su nombre, descripción, nombre de usuario que lo ejecuta, porcentaje de uso de CPU y de memoria RAM.

Al pulsar sobre un proceso, las tareas más importantes que se pueden realizar son:

- **Finalizar proceso**. Permite "matar" o finalizar la ejecución de un proceso. Esta tarea es muy utilizada en el caso de que un programa no responda.
- **Prioridad**. La prioridad permite determinar la preferencia del proceso sobre otros procesos para que lo ejecute el sistema operativo. Los tipos de prioridad, de mayor a menor, son: *Tiempo real*, *Alta*, *Por encima de lo Normal* o *Por debajo de lo normal*.
- **Abrir ubicación de archivos y Propiedades**. Ambas opciones permiten obtener información sobre el proceso: ubicación del ejecutable, permisos, etc.

Figura 5.5. Administrador de tareas de Windows

ACTIVIDADES 5.3

- Ejecute la calculadora del sistema.
- Ejecute el *Administrador de tareas*, localice el proceso que corresponde a la calculadora y finalice su ejecución.

5.1.4 PROGRAMACIÓN DE TAREAS

La programación de tareas es una herramienta muy útil ya que facilita la administración del sistema facilitando la ejecución de tareas en un momento determinado o cada cierto intervalo de tiempo. Por ejemplo, puede programar una copia de seguridad, el reinicio de un servicio, la ejecución de un determinado programa, etc.

La herramienta administrativa *Programador de tareas* permite crear y administrar las diferentes tareas que el equipo ejecuta de forma automática en el momento especificado.

Una vez iniciado el programador de tareas, puede ver las tareas programadas por el usuario pulsando directamente en la *Biblioteca del Programador de tareas* y, en la parte superior, aparecen las tareas que ha creado el usuario. Si expande el árbol puede ver las diferentes tareas que tiene programado el software del sistema.

Figura 5.6. *Programador de tareas*

Para programar una nueva tarea pulse en *Programación de tarea básica* y realice los siguientes pasos:

1. Especifique el nombre y descripción de la tarea.
2. Indique cuándo quiere ejecutar la tarea: diariamente, semanalmente, mensualmente, una vez, al iniciar el equipo, al iniciar sesión o cuando se registre un evento específico.
3. Indique la acción que desea realizar. Las acciones que se pueden realizar son: *Iniciar un programa*, *Enviar un correo electrónico* o *Mostrar un mensaje*.
4. Por último, pulse *Finalizar*.

ACTIVIDADES 5.4

- Inicie el programador de tareas y examine la biblioteca de tareas.
- Crea una nueva tarea para que se desfragmente semanalmente los discos duros del sistema.
- Crea una nueva tarea para que cada día a las 0:05h se eliminen todos los ficheros que se encuentran en el directorio *c:/tmp*.

5.1.5 PROCESO DE PARADA DEL SISTEMA

El proceso de parada del sistema resulta realmente sencillo ya que lo único que hay que hacer, una vez cerradas todas las aplicaciones, es ir al menú de *Inicio*, pulsar en la flecha que se encuentra junto al botón *Cerrar sesión*, seleccionar el botón de apagado y aparecerá la ventana de apagado del sistema (ver Figura 5.7).

Figura 5.7. *Pantalla para salir del sistema*

Windows 2008 ofrece la posibilidad de realizar un seguimiento sobre los sucesos de apagado o reinicio del equipo. El rastreador de sucesos de apagado ofrece un medio para realizar un seguimiento sistemático de los motivos por los que se reinicia o se apaga el equipo. Los sucesos se clasifican en "esperado" y "no esperado". En ambos casos el administrador deberá introducir el motivo por el cual se produjo el suceso.

El rastreador de eventos registra el motivo de cada apagado o inicio a través del servicio de registro de eventos. Puede utilizar el visor de eventos para abrir el registro del sistema y buscar los sucesos que han producido el reinicio o apagado del equipo. En la Figura 5.8 puede ver como el sistema registra los eventos y los muestra en el visor de eventos, por ejemplo el de la instalación correcta de Windows.

Figura 5.8. *Ejemplo de evento registrado en el sistema*

Si detecta que el equipo se reinicia o apaga inesperadamente utilice el visor de sucesos para determinar las causas que lo producen.

ACTIVIDADES 5.5

- Examine el registro de Windows para ver las veces que se ha apagado el equipo.

5.2 MONITORIZACIÓN DEL SISTEMA

La monitorización de equipos, usuarios, servicios y recursos del sistema operativo es una parte fundamental de la administración. Hay que seleccionar lo que se desea monitorizar y después, a través de los registros de sucesos, controlar los patrones de uso, los problemas de seguridad y las tendencias de tráfico. Windows 2008 R2 proporciona varias formas para la monitorización del sistema:

- **El monitor de confiabilidad y rendimiento**. Permite monitorizar en tiempo real el sistema, su estabilidad y rendimiento y posibilita crear alertas y registros de seguimiento.
- **El visor de eventos**. Permite ver lo que ha pasado en el sistema.

5.2.1 MONITOR DE CONFIABILIDAD Y RENDIMIENTO

Supervisar el rendimiento del sistema es una parte importante del mantenimiento y de la administración de Windows 2008. Los datos de rendimiento se utilizan para:

- Comprender la carga de trabajo y el efecto que produce en los recursos del sistema.
- Observar los cambios y las tendencias en las cargas de trabajo y en el uso de los recursos, de modo que se puedan planificar las futuras actualizaciones.
- Comprobar los cambios de configuración u otros esfuerzos de ajuste mediante la supervisión de los resultados.
- Diagnosticar problemas y componentes o procesos de destino para la optimización.

Figura 5.9. Monitor de confiabilidad y rendimiento

5.2.1.1 Monitor de rendimiento

Permite ver en tiempo real el uso de los recursos del sistema (ver Figura 5.10).

Figura 5.10. Monitor de rendimiento

Para añadir un contador al monitor del sistema, pulse en el botón de añadir y aparece la ventana *Agregar contadores* tal y como muestra la Figura 5.11 Seleccione el contador deseado y pulse el botón *Agregar*. Acepte para confirmar la adición del contador.

Figura 5.11. Monitor de rendimiento (agregar contadores)

El monitor de rendimiento permite monitorizar cualquier elemento del sistema: desde el rendimiento de la CPU al número de bits que transmite la interfaz de red *eth0*. Para conocer los posibles elementos que se pueden monitorizar pulse el *checkbox Mostrar descripción* y aparecerá en la parte baja de la ventana una breve descripción sobre cada elemento.

ACTIVIDADES 5.6

- Utilice el monitor del sistema para ver el estado de la CPU mientras que se ejecuta una aplicación (p.e. Internet Explorer).
- Configure el monitor del sistema para ver la actividad de la red y del disco duro mientras descarga un fichero de Internet.

5.2.1.2 Monitor de confiabilidad

El monitor de confiabilidad permite observar la estabilidad del sistema así como los eventos que tienen impacto en la estabilidad y detalles sobre ellos (véase la Figura 5.12). Ofrece un gráfico sencillo de estabilidad con el cual de un vistazo puede ver si el sistema ha mostrado estabilidad. También muestra el informe de estabilidad del sistema, con información de todos los eventos que tienen impacto en la estabilidad, clasificados en las siguientes cinco categorías: *Instalaciones y desinstalaciones de software*; *Errores de aplicación*; *Errores de hardware*; *Errores de Windows*; y *Errores varios*.

Figura 5.12. *Monitor de confiabilidad*

ACTIVIDADES 5.7

- Utilice el monitor de confiabilidad para ver las estadísticas de funcionamiento del sistema.

5.2.1.3 Conjunto de recopiladores de datos e informes

Los *conjuntos de recopiladores de datos* aumentan las capacidades de seguimiento del *Monitor de confiabilidad y rendimiento* ya que permiten almacenar información de registro y traza así como generar alertas.

Figura 5.13. *Conjuntos de recopiladores de datos e Informes*

Si desea crear un nuevo conjunto pulse el botón derecho, seleccione *Nuevo Conjunto de recopiladores de datos*, y podrá crear el conjunto a partir de una plantilla o manualmente. Para tener una mayor libertad seleccione *Crear manualmente (avanzado)*. En la ventana que se muestra en la Figura 5.14, debe seleccionar los tipos de datos que desea incluir en la recopilación:

- **Crear registro de datos**. Existen tres posibilidades para elegir el origen de los datos para el registro: *Contador de rendimiento* (para crear un registro de datos con los valores de los contadores de rendimiento que previamente ha indicado), *Datos de seguimiento de eventos* (registran los datos reunidos por el proveedor del sistema operativo o uno o más proveedores que no sean del sistema, por ejemplo programas; los sucesos registrados por el proveedor del sistema son: creación/eliminación de procesos, creación/eliminación de subprocesos, E/S de disco; TCP/IP de red, errores de página; y detalles de archivo) e *Información de configuración del sistema*.
- **Alerta del contador de rendimiento**. Permite definir alertas a partir del valor de los contadores del sistema. Una vez establecidos los límites de los contadores, la alerta es creada y puede ser plenamente configurada haciendo clic con el botón derecho y *Propiedades*. Dispone de diferentes pestañas para la configuración de la programación de la alerta, para establecer una condición para detener la alerta (duración o límite), planificación de acciones para la alerta y cuando ésta finalice y otras muchas más opciones.

Figura 5.14. Creación de recopiladores de datos y alertas

El uso de las capacidades de los conjuntos de recopiladores de datos tiene ciertas ventajas. La información de registros históricos puede exportarse a hojas de cálculo y bases de datos para analizarse y generar informes.

ACTIVIDADES 5.8

- Crea una alerta para que envíe un mensaje cuando el uso de CPU supere el 5%.

5.2.2 VISOR DE EVENTOS

El visor de eventos permite ver y administrar los registros de sucesos, recopilar información sobre los problemas hardware y software, y supervisar los sucesos de seguridad de Windows. Los sucesos se dividen en dos categorías generales: registros de Windows y registros de aplicaciones y servicios. Dentro de estas dos categorías además tiene otras subcategorías:

- **Registros de Windows**. Contiene eventos de Aplicación, Seguridad, Instalación, Sistema y Eventos Reenviados (originalmente deshabilitado).
- **Registros de aplicaciones y servicios**. Contiene eventos de Hardware, Internet Explorer, Key Management Service, Microsoft, Replicación DFS, Servicio de Directorio, Servicio de replicación de archivos, Servidor DNS...

Además existe la posibilidad de crear y examinar vistas personalizadas sobre cualquiera de los registros que se estén realizando.

Para abrir el visor de eventos, haga clic en *Inicio*, seleccione *Herramientas administrativas* y a continuación pulse en *Visor de eventos* (véase la Figura 5.15).

Figura 5.15. *Visor de eventos del Sistema (falta imagen)*

De forma predeterminada, el sistema registra cuatro tipos de sucesos:

- **Registro de aplicación**. Contiene los sucesos registrados por las aplicaciones o programas. Por ejemplo, un programa de base de datos podría grabar un error de fichero en el registro de aplicación.
- **Registro del sistema**. Contiene los sucesos registrados por los componentes de Windows. Por ejemplo, el error de la carga de un controlador u otro componente del sistema durante el inicio se graba en el registro del sistema. Los tipos de sucesos registrados por los componentes del sistema están predeterminados.
- **Registro de seguridad**. Permite grabar los sucesos de seguridad, como los intentos de inicio de sesión válidos y no válidos, y los sucesos relativos al uso de recursos como crear, abrir o eliminar ficheros. Un administrador puede especificar los sucesos que se van a grabar en el registro de seguridad. Por ejemplo, si ha habilitado la auditoria de inicios de sesión, los intentos de inicio de sesión en el sistema se graban en el registro de seguridad.
- **Registros de instalación**. Permite grabar los sucesos que ocurran al añadir o eliminar funciones y características de Windows, aplicaciones...

Dependiendo de cómo esté configurado el equipo se registran o no otros sucesos. Por ejemplo, si el equipo está configurado como controlador de dominio registra sucesos en dos registros adicionales: **Registro del servicio de directorio** y **Registro del servicio de replicación de archivos**.

Los tipos de sucesos que registra el sistema son: *Crítico*, *Error*, *Advertencia*, *Información*, *Acceso correcto auditado* y *Acceso erróneo auditado*.

El servicio registro de eventos de Windows se inicia automáticamente al iniciar Windows 2008. Todos los usuarios pueden ver los registros de aplicación y del sistema, pero solo los administradores tienen acceso a los registros de seguridad.

El registro de seguridad está desactivado de forma predeterminada. Puede utilizar Directiva de grupo para habilitar el *Registro de seguridad*. El administrador también puede establecer directivas de auditoria en el Registro que hagan que el sistema se detenga cuando el registro de seguridad esté lleno.

ACTIVIDADES 5.9

- Realice varios intentos de inicio de sesión con un usuario y contraseña incorrectos.
- Inicie sesión como *Administrador* y compruebe que se ha generado la alerta del intento fallido de sesión.

5.3 COPIAS DE SEGURIDAD

En Windows, las copias de seguridad se pueden realizar de dos formas diferentes: desde el intérprete de comandos o desde la herramienta gráfica de *Copias de Seguridad de Windows*. A continuación se va a ver la utilización de la herramienta gráfica por ser ésta la forma más habitual de realizar las copias de seguridad.

Si desea información sobre cómo realizar copias de seguridad con el intérprete de comandos ejecute:

```
C:\> wbadmin /?
```

La herramienta *Copias de Seguridad de Windows* permite, de una forma fácil y eficaz, realizar y restaurar copias de seguridad. Las copias de seguridad se pueden realizar de forma puntual o puede programar el trabajo para que se realice en un determinado momento (p.e. mensualmente).

Para abrir la herramienta de *Copias de seguridad de Windows* vaya a las propiedades de una unidad de disco y en la carpeta *Herramientas* pulse en el botón *Realizar copias de seguridad ahora* (véase la Figura 5.16), o bien vaya a *Inicio*, *Herramientas Administrativas*, *Copias de seguridad de Windows*.

Figura 5.16. *Propiedades del sistema C: (Herramientas)*

Si es la primera vez que utiliza la herramienta de *Copias de seguridad de Windows* el sistema informa que no se ha realizado ninguna copia de seguridad.

Figura 5.17. *Copias de seguridad de Windows*

A través del menú que aparece a la derecha (véase la Figura 5.17) puede realizar las siguientes acciones a través de asistentes:

- **Hacer programación de copia de seguridad**. Es un asistente que le ayudará para realizar copias de seguridad de archivos y carpetas de manera periódica según haya programado. Para programar copias de este tipo se debe elegir de qué desea realizar la copia de seguridad (de un servidor completo o solo algunos volúmenes), cuándo y con qué frecuencia se realizará la copia de seguridad y en qué discos duros desea almacenar la copia de seguridad.
- **Hacer copia de seguridad una vez**. Al igual que el caso anterior, se trata de un asistente que le ayudará en la creación de copias de seguridad de sus archivos y carpetas, pero éstas serán únicas por lo que no es necesario especificar una planificación para las copias.
- **Recuperar**. El asistente para restauración le ayuda a restaurar sus datos guardados previamente en una copia de seguridad.
- **Configurar opciones de rendimiento**. Para optimizar el rendimiento de las copias de seguridad se pueden elegir las opciones de realizar siempre copias de seguridad completas (de todos los archivos y carpetas del volumen seleccionado), siempre incrementales (solo de los archivos y carpetas que han cambiado o que no fueron copiados anteriormente para el volumen seleccionado), o personalizarlas completas o incrementales para cada uno de los volúmenes disponibles.
- **Conectarse a otro equipo**. Permite conectarse a otro equipo para administrar sus copias de seguridad.

Para realizar o restaurar una copia de seguridad debe utilizar una cuenta que pertenezca al grupo "Operadores de copia" o "Administradores".

5.3.1 REALIZAR UNA COPIA DE SEGURIDAD

Para realizar una copia de seguridad debe iniciar o bien el asistente para realizar la programación de una copia o bien el asistente para hacer una copia de seguridad una vez (aislada), dependiendo del tipo de copia de seguridad que desea realizar.

Recuerde que el tipo de copia de seguridad (completa o incremental) debe ser especificado antes de configurar la copia desde el asistente Configurar opciones de rendimiento.

En la Figura 5.18 puede apreciar la ventana inicial del asistente para realizar la **programación de una copia de seguridad periódica**, donde se muestra una introducción al proceso. El asistente, además de para crear copias de seguridad programadas sirve para modificar las existentes y cancelarlas.

Figura 5.18. Crear una copia de seguridad

Para realizar una copia de seguridad primero tiene que elegir el tipo de copia: copia de seguridad del servidor completo o bien de determinados volúmenes (personalizada). Después de haber seleccionado el servidor completo o volúmenes individuales que contengan datos, estado del sistema, aplicaciones, etc., para la copia se seguridad, hay que seleccionar si se va a realizar la copia una vez al día o varias veces (véase la Figura 5.19).

Figura 5.19. *Especificar la hora de la copia de seguridad*

El siguiente paso es elegir uno o varios discos destino donde se almacena la copia de seguridad. Por defecto se muestran los discos con una capacidad aceptable para la copia, aunque si pulsa el botón *Mostrar todos los discos disponibles...*, puede seleccionar alguno del resto de discos. En el caso de que quiera modificar una copia anterior, puede agregar nuevos discos para almacenar las copias o bien eliminarlos. Finalmente, etiquete el disco destino con la información que se facilita y aparecerá una ventana de confirmación. Pulse *Finalizar* para confirmar la creación de la copia de seguridad programada y se formatearán los discos destino y se aplicarán los cambios realizados. Al final, se muestra un informe sobre el proceso de creación de la copia de seguridad programada.

Figura 5.20. *Opciones de copia de seguridad*

Además, si lo desea, puede realizar una **copia de seguridad una vez de manera aislada**. Al iniciar el asistente (véase la Figura 5.20) tiene la posibilidad de elegir realizar una copia única basándonos en las configuraciones de copias de seguridad programas anteriores o bien con una configuración diferente (opción única si es la primera copia de seguridad que realizamos). Después, el proceso es similar al descrito anteriormente: seleccione si quiere realizar la copia del servidor completo o personalice la copia a determinados volúmenes, seleccione el almacenamiento para la copia (local o en carpetas compartidas remotas) y el tipo de copia de seguridad en función de su uso. Finalmente,

se muestra la ventana de confirmación y pulse el botón *Copia de Seguridad* para realizar la copia. Cuando finalice la copia, se muestra un informe con el resultado de la operación (ver Figura 5.21).

Figura 5.21. *Información sobre el trabajo de copia de seguridad*

5.3.2 RECUPERAR UNA COPIA DE SEGURIDAD

El método para restaurar una copia de seguridad es muy sencillo: inicie el asistente *Recuperar...* (véase la Figura 5.22 que recoge la ventana inicial del asistente) y seleccione si desea recuperar los datos desde el equipo local o desde otro equipo. Si selecciona el equipo local debe elegir la unidad donde se encuentra la copia de seguridad a restaurar, si por el contrario elige otro equipo tiene que especificar si la copia se encuentra en una unidad de disco o en una carpeta compartida. El siguiente paso consiste en seleccionar la fecha y hora de la copia de seguridad que se utiliza para realizar la recuperación y el tipo de recuperación que queremos: de archivos y carpetas, aplicaciones o volúmenes. A continuación, debe seleccionar los elementos que desea recuperar.

Figura 5.22. *Asistente Recuperar... para copias de seguridad (Inicio)*

Finalmente, el asistente permite seleccionar algunas opciones dependiendo del tipo de recuperación que se va a realizar. En el caso de que se encuentre recuperando archivos y carpetas seleccione la ubicación de los elementos que quiere recuperar y el tratamiento que se les dará en el caso de que se encuentren duplicados, además de los permisos que se les asignarán. Si selecciona la recuperación de aplicaciones, puede seleccionar la ubicación de la aplicación (si mantener la original o seleccionar una nueva). Pulse *Finalizar* y aparecerá una ventana que muestra el progreso de recuperación (véase la Figura 5.23).

Figura 5.23. *Progreso de la recuperación*

5.3.3 CONFIGURAR OPCIONES DE RENDIMIENTO

La ventana de configuración de las opciones de rendimiento (ver Figura 5.24) permite optimizar el rendimiento de la copia de seguridad y el servidor seleccionando el tipo de copia de seguridad (completa o incremental) que se realizará. Las opciones que se pueden configurar son:

- **Rendimiento de copia de seguridad normal**. Si selecciona esta opción se realiza una copia de seguridad completa independientemente del volumen (o volúmenes) que seleccione para la copia. Esta opción reduce la velocidad de la copia aunque proporciona un nivel de seguridad superior.
- **Rendimiento de copia de seguridad más rápido**. Si selecciona esta opción se realiza una copia de seguridad incremental sobre la copia de seguridad anterior. Este tipo de copia puede reducir el rendimiento del volumen hasta en un 200%.
- **Personalizar**. Sin duda se trata de una opción muy interesante pues permite seleccionar para cada volumen el tipo de copia de seguridad que a realizar: completa o incremental.

Figura 5.24. *Configurar opciones de rendimiento*

En la ventana "Conectarse a otro equipo" puede indicar el equipo al que quiere administrar las copias de seguridad.

ACTIVIDADES 5.10

- Crea la carpeta *D:/prueba* y copia en la carpeta los ficheros que consideres oportuno.
- Realice una copia de seguridad del disco duro de datos (*D:*) y que se almacene en el disco duro del sistema operativo (*C:*).
- Elimine la carpeta *D:/prueba*.
- Restaure la copia de seguridad creada anteriormente y compruebe que se ha restaurado la carpeta que ha eliminado en la actividad anterior.
- Programe una copia de seguridad semanal del disco duro de datos (*D:*).

RESUMEN DEL CAPÍTULO

En este capítulo se ha descrito el proceso de arranque y parada del sistema.

Se ha explicado a configurar el proceso de arranque del sistema teniendo especial cuidado en los servicios que se ejecutan en el sistema.

Además, ha aprendido planificar tareas y a administrar los procesos y servicios del sistema.

También ha aprendido a monitorizar el sistema para ver su comportamiento.

Por último, ha aprendido a realizar, recuperar y planificar las copias de seguridad del sistema.

EJERCICIOS PROPUESTOS

1. ¿Qué diferencia hay entre un servicio y un proceso?

2. Indique dos formas para ver los servicios que se ejecutan en el sistema.

3. Si es posible deshabilite el servicio RPC, ¿qué pasa?

4. Enumere las diferentes categorías de elementos que se pueden monitorizar con la herramienta de monitorización.

TEST DE CONOCIMIENTOS

1 Indique los cuatro tipos de sucesos que guarda el sistema:

a) Registro de aplicación, sistema, seguridad y instalación.
b) Registro de aplicación, sistema, usuario y instalación.
c) Registro de aplicación, seguridad, usuario y instalación.
d) Solo existen tres registros aplicación, usuario y seguridad.

2 Indique la herramienta que permite ver si se ha producido un fallo durante el inicio o la parada del sistema:

a) Visor de eventos.
b) Monitor de eventos.
c) Rastreador del sistema.
d) Ninguna de las anteriores.

3 Indique la frecuencia con la que es posible programar una copia de seguridad:

a) Diaria.
b) Semanal.
c) Mensual.
d) Todas son correctas.

4 Indique la afirmación incorrecta:

a) Una copia de seguridad completa es aquella que copia toda la información.
b) Una copia de seguridad incremental copia únicamente los ficheros que se han modificado.
c) Windows únicamente permite realizar copias de seguridad incrementales y completas.
d) Todas son correctas.

6 Administración de la red

OBJETIVOS DEL CAPÍTULO

- ✓ Diseñar e implementar los diferentes servicios de red.
- ✓ Planificar la implementación de un esquema de red.
- ✓ Instalar y configurar los diferentes servicios de red.
- ✓ Planificar la seguridad del sistema.
- ✓ Utilizar el servicio de escritorio remoto y servidor de aplicaciones.
- ✓ Configurar el servicio de actualización de sistemas.

6.1 ESQUEMA BÁSICO DE RED

Cualquier red de cierto tamaño necesita utilizar los servicios de enrutamiento, DHCP y DNS. El servicio de enrutamiento permite que el sistema pueda comunicar una red interna con la red externa como por ejemplo, Internet. El servicio DHCP permite que los ordenadores obtengan la configuración IP de forma automática. Este servicio es muy útil en el caso de conectar un portátil a la red para que obtenga su dirección IP de forma automática. Por último, los servidores DNS traducen los nombres de los *host* en direcciones IP, o viceversa.

A lo largo de la unidad se va a implementar en el servidor el esquema de red que se muestra en la Figura 6.1. Para ello, hay que realizar los siguientes pasos:

- Configurar correctamente las dos interfaces de red para que una permita el acceso a Internet y la otra a la red interna.
- Activar el servicio de enrutamiento para que los equipos de la red interna tengan acceso a Internet.
- Configurar el servidor DHCP para que los equipos cliente puedan obtener su dirección IP automáticamente.

Figura 6.1. *Esquema de red*

ACTIVIDADES 6.1

- Añade al equipo o Máquina Virtual una segunda tarjeta de red.
- Configure un equipo o Máquina Virtual como cliente tal y como indica la Figura 6.1 (p.e. puede utilizar Windows XP).

6.1.1 CONFIGURACIÓN DE LA RED

Para que el equipo trabaje correctamente en red es necesario configurar la dirección IP y el nombre del equipo.

6.1.1.1 Configuración del protocolo TCP/IP

Una vez instalado el adaptador de red, pulse en el enlace *Administrar conexiones de red* que se encuentra en el *Centro de redes y recursos compartidos* dentro del *Panel de control* y aparece la ventana de *Conexiones de red* que muestra las conexiones de red que hay instaladas en el equipo (ver Figura 6.2).

Figura 6.2. *Conexiones de red en el Centro de redes y recursos compartidos*

Para facilitar las tareas de administración, cambie el nombre de los adaptadores de red por uno que refleje mejor la red a la que está conectada (p.e. Internet, Red interna).

Seleccione la conexión de red que quiere configurar, pulse el botón derecho, elija *Propiedades* y en la ventana que aparece en la Figura 6.3 se muestran las propiedades del adaptador de red.

Figura 6.3. *Propiedades del adaptador de red*

En las propiedades del adaptador aparecen los servicios, clientes y protocolos que hay instalados. Si desea instalar o desinstalar algún servicio adicional utilice el botón *Instalar* o *Desinstalar*, respectivamente.

Para que funcione el adaptador, como mínimo, tiene que tener instalado el protocolo TCP/IP (versión 4, aunque también se encuentra ya disponible la versión 6). Para configurar el protocolo, seleccione *Protocolo de Internet* (TCP/IPv4 o TCP/IPv6) pulse el botón *Propiedades* y aparece la ventana de *Propiedades de Protocolo de Internet* (véase Figura 6.4).

Figura 6.4. *Propiedades del protocolo de Internet (TCP/IP)*

Existen dos formas de configurar el protocolo TCP/IP:

- **De forma automática**. En este caso, un servidor DHCP proporciona los parámetros de conexiones a la red. Por motivos de seguridad, no se recomienda utilizar esta opción con servidores.
- **De forma manual**. Esta opción es la recomendada para servidores o para equipos que dan servicios a otros usuarios de la red. Los parámetros que debe configurar son: *Dirección IP*, *Máscara de red*, *Puerta de enlace* y *Servidores DNS*.

Si lo desea, una interfaz de red puede utilizar varias direcciones IP. Para ello, en la pestaña *Propiedades* del protocolo TCP/IP pulse en el botón *Opciones avanzadas* y añada las direcciones IP que desee utilizar.

Si desea ver por consola la configuración de las interfaces de red puede ejecutar:

```
C:\> ipconfig
```

ACTIVIDADES 6.2

- Configure las interfaces de red del servidor tal y como muestra la Figura 6.1.
- Compruebe que el servidor tiene conexión a Internet.

6.1.1.2 Configuración del nombre del equipo y dominio

Para que su equipo funcione correctamente en el entorno de red hay que asignarle un nombre y el grupo de trabajo o dominio al que pertenece. Para cambiar el nombre del equipo e indicar el grupo de trabajo o dominio al que pertenece en la ventana *Propiedades del sistema* seleccione la pestaña *Nombre del equipo* y pulse en el botón *Cambiar*. En la ventana que puede ver en la Figura 6.5 escriba el nombre del equipo y el nombre del grupo de trabajo o dominio al que pertenezca el equipo.

Figura 6.5. *Propiedades del nombre del equipo*

ACTIVIDADES 6.3

- Asígnale al servidor el nombre *"servidorpruebas"*.
- Asígnale al equipo que actúa como cliente de la red el nombre *"oficina1"*.

6.1.2 ENRUTAMIENTO

El servicio *Enrutamiento y acceso remoto* permite que una red interna pueda tener acceso a Internet a través del servidor de Windows 2008. Para instalar el servicio debe ejecutar la herramienta *Administración del servidor* y añadir una nueva funcionalidad. Para ello pulse en *Agregar Roles*, seleccione *Servicios de acceso y directivas de redes* y a continuación seleccione el servicio *Enrutamiento y acceso de remoto*.

Una vez instalado el servicio, debe ejecutar la herramienta administrativa *Enrutamiento y acceso remoto*. Seleccione el servidor, pulse el botón derecho, seleccione *Configurar y habilitar Enrutamiento y acceso remoto*. En el asistente que se inicia debe indicar la siguiente configuración:

- Indique el tipo de servicio que desea utilizar. Para permitir que la red interna tenga acceso a Internet seleccione *Traducción de direcciones de red (NAT)*.
- Indique la interfaz de red que tiene acceso a Internet (Figura 6.6).
- Finalmente habilite el servicio.

Figura 6.6. *Asistente para la instalación del servicio de Enrutamiento*

ACTIVIDADES 6.4

- Configure el servicio de enrutamiento para que el servidor permita el acceso a Internet de la red interna.
- Compruebe que el equipo cliente tiene conexión a Internet.
- Desde el equipo cliente realice un *ping* a *www.google.es* y a la IP de servidor. ¿Qué ocurre? ¿Por qué no se puede realizar un *ping* al servidor?

6.1.3 FIREWALL DE WINDOWS

El cortafuegos de Windows Server 2008 es un cortafuegos basado en *host* que permite crear filtros para las conexiones entrantes y salientes del servidor. Además de permitir una fácil configuración, gracias a su interfaz avanzada es posible crear diferentes perfiles (conjuntos de reglas del cortafuegos y seguridad de las conexiones) que se pueden aplicar según la categoría del equipo (p.e. Red interna, VPN y Servidores). También permite la creación de reglas para reforzar las políticas de aislamiento del servidor y del dominio. Las reglas especificadas son más precisas y detalladas que en anteriores versiones, incluyendo filtros basados en usuario y grupos del Directorio Activo, direcciones IP origen y destino, número de puerto IP, configuraciones ICMP, configuraciones IPSec, tipos de servicios, interfaces, etc.

Para administrar el cortafuegos hay que ejecutar la herramienta administrativa *firewall de Windows con seguridad avanzada*. En la Figura 6.7 se muestra la ventana inicial donde puede observar las configuraciones que actualmente se están aplicando para los perfiles de dominio, red privada y red pública, permite acceso directo a todas las actividades y operaciones configurables del *firewall*.

Figura 6.7. *Ventana inicial del firewall de Windows con seguridad avanzada*

También tiene acceso a la documentación de ayuda y puede realizar acciones interesantes como la importación/exportación de directivas, la restauración de las predeterminadas y acceder a la ventana de propiedades del cortafuegos (ver Figura 6.8).

Figura 6.8. *Propiedades del firewall de Windows con seguridad avanzada*

Para aprender a administrar el *firewall* de Windows debe administrar los siguientes elementos:

- **Reglas de entrada**. Haciendo clic en *Reglas de entrada* se muestran las reglas existentes para comunicaciones entrantes al servidor. En la Figura 6.9 puede ver el listado de reglas de entrada con una amplia información sobre cada regla (nombre, grupo, perfil, si está habilitada o no la acción, protocolo, puerto local, puerto remoto, usuarios y equipos permitidos). Si selecciona una regla puede actuar sobre ella. Por ejemplo, puede habilitarla/deshabilitarla, eliminarla o ver sus propiedades.

Figura 6.9. *Reglas de entrada en firewall de Windows con seguridad avanzada*

Es posible filtrar o exportar el listado de reglas. Sin duda la operación más importante es la creación de nuevas reglas de entrada, para lo cual pulse en el enlace *Nueva regla* y siga los pasos del asistente que le guía durante todo el proceso (ver Figura 6.10).

Figura 6.10. Nueva regla de entrada en firewall de Windows con seguridad avanzada

- **Reglas de salida**. Al igual que en las reglas de entrada, se muestra el listado de todas las reglas con amplia información sobre cada una (véase la Figura 6.11).

Figura 6.11. Reglas de salida en firewall de Windows con seguridad avanzada

- **Reglas de seguridad de conexión**. La seguridad de conexión implica autenticar los equipos antes de que empiecen las comunicaciones y así asegurar la información que se envía entre ellos. El *firewall* de Windows utiliza IPSec para asegurar la comunicación mediante el intercambio de claves, la autenticación, la integridad de los datos y el cifrado de datos.
- **Supervisión**. Permite tener acceso al estado del *firewall* (ver Figura 6.12) y a cada uno de los perfiles (dominio, privado, público), ver las configuraciones predeterminadas, las reglas de entrada, de salida y de seguridad de conexiones. Haciendo clic en cada uno de los submenús de *Supervisión* puede obtener información más detallada.

Figura 6.12. *Supervisión en firewall de Windows con seguridad avanzada*

ACTIVIDADES 6.5

- Examine las reglas de entrada y de salida que tiene por defecto el *firewall* de Windows.
- Configure el *firewall* del servidor para que permita que los equipos de la red interna puedan realizar un *ping* al servidor.

6.1.4 DHCP

DHCP es un servicio fundamental para cualquier red basada en TCP/IP que tenga muchos clientes. DHCP permite que los clientes inicien y reciban de manera automática los parámetros de configuración IP (IP, máscara de red, puerta de enlace, etc.). El servicio DHCP es muy utilizado en ambientes donde hay un menor número de direcciones IP que de clientes (p.e. las conexiones a Internet). Al facilitar el servidor DHCP las direcciones IP de forma automática se consigue un mejor grado de utilización, ya que si un ordenador esta apagado o desconectado de la red, no utiliza ninguna dirección IP.

Para los dispositivos que necesitan mantener la dirección IP fija (p.e. servidor web, impresora en red), DHCP permite realizar una reserva de la dirección IP. De esta manera solo el dispositivo, a través de su dirección MAC, puede acceder a la dirección IP reservada.

La reserva de direcciones se utiliza para asignar de forma estática la dirección IP a un dispositivo que no debe cambiar de dirección IP. Por ejemplo, sería un inconveniente si una impresora de red cambia su dirección IP, ya que entonces se debería configurar continuamente el ordenador para poder imprimir.

Para instalar el servidor DHCP puede utilizar la herramientas administrativa *Administrador del servidor* y pulse en *Agregar roles*.

Una vez instalado el componente, pulse el botón derecho sobre *Equipo* y seleccione *Administrar* para abrir el *Administrador del servidor* y dentro del menú *Roles* en el *Administrador del servidor* pulse en *Servidor DHCP*. También puede seleccionar DHCP dentro del menú *Herramientas administrativas*. En la Figura 6.13 puede ver la administración del servidor DHCP en el *Administrador del servidor*.

Figura 6.13. *Servidor DHCP*

Cuando se inicia el servidor DHCP, Windows debe verificar si el servidor está autorizado para funcionar. Puede ver el estado del servidor gracias a la flecha que aparece junto al elemento DHCP. Si la flecha es roja indica que el servicio no está activo, y si es verde indica que el servidor está funcionando correctamente. En la ventana que se encuentra en la Figura 6.13 puede comprobar que el servidor está activo.

Si es la primera vez que inicia el servidor DHCP y está dentro de un dominio, verá que el servidor no esta activo. Para que un servidor DHCP pueda estar activo dentro de un dominio el administrador del dominio debe autorizar el servicio. Para autorizar el servicio pulse el botón derecho sobre *DHCP* y seleccione la opción *Administrar servidores autorizados* para añadir el servidor (también puede utilizar la opción *Agregar servidor*).

No es recomendable instalar el servidor DHCP dentro de un controlador de dominio.

6.1.4.1 Primeros pasos

Antes de empezar a configurar el servidor DHCP, es importante tener claro el diseño lógico de la red. Los datos que necesita conocer de su red son:

- Direcciones IP que va a distribuir. Estas direcciones IP se indican a través de los **ámbitos de difusión**. Además, si dentro de un ámbito de difusión no quiere repartir de forma automática todas las direcciones entonces utilice **zonas de exclusión**.
- Direcciones IP que va a reservar de forma estática (p.e. para una impresora).
- Parámetros de configuración (puerta de enlace, servidores DNS, etc.).

A la hora de realizar el diseño lógico de la red es importante tener en cuenta que dentro de una red lógica (p.e. 192.168.0.0/24) solo puede existir un único ámbito de difusión. Por ejemplo, si quiere compartir las direcciones que van desde 192.168.0.50 a la dirección 192.168.0.100 y las direcciones que van desde la 192.168.0.150 a 192.168.0.199, no puede crear dos ámbitos de difusión: uno de la dirección 50 a 100; y otro desde la 150 a la 199. Para realizar el ejemplo propuesto debe crear un único ámbito de difusión (de la 50 a la 199) y excluir las direcciones que no quiere asignar dinámicamente (de la 100 a la 149).

6.1.4.2 Crear un ámbito de difusión

Para crear un ámbito de difusión siga los siguientes pasos:

1. Seleccione el servidor DHCP correspondiente en el árbol de consola. Hay que seleccionar el menú *Acción* y escoger *Ámbito nuevo* para ejecutar el asistente.

2. Escriba el nombre y la descripción del ámbito que va a crear y pulse *Siguiente*.

3. Indique el intervalo de direcciones que distribuye el ámbito. la máscara de red y pulse *Siguiente* (véase la Figura 6.14).

Figura 6.14. *Asistente para ámbito nuevo (intervalo de direcciones)*

4. Escriba el intervalo de direcciones IP que desea excluir y pulse *Siguiente*.

5. Determine la duración de la concesión. La duración de la concesión especifica durante cuánto tiempo un cliente puede utilizar una dirección IP. Pulse *Siguiente*.

6. Para configurar las opciones DHCP hay que seleccionar *Configurar estas opciones ahora*. En caso contrario, elija *Configurar estas opciones más tarde* y pulse *Siguiente*.

7. Si ha elegido especificar las opciones DHCP, debe introducir los siguientes datos: Dirección IP del enrutador o puerta de enlace, Nombre de dominio, servidores DNS y servidores WINS.

8. Para finalizar, debe indicar si quiere activar de manera inmediata el ámbito. Si escoge no, podrá activar el ámbito manualmente más adelante. Pulse *Siguiente* y a continuación *Finalizar* para completar el asistente.

Una vez finalizado el proceso, puede ver en el administrador de servidores DHCP que el ámbito se encuentra activo. Dentro del ámbito hay cuatro opciones:

- **Conjunto de direcciones**. Muestra el conjunto de direcciones y las zonas de exclusión del ámbito.
- **Concesión de direcciones**. Direcciones que actualmente se encuentran asignadas.
- **Reservas**. Direcciones IP que se han reservado de forma estática.
- **Opciones de ámbito**. En esta zona se encuentran las opciones que el servidor proporciona a los clientes.

A través de las opciones puede establecer los parámetros de configuración que van a recibir los ordenadores clientes (puerta de enlace, DNS, servidores de impresión, etc.). Existen tres formas de establecer las opciones:

- **De forma general**. Para todo el servidor dentro de la carpeta *Opciones del servidor*.
- **Para un determinado ámbito**. Seleccione la carpeta *Opciones de ámbito* dentro del ámbito que quiere configurar.
- **Para un determinado equipo**. Realice una reserva de la dirección IP que quiere que tenga el equipo y escriba las opciones dentro de la reserva.

Para configurar las opciones de una zona, pulse el botón derecho y seleccione la opción *Opciones de configuración*. En la ventana que se muestra en la Figura 6.15, seleccione las opciones que necesite y establezca sus valores correspondientes.

Figura 6.15. *Opciones de configuración*

6.1.4.3 Reservas

Para añadir una reserva de dirección hay que realizar los siguientes pasos:

1 Pulse la carpeta *Reservas* que se encuentra dentro del ámbito donde quiere realizar la reserva.

2 Con el botón derecho del ratón seleccione *Reserva nueva* y aparece la pantalla que puede verse en la Figura 6.16.

Figura 6.16. Reserva nueva

3 Escriba el nombre de la reserva, dirección IP y la dirección MAC del equipo.

4 Indique el tipo de cliente que va a utilizar la reserva: Solo DHCP, solo BOOTP o ambos. Pulse *Agregar*.

Si quiere conocer la dirección MAC de un adaptador de red ejecute el comando:

```
C:\> ipconfig /all
```

6.1.4.4 Estadísticas

El servidor DHCP proporciona dos tipos de estadísticas sobre el uso de las direcciones IP: por ámbito o para todo el servidor. Una vez seleccionado el elemento sobre el que quiere ver su estadística, pulse el botón derecho del ratón y seleccione *Mostrar Estadísticas* (véase la Figura 6.17).

Figura 6.17. Estadísticas de ámbito

ACTIVIDADES 6.6

- Instala y configura el servidor DHCP para que distribuya automáticamente las direcciones IP 10.0.0.200 a 10.0.0.250, con la puerta de enlace 10.0.0.1 y el servidor de nombres 8.8.8.8.
- Configure el equipo cliente de Windows para que obtenga la IP de forma automática.
- Compruebe que el equipo cliente obtiene del servidor correctamente la dirección IP, ¿cómo lo has hecho?
- Realiza una reserva para que el equipo cliente siempre obtenga la IP 10.0.250.

6.2 TERMINAL SERVER

Terminal Server permite que los usuarios se conecten de forma remota a un servidor utilizando el escritorio de Windows. Los servicios de Terminal Server se pueden utilizar de dos formas diferentes:

- Como *Escritorio remoto* para que el administrador acceda al sistema.
- Como *Servidores de aplicaciones* para que cualquier usuario pueda conectarse al servidor para ejecutar una determinada aplicación.

6.2.1 ESCRITORIO REMOTO

Para administrar el servidor tan solo es necesario activar el *Escritorio Remoto,* mientras que si quiere que todos los usuarios puedan acceder al sistema de forma remota, entonces hay que instalar el servicio *Terminal Server* y el *Administrador de licencias de Terminal Server.*

Para activar el escritorio remoto debe realizar los siguientes pasos:

1. En el menú de inicio, seleccione *Equipo*, pulse el botón derecho y seleccione *Propiedades.*
2. En la ventana que aparece pulse en *Configuración avanzada del sistema* y pulse en la pestaña de *Acceso remoto* (véase la Figura 6.18).
3. Finalmente active la casilla *Permitir las conexiones desde equipos que ejecuten cualquier versión de Escritorio remoto (menos seguro)* o *Permitir solo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red (más seguro).*

Figura 6.18. *Propiedades del sistema*

ACTIVIDADES 6.7

- Active el uso del escritorio remoto en el servidor.
- Desde el equipo cliente acceda al servidor utilizando la herramienta *Conexión a Escritorio Remoto*.

6.2.2 SERVIDOR DE APLICACIONES

En Windows 2008 los servicios de Terminal Server se instalan de igual forma que otros servicios, desde el *Administrador del servidor*, haciendo clic en el enlace *Añadir Roles* seleccione *Servicios de Escritorio remoto*. Al realizar la instalación el asistente permite añadir las diferentes funciones del Escritorio remoto entre las que destacan:

- **Host de sesión de Escritorio remoto**. Es el servicio básico de *Terminal Server* y permite que los usuarios se conecten de forma remota al servidor.
- **Administrador de licencias de Escritorio remoto**. Permite administrar las licencias de acceso al escritorio remoto de los usuarios del sistema.
- **Acceso web a escritorio remoto**. Permite a los usuarios conectarse al escritorio remoto a través de un navegador web.

Para instalar correctamente el servidor de Terminal Server debe realizar los siguientes pasos:

1. Seleccione las funciones *Host* de sesión de *Escritorio* remoto y el Administrador de licencias de *Escritorio* remoto. Pulse *Siguiente*.
2. Indique si desea requerir a los usuarios autenticación a nivel de red. Lo más cómodo es indicar que no desea requerir la autenticación a nivel de red. Pulse *Siguiente*.
3. Indique el modo de licencia que ha adquirido. Existen dos modos: por dispositivo o por usuario. Si desea probar los servicios de Terminal Server seleccione *Configurar más adelante* y dispondrá de 120 días de prueba.
4. Indique los grupos de usuarios que pueden utilizar los servicios y pulse *Siguiente* hasta finalizar la instalación.
5. Reinicie el servidor.

Una vez reiniciado el equipo, en el menú *Herramientas administrativas* puede ver la carpeta *Servicios de escritorio remoto* que tiene varias herramientas para administrar el escritorio remoto entre las que destacan.

- **Administrador de licencias de Escritorio Remoto**. Terminal Server requiere de licencias para que los clientes inicien sesiones en modo servidor de aplicaciones. Permite administrar las licencias de Terminal Server requeridas para conectarse a un servidor.
- **Administrador de RemoteApp**. Utilice esta herramienta si desea usar Terminal Server como *servidor de aplicaciones* de forma remota a usuarios (véase la Figura 6.19). Los programas *RemoteApp* son programas que aparentan ejecutarse de forma local en el equipo cliente pero que obtienen acceso al servidor a través del Escritorio Remoto.

Figura 6.19. Administrador de RemoteApp

- **Administrador de Servicios de Escritorio remoto**. Permite la monitorización y supervisión de los usuarios conectados, las sesiones y los procesos de servicio Terminal Server. Además, se pueden realizar ciertas tareas administrativas como desconectar o cerrar sesiones de usuarios.

Figura 6.20. Administrador de Servicios de Escritorio Remoto

- **Configuración de host de sesión de Escritorio remoto**. Se ejecuta localmente en cada servidor de terminales y permite modificar la configuración de las opciones del servidor Terminal Server (véase la Figura 6.21). Pueden ser configuradas las opciones de nuevas conexiones, modificar las existentes o eliminarlas: seguridad, sesiones de las mismas, entorno, adaptador de red, configuración del cliente, control remoto del escritorio del usuario y otras. Puede ver la configuración de una conexión haciendo clic con el botón derecho del ratón y seleccionando *Propiedades* (véase la Figura 6.22).

Figura 6.21. Configuración de Terminal Server

Figura 6.22. Propiedades de una conexión

- **Escritorios remotos**. Este complemento permite administrar las conexiones a *Escritorio remoto* de los servidores de Terminal Server. Permite administrar varios equipos desde una sola ubicación remota y, al mismo tiempo, cambiar fácilmente de conexión.
- **Acceso web a escritorio remoto**. Permite conectarse al *Escritorio remoto* del servidor a través de un navegador Web.

ACTIVIDADES 6.8

- Instale en Windows 2008 R2 el servidor de aplicaciones y de licencia de Terminal Server.
- Desde el equipo cliente conéctate al servidor utilizando la herramienta *Conectar a Escritorio Remoto*.
- En el servidor, ejecute la herramienta *Administrador de Servicios de Escritorio Remoto* y visualice las conexiones activas.
- Examine la información que proporciona el sistema sobre cada cliente de Escritorio Remoto.
- Desde el *Administrador de Servicios de Escritorio Remoto*, finaliza todas las sesiones activas por Escritorio Remoto.

6.2.3 CLIENTE DE TERMINAL SERVER

Para conectarse al servidor de Terminal Server necesita conectarse mediante un simple navegador web o utilizando una aplicación Windows o GNU/Linux.

6.2.3.1 Aplicación Windows

En anteriores versiones como Windows Server 2003 o Windows XP es necesario instalar el cliente de escritorio remoto. En cambio, a partir de Windows Server 2008 la aplicación cliente de escritorio remoto se instala por defecto en el sistema.

Para conectarse a un servidor hay que ejecutar la aplicación *Conexión a escritorio remoto* que se encuentra en *Programas*, escriba el nombre o la dirección IP del servidor y pulse *Conectar* (véase la Figura 6.23). Si desea modificar alguna opción en la conexión al servidor (p.e. resolución de pantalla), pulse el botón *Opciones* y se muestra un amplio menú de opciones para configurar la conexión.

Figura 6.23. *Conexión a escritorio remoto*

Una vez indicada la dirección del servidor pulse el botón *Conectar* y para acceder al sistema (véase la Figura 6.24).

Figura 6.24. *Conexión a Escritorio Remoto*

ACTIVIDADES 6.9

- Configure una conexión al servidor por escritorio remoto y en pantalla completa.
- Guarde la configuración de la conexión en el escritorio.

6.2.3.2 Aplicación GNU/Linux

Si desea conectarse desde un equipo GNU/Linux, a través del escritorio remoto, a un servidor Windows la mejor herramienta que puede utilizar cualquier visor RDP. Por ejemplo, para utilizar *Remote Desktop Viewer* debe realizar su instalación ejecutando:

- **UBUNTU**

```
# apt-get install gnome-rdp
```

- **FEDORA**

```
# yum install gnome-rdp
```

Una vez realizada la instalación, ejecute la aplicación *Remote Desktop Viewer* que se encuentra dentro del menú Internet. Para conectarse al servidor pulse *New* y en la ventana que se muestra en la Figura 6.25 indique la dirección del servidor al que quiere conectarse y pulse *Ok*.

Figura 6.25. *gnome-rdp (Ubuntu)*

ACTIVIDADES 6.10

- Las siguientes actividades solo las puedes realizar cuando hayas visto el Capítulo 9.
- Instale en un sistema GNU/Linux la aplicación *gnome-rpd.*
- Utilice *gnome-rdp* para conectarse al escritorio remoto de Windows 2008 R2.

6.2.3.3 Acceso web a escritorio remoto

Además de utilizar la herramienta *Escritorio remoto,* es posible conectarse al servidor a través de un simple navegador web instalando la función *Acceso web a Escritorio remoto* que se encuentra dentro de la categoría *Servicios de escritorio remoto.*

Una vez realiza la instalación para conectarse al servidor escriba en el navegador *http://IP/RDweb* donde, lógicamente, IP es la dirección IP o nombre del servidor. Tal y como puede ver en la Figura 6.26 para tener acceso al servidor debe introducir su nombre de usuario y contraseña.

Figura 6.26. *Acceso web de TS*

ACTIVIDADES 6.11

- Instale en el servidor el complemento *Acceso web a escritorio remoto.*
- Accede al servidor mediante el complemento *Acceso web a escritorio remoto.*

6.3 WINDOWS SERVER UPDATE SERVICES

Resulta de vital importancia tener correctamente actualizados los equipos clientes y los servidores de la red. Cuando tiene pocos equipos resulta fácil mantenerlos actualizados manualmente o a través de la herramienta *Windows update* que se encuentra en el *Panel de control*. Pero cuando dispone de cientos o incluso miles de equipos, este método resulta demasiado costoso.

Windows Server Update Services (WSUS) permite a los administradores de red especificar las actualizaciones de Microsoft que se deben instalar en los diferentes equipos de la red.

6.3.1 INSTALACIÓN

Para realizar la instalación de WSUS debe realizar los siguientes pasos:

1. Instale en el servidor el rol *Windows Server Updates Services.* Durante el proceso de instalación indique el directorio donde se almacenan los datos de WSUS (p.e. *c:\WSUS*).
2. Una vez completado el proceso de instalación se inicia un asistente (véase la Figura 6.27) que le permite configurar WSUS. Durante el asistente debe configurar los siguientes elementos:

- Servidor de sincronización de contenido. Indique el servidor desde el que quiere obtener las actualizaciones. Por defecto seleccione que quiere obtener las actualizaciones desde *Windows Update*.
- Seleccione los idiomas y productos Microsoft que tiene en la empresa y que desea sincronizar.
- Indique cuándo desea realizar la actualización. Se puede realizar manualmente o automáticamente a una determinada hora.

Figura 6.27. *Configuración de WSUS*

Para instalar WSUS es necesario que el servidor disponga de conexión a Internet.

6.3.2 CLIENTE

La manera más adecuada de configurar las actualizaciones automáticas depende del entorno de red. En un entorno de Active Directory, puede utilizar el objeto Directiva de grupo (GPO) de Active Directory. En un entorno que no sea un dominio hay que utilizar las Directivas de grupo local. Tanto si utiliza el objeto Directiva de grupo local o en un controlador de dominio, debe hacer que los equipos cliente utilicen el servidor WSUS y, después, configurar las actualizaciones automáticas.

Para configurar en un equipo cliente (p.e. Windows XP) para que utilice el servidor WSUS debe realizar los siguientes pasos:

1 Ejecute el comando *gpedit.msc* y, en la ventana que aparece en la Figura 6.28, acceda a *Configuración del equipo*, *Plantillas administrativas*, *Componentes de Windows* y finalmente Windows Update.

2 Habilite como mínimo las siguientes directivas:

- **Especificar la ubicación del servicio Windows Update de la Intranet**. Indique dónde se encuentra el servidor de actualización y de informes (por ejemplo, *http://10.0.0.1*).
- **Configurar actualizaciones automáticas**. Indique cuándo y cómo se van a descargar e instalar las actualizaciones.

Figura 6.28. *Directivas de grupo*

En el equipo cliente es necesario instalar el software más reciente de Windows Update.

6.3.3 ADMINISTRACIÓN

Una vez configurados los diferentes equipos clientes, para que obtengan las actualizaciones del servidor interno es necesario realizar las siguientes tareas:

6.3.3.1 Actualizaciones

Las actualizaciones son el eje principal del sistema y por lo tanto es necesario tener un completo control de las actualizaciones que se pueden o no instalar en los equipos de la red.

En la sección de actualizaciones (véase la Figura 6.29) se muestra un resumen de todas las actualizaciones disponibles. Para poder utilizar una actualización en los equipos de la red interna es necesario aprobarla antes. Se puede aprobar la actualización para instarla en cualquier equipo o en un grupo de equipos.

Figura 6.29. *Update Services - Actualizaciones disponibles*

Figura 6.30. *Actualizaciones*

Para aprobar una actualización tan solo es necesaria, pulsar el botón derecho y seleccionar *Aprobar* (véase la Figura 6.31).

Figura 6.31. *Progreso de aprobación*

6.3.3.2 Equipos

Una vez que los equipos clientes tienen configurado la dirección del servidor WSUS, estos se actualizan siguiendo la programación realizada.

Para ver los diferentes equipos que utilizan el servidor para actualizarse puede pulsar en *Equipo, Todos los equipos* y luego en *Equipos sin clasificar.* Como puede ver en la Figura 6.32, para cada equipo se muestra su nombre, dirección IP, sistema operativo y estado de actualización.

Figura 6.32. Update Services - Equipos

Si desea más información puede pulsar sobre un equipo y obtener un informe detallado de todas las actualizaciones del sistema (véase la Figura 6.33).

Para poder generar informes de actividad es necesario instalar en el servidor la herramienta Microsoft Report Viewer 2008.

6.3.3.3 Sincronizaciones

En la sección *Sincronizaciones* puede ver las sincronizaciones que ha realizado el servidor con Windows Update para descargar todas las actualizaciones y así poder distribuirlas a los clientes de la red.

Figura 6.33. *Update Services - Actualizaciones*

ACTIVIDADES 6.12

- Instale el servicio WSUS en el servidor.
- Sincronice el servidor para ver las actualizaciones disponibles.
- Revise las actualizaciones disponibles y autoriza aquellas que se puedan aplicar en Windows XP.
- Configure el equipo o MV de Windows XP para que utilice el servidor de actualizaciones.
- Fuerce la actualización del equipo cliente.

RESUMEN DEL CAPÍTULO

En este capítulo ha aprendido a implementar un esquema de red utilizando Windows. Para ello, ha aprendido a instalar y administrar los servicios de red más importantes.

Se han explicado los diferentes modos de acceso remoto al sistema.

Por último, ha aprendido a utilizar Windows Server Update Services para administrar las actualizaciones de los sistemas Windows de su red.

EJERCICIOS PROPUESTOS

- **1.** ¿Se puede cambiar el puerto en el que trabaja el Terminal Server?
- **2.** Busque algún programa que permita obtener las direcciones MAC de todos los ordenadores que se encuentran en la red.
- **3.** Indique la diferencia que hay entre el Servidor de Aplicaciones o activar solo el Escritorio Remoto.
- **4.** Indique los pasos que hay que realizar para utilizar el servicio WSUS en la red de una empresa.

TEST DE CONOCIMIENTOS

1 Indique el servicio que permite asignar automáticamente la configuración IP a un equipo:

a) DNS.
b) DHCP.
c) HTTP.
d) PHP.

2 Indique los elementos que permite administrar el *firewall* de Windows:

a) Reglas de entrada y salida.
b) Reglas de seguridad de conexión y supervisión.
c) Reglas de entrada, salida y seguridad de conexión.
d) Todas las anteriores son correctas.

3 Indique las formas de acceder de forma remota al servidor Windows:

a) Escritorio remoto.
b) Terminal Server.
c) Telnet.
d) SSH.

4 El servicio WSUS sirve permite:

a) La interconexión con sistemas GNU/Linux.
b) Actualizar los equipos de la red.
c) La transferencia de ficheros.
d) El acceso remoto al sistema.

7 Servidores de impresión y de archivos

OBJETIVOS DEL CAPÍTULO

- ✓ Compartir recursos.
- ✓ Ver los diferentes tipos de recursos compartidos.
- ✓ Utilizar las instantáneas del sistema.
- ✓ Administrar los sistemas de ficheros distribuidos.
- ✓ Instalar y administrar un servidor de impresión.

7.1 COMPARTIR ARCHIVOS E IMPRESORAS

Los servicios *de impresión* y *de archivos* permiten compartir impresoras y archivos entre otros sistemas Windows y, a través de SAMBA, con sistemas GNU/Linux. Este servicio es bastante importante por lo que se recomienda deshabilitar el servicio *Compartir archivos e impresoras* en las tarjetas de red que tengan acceso directo a Internet.

7.1.1 COMPARTIR UNA CARPETA

Para compartir una carpeta seleccione la carpeta, pulse el botón derecho del ratón y, en el menú contextual, seleccione *Compartir con* y *Usuarios específicos.* En la ventana que aparece (véase la Figura 7.1) indique los usuarios y/o grupos que tienen acceso a la carpeta compartida y sus respectivos permisos. Los permisos que se pueden establecer son: *Lectura* o *Lectura y escritura.*

Figura 7.1. *Propiedades de Carpeta (Compartir)*

Si desea ver todos los recursos compartidos del equipo entonces acceda a *Equipo* y en el menú de la derecha pulse en *Red* (véase la Figura 7.2).

Figura 7.2. *Recursos compartidos del equipo*

Las carpetas compartidas cuyo nombre termina en el símbolo $ son carpetas ocultas y por lo tanto no son visibles directamente desde el entorno de red.

7.1.2 ACCESO A UN RECURSO COMPARTIDO

Para acceder a una carpeta compartida tan solo debe escribir en el navegador *IP_servidor*, aparece una ventana de autenticación donde debe indicar sus datos de acceso y se muestran los recursos compartidos del sistema (véase la Figura 7.3).

Figura 7.3. *Recursos compartidos de un equipo*

Además puede hacer que la carpeta se monte automáticamente en el sistema. Para ello seleccione la carpeta, pulse el botón derecho y seleccione *Conectar a unidad de red...*. Tal y como puede ver en la Figura 7.4, a partir de ahora se encuentra en *Mi PC* la unidad *Z:* y cuando acceda a la unidad se utiliza automáticamente el recurso compartido.

Figura 7.4. *Conectar a unidad de red*

Si quiere montar la carpeta por comandos debe ejecutar:

```
C:\> net use x: \\servidor\carpeta_compartida
```

ACTIVIDADES 7.1

- Crea la carpeta *Proyectos* y *Programas* dentro del disco duro de datos.
- Comparte la carpeta *Proyectos* para que el usuario *jefe* tenga permisos de escritura y los demás usuarios tengan permisos de lectura.
- Comparte la carpeta *Programas* para que todos los usuarios tengan permisos de escritura.
- Desde un equipo cliente accede a los recursos compartidos del servidor y comprueba el correcto funcionamiento del sistema.
- Configure el equipo cliente para que el recurso compartido *Programas* se monte automáticamente en la unidad *Z:*.

7.1.3 ADMINISTRAR RECURSOS COMPARTIDOS

Para administrar de forma centralizada todos los recursos compartidos, conexiones, archivos abiertos, etc., hay que utilizar la herramienta administrativa *Administración de almacenamiento y recursos compartidos* (véase la Figura 7.5).

Figura 7.5. Administración de almacenamiento y recursos compartidos

Si selecciona una carpeta compartida y pulsa el botón derecho tiene disponibles las siguientes opciones:

- **Detener uso compartido**. Permite dejar de compartir un recurso compartido.
- **Propiedades**. Permite ver las propiedades más importantes de un recurso compartido, así como configurar los permisos del recurso y su configuración avanzada.
  - **Configuración avanzada**. Permite indicar el número máximo de usuarios que pueden acceder simultáneamente al recurso y permite establecer si el recurso compartido estará disponible para los usuarios desconectados del sistema y en qué modo.
  - **Permisos**. Permite indicar los permisos locales de la carpeta y los permisos del recurso compartido (véase la Figura 7.6).

Figura 7.6. Propiedades de un recurso compartido

ACTIVIDADES 7.2

- Accede al administrador de recursos compartidos y examina los recursos que se están compartiendo.
- Desde el equipo cliente accede al recurso compartido *C$* ¿Qué ocurre? ¿Qué consecuencias puede tener compartir ese recurso?

7.1.4 INSTANTÁNEAS

Las instantáneas permiten a los usuarios ver el contenido de las carpetas compartidas en momentos anteriores. La utilización de instantáneas es útil porque permite: **recuperar archivos eliminados o sobrescritos por accidente y comparar versiones de un archivo mientras trabaja**.

Para habilitar las instantáneas en una unidad de disco debe realizar los siguientes pasos:

1. Seleccione una unidad de disco, pulse el botón derecho y seleccione *Propiedades*.
2. Pulse en la pestaña *Instantáneas* (véase la Figura 7.7), seleccione la unidad de disco y pulse el botón *Habilitar*. Cuando habilite las instantáneas en un disco, Windows realiza directamente una instantánea del recurso compartido.

Figura 7.7. *Habilitar las instantáneas*

Para personalizar las instantáneas del equipo pulse el botón *Configurar* y, en la ventana que aparece en la Figura 7.8, puede establecer dónde se guardan, cuándo se ejecutan y el tamaño máximo que pueden ocupar en disco.

Figura 7.8. *Configuración de las instantáneas*

Para mejorar el rendimiento del sistema se recomienda que guarde las instantáneas en un sistema de ficheros diferente y que modifique la programación de acuerdo con las necesidades de la empresa.

Para acceder a una instantánea, primero debe acceder al recurso compartido, seleccione el recurso en el entorno de red, pulse el botón derecho y seleccione *Propiedades*. En la pestaña *Versiones anteriores* de las propiedades de la carpeta puede ver las instantáneas del recurso compartido (véase la Figura 7.9). Sobre una versión puede ver su contenido, copiar su contenido en un directorio o restaurar la versión.

Figura 7.9. *Instantáneas (Cliente)*

ACTIVIDADES 7.3

- Active las instantáneas del disco duro de datos.
- Desde el equipo cliente accede con el usuario *jefe1*, accede a la carpeta compartida */proyectos* y crea la carpeta *importante* con el contenido que estimes oportuno.
- Accede al servidor y fuerza la creación de una instantánea de la unidad de datos.
- Desde el equipo cliente elimina la carpeta *importante*.
- Accede a la instantánea creada anteriormente y recupera la carpeta borrada en el punto anterior.

7.1.5 SISTEMAS DE ARCHIVOS DISTRIBUIDOS

Un sistema de archivos distribuidos o DFS (*Distributed File System*) permite crear y almacenar un sistema de ficheros entre varios servidores del dominio. Un DFS resulta muy útil cuando quiera compartir información entre varias oficinas y garantizar una alta disponibilidad de los datos.

Dado que DFS asigna el almacenamiento físico de varios servidores como una representación lógica (una carpeta compartida), la ventaja es que la ubicación física de los datos se hace transparente para los usuarios y las aplicaciones.

Para instalar el servicio acceda a la herramienta administrativa *Administre su servidor*, pulse en *Agregar roles* y seleccione *Servidor de ficheros*. En la ventana que aparece en la Figura 7.10 seleccione la opción *Sistemas de ficheros distribuido (DFS)* y pulse *Siguiente*. A continuación se inicia el asistente de instalación que además de instalar DFS permite crear un recurso compartido. Para aprender mejor, en el proceso de instalación, no se va a crear el recurso compartido y se creará más adelante.

Figura 7.10. *Instalando DFS*

Para administrar los sistemas de archivos distribuidos se ejecuta la herramienta administrativa *Administración de DFS*.

Figura 7.11. *Administrador de DFS*

Un espacio de nombres es una representación lógica de un almacenamiento físico que se encuentra en uno o varios servidores del dominio. Desde el punto de vista del usuario un espacio de nombres es una carpeta compartida con una serie de subcarpetas que se encuentran en diferentes servidores.

Para crear un espacio de nombres hay que realizar los siguientes pasos:

1 En el *Administrador de DFS* (véase Figura 7.11) seleccione *Espacio de nombres*, pulse el botón derecho y seleccione *Crear nuevo espacio de nombres* para iniciar el asistente que le guiará durante todo el proceso (véase la Figura 7.12).

Figura 7.12. *Crear espacio de nombres*

2 Indique el nombre del servidor dónde se va alojar el espacio de nombres.

3 Escriba el nombre del espacio de nombres.

4 Indique el tipo de espacio de nombres. Existen dos tipos: **Espacio de nombres basado en dominio** o **Espacio de nombres independiente**. El espacio de nombres basado en dominio se almacena en uno o varios servidores aumentando así la disponibilidad del recurso. Para acceder al recurso debe escribir: *dominio**recursos* (p.e. *miempresa.com**recursos*). Por otro lado, el espacio de nombres independiente funciona igual que una carpeta compartida y para acceder a ella debe escribir *servidor**recursos* (p.e. *10.0.0.1**recursos*).

5 El asistente muestra un resumen de la configuración. Pulse *Crear*.

Una vez creado el espacio de nombres resulta muy útil realizar las siguientes operaciones:

- **Añadir carpetas al espacio de nombres**. Para ello en la pestaña *Espacio de nombres* pulse en *Nueva carpeta* e indique la carpeta compartida que desea enlazar.

Figura 7.13. Espacio de nombres

- **Añadir un nuevo servidor de espacio de nombres**. Resulta muy útil añadir más servidores al espacio de nombres para mejorar su disponibilidad. Para añadir un nuevo servidor siga los siguientes pasos:

  1. Seleccione el espacio de nombres, pulse el botón derecho y seleccione *Agregar servidor de espacio de nombres...*
  2. Escriba el nombre del servidor que va almacenar el espacio de nombres y pulse *Aceptar*.

Todos los servidores que tienen el espacio de nombres tienen que tener instalado el sistema de ficheros distribuido.

Si desea ver un resumen de los servidores dónde se almacena el espacio de nombres pulse en la pestaña *Servidores de espacio de nombres* (véase la Figura 7.14).

Figura 7.14. Servidores de espacio de nombres

- **Activar la replicación de datos**. La replicación de datos va a permitir que el contenido del espacio de nombres se duplique automáticamente en todos su servidores. Para activar la replicación de datos seleccione la carpeta que quiere replicar (véase la Figura 7.14), pulse el botón derecho, seleccione la opción *Replicar carpeta...* y aparecerá el asistente que se muestra en la Figura 7.15 donde tendrá que realizar los siguientes pasos:

1. Escriba el nombre del grupo de replicación y el nombre de la carpeta replicada.

Figura 7.15. *Crear grupo de replicación de datos*

2. El asistente muestra automáticamente la idoneidad del sistema para la replicación. Pulse *Siguiente.*
3. Indique el miembro principal donde se almacenan los datos y pulse *Siguiente.*
4. Seleccione la topología de replicación dependiendo de sus necesidades.
5. Indique cuándo se va realizar la replicación (siempre o en unos días determinados) y el ancho de banda máximo que se puede consumir.
6. Finalmente pulse *Crear*.

Para no saturar la red es recomendable programar la replicación de datos fuera del horario laboral. Si necesita realizar siempre la replicación entonces es recomendable indicar el ancho de banda máximo que puede utilizar la replicación de datos.

ACTIVIDADES 7.4

- Para realizar las siguientes actividades tienes que ver el Capítulo 8. *Directorio Activo.*
- Prepare dos equipos con Windows 2008 R. El primer equipo es un controlador de dominio y el segundo equipo es un servidor autónomo.
- Configure el servidor autónomo para que actúe como controlador de dominio secundario.
- Crea un espacio de nombres y configura los servidores para que compartan una misma carpeta dentro del espacio de nombres.
- Active la replicación de datos en el espacio de nombres.

7.2 SERVIDORES DE IMPRESIÓN

Los servicios de impresión permiten compartir impresoras en una red y centralizar las tareas administrativas que se realizan en los servidores de impresión.

Existen dos formas que permiten compartir una impresora para que puedan utilizarla en red:

- **Compartir una impresora**. Es la forma más fácil y para ello hay que hacer uso del servicio *Compartir archivos e impresoras*.
- **Servidor de impresión**. Permite supervisar las colas de impresión y recibir notificaciones cuando las colas de impresión dejan de procesar trabajos de impresión. Además, permiten migrar servidores de impresión e implementar conexiones de impresora mediante la directiva de grupo.

7.2.1 COMPARTIR IMPRESORA

La forma más sencilla es *Compartir* la impresora y para ello tan solo tiene que acceder a la sección *Dispositivos e impresoras* del *Panel de control* y, en la pantalla que aparece en la Figura 7.16, seleccione la impresora, pulse el botón derecho y seleccione *Propiedades de la impresora.*

Figura 7.16. *Panel de control - Impresoras*

Tal y como puede ver en la Figura 7.17, active la opción *Compartir Impresora,* introduzca el nombre del recurso compartido y pulse *Aceptar*. Además, puede pulsar el botón *Controladores adicionales* para indicar los controladores que pueden descargarse los equipos clientes para instalar la impresora.

Figura 7.17. *Compartir impresora*

Si quiere establecer los permisos de acceso sobre la impresora acceda a la pestaña *Seguridad* y, en la ventana que aparece en la Figura 7.18 puede establecer los permisos de los diferentes usuarios y grupos que tienen acceso a la impresora.

Figura 7.18. *Permisos de acceso a la impresora*

Para administrar los trabajos puede acceder a la impresora (véase la Figura 7.19) y ver todos los trabajos que tiene pendientes así como sus características. Además, para cada trabajo puede *Pausarlo*, *Cancelarlo* o *Reiniciarlo*.

Figura 7.19. *Trabajos de la impresora*

ACTIVIDADES 7.5

- Instale y configure una impresora en el servidor.
- Comparte la impresora para que la pueda utilizar cualquier usuario del sistema.
- Instale la impresora en un equipo cliente e imprime un documento.

7.2.2 SERVIDOR DE IMPRESIÓN Y DOCUMENTOS

Para instalar el servidor de impresión, ejecute el *Administrador del servidor*, pulse en *Agregar roles* y en el asistente que aparece seleccione *Servicios de impresión y documentos*. Las funciones que se pueden instalar son:

- **Servidor de impresión**. Incluye la herramienta administrativa *Administración de impresión*.
- **Servicio LPD**. Permite a los equipos GNU/Linux acceder a la impresora compartida.
- **Impresión en Internet**. Crea un sitio web para que los usuarios puedan administrar los trabajos de impresión en el servidor.
- **Servidor de digitalización distribuida**. Recibe documentos de escáneres de red y los envía a destinos correctos.

Figura 7.20. *Agregar servicio de impresión*

Una vez completada la instalación ya dispone de la herramienta administrativa *Administración de impresión*. El *Administrador de impresión* (véase la Figura 7.21) permite administrar las impresoras del servidor así como todos sus trabajos.

Figura 7.21. *Administración de impresión*

Para activar las notificaciones e indicar la dirección donde se van a recibir, seleccione el servidor, pulse el botón derecho y seleccione la opción *Notificaciones.* Tal y como muestra la ventana de la Figura 7.22 puede activar las notificaciones por correo electrónico o hacer que el sistema ejecute automáticamente un *script* cada vez que se produzca una incidencia.

Figura 7.22. *Establecer notificaciones*

Además de realizar la administración de la impresora a través de la herramienta administrativa *Administración de impresión* también puede hacerlo a través de una página web. Para ello tiene que instalar el complemento *Impresión en Internet* y acceder a la web del servidor (p.e. *http://10.0.0.01/printers*).

Figura 7.23. *Administración Web de impresión*

7.2.3 CLIENTE

Para utilizar una impresora compartida en un equipo cliente primero hay acceder al servidor que tiene la impresora e instalarla en nuestro equipo. Para instalar la impresora, en el equipo cliente, hay que acceder al servidor escribiendo su dirección (p.e. *\\10.0.0.1*) y al introducir los datos de usuario puede ver los recursos que comparte el servidor. Por ejemplo, en la Figura 7.24 puede ver que el servidor 10.0.0.1 comparte la impresora *Hp laserJet 1320 PCL5*.

Figura 7.24. *Acceder a una impresora compartida*

Para poder utilizar la impresora pulse el botón derecho, seleccione la opción *Conectar* y automáticamente se instalan los controladores de la impresora el en el equipo. Por ejemplo, si quiere acceder a la impresora puede ir a *Impresoras y faxes* que se encuentra dentro del *Panel de Control* (véase la Figura 7.25)

Figura 7.25. *Impresora instalada*

RESUMEN DEL CAPÍTULO

En este capítulo ha aprendido a instalar y configurar los servidores de impresión y de archivos.

Ha aprendido a compartir carpetas estableciendo los permisos de acceso.

Además, ha aprendido a utilizar las instantáneas y a utilizar los sistemas de ficheros distribuidos para permitir una mayor seguridad y rendimiento en los recursos compartidos.

Por último, ha aprendido a compartir una impresora y a utilizar un servidor de impresión.

EJERCICIOS PROPUESTOS

- **1.** Realiza un breve resumen de los diferentes los roles que has visto en el capítulo.
- **2.** Indique los puertos de comunicaciones utiliza el servicio *Compartir archivos e impresoras.*
- **3.** ¿Es posible compartir un recurso de dos formas diferentes?
- **4.** Explique brevemente lo que es una instantánea.

TEST DE CONOCIMIENTOS

1 Indique la afirmación incorrecta sobre el servicio *Compartir Archivos e impresoras*:

a) Si desea acceder al servidor 10.0.0.1 hay que escribir en el navegador \\10.0.0.1.
b) Es posible montar automáticamente un recurso compartido en una unidad de red.
c) Permite compartir recursos con sistemas GNU/Linux.
d) Por razones de seguridad, el administrador no puede acceder a los recursos compartidos.

2 Un recurso compartido cuyo nombre termina en el símbolo $ es:

a) Una carpeta oculta desde el entorno de red.
b) Una carpeta visible para todos los usuarios.
c) Una carpeta donde se guardan los archivos de configuración.
d) Un disco duro compartido.

3 Indique la afirmación incorrecta:

a) Una instantánea permite acceder a un sistema de ficheros distribuidos.
b) Una instantánea permite ver el contenido de las carpetas compartidas en momentos anteriores.
c) Una instantánea permite ver el estado del equipo en un momento determinado.
d) Una instantánea permite ver el registro de accesos a una carpeta compartida.

4 Indique la afirmación incorrecta:

a) La información de un DFS se puede distribuir en uno o más controladores de dominio.
b) Un espacio de nombres es una carpeta compartida dentro del DFS.
c) Un DFS está compuesto por espacios de nombres y cada espacio de nombres está compuesto por recursos compartidos.
d) Una vez creado un espacio de nombres es posible añadir más servidores que permitan replicar su contenido.

8 Directorio activo

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer los elementos de un directorio activo.
- ✓ Saber utilizar un directorio activo.
- ✓ Planificar la puesta en marcha de un directorio activo.
- ✓ Administrar los elementos de un directivo activo.
- ✓ Saber integrar el directorio activo con otros equipos.
- ✓ Planificar la utilización de directivas de grupo.

8.1 INTRODUCCIÓN

En un entorno de red normal, un usuario puede iniciar sesión en la red con un nombre de usuario y una contraseña (p.e. *mperez*). Asumiendo que tiene los permisos necesarios, *mperez* puede conectarse a un equipo y acceder a sus ficheros o los servicios que proporciona.

Cuando hay un único servidor y pocos usuarios este modelo resulta útil. Pero en el caso de tener muchos usuarios o equipos este modelo es inviable ya que resulta muy difícil administrar el sistema. Por ejemplo, para cambiar la contraseña de un usuario hay que hacerlo en todos los equipos.

Si el sistema informático cuenta con unos cientos e incluso miles de usuarios, no cuesta ver lo difícil de resolver que pueden resultar los errores que pueden presentarse. A medida que el número de usuarios y equipos en una red crece los servicios de Directorio Activo (o dominio) se vuelven esenciales.

Un dominio consiste en una agrupación de máquinas y usuarios. Cuando un usuario se conecta a la red, debe seleccionar el dominio al que quiere entrar e introducir sus datos de usuario. Al ser autenticado en un dominio, el usuario tiene disponibles todos los recursos dados de alta en dicho dominio, sin tener que autenticarse en cada uno de los servidores que formen parte de dicho dominio. La gestión de un dominio se realiza de forma centralizada, ya que toda la información se encuentra en una base de datos almacenada en el Controlador de Dominio (DC).

Figura 8.1. *Visión general del Directorio Activo*

Los servicios de Dominio (o Directorio Activo) son la base para la infraestructura de una red. Mas concretamente proporciona los mecanismos para:

- ✓ Almacenar información acerca de usuarios, equipos y otros dispositivos y servicios de la red de la empresa de forma centralizada.
- ✓ Autenticar usuarios y equipos.
- ✓ Permitir o denegar el acceso de un usuario o equipo a un recurso de red.
- ✓ Facilitar a los usuarios la búsqueda de impresoras, recursos compartidos y otros usuarios.

En la Figura 8.1 se puede ver una visión general de la infraestructura de un Directorio Activo.

Para poder a administrar un Directorio Activo hay que tener claros los siguientes conceptos:

- **Base de datos del directorio activo**. Es donde se guarda toda la información de los objetos del dominio (usuarios, equipos, grupos, etc.).
- **Controladores de dominio o DC**. El controlador de dominio es un servidor que mantiene la base de datos de usuarios del dominio. A través de las herramientas de administración se pueden administrar los usuarios, grupos, equipos, permisos... del dominio.
- **Dominio**. Un dominio es una unidad administrativa con unas características determinadas:
  - Todos los DC replican entre sí la base de datos del directorio (datos sobre usuarios, equipos, grupos...), en consecuencia, un usuario puede autenticarse en cualquier controlador del dominio.
  - En el dominio se aplican las mismas políticas de seguridad como por ejemplo la longitud mínima de las contraseñas, número máximo de intentos antes de bloquear la cuenta, etc.
  - Los cambios de un objeto se pueden realizar en cualquier controlador de dominio y se replican en todo el dominio.
- **Bosque**. Un bosque es una colección de uno o más dominios. Al primer dominio del bosque se le llama dominio raíz. Un bosque es una instancia única del directorio. Ningún dato del directorio se replica fuera de los límites del bosque.
- **Árbol**. Los árboles son el resultado directo de los nombres DNS elegidos para los dominios del bosque. Si un dominio es subdominio de otro, ambos son considerados el mismo árbol. Por ejemplo, si *miempresa.com* tiene dos dominios, *miempresa.com* y *almeria.miempresa.com*, como ambos comparten un espacio de nombres contiguo, se consideran el mismo árbol. Si, por el contrario, los dos dominios se llaman *miempresa.com* y *miotraempresa.com*, al no tener un espacio de nombres contiguo, se tienen dos árboles diferentes.
- **Nivel funcional**. La funcionalidad de un domino o bosque depende de la mínima versión del sistema operativo que utilizan los controladores de dominio. Por ejemplo, si dispone de una red con un controlador de dominio con Windows 2003 y otro con Windows 2008, el nivel funcional es para servidores Windows 2003.
- **Relación de confianza**. Para explicar en qué consisten las relaciones de confianza se debe pensar en un dominio como un grupo de servidores que forman un único sistema junto con las posibles máquinas clientes. Todos los servidores del dominio comparten el mismo conjunto de cuentas de usuario, por lo que únicamente es necesario guardar la información de una cuenta para que tanto el controlador primario como los secundarios reconozcan dicha cuenta.

Las relaciones de confianza permiten la compartición de las bases de datos de usuarios entre varios dominios de la red, es decir, establecen un vínculo o relación por la que una cuenta de un dominio será reconocida por los servidores de los dominios que confíen en él. Mediante estos vínculos, un usuario tiene una única cuenta en un dominio, pero puede acceder a cualquier servidor de la red formado por los dominios que constituyen la relación. Gracias a las relaciones de confianza, al crear una cuenta de usuario en un dominio, ésta queda habilitada en todos los servidores de dominio de la red de confianza.

También es necesario aclarar que si un dominio confía en otro y éste último confía en un tercero, el primero no confía automáticamente en el tercero. Es decir, las relaciones se establecen entre parejas de dominios, o lo que es lo mismo, la confianza entre dominios no es una operación transitiva.

- **Equipo**. Es un equipo que se ha dado de alta en el directorio activo y por lo tanto su administración se realiza a través de las herramientas de administración del dominio.
- **Servidores autónomos**. Son servidores que no están conectados al dominio y por lo tanto su administración es totalmente independiente. Este modo de funcionamiento es especialmente útil cuando un servidor no necesita información de dominio como, por ejemplo, es el caso de un servidor web público.
- **Sitio**. Un sitio es un objeto que representa una parte de la red de la empresa en que la conectividad es buena, por ejemplo una LAN. El sitio será el objeto que imponga restricciones a la hora de efectuar la replicación de la base de datos del directorio. Dos controladores de dominio dentro de un mismo sitio se replicarán en cuestión de segundos. Por el contrario, la replicación entre sitios debe ser planificada teniendo en cuenta que las conexiones van a ser más lentas y menos fiables, en comparación con las comunicaciones dentro del sitio. Igualmente cuando un usuario inicia sesión en un dominio, el sistema intenta realizar la conexión al controlador de dominio más próximo.
- **Unidad organizativa (UO)**. El Directorio Activo es una base de datos de información que se puede organizar según una jerarquía. Los objetos de la base de datos se pueden agrupar en contenedores. Existen una serie de contenedores por defecto: Usuarios, Equipos, etc. Una UO es un tipo de contenedor que, además de agrupar objetos, actúa como límite administrativo. Esto es así porque a las unidades organizativas pueden enlazar unos objetos llamados objetos de Políticas de Grupo (GPO). Estos GPO contienen opciones de configuración que se aplicarán automáticamente a los usuarios y equipos de la UO a la que se encuentren vinculados.
- **Campos adicionales**. Además de los registros por defecto de los usuarios o equipos (p.e. nombre, organización) es posible guardar información adicional útil para el correcto funcionamiento del sistema o de las aplicaciones que se integran en el dominio.

8.2 INSTALACIÓN DEL CONTROLADOR DE DOMINIO

8.2.1 TAREAS PREVIAS

Antes de comenzar el proceso de promoción de un servidor a controlador de domino hay que dedicar un tiempo a planear la infraestructura de *Directorio Activo*. Concretamente hay que tener en cuenta los siguientes aspectos:

- El nombre del dominio y el nombre DNS. Igualmente el nombre netbios.
- El nivel funcional del dominio según la versión del sistema operativo de los servidores que forman el dominio.
- Los controladores de dominio requieren una IP y una máscara de subred fijas.
- El controlador de dominio debe tener un servidor DNS que realice la resolución de nombres. Si realiza la instalación de un nuevo bosque, el asistente instala automáticamente el rol de servidor DNS.
- El servidor que actúa de controlador de dominio debe tener una partición NTFS.

8.2.2 INSTALACIÓN

Parar realizar la instalación del Directorio Activo debe realizar los siguientes pasos:

1 Inicie la herramienta administrativa *Administrador del servidor*, pulse en la opción *Roles* y haga clic en *Agregar Roles*. El asistente muestra los servicios que tiene instalados en el sistema. Seleccione el servicio *Servicios de Dominio de Active Directory* y pulse *Siguiente*. Además de utilizar el asistente puede iniciar la instalación del Directorio Activo ejecutando el siguiente comando *dcpromo*.

2 El sistema muestra información acerca del servicio. Pulse *Siguiente* y confirme que desea realizar la instalar. A continuación se inicia el asistente de instalación de *Servicios de Dominio de Active Directory* para dar funcionalidad completa al servidor como controlador de dominio.

3 Tras una página de bienvenida el asistente pregunta la acción que desea realizar:

- **Crear el dominio en un bosque existente**. Dentro de esta opción hay otras dos, agregar el controlador de dominio a un dominio existente o bien crear un dominio nuevo. Con la primera opción se replicará la información del directorio del dominio existente y si seleccione la segunda opción, el controlador se convertirá en el primer controlador de dominio del nuevo dominio, y ofrece la posibilidad de crear una raíz de árbol de dominio nueva en lugar de un nuevo dominio secundario. Los dominios secundarios son interesantes por ejemplo para crear un nuevo dominio denominado *oficina.empresa.com* como un dominio secundario del dominio *empresa.com*. Si selecciona esta opción, el sistema le preguntará los datos de usuario del administrador del dominio principal.
- **Crear el dominio en un nuevo bosque**. Seleccione esta opción si éste es el dominio principal de su organización o si desea que el dominio nuevo sea completamente independiente del bosque actual.

Figura 8.2. *Elegir una configuración de implementación*

4 Para identificar el controlador de dominio en la red hay que especificar el nombre del dominio completo (FQDN). Este nombre no tiene por qué ser el mismo que el nombre de dominio que utiliza la organización para su presencia en Internet. Tampoco necesita estar registrado en Internet. No obstante, el empleo de un nombre de dominio registrado resulta conveniente si los usuarios de red van a tener acceso a los recursos de Internet simultáneamente con los recursos de la red local o si los usuarios externos a la organización van a tener acceso a los recursos de red local a través de Internet.

5 A continuación, el sistema solicita el nivel funcional del bosque dependiendo de la versión del sistema operativo que tengan los servidores miembros (Windows 2000, 2003, 2008 ó 2008 R2). Es importante seleccionar el nivel más alto posible ya que por ejemplo, si selecciona Windows Server 2003 algunas características avanzadas en controladores de dominios que utiliza Windows Server 2008 no estarán disponibles.

6 Una vez introducido el nombre de dominio y seleccionado su nivel funcional puede seleccionar opciones adicionales como servidor DNS, catálogo global o controlador de dominio de solo lectura (RODC). El primer controlador de dominio de un bosque debe ser un servidor de catálogo global y no un puede ser un RODC. Además, se recomienda la instalación del servidor DNS en el primer controlador de dominio.

Figura 8.3. *Opciones adicionales del controlador de dominio*

7 Establezca las carpetas donde se va a guardar la base de datos, el registro de Active Directory y la ubicación del *Volumen del Sistema Compartido* (SYSVOL). La carpeta SYSVOL almacena la copia del servidor de archivos públicos del dominio. El contenido de esta carpeta se replica en todos los controladores de dominio en el dominio. Pulse *Siguiente* para continuar.

8 Especifique la contraseña de *administración de modo de restauración de servicio de directorio* y pulse *Siguiente*.

9 En la Figura 8.4, puede ver como el asistente muestra un resumen de todas las opciones seleccionadas. Revise y confirme las opciones y pulse *Siguiente*.

Figura 8.4. Resumen de la instalación de Active Directory

Una vez puesto en marcha el Directorio Activo si quiere darle una mayor redundancia al sistema puede añadir controladores de dominio adicionales.

Si desea degradar un controlador de dominio a servidor miembro ejecute el comando dcpromo y realice los pasos que le indica el asistente.

Como el Directorio Activo necesita utilizar un servidor de nombres es recomendable que en el servidor de nombres active los reenviadores para que los clientes puedan resolver cualquier dominio. Para activar los reenviadores, en la herramienta administrativa *Servidor DNS,* seleccione el servidor, pulse el botón derecho, seleccione *Propiedades* y en la pestaña *Reenviadores* (véase la Figura 8.5) especifique varios servidores DNS públicos de confianza.

Figura 8.5. Reenviadotes del servidor DNS

ACTIVIDADES 8.1

- Examine los requisitos que tiene que tener un equipo para ser controlador de dominio.
- Ejecute en el servidor el comando *dcpromo* para crear el directorio activo *miempresa.com*.
- Configure el servidor de nombres para que utilice como reenviadores los servidores: 8.8.8.8 y 194.224.52.36.
- Compruebe desde el equipo cliente que la red interna tiene conexión a Internet.

8.3 ADMINISTRACIÓN DEL DIRECTORIO ACTIVO

8.3.1 HERRAMIENTAS ADMINISTRATIVAS

La mayor parte de las tareas administrativas en el Directorio Activo se realiza con alguna de estas herramientas:

- **Usuarios y Equipos de Active Directory**. Permite realizar las tareas diarias con usuarios, grupos, equipos, impresoras, carpetas compartidas, etc.
- **Sitios y Servicios de Active Directory**. Permite administrar la replicación y temas relacionados con la topología de la red.
- **Dominios y Confianzas**. Permite realizar las relaciones de confianza y los niveles funcionales del dominio y del bosque.

Para administrar el Directorio Activo desde un equipo que no sea controlador de dominio puede instalar Microsoft Remote Server Administration Tools (RSAT).

8.3.2 ADMINISTRACIÓN BÁSICA DE OBJETOS

La administración de los diferentes objetos del dominio (usuarios, grupos, UO, etc.) se realiza a través de la herramienta *Usuarios y equipos de Active Directory* (Figura 8.6) que se encuentra dentro de las *Herramientas administrativas*.

Figura 8.6. *Administración de usuarios y equipos del directorio activo*

A continuación se va a ver cómo se realiza la administración de los diferentes objetos del Directorio Activo:

8.3.2.1 Unidades organizativas

Son contenedores de otros objetos del Directorio Activo, que comparten unos mismos requerimientos de administración. En una unidad organizativa (UO) encontraremos usuarios, equipos, grupos y otras UO. Con ellas se puede crear contenedores en el dominio para representar las estructuras jerárquica y lógica de la empresa. Para crear una UO tan solo tiene que seleccionar el dominio u otra unidad organizativa, pulsar el botón derecho del ratón y seleccionar *Nuevo / Unidad organizativa*.

8.3.2.2 Usuarios

Las cuentas de usuario de *Active Directory* representan entidades físicas, como personas. Al crearlas se les asignan automáticamente identificadores de seguridad (SID), que se pueden usar para obtener acceso a recursos del dominio. Una cuenta de usuario:

- **Autentica la identidad de un usuario**. Permite que un usuario inicie sesión en equipos y dominios con una identidad que el dominio pueda autenticar.
- **Autoriza o deniega el acceso a los recursos del dominio**. Después de autenticar un usuario, es posible concederle o denegarle el acceso a los recursos del dominio en función de los permisos asignados en el recurso.

Para administrar los usuarios y grupos de usuarios en un controlador de dominio tiene que utilizar la herramienta administrativa *Usuarios y equipos de Active Directory* (véase la Figura 8.6).

Una de las ventajas de utilizar el Directorio Activo es que se puede centralizar toda la información de los usuarios de la empresa, de forma que cualquier usuario puede acceder a su cuenta y a sus datos desde cualquier equipo.

ACTIVIDADES 8.2

- Ejecute la herramienta administrativa *Usuarios y equipos del directorio activo* para ver los usuarios y grupos que tiene el sistema por defecto.
- Crea las unidades organizativas *Almería* y *Madrid*. Dentro de *Madrid* crea las unidades organizativas *Sucursal1* y *Sucursal2*.
- Crea en las diferentes unidades organizativas varios usuarios.

8.3.2.3 Equipos

Las cuentas de equipos de un dominio del Directorio Activo, al igual que los usuarios, son entidades de seguridad que representan a los equipos físicos.

Para dar de alta un equipo en el dominio vaya al equipo, pulse *Mi PC*, *Propiedades* y en la pestaña *Nombre de Equipo* pulse en *Cambiar* y escriba el nombre del dominio al que desea conectarse (véase la Figura 8.7). Pulse *Siguiente* y a continuación el sistema le solicita un nombre de usuario y contraseña con suficientes permisos para dar de alta un equipo en el dominio.

Figura 8.7. *Unión a un dominio*

El equipo cliente en la configuración TCP/IP debe tener como servidor DNS la dirección IP del directorio activo.

Una vez que un equipo se encuentra dentro del dominio, puede iniciar sesión en el sistema con un usuario local o del dominio.

Una vez dado el equipo de alta en el dominio, éste aparece en la sección *Computers*. Si selecciona el equipo puede realizar las acciones más impartes como ver sus propiedades o administrarlo de forma remota (véase la Figura 8.8).

Figura 8.8. *Administración remota del equipo*

Para minimizar el trabajo de administración de la red, los equipos clientes tan solo tienen la cuenta del "Administrador" para obligar a los usuarios a utilizar las cuentas del Directorio Activo.

ACTIVIDADES 8.3

- Asegúrate de que el equipo cliente tiene el nombre *Oficina1*.
- Da de alta el equipo cliente en el directorio activo.
- Inicie sesión en el equipo cliente con un usuario del dominio.
- Accede a la herramienta administrativa *Usuarios y equipos del directorio activo*, busca el equipo *Oficina1* y muévelo a la unidad organizativa *Madrid*.

8.4 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO

En cualquier sistema Windows, forme parte de un dominio o no, existen unas directivas de grupo que el administrador puede editar según su criterio para personalizar el comportamiento del equipo. Por ejemplo es posible configurar la seguridad del sistema, las impresoras, instalar y configurar el software del equipo, etc.

Cuando un administrador debe configurar las directivas de grupo de muchos equipos, resulta incómodo tener que establecer sus configuraciones y comportamientos uno por uno, especialmente si se da el caso que varios de ellos deben compartir parte o toda la configuración. Para facilitar la administración del sistema, las políticas de grupo se han integrado dentro de la administración del Directorio Activo como una utilidad de configuración centralizada en dominios Windows Server.

A continuación primero se van a ver las características más importantes de las directivas de seguridad y posteriormente aprenderá a administrar las directivas locales del sistema y las directivas de grupo del directorio activo.

8.4.1 DIRECTIVAS DE SEGURIDAD

Las directivas de grupo se definen mediante objetos del Directorio Activo denominados *Objetos de Directiva de Grupo* (*Group Policy Objects – GPO*). Un GPO es un objeto que contiene una o varias directivas de grupo que se aplican a la configuración de uno o más usuarios o equipos. Por ejemplo, puede crear un GPO que configure el fondo de escritorio y conecte una unidad de red a un recurso compartido.

Un GPO es un objeto que puede aplicarse tanto a usuarios y equipos Windows (desde Windows XP a Windows 2008 R2).

8.4.1.1 Tipos

Para crear una configuración específica para un grupo de usuarios o equipos es necesario configurar una GPO. Existen dos tipos de GPO dependiendo de su ámbito:

- **GPO locales**. Se utilizan principalmente para los equipos que no forman parte de un directorio activo y como su nombre indica, la GPO se aplica únicamente al equipo local.
- **GPO no locales**. Las GPO no locales se crean en el Directorio Activo y se vinculan a un sitio, dominio, unidad organizativa (UO), usuarios o equipos. De esta forma es posible establecer directivas que afecten a toda la empresa, a un departamento, grupo de usuarios, etc.

  De forma predeterminada, al configurar el servicio de Directorio activo crean dos GPO no locales:

  - **Directiva predeterminada de dominio**. Se vincula al dominio y afecta a todos los usuarios y equipos del dominio.
  - **Directiva predeterminada de controladores de dominio**. Esta directiva se vincula únicamente a los controladores del dominio.

Puesto que es posible que se produzcan conflictos en una misma política que se encuentra definida en distintos GPO, es necesario que exista un orden de aplicación concreto y conocido de forma que conozca qué política afecta a cada usuario o equipo sin ambigüedades. El orden de aplicación de las GPO es el siguiente:

- Se aplica la GPO local del equipo.
- Se aplican las GPO vinculadas al sitio.
- Se aplican las GPOS vinculadas al dominio.
- Se aplican las GPO vinculadas a unidades organizativas de primer nivel, posteriormente se aplican las de segundo nivel, etc.

8.4.1.2 Configuración

Las directivas de seguridad se clasifican en dos grandes grupos:

- La configuración del equipo agrupa todas las políticas o parámetros de configuración que pueden establecerse a nivel de equipo. Las GPO que afectan a un equipo se aplican cada vez que se reinicia el equipo.
- **La configuración de usuario** agrupa todas las políticas o parámetros de configuración que pueden establecerse a nivel de usuario. Las GPO que afectan a un usuario se aplican cada vez que el usuario inicia sesión en cualquier equipo del dominio.

  Internamente, cada subcategoría se divide en:

- **Directivas**:
  - **Configuración de software**. Permite la instalación automática de software.
  - **Configuraciones de Windows**. Que incluyen, entre otros aspectos, configuración de seguridad y ejecución de *scripts*.
  - **Plantillas administrativas**. Que incluyen aquellas políticas basadas en la configuración de los elementos más importantes del equipo (Componentes de Windows, Impresoras, Panel de Control, Red y Sistema).
- **Preferencias**:
  - **Configuración de Windows**. Incluye opciones de configuración como la creación de variables de entorno, creación de accesos directos, unidades de red, etc.
  - **Configuración del Panel de Control**. Incluye opciones de configuración como por ejemplo la instalación de dispositivos e impresoras, usuarios y grupos locales, opciones de energía, tareas programadas, servicios, etc.

Con la directiva "Configuración del software" puede establecer que se instale automáticamente un determinado programa en un grupo o en todos los equipos del Directorio Activo.

8.4.1.3 Aplicación

Como se ha visto, la configuración de las directivas de seguridad se aplican de dos formas diferentes:

- Para la configuración de equipo se aplica al arrancarlo y posteriormente cada 90 a 120 minutos.
- Para la configuración de usuario se aplica al iniciar sesión el usuario y cada 90-120 minutos.

Puede forzar la aplicación o refresco de las directivas de grupo utilizando el comando *gpupdate*.

8.4.2 DIRECTIVAS DE GRUPO LOCAL

Las directivas de grupo son conjuntos de opciones de configuración de usuario y equipo que especifican cómo funcionan los programas, los recursos de red, sistema operativo, etc.

Las directivas de grupos se pueden configurar para equipos, sitios, dominios o unidades organizativas. Por ejemplo, mediante las directivas de grupo, puede determinar los programas que se encuentran disponibles para los usuarios, los programas que aparecen en el escritorio, opciones de menú de inicio, configuración del sistema, etc.

Para configurar las directivas de grupo locales hay que ejecutar el comando:

```
gpedit.msc
```

y tal y como muestra la Figura 8.9, a través del *Editor de directivas de grupo local* puede configurar las directivas del sistema.

Figura 8.9. *Editor de directivas de grupo local*

ACTIVIDADES 8.4

- Ejecute la herramienta *gpedit.msc* y examina las diferentes directivas de grupo del sistema.
- Configure las directivas de grupo local para ocultar la papelera del sistema.

8.4.3 ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO

Para administrar las directivas de grupo de los equipos o usuarios del Directorio Activo, ejecute la herramienta administrativa *Administración de directivas de grupo.*

Al ejecutar la herramienta en el menú de la izquierda (véase la Figura 8.10) puede ver que en el dominio tiene la directiva general del dominio (*Default Domain Policy*), la directiva específica para los controladores del dominio (*Default Domain Controllers Policy* que se encuentra dentro de la carpeta *Domain Controllers*), y las carpetas *Clientes* y *GPO de inicio.* Además, en la estructura del dominio puede encontrar o crear las diferentes unidades organizativas que le permiten definir la estructura de la empresa.

Por ejemplo, en la Figura 8.10, se encuentra la unidad organizativa *Oficina* que contiene todos los equipos de la oficina para que tengan una misma configuración.

Figura 8.10. *Administrador de directivas de grupo*

Para crear y personalizar la GPO asociada a una unidad organizativa (p.e. para aplicarla a un grupo de equipos o clientes) debe realizar los siguientes pasos:

1. Seleccione la unidad organizativa.

2. Pulse el botón derecho y seleccione una de las siguientes opciones:
   - Crear un GPO en este dominio y vincularlo aquí.
   - Vincular un GPO existente.

3. Dependiendo de la opción seleccionada indique el nombre de la nueva directiva o seleccione la directiva que desea vincular.

4. Automáticamente aparece la GPO creada. Por ejemplo, en la Figura 8.11 se muestra la *GPO equipos oficina* dentro de la unidad organizativa *Oficina.*

Figura 8.11. GPO equipos oficina

5 Una vez que se ha creado o vinculado la directiva de grupo, seleccione la directiva y pulse *Editar* para personalizar la GPO.

6 Ya se ha creado la nueva directiva de grupo. Seleccione la nueva directiva, pulse el botón derecho y seleccione *Editar* para poder personalizar la GPO (véase la Figura 8.12).

Figura 8.12. Editor de administración de directivas de grupo

Recuerde que se aplican las directivas de grupo al reiniciar el equipo (si es configuración de equipo), al iniciar sesión un determinado usuario (si es configuración de usuario), de forma automática cada 90 minutos o al ejecutar el comando *gpupdate*.

ACTIVIDADES 8.5

- Crea y personaliza las directivas de grupo asociadas a la unidad organizativa *Madrid* y *Almería*, creadas en las anteriores actividades.

RESUMEN DEL CAPÍTULO

En este capítulo ha aprendido a utilizar un directorio activo. Para ello, primero se han descrito los diferentes elementos de un directorio activo.

También ha aprendido a realizar la puesta en marcha de un directorio activo.

Ha aprendido a administrar los diferentes elementos del directorio activo así como la integración con otros equipos.

Por último, ha aprendido a administrar las políticas de grupo del equipo local y del dominio.

EJERCICIOS PROPUESTOS

- **1.** Explique lo que es un dominio y un controlador de dominio.
- **2.** Enumere y explica brevemente los diferentes elementos que tiene un dominio.
- **3.** ¿Qué es y para qué se utiliza una unidad organizativa?
- **4.** ¿Qué es y para qué se utilizan los Objetos de Políticas de Grupo?
- **5.** Indica los tipos de políticas de grupo. ¿Cómo se configuran?
- **6.** Indica al menos 5 objetos de políticas de grupo que permitan personalizar el escritorio a los usuarios del sistema.

TEST DE CONOCIMIENTOS

1 Indique la afirmación incorrecta:

a) Un bosque es un conjunto de dominios.
b) Un controlador de dominio es el servidor donde se instala el Directorio Activo.
c) Una unidad organizativa es una agrupación de usuarios
d) Es posible iniciar sesión en un servidor autónomo con una cuenta del dominio.

2 Indique la afirmación incorrecta:

a) Es posible crear un dominio a través de la herramienta administrativa Administre su servidor.
b) Es posible crear un dominio ejecutando el comando *dcpromo*.
c) Es posible tener un controlador de dominio con todas sus unidades de disco en NFTS.
d) Al crear el dominio se instalada automáticamente el servidor de nombres.

3 Indique el tipo de directiva de seguridad que no existe:

a) Configuración de software.
b) Configuración de Windows.
c) Plantillas administrativas.
d) Aplicaciones.

4 Indique la afirmación incorrecta:

a) Las directivas de grupo se definen mediante objetos del Directorio Activo denominados *Objetos de Directiva de Grupo*.
b) Existen dos tipos de GPO: las locales y las no locales.
c) Las primeras GPO que se aplican son las GPO vinculadas al dominio
d) Es posible configurar una GPO para un determinado equipo o para un determinado usuario.