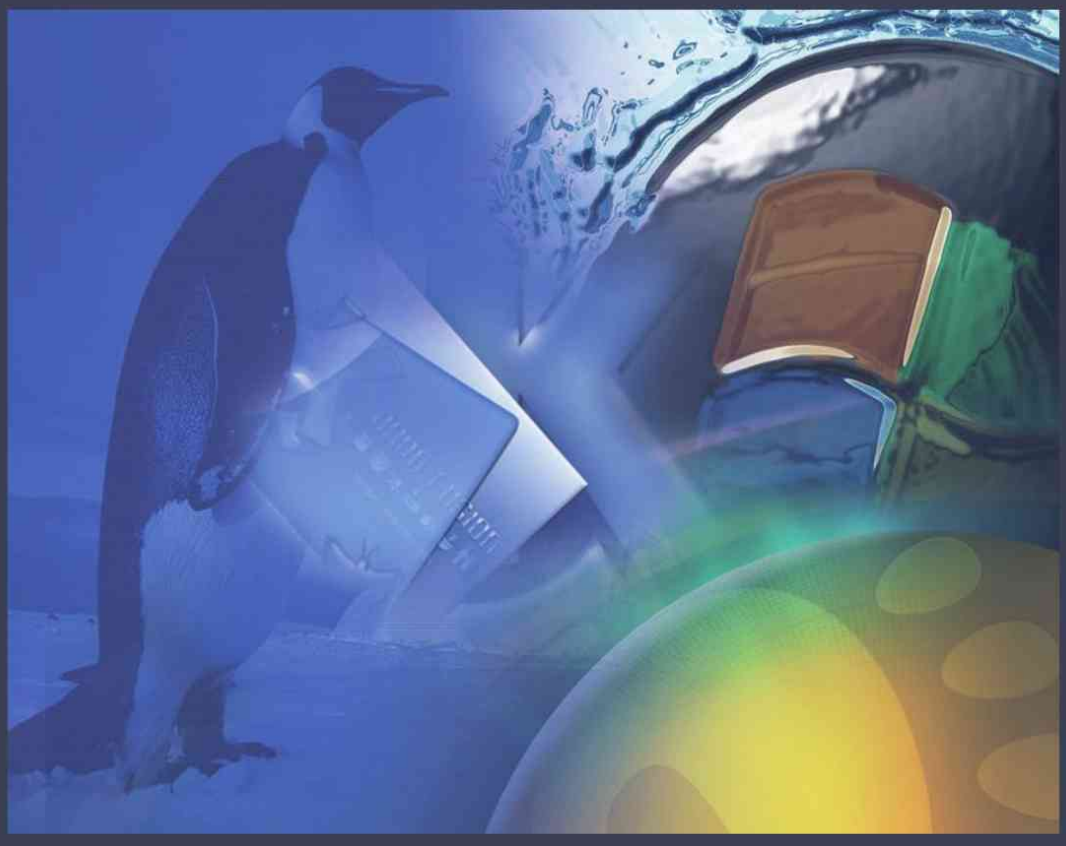
Administración de Sistemas Operativos

Un enfoque práctico

2ª EDICIÓN ACTUALIZADA



Julio Gómez López

El libro contiene material adicional.

Ra-Ma®

Administración de Sistemas Operativos

Un enfoque práctico

2.ª edición

Administración de Sistemas Operativos

Un enfoque práctico

2.ª edición

Julio Gómez López

- Profesor de la Universidad de Almería -

Ra-Ma®

La ley prohíbe
Copiar o Imprimir este libro

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS. UN ENFOQUE PRÁCTICO. 2ª EDICIÓN
© Julio Gómez López

© De la Edición Original en papel publicada por Editorial RA-MA
ISBN de Edición en Papel: 978-84-9964-082-2

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, 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

Maquetación: Gustavo San Román Borrueco
Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-410-3

E-Book desarrollado en España en septiembre de 2014.

A mi abuelo Eutimio.

ÍNDICE

INTRODUCCIÓN

Este libro estudia los aspectos fundamentales relacionados con la Administración de los Sistemas Operativos más utilizados en pequeñas y medianas empresas: Windows 2008 R2 y GNU/Linux. Los contenidos del libro se han dividido en tres bloques. En el primer bloque se estudian los aspectos generales de la administración en que destaca el estudio del hardware y software de un servidor, las redes de ordenadores y la seguridad en los sistemas informáticos. 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 las distribuciones GNU/Linux más utilizadas: Ubuntu y Fedora. Aprenderá, entre otros aspectos, a instalar y configurar el sistema operativo, gestionar las cuentas de los usuarios, administrar la red, administrar servidores, etc. Para reforzar los contenidos teóricos del curso, se han elaborado supuestos prácticos, donde el lector tendrá que realizar diversas actividades propias de la administración de sistemas.

El libro está dirigido tanto a un público académico como profesional. Como libro de texto, está pensado para el desarrollo de una asignatura relacionada con la administración de sistemas operativos. Este tipo de asignaturas pueden encontrarse en los estudios de Ingeniería Técnica de Informática de Sistemas y Gestión, así como en los estudios de Ingeniería en Informática. También puede ser utilizado en los estudios de Ciclo Formativo de Grado Superior de Informática.

Por otro lado, el libro puede ser utilizado por el profesional que se dedica a estos aspectos de la informática. Para este público, se puede utilizar como manual de referencia y/o autoestudio.

Para un mejor seguimiento en el proceso de lectura, la obra se complementa con diversas notas o consejos que debe tener en cuenta a la hora de administrar el sistema.

Nota

Las notas suelen completar la información del libro facilitando consejos, advertencias, más información, etc.

Como se ha comentado antes, el tercer bloque está orientado a los sistemas GNU/Linux Ubuntu y Fedora. La instalación y administración de ambos sistemas es muy parecida pero siempre hay pequeñas diferencias que hay que tener en cuenta. A lo largo del texto encontrará anotaciones para aprender a configurar ambos sistemas y obtener el máximo rendimiento de cada distribución.

UBUNTU

Consejo o comentario para realizar una determinada tarea en Ubuntu.

FEDORA

Consejo o comentario para realizar una determinada tarea en Fedora.

Además se pone a disposición del lector el uso de la Web *http://www.adminso.es* para completar información relacionada con la obra. Tras un proceso de registro, se tendrá acceso a diferente material electrónico como, por ejemplo, presentaciones, ficheros de configuración, etc.

TEORÍA

Capítulo 1

ASPECTOS BÁSICOS

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 este capítulo 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 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.

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.

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, sistemas RAID, routers, 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 a 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 el 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.

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.

Es muy importante conocer los componentes hardware del sistema para poder configurar y dimensionar el servidor de acuerdo a sus necesidades. 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

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 es de 19" de ancho, mientras que la gran mayoría de racks disponen de una altura de 42 U (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 o 2 U en un rack, o tal vez "4 U half" rack.

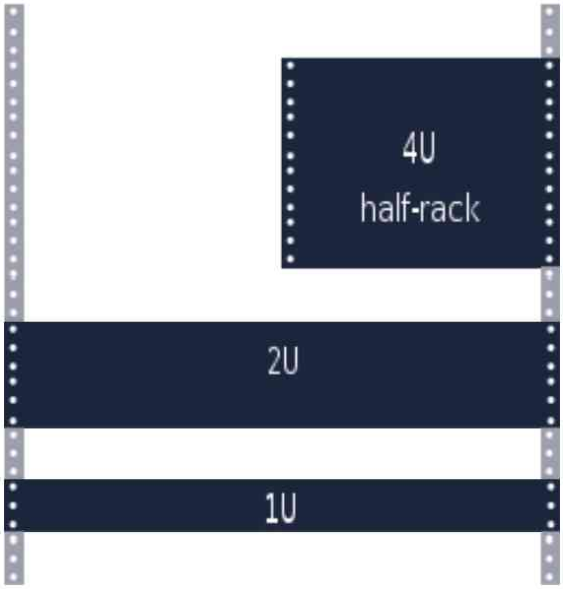


Figura 1-3. Rack

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: a) Torre; b) Blade; c) 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.

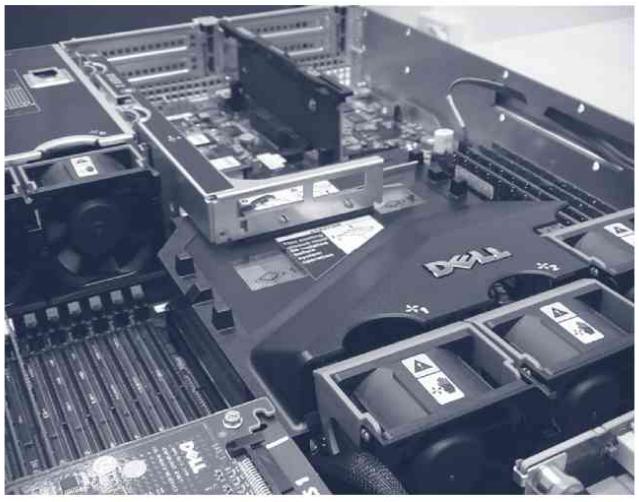


Figura 1-7. Interior de un servidor Dell R805

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.

1.2.4 Sistemas RAID

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.

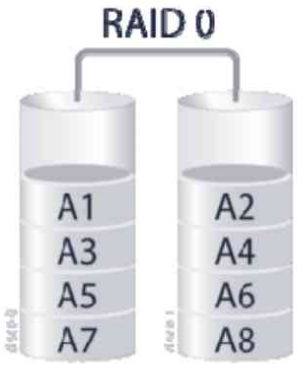


Figura 1-8. RAID 0

- **JBOB (*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 sistema RAID 1 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 pierden 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.

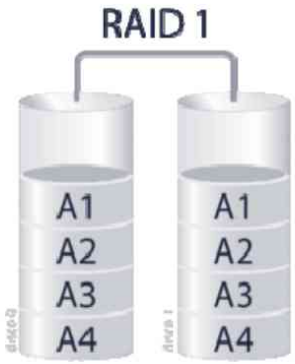


Figura 1-9. RAID 1

- **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.

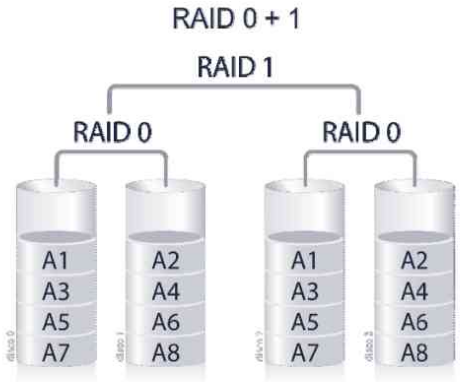


Figura 1-10. RAID 0+1

- **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 un disco duro del volumen. De esta forma si dispone de RAID nivel 5 con seis 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.

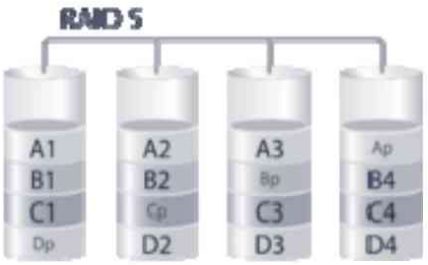


Figura 1-11 RAID 5

De esta forma, si utiliza un sistema RAID 1, 0+1 o 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

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

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. ej. Windows 7 se utiliza como cliente, Windows Server 2008 como servidor) los sistemas GNU/Linux pueden actuar como cliente o servidor.

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.

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 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 vamos a ver las características más importantes de los sistemas Windows 2008 R2 Server y GNU/Linux, así como su instalación, configuración y administración.

Capítulo 2

REDES DE ORDENADORES

Podría decirse que Internet se ha convertido en la entidad virtual más variada que ha desarrollado el hombre. El número de usuarios crece periódicamente en cientos de miles por todo el mundo, sin que parezca que vaya a dejar de aumentar. Internet es un lugar virtual donde todo el mundo es bienvenido para hacer negocios, comunicarse, buscar información o, simplemente, divertirse navegando por la red. La inmensidad de Internet, junto con las diferencias entre sus visitantes, crea una mezcla única. Sin embargo, también contiene un gran potencial para el uso indebido, el abuso y la actividad criminal. Esta capacidad para causar daños ha creado la necesidad de que existan prácticas de seguridad y dispositivos para proteger los recursos de Internet.

En este capítulo vamos a ver todos los pasos que son necesarios para la puesta en marcha de una red:

- **Creación de la red a nivel físico.** Se crea la infraestructura necesaria para poner la red en funcionamiento. Para ello se instala el cableado de la red y luego se ponen en marcha los dispositivos de interconexión (hub, switch, routers…).

- **Creación de la red a nivel lógico.** Se crean las diferentes redes lógicas y se asignan las direcciones IP a los diferentes equipos de la red.

- **Configuración de los routers.** Se configuran los routers para permitir aceptar o denegar las comunicaciones que se realizan a través de él.

2.1 CABLEADO

Los diferentes tipos de cables ofrecen distintas características de funcionamiento. La variedad de velocidad de transmisión que un sistema de cableado puede soportar se conoce como el ancho de banda. La capacidad del ancho de banda está condicionada por las características físicas que tienen los componentes del sistema de cableado.

El funcionamiento del sistema de cableado debe ser considerado no solo cuando se está cubriendo las necesidades actuales sino también con las necesidades del mañana. Conseguir esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

A continuación se describen brevemente los medios de comunicación más utilizados en la actualidad.

- **Par trenzado.** Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado.

  Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la interferencia entre pares adyacentes. Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto.

  Este cable es el más utilizado en la actualidad y permite velocidades de hasta 1 Gb/s. En la tabla 2-1 puede ver la estructura del cable, conectores, así como sus características físicas.

- **Fibra óptica.** Este cable está constituido por uno o más hilos de fibra de vidrio. Tal y como muestra la tabla 2-1, cada fibra de vidrio consta de: un núcleo central de fibra con un alto índice de refracción; una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor; y una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

  La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración. Su mayor desventaja es su coste de producción superior al resto de los tipos de cable, debido a las necesidades de empleo de vidrio de alta calidad y la fragilidad de su manejo en producción.

Dependiendo del número de haces de luz que se transmiten a la vez, se distinguen dos tipos de fibra óptica:

- **Monomodo.** En las fibras monomodo tan solo se envía un único haz de luz a través del cable. Por lo tanto, su velocidad es menor pero la distancia máxima del segmento es mucho mayor.
- **Multimodo.** Se transmiten varios haces de luz a la vez por lo que su velocidad es mayor pero la distancia de segmento es menor ya que a mayor distancia, es posible que un haz "adelante" a otro haz produciéndose un error en la transmisión.

En la tabla 2-1 puede ver la estructura de la fibra óptica y sus características.

Tabla 2-1. Estructura del cableado

	Par trenzado	Fibra óptica
Estructura interna del cable		
Conectores		
Velocidad	De 10 Mb/s a 1 Gb/s	Hasta 10 Tb/s
Distancia máxima de segmento	100 metros	Monomodo: 100 km Multimodo: 2,4 km

2.2 DISPOSITIVOS DE INTERCONEXIÓN

Los dispositivos de interconexión permiten conectar segmentos de una misma red, o redes diferentes. Los dispositivos que más se utilizan en una red son:

- **Repetidores.** Cualquier medio físico tiene una longitud máxima de segmento. Por ejemplo, la longitud máxima de un cable UTP Categoría 5 es de 100 metros. Esto quiere decir que si se utiliza un cable con una longitud mayor, en la señal eléctrica existe demasiada atenuación o

interferencias que hacen que la comunicación tenga muchos errores o que incluso sea impracticable.

Un repetidor es un dispositivo que regenera la señal transmitida evitando su atenuación; de esta forma se puede ampliar la longitud del cable que soporta la red. Por ejemplo, si queremos conectar dos equipos que se encuentran a una distancia de 150 metros, necesitaremos un repetidor que divida el cable en dos partes; de forma que ninguna exceda la longitud máxima del segmento del cable (100 metros).

- **Hub.** Un hub es un dispositivo de interconexión que permite conectar varios host o varios segmentos de una misma red. El tamaño de un hub viene determinado por el número de entradas que tiene (puertos). Existen hub desde 4 a 128 puertos.

  El funcionamiento interno del hub es como el de un "enchufe ladrón". El hub recibe una señal por un puerto y lo que hace es enviar la señal recibida por todos los demás puertos. Por lo tanto, una restricción que tiene un hub es evitar que se produzcan colisiones cuando recibe una señal por varios puertos.

  Un hub tiene dos grandes desventajas: es un dispositivo lento e inseguro ya que toda la información de un puerto se envía a los demás puertos.

Figura 2-1. Hub

- **Switch.** Al igual que un hub, un switch es un dispositivo de interconexión que permite conectar varios host o varios segmentos de una misma red. La diferencia entre un hub y un switch es que un switch tiene una pequeña memoria asociativa en la que guarda la dirección física (MAC) del equipo que está conectado a cada uno de sus puertos. De esta forma, al recibir un mensaje el switch mira la dirección de destino y lo envía solo a su destinatario.

  El switch resuelve los problemas de rendimiento y de seguridad de la red que tienen los hubs. El switch puede agregar mayor ancho de banda,

acelerar la salida de paquetes, reducir el tiempo de espera y bajar el coste por puerto.

En la figura 2-2, se puede ver un ejemplo de un switch Catalyst de Cisco System.

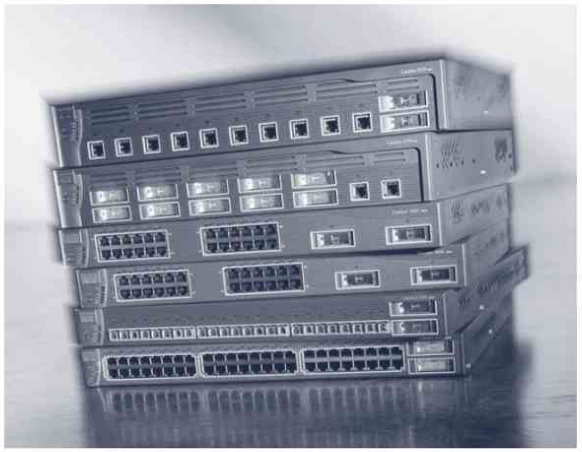


Figura 2-2. Switch Cisco Catalyst 2950

- **Gateways.** Se trata de un ordenador u otro dispositivo que interconecta redes radicalmente distintas. Son capaces de traducir información de una red a otra, como por ejemplo las pasarelas de correo electrónico. Un gateway trabaja en la capa de aplicación ya que necesita conocer el tipo de información que tiene que traducir de una red a otra.
- **Punto de acceso.** Un punto de acceso (AP, *Accesss Point*) permite crear una red inalámbrica para que los dispositivos puedan conectarse a la red a través de un adaptador inalámbrico. El punto de acceso actúa como puente entre una red Ethernet y la red inalámbrica, coordinando la transmisión y recepción de los diferentes dispositivos inalámbricos. Es importante prestar mucho cuidado a la seguridad de la red inalámbrica, ya que puede ser un lugar donde se originan muchos ataques. Lo ideal es considerar la red inalámbrica como una red no segura y limitar el acceso a equipos o servicios desde la red inalámbrica.

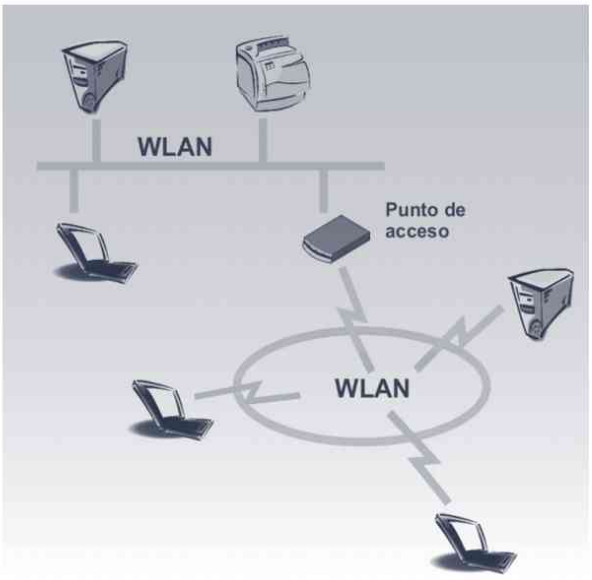


Figura 2-3. Red inalámbrica

- **Routers.** Un router es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar el tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios broadcast. También puede dar servicio de firewall.

  En la figura 2-4 puede ver un ejemplo de utilización de un router para conectar una red interna con Internet.

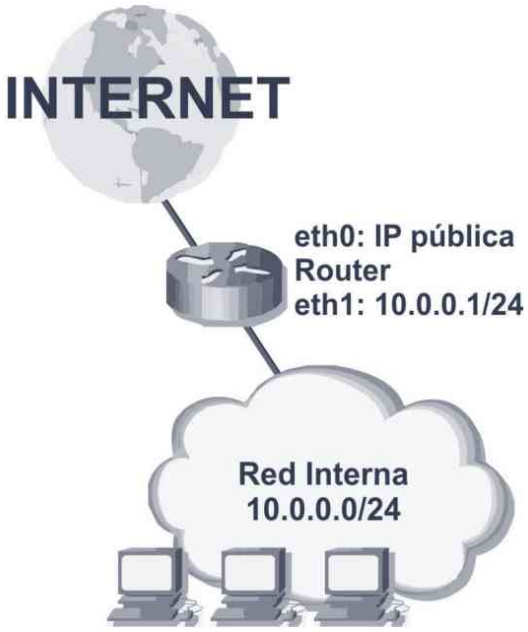


Figura 2-4. Ejemplo de utilización de un router

2.3 DIRECCIONAMIENTO IP

Cada interfaz de red de cada nodo (host o router) en una red IP se identifica mediante una dirección única de 32 bits. Las direcciones IP se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección. Por ejemplo, una dirección IP válida sería 147.156.23.208.

Si un nodo dispone de varias interfaces físicas (cosa habitual en los routers) cada una de ellas deberá tener necesariamente una dirección IP distinta. Es posible además, y en algunas situaciones resulta útil, definir varias direcciones IP asociadas a una misma interfaz física.

2.3.1 Clases de direcciones

Las direcciones IP tienen una estructura jerárquica. Tal y como muestra la figura 2-5, una parte de la dirección corresponde a la red (netid), y la otra al host dentro de la red (hostid). Cuando un router recibe un datagrama (mensaje) por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente solo contienen direcciones de red, no de host) y envía el datagrama por la interfaz correspondiente.

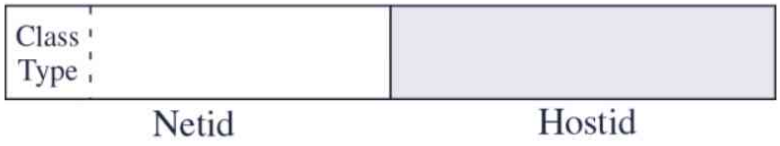


Figura 2-5. Partes de una dirección IP

En el diseño inicial de Internet se reservaron los ocho primeros bits para la red, dejando los 24 restantes para el host; se creía que con 254 redes habría suficiente para una red experimental que era fruto de un proyecto de investigación del Departamento de Defensa americano. Ya en 1980 se vio que esto resultaba insuficiente, por lo que se reorganizó el espacio de direcciones reservando una parte para poder definir redes más pequeñas. Para dar mayor flexibilidad y permitir diferentes tamaños se optó por dividir el rango de direcciones en tres partes adecuadas para redes grandes, medianas y pequeñas, conocidas como redes de clase A, B y C, respectivamente:

- Una red de clase A (que corresponde a las redes originalmente diseñadas) se caracteriza por tener a 0 el primer bit de dirección; el campo red ocupa

los 7 bits siguientes y el campo host los últimos 24 bits. Puede haber hasta 126 redes de clase A con 16 millones de hosts cada una.

- Una red de clase B tiene el primer bit a 1 y el segundo a 0; el campo red ocupa los 14 bits siguientes, y el campo host los 16 últimos bits. Puede haber 16.382 redes clase B con 65.534 hosts cada una.

- Una red clase C tiene los primeros tres bits a 110; el campo red ocupa los siguientes 21 bits, y el campo host los 8 últimos. Puede haber hasta dos millones de redes de clase C con 254 hosts cada una.

Para indicar qué parte de la dirección corresponde a la red y qué parte al host, se suele utilizar una notación denominada "máscara de red", consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host. Así, por ejemplo, diremos que una red clase A tiene una máscara 255.0.0.0, lo cual equivale a decir que los ocho primeros bits especifican la red y los 24 restantes el host. Análogamente decimos que una red clase B tiene una máscara 255.255.0.0 y una clase C una máscara 255.255.255.0. Otra notación utilizada en muchos sistemas es expresar de forma conjunta con la dirección IP el número de bits de la máscara de red. Así por ejemplo, para expresar una dirección de clase A sería 12.15.19.1/8, 12.15.19.1/16 de clase B y 12.15.19.1/24 de clase C.

Además existen direcciones de clase D (no redes) cuyos primeros cuatro bits valen 1110, que se utilizan para definir grupos multicast (el grupo viene definido por los 28 bits siguientes).

Por último, la clase E, que corresponde al valor 11110 en los primeros cinco bits, está reservada para usos futuros.

A partir de los valores de los primeros bits de cada una de las clases mencionadas anteriormente, se puede deducir el rango de direcciones que corresponde a cada una de ellas. Así pues, en la práctica es inmediato saber a qué clase pertenece una dirección determinada sin más que leer el primer byte de su dirección. La siguiente tabla resume toda la información esencial sobre los tipos de direcciones de Internet.

A modo de resumen, en la figura 2-6 puede ver un esquema de las diferentes clases de direcciones y en la tabla 2-2 puede ver las características principales de las clases de direcciones.

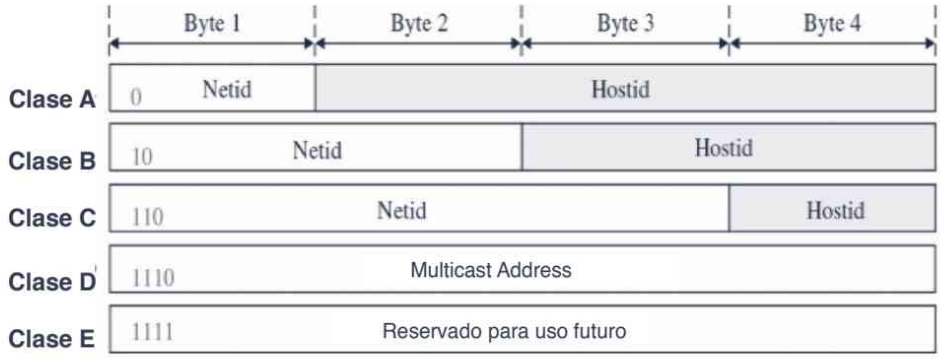


Figura 2-6. Clases de direcciones

Tabla 2-2. Características principales de las clases de direcciones

Clase	Bits reservados	Bits red/host	Número de redes	Número de ordenadores	Rango
A	*0---*	*7/24*	*126*	*16777214*	*1.0.0.0 127.255.255.255*
B	*10--*	*14/16*	*16384*	*65334*	*128.0.0.0 191.255.255.255*
C	*110-*	*21/8*	*2097152*		*192.0.0.0 223.255.255.255*
D	*1110*				*224.0.0.0 239.255.255.255*
E	*1111*				*240.0.0.0 255.255.255.255*

La asignación de direcciones válidas de Internet la realizan los NIC (NIC, *Network Information Center*). Al principio había un NIC para toda Internet pero luego se crearon NIC regionales (por continentes). Actualmente muchos países tienen un NIC propio, así ocurre en España donde el NIC es administrado por RedIRIS.

2.3.2 Direcciones específicas

Existen unas reglas y convenios en cuanto a determinadas direcciones IP que es importante conocer:

1. La dirección **255.255.255.255** se utiliza para indicar broadcast en la propia red, cualquiera que sea (y sea del tipo que sea).

2. La dirección **0.0.0.0** identifica al host actual.

3. La dirección con el **campo host todo a ceros** se utiliza para indicar la red misma, y por tanto no se utiliza para ningún host. Por ejemplo, la dirección 193.147.7.0 identifica la red clase B que pertenece a la Universidad de Valencia.

4. La dirección con el **campo host todo a unos** se utiliza como la dirección broadcast de la red indicada, y por tanto no se utiliza para ningún host. Por ejemplo, para enviar un mensaje broadcast en la red anterior, utilizaríamos la dirección 193.147.7.255.

5. La dirección con el **campo red todo a ceros** identifica a un host en la propia red, cualquiera que sea; por ejemplo, si queremos enviar un datagrama al primer host (1) de una red clase B podemos utilizar la dirección 0.0.0.1. Esto permite enviar datagramas sin saber en qué red nos encontramos, aunque es preciso conocer si es clase A, B o C para saber qué parte de la dirección es red y que parte es host.

6. La dirección **127.0.0.1** se utiliza para pruebas loopback; todas las implementaciones de IP devuelven a la dirección de origen los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte.

Como consecuencia de las reglas 3 y 4 siempre hay dos direcciones no asignables a hosts en una red. Por ejemplo, si tenemos la red 200.200.200.0 (clase C) tendremos que reservar la dirección 200.200.200.0 para denotar la red misma, y la dirección 200.200.200.255 para envíos broadcast a toda la red; dispondremos pues de 254 direcciones para hosts, no de 256.

A modo de resumen, en la tabla 2-3 puede ver un ejemplo de las diferentes direcciones específicas.

Tabla 2-3. Direcciones específicas

Dirección especial	Netid	Hostid	Ejemplo (193.147.7.32/24)
Dirección de red	*Específica*	*Todo a 0*	*193.147.7.0*
Dirección directa de broadcast	*Específica*	*Todo a 1*	*193.147.7.255*
Dirección broadcast limitada	*Todo a 1*	*Todo a 1*	*255.255.255.255*
Este host en esta red	*Todo a 0*	*Todo a 0*	*0.0.0.0*
Host específico en esta red	*Todo a 0*	*Específica*	*0.0.0.32*
Dirección loopback	*127*	*Cualquiera*	*127.0.0.1*

2.3.3 Direcciones privadas

La tabla 2-4 muestra que las direcciones de red **10.0.0.0, 172.16.0.0 a 172.31.0.0, y 192.168.0.0 a 192.168.255.0** están reservadas para redes privadas (intranets) por el RFC 1918. Estos números no se asignan a ninguna dirección válida en Internet y por tanto pueden utilizarse para construir redes privadas. Por ejemplo, detrás de un cortafuegos, sin riesgo de entrar en conflicto de acceso a redes válidas de Internet.

Tabla 2-4. Direcciones privadas

Clase	Rango	Número de redes
A	*10.x.x.x*	*1*
B	*De 172.16.x.x a 172.31.x.x*	*16*
C	*De 192.168.x.x a 192.168.255.x*	*256*

2.3.4 Subredes

A la hora de diseñar la red de una empresa uno de los aspectos que hay que tener en cuenta es optimizar el uso de redes públicas. Por ejemplo, es posible que tenga dos redes de servidores con 100 servidores cada una y desea que estén visibles en Internet.

Si se utilizan dos redes públicas de clase C se están desaprovechando los recursos de la empresa ya que una red pública de clase C puede tener 254 equipos y en el ejemplo se requieren 100. De esta forma se están desaprovechando más de la mitad de las direcciones IP disponibles en cada red pública. Hay que tener en cuenta que las direcciones IP públicas tienen un coste y que son limitadas.

En el ejemplo planteado es lógico que en vez de tener dos redes de clase C se utilice una única red para las dos redes de 100 servidores cada una. Por lo tanto, resulta útil disponer de algún mecanismo que permita dividir una red IP en trozos o subredes.

Al realizar la división de redes se va creando así un nivel jerárquico intermedio entre la red y el host; de esa forma la empresa puede, por ejemplo, solicitar una red de clase B e ir asignando fragmentos de dicha red a cada oficina a medida de que se vayan creándose. Supongamos que a la empresa se le asigna la clase B 156.134.0.0; de los 16 bits que en principio corresponden al host podría reservar los primeros 8 para la subred y dejar los 8 siguientes para el host, con lo que habría 256 subredes de 256 direcciones cada una. Desde fuera la red de la

empresa seguiría siendo 156.134.0.0, ya que la estructura de subred no sería visible.

Las subredes se añadieron a Internet en 1982, con lo que se consiguió una mayor flexibilidad en el reparto de direcciones dentro de una red.

Para dividir la red en subredes se define una *máscara* en la que están a 1 los bits de la dirección que corresponden a la red-subred, y a 0 los que corresponden al host. Por ejemplo, la máscara 255.255.255.0 divide una red clase B en 256 subredes de 256 hosts pues tiene puestos a 1 los primeros 24 bits (los 16 de la clase B más los 8 de la subred). Se pueden hacer divisiones que no correspondan con bytes enteros; por ejemplo, si la máscara fuera 255.255.252.0 se estarían reservando los primeros 6 bits del campo host para la subred y dejando 10 para el host; con lo que podría haber hasta 64 redes con 1.024 hosts cada una.

Al crear subredes hay dos direcciones de cada subred que quedan automáticamente reservadas: las que corresponden al campo host todo a 0 y todo a 1; éstas se emplean para la designación de la subred y para la dirección broadcast, respectivamente. Así, si la red 156.134.0.0 se subdivide con la máscara 255.255.255.0, se crean 256 subredes del tipo *156.134.subred.host*, siendo *156.134.subred.0* la dirección que identifica a toda la subred y *156.134.subred.255* la dirección broadcast de la subred. Por tanto, el número de hosts de una subred es siempre dos menos que el número de direcciones que abarca; por lo que no tiene sentido crear subredes con la máscara 255.255.255.254 en las que el campo host tendría un bit, pues no dispondría de direcciones útiles.

Del mismo modo que los valores todo ceros o todo unos del campo host están reservados con un significado especial, el valor todo ceros y todo unos del campo subred también son especiales. El valor todo ceros se utiliza para representar la subred misma; por ejemplo, si a la red 156.134.0.0 le aplicamos la máscara 255.255.255.0 el campo subred todo a ceros no debería utilizarse, pues resultaría ambiguo el significado de la dirección 156.134.0.0, que representaría tanto a dicha subred como a la red entera. Por otro lado, el campo subred todo a unos tampoco debería utilizarse porque de lo contrario el significado de la dirección 156.134.255.255 sería ambiguo, significaría tanto broadcast en la subred como en la red entera. Por consiguiente, en el campo subred también se pierden siempre dos direcciones, y tampoco tendría sentido crear máscaras con el campo subred de un bit.

A continuación se van a ver varios ejemplos prácticos para aprender a realizar divisiones de redes.

2.3.4.1 Ejemplo básico

Realiza la división de la dirección de red 193.147.12.0/24 en 4 redes de 50 ordenadores. ¿Cuántas direcciones IP se pierden?

empresa seguiría siendo 156.134.0.0, ya que la estructura de subred no sería visible.

Las subredes se añadieron a Internet en 1982, con lo que se consiguió una mayor flexibilidad en el reparto de direcciones dentro de una red.

Para dividir la red en subredes se define una *máscara* en la que están a 1 los bits de la dirección que corresponden a la red-subred, y a 0 los que corresponden al host. Por ejemplo, la máscara 255.255.255.0 divide una red clase B en 256 subredes de 256 hosts pues tiene puestos a 1 los primeros 24 bits (los 16 de la clase B más los 8 de la subred). Se pueden hacer divisiones que no correspondan con bytes enteros; por ejemplo, si la máscara fuera 255.255.252.0 se estarían reservando los primeros 6 bits del campo host para la subred y dejando 10 para el host; con lo que podría haber hasta 64 redes con 1.024 hosts cada una.

Al crear subredes hay dos direcciones de cada subred que quedan automáticamente reservadas: las que corresponden al campo host todo a 0 y todo a 1; éstas se emplean para la designación de la subred y para la dirección broadcast, respectivamente. Así, si la red 156.134.0.0 se subdivide con la máscara 255.255.255.0, se crean 256 subredes del tipo *156.134.subred.host*, siendo *156.134.subred.0* la dirección que identifica a toda la subred y *156.134.subred.255* la dirección broadcast de la subred. Por tanto, el número de hosts de una subred es siempre dos menos que el número de direcciones que abarca; por lo que no tiene sentido crear subredes con la máscara 255.255.255.254 en las que el campo host tendría un bit, pues no dispondría de direcciones útiles.

Del mismo modo que los valores todo ceros o todo unos del campo host están reservados con un significado especial, el valor todo ceros y todo unos del campo subred también son especiales. El valor todo ceros se utiliza para representar la subred misma; por ejemplo, si a la red 156.134.0.0 le aplicamos la máscara 255.255.255.0 el campo subred todo a ceros no debería utilizarse, pues resultaría ambiguo el significado de la dirección 156.134.0.0, que representaría tanto a dicha subred como a la red entera. Por otro lado, el campo subred todo a unos tampoco debería utilizarse porque de lo contrario el significado de la dirección 156.134.255.255 sería ambiguo, significaría tanto broadcast en la subred como en la red entera. Por consiguiente, en el campo subred también se pierden siempre dos direcciones, y tampoco tendría sentido crear máscaras con el campo subred de un bit.

A continuación se van a ver varios ejemplos prácticos para aprender a realizar divisiones de redes.

2.3.4.1 Ejemplo básico

Realiza la división de la dirección de red 193.147.12.0/24 en 4 redes de 50 ordenadores. ¿Cuántas direcciones IP se pierden?

Para realizar la división correctamente se realizan los siguientes pasos:

- **Calculo la dirección de red**

  193.147.12.0/24

- **Paso la parte hostid de la red a binario**

  193.147.12.00000000/24

- **Calculo el número de bits que necesito para dividir ($2^n \geq n^o$ de divisiones)**

  $2^2 \geq 4$ → Utilizo 2 bits

- **Calculo el número de ordenadores que puede tener cada subred**

  La nueva máscara de red es de 26 bits (24 + 2) luego el número de equipos de cada red es $2^{(32-26)} = 2^6 = 64$ equipos. Realmente son 62 equipos ya que por cada red se pierden 2 direcciones IP (la dirección de red y la de broadcast).

- **Realizo las divisiones**

193.147.12.00000000/24

193.147.12.00000000/26 = 193.147.12.0/26
- 0 → Dirección de red
- 1.. 62 → IP para equipos
- 63→ Dirección broadcast

193.147.12.01000000/26 = 193.147.12.64/26
- 64→ Dirección de red
- 65…126→ IP para equipos
- 127→ Dirección broadcast

193.147.12.10000000/26 = 193.147.12.128/26
- 128→ Dirección de red
- 129.. 190→ IP para equipos
- 191→ Dirección broadcast

193.147.12.11000000/26 = 193.147.12.192/26
- 192→ Dirección de red
- 193...254→ IP para equipos
- 255→ Dirección broadcast

Como tengo 4 redes y se pierden 2 direcciones IP por cada red, en total pierdo 8 IP (antes se perdían únicamente 2 IP).

2.3.4.2 Varias subredes

Realiza la división de la dirección de red 193.147.12.0/24 en 3 redes de 50 ordenadores y 4 redes de 12 ordenadores. ¿Cuántas direcciones IP se pierden?

En este caso la división de la red hay que hacerla en dos pasos. Primero se realiza la división de la red con un mayor número de ordenadores y luego el resto.

1ª DIVISIÓN: 3 redes de 50 ordenadores

- **Calculo la dirección de red**

  193.147.12.0/24

- **Paso la parte hostid de la red a binario**

  193.147.12.00000000/24

- **Calculo el número de bits que necesito para dividir ($2^n \geq n^o$ de divisiones)**

  $2^2 \geq 4$ → Utilizo 2 bits

- **Calculo el número de ordenadores que puede tener cada subred**

  La nueva máscara de red es de 26 bits (24 + 2) luego el número de equipos de cada red es $2^{(32-26)} = 2^6 = 64$ equipos. Realmente son 62 equipos ya que por cada red se pierden 2 direcciones IP (la dirección de red y la de broadcast).

- **Realizo las divisiones**

193.147.12.00000000/24

193.147.12.00000000/26 = 193.147.12.0/26
- 0 → Dirección de red
- 1.. 62 → IP para equipos
- 63→ Dirección broadcast

193.147.12.01000000/26 = 193.147.12.64/26
- 64→ Dirección de red
- 65…126→ IP para equipos
- 127→ Dirección broadcast

193.147.12.10000000/26 = 193.147.12.128/26
- 128→ Dirección de red
- 129.. 190→ IP para equipos
- 191→ Dirección broadcast

193.147.12.11000000/26 = 193.147.12.192/26 *Red libre para seguir diviendo*

En este momento ya tengo las 3 redes de 50 equipos y una red libre. Ahora, voy a seguir dividiendo la dirección de red que queda libre.

2ª DIVISIÓN: 4 redes de 12 ordenadores

- **Calculo la dirección de red**

  193.147.12.192/26

- **Paso la parte hostid de la red a binario**

  193.147.12.11000000/26

- **Calculo el número de bits que necesito para dividir ($2^n \geq n^o$ de divisiones)**

  $2^2 \geq 4$ → Utilizo 2 bits

- **Calculo el número de ordenadores que puede tener cada subred**

  La nueva máscara de red es de 28 bits (26 + 2) luego el número de equipos de cada red es $2^{(32-28)} = 2^4 = 16$ equipos. Realmente son 14 equipos ya que por cada red se pierden 2 direcciones IP (la dirección de red y la de broadcast).

- **Realizo las divisiones**

193.147.12.11000000/26

193.147.12.11000000/26 = 193.147.12.192/28 { 192 → Dirección de red; 193.. 206→ IP para equipos; 207→ Dirección broadcast

193.147.12.11010000/26 = 193.147.12.208/28 { 208→ Dirección de red; 209…222→IP para equipos; 223→ Dirección broadcast

193.147.12.11100000/26 = 193.147.12.224/28 { 224→ Dirección de red; 225..238→ IP para equipos; 239→ Dirección broadcast

193.147.12.11110000/26 = 193.147.12.240/28 { 240→ Dirección de red; 241...254→ IP para equipos; 255→ Dirección broadcast

Resultado final

El resultado final sería:

- 193.147.12.00000000/24
  - 193.147.12.0/26 (red de 50 equipos)
  - 193.147.12.64/26 (red de 50 equipos)
  - 193.147.12.128/26 (red de 50 equipos)
  - 193.147.12.192/26
    - 193.147.12.192/28 (red de 12 equipos)
    - 193.147.12.208/28 (red de 12 equipos)
    - 193.147.12.224/28 (red de 12 equipos)
    - 193.147.12.240/28 (red de 12 equipos)

Como tengo un total de 7 redes y se pierden 2 direcciones IP por cada red, en total se pierden 14 IP (antes se perdían únicamente 2 IP).

Más información

Existen programas que nos permiten dividir redes. Por ejemplo, el programa IP SubNet Calculator de http://www.wildpackets.com/products/free_utilities/ipsubnetcalc/overview

2.4 CONFIGURACIÓN DE ROUTERS

Como hemos visto anteriormente, un router es un dispositivo de interconexión que permite regular el tráfico que pasa entre varias redes. Un router es muy útil a la hora de defendernos de posibles intrusiones o ataques externos. Pero como desventaja es que un router no se configura por sí solo. Mientras que un router bien configurado puede ser muy útil, un router mal configurado no nos proporciona ningún tipo de protección o, simplemente, no llega a comunicar dos redes.

2.4.1 Tablas de enrutado

Para configurar un router hay que crear lo que se denomina "tabla de enrutado". En ella se guardan las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino. Existen dos tipos de encaminamiento: "encaminamiento clásico" y "encaminamiento regulado".

2.4.1.1 Encaminamiento clásico

Con el "encaminamiento clásico", las reglas utilizadas para encaminar los paquetes se basan, exclusivamente, en la dirección destino que aparece en la cabecera del paquete. Así se distinguen las siguientes reglas:

- Permitir un equipo de nuestra red.
- Permitir cualquier equipo de nuestra red.
- Permitir un equipo de otra red.
- Permitir cualquier equipo de otra red.

La última regla (por defecto) se aplica en el caso de que no se cumpla ninguna de las anteriores y se suele utilizar para poder enviar los mensajes a la puerta de enlace de la red.

2.4.1.2 Encaminamiento regulado

Sin embargo, en la actualidad, con la explosión del uso de Internet y la llegada del concepto de calidad de servicio (QoS) y la seguridad, los routers utilizan el llamado "encaminamiento regulado", con el que, a la hora de escribir la tabla de enrutado, se pueden utilizar los siguientes elementos:

- **Interfaz** de red por donde se recibe la información.
- **Origen/Destino** del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP, pero algunos routers permiten utilizar como dirección origen y destino usuarios o grupos de usuarios.
- **Protocolo.** Permite o deniega el acceso a los puertos; es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto para que un cliente (que inicia la conexión) pueda conectarse. Por ejemplo, un servidor web trabaja en el puerto 80, un servidor de FTP en el puerto 21, etc.
- **Seguimiento.** Indica si el router debe de realizar un seguimiento de los lugares por los que pasa un mensaje.
- **Tiempo.** Espacio temporal en el que es válida la regla.
- **Autenticación de usuarios.** Indica si el usuario debe de estar autenticado para utilizar la regla.
- **Acción.** Especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:
  - **Aceptar.** Deja pasar la información
  - **Denegar.** No deja pasar la información
  - **Reenviar.** Envía el paquete a una determinada dirección IP.

Nota

No es lo mismo encaminamiento regulado que regular el encaminamiento. Como se ha visto, el primer concepto hace referencia a la toma de decisiones de encaminamiento basándonos en más argumentos que solo la dirección de destino. Sin embargo, regular el encaminamiento es establecer normas administrativas al encaminamiento, independientemente de las tablas de rutas.

Existen diferentes tipos de routers por lo que en un principio puede caer en la tentación de pensar que el proceso de configuración para cada router es totalmente diferente a los demás. Los router más utilizados son:

- *FireWall 1* de CheckPoint.
- *Private Internet Exchange (PIX)* de Cisco System.
- *IOS Firewall Feature Set* de Cisco System.
- *Firewall del núcleo* de Linux, Iptables.
- *Enterprise Firewall* de Synmatec.
- *Internet Security and Acelerador (ISA Server)* de Microsoft.

Si se comparan los elementos que utilizan los diferentes routers (ver tabla 2-5) puede ver cómo los más utilizados a la hora de realizar una tabla de enrutado son la **interfaz**, la **dirección origen y destino**, el **puerto** y la **acción** que debe realizar el router.

Tabla 2-5. Comparativa sobre los elementos de las tablas de enrutado

Modelo	*Interfaz*	*Origen /Destino*	*Protocolo*	*Seguimiento*	*Tiempo*	*Autenticación de usuarios*	*Acción*
FireWall 1	√	√**	√	√	√		√
PIX	√	√	√*				√
IOS Firewall	√	√	√				√
Firewall Linux	√	√	√				√
Enterprise Firewall	√	√**	√		√	√	√
ForeFront (Microsoft)	√	√**	√*		√	√	√

* Distingue entre puerto de origen y destino
** Permiten especificar como origen o destino direcciones IP o usuarios.

A la hora de indicar la **dirección de origen** o la **dirección de destino** es importante utilizar la máscara de red para indicar un mayor o menor número de ordenadores. Así, por ejemplo, si en la dirección destino utiliza la dirección de clase B 142.165.2.0/16 se hace referencia a todas las direcciones IP del tipo 142.165.x.x. Si utiliza la dirección de clase C 192.165.2.0/24, hace referencia a las direcciones del tipo 192.165.2.x. Por tanto, si aumenta la máscara de red, se disminuye el número de direcciones IP a las que se hace referencia y si disminuimos la máscara de red, entonces se hace referencia a un mayor número de direcciones IP. En la tabla 2-6, puede ver algunas de las posibilidades más habituales.

Tabla 2-6. Ejemplos de utilización de la máscara de red en la configuración de routers

Ejemplo	Comentario
192.165.2.23/32	*Representa a un único ordenador (p. ej. servidor web)*
192.165.2.0./24	*Representa a todas las direcciones IP del tipo 192.165.2.X*
192.165.0.0/16	*Representa a todas las direcciones IP del tipo 192.165.X.X*
192.0.0.0/8	*Representa a todas las direcciones IP del tipo 192.X.X.X*
0.0.0.0/0	*Representa a todas las direcciones IP del tipo X.X.X.X*

Durante el filtrado de paquetes se aplica la regla de "coincidencia total". Todos los criterios de la regla tienen que coincidir con el paquete entrante; en caso contrario, no se aplica la regla. Esto no significa que se rechace el paquete o que se elimine, sino que la regla no entra en vigor. Normalmente, las reglas se aplican en orden secuencial, de arriba hacia abajo. Aunque hay varias estrategias para implementar filtros de paquetes, las dos que se describen a continuación son las más utilizadas por los especialistas de seguridad:

- **Construir reglas desde la más específica a la más general.** Esto se hace así para que una regla general no "omita" a otra más específica, pero conflictiva, que entra dentro del ámbito de la regla general.
- **Las reglas deberían ordenarse de tal forma que las que más se utilizan estén en la parte superior de la lista.** Esto se hace por cuestiones de rendimiento. Normalmente un router detiene el procesamiento de una lista cuando encuentra una coincidencia total.

2.4.2 Ejemplo de creación de una tabla de enrutado

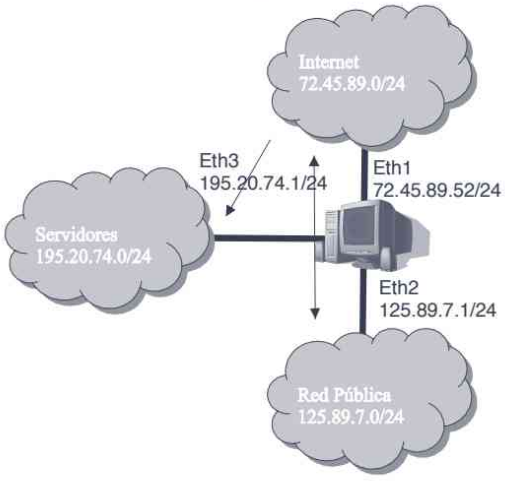
La figura 2-7 muestra un router conectado a tres redes diferentes. El objetivo es crear el conjunto de reglas para permitir que: la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

La tabla de enrutado representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes. Las notas acerca de la implementación se incluyen siguiendo la descripción de cada línea del conjunto de reglas.

Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de

servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.



	Interfaz	Dirección origen	Dirección destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.7/32	25, 110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

Figura 2-7. Ejemplo de red y de tabla de enrutado

- **Regla 1.** Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 195.20.74.5 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio web, por lo que no hay restricción en las direcciones IP de origen.
- **Regla 2.** Esta regla permite el acceso entrante a los puertos 25 y 110, que normalmente se utiliza para correo electrónico (el puerto 25 es el servidor smtp o correo saliente y el puerto 110 es el servidor pop3 o correo entrante). El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, como no se puede predecir quién va a tener acceso al servidor de correo no se restringen las direcciones IP de origen.
- **Regla 3.** Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la regla 1 y 2, si se ejecuta antes, se permite el tráfico que va dirigido a los servidores web y correo

electrónico. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a ningún servidor.

- **Reglas 4 y 5.** La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.
- **Regla 6.** Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.

Capítulo 3

SERVICIOS

3.1 INTRODUCCIÓN

Los orígenes de Internet hay que situarlos en ARPANET, una red de ordenadores establecida por ARPA en septiembre de 1969. El departamento de defensa de los Estados Unidos fundó esta Agencia de Proyectos de Investigación Avanzada en 1958 para movilizar recursos procedentes del mundo universitario principalmente, a fin de alcanzar la superioridad tecnológica militar sobre la Unión Soviética. La construcción de ARPANET se justificó como medio de compartir el tiempo de computación en línea de los ordenadores entre varios centros de informática y grupos de investigación de la agencia. Para establecer una red informática se basó en una revolucionaria tecnología de transmisión de telecomunicaciones, la conmutación de paquetes (*packet switching*), desarrollada de manera independiente por Paul Baran (colaborador del Pentágono) y por Donald Davies de Gran Bretaña. El diseño de una red de comunicaciones flexible y descentralizada era una propuesta del Departamento de Defensa para construir un sistema de comunicaciones militar, capaz de sobrevivir a un ataque nuclear. Los primeros nodos de la red eran universidades, en 1969 había 3 y en 1971 había 15. En 1972 tuvo lugar la primera demostración con éxito de ARPANET, durante un congreso internacional en Washington DC.

El siguiente paso consistió en posibilitar la conexión de ARPANET con otras redes de ordenadores, comenzando por las redes de comunicaciones que ARPA estaba gestionando: PRNET y SATNET. Esta posibilidad introdujo un nuevo concepto: la red de redes. En 1973, dos informáticos, Robert Kahn y Vint Cert, elaboraron un trabajo en el que esbozaban la arquitectura básica de Internet. Cerf y Kahn se basaron en los diseños del Network Working Group, un grupo

técnico formado en los sesenta por representantes de diversos centros de informática conectados mediante ARPANET, y entre los que se incluían el propio Cerf, Steve Crocker y Jon Postel. Para conseguir que las redes de ordenadores pudieran comunicarse entre ellas, eran necesarios unos protocolos de comunicación estandarizados. En el año 1973, durante un seminario en Stanford un grupo de investigadores, liderados por Cerf, consiguió alcanzar parcialmente este objetivo gracias al diseño del Protocolo de Control de Transmisión (TCP). En 1978, Cerf junto a otros investigadores, dividieron TCP en dos partes, añadiendo el protocolo interredes (IP) y creando así el protocolo TCP/IP estándar sobre el que aún opera Internet. Aún así, ARPANET continuó utilizando un protocolo diferente, el NCP, durante cierto tiempo. En 1975 ARPANET fue transferida a la Agencia de Comunicaciones de la Defensa, con objeto de facilitar la comunicación entre ordenadores de diferentes divisiones de las fuerzas armadas. La DCA decidió crear una conexión entre las diversas redes bajo su control y estableció la Red de Datos de la Defensa que operaba con el protocolo TCP/IP. El 1983, el Departamento de Defensa, preocupado por posibles violaciones de seguridad, decidió crear la red MIL-NET, destinada exclusivamente a funciones militares. ARPANET se convirtió en ARPA-INTERNET, y se destinó a la investigación. En 1984, la Fundación Nacional para la Ciencia estableció su propia red informática de comunicaciones (NSFNET), y en 1990 ARPANET, tecnológicamente obsoleta, fue desmontada.

Con la tecnología para la creación de redes informáticas abierta al dominio público y con las telecomunicaciones en pleno proceso de desregularización, la NSF procedió inmediatamente a la privatización de Internet. En 1995, se cerró la NSFNET dando paso con ella al uso privado de Internet. A principios de los noventa, una serie de proveedores de servicios Internet construyeron sus propias redes y establecieron pasarelas con fines comerciales. A partir de ese momento, Internet comenzó a desarrollarse rápidamente, como una red global de redes informáticas, desarrollo propiciado por el diseño original de ARPANET, basado en una arquitectura descentralizada en varias capas y protocolos abiertos de comunicación. En estas condiciones, se pudo ampliar la red gracias a la incorporación de nuevos nodos e infinitas reconfiguraciones de la misma para ir acomodándola a las necesidades de comunicación.

Ahora bien, ARPANET no fue la única fuente para la construcción de Internet, tal y como lo conocemos hoy. La forma actual de Internet es también el resultado de una tradición de interconexión informática autónoma y alternativa. Uno de los componentes de esta tradición fue la corriente de los Tablones de Anuncios Electrónicos (BBS: *Bulletin Board Systems*) que surgió de la conexión en red de PC a finales de los años setenta. En 1977, dos estudiantes de Chicago diseñaron un dispositivo (MODEM) que permitía transferir archivos entre sus PC, y en 1978, el *Computer Bulletin Board System* permitía a los PC archivar y transmitir mensajes. Decidieron difundir ambos programas en el dominio público. En 1983, Tom Jennings, un programador que entonces trabajaba en California, creó

su propio programa BBS, FIDO, y puso en marcha una red de BBS, FIDONET. FIDONET en el año 2000 contaba con 40.000 nodos y unos tres millones de usuarios. Aunque esta cifra representa tan solo una mínima fracción del total de usuarios de Internet, el uso de la red BBS y la cultura simbolizada por FIDONET tuvieron una enorme influencia de la configuración del Internet global.

La comunidad de usuarios de UNIX representó una tendencia decisiva en la conexión informática en red. UNIX es un sistema operativo creado por los laboratorios Bell, que posteriormente lo entregaron a las universidades en 1974, junto al código fuente y el permiso expreso para modificar dicho código. UNIX se convirtió en la lengua de la mayor parte de los departamentos universitarios de informática y los estudiantes pronto se adiestraron en su manejo. Más tarde, en 1978, los laboratorios Bell distribuyeron su programa UUCP que permitía copiar archivos de un ordenador a otro. En 1980, difundieron gratuitamente una versión mejorada de este programa en un seminario de usuarios UNIX. Esto permitió la formación de redes de comunicación de ordenadores, Usernet news, fuera del eje troncal de ARPANET, extendiendo con ello considerablemente la práctica de la comunicación informática. En verano de 1980, Usernet News llegó al departamento de informática de la Universidad de California, Berkeley, donde un grupo de doctorandos estaba trabajando en adaptaciones y aplicaciones UNIX. Como Berkeley era un nodo ARPANET, este grupo de estudiantes desarrolló un programa diseñado para tender un puente entre las dos redes. A partir de ese momento, USENET, quedó ligada a ARPANET, y las dos acabaron uniéndose para formar Internet.

Otro de los grandes avances de la tradición de usuario de UNIX fue el movimiento del software libre, o sea, el propósito predeterminado de permitir el acceso abierto a toda la información existente sobre sistemas de software.

Lo que hizo posible que Internet abarcara a todo el planeta fue el World Wide Web. Ésta es una aplicación para compartir información desarrollada en 1990 por un programador inglés, Tim Berners-Lee. Aunque él mismo no era consciente de ello, su trabajo estaba en consonancia con una larga tradición de ideas y proyectos técnicos llevados a cabo a lo largo de los cincuenta años precedentes, con la idea de enlazar entre sí diversas fuentes de información mediante un sistema interactivo de computación. Pero fue Berners-Lee quien hizo realidad todos estos sueños a base de perfeccionar el programa Enquire que había ideado en 1980. Bernes-Lee definió y elaboró el software que permitía sacar e introducir información desde cualquier ordenador conectado a través de Internet (http, HTML y URI, posteriormente denominado URL). En colaboración con Robert Cailliau, construyeron un programa navegador/editor en diciembre de 1990 y dieron el nombre de World Wide Web a este sistema de hipertexto. CERN divulgó en la red el software para el browser WWW en agosto de 1991. Una serie de hackers de todo el mundo comenzaron a desarrollar sus propios navegadores, basándose en el

trabajo de Berners-Lee. La primera versión modificada fue Erwise, desarrollado por el Instituto Tecnológico de Helsinki en abril de 1992. Poco después, Viola, en la Universidad de Berkeley, creó su propia adaptación. De estas versiones modificadas de la WWW, la que tenía una orientación más comercial era Mosaic. Mosaic incorpora una capacidad gráfica avanzada, para poder obtener y distribuir imágenes a través de Internet, así como una serie de técnicas de interfaz importadas del mundo multimedia. Hicieron público su software en Usernet en enero de 1993, gratis como la World Wide Web. Mosaic Communications, posteriormente se vio obligada a cambiar su nombre por Netscape Navigator.

Así, para mediados de los noventa, Internet estaba ya privatizado y su arquitectura técnica abierta permitía la conexión en red de todas las redes informáticas de cualquier punto del planeta, la World Wide Web podía funcionar con el software adecuado y habia navegadores de fácil uso a distribución de los usuarios. A pesar de que Internet estaba ya en la mente de los informáticos desde principios de los setenta, para la gente, para las empresas y para la sociedad en general, Internet nació en 1995.

Desde que en 1983, Tom Jennigs, creó el primer servicio de Internet (BBS) han ido apareciendo nuevos servicios que han contribuido a la gran expansión de Internet. Sin duda alguna Internet ha cambiado nuestras vidas al igual que nosotros, con las necesidades que plantea la sociedad, hace que cambie Internet. Hoy en día Internet es una gran red que nos permite acceder a múltiples servicios. Por ejemplo, consultar una página web, enviar correos electrónicos, videoconferencia, etc.

Aunque los servicios más conocidos en Internet es el servidor web y de correo electrónico, también existen otros servicios necesarios y menos conocidos que permiten crear la infraestructura de una red. Estos servicios son los siguientes:

- **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.ual.es* equivale a 150.214.156.62.

Además de los servicios ya comentados existen otros muchos servicios como, por ejemplo, compartir datos, acceso remoto a sistema, monitorización de equipos, etc. A continuación se van a ver los servicios más utilizados.

3.2 SERVICIO DHCP

El mantenimiento y la configuración de los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IP así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace…, conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP; o se dispone de un sistema de asignación dinámica y flexible que permita reutilizar las direcciones de tal forma que solo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente que tenemos, algo inviable con el número de usuarios conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

El servidor DHCP se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Los datos mínimos que un servidor de DHCP proporciona a un cliente son:

- Dirección IP.
- Máscara de red.
- Puerta de enlace o gateway.
- Dirección IP del servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- **Asignación dinámica.** Asigna direcciones IP libres de un rango de direcciones establecido por el administrador en el fichero */etc/dhcpd.conf*. Es el único método que permite la reutilización dinámica de las direcciones IP.
- **Asignación por reservas.** Si queremos que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración para una determinada dirección MAC se asignará una dirección IP.

Éste método es muy útil para aquellos dispositivos que no queramos que cambien de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP deberemos configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

3.3 SERVICIO DNS

Los equipos informáticos se comunican entre sí mediante una dirección IP como 150.214.150.30. Sin embargo nosotros preferimos utilizar nombres (p.e. *www.adminso.es*) porque son más fáciles de recordar y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.

Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del fichero */etc/hosts* (Linux) o *c:/windows/system32/driver/etc/hosts* (Windows) en los que se guarda cada nombre junto a su respectiva dirección IP. Con todo, esta opción presenta varios problemas.

Por un lado, todos los equipos de la red están obligados a conocer cualquier cambio para actualizar sus ficheros apropiadamente. Es decir, ante, por ejemplo, la inserción de un nuevo elemento en la red, debe añadirse en los ficheros locales de cada equipo los datos referentes a su nombre y dirección IP. Este hecho indica la poca escalabilidad y manejabilidad de esta opción, sobre todo si hablamos de Internet o, sin llegar a este extremo, de cualquier red local que tenga, por ejemplo, más de veinte ordenadores.

Además, el mantenimiento tan descentralizado y dependiente de ficheros locales conlleva un alto riesgo de falta de sincronización y descoordinación entre los equipos de la red y, por tanto, de la información que manejan.

Para paliar estos problemas se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se dispone de uno o más servidores encargados de resolver los nombres de los equipos pertenecientes a su ámbito, consiguiendo, por un lado, la centralización necesaria para la correcta sincronización de los equipos, un sistema jerárquico que permite una administración focalizada y, también, descentralizada y un mecanismo de resolución eficiente.

3.3.1 Espacio de nombres de dominio

Al igual que los sistemas de fichero se organizan en árboles jerárquicos y el nombre absoluto de un fichero es el formado por los distintos directorios que

recorremos hasta encontrar el fichero, separados por el carácter '/' (o '\' en sistemas Windows), el sistema de nombres de dominios también se estructura con un árbol jerárquico en el que las distintas ramas que encontramos reciben el nombre de dominio y el nombre completo de un equipo –el equivalente al nombre de un fichero– o FQDN –path absoluto– es el nombre resultante de recorrer todos los dominios por los que pasamos desde las hojas hasta la raíz del árbol utilizando, en este caso, el carácter '.' como separador (véase la figura 3-1).

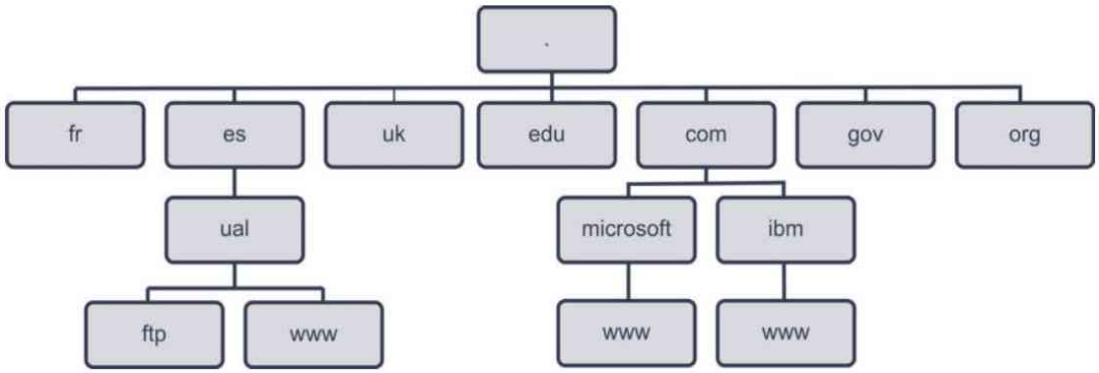


Figura 3-1. Ejemplo de jerarquía de los dominios en Internet

El sistema de nombres de Internet presenta, por tanto, una estructura jerárquica en árbol, en el que cada rama constituye lo que se denomina un dominio de Internet, y dependiendo de la profundidad del árbol, hablaremos de dominios de primer, segundo o tercer nivel –pudiendo existir más, aunque no es habitual–.

En el primer nivel del árbol encontramos que los nombres de los nodos ya están establecidos de antemano, existiendo dos tipos de divisiones: geográfica y organizativa. Con la primera se distingue una rama –dominio– por país: .es para España; .uk para Gran Bretaña; .de para Alemania,... Con la segunda se establece una rama por tipo de organización: .com para empresas, independientemente del país en el que se encuentren; .int para organizaciones establecidas mediante tratados internacionales; .org para organizaciones no gubernamentales y, por último, .edu, .gov y .mil para organizaciones educativas, del gobierno y el ejército de EEUU. Posteriormente, se han introducido nuevos dominios de primer nivel como .name para nombres de personas; .info para proveedores de servicios de información; .web para empresas relativas a servicios web; etc.

Cada rama del árbol jerárquico en el que se estructura el sistema de nombres de dominio, recibe el nombre de dominio y, para la resolución global de nombres no es determinante quién se encarga de mantener la información asociada

a cada dominio. Con esta estructura, la asignación de nombres de una rama del árbol de primer nivel se delega en un responsable –la empresa pública REDES para España– el cual puede decidir, a su vez, delegar la autoridad de resolución de los nombres de las distintas ramas en las que se divide, en otras corporaciones.

Por ejemplo, la asignación de nombres de dominio de Internet y la creación de subdominios inferiores para la rama .es, recae, como ya se ha comentado, en la empresa pública REDES que delega, a su vez, en el Servicio de Informática de la Universidad de Almería la gestión del dominio de segundo nivel *ual.es* que decidirá la asignación de nombres y subdominios para esta rama del árbol. Este concepto, definido como Delegación de Autoridad es muy importante dentro del sistema de resolución. Existe, para cada dominio de primer nivel, un organismo encargado de gestionar los datos de resolución de su dominio y se dice que tiene delegada la autoridad de resolución. Cada autoridad puede decidir, a su vez, crear otras ramas dentro del árbol y delegar la resolución de los nombres asignados por debajo, a otros organismos o empresas. Los organismos o empresas que gestionan estos dominios, denominados de tercer nivel, a su vez, pueden permitir la creación de más subdominios y delegar o no la resolución de nombres para ellos.

En un determinado nivel pueden coexistir ramas (subdominios) y nodos finales cuyo nombre se formará con las etiquetas –no nulas y con un máximo de 63 caracteres por nivel– de cada rama, recorriendo el árbol desde la posición del nodo hasta la raíz, separando tal y como se ha comentado, cada transición con un '.'. Este sistema genera un sistema de nombres jerárquico y descriptivo que facilita la localización de los equipos.

Por otra parte, el sistema de resolución de nombres permite la llamada resolución inversa, según la cual, dada una dirección IP, deberíamos obtener su nombre asociado. Para que la estructura sea coherente también con esta función, se debe crear una rama del árbol que permita dicha resolución. El nombre que recibe el dominio de primer nivel encargado de la representación distribuida de los datos para la resolución inversa es "arpa" y el de segundo nivel es el de "in-addr". Por debajo de estos, se crea una rama por cada octeto de la dirección IP, es decir, cuatro nodos más en el árbol, de tal manera que el FDQN para la resolución inversa, de, por ejemplo, la dirección IP 150.214.156.62 tiene el registro **150.214.156.62.in-addr.arpa** (véase la figura 3-2).

Un servidor DNS puede encargarse de gestionar los datos de un dominio completo o parte de un dominio. El conjunto de datos que puede administrar un servidor de nombres recibe el nombre de zona. En la figura 3-3 podemos ver que el servidor DNS será el encargado de gestionar los datos del dominio ual.es

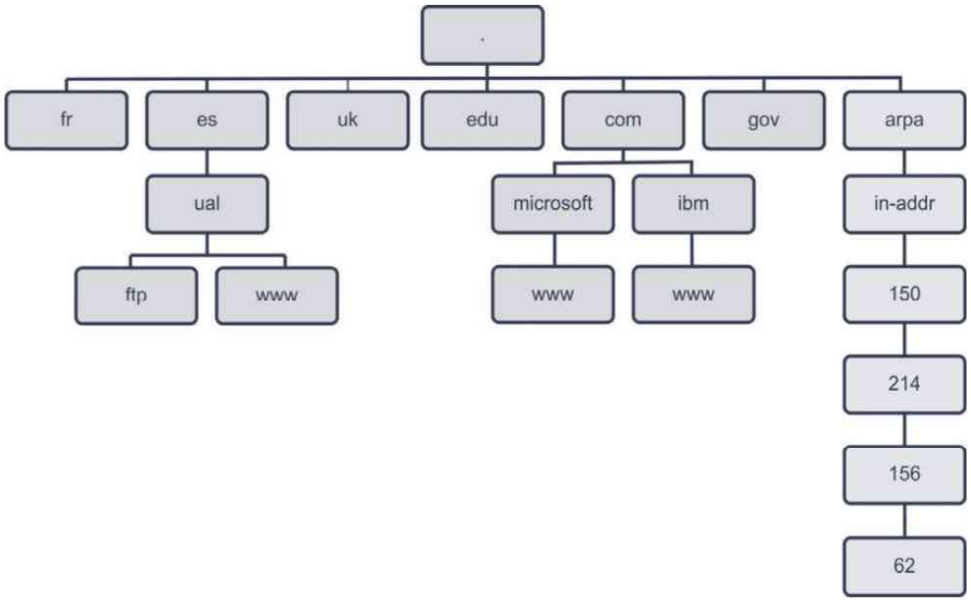


Figura 3-2. Árbol jerárquico con resolución inversa

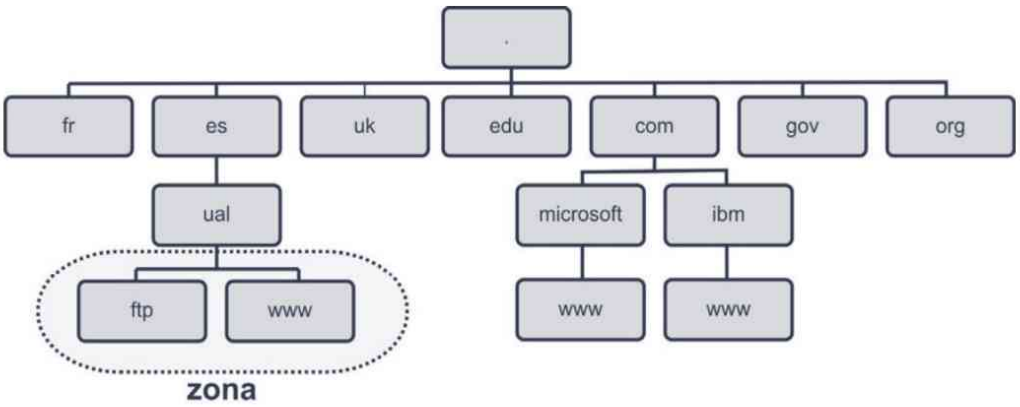


Figura 3-3. Representación de una zona gestionada por un servidor

Por otra parte, con la importancia que ha adquirido la resolución de nombres –nadie usa ya las direcciones IP, sino los nombres asociados– una característica crucial es la máxima disponibilidad del servicio. Para ello, una buena solución es que existan varios servidores independientes capaces de realizar el mismo servicio de tal forma que la autoridad de resolución de zona siga recayendo en un servidor aunque éste puede permitir que otros puedan responder a requerimientos de los clientes. Los servidores que tienen asignada la autoridad de resolución de nombres y que gestionan la base de datos de la zona, reciben el nombre de servidores primarios. Los servidores que pueden resolver requerimientos para una zona, pero que la fuente de información la obtienen de otro servidor, reciben el nombre de servidores secundarios.

Para que no existan problemas de sincronización entre servidores, los secundarios deben conseguir sus datos del servidor primario mediante el proceso llamado "transferencia de zona" que no es más que el traspaso de todas los pares dirección IP-nombre simbólico que gestiona el servidor. Cada vez que se modifique un dato del servidor primario debe transmitirse a todos los secundarios que estén declarados para el correcto funcionamiento del sistema.

De esta forma, no solo se consigue aumentar la disponibilidad del servicio, sino hacerlo más eficiente ya que la carga de trabajo puede repartirse entre distintos servidores. Si el objetivo es exclusivamente éste, existe otro tipo de servidores llamados caché cuya finalidad es la de responder a peticiones de resolución, consultando, previamente, las peticiones almacenadas en memoria y, si no se corresponde con ninguna de ellas, iniciar el proceso de resolución de nombres recursivo visto anteriormente. Los servidores caché solo son útiles si el número de usuarios es suficientemente elevado para sacar provecho de la caché de direcciones.

3.3.2 Registrar un dominio

Cualquier persona física con residencia en España así como empresas constituidas según la legislación española, puede solicitar el registro de dominios a través de *http://nic.es* o bien por medio de los agentes registradores acreditados (*http://www.nic.es/listado-agentes/agenteRegistrador/1447*). Los nombres de dominio se deben, según la reglamentación española, corresponder con:

- Nombre (o abreviatura) de una empresa que la identifique de forma inequívoca.
- Nombres comerciales o de marcas.
- Nombre de personas tal y como aparecen en su DNI, con un máximo de 60 caracteres.
- Nombres de profesiones y el apellido o nombre del profesional que se dedica a dicha labor o del nombre del establecimiento.
- Denominaciones de origen, en cuyo caso debe solicitarlo el órgano regulador de dicha denominación.

Una vez registrado el dominio podremos acceder a una web que nos permitirá gestionar los distintos registros del dominio. Por ejemplo, en la figura 3-4 se muestra la interfaz de gestión del dominio *adminso.es* en *http://www.arsys.es*.

Nota

Los cambios que realices en un registro están visibles en Internet antes de 24 horas.

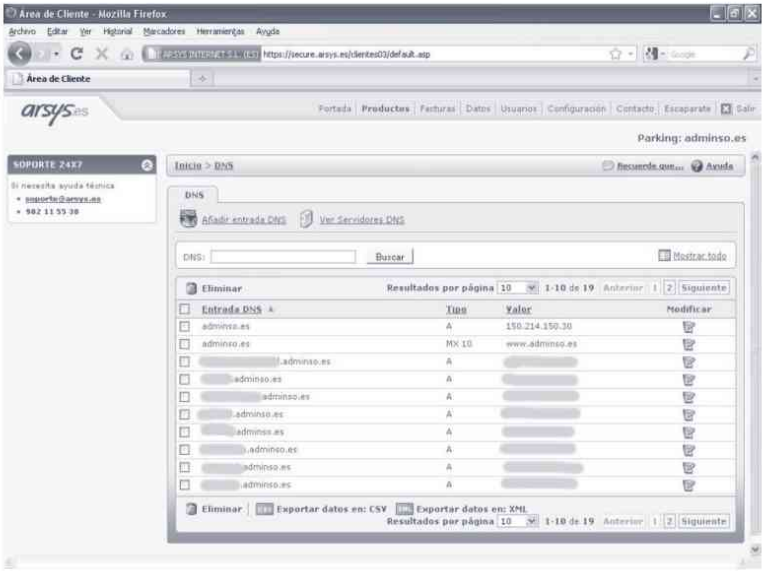


Figura 3-4. Gestión del dominio adminso.es

3.3.3 Tipos de registro

Tal y como se ha visto anteriormente, un servidor de nombres es el encargado de gestionar un dominio o parte de un dominio. El conjunto de datos que administra el servidor recibe el nombre de zona. Por ejemplo, el servidor de nombres de la Universidad de Almería es el encargado de gestionar la zona ual.es.

Para administrar una zona existe un servidor DNS primario y, normalmente, además del servidor primario se dispone de uno o más servidores secundarios que únicamente realizan una copia de la zona. De esta forma, existen tres tipos de servidores:

- **Primarios.** Son los que guardan los datos del espacio de nombres en sus ficheros. Requiere la siguiente información: fichero de configuración y los ficheros de datos para la resolución directa e inversa.

- **Secundarios.** Obtienen los datos de servidores primarios mediante una transferencia de zona. La única información que requieren este tipo de

servidores es el fichero de configuración y el fichero de datos obtenidos del servidor primario.

- **Caché.** Ejecuta el software del servidor pero no contienen los ficheros de base de datos. Aprende las respuestas de otros servidores, las guarda y las usa para responder a resoluciones futuras. La única información que requiere es la de caché.

La comunicación entre los servidores DNS se realiza mediante lo que se llama una *transferencia de zona*.

Una zona (p. ej., *adminso.es*) tiene registros (p. ej., *www.adminso.es*) que son los encargados de asociar un nombre a una dirección IP. En la tabla 3-1 se muestran los diferentes tipos de registros de un servidor de nombres entre los que se destacan:

- **Registro tipo A.** Es el más utilizado y permite asociar un nombre (p. ej., *www.adminso.es*) con una dirección IP (p.e.: 150.214.153.30).

- **Registro tipo CNAME.** Permite establecer un alias entre dos registros. Por ejemplo, *www.adminso.es* es igual que *ftp.adminso.es*.

- **Registro MX.** Este registro es muy importante ya que permite indicar dónde se encuentra el servidor de correo electrónico (Mail eXchanger). Este tipo de registro se asocia siempre a otro nombre y permite asignar prioridades en los servidores. Así la entrada MX10 indica el primer servidor de nombres, MX20 el segundo, etc.

Tabla 3-1. Tipos de registro

Registro	Función
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.
HINFO	Descripción de la computadora. CPU y S.O.
WKS	Servicios públicos disponibles en la computadora.

3.4 SERVICIO FTP

FTP es el protocolo más antiguo de la capa de aplicación TCP/IP que permite la transferencia de ficheros. FTP define un protocolo cliente/servidor que describe la manera en que se establece la comunicación entre los servidores y clientes FTP. Concretamente, permite el envío y la recepción de archivos del servidor.

Aunque pueden contemplarse otras posibilidades, hay dos tipos fundamentales de acceso a través de FTP:

- **Anónimo.** La comunicación se realiza sin ningún tipo de identificación y, por lo tanto el usuario tendrá muy pocos privilegios en el servidor. En este caso, el usuario estará confinado en un directorio público donde puede descargar los archivos allí ubicados pero sin posibilidad de escribir o modificar ningún fichero.
- **Acceso autorizado.** El usuario establece la comunicación con una cuenta de usuario. Tras identificarse, se confina al usuario a su directorio predeterminado desde donde puede descargar ficheros y, si la política del sistema lo permite, también escribir. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.

Existen programas que permiten conectarse cómodamente a un servidor FTP (p. ej., filezilla, cuteftp, vsftp, Internet Explorer). Sin embargo, la forma más simple de utilizar un servidor FTP es estableciendo una conexión por línea de comandos. Para conectarse a un servidor ejecute ftp servidor en el intérprete de comandos de su sistema, y utilice los comandos FTP que aparecen en la tabla 3-2; sin importar el sistema operativo que utilice.

Tabla 3-2. Comandos FTP

Comando	Descripción
ascii	Establece el tipo de transferencia de archivos a la modalidad ASCII.
bell	Emite una señal acústica cuando se completa un comando.
binary	Establece el tipo de transferencia de archivos a modalidad binario.
bye	Finaliza la sesión ftp y cierra.
cd	Cambia el directorio de trabajo del ordenador remoto.
cdup	Cambia el directorio de trabajo del ordenador remoto al raíz.
close	Finaliza la sesión ftp.
delete	Borra archivos remotos.
dir	Lista el contenido del directorio remoto.
get	Obtiene un archivo del ordenador remoto.
help	Muestra la ayuda.
lcd	Cambia el directorio local de trabajo.

ls	Lista el contedio del directorio remoto.
mkdir	Crea un directorio.
open	Establece una conexión con el servidor ftp remoto.
put	Envía un archivo al ordenador remoto.
pwd	Muestra el directorio de trabajo en la máquina remota.
quit	Finaliza la sesión ftp y sale.
rename	Renombra un archivo.
rrmdir	Elimina un directorio de la máquina remota.
status	Muestra el estado actual.
system	Muestra información sobre el sistema remoto.
user	Envía nueva información de usuario.

3.5 SERVICIO WEB

Conocido con el nombre de World Wide Web, o más concretamente, por sus siglas WWW que, además, aparecen en el nombre de prácticamente todos los servidores web, el servicio web es, posiblemente, el servicio más extendido y utilizado de los que se ofrecen en Internet, con el permiso del sistema de correo electrónico.

El servidor web se encarga del almacenaje y la difusión de información mediante la distribución de páginas HTML. Su arquitectura se basa en la archiconocida cliente-servidor, típica de los servicios basados en TCP/IP, en la que se distinguen: el proceso servidor, como por ejemplo, Apache, Internet Information Server e Iplanet y el proceso cliente (también llamado navegador), como Mozilla Firefox, Google Chrome, Internet Explorer, etc.

El servidor es el que almacena y sirve las páginas HTML. Los navegadores se encargan, además de realizar la petición de la página deseada, de interpretarla y mostrar el resultado al usuario. Para que el cliente y el servicio se entiendan, se comunican mediante el protocolo HTTP. Éste es un protocolo orientado a conexión y del tipo de solicitud-respuesta, es decir, no se guarda información de estado sino que toda interacción entre el cliente y el servidor se fundamenta en pedir y servir.

Para identificar qué página desea un cliente, éste realiza una petición con la que especifica toda la información necesaria para que tanto el navegador como el servidor web interpreten correctamente qué recurso desea el cliente y dónde se encuentra. La petición se realiza mediante el llamado localizador universal de recursos (URL).

Para solicitar páginas y visualizarlas, los clientes web (navegadores) presentan un entorno gráfico y amigable que facilita la navegación por la WWW. Existen multitud de navegadores con la misma funcionalidad y, prácticamente, con las mismas características. Las principales diferencias entre los clientes web residen en el número e importancia de vulnerabilidades que presentan así como en

diferentes matizaciones que existen en cuanto a la interpretación del código HTML y que puede impedir la correcta visualización de algunas páginas en determinados clientes. En la figura 3-5 puede ver dos navegadores diferentes: a la izquierda Google Chrome y a la derecha Mozilla Firefox.

Figura 3-5. Ejemplos de clientes web

En la actualidad existen varios servidores web tanto para sistemas GNU/Linux como para sistemas Windows. Como se observa en la gráfica de la figura 3-6, Apache es el servidor web más utilizado en Internet muy por encima del resto de competidores.

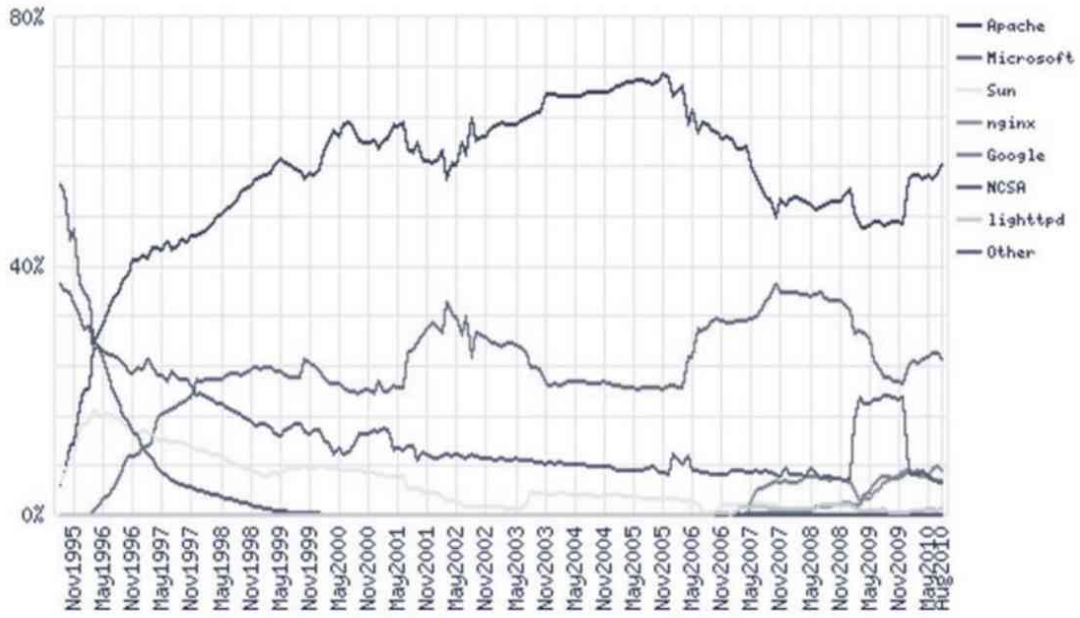


Figura 3-6. Cuota de mercado de servidores web (Fuente: http://www.netcraft.com)

3.6 SERVICIO DE CORREO ELECTRÓNICO

El sistema de correo electrónico es, junto al WWW, el servicio proporcionado en Internet que más importancia y auge ha presentado, al menos en cuanto al número de usuarios se refiere. De hecho, se considera como uno de los principales factores que ha popularizado el uso de Internet.

Este servicio es un sistema para la transferencia mensajes, rápido y eficiente, ideado bajo la arquitectura cliente-servidor típica de Internet. No es simplemente un programa cliente que se comunica con un servidor mediante un protocolo de aplicación, sino que está compuesto por varios subsistemas, cada uno con una funcionalidad determinada que interaccionan entre sí mediante distintos protocolos de aplicación. La funcionalidad que todo usuario espera de este sistema es:

- Composición del mensaje.
- Transferencia desde el origen al destino sin intervención del usuario.
- Generación de un informe de la transmisión del mensaje.
- Visualización de los correos recibidos.
- Gestión de los correos: lectura, borrado, almacenaje…

Otras características que puede aportar un sistema de correo electrónico a un usuario son, por ejemplo, la redirección de correos de unas cuentas a otras, listas de correo, correo de alta prioridad o cifrado...

Tal y como se muestra en la figura 3-7, el sistema de correo electrónico lo constituyen cuatro componentes:

- **Cliente de correo (MUA).** Ofrece los mecanismos necesarios para la lectura y composición de los mensajes de correo.
- **Servidor de salida (MTA).** Recibe el correo electrónico y lo envía al servidor de entrada del dominio del receptor.
- **Servidor de entrada (MTA).** Almacena los correos electrónicos enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido.
- **Agente de acceso.** Se encarga de conectar un agente de usuario al mensaje almacenado mediante protocolos de aplicación como POP e IMAP.

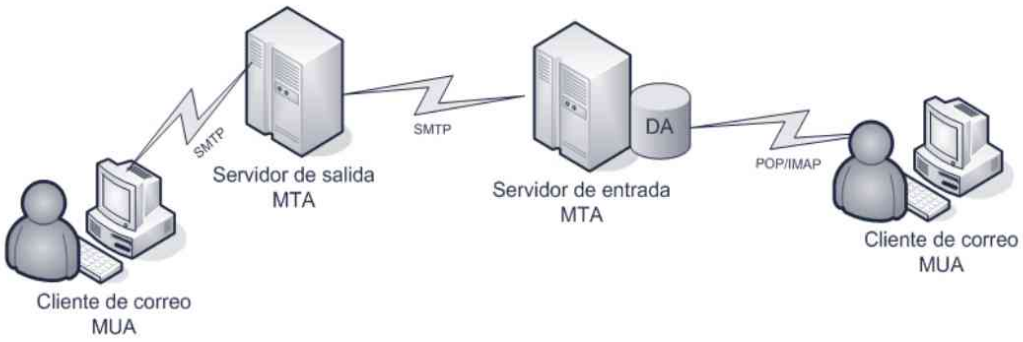


Figura 3-7. Arquitectura del sistema de correo electrónico.

Para comunicar los distintos subsistemas que componen la arquitectura del servicio de correo, se dispone de los protocolos:

- **Simple Mail Transport Protocol (SMTP)** encargado del transporte de los mensajes de correo.
- **Postal Office Protocol (POP)** e **Internet Message Access Protocol (IMAP)** encargados, ambos, de comunicar a los agentes de usuario (MUA) con los agentes de entrega de correo (MDA). Además, permiten la gestión, por parte de los usuarios, de sus buzones de correo.

El cliente de correo electrónico es una aplicación que proporciona al usuario una interfaz –más o menos amigable– con los mecanismos necesarios para escribir, recibir y contestar a mensajes. La figura 3-8 muestra el cliente de correo Evolution.

Existen clientes de correo electrónico basados en diferentes interfaces, de texto o gráfica, que introducen más o menos familiaridad y coste de aprendizaje para el usuario, pero todos presentan las mismas funciones: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.

Nota

Si desea gestionar el correo electrónico en un terminal en Linux puede ejecutar el comando mail.

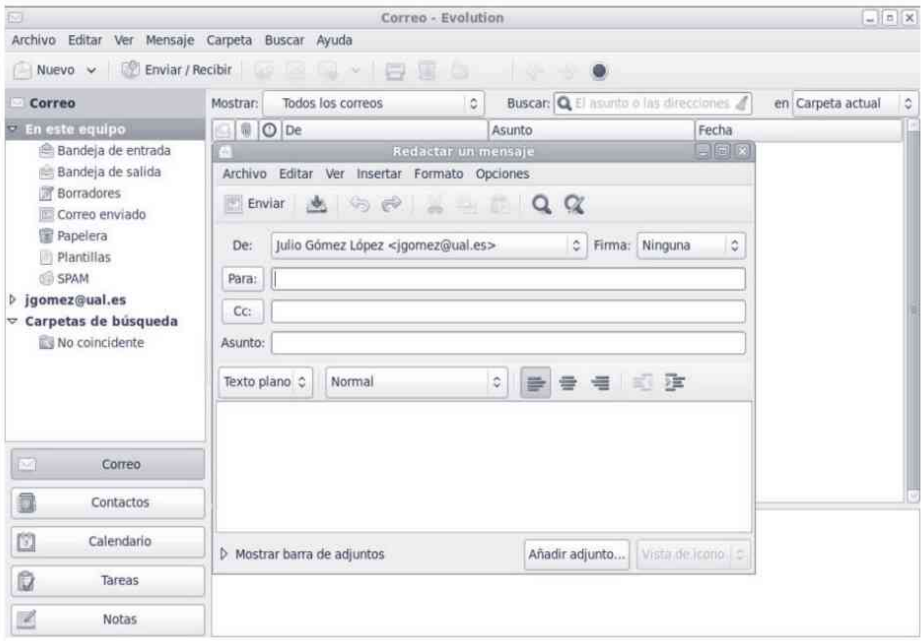


Figura 3-8. Cliente de correo clásico

Cuando se inicia el cliente, lo primero que realiza es la lectura de los correos recibidos en su buzón de entrada y su presentación al usuario indicando la fecha de llegada, el emisor, si ya se ha leído o no, la prioridad o importancia....

Para leer el correo electrónico se pueden usar dos protocolos: POP (Protocolo de oficina postal) e IMAP (Protocolo de acceso a correo de Internet). La principal diferencia entre ambos es que POP realiza la gestión del correo sobre el equipo desde el que se conecta el cliente mientras que IMAP realiza la gestión sobre el servidor (los mensajes y las carpetas para ordenarlos están almacenadas en el servidor).

Por otro lado, cuando envía un correo electrónico, los pasos que realiza el sistema para la entrega del mensaje son:

- El cliente se conecta al servidor de salida y le proporciona el mensaje a enviar, almacenándose en la cola de espera definida por el servidor.
- Cuando el servidor de salida revisa su cola y ve el mensaje en espera, inicia el proceso de transmisión al destinatario, obteniendo la dirección del servidor de destino mediante el sistema de nombres de dominio.
- Se establece una conexión TCP hacia el servidor de correo entrante del destinatario, mandando una copia del mensaje. Una vez que el servidor de salida origen y el servidor de entrada del destino acuerdan la recepción de la copia, el servidor origen borra su copia local del mensaje.

- Si ocurre algún fallo, el proceso de transferencia registra la hora en que se intentó la entrega y termina dejando el mensaje en la cola hasta que se reinicie todo el proceso. Si transcurrido un tiempo el mensaje no ha podido ser entregado, se devuelve al emisor un mensaje informándole del error.

3.7 SERVICIO DE 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.

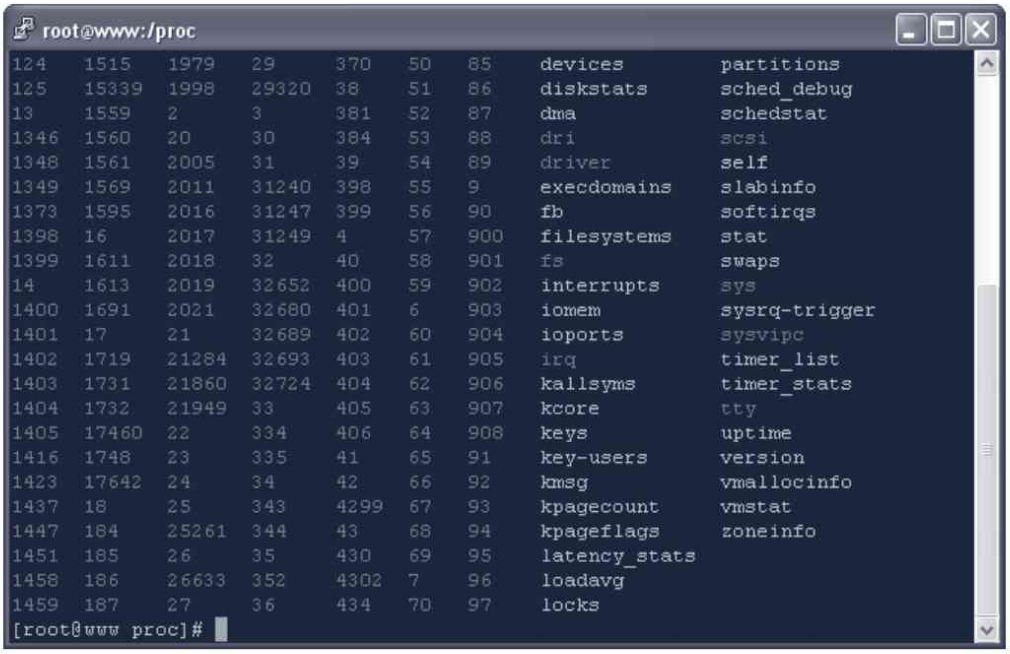


Figura 3-9. Conexión remota por SSH con PuTTY

- **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).

Figura 3-10. Conexión a Escritorio remoto

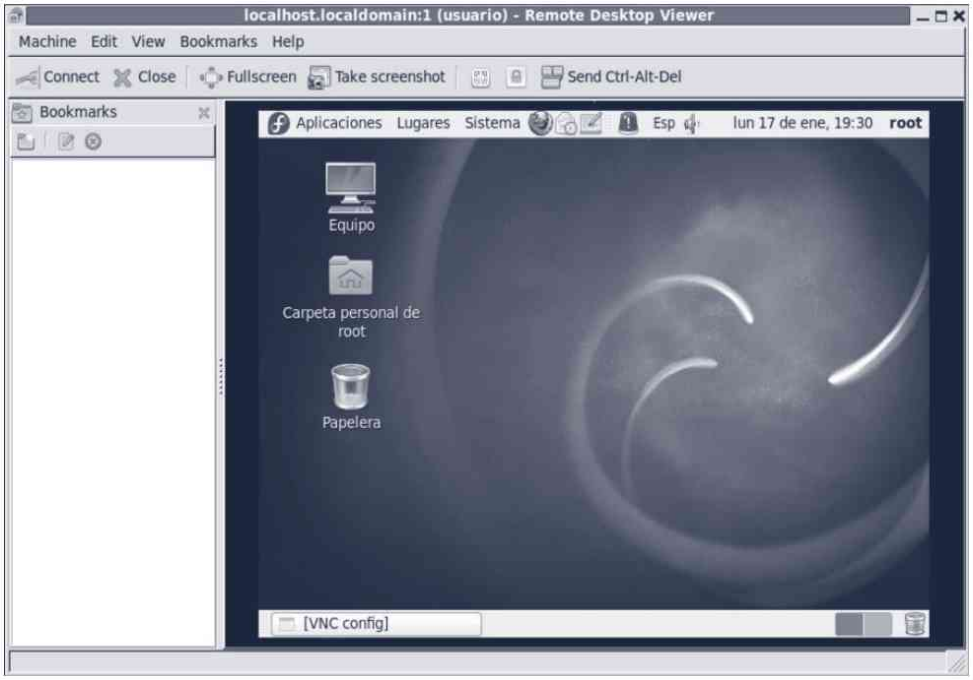


Figura 3-11. Acceso al servidor por VNC con Vinagre (Linux)

Capítulo 4

SEGURIDAD

Según la Real Academia de la Lengua, seguridad es la cualidad de seguro, es decir, de estar libre y exento de todo daño, peligro o riesgo. En informática, como en tantas facetas de la vida, la seguridad entendida según la definición anterior es prácticamente imposible de conseguir, por lo que se ha relajado acercándose más al concepto de fiabilidad; se entiende un sistema seguro como aquel que se comporta como se espera de él.

De los sistemas informáticos, ya sean sistemas operativos, servicios o aplicaciones, se dice que son seguros si cumplen las siguientes características:

- **Confidencialidad.** Requiere que la información sea accesible únicamente por las entidades autorizadas.

- **Integridad.** Requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos.

- **No repudio.** Ofrece protección a un usuario frente a otro usuario que niegue posteriormente que se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

- **Disponibilidad.** Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

4.1 LAS DIEZ LEYES INMUTABLES DE LA SEGURIDAD

Una de las tareas más importantes del administrador del sistema es que todo funcione de forma segura. Scout Culp, de Microsoft Security Response Center, en el artículo "The ten inmutable laws of security" indica las leyes que hay que tener en cuenta para mantener la seguridad de un sistema:

1. **Si alguien puede convencerle de que ejecute su programa en su equipo, dejará de ser su equipo.** Con frecuencia, los atacantes intentan animar al usuario a instalar software en nombre de éste. Muchos virus y caballos de Troya funcionan de esta forma. Por ejemplo, el virus ILOVEYOU tuvo éxito porque los usuarios impacientes ejecutaron la secuencia de comandos cuando llegaba en un mensaje de correo electrónico. Otra variante son las aplicaciones de espionaje. Una vez instaladas, las aplicaciones de espionaje supervisan las actividades de un usuario en su equipo y muestran los resultados al atacante.
2. **Si alguien puede modificar el sistema operativo, dejará de ser su equipo.** Si un atacante puede reemplazar o modificar cualquiera de los ficheros del sistema operativo o determinados componentes hardware del sistema, ya no podrá confiar en su equipo. Por ejemplo, un atacante puede reemplazar el fichero *passfilt.dll* que se utiliza para reforzar la complejidad de las contraseñas con una versión del fichero que también registre todas las contraseñas utilizadas en el sistema. Si el sistema operativo se ve comprometido o no puede comprobar si se ha comprometido, ya no debe confiar en el sistema.
3. **Si alguien tiene acceso físico sin restricciones a su equipo, dejará de ser su equipo.** Cuando un atacante tenga acceso físico a un equipo, poco podrá hacer por evitar que el atacante obtenga privilegios administrativos sobre el sistema operativo. Con los privilegios administrativos comprometidos, prácticamente todos los datos almacenados de forma persistente se verán afectados. De igual forma, un atacante con acceso físico podrá instalar hardware o software para supervisar y registrar pulsaciones de forma transparente al usuario. En caso de que un equipo se vea físicamente comprometido no confíe en él.
4. **Si permite que alguien cargue programas en su sitio web, dejará de ser su sitio web.** Un atacante que pueda ejecutar aplicaciones o modificar código en el sitio web podrá apropiarse de él. Un corolario de esta ley es

que si un sitio web solicita datos al usuario, los atacantes pueden intentar introducir datos incorrectos. Por ejemplo, si tiene un formulario que solicite un número entre 1 y 100. Mientras que los usuarios normales escribirán números en el intervalo de datos especificado, un atacante intentará utilizar cualquier dato que considere que "rompe" con la aplicación de servidor (algunos de estos ataques son XSS o SQL inyectado).

5. **Las contraseñas débiles anulan una seguridad fuerte.** Aunque un diseño de red sea seguro, si los usuarios y administradores utilizan contraseñas en blanco, predeterminadas o sencillas, la seguridad será del todo ineficaz si un atacante consigue descifrar la contraseña o consigue realizar un ataque de fuerza bruta.

6. **Una máquina es tan segura como digno de confianza sea el administrador.** Una constante en todas las redes es que se debe confiar en los administradores de red. Cuantos más privilegios administrativos tenga un administrador, más confianza habrá que tener en éste. Es decir, si no confía en alguien, no le conceda privilegios administrativos.

7. **Los datos de cifrado son tan seguros como las claves de descifrado.** Ningún algoritmo de cifrado protegerá el texto cifrado de cualquier ataque en caso de que éste posea o pueda conseguir la clave de descifrado.

8. **Un programa antivirus no actualizado es poco más seguro que no disponer del mismo.** Siempre aparecen nuevos virus informáticos, gusanos y caballos de Troya, y los ya existentes evolucionan. Por tanto, el software antivirus puede quedarse desfasado rápidamente. A medida que surjan nuevos o modificaciones de lo existentes, se deberá actualizar el antivirus.

9. **El anonimato absoluto no es práctico en la vida real ni en la web.** Dos aspectos relacionados con la seguridad que a menudo se suelen confundir son la *privacidad* y el *anonimato*. El anonimato significa que la identidad y los detalles sobre un usuario son completamente desconocidos e imposibles de rastrear, mientras que la privacidad significa que la identidad y los detalles sobre la misma no se revelan. La privacidad es esencial, y la tecnología y las leyes posibilitan conseguirlo. Por otra parte, el anonimato no es posible ni práctico cuando el usuario está en Internet, o cuando se utilizan equipos en general.

10. **La tecnología no es una panacea.** Aunque la tecnología puede asegurar los equipos y las redes informáticas, no es una solución (ni lo será nunca) por sí misma. Por ejemplo, si tenemos un router y no lo configuramos correctamente éste no valdrá para nada.

4.2 CONCEPTOS BÁSICOS SOBRE SEGURIDAD

El tratamiento de los posibles incidentes de seguridad exige que toda organización tenga definida una política de seguridad cuya función sea establecer las responsabilidades y reglas necesarias para evitar amenazas y minimizar los efectos de éstas. Lo primero que se debe realizar es identificar qué queremos proteger.

Desde el punto de vista informático, existen tres tipos de elementos que pueden sufrir amenazas: hardware, software y datos. El más sensible, y en el que se basa casi toda la literatura sobre seguridad, son los datos, ya que es el único elemento que depende exclusivamente de la organización. Es decir, tanto el hardware como el software, si en la peor de las situaciones se pierden, siempre se pueden adquirir y/o instalarlos; pero los datos pertenecen a la organización y nadie puede, en el caso de pérdida, proporcionárnoslos. Sin embargo, la seguridad se debe entender a todos los niveles y aplicarla a todos los elementos.

4.2.1 Amenazas de seguridad

Se entiende por amenaza una condición del entorno del sistema de información (p. ej., persona, máquina, idea, etc.) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas de seguridad pueden caracterizarse modelando el sistema como un flujo de información; desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Tal y como puede ver en la figura 4-1, las cuatro categorías generales de amenazas o ataques son los siguientes:

- **Interrupción.** Un recurso del sistema es destruido o se vuelve no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- **Intercepción.** Una entidad no autorizada consigue acceso a un recurso. Éste es un ataque contra la confidencialidad. La entidad no autorizada

podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son interceptar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- **Modificación.** Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es alterar un programa para que funcione de forma diferente, modificar el contenido de un fichero o de un mensaje transferido por la red.

- **Fabricación.** Un ataque contra la autenticidad es cuando una entidad no autorizada inserta objetos falsificados en el sistema. Ejemplos de este ataque son la inserción de mensajes espurios (mensajes basura) en una red o añadir registros a un fichero.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

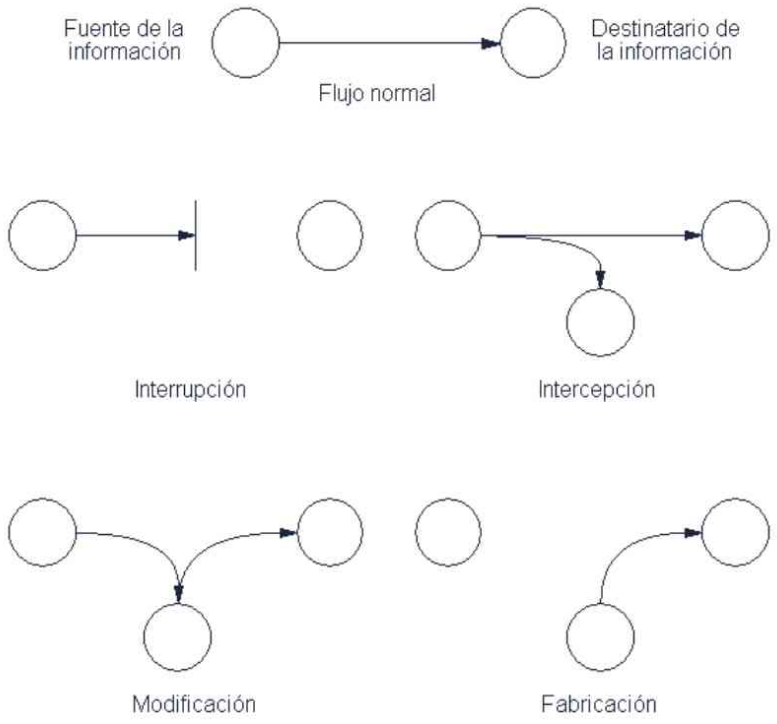


Figura 4-1. Tipos de amenazas

4.2.2 Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información de lo que está siendo transmitido. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

4.2.3 Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad.** El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como ocurre al robar la contraseña de acceso a una cuenta.
- **Reactuación.** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta.
- **Modificación de mensajes.** Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de euros en la cuenta A” podría ser modificado para decir “Ingresa un millón de euros en la cuenta B”.

- **Degradación fraudulenta del servicio.** Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios (mensajes basura). Entre estos ataques se encuentran los de denegación de servicio. La denegación de servicio consiste en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

4.2.4 Tipos de ataques

En la tabla 4-1, puede ver una tabla resumen de los ataques más usuales:

Tabla 4-1. Tipos de ataques

Nombre	Descripción
Sistemas	
Explotar bugs del software	Utilizar fallos de seguridad en el software para atacar un sistema.
Romper contraseñas	Fuerza bruta o ataques basados en diccionarios que permiten obtener las contraseñas del sistema o de un determinado servicio.
Red	
Barridos de ping	Utilización del protocolo ICMP para determinar los equipos activos de una red.
Confianza transitiva	Aprovechar la confianza UNIX entre usuarios o hosts para tomar sus privilegios.
DNS spoofing	Falsificación de una entrada DNS que apunta a un servidor no autorizado.
DOS	Ataque de denegación de servicio (DOS) que consiste en saturar un sistema para impedir la utilización correcta del sistema.
Hijacking	Permite a un usuario robar una conexión de un usuario que ha sido autenticado en el sistema.
Man in the middle	A través del ataque ARP spoofing el atacante se sitúa en medio de la comunicación entre varios equipos para realizar otros ataques como sniffer, spoofing, phising, etc.
Mensajes de control de red o enrutamiento fuente	Se envían paquetes ICMP para hacer pasar los paquetes por un router comprometido.
Navegación anónima	No se considera directamente un ataque pero la suelen utilizar los atacantes para realizar sus fechorías. Se denomina navegación anónima cuando un usuario utiliza diferentes servidores Proxy para ocultar su dirección IP.
Phising	Ataque informático que consiste en falsificar un sitio web para poder obtener las contraseñas de sus usuarios.
Reenvío de paquetes	Retransmisión de paquetes para engañar o duplicar un mensaje (p. ej., una transferencia).

Sniffer	Programa o equipo que registra todo el tráfico de una red. Se utiliza especialmente para obtener las contraseñas de los sistemas.
Spoofing	El atacante envía paquetes con una dirección fuente incorrecta. Las respuestas se envían a la dirección falsa. Pueden usarse para: Acceder a recursos confiados sin privilegios Para DoS (Seny of Service) directo como indirecto o recursivo.
Servidores web	
Inyección SQL	Ataque que consiste en modificar las consultas SQL de un servidor web para poder realizar consultas SQL maliciosas.
LFI (Local File Inclusión)	Ataque informático que consiste en hacer que un servidor ejecute un script que está alojado en el mismo servidor.
RFI (Remote File Inclusion)	Ataque informático que consiste en hacer que un servidor ejecute un script que está alojado en una máquina remota.
XSS (Cross Site Scripting)	Consiste en engañar al servidor web para que ejecute un script malicioso en el navegador del cliente que visita una determinada página.
Aplicaciones	
Crack	Software que permite romper la protección de una aplicación comercial.
Keylogger	Software o hardware que registra todas las pulsaciones de teclado que se realizan en el sistema.
Rootkit	Software que se instala en un sistema y oculta toda la actividad de un usuario (el atacante).
Troyano	Software que se instala en el ordenador atacado que permite al atacante hacerse con el control de la máquina.
Virus	Software que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del equipo sin el permiso o el conocimiento del usuario.
Varios	
Ingeniería social	Atacante que consiste en convencer a un usuario legítimo para que facilite información (contraseñas, configuraciones, etc.).
Rubber-hosse	Utilizar soborno o tortura para obtener una determinada información.

4.3 OBTENCIÓN DE INFORMACIÓN DE UN ATACANTE

Es importante conocer la metodología que sigue un atacante para poder defendernos mejor de él. La expresión “conoce a tu enemigo” es válida también en el mundo de la informática.

El primer paso que realiza un atacante es la exploración. En la exploración, el atacante obtiene una lista de direcciones IP y de red utilizando descargas de transferencias de zona y consultas whois (en la figura 4-2, puede ver un ejemplo de consulta whois). Estas técnicas proporcionan información valiosa a los atacantes, incluyendo nombres de empleados, números de teléfono, rangos de direcciones IP, servidores DNS, etc.

Figura 4-2. Consulta whois

Uno de los pasos básicos de exploración de una red para determinar qué sistemas están activos, es llevar a cabo un barrido de ping automatizado en un rango de direcciones IP y de bloques de red. *Ping* se utiliza tradicionalmente para enviar paquetes *ICMP ECHO* a un sistema destino, en un intento de obtener un *ICMP ECHO_REPLY* que indica que el sistema destino está activo (vivo). Aunque enviar un *ping* resulta un método aceptable para determinar el número de sistemas activos en una red pequeña o de tamaño medio, no es eficiente en redes corporativas de mayor tamaño. Para llevar a cabo exploraciones de redes de clase A es necesario varias horas.

En la figura 4-3 se puede ver cómo el comando *ping –sP 192.168.0.0/24* permite detectar los equipos activos.

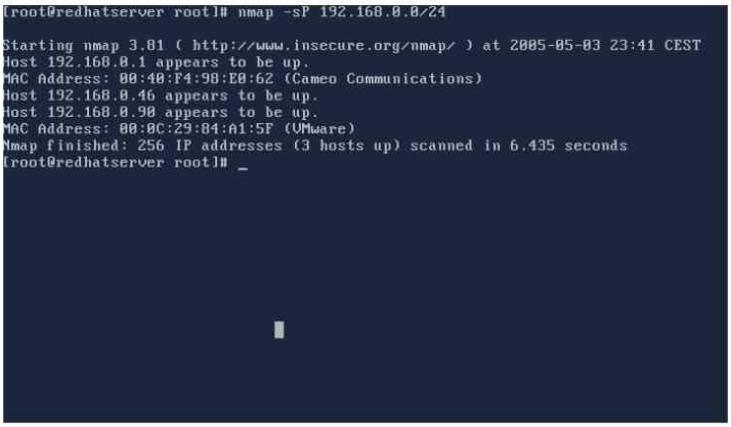


Figura 4-3. nmap –sP 192.168.0.1/24

Una vez identificados los sistemas que están activos mediante el uso de barridos *ping*, el siguiente paso que realiza un atacante es la exploración de puertos.

La exploración de puertos es el proceso de conexión a puertos UDP y TCP del sistema destino que nos permite determinar los servicios que se están ejecutando. Identificar los puertos que están a la escucha es crítico para determinar el tipo de sistema operativo y aplicaciones que se están utilizando. Los servicios activos que estén a la escucha pueden permitir que un usuario no autorizado tenga acceso a sistemas que no estén bien configurados o que ejecuten una versión de software que tenga vulnerabilidades de seguridad conocidas. Los objetivos que se persiguen con la exploración de puertos son los siguientes:

- Identificar los servicios TCP y UDP que se están ejecutando en el sistema.
- Identificar el tipo de sistema operativo instalado en el sistema.
- Identificar las versiones o aplicaciones específicas de un determinado servicio.
- Identificar las vulnerabilidades del sistema.

En la figura 4-4 se puede ver el esquema general del proceso de obtención de información por parte de un atacante.

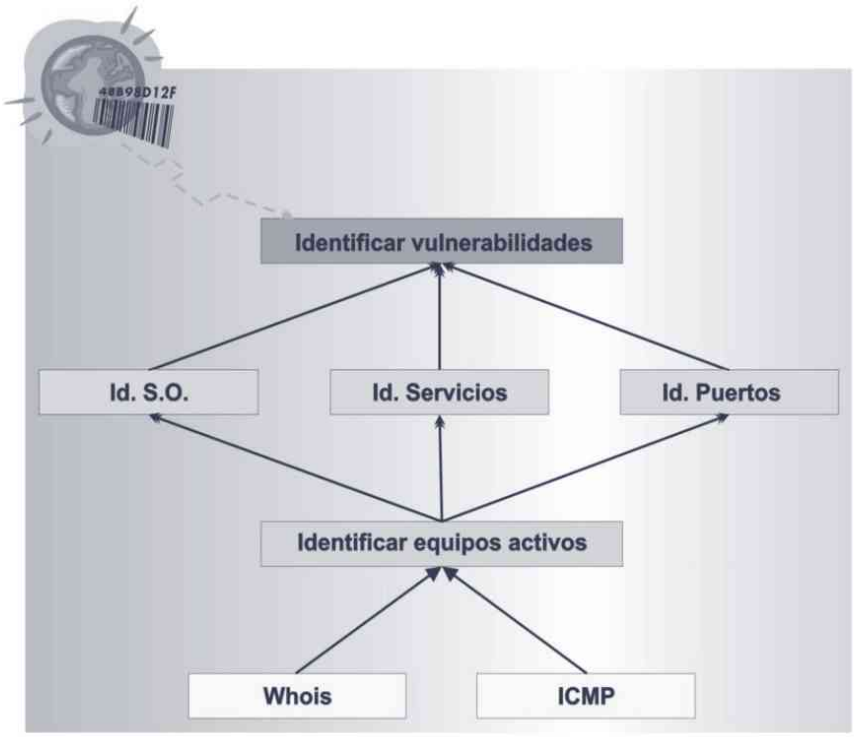


Figura 4-4. Esquema general del proceso de obtención de información

Los sistemas operativos son configurables, y por tanto pueden engañar a un posible atacante con información incorrecta. Cuestiónese las siguientes preguntas:

- ¿Qué pasaría si identificásemos servicios de forma incorrecta? Por ejemplo, identificamos un servidor de correo qmail en una máquina con Exchange.
- ¿Qué pasaría si identificamos mal el sistema operativo?
- ¿Qué pasaría si los equipos activos realmente no existen?

Un atacante obtiene las vulnerabilidades del sistema a partir de la información de los servicios y servidores. Por tanto, si esta información es incorrecta, el atacante, que se encuentra engañado, jamás va a realizar con éxito su ataque. Es imposible utilizar los fallos de seguridad en el servidor de correo de Windows (p. ej., *Exchange*) en el sistema de correo de Linux (p. ej., *qmail*).

4.3.1 Identificar los servicios TCP y UDP

La exploración de puertos permite identificar los puertos TCP y UDP que un equipo remoto tiene abiertos. De esta forma, si un equipo tiene abierto el puerto 80 entonces el equipo tiene un servidor web.

Utilizar una buena herramienta de exploración de puertos resulta crítica durante el proceso de rastreo. Existen muchos escaneadores de puertos disponibles tanto para Unix como para Windows. En Windows un ejemplo lo puede encontrar en la herramienta *SuperScan* (figura 4-5) y la todopoderosa herramienta *nmap* en GNU/Linux (figura 4-6).

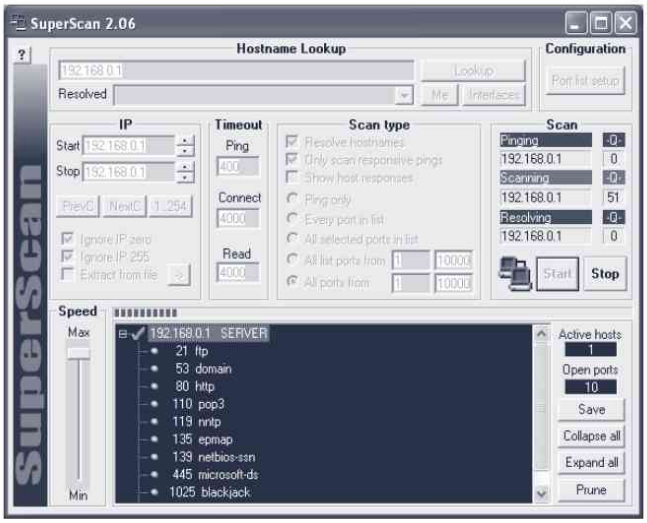


Figura 4-5. SuperScan

Figura 4-6. nmap

4.3.2 Identificar el sistema operativo

El primer objetivo de la exploración de puertos es identificar los puertos TCP y UDP que están a la escucha en el sistema destino. Nuestro segundo objetivo es determinar el tipo de sistema operativo instalado. Para poder determinar el sistema operativo de un equipo es necesario utilizar herramientas de rastreo de pilas.

El rastreo de pilas es una técnica extremadamente potente que nos permite averiguar rápidamente, y con gran probabilidad de acierto, cuál es el sistema operativo instalado en el host. En esencia, existen muchos matices que diferencian el desarrollo de pilas IP de los distintos fabricantes. A la hora de implementar el protocolo TCP/IP cada fabricante suele interpretar a su manera la normativa RFC específica. Por tanto, mediante la detección de estas pequeñas diferencias podemos realizar suposiciones razonables de cuál es el sistema operativo que se está utilizando. Para obtener la máxima fiabilidad, el rastreo de pilas necesitará que al menos un puerto esté a la escucha.

Existen varias herramientas de Linux que nos permiten detectar el sistema operativo de un equipo remoto: *xprobe 2* (*http://www.sys-security.com*) y Nmap (*http://www.insecure.org/nmap*). En la figura 4-7 puede ver un ejemplo de utilización de *nmap* para detectar el sistema operativo de un router SonicWall.

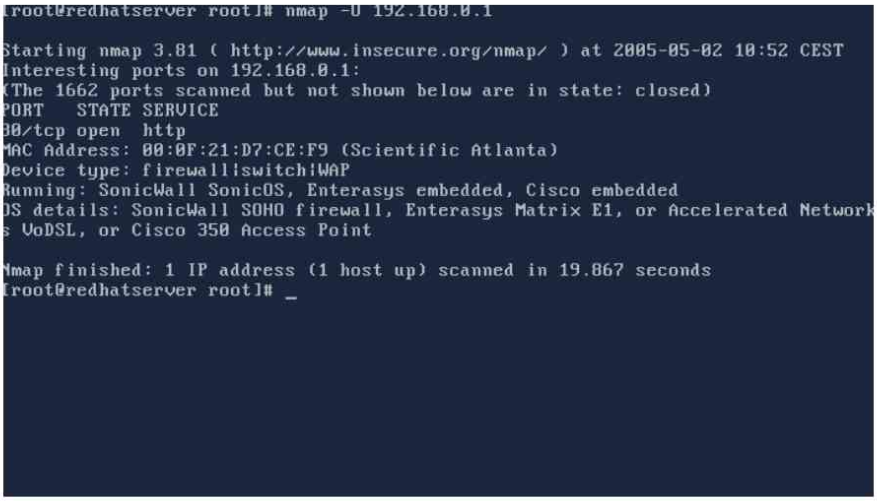


Figura 4-7. nmap –O 192.168.0.1

4.3.3 Identificar las versiones de los servicios

También puede utilizar el escaneado de puertos para identificar las versiones de los servicios de un equipo. Una vez que un atacante detecta la versión de un servicio, utiliza dicha información para utilizar las vulnerabilidades de dicho servicio.

La aplicación *amap* de Linux (*http://www.thc.org/releases.php*) permite averiguar qué aplicación está corriendo en un puerto determinado. En la figura 4-8, puede ver cómo la aplicación *amap* ha detectado correctamente que el servidor web instalado en el equipo 192.168.0.1 es Internet Information Server 5.0.

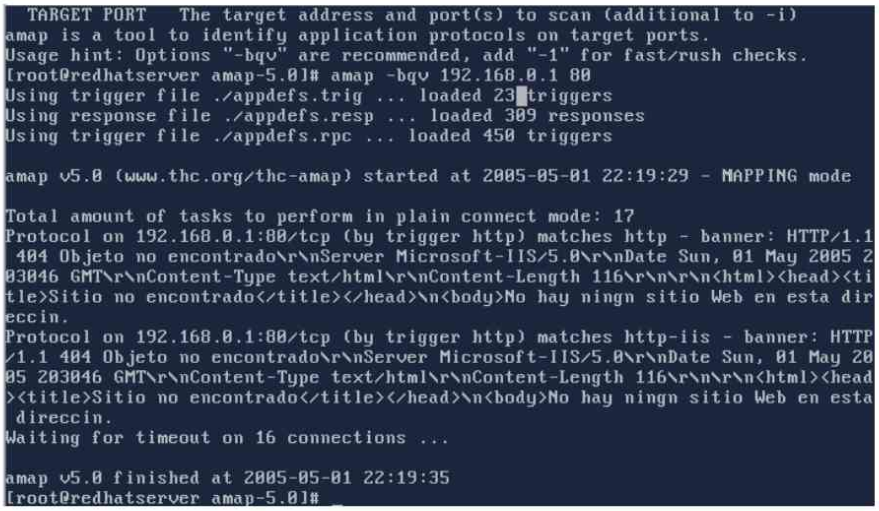


Figura 4-8. amap

Otra forma de obtener la versión de los servicios es utilizando el comando *nmap* de la siguiente forma:

```
# nmap -A <IP>
```

4.3.4 Escaneo de vulnerabilidades

Una vez que un atacante ha detectado los equipos que hay activos en una red, el sistema operativo de cada equipo y hasta el tipo de servidor que tiene instalado, lo único que queda es detectar las vulnerabilidades del sistema.

Existen dos formas de buscar las vulnerabilidades del sistema: consultar páginas web o listas de distribución de seguridad; o a través de herramientas que automatizan la búsqueda de vulnerabilidades. Entre las páginas web más conocidas podemos destacar *http://www.cert.org* y *www.webzcan.com/Vulns/pVuln.htm*.

Para buscar vulnerabilidades en un sistema puede utilizar las aplicaciones: *MBSA*, *GFILanGuard* y *Nessus*. Mientras que las dos primeras herramientas están orientadas a sistemas Windows, *nessus* permite analizar sistemas Windows y Linux.

Una vez detectadas las vulnerabilidades del sistema, para aprovecharlas un atacante puede buscar información sobre exploits o de alguna vulnerabilidad a través de la página *http://www.packetstormsecurity.org* (figura 4-9) o *http://www.exploit-db.com/*. Otra forma de atacar un sistema es utilizar la herramienta *metasploit http://www.metasploit.com* (véase la figura 4-10) que a través de una interfaz web permite aprovechar las vulnerabilidades del sistema.

Figura 4-9. http://www.packetstormsecurity.org/

Figura 4-10. http://www.metasploit.com

A continuación vamos a ver las herramientas más importantes que permiten detectar vulnerabilidades del sistema:

4.3.4.1 Microsoft Baseline Security Analizer (MBSA)

Microsoft Baseline Security Analizer (MBSA) permite comprobar las actualizaciones y vulnerabilidades del sistema en equipos basados en Windows. En la figura 4-12, puede ver un ejemplo de utilización de MBSA.

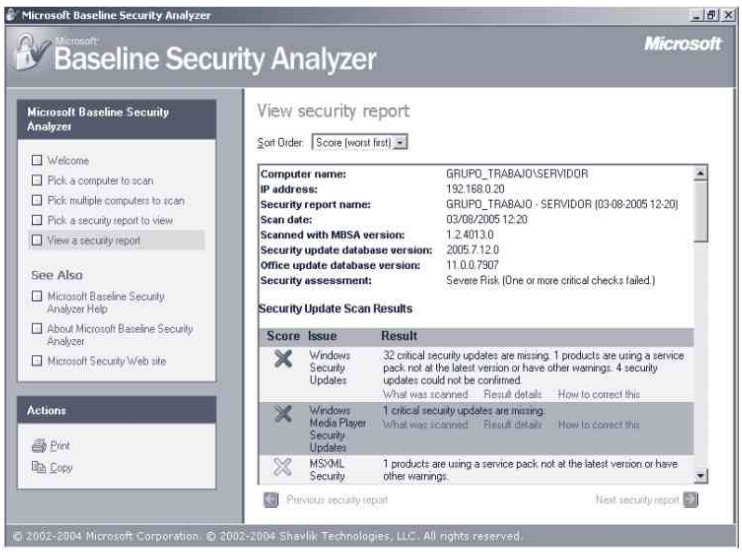


Figura 4-11. MBSA (Microsoft Baseline Security Analyzer)

4.3.4.2 GFI Languard

Si el equipo a analizar tiene habilitado "*Compartir archivos e impresoras de Microsoft*" utilice la herramienta *GFI LANguard* (véase la figura 4-13). *GFI LANguard* es una herramienta que proporciona todo tipo de información del sistema: actualizaciones instaladas, usuarios, grupos de usuarios, etc.

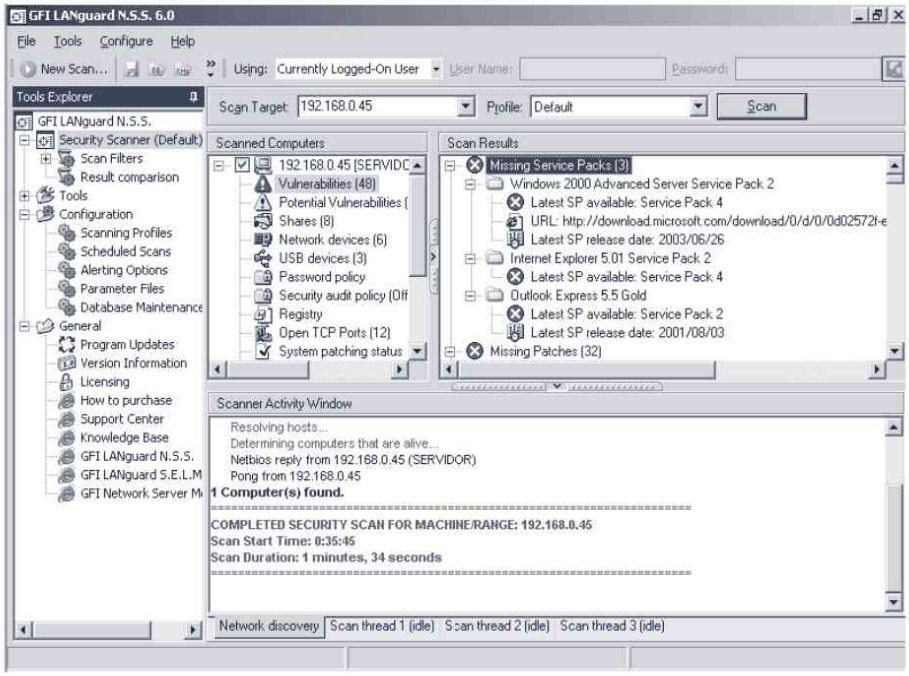


Figura 4-12. GFI LANguard

4.3.4.3 Retina Network Security Scanner

Retina es uno de los mejores escaneadores de vulnerabilidades que existe en el mercado para usar en sistemas Windows. El equipo que ha desarrollado el proyecto *Eye Digital Security* se caracteriza por un gran trabajo en el conocimiento de problemas de seguridad y la actualización en la base de datos retina es casi continua.

Retina es un software comercial de ámbito profesional que permite tanto a administradores como hackers obtener información muy detallada sobre las vulnerabilidades de un equipo. La aplicación está diseñada para que el usuario no tenga problemas en su uso. Además incorpora un sistema de generación de formularios que permite realizar informes de seguridad con un alto nivel de detalle.

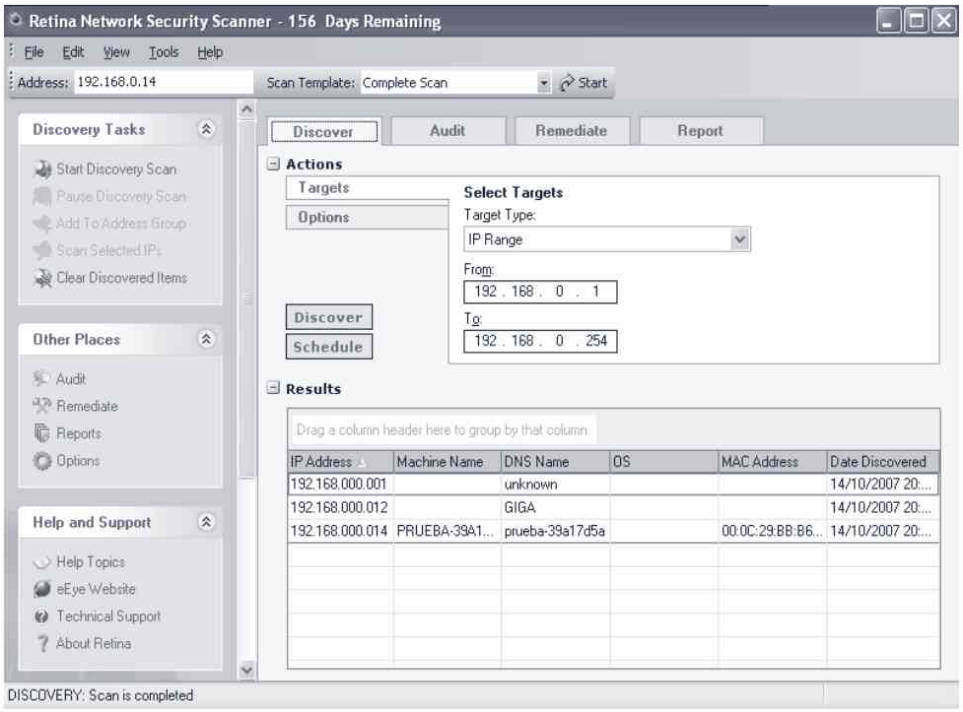


Figura 4-13. Retina

4.3.4.4 Shadow Security Scanner

Esta famosa herramienta comenzó en sus inicios como una utilidad hacker y debido a la creciente necesidad informática de tener implementaciones seguras en las empresas, se fue desarrollando un sistema gráfico muy amigable que alberga diversas opciones de configuración que hacen de esta utilidad una opción muy aceptable. La empresa creadora del proyecto *Safety-Lab* (*http://www.safety-lab.com*) actualiza frecuentemente la base de datos de vulnerabilidades del programa.

Existen varios tipos de escaneos de vulnerabilidades que se pueden personalizar mediante reglas ya establecidas o creadas por el usuario. Estas reglas están formadas por módulos que clasifican un conjunto de bugs que afectan a un software o servicio específico. Antes de analizar la seguridad de un equipo, hay que configurar una regla con los módulos que más se acerquen al perfil de la víctima; esto es crucial ya que hacer escaneos a modo completo suele ser contraproducente en términos de pérdida de tiempo y problemas con cortafuegos. Un ejemplo muy sencillo es que si tiene un sistema web con IIS entonces es inútil probar los fallos de seguridad propios del servidor Apache en GNU/Linux.

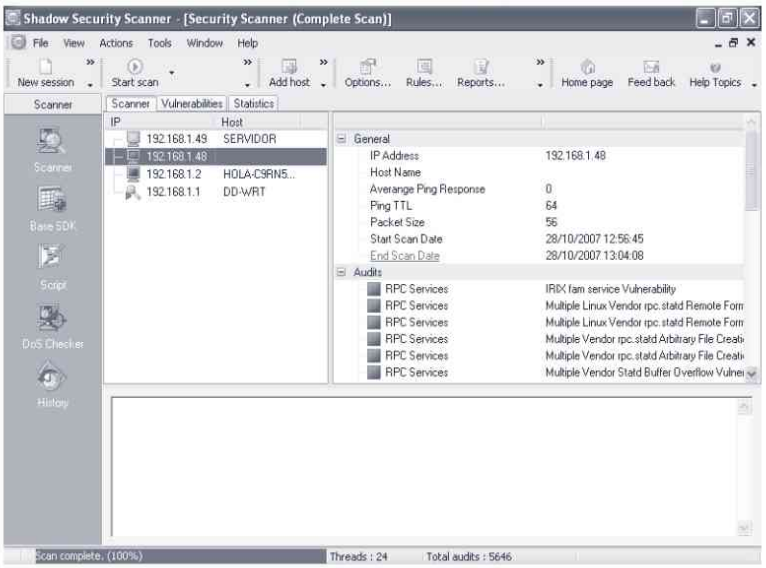


Figura 4-14. Shadow Security Scanner

4.3.4.5 Nessus

Nessus Security Scanner (*http://www.nessus.org/nessus/*) es una herramienta licenciada bajo GPL que permite detectar las vulnerabilidades de un sistema. La principal característica de esta herramienta es que se basa en un modelo cliente/servidor, lo que permite tener el servidor desde el que se realiza el escaneo y desde el cliente conectarse al servidor para iniciar un escaneo, ver informes, etc.

Nessus va incorporado en muchas distribuciones LiveCD como es el caso de Backtrack. Para utilizar Nessus tan solo tendrá que escribir en el navegador *http://localhost:8834* y empezar a realizar el escaneo de vulnerabilidades.

Figura 4-15. Nessus

4.4 MEDIDAS DE SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS

Muchas veces se comete el error de pensar que la seguridad consiste, básicamente, en evitar las intrusiones en nuestro sistema. Sin duda alguna, como dice el dicho, "más vale prevenir que curar", pero además se debe tener en cuenta otros factores que ayudan a mejorar la seguridad: detectar cuándo se produce una intrusión, poder restaurar nuestro sistema y poder identificar las acciones que ha realizado un intruso. Según esto, también se puede definir la seguridad de un sistema informático como los mecanismos de prevención, detección, restauración y análisis que se lleven a cabo para garantizar la seguridad del sistema.

- **Prevención.** En esta etapa se toman las acciones necesarias para prevenir una posible intrusión. Estas acciones se pueden realizar tanto a nivel de software (actualización del sistema), a nivel hardware (p. ej., asegurar físicamente nuestro servidor) o de red (p. ej., filtrado de puertos).

- **Detección.** Si por desgracia se produce una intrusión en el sistema, es recomendable detectar el momento en que se produce, y tomar las medidas necesarias para que no pueda dañar nuestro sistema (filtrar puertos, apagar el equipo, etc.).

- **Restauración.** Una vez que nuestro sistema ha sido atacado, entonces será necesario restaurarlo con las copias de seguridad realizadas anteriormente.

- Y por último, el **análisis forense** nos permite determinar las acciones que ha realizado nuestro atacante: desde ver qué agujeros de seguridad ha utilizado para entrar en nuestro equipo, hasta ver las acciones que ha realizado en nuestro sistema. De esta forma podemos asegurar nuestro sistema ante posibles ataques futuros.

Tal y como puede verse en la figura 4-16, la etapa de prevención se realiza antes de que se produzca un ataque, la etapa de detección durante el ataque y las etapas de recuperación y análisis forense se realizan después del ataque.

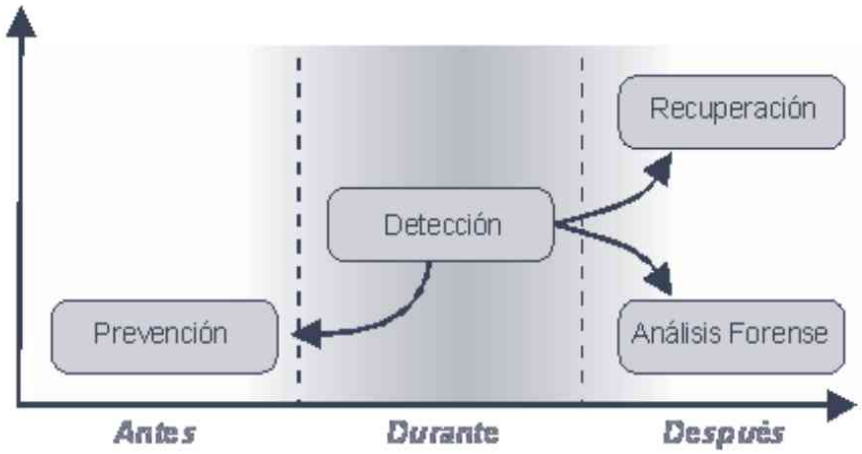


Figura 4-16. Distribución temporal de las etapas de la seguridad de un sistema

4.4.1 Prevención

Los mecanismos de seguridad preventivos son todas aquellas acciones que van encaminadas a prevenir cualquier amenaza a la confidencialidad, integridad, no repudio y disponibilidad de los elementos críticos del sistema. Por la propia definición de estas características, también se debe proporcionar mecanismos de autenticación y de control de acceso que garanticen la identificación, autenticación y gestión de perfiles aplicables a los recursos para determinar qué usuario y bajo qué condiciones pueden o no acceder al recurso solicitado para la acción indicada.

Para garantizar la seguridad de un sistema informático hay que centrarse en tres pilares básicos:

- **Seguridad física.** Es la encargada de asegurar físicamente los equipos y el cableado ante cualquier amenaza física (p. ej., rotura, robo, caída de alimentación del sistema).
- **Seguridad lógica.** Es la encargada de garantizar que los servicios y sistemas operativos funcionan correctamente y no tienen ningún fallo de seguridad que pueda ser utilizado por un atacante.
- **Seguridad de red.** Permite configurar correctamente la red para garantizar que las comunicaciones se realizan correctamente y de limitar el impacto de un ataque. Además, dentro de esta categoría también se engloba la **seguridad de las comunicaciones** que permite asegurar las comunicaciones para que no sean monitorizadas o modificadas.

A continuación se van a analizar cada uno de los elementos de seguridad.

4.4.1.1 Seguridad física

El equipamiento hardware de un sistema informático es, probablemente, la parte más cara, aunque, por el contrario, la más fácil de reemplazar. Sin embargo, existen unas pautas generales, muchas de ellas dictadas por el sentido común, que pueden ayudar a prevenir problemas con el hardware del sistema y de la red de comunicaciones.

Las principales amenazas contra el hardware son las personas, intencionadamente o no pueden dañar el sistema, las catástrofes naturales como inundaciones, terremotos…, y campos electromagnéticos no controlados.

Desde el punto de vista de la prevención, es altamente recomendable aislar los elementos hardware en recintos cerrados y protegido su acceso mediante cualquier mecanismo. Dependiendo de la importancia de la organización y su sistema a proteger puede ir desde una simple puerta con llave hasta los más modernos controles de acceso mediante reconocimiento de huella dactilar u ocular, que impida el acceso a personal no autorizado. En el caso de las instalaciones de redes de computadores, el cableado debe distribuirse mediante elementos que impidan el acceso de cualquier usuario a ellos que, por la simple alteración del campo electromagnético del cable, con la herramienta apropiada, puede detectarse la información que se transmite y afectar a la confidencialidad de las transmisiones.

Además, situar los equipos en el suelo del recinto puede ser problemático ya que en caso de inundación del recinto, el agua puede afectar a la integridad física del hardware. Por el contrario, situarlos en altura también puede ser un problema si no está suficientemente anclado para impedir, ante eventuales movimientos o golpes fortuitos, que caiga al suelo.

Además, desde el punto de vista de la integridad y la disponibilidad del hardware, se debe tener en cuenta las condiciones de la electricidad. Cualquier pico de tensión que llegue al sistema puede afectar a su integridad, por lo que se debería proteger. Por el contrario, las caídas de tensión afectan a la disponibilidad del hardware –se apaga, con la posible pérdida de información y disponibilidad que puede acarrear–.

Para manejar las fluctuaciones de la corriente eléctrica, el principal mecanismo aplicable sería la instalación de un Sistema de Alimentación Ininterrumpida (SAI) que, ante bajadas de tensión, son capaces de proporcionar corriente eléctrica a los equipos durante un tiempo determinado.

Por último, otro aspecto a considerar dentro de la seguridad física de los sistemas es la temperatura ambiente de los recintos donde se sitúan. Es recomendable, para el correcto funcionamiento y mantenimiento que se disponga de equipos de aire acondicionado independientes del resto para las salas con servidores y hardware de red que mantengan una temperatura estable en torno a los

20º. En este caso, debemos tener mucho cuidado de situar los equipos en el entorno de influencia de las máquinas internas del aire acondicionado para impedir que cualquier escape de agua que puedan sufrir, afecte al equipamiento informático.

En el caso de redes de computadores y, también para los servidores, se debe tener especial precaución con la situación del hardware o paso de cables por entornos con alto ruido electromagnético que puede afectar a los sistemas y comunicaciones. Lo mejor es evitarlos, pero si es imposible, debe de aislarse los distintos elementos afectados.

4.4.1.2 Seguridad en los equipos

Una vez que físicamente el equipo está protegido, el siguiente aspecto que hay que tener en cuenta es la seguridad lógica del sistema y de los servicios que ofrece.

Para proteger los equipos es muy importante tener en cuenta todos los aspectos relativos a la seguridad de nuestro sistema (servicios, configuración de red, sistema de ficheros, cuentas de usuario y sistema operativo) y no dejar ninguna brecha de seguridad que pueda ser utilizada por un atacante.

Una vez instalado el sistema operativo, es importante asegurarlo para trabajar con un sistema "limpio" de intrusos. Para ello, puede realizar una serie de directivas que le permiten garantizar la seguridad de su equipo. Algunas de las medidas se realizan de forma puntual y otras se deben efectuar continuamente.

De forma periódica debe desarrollar las siguientes tareas:

- **Actualizar las aplicaciones y servidores.** Para ello, puede utilizar una lista de distribución de seguridad (p. ej., *http://www.hispasec.com*) o consultar la web del fabricante.
- **Bloquear los ficheros de configuración.** Marque los ficheros de configuración del sistema como inalterables. Por ejemplo, en Linux utilice el comando *chattr*.
- **Comprobar la integridad del sistema de ficheros.** Utilice aplicaciones que le permitan verificar la integridad de la información almacenada en los sistemas de ficheros. Para detectar cualquier cambio en el sistema de ficheros, el programa ejecuta varios checksums de todos los binarios importantes y ficheros de configuración, y los compara con una base de datos con valores de referencia aceptados como válidos.
- **Comprobar la integridad de las contraseñas.** Utilice programas de fuerza bruta para comprobar la fortaleza de las contraseñas (p. ej., *John the Ripper*).

- **Comprobar la seguridad del sistema.** Utilice programas que le permitan detectar las vulnerabilidades de su sistema (p. ej., *nessus*).
- **Comunicaciones.** Para prevenir cualquier ataque lo mejor es activar el firewall del sistema para cerrar todos los puertos del servidor y abrir únicamente los extrictamente necesarios. Además, para los servicios potencialmente peligrosos se limitará su acceso por dirección IP. Por ejemplo, si es necesario utilizar un servidor ftp interno entonces se restringirá su acceso únicamente a la red interna de la empresa o incluso a un determinado equipo.
- **Usuarios.** Es muy importante tener una política correcta en la administración de los usuarios para garantizar la seguridad del sistema. Los aspectos que hay que tener en cuenta son: establecer una política de seguridad para las contraseñas (longitud, caducidad,..), limitar el uso de las cuentas con privilegios, establecer correctamente los permisos de acceso a los recursos del sistema; registrar el acceso al sistema y a los recursos.
- **Servicios.** Es muy importante que el servidor ofrezca únicamente los servicios extrictamente necesarios. Para ello, lo mejor es instalar en el servidor únicamente los servicios que va a ofrecer el servidor (p. ej., servidor web) y configurarlos correctamente.
- **Antivirus.** En los sistemas Windows es muy importante utilizar un antivirus correctamente actualizado. Además de utilizar un antivirus en los equipos o servidores, también es posible instalar un antivirus en el servidor que actúe como router para que automáticamente elimine cualquier virus o tráfico span.
- **Ficheros de registro.** Los ficheros de registro del sistema guardan información de la actividad del sistema. Es totalmente necesario examinar los ficheros de registros para determinar qué ha ocurrido en el sistema cuando se ha producido un determinado error. Además, es necesario examinar de forma periódica los ficheros de registro del sistema para ver que el sistema está funcionando correctamente.

4.4.1.3 Seguridad perimetral

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 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 uno 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.

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 4-18). 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.

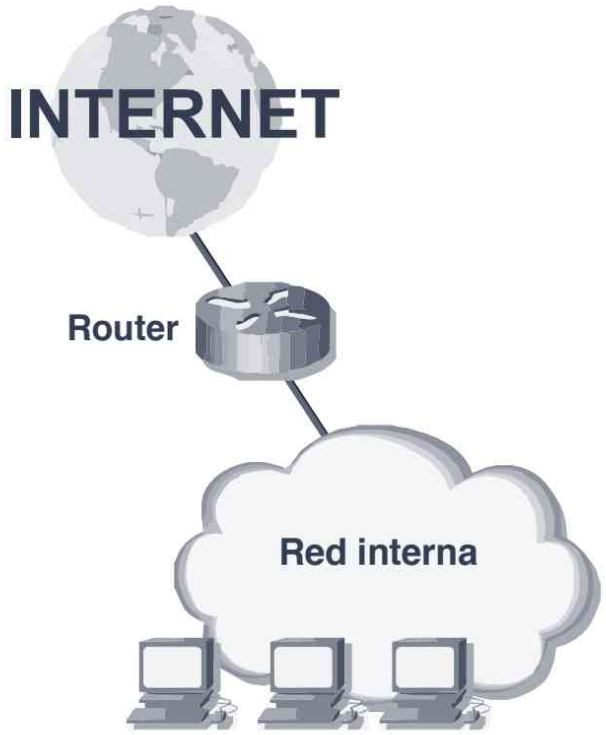


Figura 4-17. Arquitectura de router de selección

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 demilitarizada.*

Esquema de red con una zona neutra

Este 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 4-19 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.

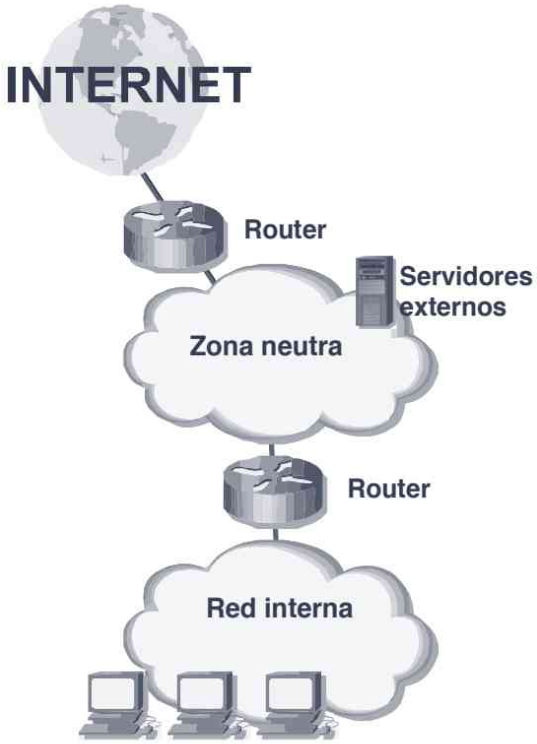


Figura 4-18. Esquema de red con una zona neutra y una red interna

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 esté 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 4-19) puede realizar las modificaciones que estime oportunas para adaptarlo a sus necesidades. A continuación, a modo de 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 4-20). 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.

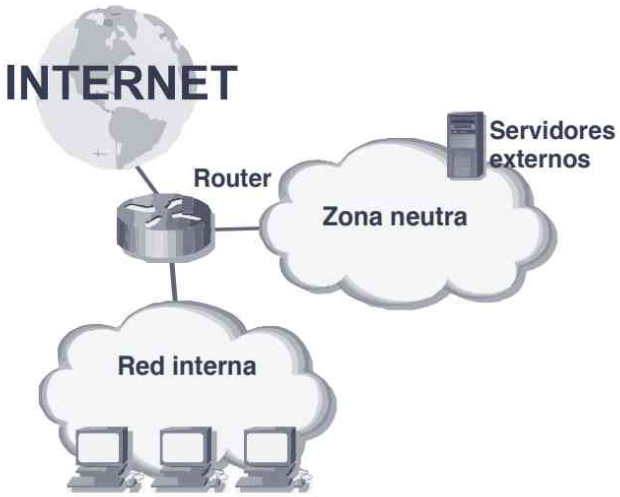


Figura 4-19. Esquema de red con una zona neutra y una red interna utilizando un único router

- **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 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 4-21 se puede ver un esquema de red que tiene dos redes internas.

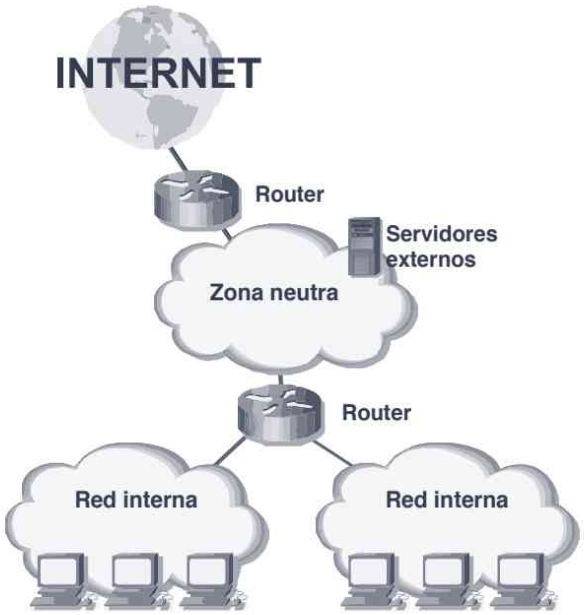


Figura 4-20. Esquema de red con una zona neutra y una red interna utilizando un único router

- **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 4-22 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. ej., 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.

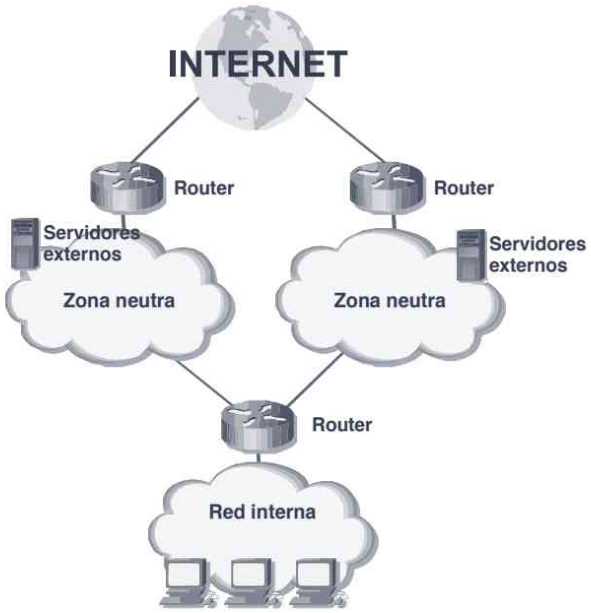


Figura 4-21. Esquema de red con dos zonas neutras y una red interna

4.4.2 Detección: sistemas de detección de intrusos

Actualmente, la estrategia de control de intrusos más utilizada es la seguridad perimetral, basada en la utilización de cortafuegos. Pero los cortafuegos proporcionan una eficaz primera línea de defensa frente a amenazas externas. Una mala configuración del cortafuegos (p. ej., errores en su software, hardware, pobre política de seguridad) pueden volver completamente inútil el mejor de los cortafuegos. Por ello se vuelve necesaria la utilización de Sistemas de Detección de Intrusos (*Intrusión Detection System, IDS*) que vigila la red en busca de comportamientos sospechosos.

Los sistemas de detección de intrusos permiten detectar actividad inadecuada, incorrecta o anómala dentro de la red. Por tanto, en su sentido más

amplio, un buen IDS será capaz de detectar las acciones de atacantes externos (intrusiones propiamente dichas), así como la actividad anormal de los atacantes internos dentro de la red.

Uno podría preguntarse ¿para qué necesitamos un IDS si ya tengo un cortafuegos? ¿No bloquea éste todos los ataques? Un cortafuegos bien configurado bloquea el acceso por puertos y protocolos excepto a unos cuantos especificados por el administrador, en los cuales se desea ofrecer ciertos servicios, como por ejemplo el servicio web en el puerto TCP 80. Esto significa que se permitirá la entrada de tráfico dirigido a esos puertos, dándolo por bueno.

El primer problema reside en la capacidad de atacar un servidor a través de puertos permitidos. Por ejemplo, el gusano *Nimda* se propagó por un agujero de IIS en servidores Windows 2000, enviando comandos para su ejecución en el servidor ¡a través del puerto 80! Por tanto, estaba permitido su paso a través del cortafuegos. Un IDS se habría dado cuenta de que algo estaba ocurriendo.

El segundo problema radica en que, normalmente, las reglas del cortafuegos bloquean el tráfico de entrada, pero no el de salida. Precisamente, *Nimda* establece sesiones de TFTP desde dentro de la red protegida por el cortafuegos hacia fuera, burlando la protección de éste.

Un buen IDS responde eficientemente ante ataques internos y ataques externos a través de las rutas legítimas que explotan reglas permitidas por el cortafuegos.

Ahora bien, ¿qué se entiende por actividad anómala? O, ¿qué se considera como intrusión? Aunque la definición de intrusión puede variar en función del IDS utilizado, en general se consideran intrusiones las siguientes actividades:

- **Reconocimiento.** Los intrusos suelen explorar una red antes de intentar atacarla utilizando técnicas como barridos de *ping*, exploración de puertos TCP y UDP, identificación del SO, intentos de inicio de sesión, etc. Mientras que un cortafuegos puede limitarse a bloquear esos sondeos, el IDS hará saltar una alarma.

- **Explotación.** Una vez que en la fase de reconocimiento se ha identificado el objetivo a atacar, el intruso intenta utilizar “agujeros” del sistema (p. ej., fallos en servicios web, en los navegadores de los usuarios). Muchos de estos ataques pasarán completamente desapercibidos en el cortafuegos, mientras que un buen IDS alertará de ellos

- **Denegación de servicio.** El ataque de denegación de servicio consiste en el uso masivo de un recurso o servicio de forma que se degrade el correcto funcionamiento del sistema. Por ejemplo, es posible realizar un ataque distribuido de forma que cientos o miles de equipos le soliciten una página a un servidor web. De esta forma, al recibir el servidor un número masivo de peticiones éste no puede procesarlas (o lo hace muy lento) de forma que los usuarios no pueden utilizar el sistema.

Tarros de miel

Un tarro de miel (honeypot) simula uno o más sistemas fáciles de atacar con el fin de tentar a potenciales intrusos. El honeypot facilita ser invadido y entonces avisa de la intrusión al administrador del sistema.

Gracias a esta estratagema, el honeypot permite proteger otras partes de la red al atraer sobre sí mismo la atención de los atacantes, quienes se concentran en este blanco aparentemente fácil, pero que no contiene información valiosa ni puede ocasionar daños.

Para que el engaño sea más completo, algunos honeypots simulan diferentes sistemas operativos, para observar a cuál de ellos se dirige el atacante.

Por último, los honeypots suelen proporcionar evidencias forenses, ya que el atacante suele dejar en ellos las huellas necesarias que permitan rastrear sus pasos.

4.4.3 Colocación de un NIDS

La colocación de un NIDS en la red se debe realizar en función del tráfico que desea vigilar: tráfico de entrada o de salida. Es posible situar el IDS de las siguientes formas:

- **Delante del firewall.** Puede detectar todos los ataques producidos, aunque muchos de ellos no se hagan efectivos. Genera gran cantidad de información en los logs.
- **Detrás del firewall.** Permite analizar todo el tráfico que entra en la red (y que sobrepasa el firewall). Monitoriza únicamente el tráfico que haya entrado realmente en la red y que no ha sido bloqueado por el firewall.
- **Delante y detrás del firewall.** El control que se ejerce es mayor. Permite efectuar una correlación entre ataques detectados en un lado y otro.
- **Firewall/NIDS.** Es posible utilizar un único equipo para que realice las funciones de firewall y de NIDS a la vez.

Físicamente, tal y como muestra la figura 4-22, es posible conectar un NIDS a la red de varias formas:

- **Switch.** Si desea que el NIDS reciba todo el tráfico de la empresa entonces tiene que utilizar un swtich que tenga un puerto replicador. La función del puerto replicador es que el switch envía todo el tráfico que pasa por el switch al puerto replicador para que lo pueda procesar el IDS.
- **Bridge.** Si lo desea puede configurar un equipo GNU/Linux para que actúe de puente (bridge) entre dos redes diferentes.

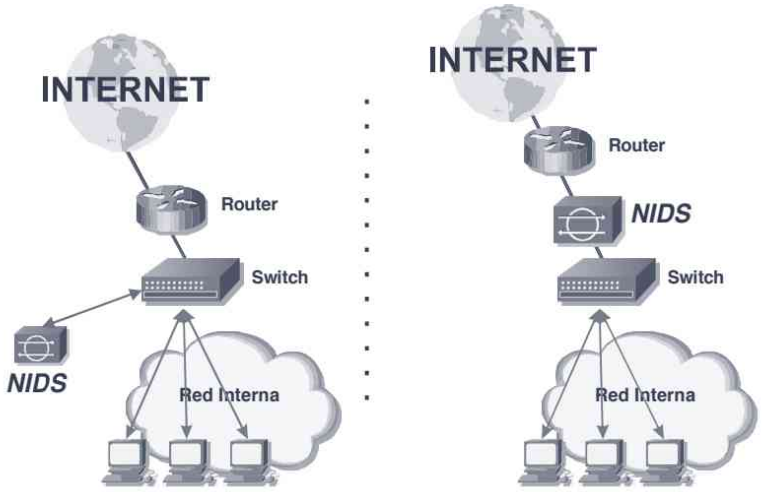


Figura 4-22. Esquemas de red de un NIDS: a) switch y b) bridge

4.4.4 Tipos de sistemas de detección de intrusos

Existen distintos tipos de IDS, atendiendo a distintas clasificaciones establecidas de acuerdo a las características que se usen para establecer dicha clasificación. Cada uno de ellos se caracteriza por diferentes aproximaciones de monitorización y análisis, y presenta distintas ventajas y desventajas.

Las clasificaciones de los IDS son las siguientes:

- **Según su enfoque.** Permite clasificar los IDS según el tratamiento que se realiza sobre los datos. Existen los IDS basados en anomalías, en detección de uso incorrecto y los híbridos.
- **Según el origen de datos.** Los IDS pueden monitorizar la red (NIDS, Network IDS), un equipo (HIDS, Host IDS) o ambos sistemas (IDS híbridos).

- **Según su estructura.** Los IDS pueden trabajar de forma individual o compartir datos con otros sistemas. De esta forma surgen los IDS con estructura centralizada o distribuida.
- **Según su comportamiento.** Se pueden clasificar los IDS según su comportamiento al detectar una intrusión. Los IDS pasivos solo alertan de una intrusión mientras que los activos (IPS o IDPS) alertan y actúan sobre la intrusión. Por ejemplo, pueden indicarle al cortafuegos que deniegue todas las comunicaciones del atacante.

En la figura 4-23, se muestran los distintos sistemas de detección de intrusos atendiendo a diferentes clasificaciones.

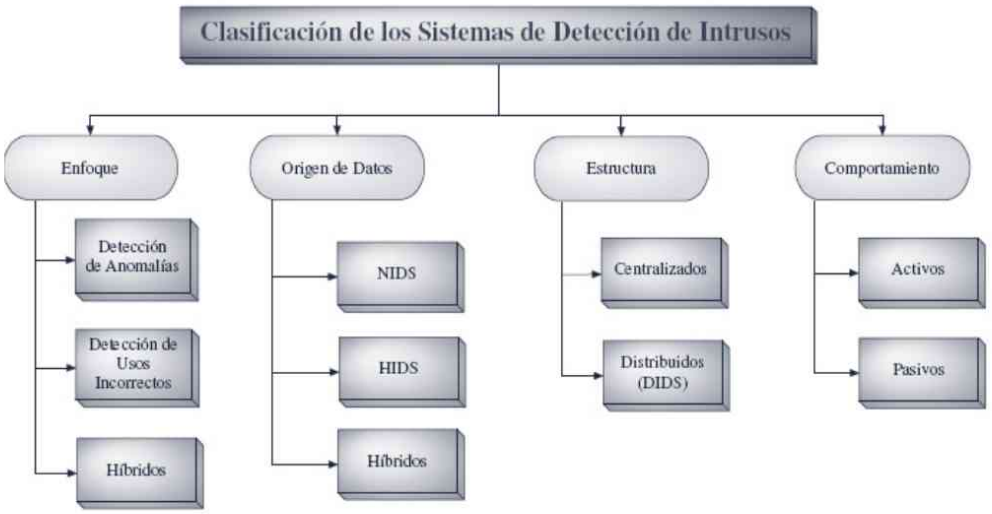


Figura 4-23. Clasificación de los IDS

A continuación vamos a analizar las clasificaciones más importantes:

4.4.4.1 Tipos de IDS en función del enfoque

Existen dos grandes tipos de sistemas de detección de intrusos: los sistemas basados en patrones (o uso indebido) o los basados en anomalías. Además de estos dos tipos existen los sistemas híbridos que surgen con la combinación de los sistemas basados en detección de anomalías y de uso incorrecto. En la figura 4-24 se muestra la estructura de los IDS basados en detección de anomalías y de uso indebido.

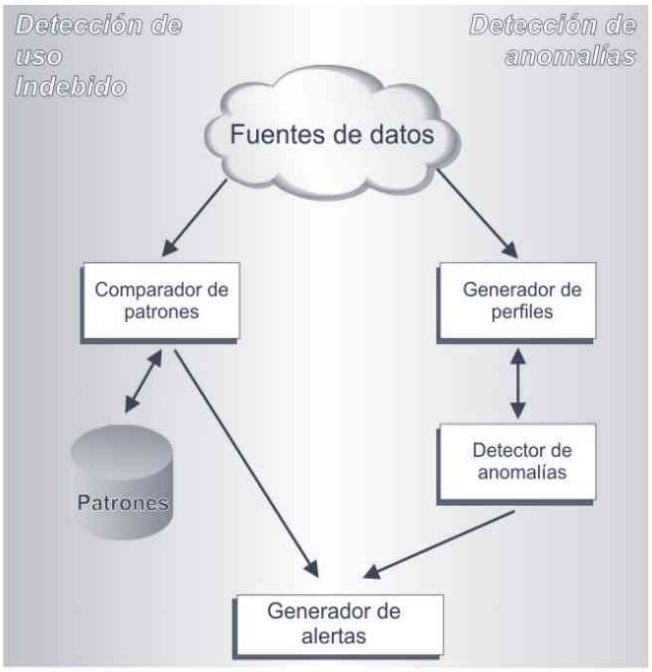


Figura 4-24. Esquema general de un IDS

Detección de anomalías

El IDS toma como referencia una idea estereotipada de lo que es el comportamiento "normal" del sistema y examina continuamente la actividad que está teniendo lugar, de manera que cualquier desviación de la norma se considera como sospechosa.

Por ejemplo, si un usuario normalmente inicia una sesión 2 veces al día, 30 inicios de sesión consecutivos pueden considerarse como sospechosos. Si un usuario nunca se conecta fuera del horario de trabajo, una conexión a las 4:00 de la mañana hará sospechar igualmente. Si un usuario nunca accede a la base de datos empresarial ni compila código fuente, puede resultar extraño que un día lo haga.

Igualmente, existen aplicaciones del sistema independientes del usuario que poseen unos patrones de uso bien definidos, por lo que si se detectan cambios en ellos, pueden indicar la acción de un atacante.

Por otro lado, si el IDS registra una sobrecarga inusual de recursos en la red, uso de disco, CPU, base de datos u otros recursos, podría indicar la realización de un ataque.

El punto fuerte de la detección de anomalías estriba en la capacidad de detectar ataques nuevos totalmente desconocidos. Dado que el IDS debe ser "inteligente", ha de tomar decisiones que pueden ser correctas o erróneas. Por tanto, el problema de los IDS basados en anomalías es que pueden equivocarse.

Detección de uso indebido

En este caso, el IDS posee unos patrones de ataques (o uso indebido) también conocidos como firmas (signatures), basadas en ataques o penetraciones pasadas. El comportamiento de este tipo de IDS se asemeja al de un antivirus ya que su objetivo consiste en buscar la presencia de estas firmas en el tráfico de la red o en las peticiones enviadas a los hosts.

El mayor inconveniente de la detección de firmas es que no permite detectar ataques novedosos y, además, necesitan ser actualizados constantemente cada vez que se descubre un nuevo tipo de ataque.

La detección de uso incorrecto suele implantarse por medio de sistemas expertos, razonamiento basado en modelos, análisis de transición de estados o redes neuronales.

4.4.4.2 Tipos de IDS en función del origen de datos

Existen dos tipos de IDS: los IDS basados en red (NIDS) y los IDS basados en host (HIDS).

NIDS

Los sistemas de detección de intrusos basados en red (NIDS) son aplicaciones que analizan todo el tráfico de la red en busca de intrusiones. Funcionan de forma muy similar a como lo hacen los sniffers. Examinan cada paquete, comprobando su contenido con una plantilla o base de datos de firmas de ataques, con el fin de detectar si el paquete examinado se corresponde con algún tipo de ataque. Las ventajas de los NIDS son:

- Se instalan en segmentos de red, por lo que con un solo NIDS puede detectar ataques en todos los equipos conectados a dicho segmento, a diferencia de los HIDS, que exigen tener que instalar uno en cada equipo.
- Resultan independientes de la plataforma utilizada por los distintos equipos de la red.
- Al examinar de forma abstracta los paquetes de tráfico que circulan por la red, son capaces de detectar ataques basados en manipulación de cabeceras IP o ataques de denegación de servicio que serían capaces de bloquear un servidor.
- Resultan invisibles para los atacantes, a diferencia de los HIDS, que siempre dejan huella en el sistema en el que se han instalado.

Sus desventajas son:

- Son ineficaces en sistemas con tráfico cifrado.
- Su funcionamiento se vuelve inviable en redes de alta velocidad impidiendo al NIDS analizar todos los paquetes a tiempo.
- Si se produce una congestión momentánea de la red, el NIDS podría empezar a perder paquetes.
- Debido a que operan en entornos heterogéneos (Windows, Linux, Sun, etc.) podrían no ser capaces de definir la relevancia de un ataque en cada plataforma.

HIDS

Los sistemas de detección de intrusos basados en host (HIDS) residen en el propio host que monitorizan, por lo que tienen acceso a información recolectada por las propias herramientas de auditoria del host (registros de actividad, accesos al sistema de ficheros, logs de registro, etc.). Las ventajas de los HIDS son:

- Detectan mejor los ataques desde dentro del equipo, ya que monitorizan inicios de sesión, cambios en ficheros, en el registro, etc.
- Son capaces de asociar usuarios y programas con sus efectos en el sistema.
- Los HIDS forman parte del propio blanco, por lo que pueden informar con gran precisión sobre el estado del blanco atacado.
- Solo se preocupan de proteger el host en el que residen sin necesitar monitorizar todo el tráfico que circula por la red, por lo que no consumen tantos recursos como el NIDS y no afectan (tanto) al rendimiento del sistema.

Las desventajas de los HIDS son:

- Su principal inconveniente es su lentitud de respuesta en comparación con los sistemas NIDS. Si se limitan a analizar los registros de actividad y cambios en el sistema de ficheros, descubren los ataques cuando ya han tenido lugar y puede ser demasiado tarde para actuar.
- Otro inconveniente es la dificultad de su implantación, ya que al estar instalados en varias máquinas diferentes es necesario el desarrollo en distintas plataformas. Como consecuencia, la mayoría de los fabricantes ofrecen HIDS para una o dos plataformas (p. ej., Solaris y Windows). No obstante, para paliar estos problemas muchos HIDS utilizan lenguajes multiplataforma como PERL o Java, aunque aún así el tipo de ficheros y registros a monitorizar sigue dependiendo de la plataforma.

- Al residir en el host, desde el momento en el que éste haya sido atacado con éxito, uno no puede confiar en sus informes, que podrían haber sido manipulados por un atacante excepcionalmente habilidoso.
- A diferencia de los NIDS, ante un ataque severo (p. ej., denegación de servicio), si el host cae, el HIDS cae con él sin generar ninguna alerta.
- Dado que un HIDS solo vigila el host en el que reside, para obtener una imagen global del estado del sistema es necesario agregar y correlacionar la información procedente de los distintos HIDS en uno o varios servidores centrales.

La figura 4-25 muestra un ejemplo de utilización de sistemas de detección de intrusos. Mientras que el HIDS instalado en el servidor web es capaz de vigilar todos los intentos de intrusiones realizados únicamente al servidor web, el NIDS que conecta las dos redes es capaz de vigilar todo el tráfico que circula entre Internet, la red privada y la zona neutra.

Al ver las ventajas y desventajas de cada sistema de detección de intrusos, se ve claramente la necesidad de instalar ambos sistemas en una red, bien sea un mismo producto el que desempeñe ambas funciones. De esta forma, se obtienen las ventajas de cada uno de ellos, a la vez que se compensan sus debilidades. La tendencia actual en los fabricantes apunta a la evolución hacia sistemas híbridos, que combinan lo mejor de ambos tipos.

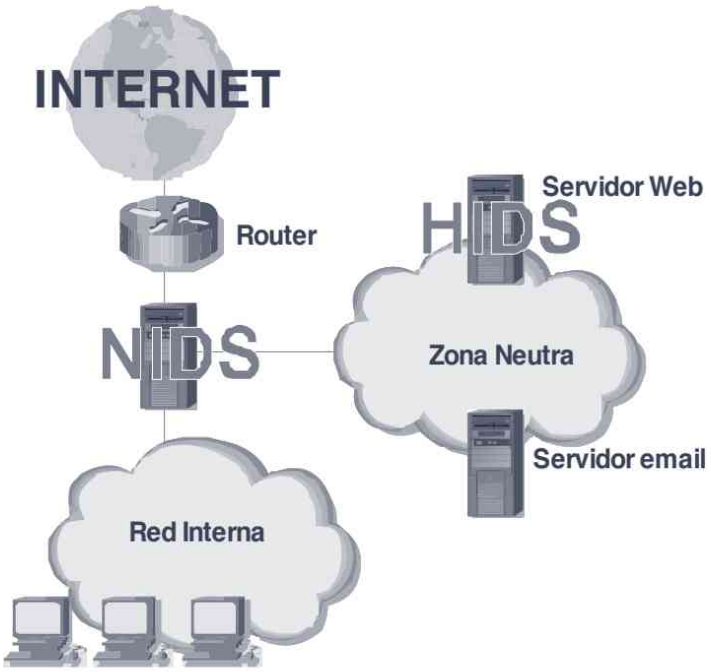


Figura 4-25. Sistemas de detección de intrusos

4.4.5 Recuperación: copias de seguridad

Los mecanismos preventivos pueden evitar muchos problemas y ataques pero no garantizan estar exentos de todo riesgo o daño. Tras detectar que la seguridad ha sido comprometida, una de las tareas del administrador del sistema afectado será recuperarlo y dejarlo tal y como estaba antes del incidente.

Lo primero que un administrador debe realizar a la hora de diseñar un sistema de copias de seguridad es planificar la estrategia a seguir para cumplir la política de seguridad de la organización. Por ejemplo, en un ambiente universitario dedicado a aulas de prácticas de informática, se puede establecer que las copias de seguridad afecten, exclusivamente a los sistemas de ficheros de los equipos de las aulas. De esta forma, ante una posible caída (situación bastante probable) se pueden recuperar los equipos en el menor tiempo posible pero se pierden los datos de los usuarios.

La finalidad de las copias de seguridad puede ser recuperar todo el sistema completo. Lo que todo administrador debe tener en cuenta es:

- **¿Qué se debe copiar?** Como se ha comentado, deberá ajustarse a lo definido en la política de seguridad de la organización.
- **¿Dónde se encuentra?** Si el sistema de copias está centralizado en un equipo, no solo debe saber el lugar del sistema de ficheros en el que se encuentran los ficheros a copiar, como ocurre en el caso de disponer de un sistema de copias local, sino que también debe conocer en qué equipos de la red se encuentran.
- **¿Quién y dónde se realizará la copia**? Se debe conocer quién asume la responsabilidad de gestionar las copias de seguridad y en qué soporte y dispositivo se realizará.
- Por último, se debe indicar **bajo qué condiciones se realizará la copia de seguridad** y con qué frecuencia para que se cubra perfectamente las necesidades de recuperación. Un sistema en el que los datos que queremos copiar cambian frecuentemente, obliga a tener copias de seguridad frecuentes para no correr el riesgo de perder información.

4.4.5.1 Tipos y estrategias de copias

La estrategia de las copias de seguridad debe definir claramente los puntos vistos anteriormente. En base a qué queremos copiar, se distinguen tres tipos de copias: completa, incremental y diferencial. Con la primera se realiza una copia completa de los sistemas de ficheros del equipo a copiar para poder recuperarlo en su totalidad. Con las copias incrementales, lo que se realiza es una copia parcial del sistema de fichero, en concreto, se copian los ficheros modificados o creados desde

la última copia que se realizó. Con las copias diferenciales, lo que se realiza es una comparación del contenido de los ficheros a la hora de determinar qué se debe copiar. Presenta todas las ventajas de las incrementales y ocupa menos espacio.

En la tabla 4-3 puede ver las principales características de las diferentes estrategias de copias de seguridad.

La copia de seguridad completa de un sistema puede, dependiendo del tamaño de sus sistemas de fichero, consumir mucho tiempo y, además, la recuperación de ficheros individuales en este tipo de copias puede también presentar inconvenientes como el tiempo de búsqueda y recuperación en el soporte de almacenamiento. Por el contrario, las copias incrementales permiten la recuperación rápida de ficheros individuales, aunque se debe disponer de un mecanismo que garantice que recuperamos la última versión del fichero.

Tabla 4-2. Características de las estrategias de copia

Estrategia	Ventajas	Inconvenientes
Completa	Se copian todos los ficheros. Fácil recuperación total y parcial del sistema.	Consumo de espacio.
Incremental	Más rápida de realizar que sucesivas copias completas. Requiere menos espacio. Permite la conservación de varias versiones de un mismo fichero.	Se pueden copiar ficheros cuyo contenido no ha cambiado. Se necesitan todos las copias incrementales para recuperar un sistema, además de la completa. La restauración de ficheros individuales consume tiempo ya que se debe buscar por las copias incrementales.
Diferencial	Todas las de la incremental. Requiere menos espacio.	Todas las de la incremental menos la primera. No todas las herramientas permiten copias diferenciales.

Por otra parte, otra clasificación, en función de qué se copia y con qué frecuencia, es la basada en niveles, donde el nivel 0 es una copia completa del sistema y el resto de niveles son copias incrementales que se basan en el nivel anterior. Es decir, las copias de nivel 1 son incrementales donde se copia todo aquello que se ha modificado o creado desde que se realizó la última copia de nivel 0; las copias de nivel 2 son aquéllas que guardan los ficheros modificados o creados desde que se realizó la última copia de nivel 1 y, así sucesivamente, todos los niveles que queramos, aunque no es recomendable más de tres niveles, siempre dependiendo del sistema a copiar y la frecuencia y número de ficheros que cambian con respecto al sistema original.

La diferencia entre realizar unas copias completas (nivel 0) o incremental (nivel 1) es la cantidad de información que se copia y, por tanto, el tiempo que lo que tardará en realizarse y, posteriormente, la posibilidad de recuperar eficientemente ficheros individuales y el sistema en su totalidad. Cuando se tiene un sistema informático en el que la información que cambia es poca y poco frecuente, parece mejor opción realizar una copia completa del sistema y, a partir de ésta, realizar copias incrementales. Por el contrario, en sistemas informáticos donde el sistemas de ficheros cambia frecuentemente, la mejor opción será la de realizar copias de seguridad completas cada noche.

Entre ambos extremos, se disponen una serie de estrategias en las que se define cuándo hacemos una copia de cada nivel que persigue optimizar las copias de seguridad que se realizan para que éstas no sean excesivas, ni consuman muchos recursos ni, por el contrario, se pierda información.

Un plan de prevención genérico, que puede adaptarse a muchas organizaciones, es aquél en el que por ejemplo:

- El primer lunes de cada mes se realiza una copia de nivel 0 del sistema.
- El resto de lunes y primer martes del mes, se realiza una copia de seguridad de nivel 1.
- El resto de días se realiza una copia de seguridad de nivel 2, en la que cada semana se toma como referencia la copia de seguridad de nivel 1 realizada el lunes de dicha semana o el martes, si coincide con inicio del mes.

Con este plan, para recuperar un sistema completo, se debe:

- Primero recuperar todos los ficheros almacenados en la copia de nivel 0 del mes actual.
- Después se debe recuperar los ficheros de la copia de nivel 1 de la semana actual.
- Para finalizar se recuperan los ficheros de la última copia de nivel 2 realizada.

Con este plan de trabajo los cambios realizados en el sistema desde que se realiza la última copia de nivel 2 hasta que al siguiente día se realiza la nueva, se pueden perder ya que no se realiza, en ese período de tiempo, ninguna copia de ficheros. Por eso, se pretende salvaguardar la información de entornos muy cambiantes, como por ejemplo los sistemas de gestión de base de datos, la mejor opción es replicar los datos en dos sistemas diferentes que garanticen la disponibilidad de la información durante el período de tiempo que transcurre entre copias. Sin embargo, esta estrategia debe ser complementaria y no sustituir las copias de seguridad propiamente dichas. Por ejemplo, cuando accidentalmente –o

no–, se borre un dato de una tabla de la base de datos, inmediatamente se borrará en la réplica, quedando solo el recurso de las copias de seguridad para recuperarlo.

4.4.5.2 Buenas costumbres

Tan importante como seguir una buena estrategia de copias de seguridad, es adquirir una serie de costumbres que permiten prevenir problemas con las copias realizadas. El simple hecho de realizar copias no garantiza que podamos recuperar información ya que, por ejemplo, puede ocurrir que las copias estén mal conservadas y fallen cuando se desee recuperar un fichero.

Lo primero que se debe tener en cuenta es que las copias se pueden realizar en muchos dispositivos, pero nunca en el mismo del cual estamos tomando los datos. Si, por ejemplo, copiamos datos de un sistema de fichero en un disco en otra partición del mismo disco, si éste se estropea, se pierde tanto los datos originales como la copia.

Para evitar errores y reutilizar un soporte con información salvaguardada en procesos anteriores que no debería modificarse, es bueno, por una parte, una correcta etiquetación de los soportes de almacenamiento, indicando de manera clara y legible de qué se trata y qué contiene –la copia de qué día–; por otra, también deberían protegerse contra escritura para eliminar la posibilidad de borrados accidentales.

Es una buena costumbre, que evitará posibles sustos y detectará errores con los soportes de almacenamiento, comprobar el estado de la copia de seguridad realizada. Además, es bueno no reutilizar eternamente las mismas cintas, CD…, y cambiarlos antes de que empiecen a dar errores, sobre todo para evitar problemas con la recuperación de la información cuando la necesitemos.

Además, no se debería almacenar las unidades del soporte utilizadas para las copias de seguridad en el mismo recinto donde están los equipos cuya información se guarda en dichas unidades. El motivo es simple: si ocurre, por ejemplo un incendio que arrasa el recinto, acaba con los equipos y con sus copias de salvaguarda. También, respecto al almacenamiento de las copias de seguridad, se debe tener en cuenta las propiedades de los medios de salvaguarda y analizar las condiciones ambientales: humedad, posibles campos electromagnéticos…

Por último, y más como medida que favorece la utilización de los recursos, es mejor realizar las copias de seguridad cuando los usuarios no están trabajando, por la noche o a la hora de la comida. Por un lado, garantizaremos la copia de las últimas versiones –si un usuario guarda un segundo después de que copiemos, si se debe recuperar la versión del día y hora, puede que no sea lo que espera–; por otro, no se compite por los recursos que podría ralentizar el sistema y producir quejas en los usuarios.

4.4.6 Técnicas de análisis forense

Debido a la creciente importancia de los sistemas de información, no solo por la repercusión social sino también por la importancia de los datos y operaciones que se realizan con sistemas informáticos, los estados han legislado los llamados "delitos informáticos". Con ello, al igual que ocurre en otros ámbitos judiciales, para aplicar las penas marcadas en la ley, es necesario la aportación de pruebas fidedignas que demuestren la culpabilidad de los acusados.

Por este motivo y, sin llegar a reclamaciones judiciales, por el interés profesional de los responsables de los sistemas en conocer qué, quién y cómo ha violado la seguridad del sistema informático, surgen las técnicas de análisis forense.

Estas técnicas, definen el conjunto de acciones encaminadas a averiguar qué ha pasado con un equipo al que se le ha comprometido la seguridad y, por otra, el procedimiento para recoger pruebas fiables y fidedignas que puedan ser usadas en procedimientos judiciales.

Los objetivos, por tanto, del análisis forense son:

- Averiguar qué ha pasado.
- Cómo se ha realizado la intrusión.
- Qué consecuencias ha tenido.
- Quién ha sido.
- Y todo ello con el procedimiento utilizado y herramientas de apoyo fuera de toda duda y respetando las leyes vigentes en materia, sobre todo, de privacidad.

4.4.6.1 Recopilación de evidencias

Cuando se ha detectado la intrusión en un sistema informático, el primer paso a tomar es el de asegurar el escenario de la intrusión para intentar conseguir el máximo número de evidencias posible. Para ello, se deberá determinar los sistemas afectados, tras lo que, para cada uno de ellos en particular, se deberá comprobar si están encendidos o apagados.

Si el equipo a analizar está encendido, un primer paso a realizar si dispone de terminal gráfico es fotografiarlo, para reflejar de forma inequívoca qué está mostrando por pantalla (por ejemplo, muchos sistemas Unix muestran en el terminal información de eventos que ocurren en el sistema) y tomar las evidencias volátiles, aquellas que se pierden tras el apagado del equipo. La información que, en este momento, se puede conseguir para su posterior análisis es:

- Conexiones abiertas y entre qué equipos y con qué interfaces de red.
- Procesos ejecutándose en memoria, ficheros abiertos y qué procesos están accediendo a ellos.
- En el caso de sistemas Linux, el contenido del sistema de ficheros /proc.
- Usuarios presentes en el sistema y qué procesos están ejecutando.
- Fecha y hora actual del sistema, fotografiándola si es necesario.
- Ficheros temporales del sistema.
- Estado de la red, con las tablas de rutas y arp.
- Tiempos de modificación, acceso y creación de los ficheros.
- Copias de los registros y caché del procesador.

Tras la recopilación de las evidencias volátiles, y antes de recopilar las evidencias no volátiles, se debería desconectar las conexiones de red, tanto de los medios guiados como no guiados, para impedir conexiones externas y, por último, apagar el equipo comprometido quitando directamente la alimentación eléctrica, para asegurar las evidencias que existan en los sistemas de ficheros montados.

Casi siempre, las evidencias no volátiles se localizan en los sistemas de ficheros por lo que se debe analizar su contenido en busca de más datos de la intrusión. Existen dos aproximaciones:

- El equipo comprometido se arranca con una distribución live-cd para analizar los sistemas de fichero afectados.
- Se conecta el sistema de ficheros afectado a otro equipo que dispone de las herramientas necesarias para su análisis.

Otra variante, y mejor opción ya que no afecta al sistema comprometido, es proporcionar una copia exacta, realizada bit a bit, de los sistemas de fichero al equipo de análisis, previo cálculo de un resumen HASH para validar la copia.

4.4.6.2 Análisis e investigación de las evidencias

En esta fase, basándose en los datos conseguidos en la fase de recuperación, un administrador debe buscar quién realizó la intrusión, qué acciones emprendió, cuándo se llevó a cabo y cómo lo logró.

Para ello, se deberá buscar correlaciones entre los datos adquiridos en la fase anterior, los logs de sistema y acciones realizadas desde el equipo comprometido y que estén registradas en su sistema de ficheros. Se deberá prestar especial atención a evidencias que pueden existir en localizaciones difíciles de

detectar como el espacio entre particiones o sectores, el espacio no asignado y los ficheros *swap*.

Los problemas que nos podemos encontrar van encaminados a cómo se han conservado los datos: pueden estar cifrados y, dependiendo del software utilizado y del algoritmo de encriptación, puede ser virtualmente imposible de romper su seguridad, que tengamos que manejar excesivos ficheros de datos o que estén corruptos.

Además, deberemos buscar signos de estenografía (proceso de ocultación de datos dentro de otros datos de un fichero) como la instalación de herramientas para aplicar estas técnicas y buscar posible información oculta en ficheros.

Para poder reproducir los pasos del ataque, una buena estrategia suele ser disponer de una máquina virtual con el mismo sistema que el equipo comprometido. Esta técnica puede ayudarnos a comprender determinadas evidencias y ayudarnos en la conclusión.

4.4.6.3 Presentación de la información

En esta última fase, los administradores deben presentar, con un lenguaje claro y sencillo, sin tecnicismos, los resultados obtenidos en las fases anteriores y las conclusiones a las que se ha llegado. Además, es una buena costumbre, explicar y justificar el método empleado.

WINDOWS 2008 R2

Capítulo 5

INSTALACIÓN Y CONFIGURACIÓN

5.1 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 5-1. 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?, ¿cómo organizo el sistema de ficheros?...

En la tabla 5-1, puede ver los requisitos mínimos para poder utilizar Windows 2008 R2 Server.

Tabla 5-1. 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.*

Nota

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

5.1.1 Primeros pasos

Para iniciar la instalación debe realizar los siguientes pasos:

- 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.
- 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 5-2).
- Seleccione la versión del sistema operativo que desea instalar (Standard, Enterprise o Datacenter) y acepte los términos de la licencia.
- 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 que se encuentran instalados en el sistema. 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 5-3 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 5-2. Instalación de Windows 2008 Server

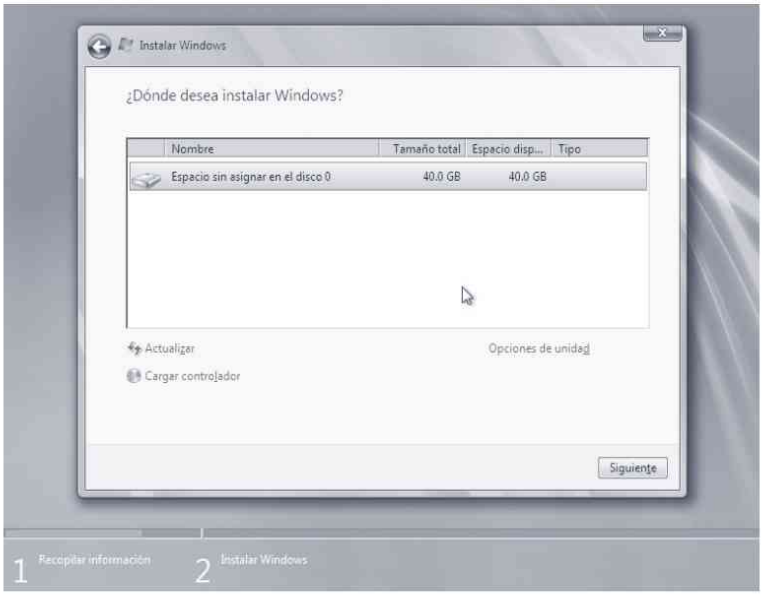


Figura 5-3. Elección de disco y partición para Windows 2008 Server

5.1.2 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 5-4), el sistema se reinicia para completar la instalación y configurar de manera automática el sistema.

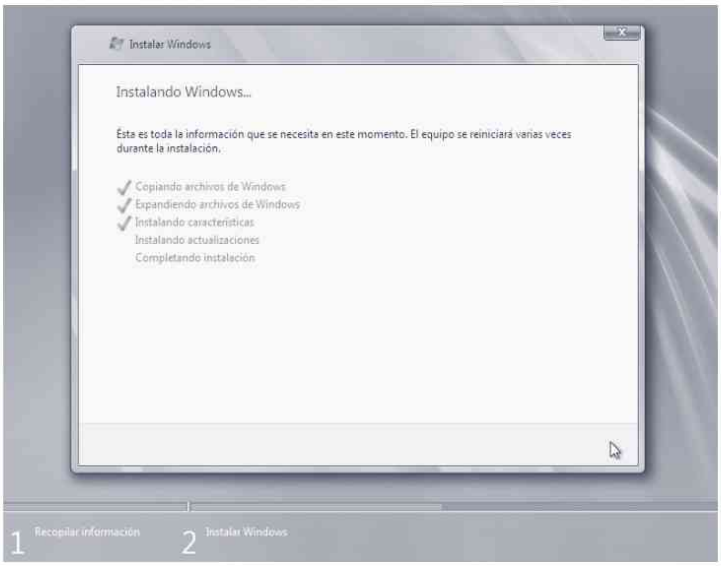


Figura 5-4. Pasos de instalación de Windows 2008

5.1.3 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 y configura de forma automática las interfaces de red. Una vez realizadas, automáticamente, las configuraciones adicionales finaliza todo el proceso pidiendo al usuario la introducción de contraseña para el usuario *Administrador* (véase figura 5-5).

Figura 5-5. 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 (véase figura 5-6), 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...

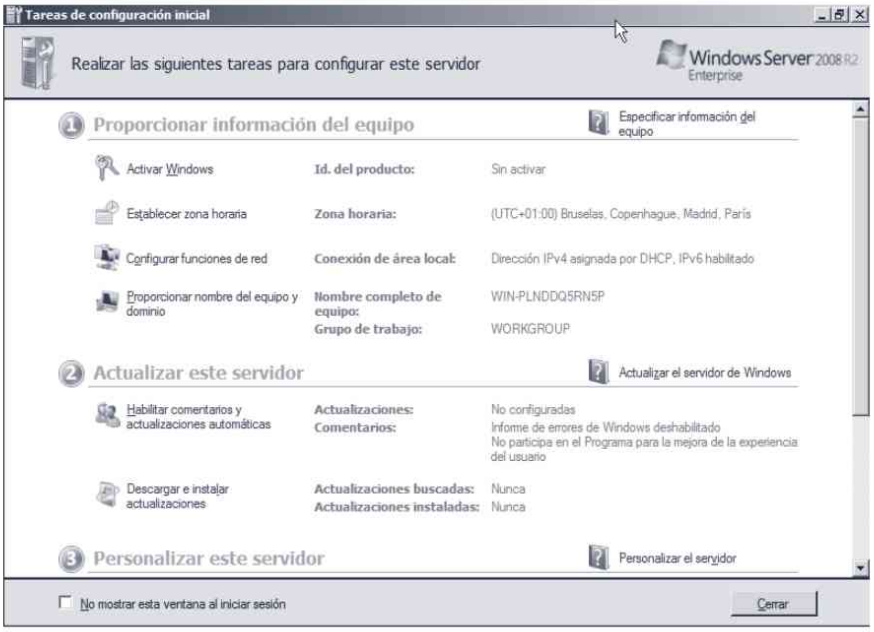


Figura 5-6. Tareas de configuración inicial

Seguridad

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

5.2 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 5-7). En esta herramienta dispone del menú *Roles*, en el que puede ver los roles que actualmente estén instalados e iniciar asistentes para agregar o quitar roles.

Para iniciar alguno de estos asistentes y agregar o quitar alguna función pulse en el enlace *Agregar roles* o *Quitar roles*. Una vez que el asistente se ha iniciado, puede observar la lista de roles disponibles para su instalación (véase la figura 5-8). 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.

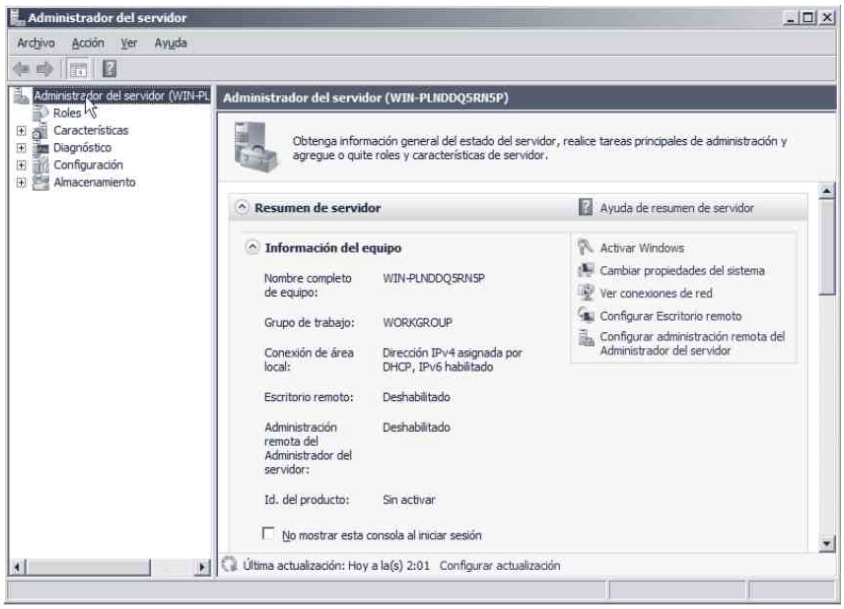


Figura 5-7. Funciones y características de Windows en el Administrador del Servidor

Nota

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

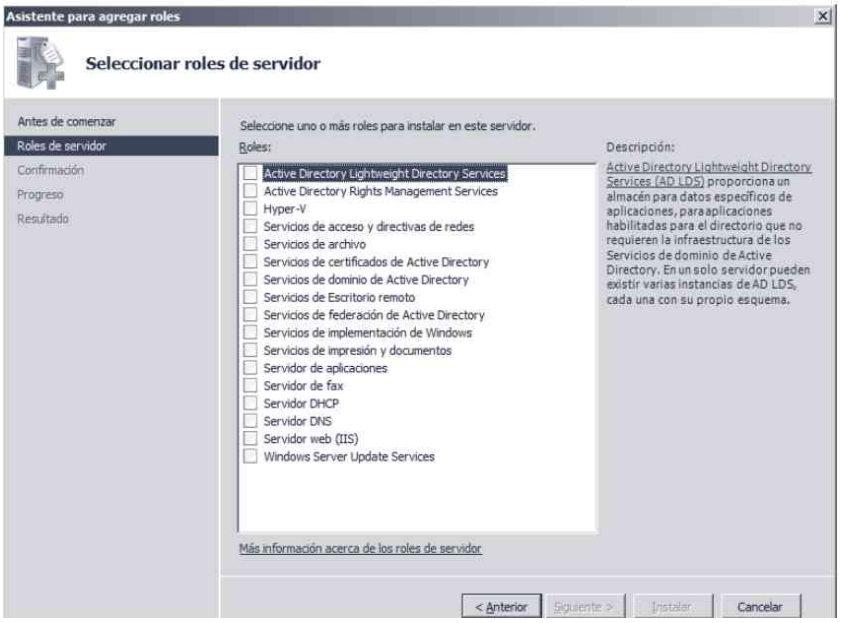


Figura 5-8. Agregar/Quitar funciones de Windows

De igual forma que puede agregar o quitar roles del servidor, existe la posibilidad de agregar o quitar características, tal y como se puede observar en la figura 5-9.

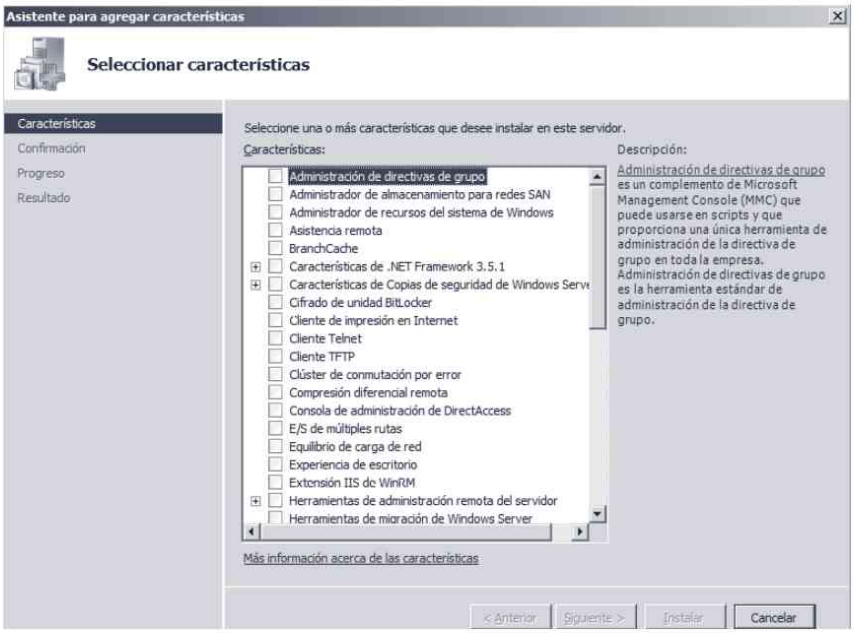


Figura 5-9. Agregar/Quitar características de Windows

Capítulo 6

PUESTA EN MARCHA DEL SISTEMA

6.1 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 y equipos del Directorio Activo.** 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.

6.1.1 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. Por defecto, 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 el sistema. 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.

Nota

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

6.1.2 El administrador de usuarios

El administrador de usuarios permite gestionar de una manera fácil los usuarios y los grupos de usuarios del sistema. Para utilizar el administrador de usuarios en el menú de inicio pulse el botón derecho del ratón sobre *Equipo*, seleccione *Administrar* y luego *Usuarios y grupos locales* que se encuentra en la categoría *Configuración* del *Administrador del servidor* (véase la figura 6-1). 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*.

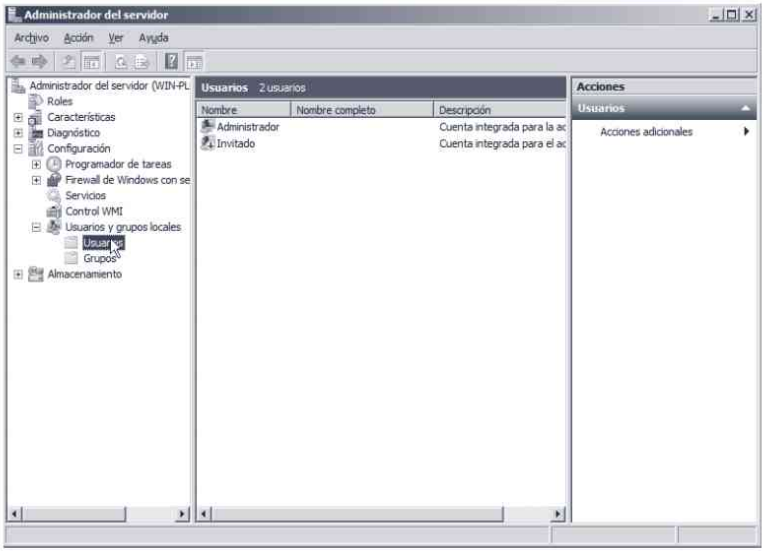


Figura 6-1. Usuarios y grupos locales en Administrador del servidor/Configuración

Nota

Si utilizas un Directorio Activo entonces para administrar los usuarios deberás utilizar la herramienta "Administración de usuarios y equipos del directorio activo" (véase el capítulo 11).

6.1.2.1 Crear una cuenta de usuario

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

- 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.
- En la ventana que aparece (véase la figura 6-2) 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 6-2. 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***.**

6.1.2.2 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 6-3). El número de pestañas que aparece en la ventana *Propiedades* varía dependiendo de los servicios instalados en el sistema.

A continuación se van a ver las pestañas más utilizadas:

- 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 (véase la figura 6-4) que permite escribir los nombres de los grupos a los que pertenece. Si no se acuerda de los nombres de los grupos puede verlos pulsando el botón *Avanzadas*.

Figura 6-3. Usuarios (Propiedades de un usuario)

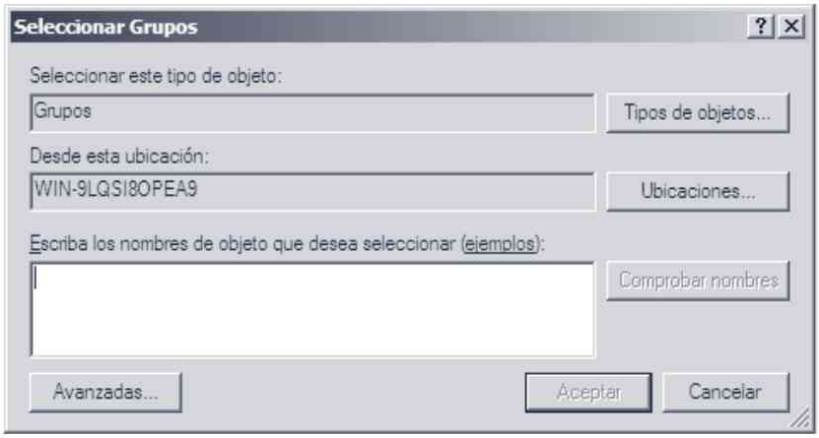


Figura 6-4. Gestión de grupos

- En la pestaña *Perfil* (véase la figura 6-5) puede establecer el perfil y el directorio particular de un usuario.

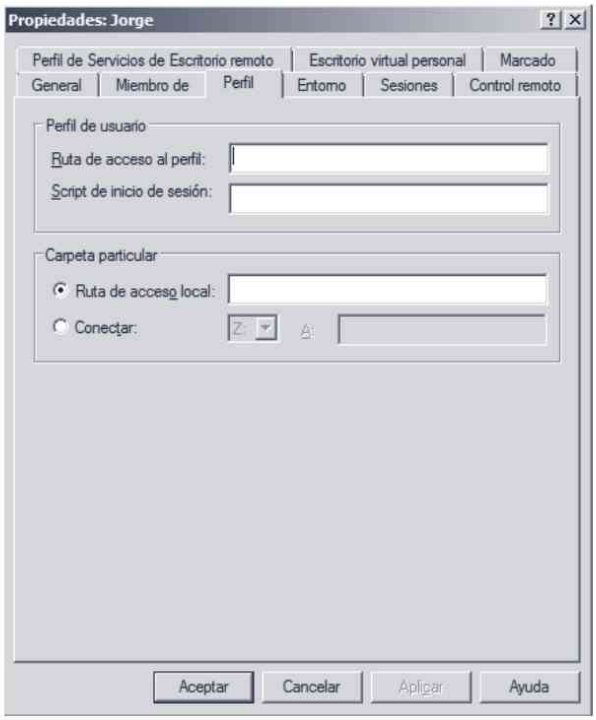


Figura 6-5. Pestaña "Perfil" de la carpeta "Propiedades de usuario"

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 el directorio es visible cuando el usuario se conecte desde la máquina en la que se ha definido, mientras que si utiliza un directorio de red, éste es 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*\).

6.1.2.3 Comandos

Aunque lo normal es utilizar el entorno gráfico, también puede administrar los usuarios del sistema utilizando el *Símbolo del sistema.* En la tabla 6-1 se muestran los comandos más utilizados.

Tabla 6-1. Comandos para la administración de usuarios

Comando	Ejemplo	Descripción
net user	net user	Muestra los usuarios del sistema (véase la figura 6-6).
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

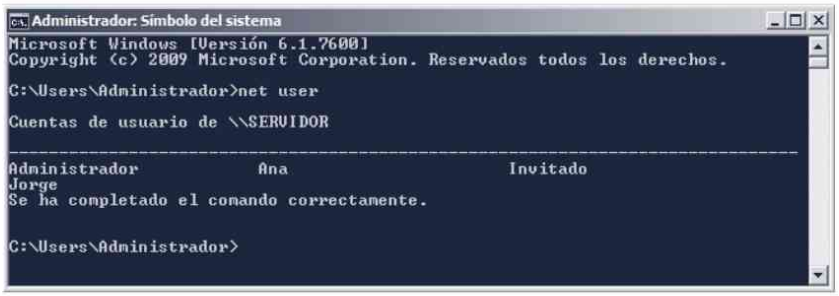


Figura 6-6. net user

Nota

Si desea conocer más opciones consulte la ayuda ejecutando:

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

6.1.3 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. Quizá 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. ej., 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 la figura 6-7).

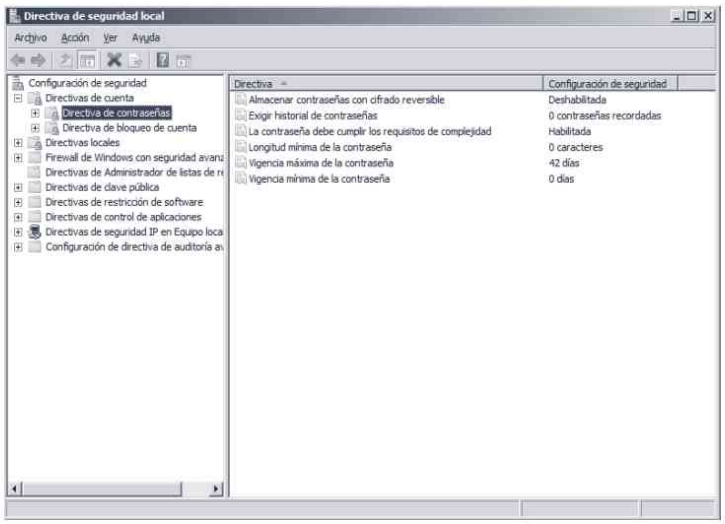


Figura 6-7. Configuración de seguridad local

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 contraseña 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 sea 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 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 hacer si es totalmente necesario.

Tabla 6-2. 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.

Consejo

Es recomendable establecer una política de seguridad que permita que las contraseñas tengan una longitud mínima de 10 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 6-3 puede ver la configuración predeterminada de bloqueo de cuentas.

Tabla 6-3. 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 se puede hacer en 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.

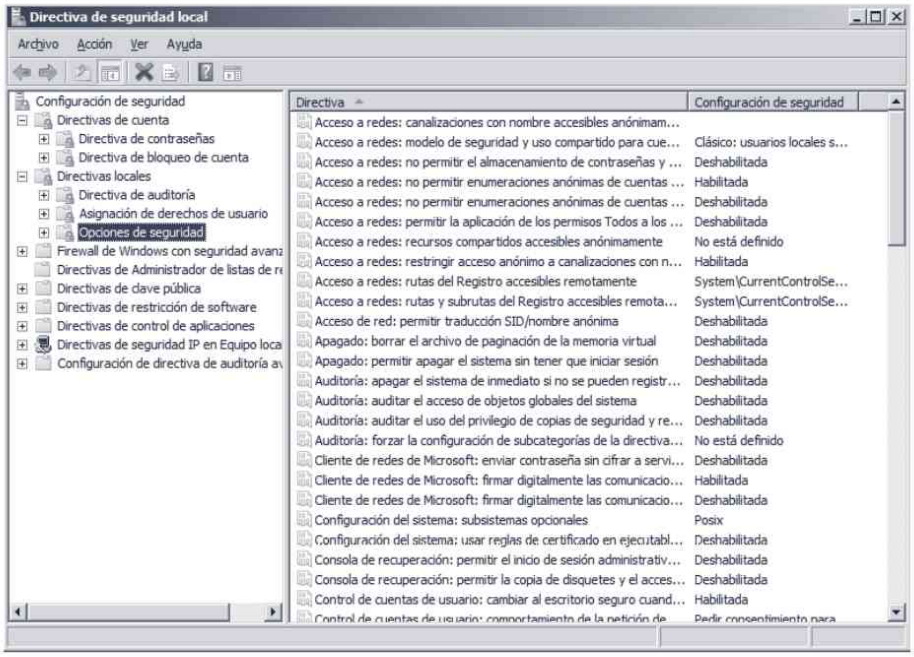


Figura 6-8. Directivas locales

6.2 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.

6.2.1 Administrador de discos

La herramienta *Administración de discos*, que se muestra en la figura 6-9, 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.

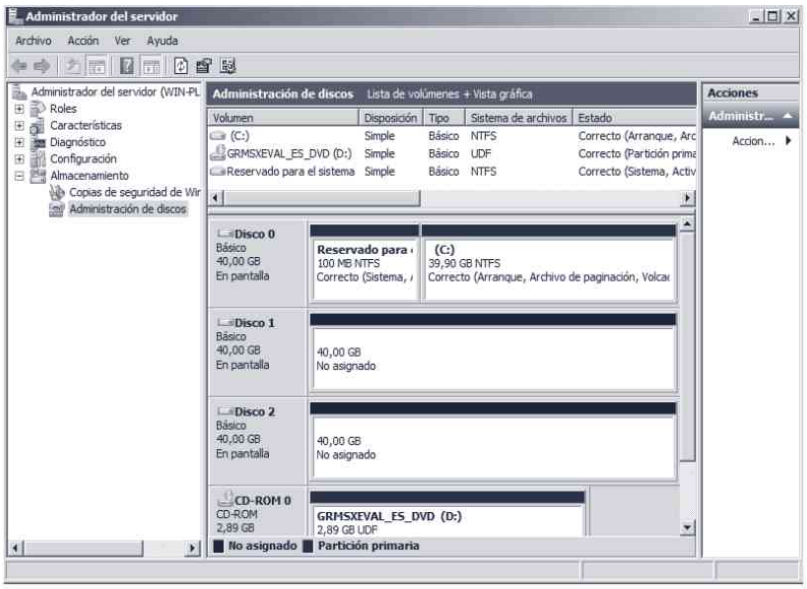


Figura 6-9. Administración de discos de Windows 2008

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. ej., 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 6-9).

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 6-10), 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).

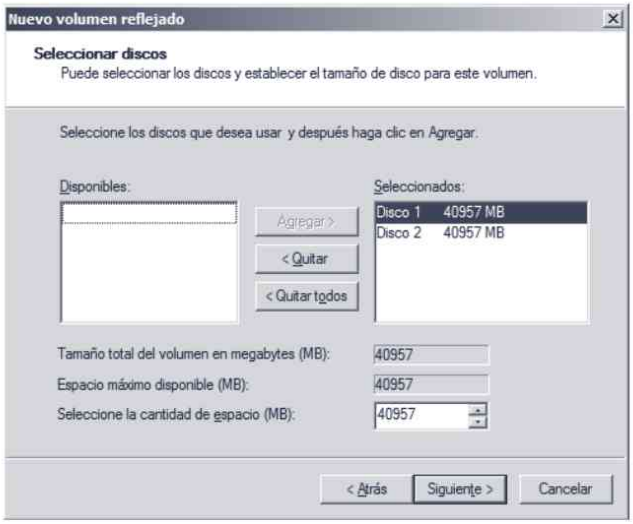


Figura 6-10. Selección de discos en el Asistente para crear volúmenes

Una vez finalizado el proceso de formateo del sistema de ficheros, el administrador de discos muestra el estado de las unidades (véase figura 6-11). En la figura puede ver cómo se ha creado un disco espejo a partir de dos unidades de disco.

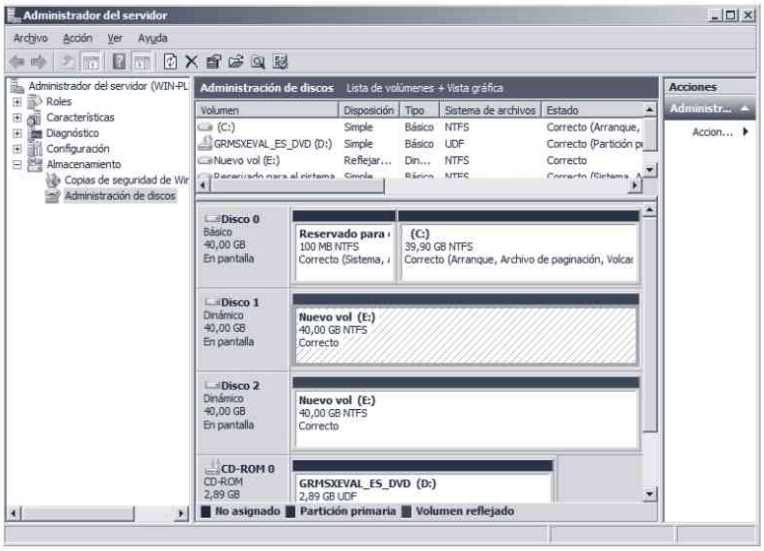


Figura 6-11. Asistente para crear volúmenes

Consejo

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
```

Consejo

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

6.2.2 Cuotas de disco

Las cuotas de disco permiten realizar un seguimiento y controlar el uso del espacio de disco de los volúmenes. Los administradores suelen utilizar 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 6-12, 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.

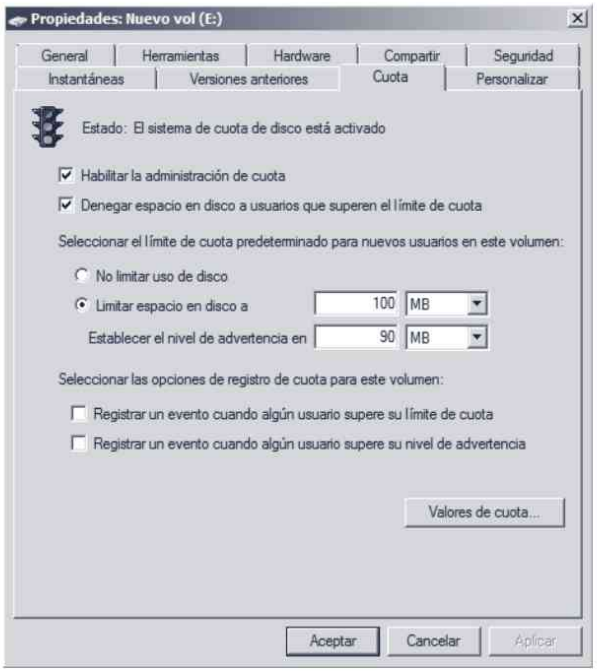


Figura 6-12. Administrador de las cuotas de disco

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 6-13 muestra cómo el usuario *Maria* ha excedido el límite establecido (100 MB), mientras que el usuario *Jperez* está por debajo del límite.

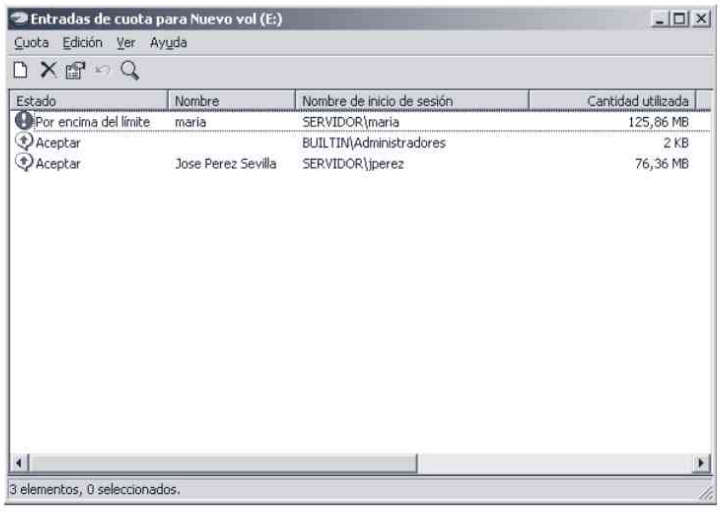


Figura 6-13. Administrador de las cuotas de disco (estado de las cuotas de usuario)

Advertencia

Para utilizar las cuotas de usuario en un disco duro el sistema de ficheros tiene que ser NTFS.

6.3 PERMISOS

Los sistemas Windows ofrecen una gran libertad para establecer los permisos de acceso a un sistema de ficheros o carpetas ya que permiten 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 aquéllos 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. ej., carpeta o disco duro) hay que seleccionar la carpeta, pulse el botón derecho y seleccione *Propiedades.* Tal y como puede ver en la figura 6-14, 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.

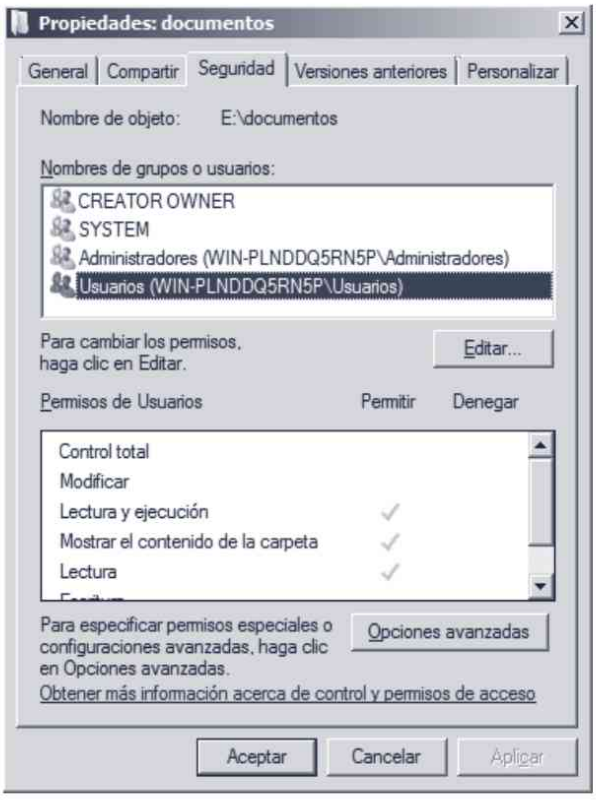


Figura 6-14. Permisos de una carpeta

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 6-14 puede ver que los *Usuarios* tienen permisos de lectura en la carpeta *e:\Documentos*. Como los permisos aparecen sombreados, los permisos se heredan 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 6-15 desactive la casilla *Incluir todos los permisos heredables del objeto primario de este objetivo* y

automáticamente el sistema pregunta si desea copiar o eliminar los permisos del objeto superior.

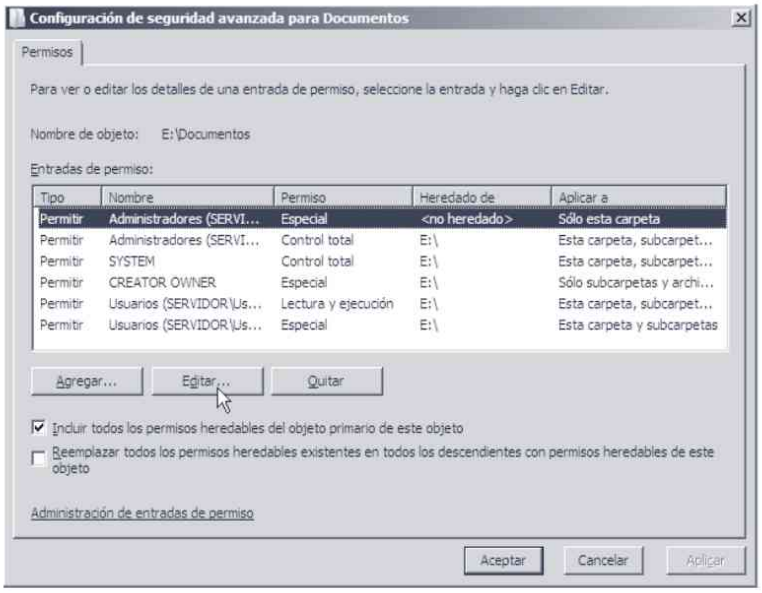


Figura 6-15. Permisos - Configuración avanzada

Para modificar los permisos pulse el botón *Editar* y en la ventana que aparece en la figura 6-16 puede añadir los usuarios o grupos a los que quiere establecer los permisos de acceso.

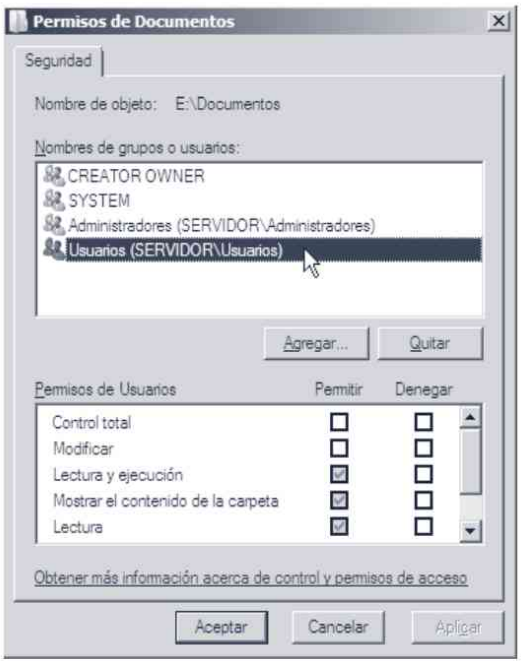


Figura 6-16. Permisos de una carpeta

Capítulo 7

ADMINISTRACIÓN BÁSICA DEL SISTEMA

7.1 ARRANQUE Y PARADA

7.1.1 Configuración del gestor de arranque del SO

Hay varias formas de indicar al gestor de arranque, el programa *osloader*, qué sistema operativo debe utilizar al iniciar el sistema.

Para configurar el gestor de arranque, en el menú *Inicio*, seleccione *Equipo*, pulse 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 7-1 puede especificar el sistema operativo que se inicia por defecto y el tiempo de espera que se muestra en el menú *Inicio*.

Figura 7-1. Inicio y recuperación de nuestro sistema

Además, también puede indicar la acción que se realiza cuando se produce un error en el sistema operativo.

Otra forma de administrar el gestor de arranque es ejecutando la herramienta *msconfig* (véase la figura 7-2).

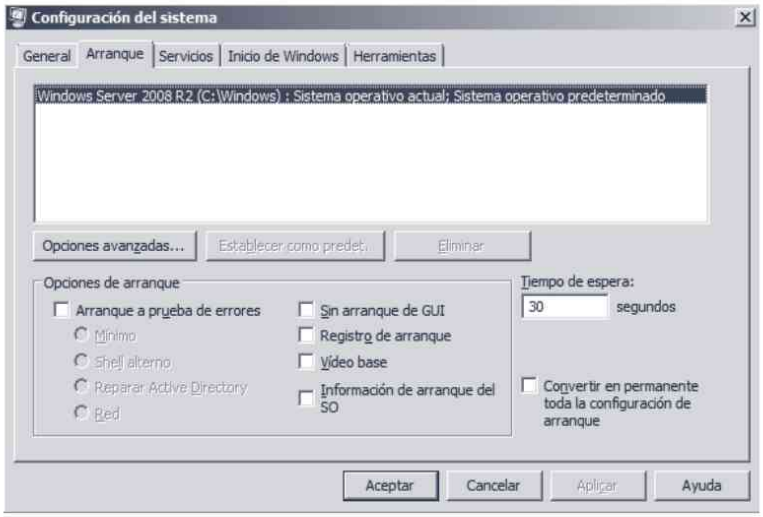


Figura 7-2. msconfig/Arranque

7.1.2 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. ej., monitores del sistema, administración de actualizaciones). Para ejecutar el administrador de servicios vaya a *Inicio*, *Herramientas administrativas* y ejecute *Servicios* (véase la figura 7-3).

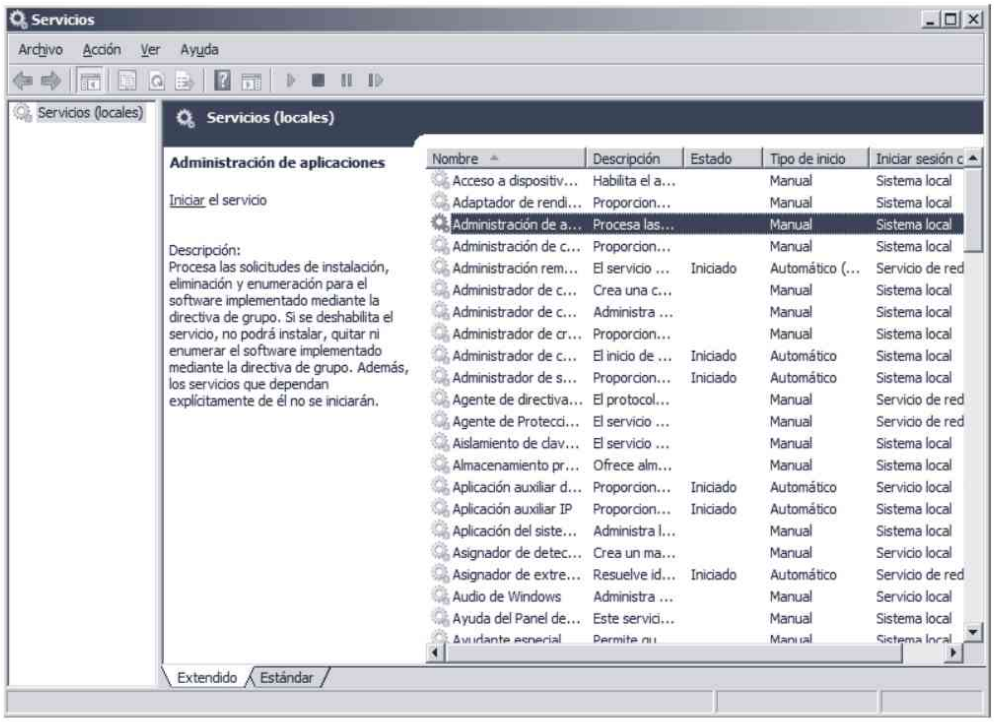


Figura 7-3. Administrador de servicios

Para ver las propiedades de un servicio haga doble clic con el ratón sobre el servicio deseado (véase la figura 7-4). 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*.

Alerta de seguridad

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

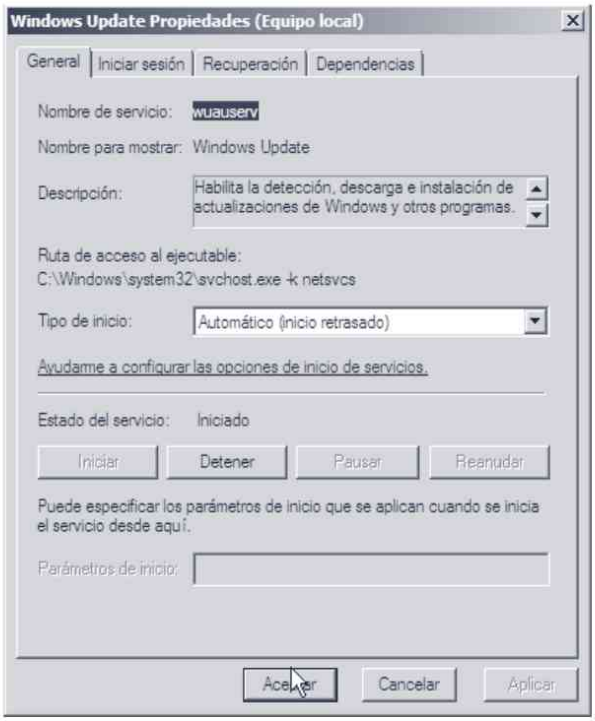


Figura 7-4. Administrador de servicios (propiedades de un servicio)

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.

Nota

Si quiere administrar los servicios del sistema por comandos puede ejecutar el comando:

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

7.1.3 Procesos

Los procesos son programas en ejecución por parte del usuario o del sistema. 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 7-5, 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.

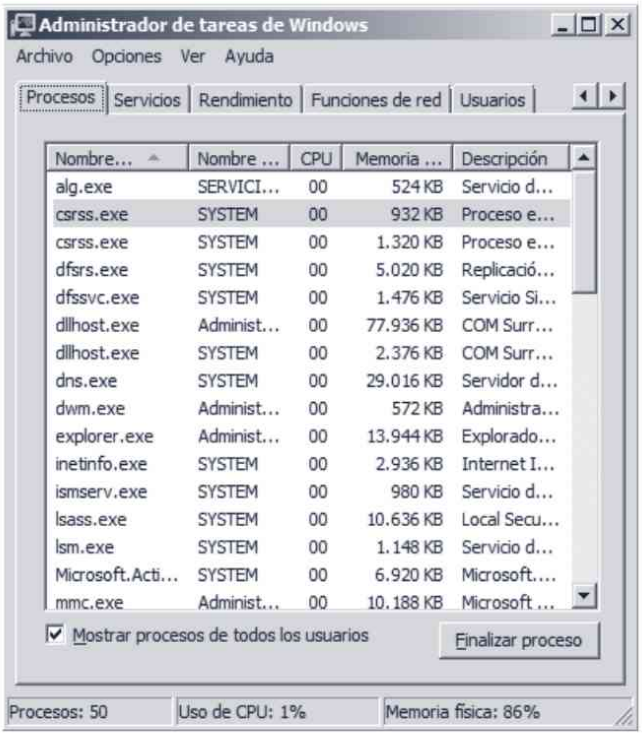


Figura 7-5. Administrador de tareas de Windows

7.1.4 Programación de tareas

La programación de tareas es una herramienta muy útil que proporciona la administración del sistema facilitando la ejecución de tareas en un momento determinado o en un 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.

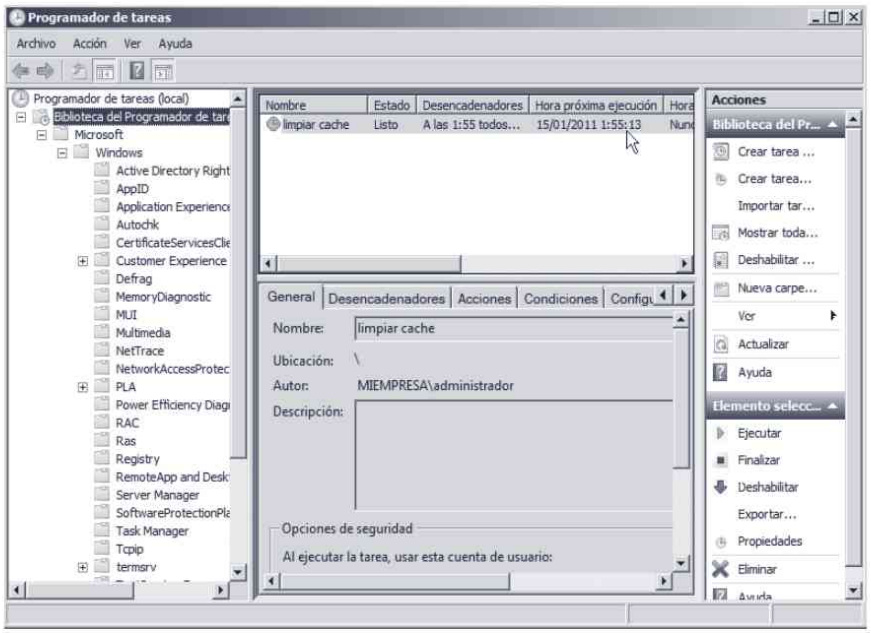


Figura 7-6. Programador de tareas

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

- Especifique el nombre y descripción de la tarea.
- 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.
- Indique la acción que desea realizar. Las acciones que se pueden realizar son: Iniciar un programa, Enviar un correo electrónico o Mostrar un mensaje.
- Por último, pulse *Finalizar*.

7.1.5 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 *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 (véase la figura 7-7).

Figura 7-7. 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 debe 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 7-8 puede ver cómo el sistema registra los eventos y los muestra en el visor de eventos, por ejemplo el de la instalación correcta de Windows.

Nota

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

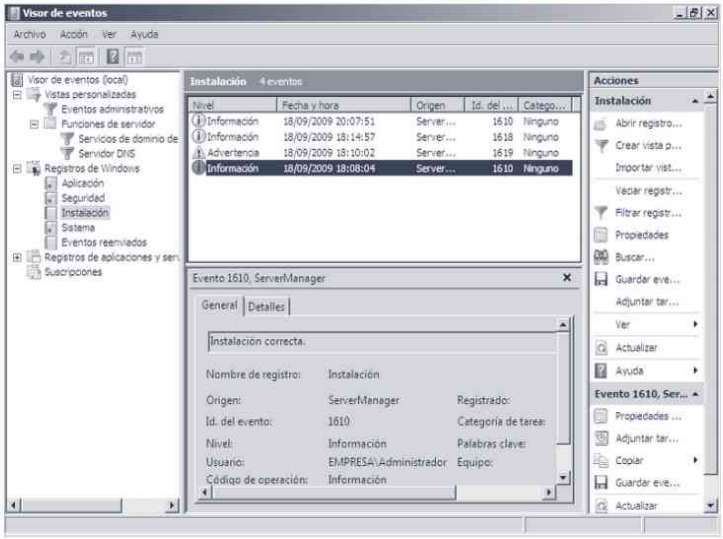


Figura 7-8. Ejemplo de evento registrado en el sistema

7.2 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.

7.2.1 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.

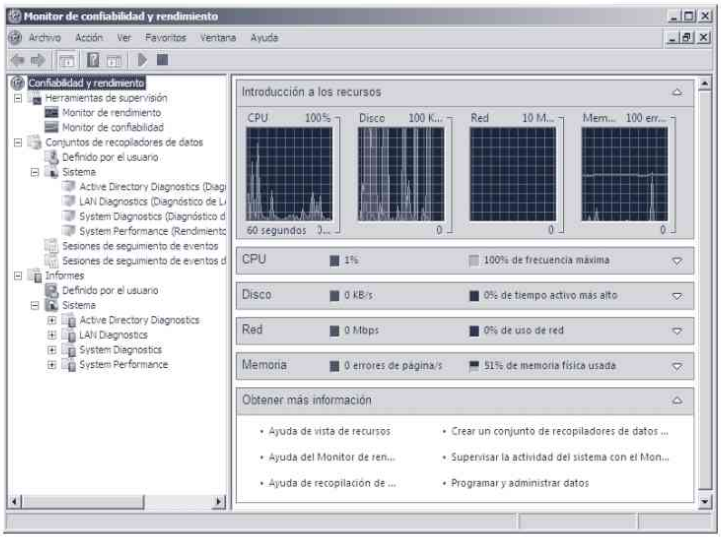


Figura 7-9. Monitor de confiabilidad y rendimiento

7.2.1.1 Monitor de rendimiento

El monitor de rendimiento permite ver en tiempo real el uso de los recursos del sistema (véase la figura 7-10).

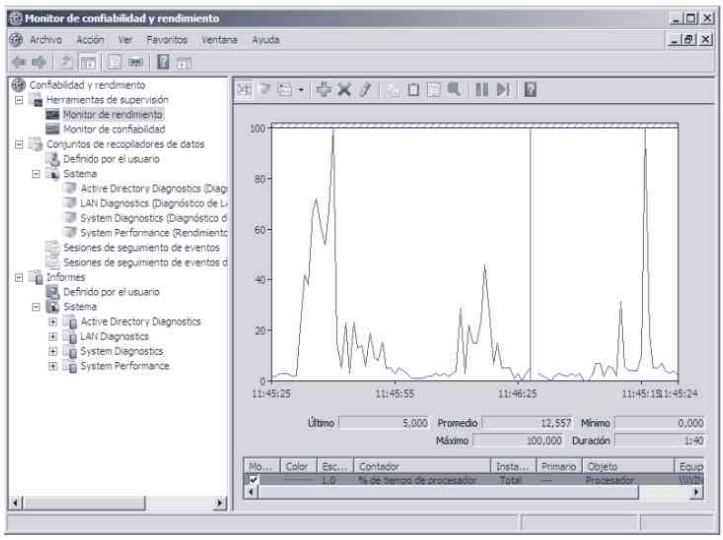


Figura 7-10. Monitor de rendimiento

Para añadir un contador al monitor del sistema, pulse en el botón  y aparece la ventana *Agregar contadores* tal y como muestra la figura 7-11. Seleccione el contador deseado y pulse el botón *Agregar*. Acepte para confirmar la adición del contador.

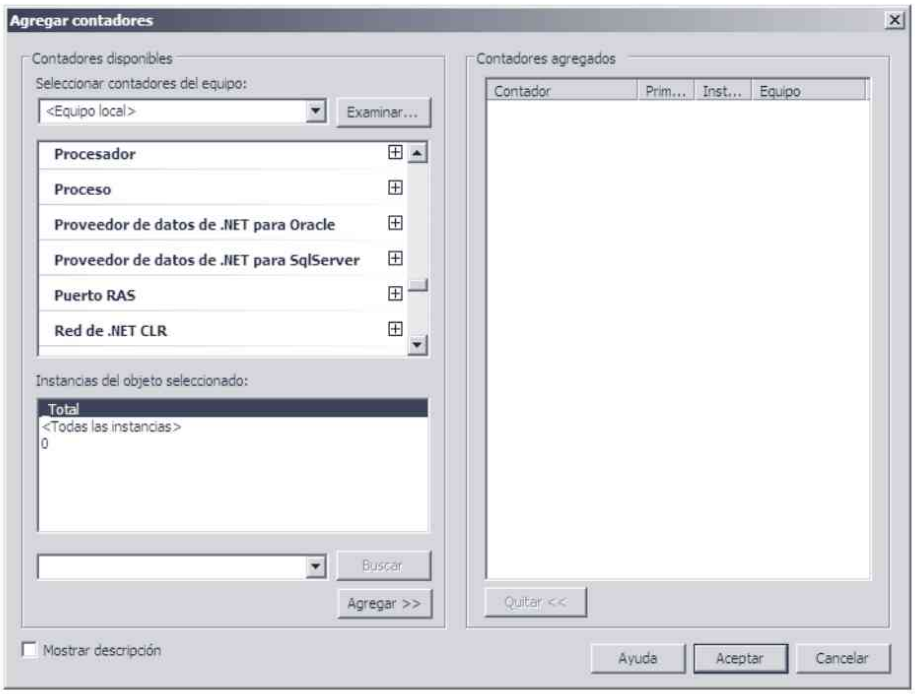


Figura 7-11. Monitor de rendimiento (agregar contadores)

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 aparece en la parte baja de la ventana una breve descripción sobre cada elemento.

7.2.1.2 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 7-12). 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*.

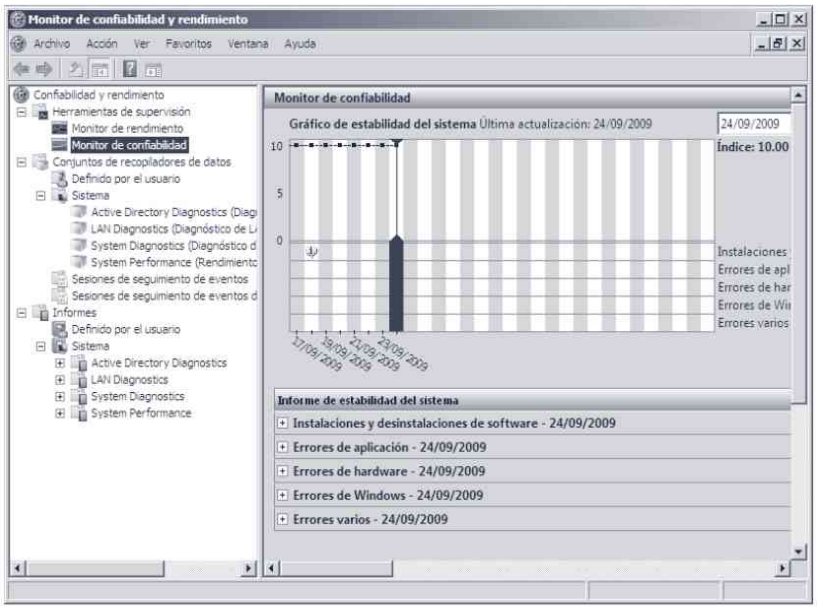


Figura 7-12. Monitor de confiabilidad

7.2.1.3 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.

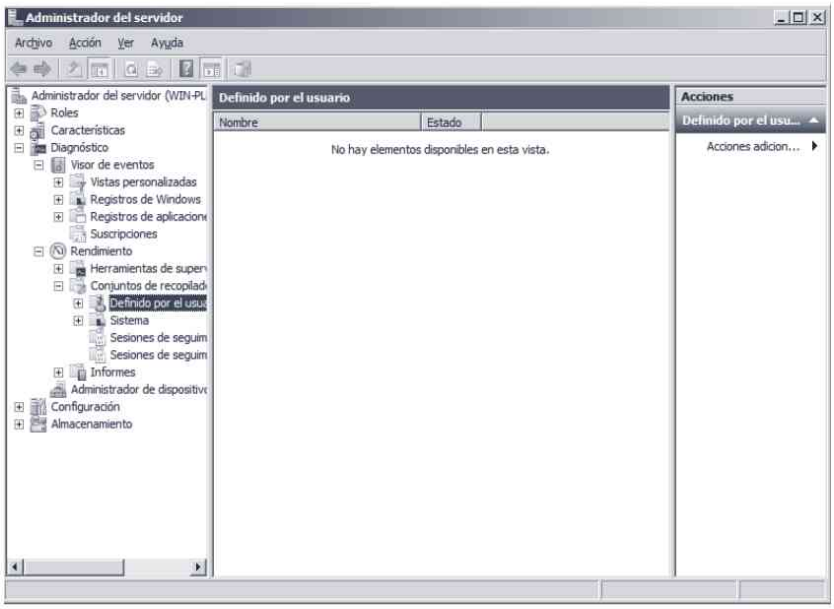


Figura 7-13. Conjuntos de recopiladores de datos e informes

Si desea crear un nuevo conjunto pulse el botón derecho, seleccione *Nuevo conjunto de recopiladores de datos*, y puede 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 7-14, 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.

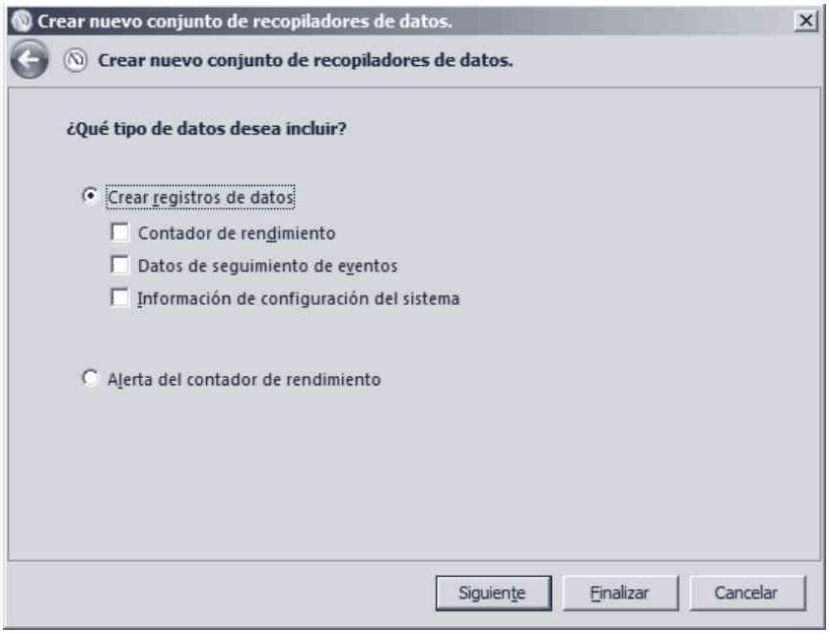


Figura 7-14. Creación de recopiladores de datos y alertas

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.

7.2.2 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 7-15).

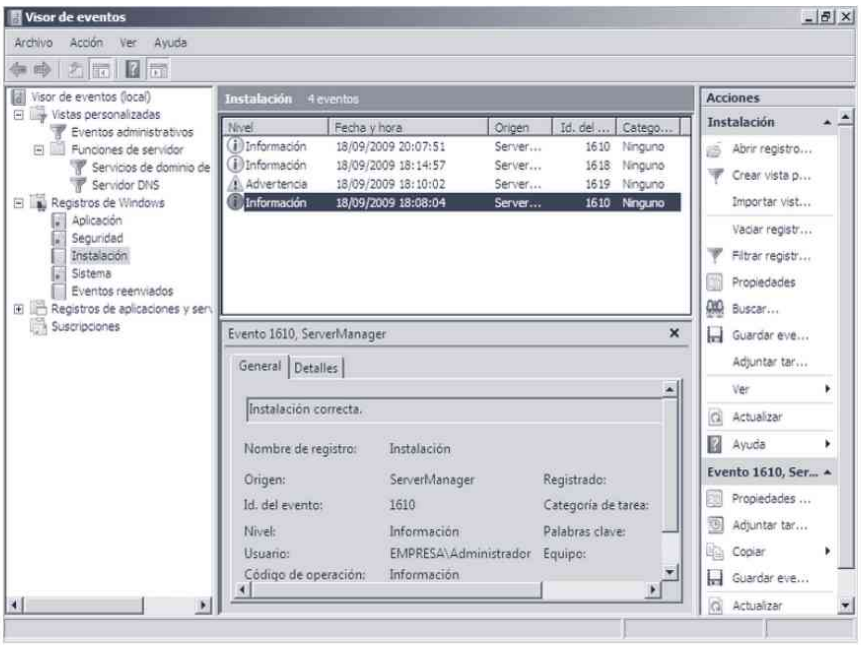


Figura 7-15. Visor de eventos del sistema

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 la *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.

7.3 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.

Nota

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. ej., 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 7-16), o bien vaya a *Inicio*, *Herramientas administrativas*, *Copias de seguridad de Windows*.

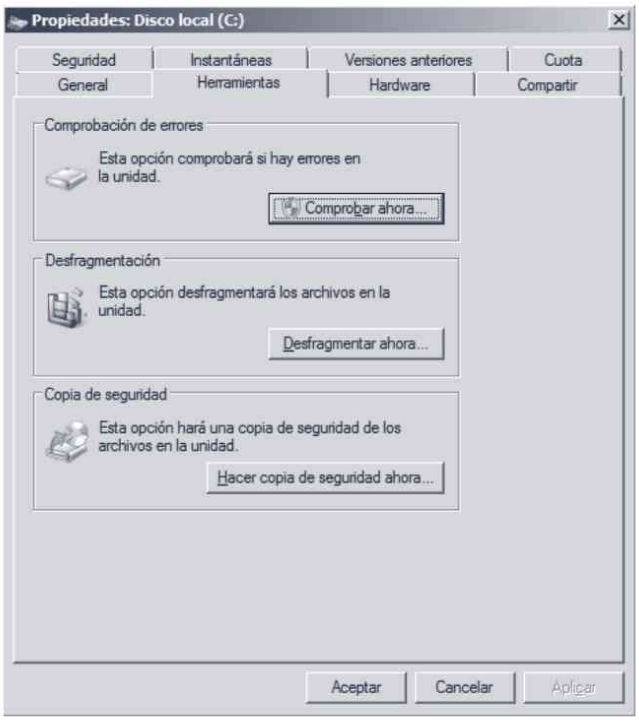


Figura 7-16. Propiedades del sistema C: (Herramientas)

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

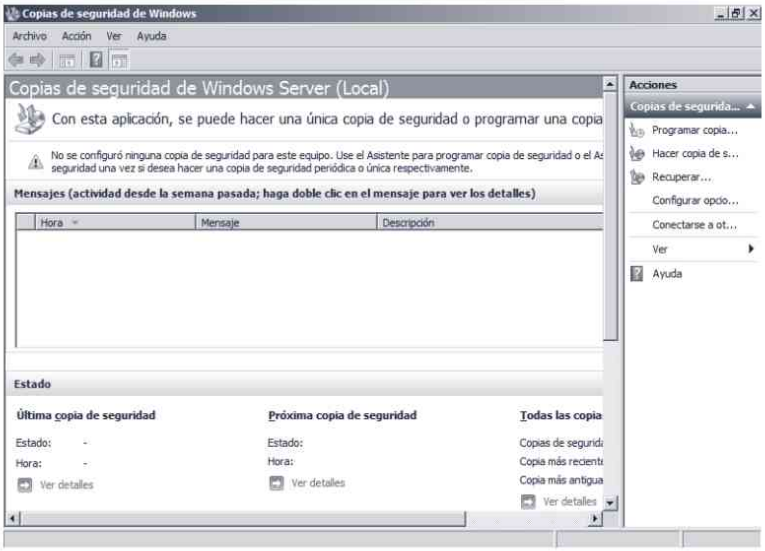


Figura 7-17. Copias de seguridad de Windows

A través del menú que aparece a la derecha (véase la figura 7-17) puede realizar las siguientes acciones a través de asistentes:

- **Hacer programación de copia de seguridad.** Es un asistente que le ayuda a 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 ayuda 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.

Advertencia

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

7.3.1 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.

Advertencia

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 7-18 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 7-18. 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 seleccionar el servidor completo o volúmenes individuales que contengan datos, estado del sistema, aplicaciones,... 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 7-19).

Figura 7-19. 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 aparece 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.

Además, si lo desea, puede realizar una **copia de seguridad una vez de manera aislada**. Al iniciar el asistente (véase la figura 7-20) tiene la posibilidad de elegir realizar una copia única basándonos en las configuraciones de copias de seguridad de 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 finaliza la copia se muestra un informe con el resultado de la operación (véase la figura 7-21).

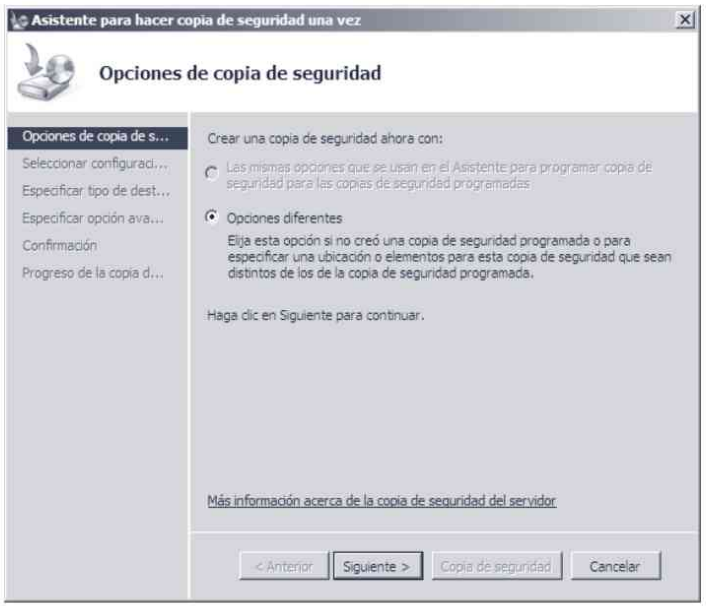


Figura 7-20. Opciones de copia de seguridad

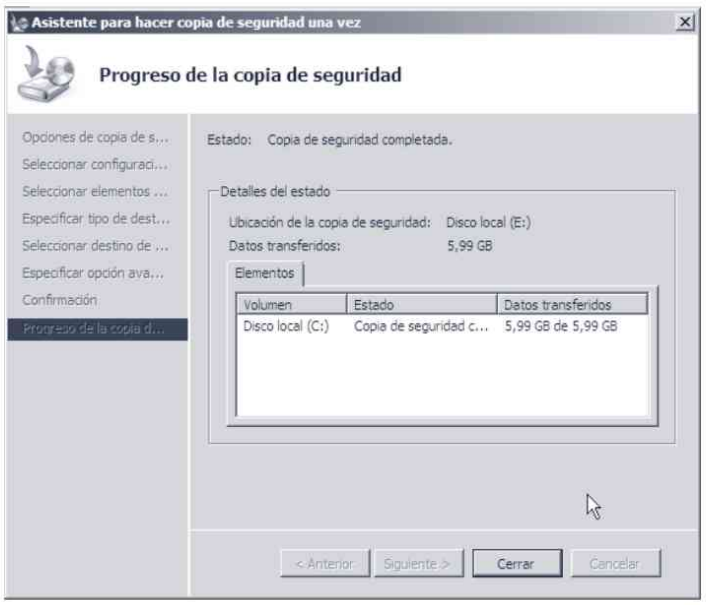


Figura 7-21. Información sobre el trabajo de copia de seguridad

7.3.2 Recuperar una copia de seguridad

El método para restaurar una copia de seguridad es muy sencillo: inicie el asistente *Recuperar...* (véase la figura 7-22 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.

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 les dará en el caso de que se encuentren duplicados, además de los permisos que se les asignan. Si selecciona la recuperación de aplicaciones, puede seleccionar la ubicación de la aplicación (si mantener la original o seleccionar una nueva). Al pulsar el botón *Finalizar* aparece una ventana que muestra el progreso de recuperación (véase la figura 7-23).

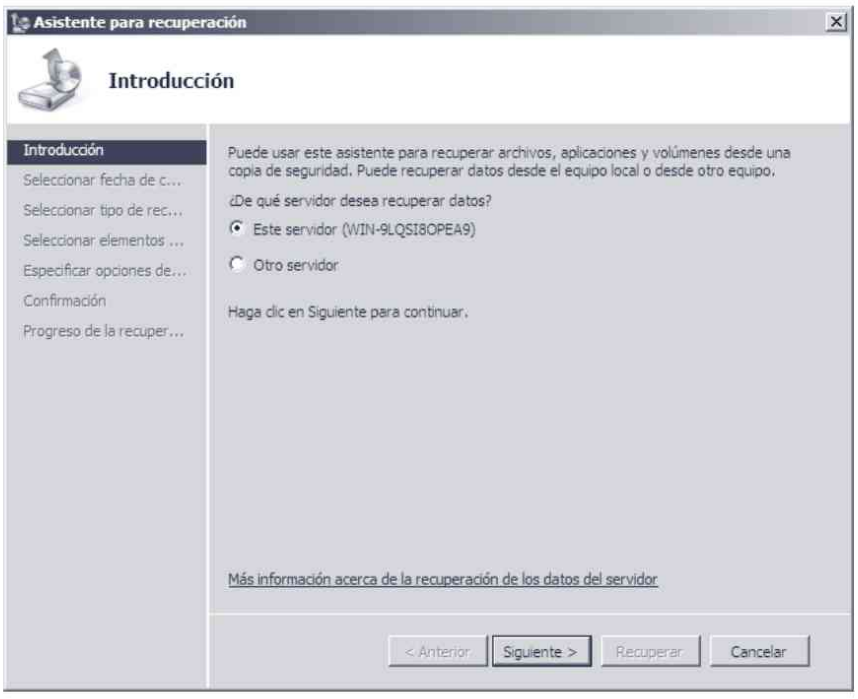


Figura 7-22. Asistente Recuperar... para copias de seguridad

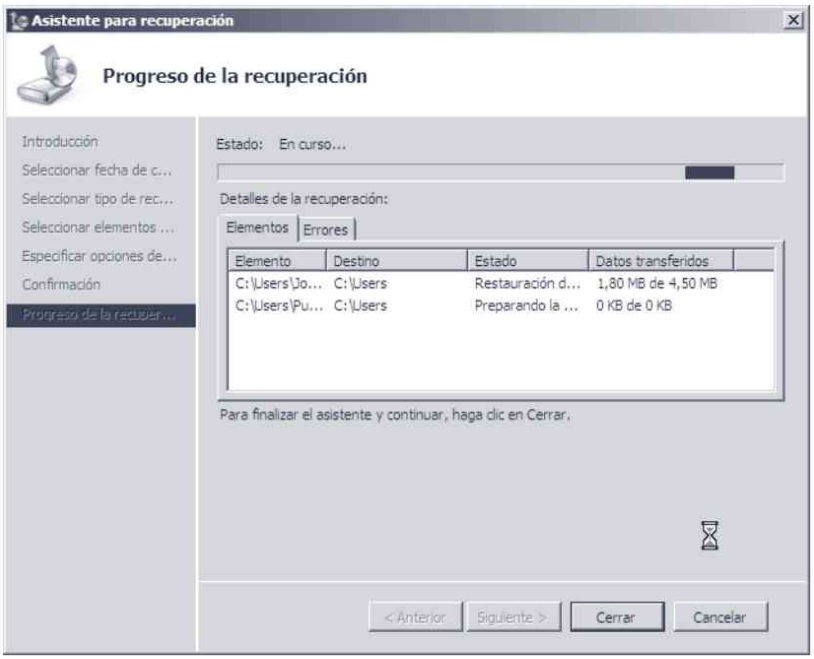


Figura 7-23. Progreso de la recuperación

7.3.3 Configurar opciones de rendimiento

La ventana de configuración de las opciones de rendimiento (véase la figura 7-24) 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 va a realizar: completa o incremental.

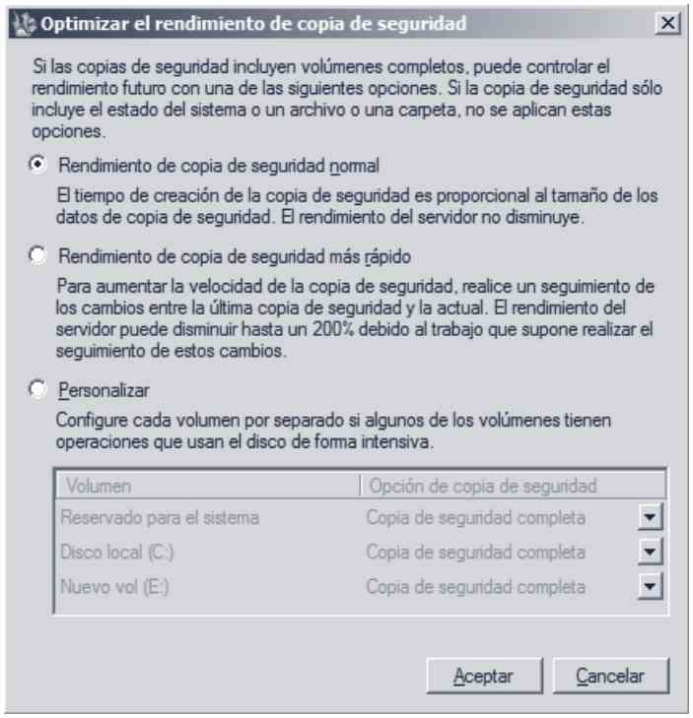


Figura 7-24. Configurar opciones de rendimiento

Consejo

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

Capítulo 8

ADMINISTRACIÓN DE LA RED

8.1 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 del capítulo se va a implementar en el servidor el esquema de red que se muestra en la figura 8-1. 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.

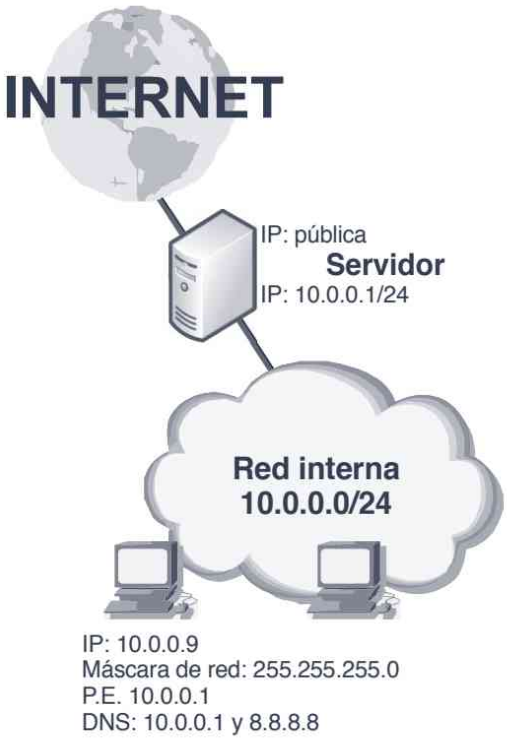


Figura 8-1. Esquema de red

8.1.1 Configuración de la red

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

8.1.1.1 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 *Conexiones de red* que muestra las conexiones de red que hay instaladas en el equipo (véase la figura 8-2).

Consejo

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. ej., 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 8-3 se muestran las propiedades del adaptador de red.

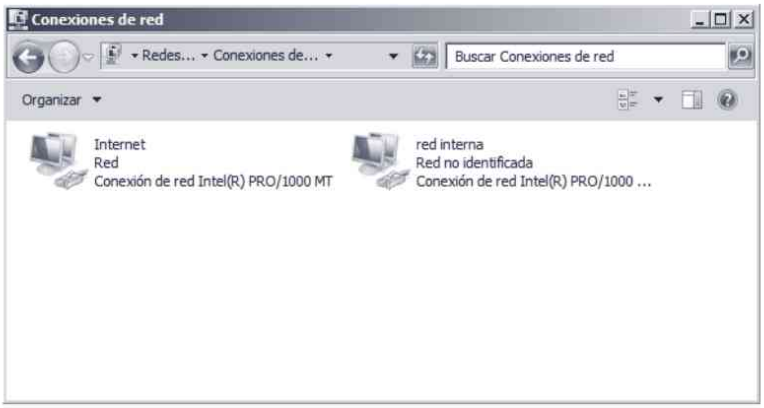


Figura 8-2. Conexiones de red en el Centro de redes y recursos compartidos

Figura 8-3. 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 *Propiedades de protocolo de Internet* (véase la figura 8-4).

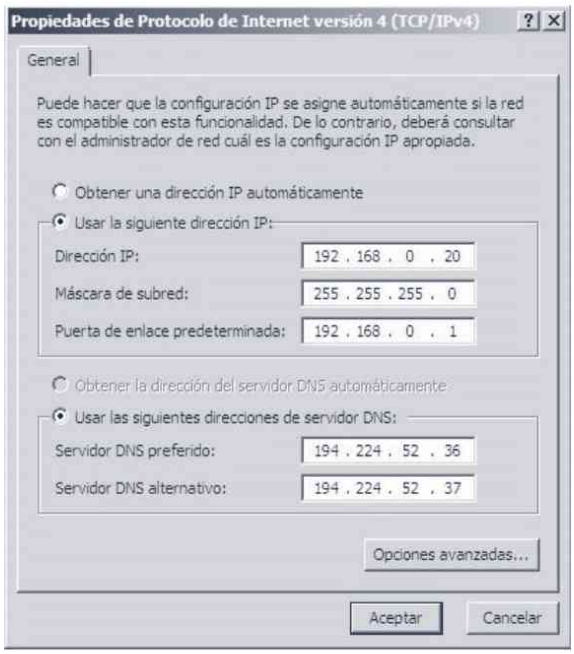


Figura 8-4. Propiedades de protocolo de Internet (TCP/IP)

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.

Nota

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.

Nota

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

```
C:\> ipconfig
```

8.1.1.2 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 8-5 escriba el nombre del equipo y el nombre del grupo de trabajo o dominio al que pertenece el equipo.

Figura 8-5. Propiedades del nombre del equipo

8.1.2 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 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 8-6).
- Y finalmente habilite el servicio.

Figura 8-6. Asistente para la instalación del servicio de enrutamiento

8.1.3 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. ej., red interna, VPN, 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 8-7 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.

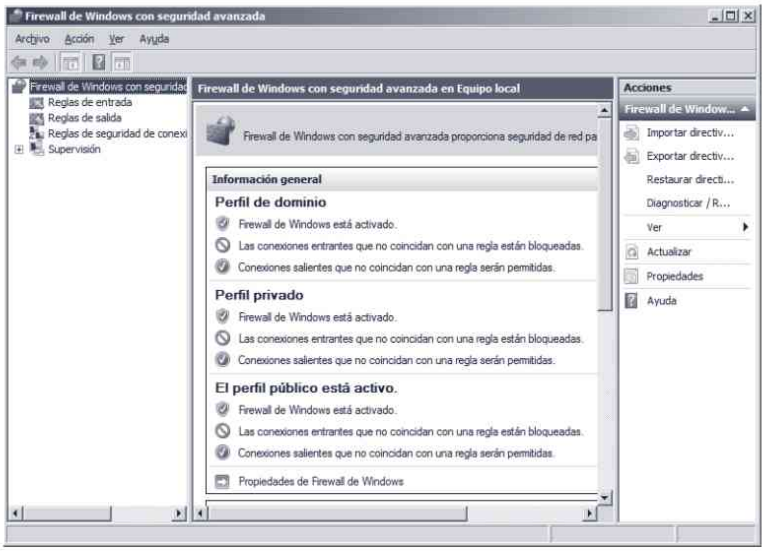


Figura 8-7. Ventana inicial del firewall de Windows con seguridad avanzada

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 (véase la figura 8-8).

Figura 8-8. 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 8-9 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.

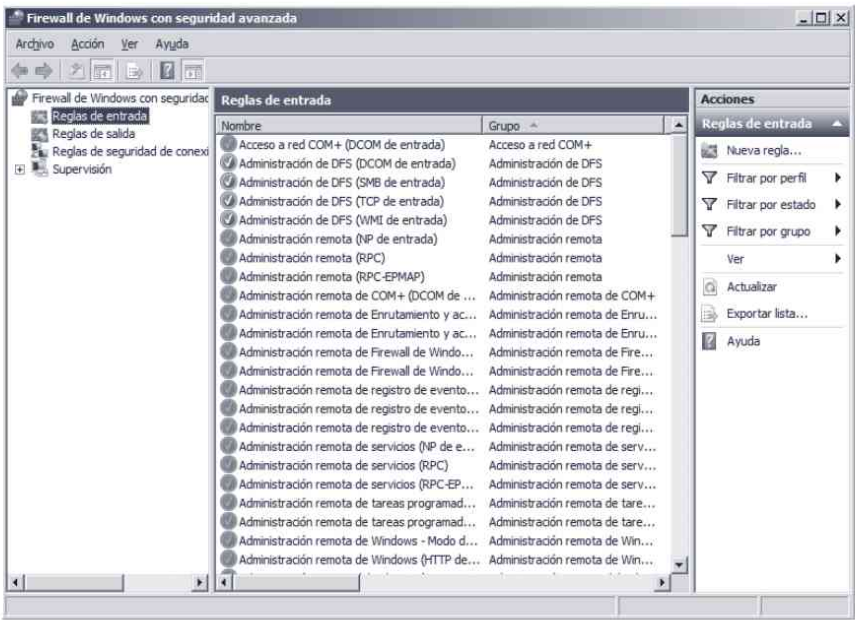


Figura 8-9. Reglas de entrada en firewall de Windows con seguridad avanzada

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 (véase la figura 8-10).

- **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 8-11).

- **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.

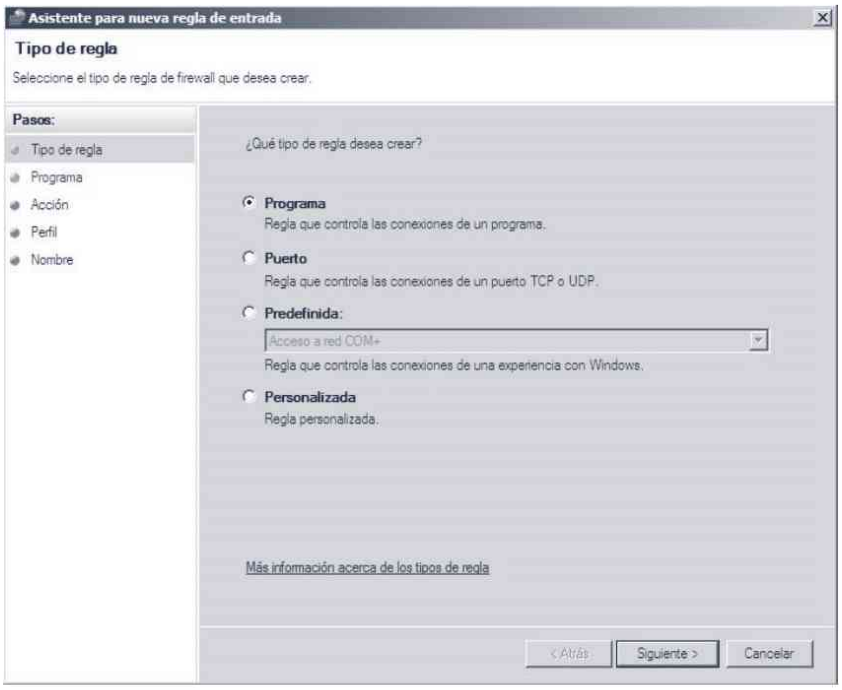


Figura 8-10. Nueva regla de entrada en firewall de Windows con seguridad avanzada

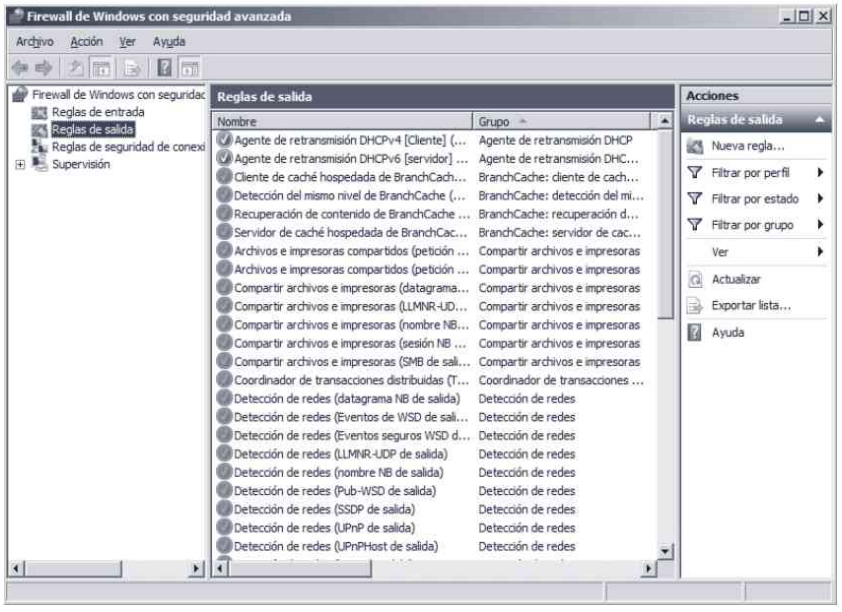


Figura 8-11. Reglas de salida en firewall de Windows con seguridad avanzada

- **Supervisión.** Permite tener acceso al estado del firewall (véase la figura 8-12) 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.

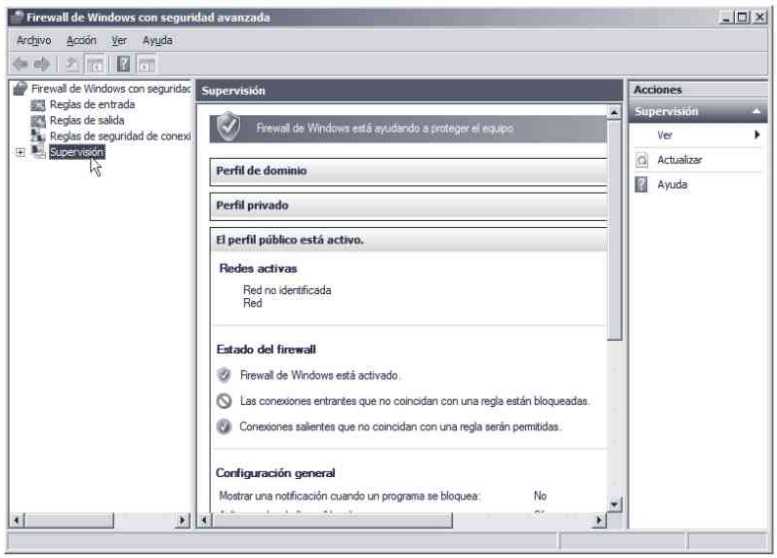


Figura 8-12. Supervisión en firewall de Windows con seguridad avanzada

8.1.4 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. ej., 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 está apagado o desconectado de la red, no utiliza ninguna dirección IP.

Para instalar el servidor DHCP puede utilizar la herramienta administrativa *Administrador del servidor* y pulse en *Agregar roles*. Durante el proceso de instalación puede configurar el ámbito de difusión del servidor DHCP y sus diferentes opciones. Para aprender mejor a configurar el servidor DHCP vamos a realizar la configuración de forma independiente al proceso de instalación.

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 8-13 puede ver la administración del servidor DHCP en el *Administrador del servidor*.

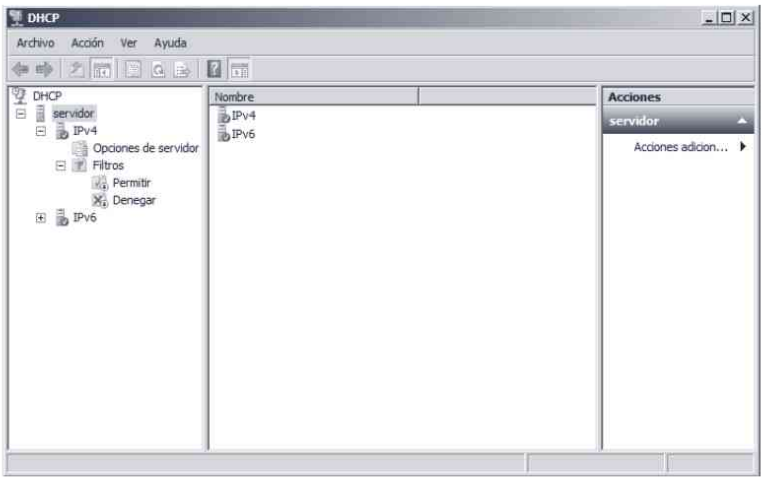


Figura 8-13. Servidor DHCP

Cuando se inicia el servidor DHCP Windows verifica 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 8-13 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 está 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*).

Nota

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

8.1.4.1 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. ej., 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. ej., 10.0.0.0/24) solo puede existir un único ámbito de difusión. Por ejemplo, si quiere compartir las direcciones que van desde 10.0.0.50 a la dirección 10.0.0.100 y las direcciones que van desde la 10.0.0.150 a 10.0.0.199, 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).

8.1.4.2 Crear un ámbito de difusión

Para crear un ámbito de difusión siga los siguientes pasos:

- Seleccione el servidor DHCP correspondiente en el árbol de consola. Hay que seleccionar el menú *Acción* y escoger *Ámbito nuevo* para ejecutar el asistente.
- Escriba el nombre y la descripción del ámbito que va a crear y pulse *Siguiente*.
- Indique el intervalo de direcciones que distribuye el ámbito, la máscara de red y pulse *Siguiente* (véase la figura 8-14).

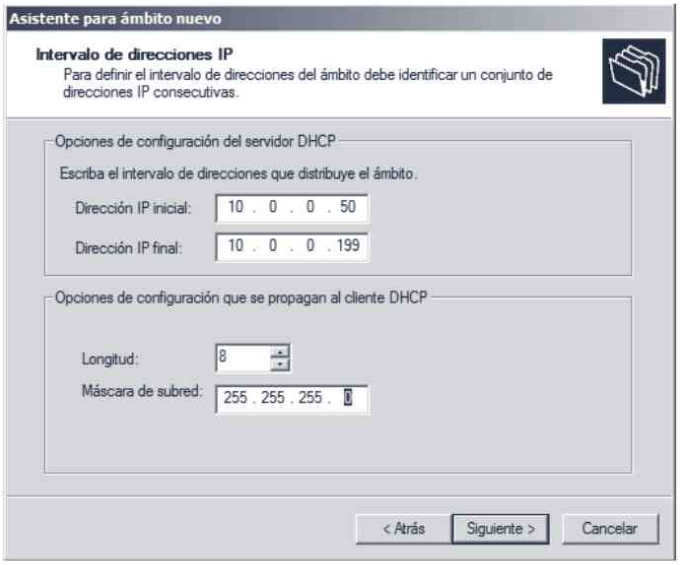


Figura 8-14. Asistente para ámbito nuevo (intervalo de direcciones)

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

- Determine la duración de la concesión. La duración de la concesión especifica durante cuánto tiempo un cliente puede utilizar una dirección IP. Pulse *Siguiente*.
- Para configurar las opciones DHCP hay que seleccionar *Configurar estas opciones ahora*. En caso contrario, elija *Configurar estas opciones más tarde* y pulse *Siguiente*.
- 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.
- 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, vaya a *Opciones de ámbito* y pulse sobre la opción que quiera configurar. En la ventana que se muestra en la figura 8-15, seleccione las opciones que necesite y establezca sus valores correspondientes.

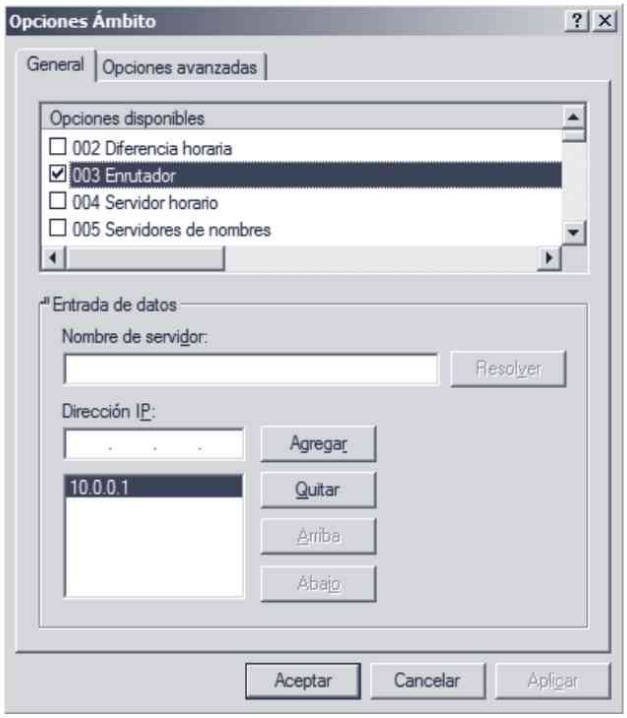


Figura 8-15. Opciones de configuración

8.1.4.3 Reservas

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

- Pulse la carpeta *Reservas* que se encuentra dentro del ámbito donde quiere realizar la reserva.
- Con el botón derecho del ratón seleccione *Reserva nueva* y aparece la pantalla que puede verse en la figura 8-16.
- Escriba el nombre de la reserva, dirección IP y la dirección MAC del equipo.
- Indique el tipo de cliente que va a utilizar la reserva: solo DHCP, solo BOOTP o ambos. Pulse *Agregar*.

Nota

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

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

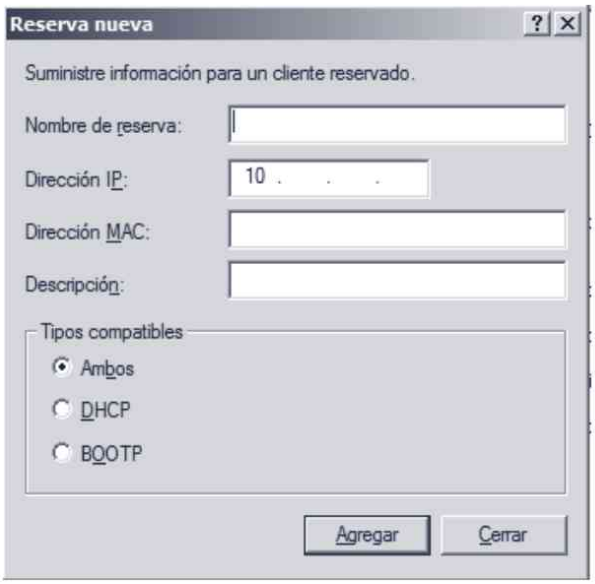


Figura 8-16. Reserva nueva

8.1.4.4 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 8-17).

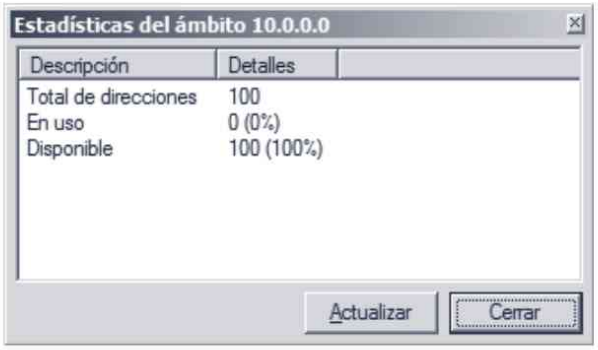


Figura 8-17. Estadísticas de ámbito

8.1.5 DNS

Como se vio en el *Capítulo 3. Servicios de Internet* los servidores DNS se utilizan para crear una correspondencia entre un nombre y una dirección IP, o viceversa.

8.1.5.1 Instalación y configuración

Para instalar el servidor DNS utilice la herramienta administrativa *Administrador del servidor* y pulse en *Agregar roles*.

Una vez instalado el componente, para administrarlo seleccione *Equipo* en el escritorio, pulse el botón derecho y seleccione *Administrar* o ejecute *DNS* que se encuentra dentro de las herramientas administrativas (véase la figura 8-18).

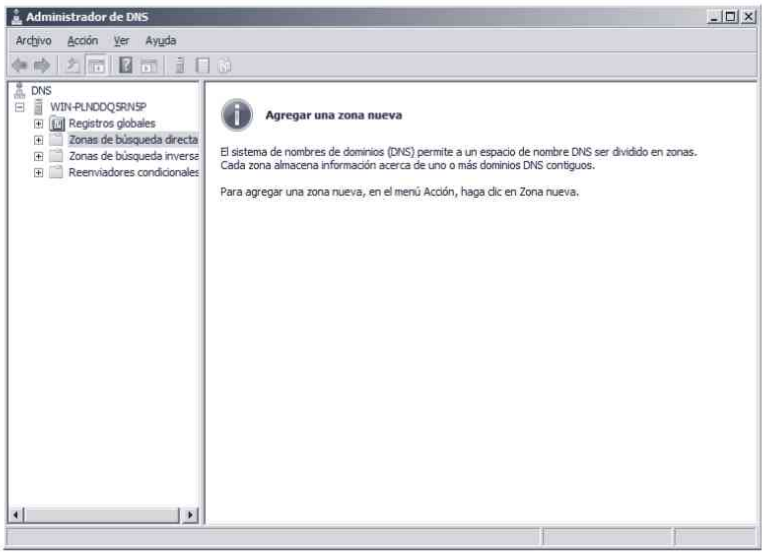


Figura 8-18. Servidor DNS

Nota

Si el servidor es un controlador de dominio, el servidor DNS ya se encuentra instalado.

8.1.5.2 Habilitar los reenviadores

Un reenviador ayuda a resolver cualquier consulta DNS que no se encuentre en la base de datos local. Es necesario habilitar los reenviadores si quiere que la red local tenga salida a Internet. Por ejemplo, si consulta la dirección *www.adminso.es*, nuestro servidor DNS consultará su base de datos, y si no encuentra el registro le preguntará a los reenviadores (otros servidores DNS). Para activar los reenviadores pulse el botón derecho del ratón sobre el nombre del servidor y seleccione *Propiedades.* Pulse en la pestaña *Reenviadores,* pulse *Editar* y añada la dirección IP de los servidores DNS que quiere utilizar como reenviadores (véase la figura 8-19).

Figura 8-19. Configuración de los reenviadores

8.1.5.3 Crear una nueva zona

Una zona permite almacenar partes del espacio de nombres DNS de modo que un solo servidor DNS pueda atender a una parte del espacio de nombres. Existen dos tipos de zonas de búsqueda:

- **Zonas de búsqueda directa.** Son el tipo de zonas que se suele asociar con los servidores DNS ya que permiten obtener una dirección IP a partir de un nombre.
- **Zonas de búsqueda inversa.** Su uso es menos frecuente y permite obtener un nombre a partir de una dirección IP. Por motivos de seguridad, no se recomienda utilizar zonas de búsqueda inversa ya que un posible atacante puede determinar los dominios a los que da servicio un servidor mediante su dirección IP.

Para crear una zona realice los siguientes pasos:

1. Seleccione el servidor donde quiera crear la zona, pulse el botón derecho del ratón y seleccione *Zona nueva*.

2. Aparece la pantalla de inicio del asistente que le guía durante la creación de la nueva zona. Pulse *Siguiente.*
3. Indique el tipo de zona que quiere crear:
   - **Zona principal.** Crea una zona que puede actualizarse directamente en este servidor.
   - **Zona secundaria.** Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar la carga de los servidores primarios.
   - **Zona de código auxiliar.** Crea una copia que contiene solo servidor de nombres (NS), inicio de autoridad (SOA) y registros de hosts (A). Un servidor que contiene una zona de código auxiliar no tiene privilegios sobre la zona.
4. Para proporcionar actualizaciones seguras y almacenamiento integrado active la casilla *Almacenar la zona en Active Directory*. En caso contrario la información se guardará en un fichero de texto.
5. Seleccione *Zona principal* y si es posible active el almacenamiento en el Active Directory. Pulse *Siguiente.*
6. Seleccione el tipo de zona de búsqueda que quiere crear: *Zona de búsqueda directa o indirecta.* La opción recomendada es *Zona de búsqueda directa*. Pulse *Siguiente.*
7. Escriba el nombre de la zona (p. ej., miempresa.com) y pulse *Siguiente*.
8. Si ha decidido en el paso 4 guardar la información en un fichero de texto, ahora el ordenador le pregunta si crea un archivo para la zona, o por el contrario si quiere utilizar uno ya existente. El archivo debe tener el formato *nombre_del_dominio.dns* y se almacenará en *c:\Winnt\system32\Dns*. Por ejemplo, para el dominio *miempresa.com* se crea el archivo *miempresa.com.dns*.
9. Indique si quiere permitir las actualizaciones dinámicas. Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros en el DNS cuando se produzcan cambios. Seleccione la opción que más le interese:
   - Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory).
   - Permitir todas las actualizaciones dinámicas (seguras y no seguras).
   - No admitir actualizaciones dinámicas.

10. Para finalizar, tal y como muestra la figura 8-20, el sistema le muestra un resumen de las opciones seleccionadas. Si está de acuerdo pulse *Finalizar.*

Figura 8-20. Finalización del Asistente para nueva zona

Una vez finalizado el proceso, la zona se encuentra activa en la zona de búsqueda especificada en el paso 6. En la figura 8-5 puede ver que se ha creado la zona *miempresa.com* en la zona de búsqueda directa.

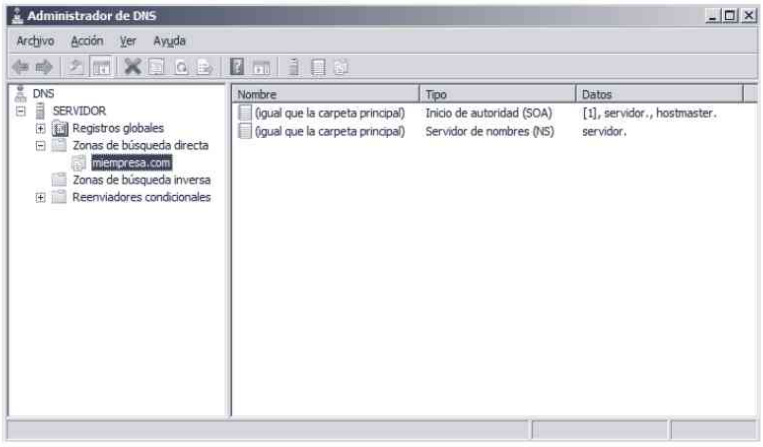


Figura 8-21. Servidor DNS

8.1.5.4 Crear registros

Los servidores DNS de Windows utilizan una nomenclatura diferente a los demás servidores DNS (los servidores basados en Linux o de Internet). En la tabla 8-1, puede ver la equivalencia entre los registros más importantes de los diferentes sistemas.

Tabla 8-1. Tipos de registros DNS

Nombre	Código	Descripción
Host	*A*	*Dirección de anfitrión. Asigna un nombre a una dirección.*
Alias	*CNAME*	*Nombre canónico. Establece un alias para un nombre verdadero.*
Intercambiador de correo	*MX*	*Intercambio de correo. Especifica qué máquinas intercambian correo.*

Para crear un registro, seleccione la zona, pulse el botón derecho y seleccione la opción deseada: *Crear nuevo host*, *Crear nuevo alias* o *Crear nuevo intercambiador de correo.*

Si selecciona *Crear nuevo host* tiene que escribir el nombre del host, la dirección IP asociada y debe confirmar si quiere crear un registro PTR en la zona inversa (véase la figura 8-22).

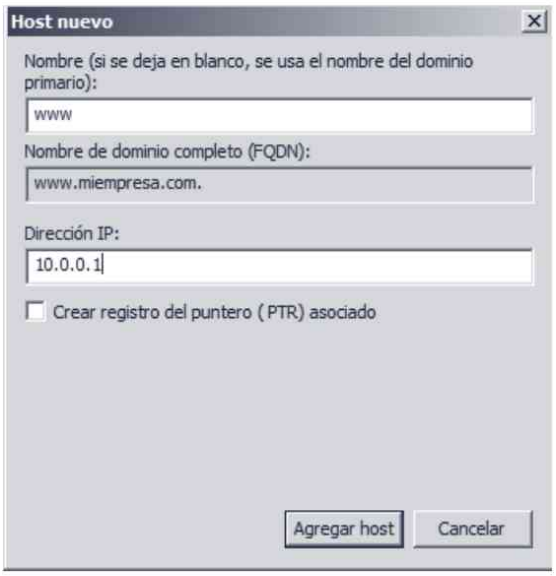


Figura 8-22. Crear un host nuevo

Si selecciona *Crear nuevo alias* (véase la figura 8-23) debe escribir el nombre del alias y el registro completo para el host de destino.

Y si selecciona *Crear nuevo intercambiador de correo* aparece la pantalla que se encuentra en la figura 8-24. Debe escribir el nombre del servidor de correo (esta entrada debe estar dada de alta como host) y la prioridad del servidor de correo. La prioridad va de 10 en 10, y la prioridad más alta es la 10, después la 20, etc.

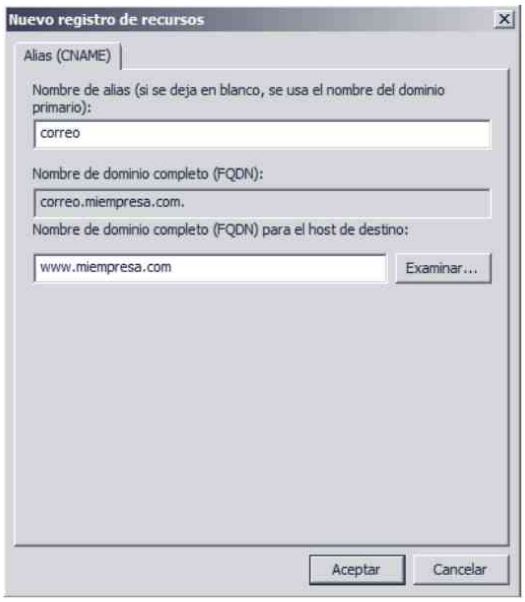


Figura 8-23. Crear nuevo alias

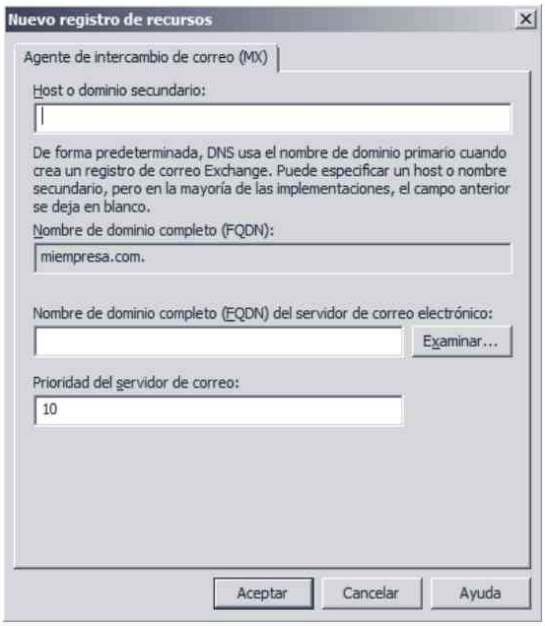


Figura 8-24. Servidor DNS

8.1.5.5 Crear subdominios y delegaciones de zona

En la mayor parte de las empresas de tamaño medio o grande hay que crear zonas y delegar la administración de otras zonas a otros servidores DNS. Esto facilita el trabajo de los administradores ya que no se crean espacios de nombres de

gran tamaño albergado en una única zona por un solo servidor. De esta manera puede que tenga una zona que contenga el dominio raíz *miempresa.com* y el subdominio *servicios.miempresa.com*. Sin embargo, puede que haya delegado el subdominio *departamentos.miempresa.com* a otro servidor DNS.

Para crear un subdominio, seleccione el dominio donde quiere crear el subdominio, pulse el botón derecho del ratón y seleccione *Dominio nuevo*. En la pantalla que aparece (véase la figura 8-25) escriba el nombre del subdominio y pulse *Aceptar*.

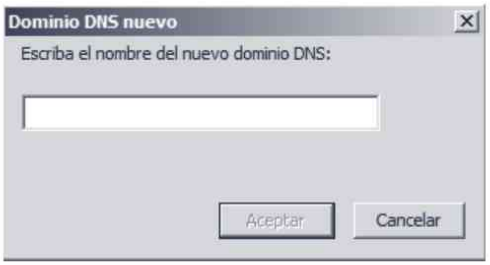


Figura 8-25. Servidor DNS

Si desea delegar un subdominio, seleccione el dominio principal, pulse el botón derecho del ratón y seleccione *Delegación nueva.* En la pantalla que aparece (véase la figura 8-26) escriba el nombre del subdominio y pulse *Siguiente.* A continuación escriba los nombres o direcciones IP de los servidores DNS a los que desea transferir el control. Pulse *Siguiente*. Por último, el asistente le muestra un resumen de las opciones seleccionadas, pulse *Finalizar.*

En la figura 8-11 puede ver cómo se ha creado el subdominio *servicios* y se ha transferido el control de la zona *departamentos*.

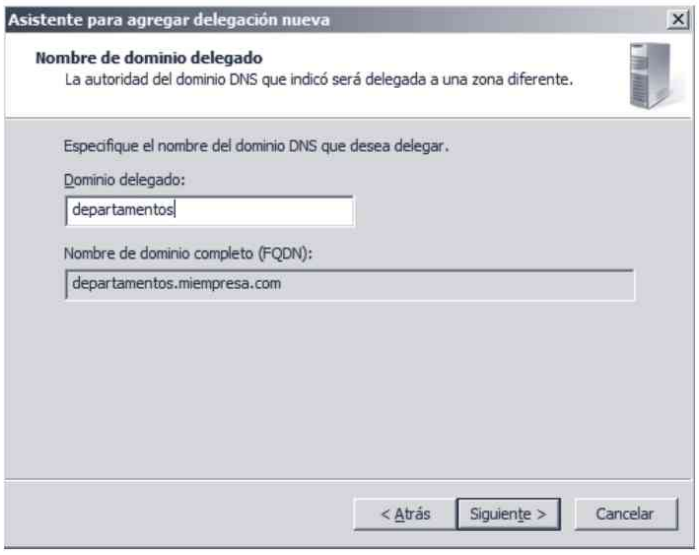


Figura 8-26. Delegación nueva del servidor DNS

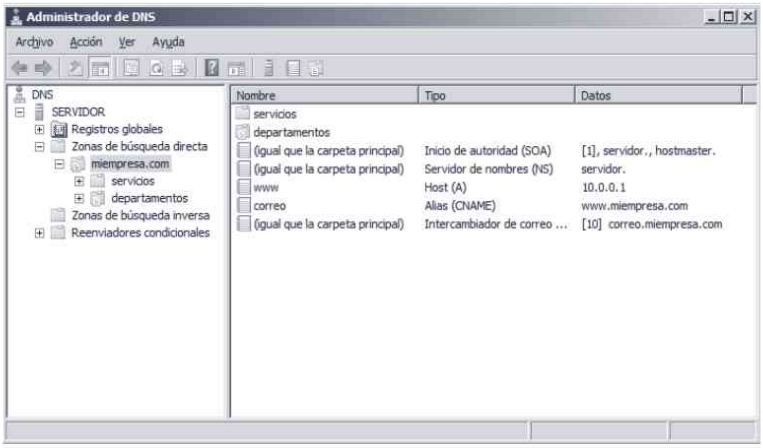


Figura 8-27. Servidor DNS

8.1.5.6 Visor de sucesos del servidor DNS

Windows proporciona el registro de eventos DNS para mantener un registro de errores, advertencias y otros sucesos ocurridos en el servidor DNS. Para configurar los eventos que va a registrar el sistema, vaya al servidor DNS, pulse el botón derecho y seleccione Propiedades. Tal y como puede ver en la figura 8-28 en la pestaña *Registro de eventos* puede indicar el tipo de información que registra: ningún evento, solo errores, errores y advertencias, o todos los eventos.

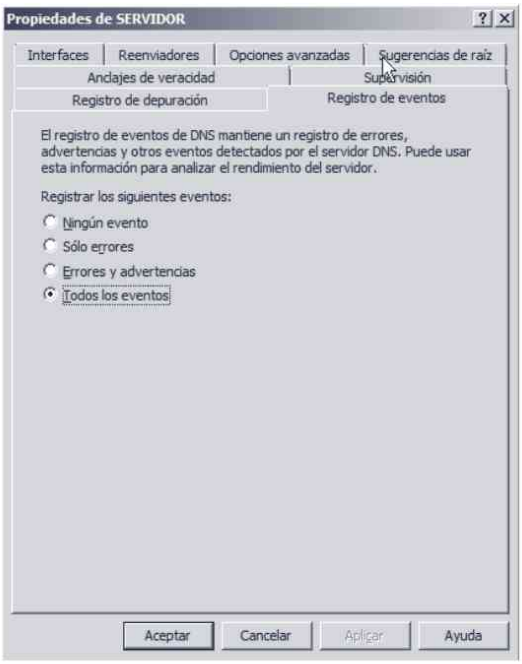


Figura 8-28. Registro de sucesos del servidor DNS

Para ver los sucesos registrados en el servidor DNS (véase la figura 8-29) en la ventana de administración DNS pulse en *Registros globales* y *Eventos DNS.*

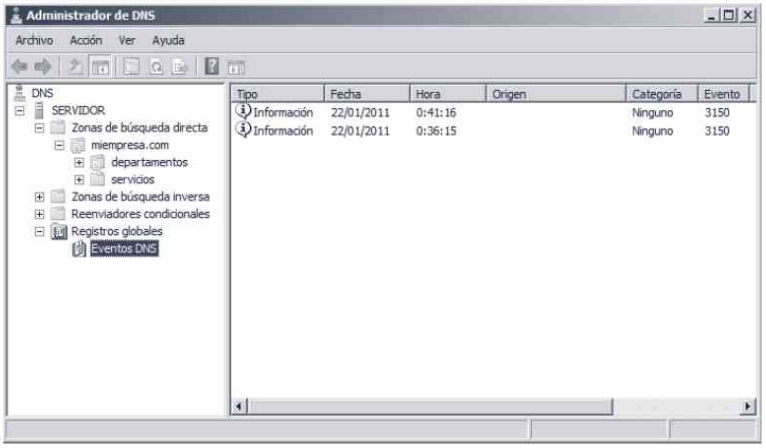


Figura 8-29. Visor de sucesos DNS

8.1.5.7 Cliente DNS

Para configurar el servidor DNS en un ordenador que actúa de cliente, vaya a *Propiedades de Protocolo (TCP/IP)* del adaptador y ponga la dirección IP del servidor DNS (véase la figura 8-14). Para comprobar su funcionamiento ejecute la orden *ping <entrada dns>* en el símbolo del sistema. Por ejemplo, en la figura 8-15 puede ver que al ejecutar el comando *ping www.miempresa.com* el servidor DNS devuelve la dirección IP 10.0.0.1.

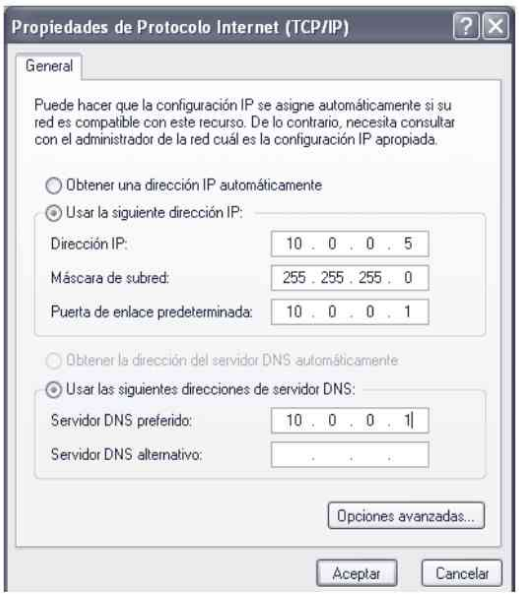


Figura 8-30. Propiedades del Protocolo Internet (TCP/IP)

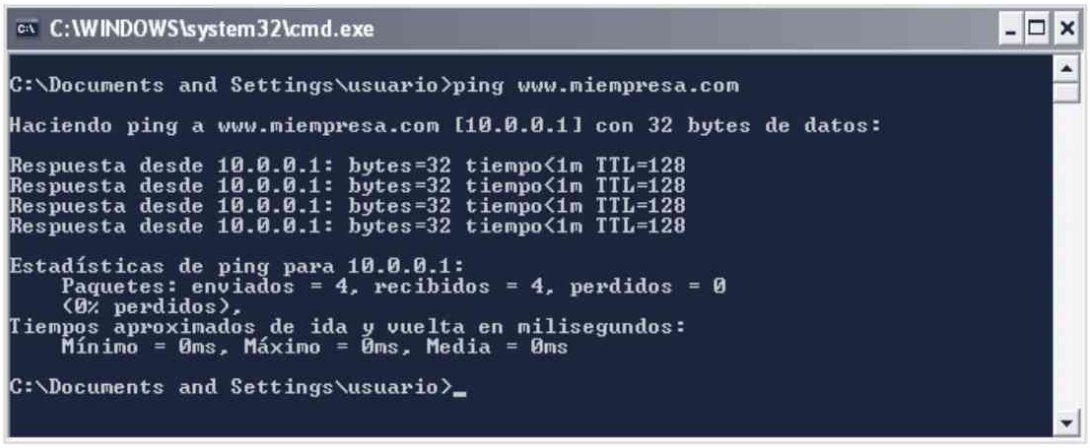


Figura 8-31. Resultado del comando ping www.miempresa.com

8.1.5.8 Seguridad

Posiblemente controlar un servidor DNS sea uno de los objetos más preciado por un hacker. Si un hacker llega a controlar un servidor DNS podrá redirigir las páginas o el tráfico de la empresa. Si se redirigen las páginas de la empresa, puede hacer que cuando se visite el portal de la empresa (p. ej., *www.miempresa.com*) se visualice otro portal distinto. Y si redirige el tráfico de la empresa, puede hacer que los datos (correos electrónicos, transacciones bancarias, etc.) pasen por un servidor que controla y con la ayuda de un sniffer registrar todos los datos.

Además de los ataques activos comentados anteriormente, también puede realizar un ataque pasivo al obtener toda la estructura interna de la red.

Para asegurar su servidor DNS, siga las siguientes medidas:

- **Implementación de zonas integradas de Active Directory.** Como se ha comentado anteriormente, las zonas integradas de Active Directory almacenan la información de zona en el contexto de nombres del dominio, en lugar de un archivo de texto en el sistema de archivos local.
- **Implantación de servidores DNS internos y externos independientes.** Incluso aunque utilice los mismos dominios en el servidor interno y externo, debería crear zonas independientes para los servidores DNS internos y externos. Los servidores externos solo deben incluir los registros de recursos DNS accesibles desde Internet. Y los DNS internos deben incluir los registros de recursos accesibles de forma interna y puede incluir los registros externos. La figura 8-16 muestra un ejemplo de arquitectura de red, donde se utilizan servidores DNS internos y externos.

- **Restringir el tráfico DNS en el servidor de seguridad.** Para restringir el tráfico DNS en el servidor de seguridad debe disponer de un servidor interno y otro externo. Puede restringir el tráfico de dos formas:
  - **Impedir que los clientes DNS externos consulten el DNS interno.** A través del cortafuegos de la zona neutra debe cerrar el puerto del servicio DNS (puerto 53 TCP y UDP) para que los clientes de Internet no tengan acceso al servidor DNS interno.
  - **Impedir que los clientes DNS internos consulten directamente los servidores DNS de Internet.** Para ello, los clientes internos deben utilizar como único servidor DNS el servidor interno de la empresa. Y el servidor interno de la empresa tendrá correctamente configurados los reenviadores para responder a cualquier petición DNS.

- **Restringir la actualización dinámica de hosts.** Las actualizaciones dinámicas permiten que los equipos DNS se registren y actualicen sus registros del servidor DNS.

- **Restricción de transferencias de zona.** Otro método que los atacantes pueden utilizar para obtener los datos de zona DNS es realizar una transferencia de zona, transfiriendo todos los registros de la zona al servidor DNS del atacante. Los atacantes pueden realizar esta tarea ejecutando el siguiente comando en la consola *nslookup*:

```
ls -d dominioDNS
```

Este comando intenta conseguir todos los registros de recursos DNS del *dominioDNS* solicitando una transferencia de zona desde el servidor DNS que ejecutó el comando *nslookup.*

Para bloquear este tipo de ataques restringa las transferencias de zona. Para ello, seleccione el dominio que quiere asegurar, pulse el botón derecho del ratón y ejecute *Propiedades*. En la pestaña *Transferencia de zona*, active la casilla *Solo a los servidores de la ficha Nombres de servidores* o active la casilla *Solo a los siguientes servidores* e introduzca la dirección del servidor DNS que tiene permiso para recibir la transferencia de zona (véase la figura 8-32).

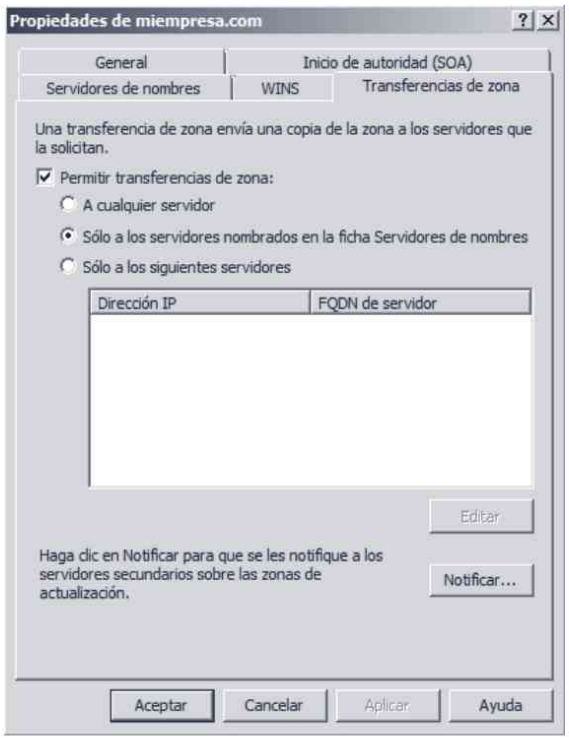


Figura 8-32. Restringir la transferencia de zona

8.2 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.

8.2.1 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:

- En el menú *Inicio* seleccione *Equipo,* pulse el botón derecho y seleccione *Propiedades.*

- En la ventana que aparece pulse en *Configuración avanzada del sistema* y pulse en la pestaña *Acceso remoto* (véase la figura 8-33).
- 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)*.

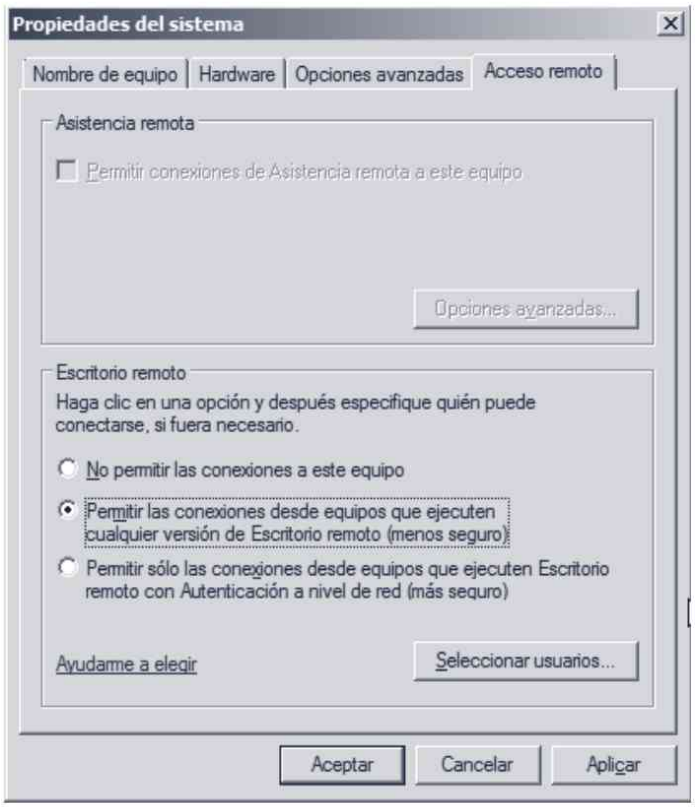


Figura 8-33. Propiedades del sistema

8.2.2 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:

- Seleccione las funciones *Host de sesión de escritorio remoto* y el *Administrador de licencias de escritorio remoto.* Pulse *Siguiente.*

- 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.*

- 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.

- Indique los grupos de usuarios que pueden utilizar los servicios y pulse *Siguiente* hasta finalizar la instalación.

- 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 8-34). 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 8-34. 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.

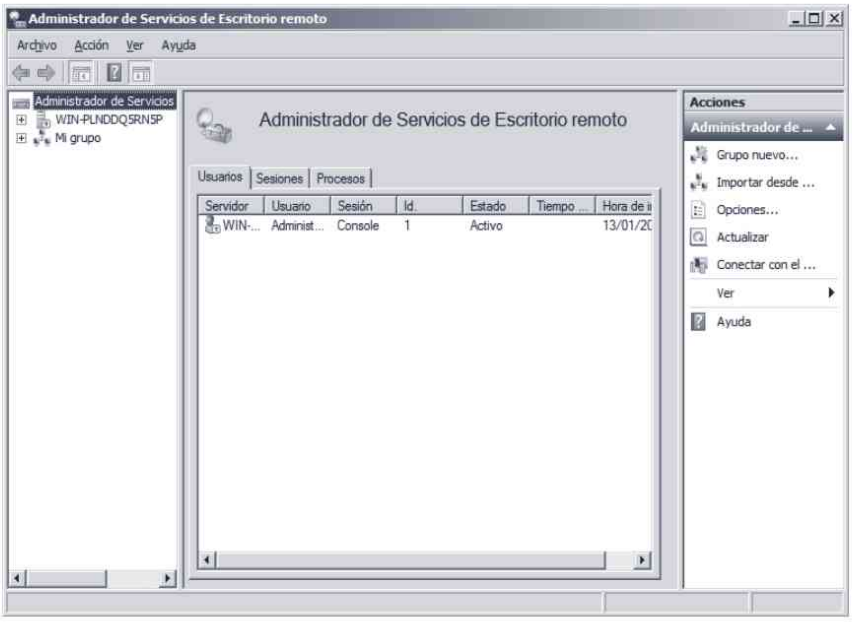


Figura 8-35. Administrador de Servicios de escritorio remoto

- **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 8-36). 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 8-37).

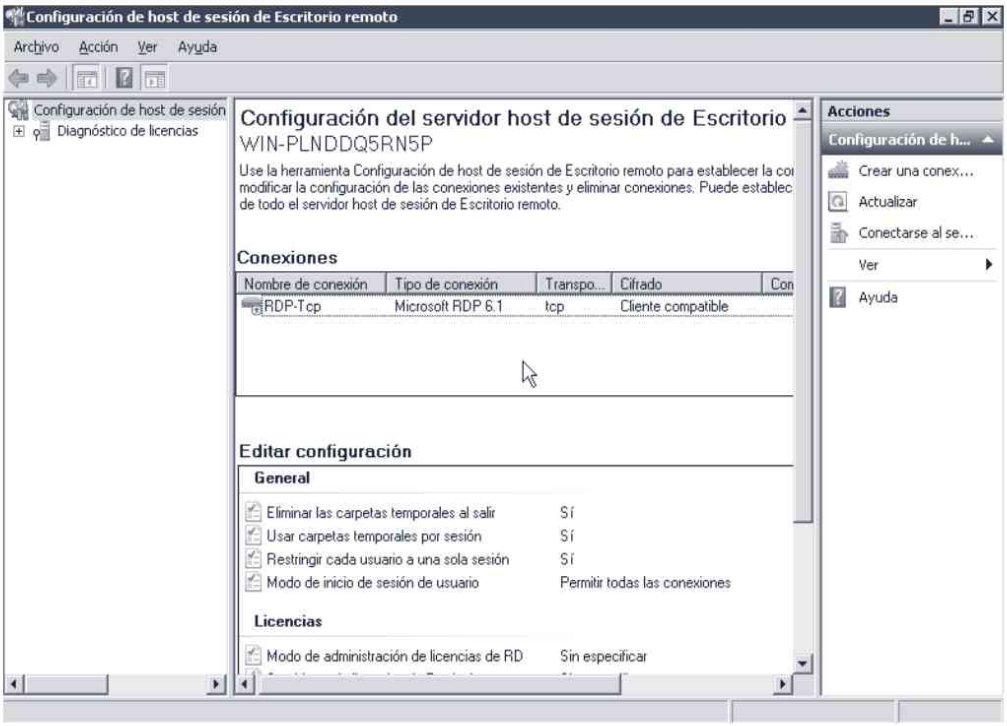


Figura 8-36. Configuración de Terminal Server

- **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.

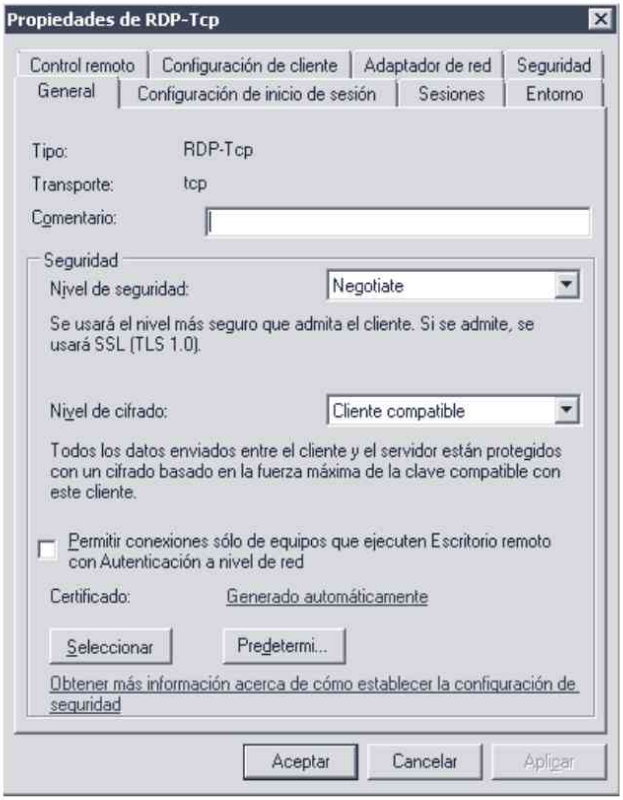


Figura 8-37. Propiedades de una conexión

8.2.3 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.

8.2.3.1 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 8-38). Si desea modificar alguna opción en la conexión al servidor (p. ej., resolución de pantalla), pulse el botón *Opciones* y se muestra un amplio menú de opciones para configurar la conexión.

Figura 8-38. Conexión a escritorio remoto

Una vez indicada la dirección del servidor pulse el botón *Conectar* para acceder al sistema (véase la figura 8-39).

Figura 8-39. Conexión a escritorio remoto

8.2.3.2 Aplicación GNU/Linux

Si desea conectarse desde un equipo GNU/Linux a un servidor Windows puede utilizar un 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 8-40 indique la dirección del servidor al que quiere conectarse y pulse *Ok.*

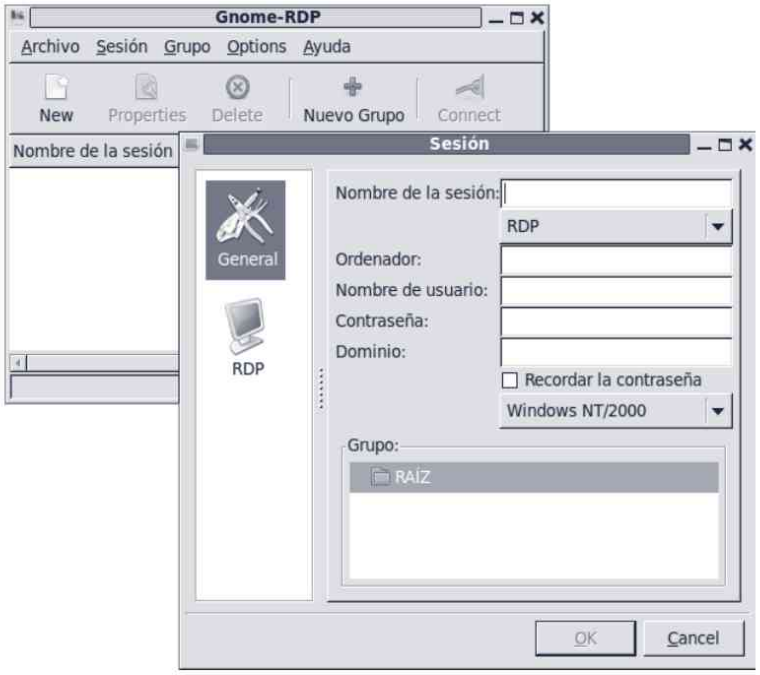


Figura 8-40. gnome-rdp (Ubuntu)

8.2.3.3 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 8-41 para tener acceso al servidor debe introducir su nombre de usuario y contraseña.

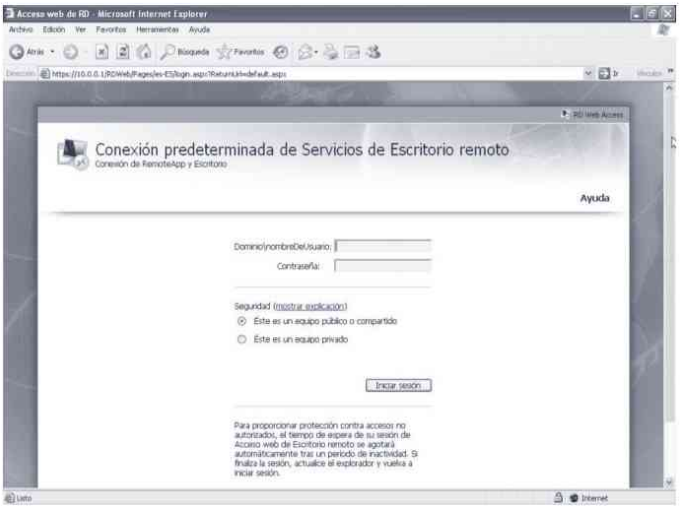


Figura 8-41. Acceso web de TS

8.3 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.

8.3.1 Instalación

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

- 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. ej., *c:\WSUS*).
- Una vez completado el proceso de instalación se inicia un asistente (véase la figura 8-42) 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.

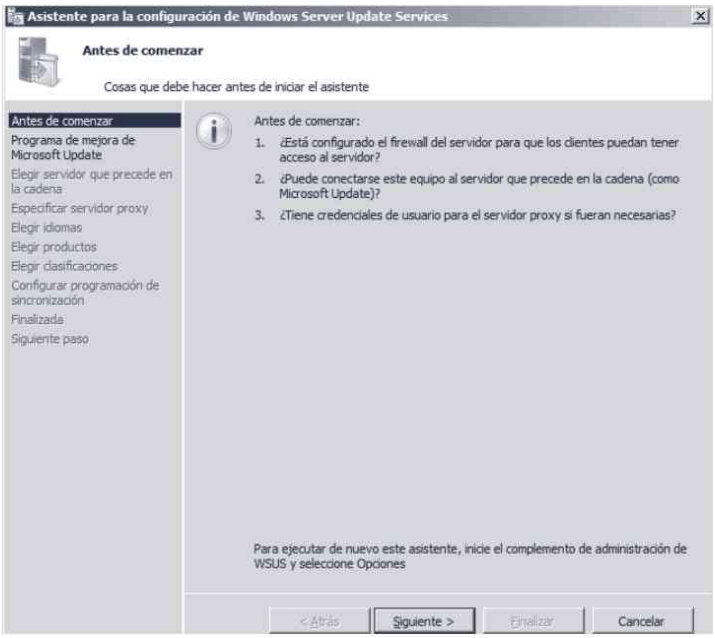


Figura 8-42. Configuración de WSUS

Nota

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

8.3.2 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 en un controlador de dominio, debe hacer que los equipos cliente utilicen el servidor WSUS y, después, configurar las actualizaciones automáticas.

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

- Ejecute el comando *gpedit.msc* y, en la ventana que aparece en la figura 8-43, acceda a *Configuración del equipo*, *Plantillas administrativas, Componentes de Windows* y finalmente Windows Update.
- 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.

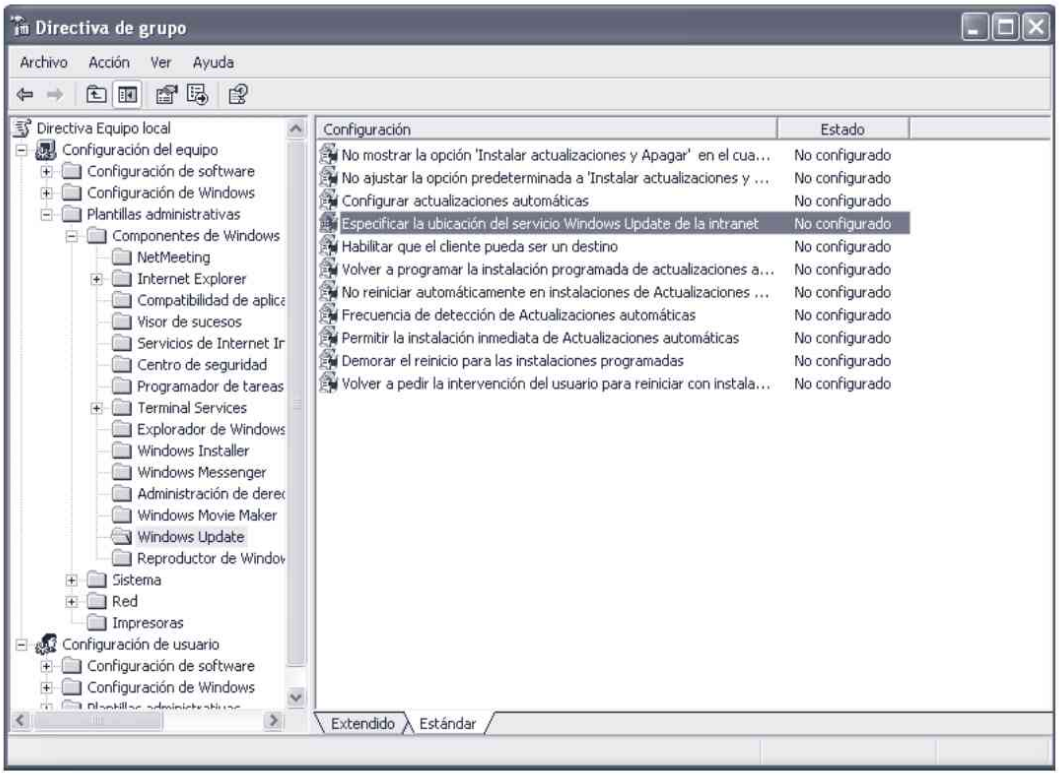


Figura 8-43. Directivas de grupo

Nota

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

8.3.3 Administración

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

8.3.3.1 Actualizaciones

Las actualizaciones son el eje principal del sistema y, por 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 8-44) 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.

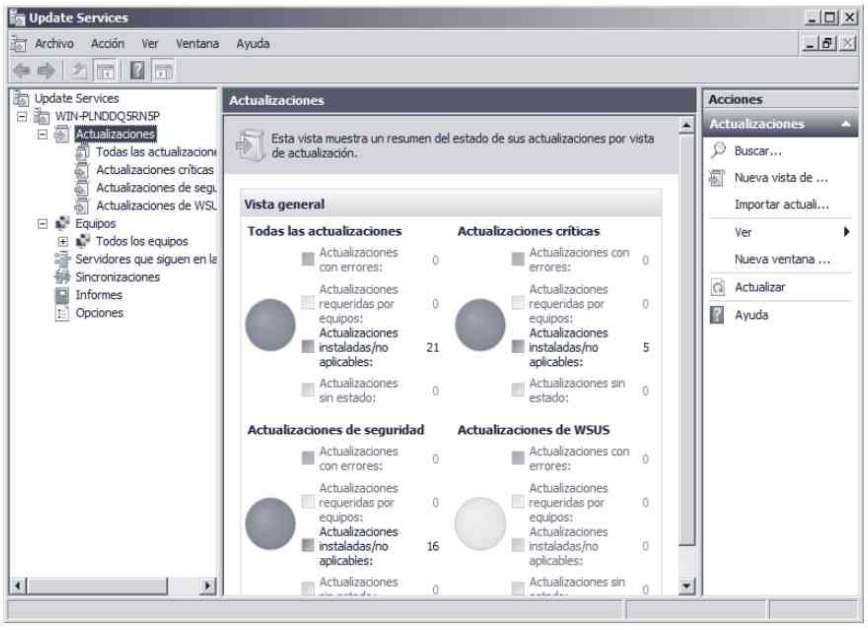


Figura 8-44. Update Services-Actualizaciones disponibles

Para aprobar una actualización tan solo necesita pulsar el botón derecho y seleccionar *Aprobar* (véase la figura 8-46).

8.3.3.2 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 8-47, para cada equipo se muestra su nombre, dirección IP, sistema operativo y estado de actualización.

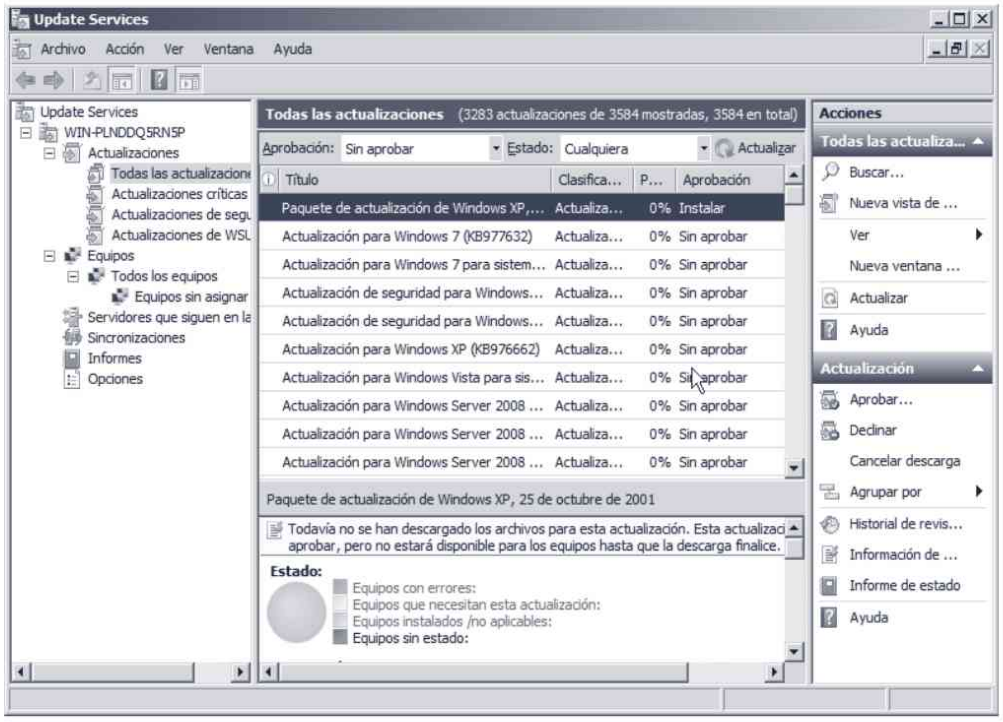


Figura 8-45. Actualizaciones

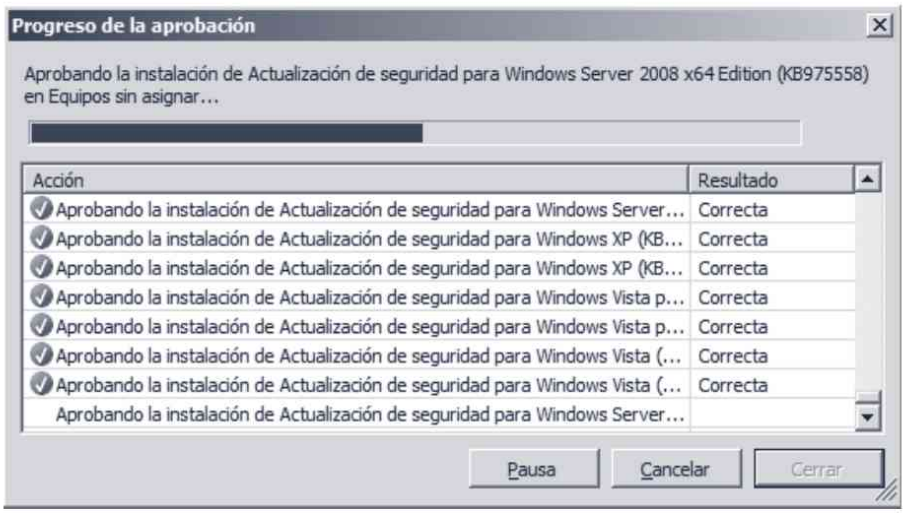


Figura 8-46. Progreso de aprobación

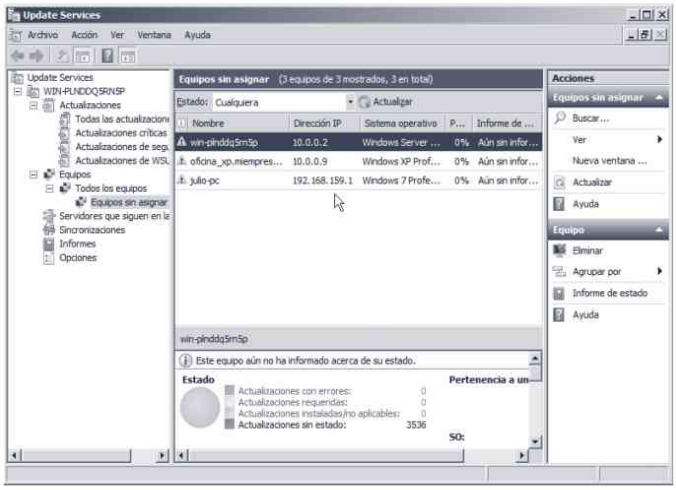


Figura 8-47. Update Services-Equipos

Si desea más información puede pulsar sobre un equipo y obtener un informe detallado de todas las actualizaciones del sistema (véase la figura 8-48).

Nota

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

8.3.3.3 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.

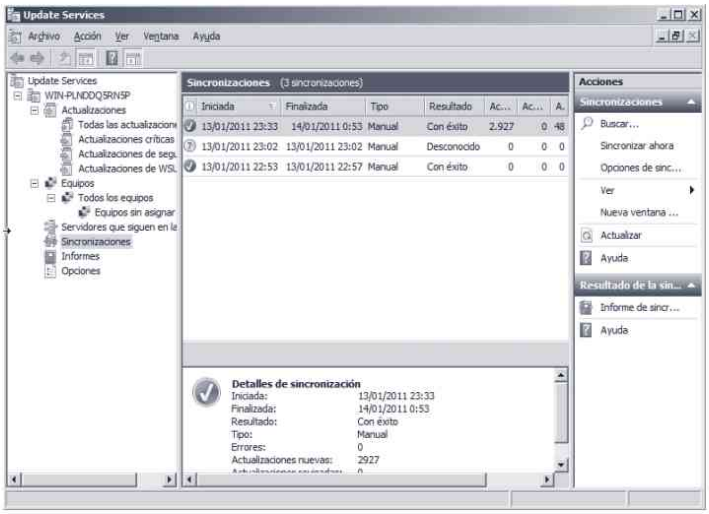


Figura 8-48. Update Services-Actualizaciones

Capítulo 9

SERVIDORES DE IMPRESIÓN Y DE ARCHIVOS

9.1 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 Linux.

9.1.1 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 9-1) 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.*

Nota

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

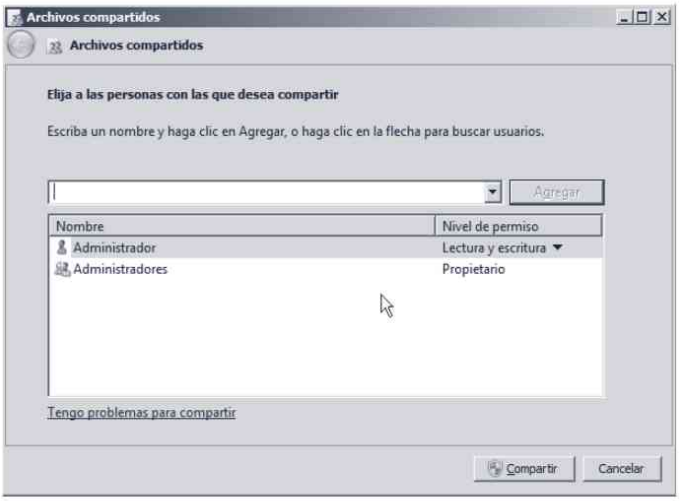


Figura 9-1. Propiedades de Carpeta (Compartir)

Si desea ver los recursos compartidos del equipo entonces acceda a *Equipo* y en el menú de la derecha pulse en *Red* (véase la figura 9-2).

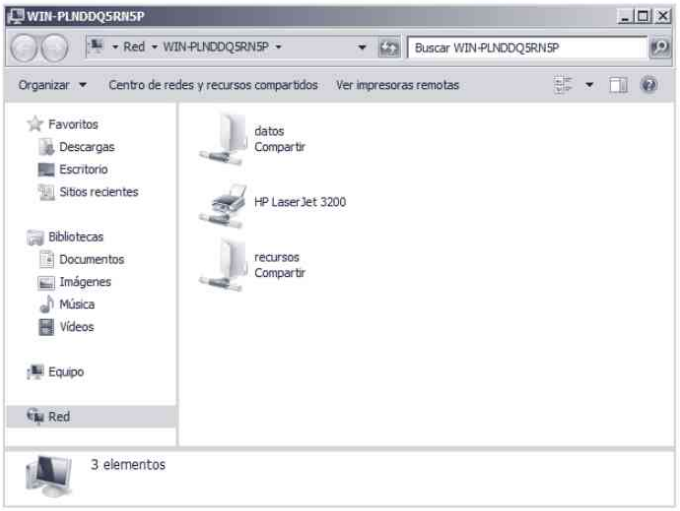


Figura 9-2. Recursos compartidos del equipo

Nota

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.

9.1.2 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 9-3).

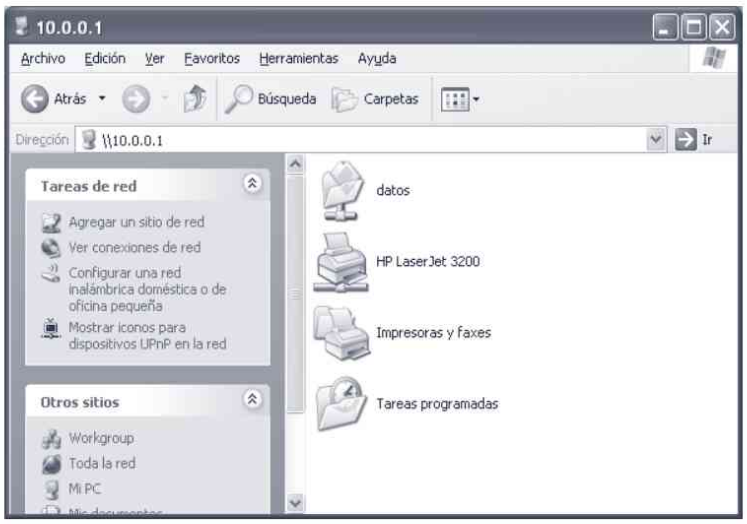


Figura 9-3. Recursos compartidos de un equipo

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 9-4, 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 9-4. Conectar a unidad de red

Nota

Si quiere montar la carpeta por comandos debe ejecutar:

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

9.1.3 Administrar recursos compartidos

Para administrar de forma centralizada todos los recursos compartidos, conexiones, archivos abiertos,... hay que utilizar la herramienta administrativa *Administración de almacenamiento y recursos compartidos* (véase la figura 9-5).

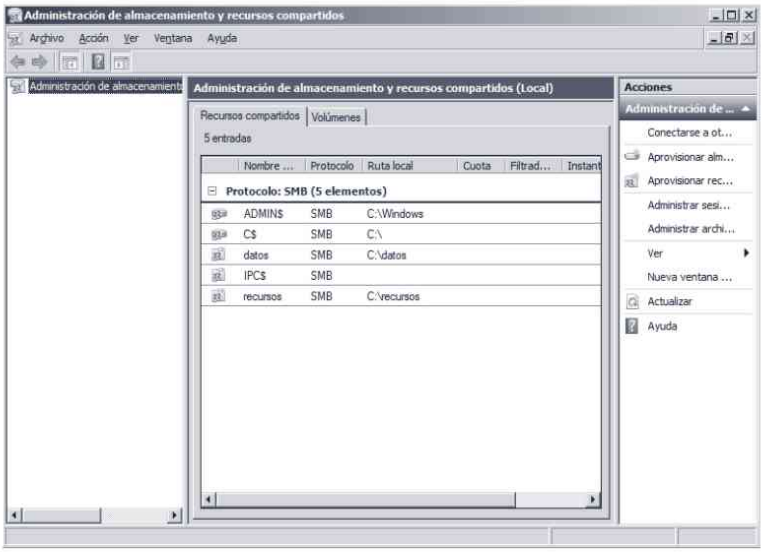


Figura 9-5. Administración de almacenamiento y recursos compartidos

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 9-6).

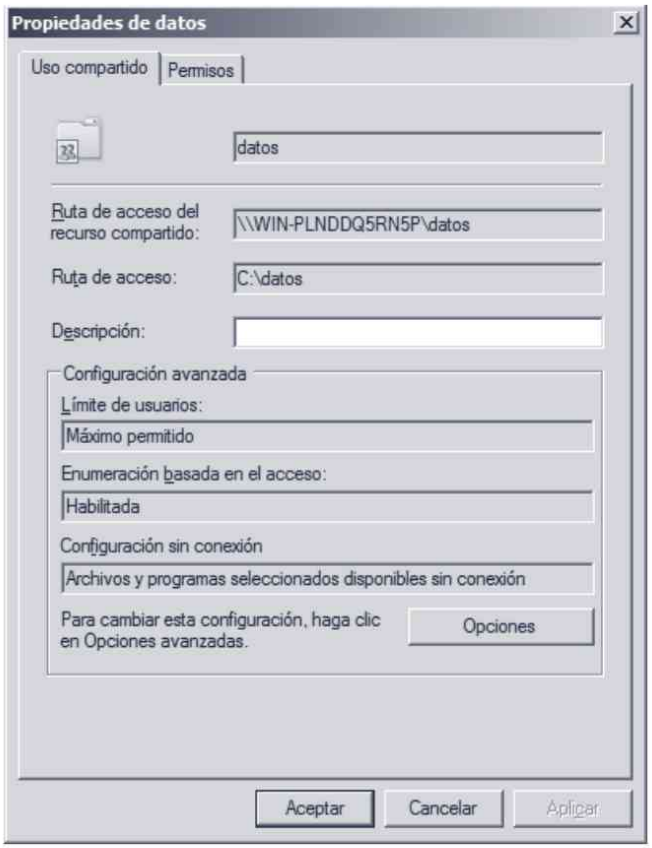


Figura 9-6. Propiedades de un recurso compartido

9.1.4 Instantáneas

Las instantáneas permiten a los usuarios ver el contenido de las carpetas compartidas en momentos anteriores. La utilización de instantáneas es muy 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:

- Seleccione una unidad de disco, pulse el botón derecho y seleccione *Propiedades.*
- Pulse en la pestaña *Instantáneas* (véase la figura 9-7), 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.

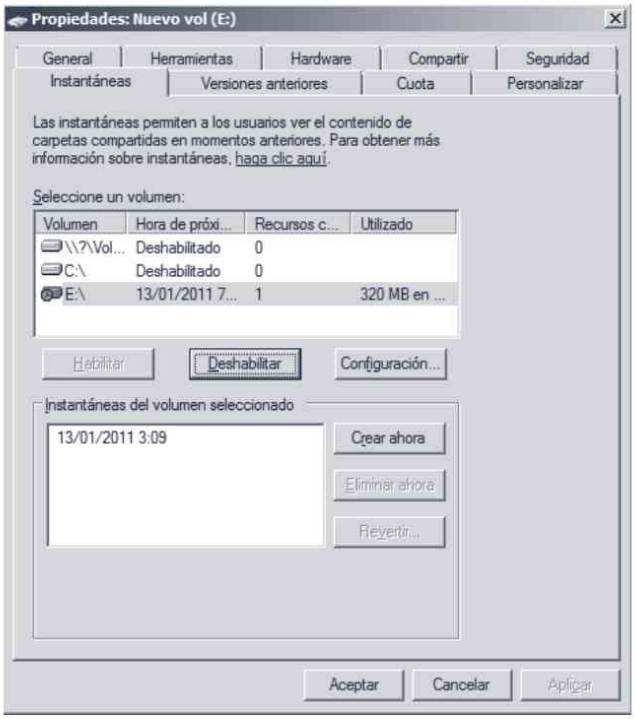


Figura 9-7. Habilitar las instantáneas

Para personalizar las instantáneas del equipo pulse el botón *Configurar* y en la ventana que aparece en la figura 9-8 puede establecer dónde se guardan, cuándo se ejecutan y el tamaño máximo que pueden ocupar en disco.

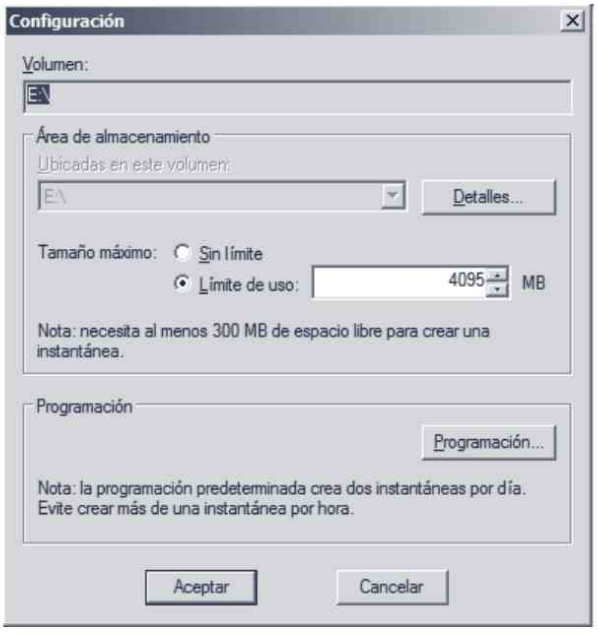


Figura 9-8. Configuración de las instantáneas

Nota

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 9-9). Sobre una versión puede ver su contenido, copiar su contenido en un directorio o restaurar la versión.

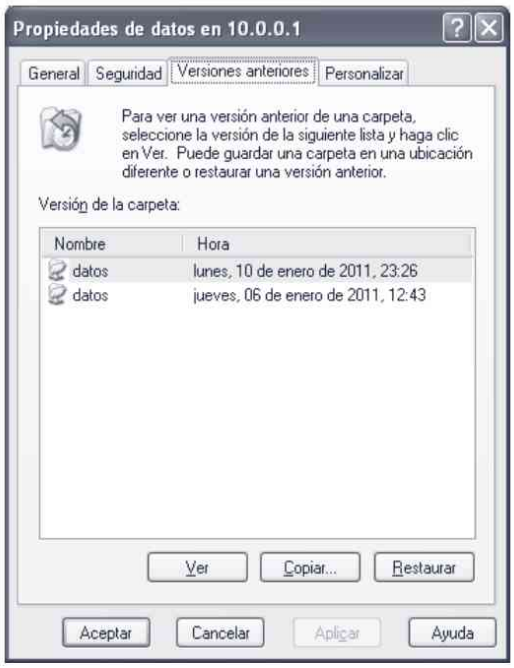


Figura 9-9. Instantáneas (Cliente)

9.1.5 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 redes 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 9-10 seleccione la opción *Sistema 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 ahora el recurso compartido y se creará más adelante.

Figura 9-10. Instalando DFS

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

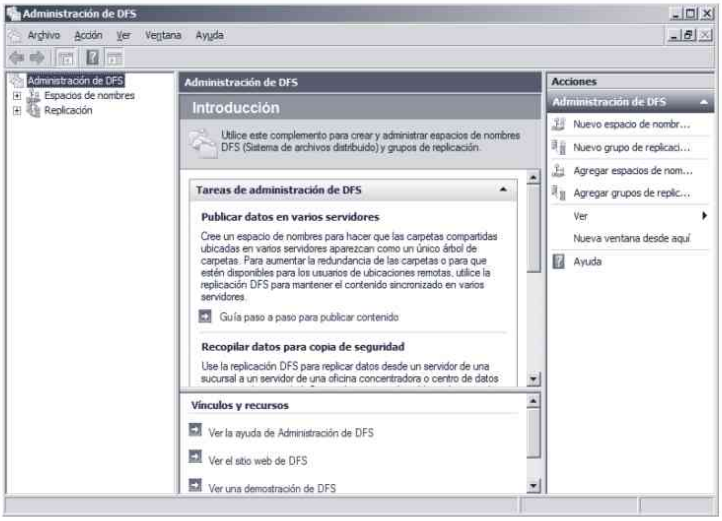


Figura 9-11. Administrador de DFS

9.1.5.1 Crear espacio de nombres

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:

- En el *Administrador de DFS* (véase la figura 9-11) seleccione *Espacio de nombres*, pulse el botón derecho y seleccione *Crear nuevo espacio de nombres* para iniciar el asistente que le guía durante todo el proceso (véase la figura 9-12).

Figura 9-12. Crear espacio de nombres

- Indique el nombre del servidor donde se aloja el espacio de nombres.
- Escriba el nombre del espacio de nombres.
- 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.ej., *\\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. ej., *\\10.0.0.1\recursos*).

- 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.

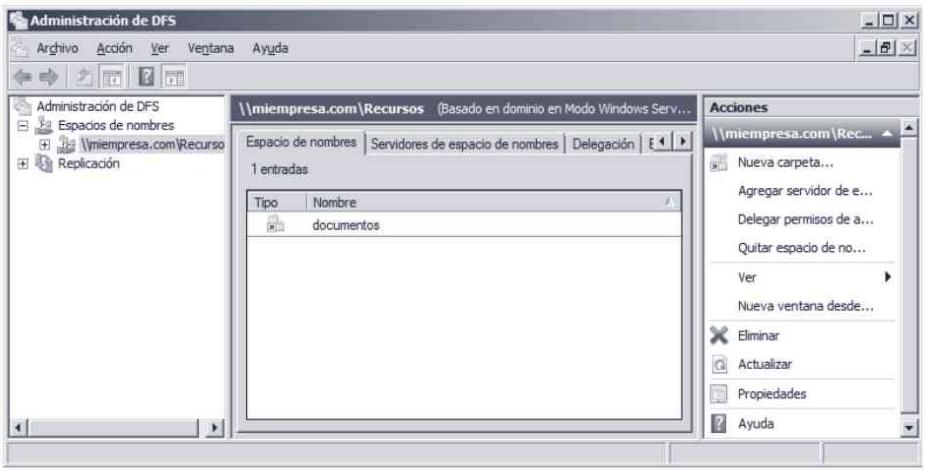


Figura 9-13. Espacio de nombres

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

Nota

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 donde se almacena el espacio de nombres pulse en la pestaña *Servidores de espacio de nombres* (véase la figura 9-14).

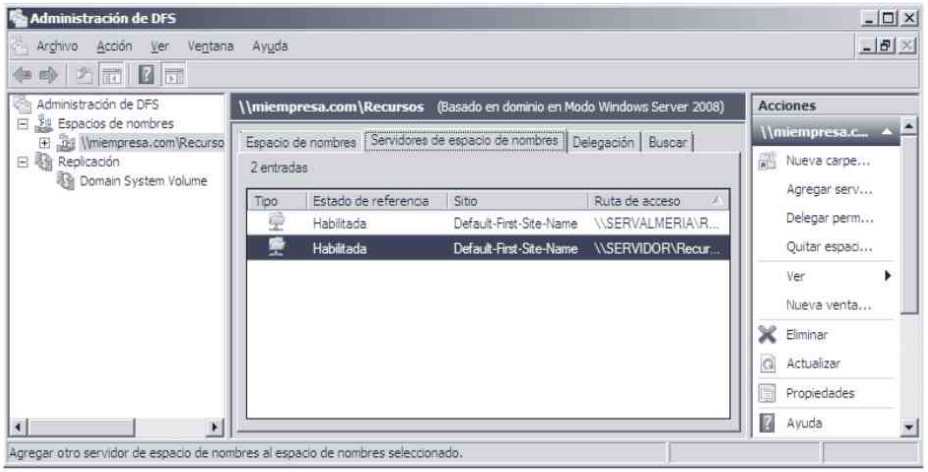


Figura 9-14. Servidores de espacio de nombres

- **Activar la replicación de datos.** La replicación de datos permite 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 9-14), pulse el botón derecho, seleccione la opción *Replicar carpeta…* y se inicia el asistente, que se muestra en la figura 9-15, en el que debe realizar los siguientes pasos:
  - Escriba el nombre del grupo de replicación y el nombre de la carpeta replicada.

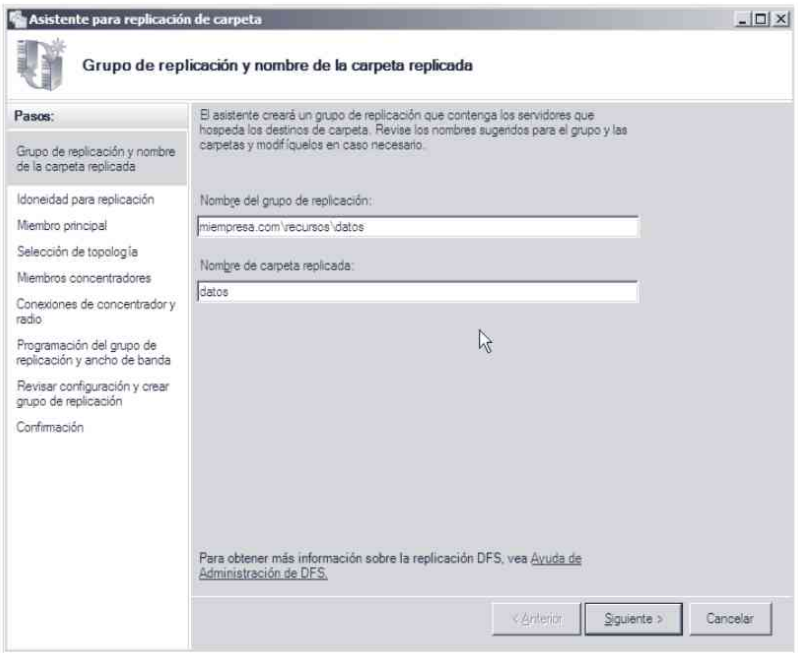


Figura 9-15. Crear grupo de replicación de datos

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

Nota

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.

9.2 SERVIDORES DE IMPRESIÓN

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

Existen dos formas de compartir una impresora 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, permite migrar servidores de impresión e implementar conexiones de impresora mediante la directiva de grupo.

9.2.1 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 9-16, seleccione la impresora, pulse el botón derecho y seleccione *Propiedades de la impresora*.

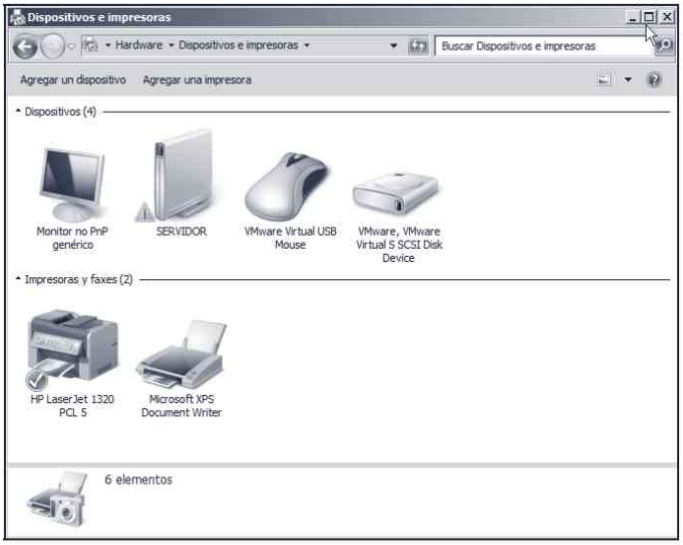


Figura 9-16. Panel de control - Impresoras

Tal y como puede ver en la figura 9-17, 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.

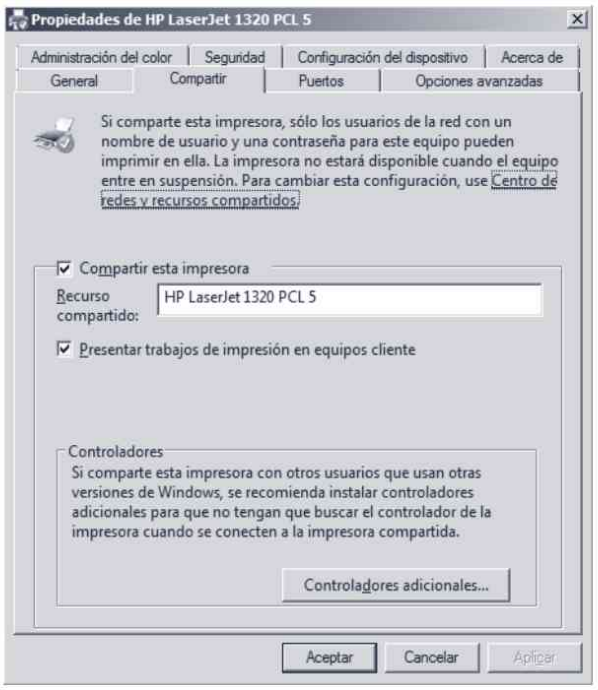


Figura 9-17. Compartir impresora

Si quiere establecer los permisos de acceso sobre la impresora acceda a la pestaña *Seguridad* y, en la ventana que aparece en la figura 9-18, puede establecer los permisos de los diferentes usuarios y grupos que tienen acceso a la impresora.

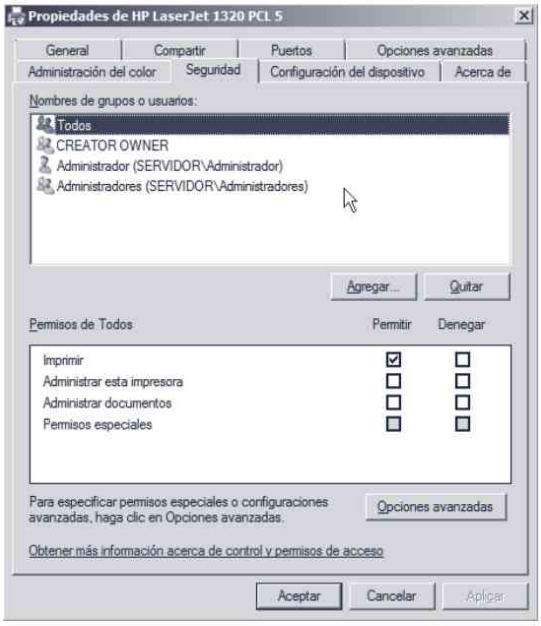


Figura 9-18. Permisos de acceso a la impresora

Para administrar los trabajos puede acceder a la impresora y ver todos los trabajos que tiene pendientes así como sus características (véase la figura 9-19). Además, para cada trabajo puede *Pausarlo*, *Cancelarlo* o *Reiniciarlo.*

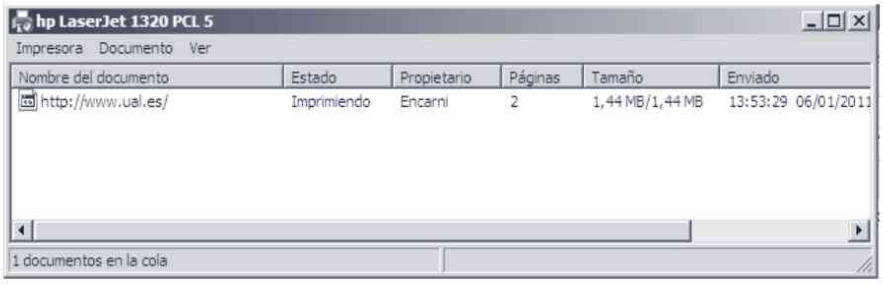


Figura 9-19. Trabajos de la impresora

9.2.2 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.
- **Servidor de digitalización distribuida.** Recibe documentos de escáneres de red y los envía a destinos correctos.

Figura 9-20. 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 9-21) permite administrar las impresoras del servidor así como todos sus trabajos.

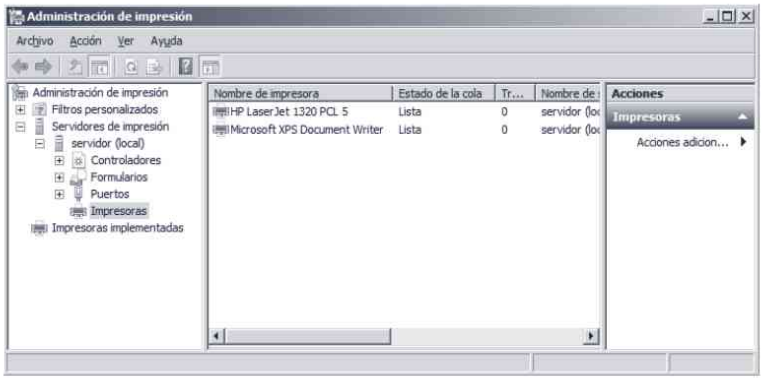


Figura 9-21. Administración de impresión

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 9-22 puede activar las notificaciones por correo electrónico o hacer que el sistema ejecute automáticamente un script cada vez que se produzca una incidencia.

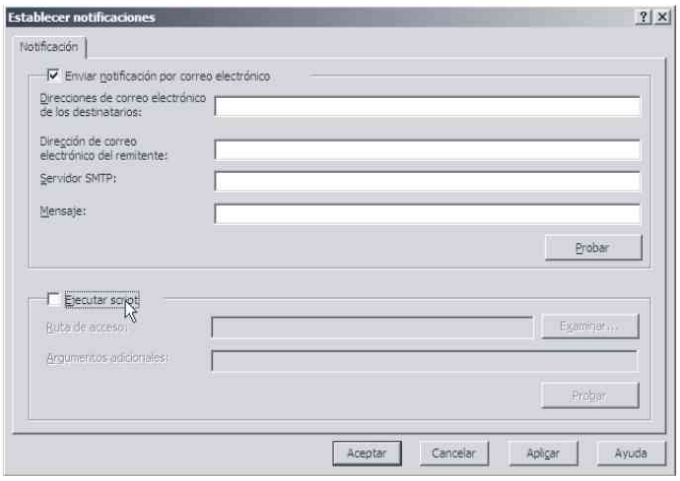


Figura 9-22. Establecer notificaciones

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. ej., *http://10.0.0.01/printers*).

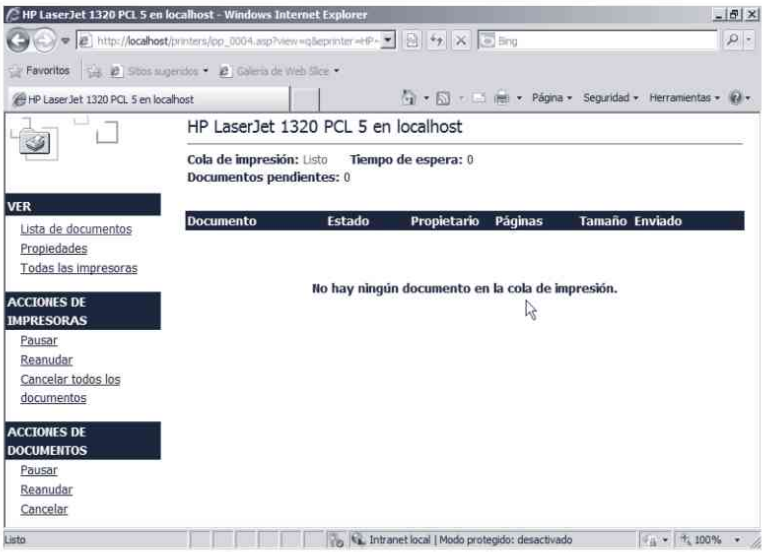


Figura 9-23. Administración web de impresión

9.2.3 Cliente

Para utilizar una impresora compartida en un equipo cliente primero hay acceder al servidor que tiene la impresora e instalarla en el equipo. Para instalar la impresora, en el equipo cliente, hay que acceder al servidor escribiendo su dirección (p. ej., **\\10.0.0.1**) y al introducir los datos de usuario puede ver los recursos que comparte el servidor. Por ejemplo, en la figura 9-24 puede ver que el servidor 10.0.0.1 comparte la impresora *Hp laserJet 1320 PCL5.*

Figura 9-24. 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 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 9-25).

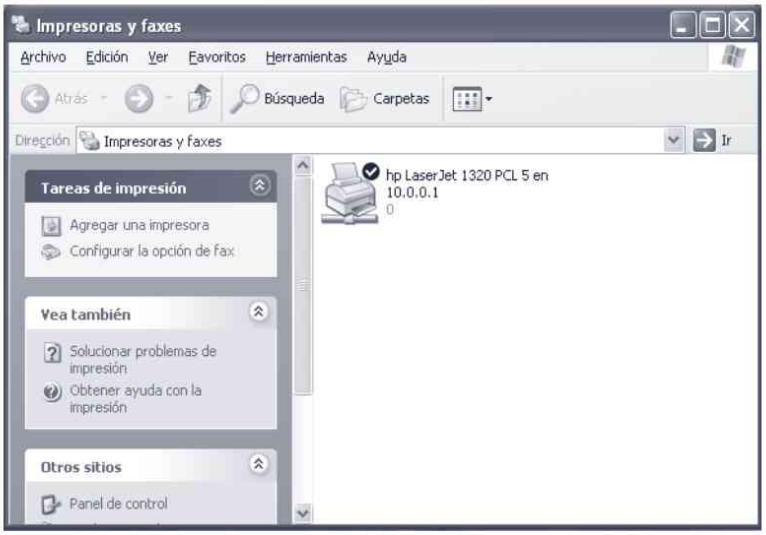


Figura 9-25. Impresora instalada

Capítulo 10

SERVICIOS DE INTERNET

Windows proporciona un conjunto de servicios que ofrecen soporte por parte del servidor para los protocolos de Internet más populares en el nivel de las aplicaciones, lo que permite que el servidor actúe como un servidor web o servidor de FTP. Los servicios básicos de Internet se hallan completamente integrados a través de Internet Information Server (IIS).

Otro servicio muy utilizado es el correo electrónico. Microsoft Exchange 210 Server es el servidor de correo electrónico de Microsoft y está diseñado para cubrir las necesidades de cualquier organización, grande o pequeña, acerca de colaboración y mensajería.

10.1 SERVIDOR WEB

10.1.1 Instalación

Para instalar el servicio web acceda a la herramienta administrativa *Administre su servidor*, pulse en *Agregar roles* y seleccione *Servidor web (IIS).* En la ventana que aparece en la figura 10-1, si es necesario, seleccione el tipo de tecnología para el desarrollo de aplicaciones (p. ej., ASP, ASP.NET, CGI) y para mejorar la seguridad del servidor web seleccione las opciones *Filtros ISAPI* y *Restricciones de IP y dominio.*

Figura 10-1. Agregar rol servidor web (IIS)

Una vez completado el proceso de instalación, para ver que el servidor web funciona correctamente acceda a un navegador y escriba la dirección *http://localhost* (véase la figura 10-2).

Figura 10-2. Servidor web (página de inicio – remota)

Si desea cambiar la página web inicial acceda al directorio *c:\inetpub\wwwroot* y modifique el contenido del directorio por la web que estime oportuna.

10.1.2 Administración

Para administrar el servidor inicie el *Administrador de Internet Information Services (IIS)* que se encuentra en *Herramientas administrativas* y haga clic sobre el servidor. Como puede ver en la figura 10-3, desde esta herramienta posee acceso directo a todo tipo de operaciones sobre el servidor.

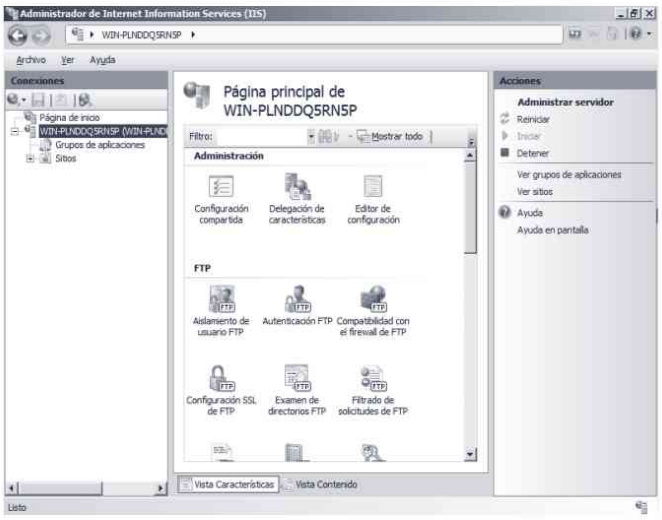


Figura 10-3. Servidor web (Administración del servidor)

Por defecto, IIS tiene habilitado el sitio web *Default* que aloja la web por defecto del servidor y que se encuentra en el directorio *c:/inetpub/www*. Si desea configurar el sitio web por defecto o añadir nuevos sitios, pulse en *Sitios* (véase la figura 10-4).

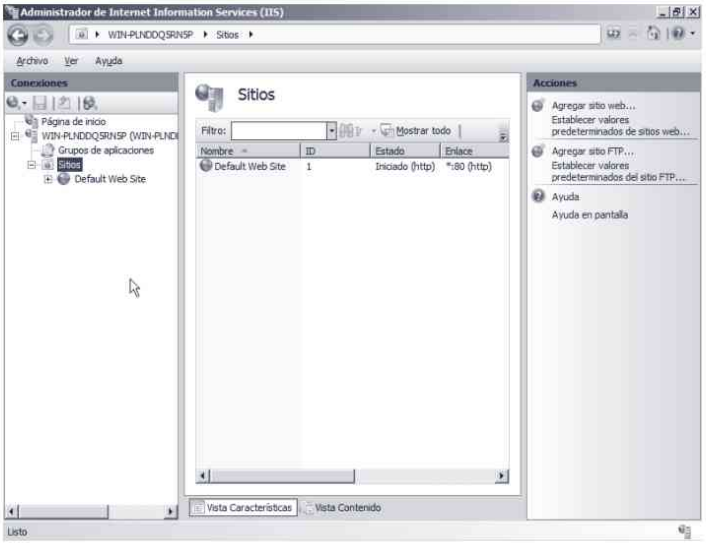


Figura 10-4. IIS - Sitios

Para configurar un sitio web seleccione el sitio web, pulse el botón derecho del ratón y seleccione *Administrar sitio web...* y *Configuración avanzada* (véase la figura 10-5). A continuación se explican los parámetros más importantes:

- **Enlaces.** Se configura al crear el sitio web y permite especificar la combinación de IP, puerto y nombre del host por donde se atienden las peticiones.
- **Inicio automático.** Permite indicar si el sitio web se inicia automáticamente al iniciar el sistema.
- **Ruta física.** Directorio del disco duro donde se encuentra el sitio web.
- **Límite de conexión.** Permite limitar el uso de la red que utiliza el sitio web. La limitación de la red se puede realizar por número de conexiones o por el ancho de banda consumido.
- **Protocolos habilitados.** Especifica los protocolos que se pueden utilizar para obtener acceso a una aplicación. El valor predeterminado es http que habilita los protocolos HTTP y HTTPS.

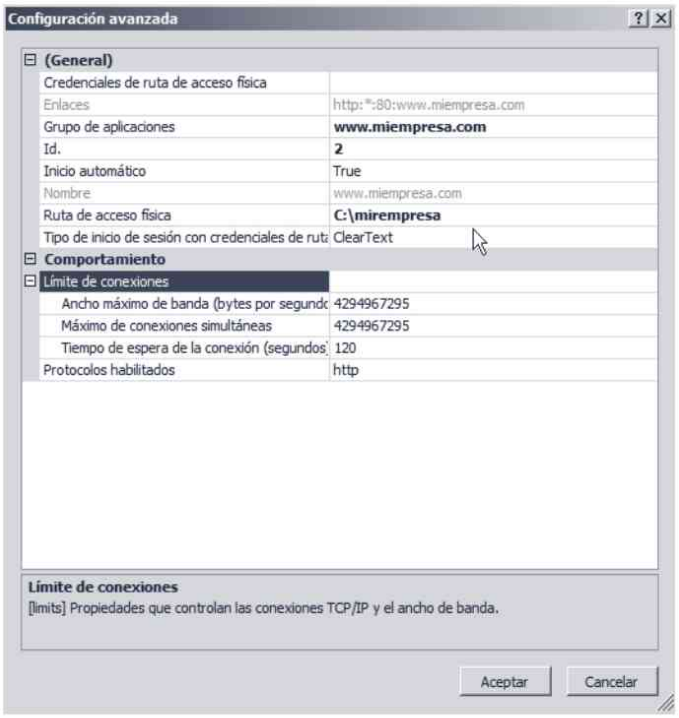


Figura 10-5. Configuración avanzada de un sitio web

Además de esta configuración avanzada, existen otros métodos también sencillos para configurar las características del sitio web. Por ejemplo, puede modificar la configuración básica (nombre del sitio, grupo de aplicaciones, ruta de

acceso física...) haciendo clic en *Configuración básica* que se encuentra en el menú de la derecha *Modificar sitio* (véase la figura 10-6).

Figura 10-6. Configuración básica de un sitio web

En la parte central de la ventana del sitio web (véase la figura 10-7) además de poder ver el contenido del sitio web dispone de numerosos accesos directos para la administración del sitio. Por ejemplo, puede configurar cualquier elemento del sitio (p. ej., *Permisos del Administrador de IIS*, *ASP.NET*). Los elementos de configuración más importantes son:

- **Almacenamiento en caché de resultados.** Permite especificar las reglas para almacenar el contenido servido en la caché de resultados.
- **Asignaciones de controlador.** Permite indicar recursos que controlen respuestas para los tipos de solicitud específicos.
- **Autenticación.** Permite configurar la autenticación tanto para el sitio como para las aplicaciones.
- **ASP, CGI, etc.** Permite realizar la configuración relativa a los diferentes tipos de aplicaciones.
- **Compresión.** Permite establecer la compresión de las respuestas.
- **Configuración de SSL.** Permite especificar los requisitos para los certificados de cliente y Secure Socket Layer (SSL).
- **Documento predeterminado.** Permite establecer el nombre del archivo predeterminado que se devuelve en una respuesta cuando una solicitud no indica ningún archivo.
- **Encabezados de respuesta HTTP.** Permite configurar encabezados HTTP para ser agregados en las respuestas del sitio.

- **Examen de directorios.** Permite establecer la información que se muestra cuando se examinan los directorios.
- **Filtros ISAPI.** Permite especificar los filtros ISAPI que desea utilizar. Un filtro ISAPI es un programa que responde a sucesos durante el procesamiento de una petición.
- **Módulos.** Permite configurar los diferentes módulos para el procesamiento de solicitudes en el servidor web.
- **Páginas de errores.** Existe la posibilidad de personalizar las páginas de error del sitio web.
- **Redirección HTTP.** Permite especificar reglas para redireccionar ciertas solicitudes a otro archivo o dirección URL.
- **Registro.** Permite configurar la forma en la que el servidor registra las solicitudes.
- **Reglas de autorización.** Permite configurar las reglas para autorizar a los usuarios a obtener acceso para aplicaciones y sitios web.
- **Restricciones de direcciones IPv4 y dominios.** Permite restringir o permitir el acceso a contenido web dependiendo de la dirección IP o el dominio origen de la solicitud.
- **Tipos MIME.** Para poder configurar extensiones y tipos de contenidos asociados.

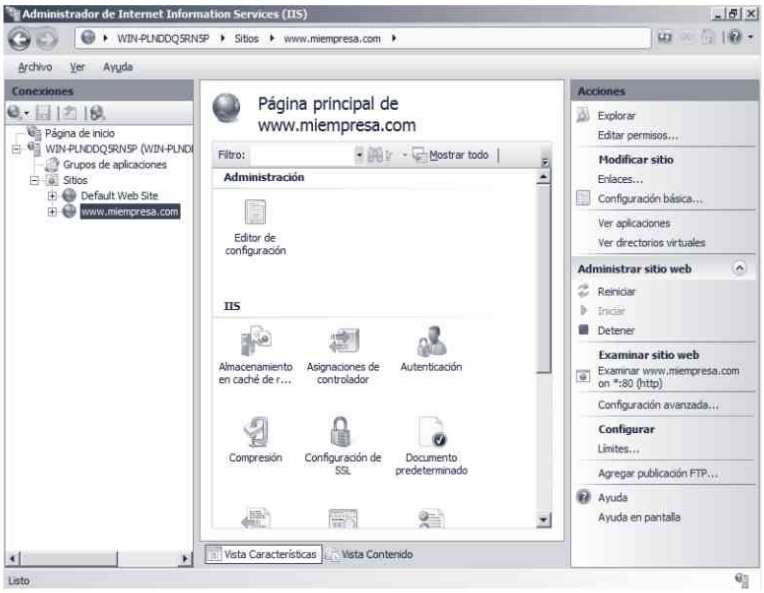


Figura 10-7. Sitio web en IIS

10.1.3 Creación de un nuevo sito web

Antes de crear un nuevo sitio web es necesario configurar el servidor DNS para que la entrada del dominio (p. ej., *www.miempresa.com*) apunte a la dirección IP del servidor web. Si desea información sobre servidores DNS consulte el *Capítulo 8. Administración de la red.*

Seguridad

Si su portal es público asegúrese que tiene configuradas correctamente las entradas de los DNS en Internet.

Una vez que tiene la entrada DNS activa, para crear un nuevo sitio web realice los siguientes pasos:

- Pulse el botón derecho sobre *Sitios web* y seleccione en el menú contextual la opción *Agregar sitio web* para abrir la ventana que le permitirá introducir los datos del sitio (véase la figura 10-8). Como mínimo, debe introducir el nombre del sitio (p. ej., *www.miempresa.com*), la ruta de acceso físico donde se encuentra el sitio web (p. ej., *c:\inetpub\miempresa*) y el nombre del host por donde el servidor recibe las peticiones (*www.miempresa.com*).

- Marque la casilla *Iniciar sitio web inmediatamente*.

- Pulse el botón *Aceptar* para guardar la información y crear (e iniciar si lo consideró) el sitio.

Cuando finalice el proceso puede ver el nuevo sitio web dentro de la categoría *Sitios web*. Una vez creado ya puede realizar toda la configuración que se ha visto en el apartado anterior. Se recomienda configurar en primer lugar los permisos de acceso que desea definir para el directorio principal de su servidor haciendo clic con el botón derecho en el nombre del sitio y eligiendo *Editar permisos*. Podrá permitir o denegar para los usuarios y grupos de usuarios las siguientes acciones: Control total, Modificar, Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura, Escritura, y Permisos especiales.

Figura 10-8. Creación de un nuevo sitio web

Seguridad

Es recomendable almacenar los documentos de los servidores web en una unidad de disco independiente de los datos del sistema operativo. La unidad debe tener el sistema de ficheros NTFS.

Para comprobar que su sitio está configurado correctamente cree en el directorio raíz del sitio web (especificado durante la instalación) una página web con nombre *default.htm*. Escriba en el navegador la dirección del dominio (en el ejemplo, *http://www.miempresa.com*) y podrá ver su página web (véase la figura 10-9).

Más información

De forma predeterminada se habilita el registro que almacena todas las peticiones que recibe el sitio web. El registro se encuentra en %SystemDrive%\inetpub\logs\LogFiles.

Figura 10-9. Página de prueba del dominio http://www.miempresa.com

10.1.4 Creación de un directorio virtual

Un sitio web sirve todos los archivos y carpetas que se encuentran en su directorio de trabajo (por defecto, *c:\inetpub\wwwroot*). Si desea publicar una determinada carpeta puede copiarla dentro del directorio de trabajo. Pero si quiere publicar una carpeta que se encuentra en otro directorio y conservar su ubicación original entonces tiene que crear un directorio virtual. Un directorio virtual permite que el servidor web pueda publicar una carpeta que no se encuentra en el directorio de trabajo.

Para crear un directorio virtual, seleccione el servidor web, pulse el botón derecho y seleccione *Agregar directorio virtual* para abrir la ventana que le permitirá introducir toda la información necesaria (véase la figura 10-10).

La información que debe cumplimentar es la siguiente:

- Escriba el alias que quiere utilizar para el directorio virtual.
- Escriba la ruta de acceso física a la carpeta donde se ubica el contenido.
- Indique cómo será la conexión al directorio virtual (credenciales de ruta de acceso para usuario específico o de usuario de una aplicación –autenticación de paso a través–).
- Pulse el botón *Aceptar* para añadir el directorio virtual.

Figura 10-10. Agregar directorio virtual a un sitio web

Una vez creado el directorio virtual aparece en la vista del sitio web (véase la figura 10-11).

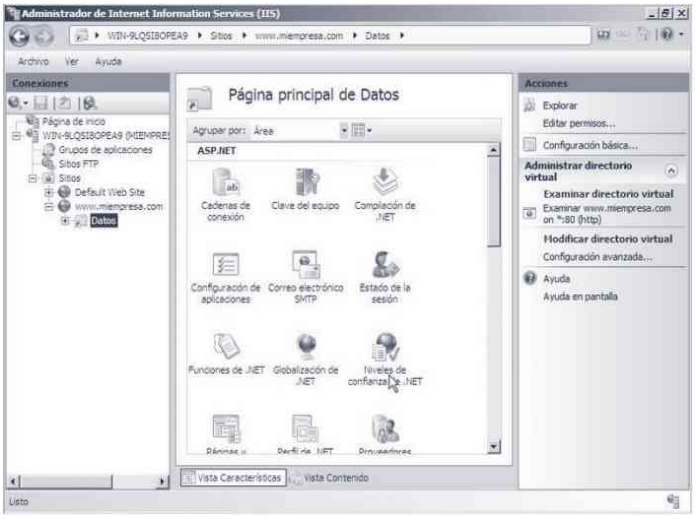


Figura 10-11. Nuevo directorio virtual dentro del sitio web

10.1.5 Extensiones de servicio web

Con el fin de adoptar una actitud previsora contra usuarios malintencionados y atacantes, IIS no se instala de forma predeterminada en Windows 2008. Además el servicio IIS se instala inicialmente en modo altamente seguro. De forma predeterminada, IIS solo sirve contenido estático, por lo que algunas de las extensiones (p. ej., ASP o CGI) no funcionan a menos que se habiliten.

En la parte central de la ventana de servidor web (véase la figura 10-12) disponemos de accesos directos a estas extensiones y que permiten configurarlas según nuestras necesidades. Es muy importante utilizar el acceso *Asignaciones de controlador*, donde puede:

- Permitir o prohibir determinadas extensiones de servicio web.
- Agregar nuevas extensiones de servicio web.
- Permitir las extensiones de servicio web a las que puede llamar una aplicación específica.
- Prohibir que se ejecuten todas las extensiones de servicio web en el equipo local.

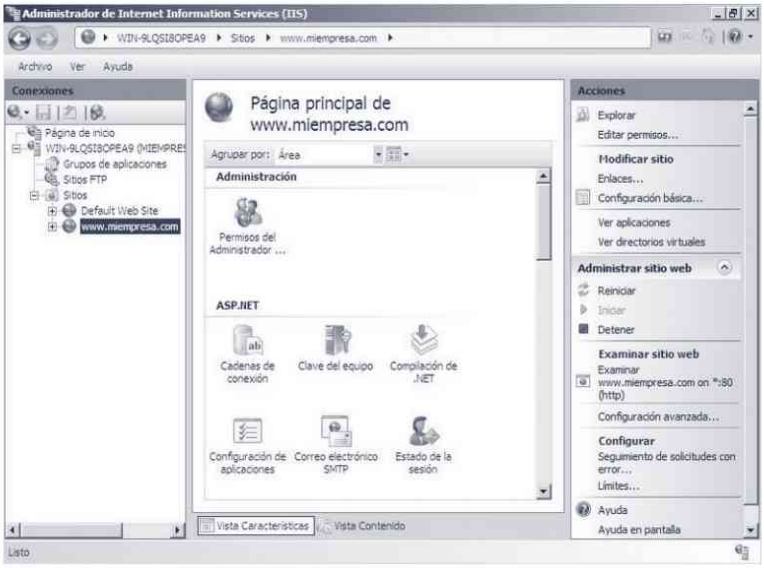


Figura 10-12. Servidor web

10.1.6 Seguridad

A continuación se van a ver los aspectos más importantes que hay que tener en cuenta para proteger el servidor web.

10.1.6.1 Filtros ISAPI

Los filtros de interfaz de programación de aplicaciones para servidores de Internet (ISAPI) son DLL opcionales que llevan a cabo acciones concretas cuando IIS procesa una solicitud http de un cliente. Los filtros ISAPI realizan su acción antes de que el servidor responda realmente a la propia solicitud de http, por lo que permiten establecer un primer nivel de seguridad ante un posible ataque.

Existen muchos tipos de filtros ISAPI, pero uno de los más utilizados es UrlScan. UrlScan es una herramienta de seguridad que restringe los tipos de peticiones HTTP que puede procesar Internet Information Services. Al bloquear peticiones HTTP concretas, se previene la posibilidad de que peticiones potencialmente dañinas puedan alcanzar el servidor.

Para utilizar UrlScan primero debe descargarlo de la página *http://www.iis.net/extensions/UrlScan* y realizar el proceso de instalación. Una vez completado el proceso de instalación para activarlo pulse en el acceso directo *Filtros ISAPI* de la parte central de la ventana y añada el filtro que se encuentra en la carpeta *c:\system32\inetsrv\UrlScan* (véase la figura 10-13).

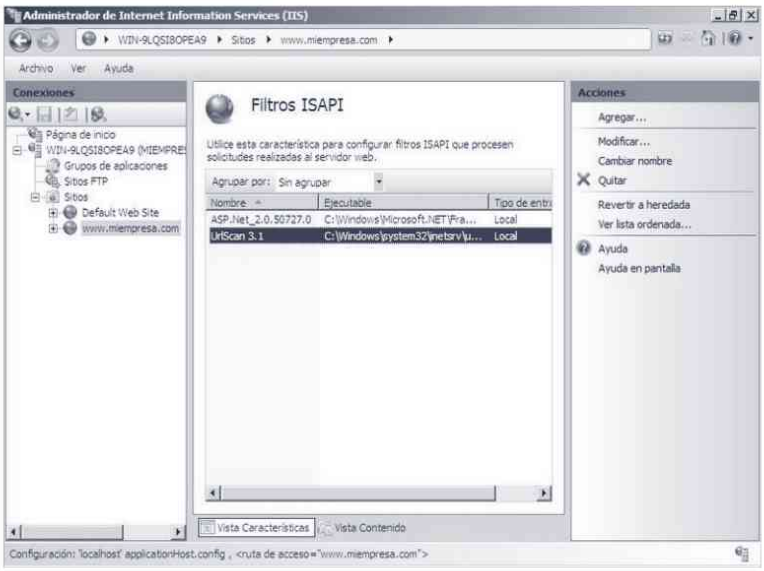


Figura 10-13. Filtros ISAPI - UrlScan

10.1.6.2 Seguridad en directorios

El control de seguridad de directorios se puede realizar de dos formas diferentes: habilitando la autenticación y el control de acceso, y estableciendo restricciones por nombre de dominio y dirección IP.

Autenticación

Para acceder a la ventana de configuración de la autenticación y el control de acceso, haga doble clic en el acceso directo *Autenticación.* En la ventana que aparece (véase la figura 10-14) puede establecer autenticación anónima (utilizando la cuenta de usuario IUSR_MAQUINA) o puede habilitar el acceso autenticado. Existen cinco formas de autenticación: autenticación básica (la contraseña se manda en texto no cifrado), autenticación de texto implícita (mucho más segura

que la básica), autenticación de Windows (solo para uso en el entorno de Intranet, para autenticar las conexiones de cliente en el dominio), la autenticación mediante formularios (para autenticación a sitios de tráfico alto o a aplicaciones de servidores públicos) y suplantación de ASP.NET (esta autenticación se utiliza cuando se ejecutan aplicaciones ASP.NET en un contexto de seguridad diferente del predeterminado).

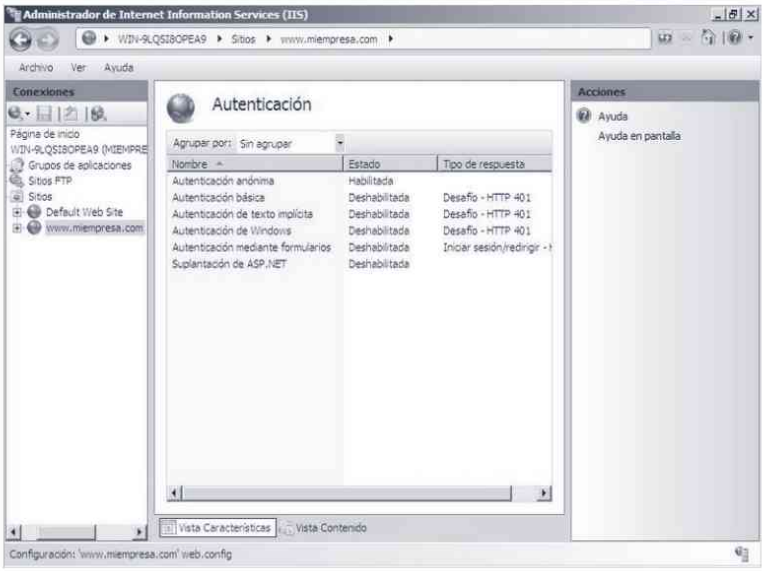


Figura 10-14. Autenticación del sitio web

Una vez habilitado un método de autenticación, al acceder al sitio web aparece una ventana de autenticación (véase la figura 10-15).

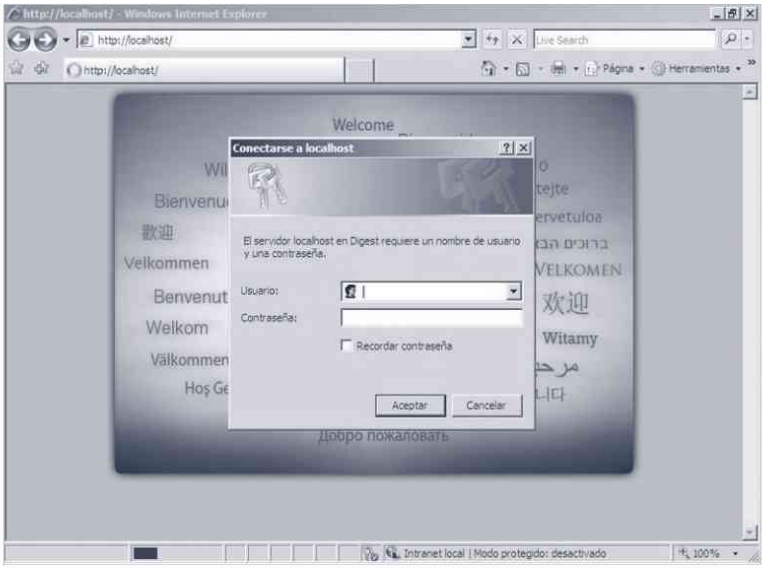


Figura 10-15. Autenticación del cliente

Restricciones de direcciones IP y dominios

De igual forma, en la ventana del sitio web, también es posible restringir o permitir el acceso al sitio web desde una determinada dirección IP o un nombre de dominio DNS concretos. La figura 10-16 muestra la ventana *Restricciones de direcciones IPv4 y dominios*. Las restricciones se pueden establecer de dos formas diferentes:

- Agregar una entrada de permiso para una dirección IPv4 o dominio específica, o un intervalo de direcciones IPv4.
- Al contrario, agregar una entrada de denegación para una dirección IPv4 o dominio específico, o un intervalo de direcciones IPv4.

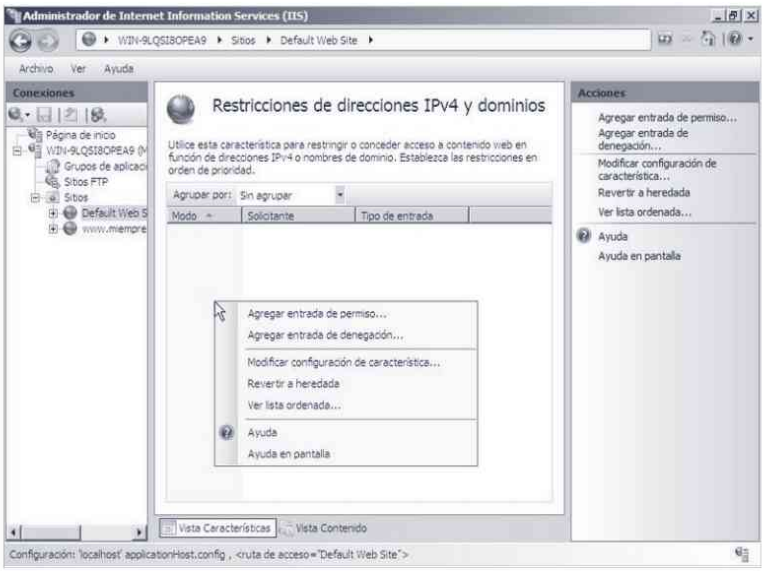


Figura 10-16. Restricciones de direcciones IPv4 y dominios

10.1.6.3 Conexiones seguras SSL

Para poder permitir comunicaciones seguras es necesario utilizar un certificado de seguridad para el sitio web que se desea proteger. Puede obtener el certificado a través de una empresa certificadora oficial o puede emitir su propio certificado.

La ventaja de comprar el certificado a una empresa oficial es que los navegadores de Internet confiarán directamente en el certificado; y si lo emitimos nosotros, el navegador le mostrará un mensaje indicándole que la empresa emisora no es de confianza. La principal ventaja de emitir nuestro propio certificado es que es gratuito.

Para instalar el certificado, seleccione el sitio web donde quiere instalar el certificado, seleccione el acceso directo *Certificados de servidor* y en la ventana que aparece en la figura 10-17 puede realizar las siguientes acciones:

- **Importar un certificado.** Permite importar un certificado existente. Para ello debe indicar su ubicación e introducir su contraseña.
- **Crear una solicitud de certificado.** Inicia un asistente que le guía en el proceso. Primero debe introducir información relativa al nombre distintivo: Nombre común, organización, Unidad organizativa, Ciudad o localidad, Estado o provincia, y País o región. Después, especifique el proveedor de servicios criptográficos y la longitud en bits. Indique el nombre del fichero donde se almacena la solicitud y pulse *Finalizar*. El fichero generado tiene que enviarlo a la autoridad certificadora (CA) y continuar con el siguiente paso.
- **Completar solicitud de certificado.** Permite completar una solicitud de certificado que contiene la respuesta de la entidad de certificación.
- También puede **Crear un certificado de dominio (**para lo cual hay que especificar una entidad de certificación en línea) o **Crear certificado autofirmado**.

Para comprobar si el certificado funciona correctamente acceda al sitio web (en el ejemplo *https://www.miempresa.com*) y compruebe si se activa el "candado" de seguridad que se encuentra en la parte inferior derecha de la página. Si pulsa en el candado puede ver los datos del certificado de seguridad.

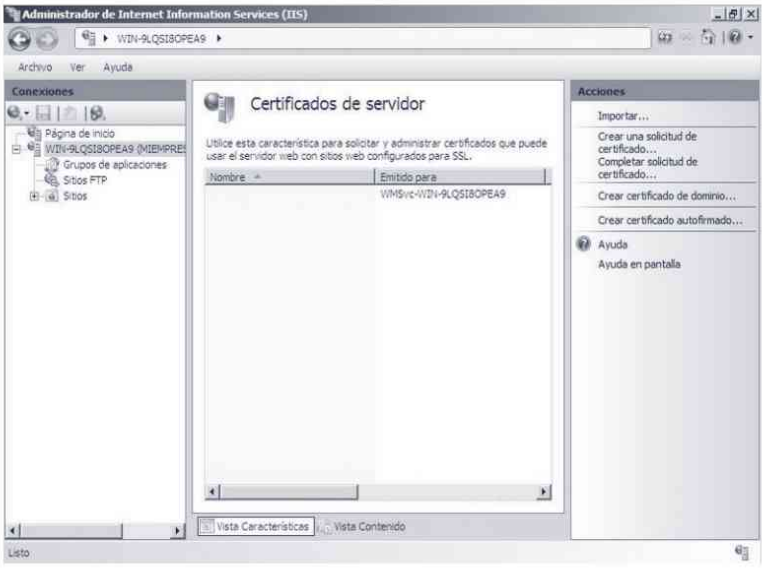


Figura 10-17. Certificados de servidor

10.2 SERVIDOR FTP

10.2.1 Instalación

Para instalar el servicio FTP acceda a la herramienta administrativa *Administre su servidor*, pulse en *Agregar roles* y seleccione *Servidor web (IIS).* En la ventana que aparece, seleccione la opción *Servidor FTP* y complete el proceso de instalación.

Para crear un sitio FTP, inicie el *Administrador de Internet Information Services (IIS)*, seleccione *Sitios* y en el menú de la derecha puede realizar las siguientes acciones: *Agregar sitio ftp* o *Establecer los valores predeterminados del sitio FTP*.

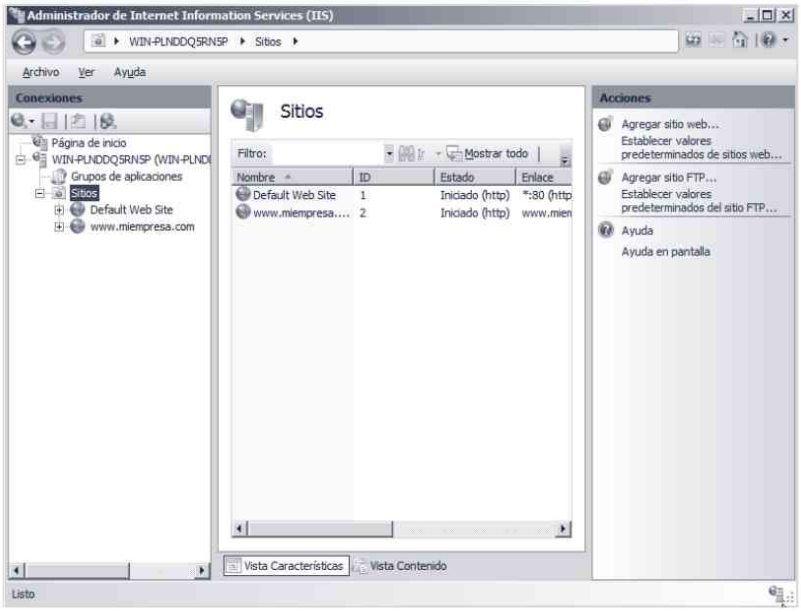


Figura 10-18. Administrador de IIS

10.2.2 Creación de un nuevo sitio FTP

Para crear un nuevo sitio pulse en el enlace *Agregar sitio FTP* y se inicia un asistente en el que debe realizar los siguientes pasos:

- Introduzca el nombre del sitio y el directorio donde se almacena (véase la figura 10-19).
- Indique la interfaz de red y el puerto por donde el servidor FTP recibe las peticiones. Y si lo desea, habilite SSL para mejorar la seguridad del servidor.

- Indique el tipo de autenticación del sitio (anónima o básica) y los usuarios autorizados.

Figura 10-19. Agregar sitio FTP

Al crear el sitio FTP, el sistema le asigna los valores predeterminados: número de conexiones, seguridad, mensajes, etc. Es posible que desee configurar a su medida un sitio FTP. Para ello, seleccione el sito FTP, pulse el botón derecho y seleccione *Administración del sitio FTP* y *Administración avanzada.*

Además, si accede dentro del sitio puede ver las diferentes herramientas que le permiten configurar el sitio FTP (véase la figura 10-20).

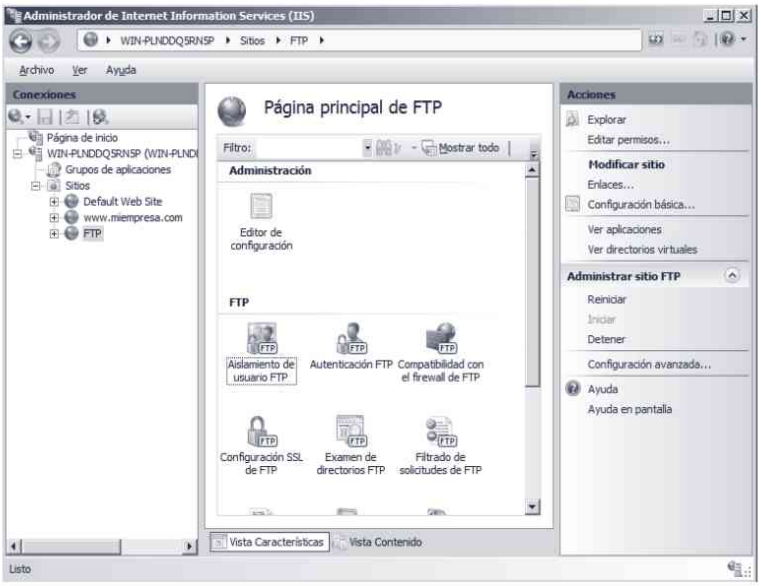


Figura 10-20. Página principal del sitio FTP

10.2.3 Creación de un directorio virtual

Un sitio FTP sirve todos los archivos y carpetas que se encuentran en el directorio de trabajo (por defecto, *c:\inetpub\ftproot*). Si desea compartir una determinada carpeta, puede copiar la carpeta dentro del directorio de trabajo. Pero si quiere compartir una carpeta y conservar su ubicación original tiene que crear un directorio virtual. Un directorio virtual permite que el sitio FTP pueda compartir una carpeta que no se encuentra en su directorio de trabajo.

Para administrar los directorios virtuales, en el menú de la derecha del sitio FTP (véase la figura 10-20) pulse en el enlace *Ver directorios virtuales*.

Para añadir un directorio virtual, pulse en el enlace *Agregar directorio virtual* y en la ventana que aparece en la figura 10-21 introduzca el alias y la ruta a la carpeta donde se ubica su contenido.

Figura 10-21. Agregar directorio virtual

10.2.4 Utilización

Para comprobar el correcto funcionamiento del servidor FTP utilice un programa cliente de FTP (p. ej., wsftp o Filezilla) o a través del navegador escriba: **ftp://IP**. Donde IP es la dirección IP o el nombre del servidor FTP. Si quiere conectarse con un usuario determinado entonces escriba en el navegador **ftp://nombre_usuario@IP**.

10.2.5 Seguridad

Para proteger el servidor es recomendable tener en cuenta los siguientes consejos:

- **Permitir solo acceso anónimo.** Al igual que la mayoría de los protocolos, los datos de los usuarios (nombre y contraseña) viajan a través de Internet en texto plano, pudiéndose recoger por un sniffer. Para evitar la interceptación de las credenciales utilice solo conexiones anónimas.
- **Deshabilite el permiso Escribir en el servidor FTP.**
- **Utilice una cuenta de usuario anónima personalizada.** Por defecto, el servidor web y FTP utilizan la misma cuenta de usuario anónimo. Si quiere diferenciar los servicios, cree una cuenta de usuario personalizada.
- **Habilitar el registro.** Habilite el registro de todas las conexiones FTP.
- **Restrinja el acceso al servidor por direcciones IP.** Indique las direcciones IP que van a poder acceder a su servidor. De esta forma evita que su servidor sea utilizado como equipo para almacenar información ajena a la empresa.
- **Aísle a los usuarios en su directorio particular FTP.**

10.3 SERVIDOR DE CORREO ELECTRÓNICO (EXCHANGE)

Microsoft Exchange 2010 Server está diseñado para cubrir las necesidades de cualquier organización, grande o pequeña, en aspectos de colaboración y mensajería. En Exchange, las direcciones de correo electrónico, los grupos de distribución y otros recursos de directorio se almacenan en la base de datos del directorio activo.

A continuación se va a realizar la puesta en marcha y configuración básica del servidor de correo electrónico Exchange.

10.3.1 Instalación

Tras lanzar el archivo ejecutable (*setup.exe*) de Exchange 2010, aparece la ventana que se encuentra en la figura 10-22 que le permite ver la documentación de Exchange así como enlaces para más información sobre los servicios hospedados de Exchange y Microsoft Forefront Security (dando la posibilidad de instalarlo) para Exchange.

Figura 10-22. Inicio de la instalación de Exchange

Además, muestra los distintos pasos para realizar la instalación de Exchange; aunque algunos se omiten si se trata de instalar componentes que ya tenemos disponibles:

- Paso 1: Instalar .NET Framework.
- Paso 2: Instalar Microsoft Windows Powershell.
- Paso 3: Seleccione la opción de idioma de Exchange.
- Paso 4: Instalar Microsoft Exchange.
- Paso 5: Obtener las actualizaciones críticas para Microsoft Exchange.

Seguridad

Aunque no es obligatorio, para mejorar la seguridad del sistema, es recomendable que no instale el servidor de correo en un controlador de dominio.

Para iniciar el proceso de instalación pulse sobre el paso que necesite iniciar (por ejemplo, es posible que los componentes de los pasos 1, 2 y 3 se encuentren instalados, por tanto pulse en el paso 4 directamente para instalar Exchange). Al pulsar en el enlace del paso 4 se inicia el proceso de instalación de Exchange. Tras mostrar una introducción al proceso pulse *Siguiente* y aparece la licencia del producto. Después de aceptar la licencia y pulsar *Siguiente*, debe elegir entre realizar una instalación típica o personalizada y la ruta donde se instalará.

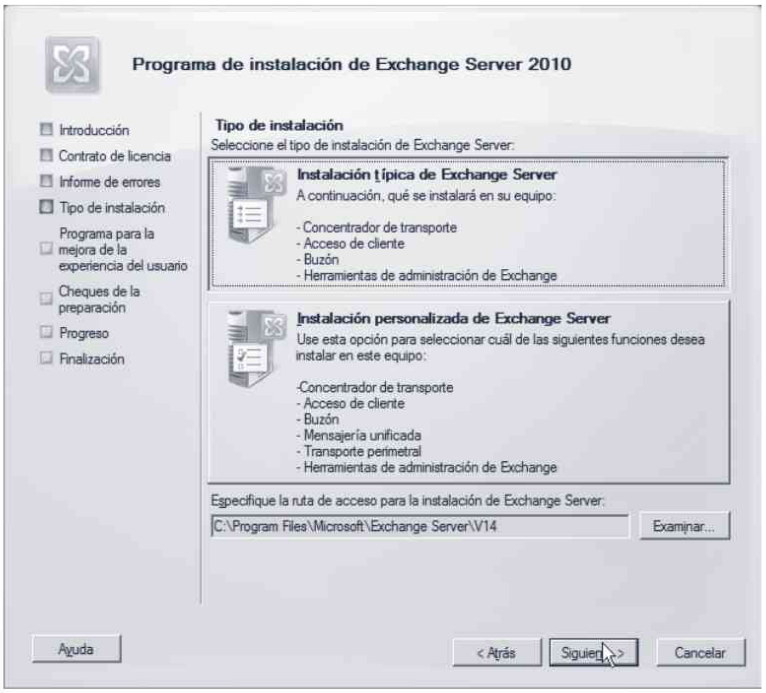


Figura 10-23. Seleccionar componentes de Exchange

Los elementos disponibles en cada tipo de instalación son los siguientes:

- **Instalación típica de Exchange Server:** *Concentrador de transporte*, *Acceso de cliente*, *Buzón* y *Herramienta de administración de Exchange*.
- **Instalación personalizada de Exchange Server:** Además de lo elementos de la instalación típica es posible instalar los siguientes elementos: *Mensajería unificada* y *Transporte perimetral*.

Una vez seleccionado el tipo de instalación, debe introducir el nombre de la organización e indicar si hay clientes con clientes de correo anteriores. Después, el instalador realiza las comprobaciones de preparación para la instalación, tras lo cual se muestra si hay errores de configuración y en definitiva si el servidor está preparado para albergar Exchange Server. Si todo es correcto, pulse en *Instalar* para comenzar la instalación.

Una vez completado el proceso de instalación (véase la figura 10-24), pulse el botón *Finalizar*. Se inicia la *Consola de administración de Exchange* y es necesario reiniciar el servidor para completar la instalación.

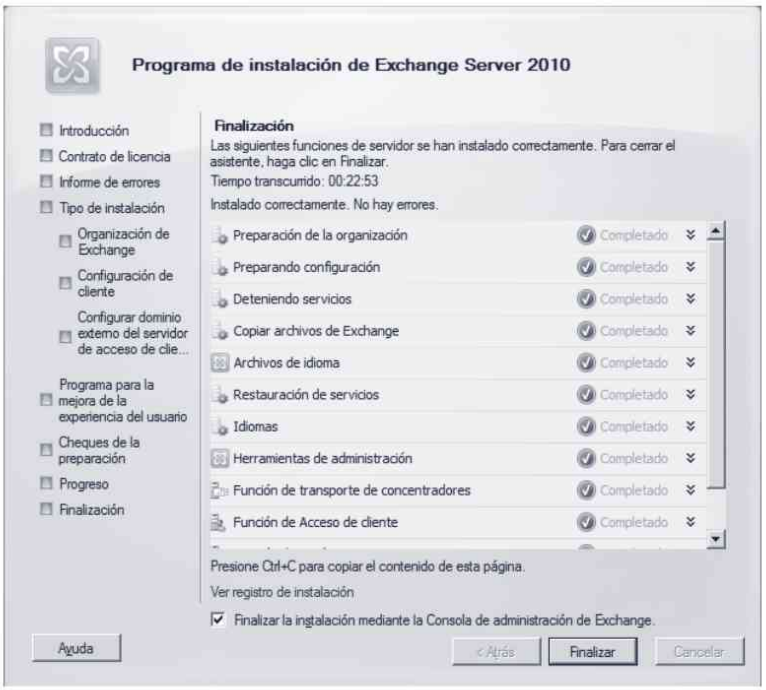


Figura 10-24. Progreso de la instalación

10.3.2 Configuración

Para configurar las opciones generales de Exchange debe utilizar la herramienta *Consola de administración de Exchange* y si desea realizar una configuración puntual sobre un usuario (p. ej., modificar las propiedades de una cuenta de correo) debe realizarlo a través del Directorio Activo. A continuación van a ver las opciones más importantes.

10.3.2.1 Configuración general: Consola de Administración de Exchange

Una organización es el punto de partida de la jerarquía de Exchange. Los límites de la organización de Exchange definen los límites de su entorno. En otras palabras, el almacenamiento de la información de Exchange no proporciona información a los usuarios o los servidores externos de la organización, a menos que se especifiquen estas identidades a Exchange Server.

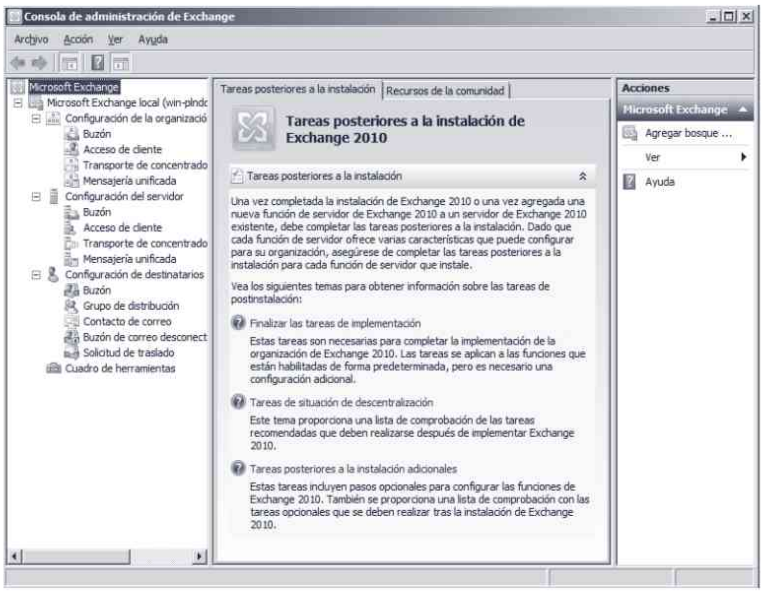


Figura 10-25. Consola de administración de Exchange

Al instalar Exchange es necesario asignar el nombre de la organización, el cual se asocia permanentemente a Exchange Server. La consola de administración de Exchange (véase la figura 10-25) permite configurar los diferentes componentes de la organización:

- **Configuración de la organización.** Permite configurar las opciones globales de la organización Exchange, pudiendo configurar funciones de acceso administrativo para usuarios y grupos. Las configuraciones realizadas afectan a todos los servidores que tengan una función de servidor específica. Dentro de esta configuración existen las siguientes secciones que representan estas funciones de servidor:
  - **Buzón.** Permite configurar las funciones de servidor de buzón. Puede mantener listas de direcciones, carpetas personalizadas administradas, directivas de buzón de administración de registros de mensajería (MRM) y libretas de direcciones sin conexión (OAB) existentes o crear otras nuevas.
  - **Acceso de cliente.** Permite crear y administrar directivas de buzón de Exchange y aplicar un conjunto común de directivas o configuraciones de seguridad a un grupo de usuarios.
  - **Transporte de concentradores.** Esta función es implementada en el Directorio Activo de la organización. Administra todo el flujo de correo interno, aplica las directivas de enrutamiento de mensajes de la organización y es el responsable de la entrega de mensajes a un buzón de destinatario. Define cómo y cuándo se envían los mensajes. Puede

definir una configuración que incluya el nombre de cuenta de la persona principal, las cuotas y los filtros de mensajes de manera predeterminada. Los filtros pueden descartar los mensajes de remitentes específicos y redirigirlos en función del remitente.

- **Mensajería unificada.** Se aplica también a toda la organización y permite administrar los planes de marcado, puertas de enlace IP y operadores automáticos de mensajería unificada.

- **Configuración de servidores.** Permite configurar los servidores Exchange y los componentes de los que disponen (por ejemplo, bases de datos, protocolos, administración de registro de mensajería...). Permite definir los servicios activos (p. ej., IMAP4, POP3, SMTP) y los grupos de almacenamiento de los servidores. Un grupo de almacenamiento es un contenedor de almacenamiento para buzones y carpetas públicas. Si desea configurar los parámetros de configuración de un servidor, seleccione el servidor, pulse *Propiedades* y establezca los parámetros de configuración apropiados. Por ejemplo, si configura un servidor de correo electrónico saliente (SMTP) puede establecer los parámetros de autenticación, límites de los mensajes, etc. Al igual que en la configuración de la organización se disponen de los mismos elementos de configuración:

  - **Buzón.** Permite administrar las bases de datos de los buzones de los servidores con esta función instalada.

  - **Acceso de cliente.** Permite gestionar las libretas de direcciones sin conexión, la función Microsoft Outlook Web Access y el acceso desde dispositivos móviles con ActiveSync.

  - **Transporte de concentradores.** Permite listar todos los servidores con esta función, y configurar los conectores de recepción SMTP de Exchange que no son sino la puerta de enlace por la que se reciben los mensajes.

  - **Mensajería unificada.** Permite configurar aspectos relacionados con mensajes de voz, de fax, correos electrónicos... a los que tienen acceso los usuarios.

- **Configuración de destinatarios.** Utilice esta sección para configurar los destinatarios en la organización. Un destinatario es una entidad que puede recibir correo de Exchange. Esto incluye usuarios, contactos, grupos y otros recursos. Se pueden administrar los buzones de Exchange, los usuarios de correo, contactos de correo, grupos de distribución de Exchange... por ejemplo. También dispone de cuatro secciones que puede administrar:

- **Buzón.** Permite administrar los usuarios de buzón y buzones de recursos (salas y equipos). Se puede también habilitar la mensajería unificada y los dispositivos móviles.
- **Grupo de distribución.** Permite administrar los grupos de distribución de correo.
- **Contacto de correo.** Gestiona todo lo relacionado con contactos de correo.
- **Buzón desconectado.** Desde aquí puede ver y conectar buzones deshabilitados.

- **Cuadro de herramientas.** Tal y como puede ver en la figura 10-26, Exchange cuenta con un conjunto muy amplio de herramientas que permiten configurar y optimizar el rendimiento del sistema.

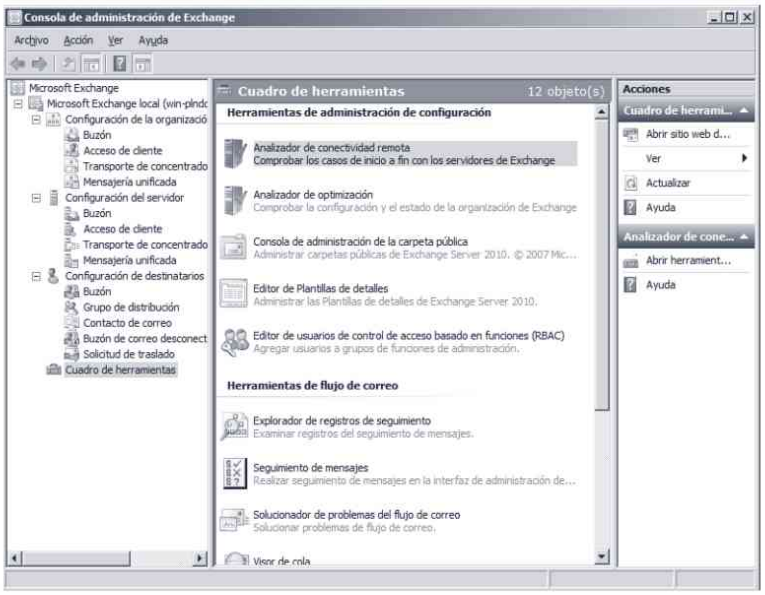


Figura 10-26. Cuadro de herramientas

Para empezar a trabajar debe actualizar los datos de la organización. Para ello seleccione *Microsoft Exchange local*, pulse el botón derecho del ratón, seleccione *Recopilar datos de mantenimiento de la organización* y en la ventana que aparece en la figura 10-27 pulse *Siguiente* y posteriormente *Recopilar.* A partir de ahora en la página principal de la consola de administración de Exchange ya debe reconocer correctamente el servidor con sus bases de datos.

Figura 10-27. Recopilar datos de mantenimiento de la organización

10.3.2.2 Configuración de cuentas de usuario

Como se ha comentado anteriormente, Exchange se integra totalmente en el directorio activo de Microsoft. Una vez instalado Exchange, al crear un nuevo usuario puede ver cómo se crea automáticamente su cuenta de correo (véase la figura 10-28).

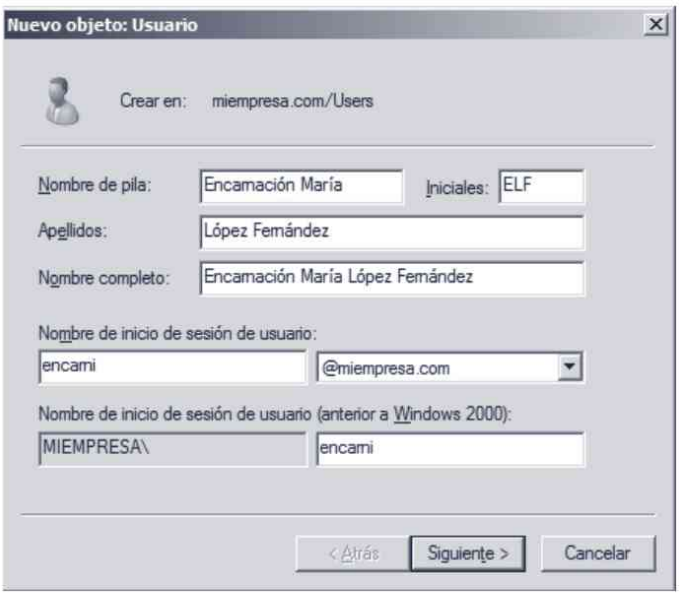


Figura 10-28. Nuevo usuario

De la misma forma al acceder a las *Propiedades de usuario*, en la pestaña *Configuración de destinatarios* puede encontrar las siguientes opciones para la configuración del correo:

- **Direcciones de correo electrónico.** Muestra las direcciones de correo electrónico del usuario. Si lo desea, puede añadir nuevas direcciones de correo para un mismo usuario o editar las existentes.
- **Configuración del buzón.** Permite administrar los registros de mensajería y las cuotas de almacenamiento del usuario (configurar advertencias del buzón, límites de tamaño, cuánto tiempo se guardan los elementos eliminados...).
- **Características de buzón.** Permite habilitar o deshabilitar los servicios y características del buzón del usuario, protocolos que puede usar: Outlook Web Access, Exchange ActiveSync, Mensajería unificada, MAPI, POP3, IMAP4, y ver sus propiedades.
- **Configuración de flujo de correo.** Nos ayuda a establecer la configuración de la cuenta del usuario en cuanto a opciones de entrega (permisos delegados y dirección de reenvío), restricciones en el tamaño de los mensajes y restricciones en la entrega de mensajes (qué remitentes tienen permiso o tienen prohibido enviar mensajes al destinatario).
- **General.** Además, en la pestaña *General* se han añadido campos que nos permiten especificar el nombre simple asociado a la cuenta de correo, si queremos ocultar un usuario de las listas de distribución, ver y modificar los permisos de acceso al buzón, etc.

10.3.2.3 Múltiples dominios

Para poder albergar cuentas de usuarios de varios dominios hay que realizar dos tareas: permitir crear usuarios de un dominio distinto al principal, e indicarle al servidor de correo que reciba los mensajes del dominio.

Para permitir la creación de usuarios de un dominio distinto, ejecute la aplicación *Dominios y confianza de Active Directory* (véase la figura 10-29). Seleccione *Dominios y confianza de Active Directory*, pulse el botón derecho y seleccione *Propiedades* (véase la figura 10-30).

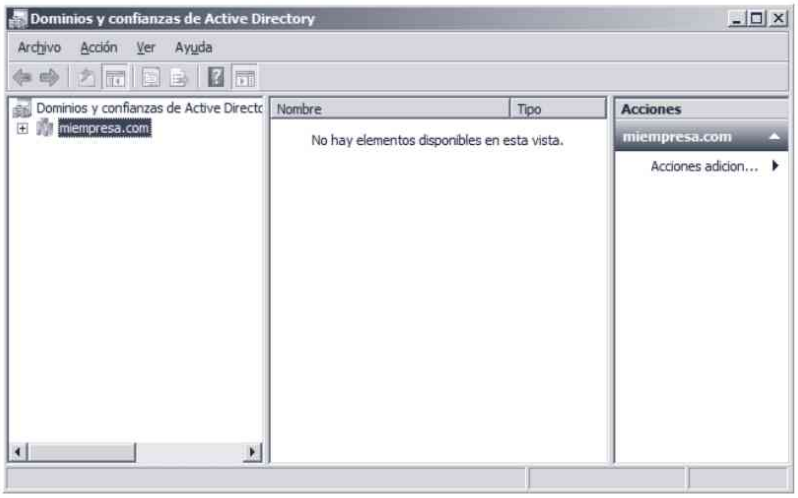


Figura 10-29. Dominios y confianza de Active Directory

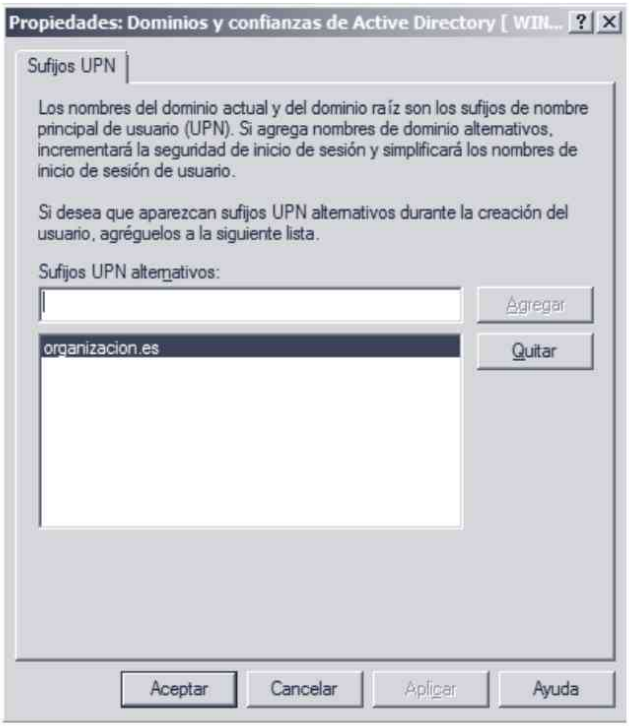


Figura 10-30. Sufijos UPN

En la pestaña *Sufijos UPN* añada los sufijos alternativos del dominio (p. ej., *organización.es*). Una vez creado el nuevo sufijo UPN cuando cree un nuevo usuario podrá elegir el dominio al que pertenece (véase la figura 10-31).

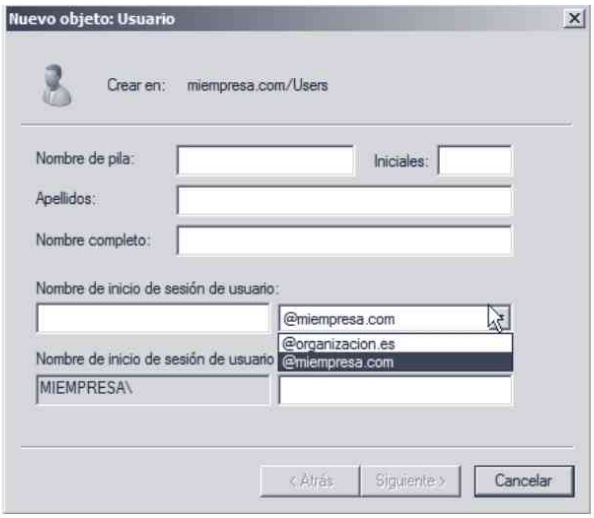


Figura 10-31. Creación de un usuario (múltiples dominios)

Una vez configurado el Directorio Activo, para poder crear usuarios de diferentes dominios, es necesario indicarle al servidor de correo que acepte los correos electrónicos que van dirigidos a los usuarios del nuevo dominio. Para ello en la herramienta *Consola de administración de Exchange*, acceda a la *Configuración de la organización*, *Transporte de concentradores* y seleccione la pestaña *Directivas de dirección de correo electrónico* (véase la figura 10-32).

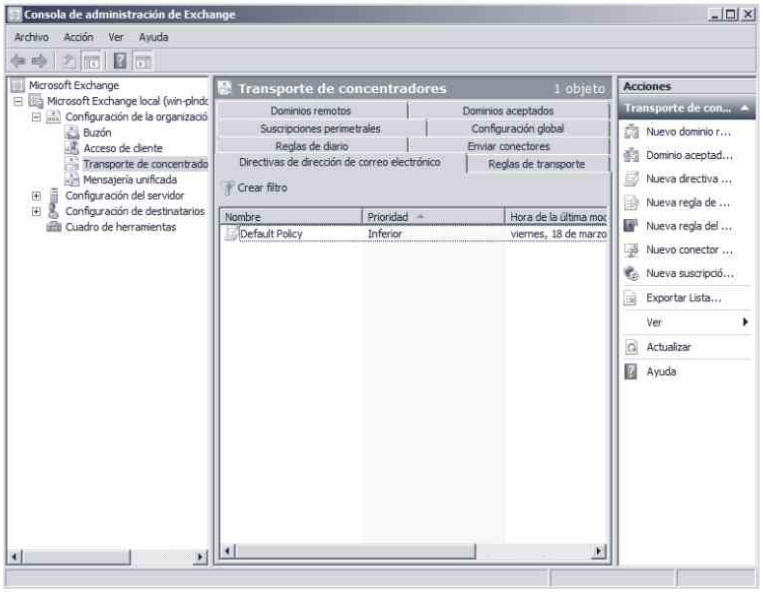


Figura 10-32. Directivas de direcciones de correo electrónico

Las directivas de dirección de correo electrónico le indican al servidor las direcciones de correo electrónico para que los destinatarios puedan enviar y recibir

correo. Pulse el botón derecho, seleccione *Nueva directiva de dirección de correo electrónico* y se inicia un asistente para crear la directiva: escriba el nombre de la directiva (en el ejemplo *organización*) y seleccione los destinatarios a incluir. Después puede configurar las condiciones de la directiva y en la pestaña *Direcciones de correo electrónico* añada la dirección de correo del tipo SMTP con el valor de la dirección (en el ejemplo de la figura 10-33, *@organizacion.es*). Pulse *Siguiente* para introducir la programación de aplicación de la directiva. Se muestra un resumen del proceso, pulse *Nuevo* y finalmente pulse *Finalizar* para salir del asistente y concluir.

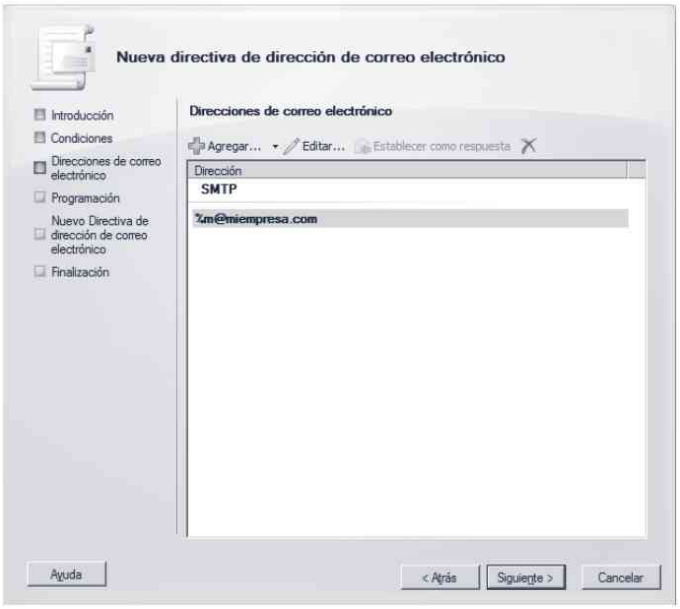


Figura 10-33. Crear directivas de direcciones de correo electrónico

Nota

Recuerde que para recibir los correos debe tener creada la entrada Mail Exchanger (MX10) en el servidor DNS.

10.3.2.4 WebMail

Si lo desea puede activar el servicio WebMail para permitir que los usuarios accedan a su correo electrónico a través del navegador web. Para comprobar si tiene activo el servicio ejecute la herramienta *Consola de administración de Exchange* y en *Configuración de servidores* haga clic en *Acceso de cliente* y finalmente seleccione su servidor. Compruebe la pestaña *Outlook Web Access* de la parte inferior central de la ventana (véase la figura 10-34).

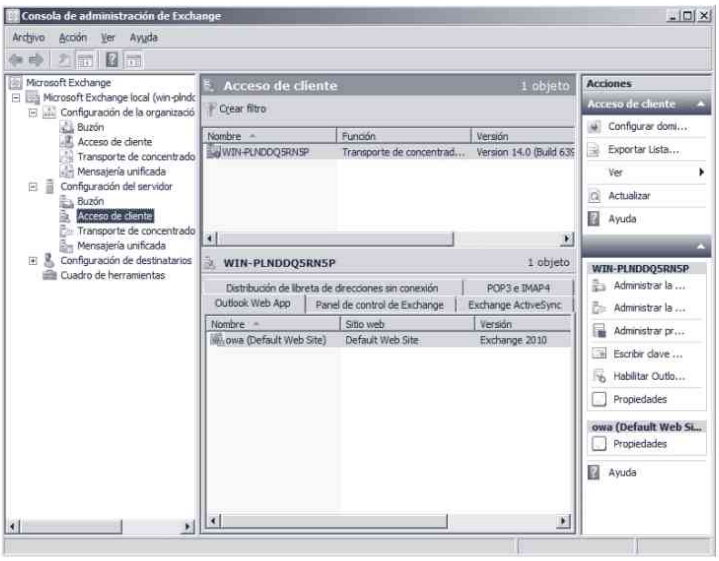


Figura 10-34. WebMail – Consola de administración de Exchange

Si se encuentra activo el servicio, puede comprobar en el *Administrador de Internet Information Services (IIS)* que existe el directorio virtual */owa* (véase la figura 10-35).

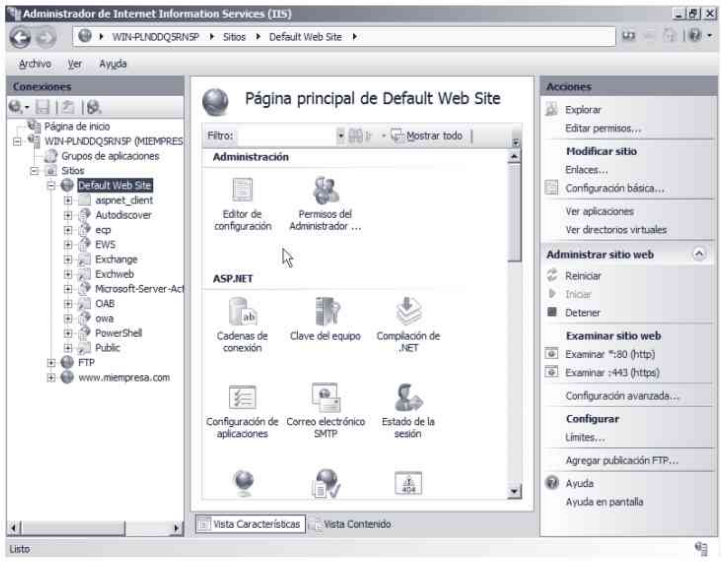


Figura 10-35. Administración del sitio web en IIS

Para utilizar WebMail, abra el explorador de Internet, escriba la dirección de su servidor web (si es el predeterminado, *http://localhost/owa*), introduzca su nombre de usuario y contraseña (véase la figura 10-36), y podrá ver su correo a través de WebMail tal y como muestra la figura 10-37.

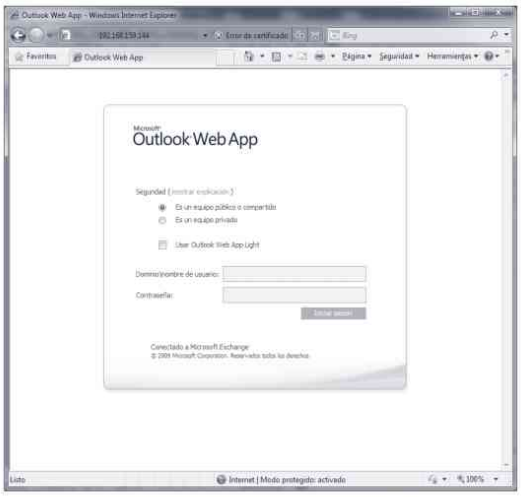


Figura 10-36. Acceso a WebMail

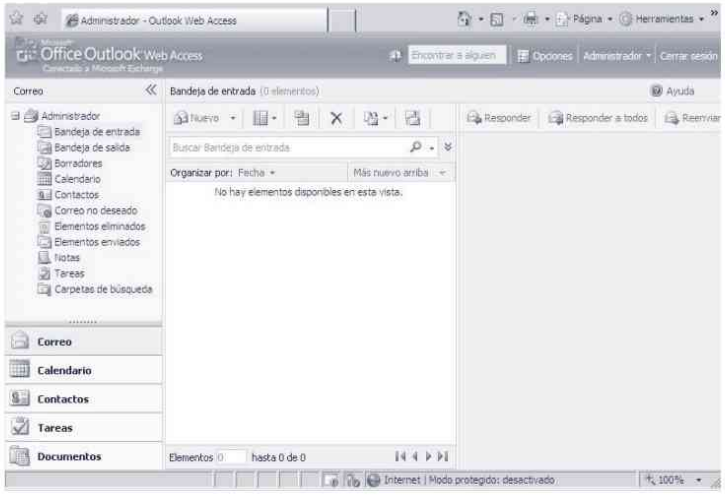


Figura 10-37. WebMail

10.3.3 Seguridad

Proteger un servidor de correo siempre es una tarea delicada. Instalar un antivirus, proteger el servidor contra el spam… son medidas básicas que hay que realizar. A continuación se van a ver las medidas más importantes para proteger el servidor de correo.

10.3.3.1 Proteger contra direcciones IP falsas

Una de las maneras más habituales de atacar un sistema de correo electrónico es manipular el campo *desde* de un mensaje. El protocolo simple de transferencia (SMTP) no verifica la identidad de un usuario, pero se pueden

realizar algunas acciones en Exchange para tratar de reducir al mínimo los mensajes falsos.

Uno de los peores problemas que plantean las direcciones falsas son los ataques externos que utilizan una dirección de correo interno. Este sistema se puede utilizar de diferentes maneras; con frecuencia, se usa para persuadir a otro usuario que proporcione información confidencial que, a su vez, se utiliza para realizar otros ataques.

Si recibe mensajes directamente de otros dominios de Internet, puede configurar el servidor (SMTP) para que realice la búsqueda inversa de los mensajes de correo electrónico entrantes en el Sistema de nombres de dominio (DNS). De esta manera se comprueba si la dirección IP del servidor de correo (y el nombre del dominio completo) del remitente corresponde al nombre de dominio indicado en el mensaje.

La búsqueda inversa supone una carga adicional para el servidor Exchange y también requiere que el servidor Exchange pueda ponerse en contacto con las zonas de búsqueda inversa del dominio remitente.

10.3.3.2 Habilitar la seguridad para los objetos de Exchange

Al igual que con cualquier aplicación de su entorno, cuando se definen los permisos para Exchange debe comprobar las funciones que los administradores de Exchange tienen en el entorno y darles solo los permisos necesarios. Para simplificar el proceso, Exchange utiliza grupos administrativos. Un grupo administrativo es un conjunto de objetos de Exchange que se recopilan con fines de administración y delegación de permisos.

En algunos casos, el Asistente para delegar la administración de Exchange no proporciona suficiente nivel de detalle para asignar la seguridad. Se puede modificar la ficha de seguridad de cada objeto en Exchange. No obstante, de forma predeterminada solo se muestra la ficha de seguridad de los siguientes objetos:

- Listas de direcciones.
- Listas globales de direcciones.
- Bases de datos (almacenes de buzones y carpetas públicas).
- Jerarquía de carpetas públicas de nivel superior.

10.3.3.3 Buenas prácticas

La herramienta *Microsoft Exchange Best Practices Analyzer* permite a los administradores obtener un informe detallado con una lista de recomendaciones de

Microsoft que se pueden aplicar al entorno para conseguir un mejor rendimiento, estabilidad y tiempo de respuesta.

Esta herramienta está disponible por defecto con Exchange en el menú *Cuadro de herramientas* (véase la figura 10-38). Si ejecuta la herramienta puede realizar el análisis del servidor de correo (véase la figura 10-39). Una vez finalizado el análisis, la herramienta le genera un informe con las prácticas recomendadas.

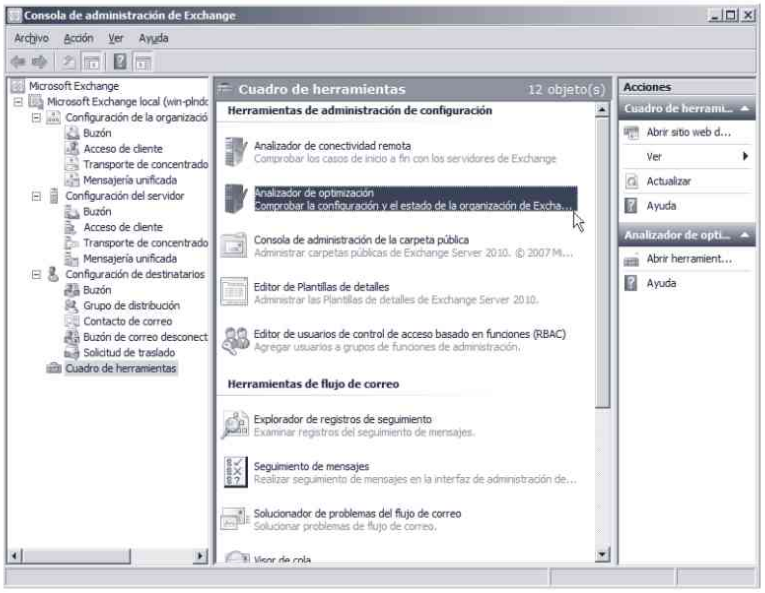


Figura 10-38. Analizador de optimización

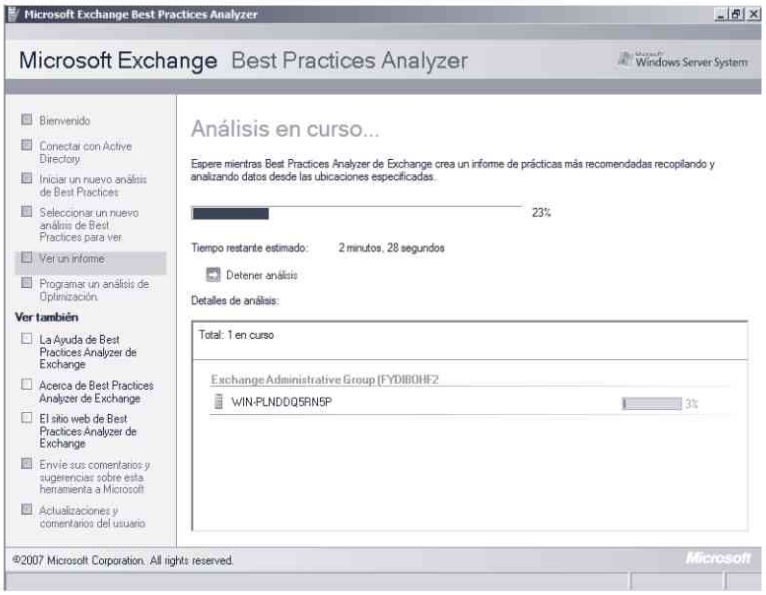


Figura 10-39. Best Practices Analyzer

10.3.3.4 Filtro inteligente de mensajes de Exchange

La herramienta *Content Filter Agent* permite ayudar a determinar la probabilidad de que cada mensaje de correo entrante sea o no correo no deseado. Basándose en esta probabilidad puede elegir bloquear los mensajes de correo en la puerta de enlace o en el almacén del buzón.

Para instalar el *Content Filter Agent* vaya al menú de *Inicio -> Programas -> Exchange* y ejecute *Exchange Management Shell*. Vaya al directorio *c:/Archivos de programa/Microsoft/Exchange Server/V14/Scripts* y ejecute el comando *install-AntispamAgents.ps1* para instalar los diferentes componentes anti-spam, entre ellos el *Content Filter Agent* (véase la figura 10-40).

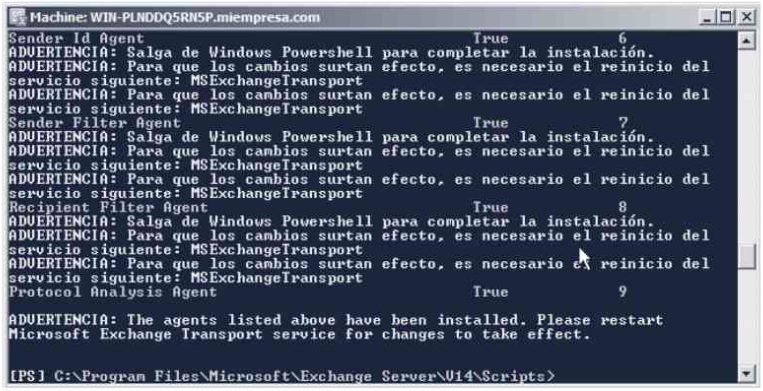


Figura 10-40. Instalación del Content Filter Agent

Para acceder a la herramienta vaya al *Filtro de correo no deseado* (véase la figura 10-41) y puede ver que se pueden denegar los correos electrónicos por los siguientes criterios: *Filtrado de contenido*, *Filtrado de destinatarios*, *Filtrado de remitentes, Id del remitente*, *Listado de direcciones IP bloqueadas*, *Listado de direcciones IP permitidas*, *Proveedores de las listas de direcciones IP bloqueadas*, *Proveedores de las listas de direcciones IP permitidas* y *Reputación del remitente*.

Como puede ver, son muchos los componentes instalados y que aportan funcionalidades muy interesantes. Una vez instalado el filtrado y reiniciado el servicio de transporte de Microsoft Exchange, se puede proceder a su configuración teniéndolo disponible en la *Consola de administración de Exchange* bajo las secciones *Configuración de la organización*, *Transporte de concentradores*, *Contra el correo electrónico no deseado* y *Filtrado de contenido* si se trata de un servidor concentrador de transporte o bajo la sección *Perimetral* si se trata de un servidor perimetral de Exchange.

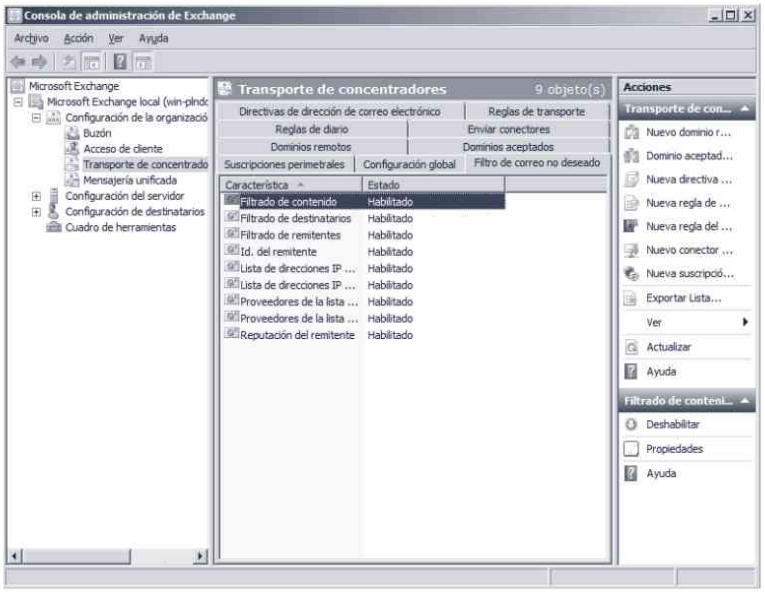


Figura 10-41. Filtrado de contenidos

Al hacer clic con el botón derecho sobre *Filtrado de contenido*, seleccione *Propiedades*, y en la pestaña *Acción* puede establecer los umbrales de confianza de correo no deseado (SCL) para el servidor. Si el valor SCL es bajo se bloquean más mensajes que pueden ser correos no deseados, pero también aumenta la probabilidad de bloquear mensajes correctos. Existen tres umbrales para casos en los que desea eliminar, rechazar, o poner en cuarentena los mensajes.

Todos los componentes citados arriba se habilitan por defecto. Si desea deshabilitar alguno de ellos, solo debe hacer clic con el botón derecho sobre el componente y seleccionar *Deshabilitar*. También es posible habilitar/deshabilitar cada filtro en cada uno de los servidores de manera independiente.

Capítulo 11

DIRECTORIO ACTIVO

11.1 INTRODUCCIÓN

En un entorno de red normal, un usuario puede iniciar sesión en la red con un nombre de usuario y una contraseña (p. ej., *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 que pueden resultar resolver 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.

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).

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 11-1 se puede ver una visión general de la infraestructura de un Directorio Activo.

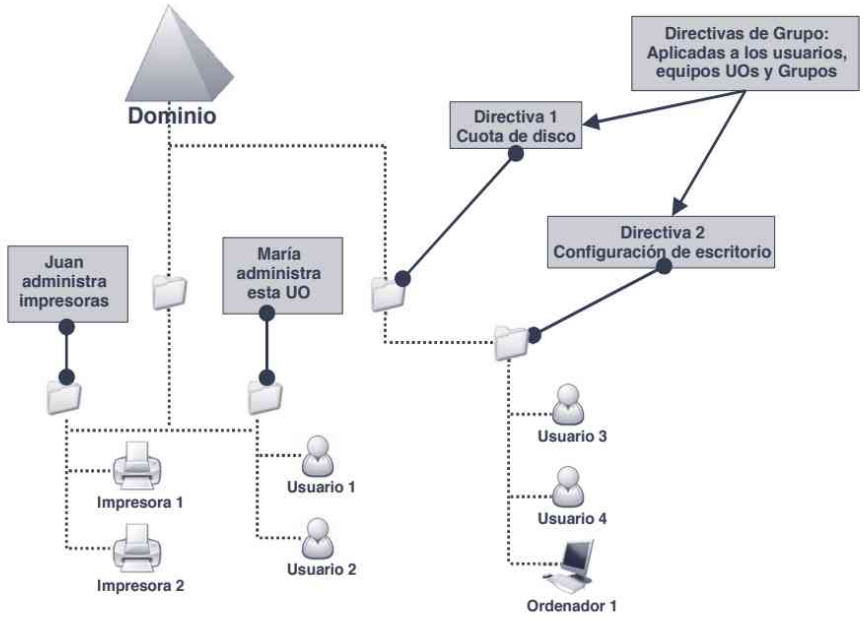


Figura 11-1. Visión general del Directorio Activo

Para poder 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 y 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 para servidores es 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 es 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 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 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 replican 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,… 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. ej., nombre, organización) es posible guardar información adicional útil para el correcto funcionamiento del sistema o de las aplicaciones que se integran en el dominio.

11.2 INSTALACIÓN DEL CONTROLADOR DE DOMINIO

11.2.1 Tareas previas

Antes de comenzar el proceso de promoción de un servidor a controlador de dominio 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.

11.2.2 Instalación

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

- 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.*
- El sistema muestra información acerca del servicio. Pulse *Siguiente* y confirme que desea realizar la instalación. 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.

- 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 selecciona la segunda opción, el controlador se convierte 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 pregunta 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.

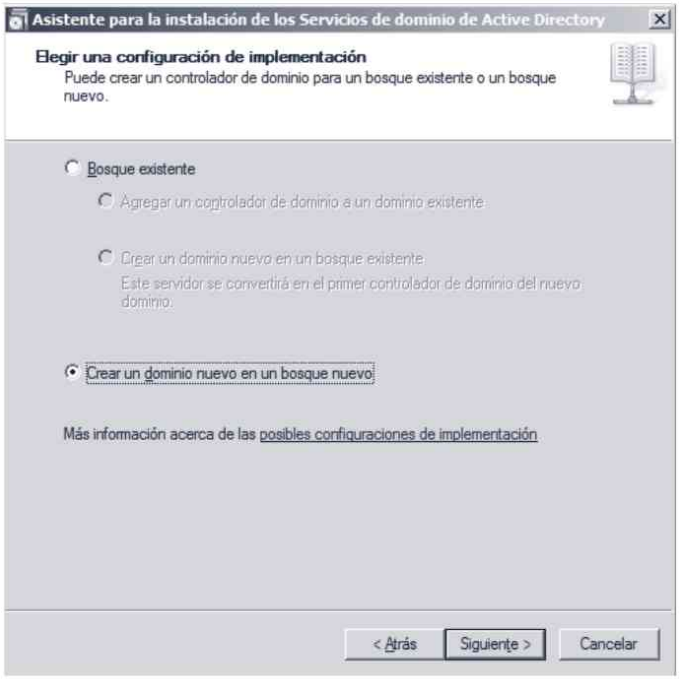


Figura 11-2. Elegir una configuración de implementación

- 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.

- 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 o 2008R2). 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.
- 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 puede ser un RODC. Además, se recomienda la instalación del servidor DNS en el primer controlador de dominio.

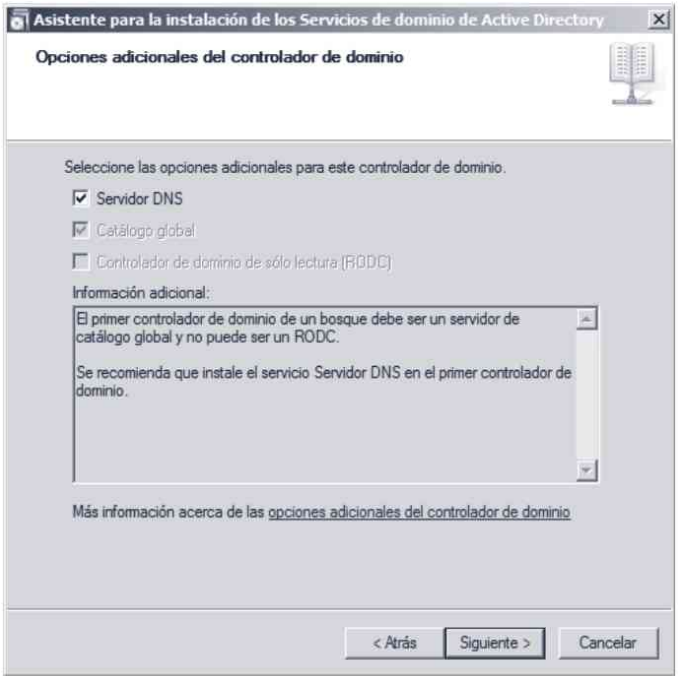


Figura 11-3. Opciones adicionales del controlador de dominio

- Establezca las carpetas donde se guardan 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.

- Especifique la contraseña de *administración de modo de restauración de servicio de directorio* y pulse *Siguiente*.
- En la figura 11-4, puede ver cómo el asistente muestra un resumen de todas las opciones seleccionadas. Revise y confirme las opciones y pulse *Siguiente*.

Figura 11-4. Resumen de la instalación de Active Directory

Nota

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

Nota

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 11-5) especifique varios servidores DNS públicos de confianza.

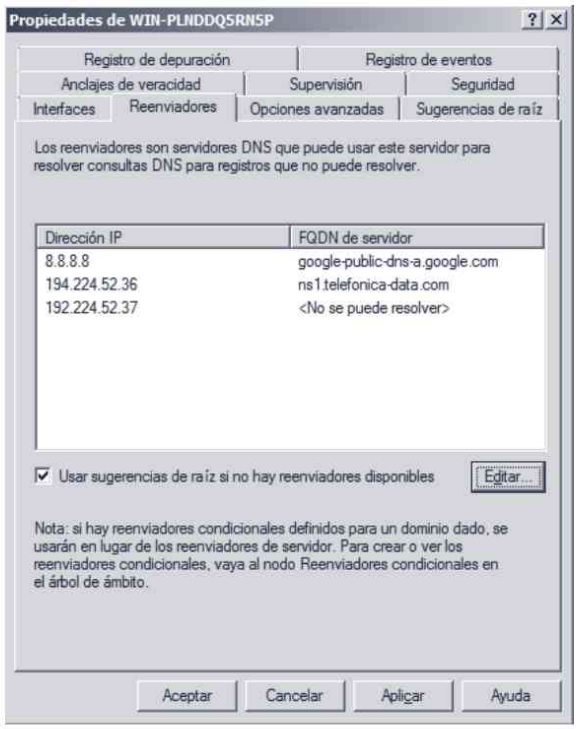


Figura 11-5. Reenviadores del servidor DNS

11.3 ADMINISTRACIÓN DEL DIRECTORIO ACTIVO

11.3.1 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.

Nota

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

11.3.2 Administración básica de objetos

La administración de los diferentes objetos del dominio (usuarios, grupos, UO,..) se realiza a través de la herramienta *Usuarios* y *equipos de Active Directory* (véase la figura 11-6) que se encuentra dentro de *Herramientas administrativas*.

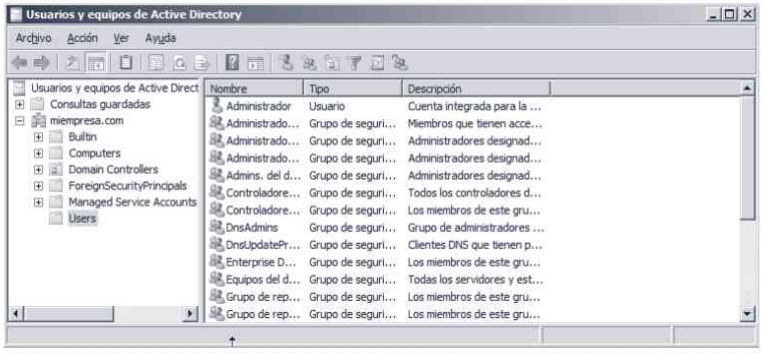


Figura 11-6. Administración de usuarios y equipos del directorio activo

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

11.3.2.1 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 OU. 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.*

11.3.2.2 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 11-6).

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.

11.3.2.3 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.

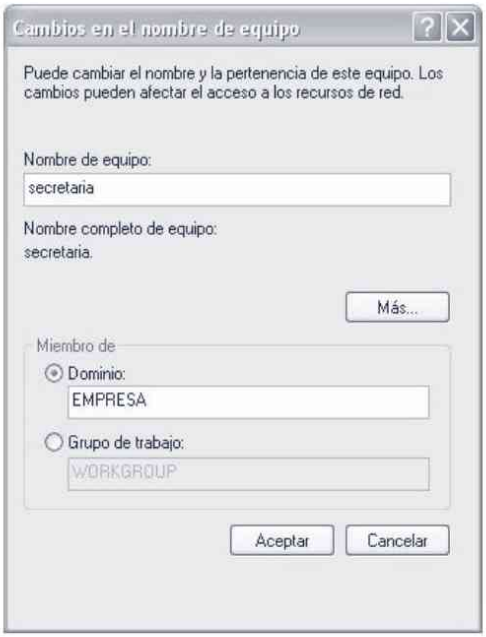


Figura 11-7. Unión a un dominio

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 11-7). 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.

Nota

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 11-8).

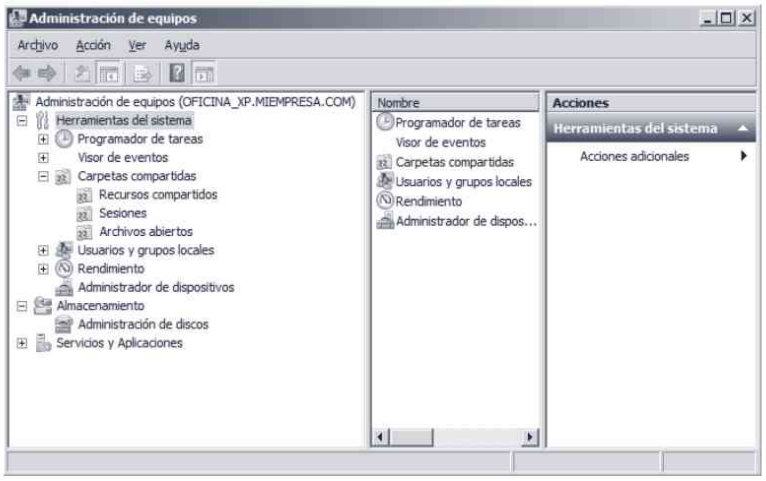


Figura 11-8. Administración remota del equipo

Nota

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.

11.4 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.

11.4.1 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 2008R2).

11.4.1.1 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(s) 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 GPO vinculadas al dominio.
- Se aplican las GPO vinculadas a unidades organizativas de primer nivel, posteriormente se aplican las de segundo nivel, etc.

11.4.1.2 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,** incluyendo 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.

Nota

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.

11.4.1.3 Aplicación

Como ha visto anteriormente, 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.

Nota

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

11.4.2 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 11-9, a través del *Editor de directivas de grupo local* puede configurar las directivas del sistema.

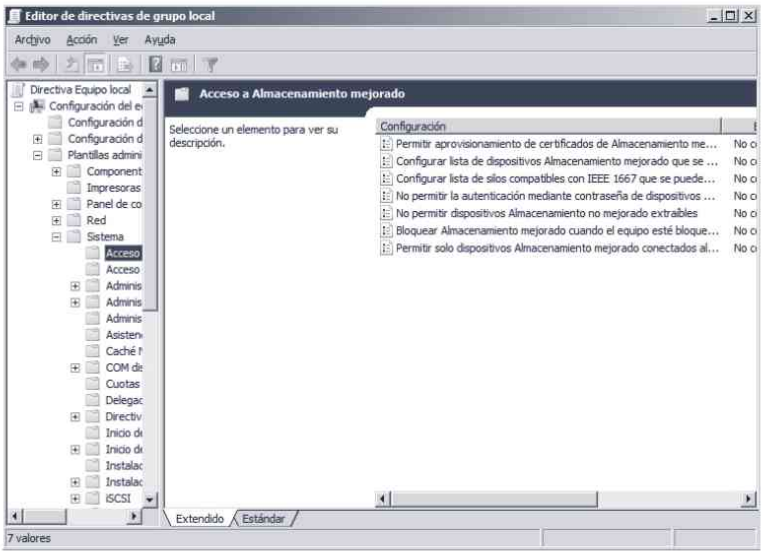


Figura 11-9. Editor de directivas de grupo local

11.4.3 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 11-10) 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 11-10, se encuentra la unidad organizativa *Oficina* que contiene todos los equipos de la oficina para que tengan una misma configuración.

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

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

- Dependiendo de la opción seleccionada indique el nombre de la nueva directiva o seleccione la directiva que desea vincular.
- Automáticamente aparece la GPO creada. Por ejemplo, en la figura 11-11 se muestra la *GPO equipos oficina* dentro de la unidad organizativa *Oficina.*

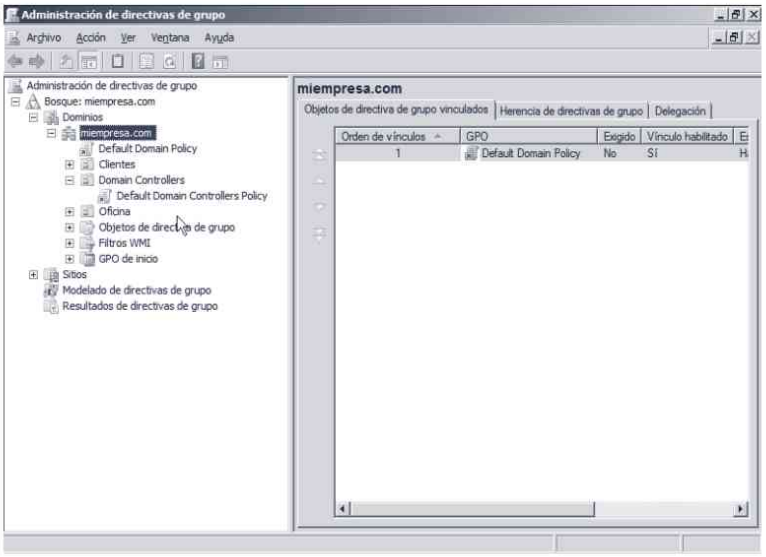


Figura 11-10. Administrador de directivas de grupo

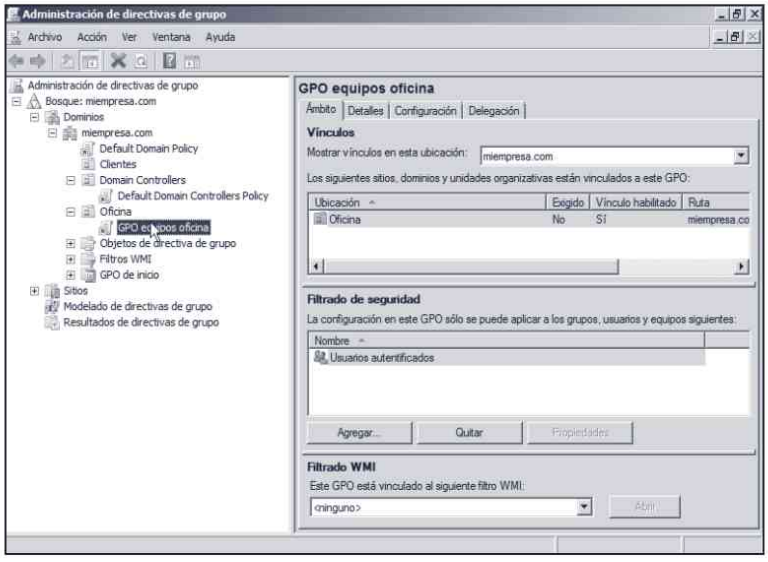


Figura 11-11. GPO equipos oficina

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

- 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 11-12).

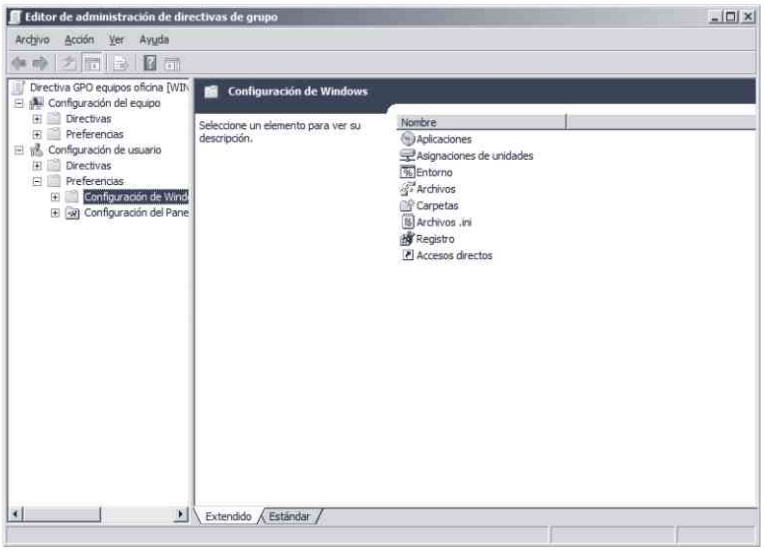


Figura 11-12. Editor de administración de directivas de grupo

Nota

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 gpudate.

GNU/LINUX

Capítulo 12

INSTALACIÓN Y CONFIGURACIÓN

12.1 INTRODUCCIÓN

Linux fue concebido por el finlandés Linus Torvalds, estudiante de la Universidad de Helsinki, quien comenzó trabajando sobre el código fuente de Minix (un pequeño UNIX desarrollado por Andy Tanembaum) para lograr un Unix mínimo, capaz de ejecutar al menos un shell y un compilador. Primero fue la versión 0.02 ya que la 0.01 nunca llegó a ser compilada con éxito. Luego Linus anunció en Internet su proyecto de la siguiente manera:

"Si suspiras al recordar aquellos días cuando los hombres eran hombres y escribían sus propios manejadores (drivers). Si te sientes sin ningún proyecto interesante y te gustaría tener un verdadero sistema operativo que pudieras modificar a placer. Si te resulta frustrante tener solo Minix. Entonces este artículo es para ti".

De esa forma Linux fue liberado en Internet y la respuesta de los programadores y usuarios de UNIX fue contundente. Pronto todos querían aportar sus conocimientos para que Linux se convirtiera en un sistema operativo estable, robusto y potente. Finalmente llegó la primera versión estable del kernel, la versión 1.0. De allí en adelante, Linux fue evolucionando a un ritmo vertiginoso hasta convertirse en un fuerte rival de los sistemas operativos comerciales.

Desde su aparición, los sistemas GNU/Linux han ido evolucionando y mejorando sus prestaciones drásticamente. Hoy en día puede encontrar los sistemas GNU/Linux en multitud de sistemas: desde grandes servidores hasta pequeños equipos domésticos como teléfonos móviles.

Tux

Tux es el nombre de la mascota oficial de Linux. Fue creada por Larry Ewing en 1996.

La idea de que la mascota de kernel Linux fuera un pingüino provino del mismo Linus Torvalds, ya que, según se cuenta, cuando era niño le picó un pingüino, y le resultó simpática la idea de asociar un pingüino a su proyecto.

12.1.1 Distribuciones

El kernel del sistema operativo Linux fue desarrollado por Linus Torwards y licenciado bajo GPL. Pero un sistema GNU/Linux no es solo su núcleo ya que existen hoy en día un gran número de aplicaciones desarrolladas también bajo licencias libres que permiten que los sistemas GNU/Linux tengan una gran versatibilidad y funcionalidad.

Nota

La Fundación Linux realizó un interesante cálculo acerca de cuál sería la cifra que una empresa debería abonar para desarrollar desde cero la distribución Fedora 9.

El trabajo concluyó que el coste total de desarrollo de Fedora 9 tiene un valor de 10.800 millones de dólares.

Existen muchas aplicaciones desarrolladas bajo licencia libre pero, sin duda alguna, las más importantes son: OpenOffice (*http://www.openoffice.org*), Apache (*http://www.apache.org*), firefox (*http://www.firefox.org*). Estos son solamente unos ejemplos, pero existen aplicaciones libres para cualquier uso que imagines.

Puesto que el kernel y las aplicaciones son libres entonces puede crear su propio sistema operativo con los programas que más le gusten y crear su propia distribución; lógicamente nuestra distribución también tendrá que ser libre. Una distribución es una agrupación de un conjunto de programas, imágenes, temas de escritorio, etc.

URL de interés

Si desea hacer su propia distribución GNU/Linux es recomendable que acceda a http://www.instalinux.com/ donde a través de un asistente podrá personalizar y crear su propia distribución.

Existen muchas iniciativas, tanto empresariales como gubernamentales, de crear su propia distribución. Un claro ejemplo lo puede encontrar en las distribuciones Guadalinex (de la Junta de Andalucía), gnuLinex (de Extremadura), tripxbox (distribución empresarial de telefonía IP), etc.

A partir de la libertad de los usuarios, empresas y organismos para personalizar su propia distribución, han surgido una gran cantidad de distribuciones que nacen, evolucionan, derivan en otras distribuciones y cómo no, algunas mueren.

En la tabla 12-1 puede ver algunas de las distribuciones más utilizadas actualmente.

Tabla 12-1. Distribuciones más utilizadas

Nombre	URL
Debian	*http://www.debian.org*
Fedora	*http://fedoraproject.org*
Gentoo Linux	*http://www.gentoo.org*
Mandrila Linux	*http://www.mandriva.com*
OpenSuse	*http://www.opensuse.org*
Slackware	*http://www.slackware.com*
Ubuntu	*http://www.ubuntu.com*
Sabayon	*http://sabayonlinux.org*
Puppy Linux	*http://www.puppylinux.org*
SLAX	*http://www.slax.org*
Linux Mint	*http://www.linuxmint.com*
PC LinuxOS	*http://pclinuxos.com*
Mandriva	*http://www.mandriva.com*
CentOS	*http://www.centos.org*
FreeBSD	*http://www.freebsd.org*
Kubuntu	*http://www.kubuntu.org*

URL de interés

En la web http://distrowatch.com puede ver y descargar cualquier distribución.

En *http://futurist.se/gldt* puede ver un mapa de distribuciones GNU/Linux que abarca su evolución, derivaciones y bifurcaciones en el tiempo partiendo de las distribuciones "matrices" como son Debian, Slackware y RedHat.

Figura 12-1. Algunas distribuciones Linux

12.1.2 Licencias de software

Sin duda alguna no se puede hablar de los sistemas GNU/Linux sin mencionar las licencias de software libre, germen de todo el desarrollo de los sistemas GNU/Linux.

La licencia pública general de GNU, más conocida como GNU GPL, es una licencia creada por la Free Software Fundation en 1989. Su principal objetivo es garantizar la libertad de compartir y modificar el software. El término libre (*free*) se refiere a la libertad de poder modificar y distribuir el software, no a su precio.

Figura 12-2. Logo GNU

Al desarrollar un programa, escribir un artículo o crear cualquier obra que desea distribuir libremente, puede optar por dos caminos diferentes: dominio público o licencia libre. Lógicamente, las dos opciones permiten liberar el software garantizando la autoría de la obra.

Si crea una aplicación para dominio público, el software estará disponible de forma gratuita para otras personas pero el código fuente no estará disponible. Por el contrario, si elige una licencia libre, entonces el proceso es mucho más enriquecedor ya que pone disponible el código fuente por lo que permite que otros programadores puedan modificar, mejorar o adaptar nuestro software a sus necesidades.

Cuando se licencia un software bajo GPL se permiten los siguientes grados de libertades:

- **Libertad 0.** Ejecutar el programa sea cual sea nuestro propósito.
- **Libertad 1.** Estudiar el funcionamiento del programa y adaptarlo a sus necesidades.
- **Libertad 2.** Redistribuir copias.
- **Libertad 3.** Mejorar el programa y luego distribuirlo.

Lógicamente, los términos de la licencia permiten la libertad de poder utilizar y adaptar el software a sus necesidades pero el resultado debe seguir siendo libre. Este punto es muy importante ya que permite que no se "rompa" la cadena de software libre.

Actualmente se encuentra en vigor GPL versión 3 que fue publicada en 2007 y define aspectos de una forma mucho más precisa sobre el uso del software licenciado GPL.

URL de interés

En http://www.gnu.org/philosophy/fsfs/free_software.es.pdf puede encontrar el libro "Software libre para una sociedad libre" del gurú del software libre Richard M. Stallman.

Nota

Las licencias Creative Commons están inspiradas en la licencia GPL pero están destinadas a facilitar el uso y distribución de los contenidos garantizando la autoría de la obra.

12.2 INSTALACIÓN

El proceso de instalación del sistema GNU/Linux resulta bastante sencillo gracias al asistente que le guía durante todo el proceso de instalación. Antes de iniciar la instalación necesita tener en cuenta el uso que le va a dar al sistema ya que de ello dependerá mucho el hardware del equipo. Como regla general necesita

un equipo con al menos 512 MB de RAM y unos 5 GB de disco duro. Aunque todo depende del uso que quiera darle al sistema.

A continuación se va a realizar la instalación de las dos distribuciones más utilizadas Ubuntu y Fedora. Para poder realizar el proceso de instalación antes de nada debe descargar el CD de la distribución que puede descargar de la web oficial o de *http://www.linuxiso.org*.

Consejo

Si lo desea puede realizar la instalación en una máquina virtual. De esta forma puede trabajar con su equipo normalmente sin miedo a perder los datos del sistema.

12.2.1 Ubuntu

En Ubuntu (*http://www.ubuntu.com/*) existen tres versiones: *Desktop* (para equipos de escritorio), *Netbook* (para portátiles) y *Server* (para servidores). Además, para cada tipo puede utilizar la versión de 32 bits y de 64 bits. Como el objetivo del curso es aprender a administrar un servidor, a continuación se va a realizar la instalación de la versión *Server.*

Para iniciar la instalación debe iniciar el equipo con el CD de la distribución. 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 CD.

Una vez iniciado el equipo seleccione el idioma que quiere utilizar durante el proceso de instalación y que aparece el menú de arranque que se muestra en la figura 12-3.

Figura 12-3. Menú de arranque de Ubuntu

Para realizar la instalación del sistema hay que seleccionar la opción *Instalar Ubuntu Server* y realizar los siguientes pasos:

Pasos previos

- El primer paso que debe realizar es indicar el país. Para ello seleccione el continente *Europe*, pulse *Enter* y en la pantalla que aparece seleccione *Spain.*

Figura 12-4. Seleccionando el idioma

- A continuación indique el idioma del teclado. Para ello puede iniciar el asistente que le solicita presionar una serie de teclas o seleccione directamente desde el menú el tipo de teclado.
- Escriba el nombre del equipo y pulse *Continuar.*

Figura 12-5. Nombre del equipo

- El sistema indica la zona horaria. Si lo desea puede cambiarla o aceptarla pulsando *Enter.*

Particionamiento

- Ahora llega el momento más importante del proceso de instalación y en el que debe tener más cuidado: el particionamiento del sistema de ficheros.

Nota

Tiene que tener cuidado al crear las particiones porque puede perder la información del sistema.

El particionamiento del sistema de ficheros permite especificar y crear las particiones que necesita el sistema operativo. Como mínimo, las particiones que debe crear para que el sistema funcione correctamente son dos: una de Linux native y otra de Linux swap. La primera partición (Linux native), con punto de montaje /, es donde se guardan todos los datos del sistema y de los usuarios. La segunda partición (Linux swap) la utiliza internamente el sistema operativo como zona de intercambio con la

memoria principal cuando la carga de trabajo del sistema es alta. El tamaño recomendado de la partición swap es el doble de capacidad de la memoria RAM que tiene nuestro sistema.

Figura 12-6. Particionamiento del sistema

Tal y como puede ver en la figura 12-6, el proceso de instalación permite realizar el particionamiento de forma automática o manual. De forma automática puede utilizar todo el espacio del disco utilizando particiones (*Guiado –utilizar todo el disco*), utilizando volúmenes (*Guiado – utilizar el disco completo y configurar LVM*) o cifrando el sistema de ficheros (*Guiado –Utilizar todo el disco y configurar LVM cifrado*).

Nota

Para tener una mayor seguridad en el sistema puede indicar que se cifren automáticamente los datos de las particiones.

Si es la primera vez que instala Ubuntu puede utilizar la opción "*Guided - use entire disk"* aunque lo recomendable es crear el particionamiento de forma manual dependiendo de sus necesidades.

Al seleccionar el particionamiento manual el sistema muestra los discos duros del equipo (véase la figura 12-7).

Figura 12-7. Particionando el disco duro

Para crear una partición hay que seleccionar el disco duro y pulsar *Enter*. Como el disco duro que se va a utilizar es nuevo el sistema informa de que no tiene ninguna tabla de particiones y que va a crear una tabla de particiones vacía.

A continuación seleccione el espacio libre del disco duro y pulse *Enter* para crear una nueva partición. Para crear la partición debe indicar su tamaño, tipo de partición (primaria o lógica) y su posición (al principio o al final del disco duro). Finalmente, tal y como puede ver en la figura 12-8, hay que indicar el tipo de sistema de ficheros y punto de montaje. Como es la primera partición mantenga las opciones por defecto (Ext4 montado en el directorio /) y pulse *Done setting up the partition.*

Se crea la partición de memoria de intercambio (Swap) con aproximadamente el doble de tamaño que la memoria RAM del equipo.

Una vez creadas las dos particiones (véase la figura 12-9) pulse *Finalizar el particionamiento y escribir los cambios en el disco*. El asistente solicita confirmación para crear la tabla de particiones.

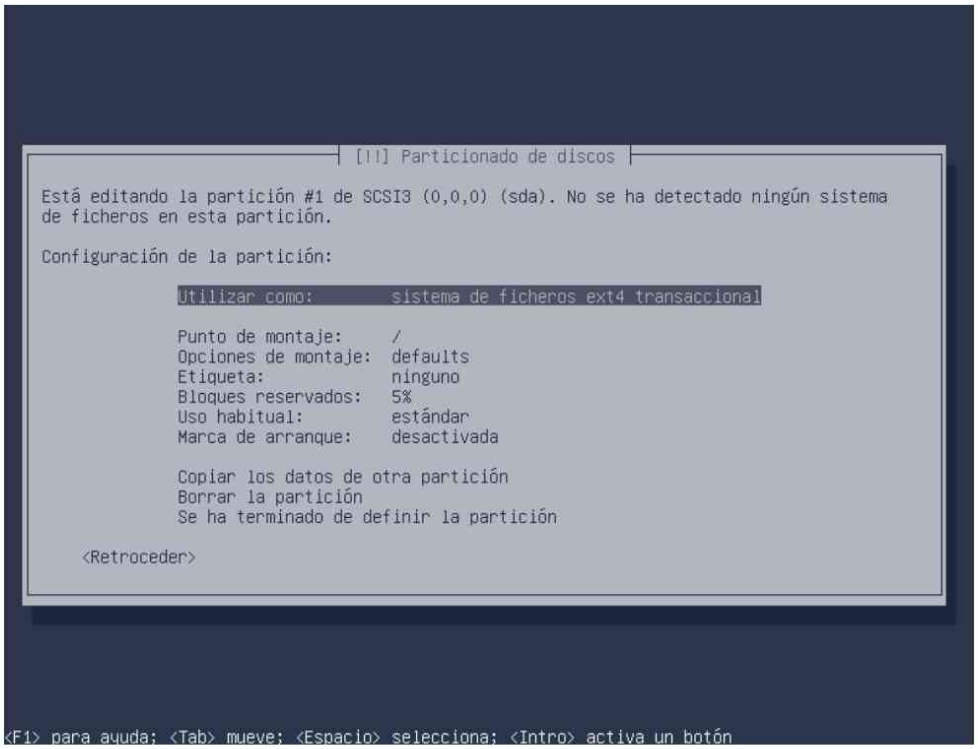


Figura 12-8. Creando una nueva partición

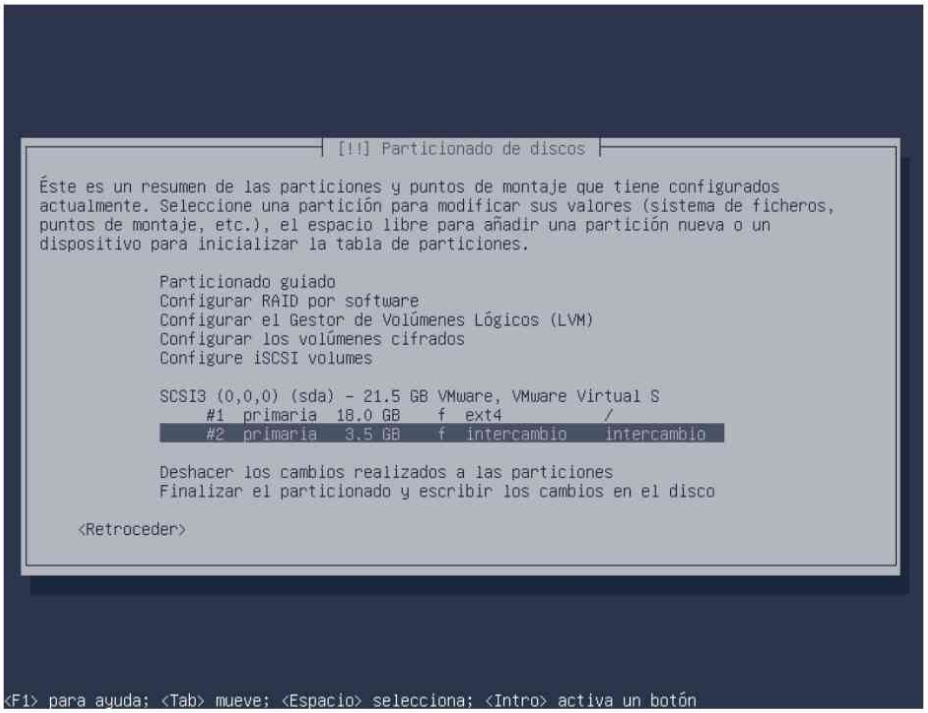


Figura 12-9. Particionamiento completado

- Se inicia el proceso de instalación de los elementos básicos del sistema.

Figura 12-10. Proceso de instalación del sistema base

- A continuación se da de alta un usuario para poder utilizar el sistema. Para ello hay que introducir su nombre completo, login y contraseña. Para mejorar la seguridad del sistema puede cifrar el directorio */home* de los usuarios.

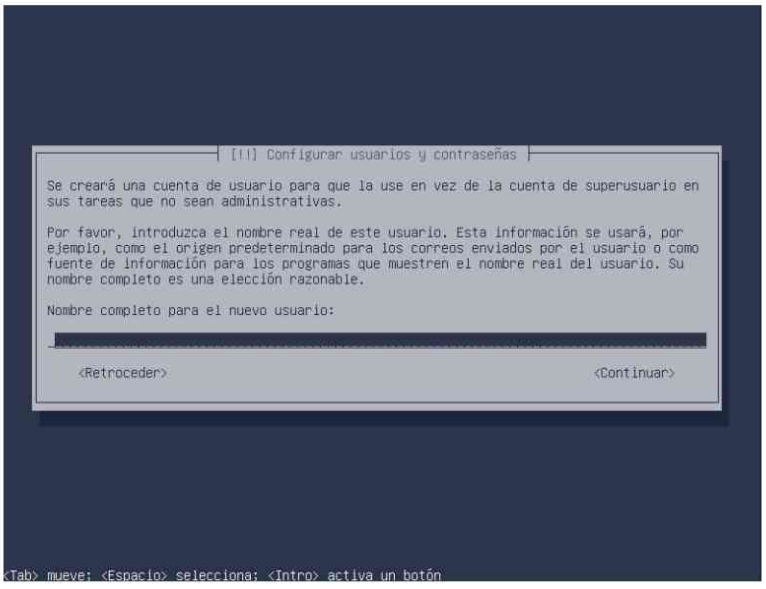


Figura 12-11. Nuevo usuario

Figura 12-12. Cifrado del directorio /home

- Se inicia el proceso de instalación del software. Como la distribución Ubuntu se va actualizando constantemente el proceso de instalación permite instalar automáticamente las actualizaciones de seguridad. Para ello en la ventana que aparece en la figura 12-13 seleccione la opción *Instalar actualizaciones de seguridad automáticamente*.

Figura 12-13. Aplicar actualizaciones en el sistema

- Transcurridos unos instantes hay que indicar los servicios que desea instalar (véase la figura 12-14). Para empezar no se va a seleccionar ningún servicio, para instalarlos y configurarlos manualmente durante el curso.

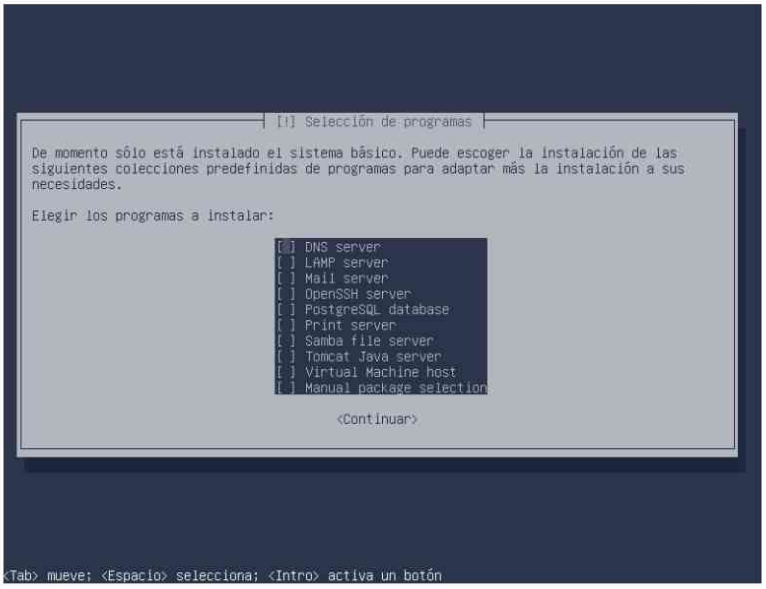


Figura 12-14. Silenciando software

- Para finalizar, debe instalar GRUB como gestor de arranque por lo que pulse *Sí* (véase la figura 12-15).

Figura 12-15. Gestor de arranque

- Una vez finalizada la instalación pulse *Continuar* para reiniciar el equipo y poder empezar a utilizar el sistema.

Figura 12-16. Shell del sistema

12.2.2 Fedora

Para realizar el proceso de instalación de Fedora (*http://www.fedoraproject.org*) debe iniciar el equipo con el DVD de Fedora y en la pantalla inicial de arranque indicar que quiere iniciar el equipo desde el CD. Si el equipo no muestra el menú de arranque puede acceder a la BIOS del equipo y configurarla para que arranque el sistema directamente desde CD.

Figura 12-17. Menú de arranque de Fedora

Una vez iniciado el equipo aparece el menú de arranque que se muestra en la figura 12-17 y que tiene las siguientes opciones:

- Las dos primeras opciones permiten realizar el proceso de instalación o actualización del sistema con la única diferencia de que la segunda opción utiliza el modo básico de vídeo. Se recomienda el modo *Install system with basic video driver* cuando Fedora no reconoce correctamente la tarjeta de vídeo.

- La tercera opción, *Rescue installed system*, permite iniciar el proceso de recuperación del sistema en caso de fallo. Lógicamente, para poder restaurar el sistema necesita la contraseña del administrador del sistema (*root*).
- Y la última opción, *Boot from hard disk*, permite iniciar el proceso de arranque directamente desde el disco duro y, por tanto, no inicia el proceso de instalación de Fedora.

A continuación se va a analizar el modo de instalación *Install or upgrade an existing system*, el cual se realiza a través de una interfaz gráfica.

Los pasos de la instalación son:

Pasos previos

- Antes de iniciar el proceso de instalación, hay que comprobar que el DVD es correcto y no presenta ningún fallo. Para ello, tal y como se muestra en la figura 12-18, puede iniciar el proceso de comprobación. Este proceso es largo ya que debe leer todo el contenido del DVD y calcular su firma digital. Si está seguro de que el disco es correcto entonces pulse *Skip*.

Figura 12-18. Test media

- Aparece la pantalla principal del asistente de instalación, pulse *Siguiente.* A continuación seleccione el idioma que va a utilizar durante el proceso de instalación y el idioma del teclado (véase la figura 12-19).

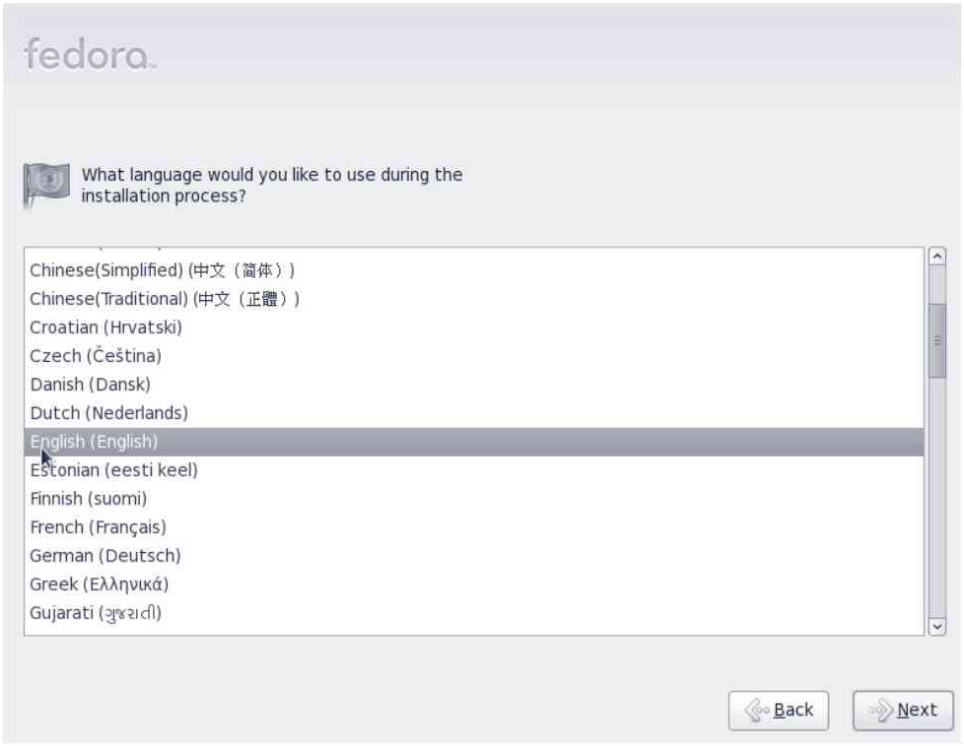


Figura 12-19. Seleccionar idioma

- A continuación debe indicar los dispositivos de almacenamiento que se utilizan durante el proceso de instalación (véase la figura 12-20). Existen dos tipos de dispositivos:
  - **Dispositivos de almacenamiento básicos.** Permite utilizar dispositivos de almacenamiento clásicos como es el caso de discos duros conectados directamente al equipo.
  - **Dispositivos de almacenamiento especializados.** Permite utilizar dispositivos de almacenamiento avanzados que normalmente no se encuentran conectados al equipo. Por ejemplo, permite instalar Fedora en una unidad NAS (sistema de almacenamiento en red).

  Seleccione *Dispositivos de almacenamiento básicos* y pulse *Siguiente.*

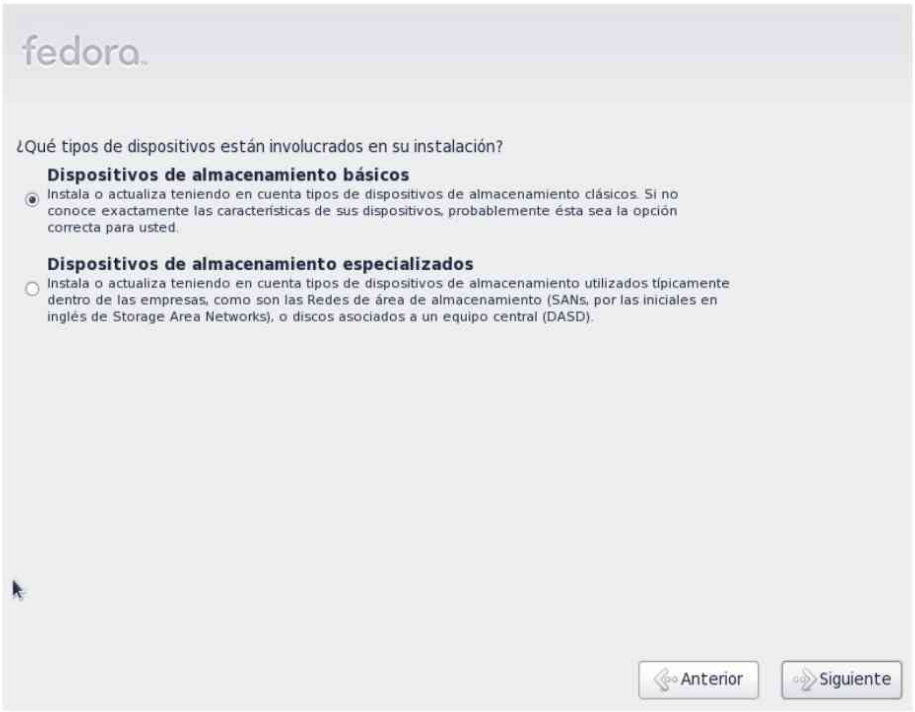


Figura 12-20. Dispositivos involucrados en el proceso de instalación

- Introduzca el nombre del equipo y seleccione la zona horaria.

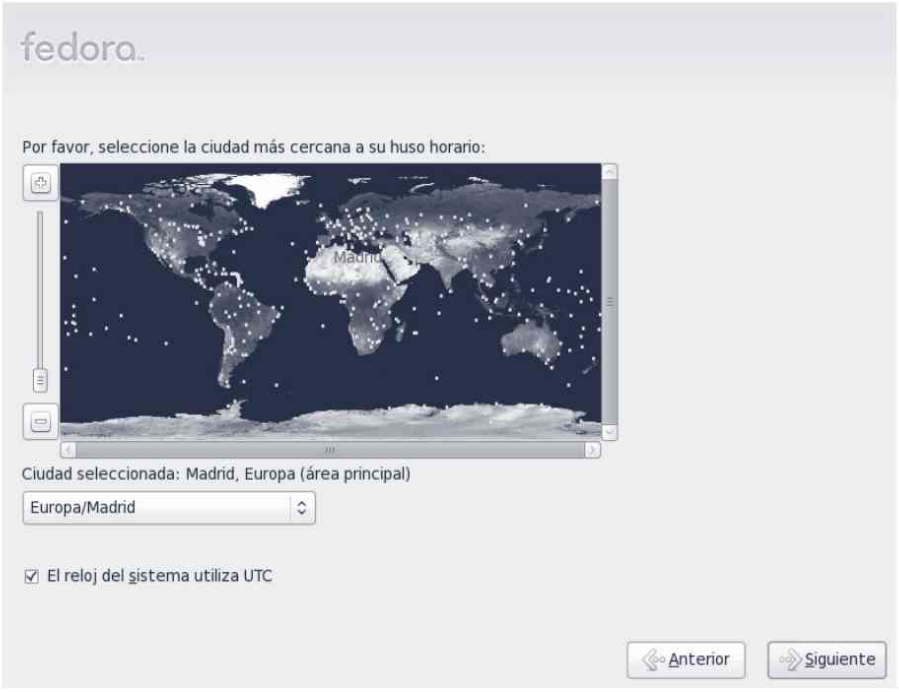


Figura 12-21. Zona horaria

- Introduzca la contraseña para el administrador del sistema (*root*). Es muy importante guardar la contraseña ya que sin ella no puede acceder al sistema.

Particionamiento

- Ahora llega el momento más importante del proceso de instalación y en el que debe tener más cuidado: el particionamiento del sistema de ficheros.

> ***Nota***
>
> *Hay que tener cuidado al crear las particiones porque puede perder la información del sistema.*

Figura 12-22. Particionamiento del sistema

El proceso de instalación permite realizar el particionamiento de forma automática o manual (figura 12-22). De forma automática puede *Usar todo el espacio*, *Reemplazar el sistema Linux existente*, *Achicar el sistema actual* o *Usar el espacio libre.* De forma manual puede utilizar la última opción, *Crear diseño personalizado.*

Si es la primera vez que va a instalar Fedora puede utilizar la opción *Usar todo el espacio* aunque lo recomendable es *Crear el diseño personalizado* para crear el particionamiento dependiendo de sus necesidades. Lo recomendable es crear una partición para el sistema (/) y otra partición swap con al menos el doble de tamaño que la memoria RAM del sistema. En la figura 12-23, puede ver un ejemplo de cómo debe quedar el sistema de ficheros.

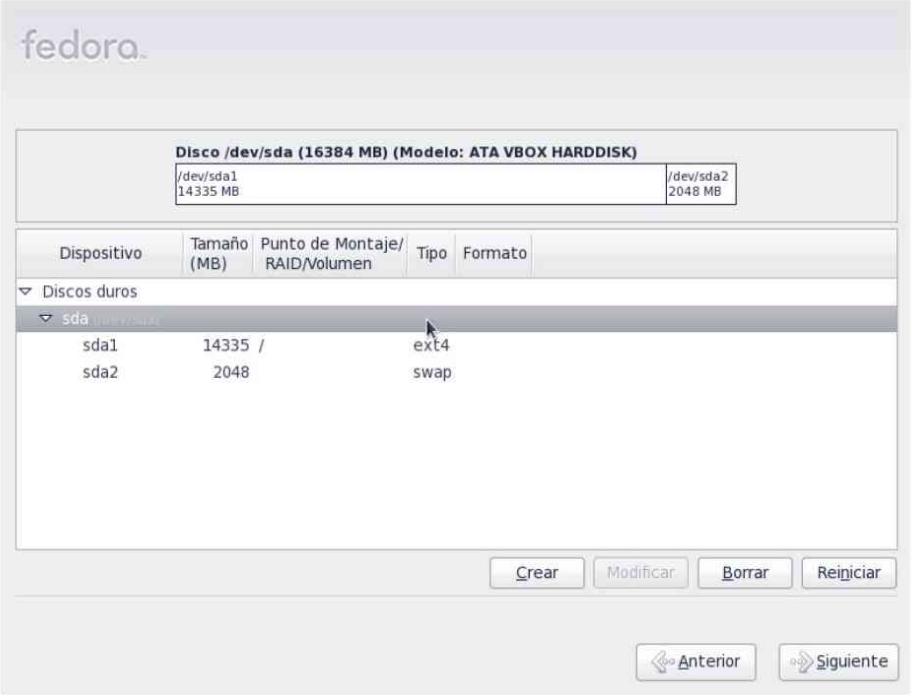


Figura 12-23. Particionamiento manual

- Configure el gestor de arranque para indicar los sistemas operativos que pueden iniciarse en el equipo, el sistema de arranque por defecto y la partición donde se instala el gestor de arranque.
- Seleccione las aplicaciones que desea instalar en el sistema. Tal y como muestra la figura 12-24, puede seleccionar los siguientes grupos de aplicaciones: *Entorno gráfico*, *Desarrollo de software*, *Servidor web* y *Mínima.* Si lo desea, puede personalizar completamente la instalación seleccionando la opción *Personalizar ahora* y pulsando *Siguiente.*

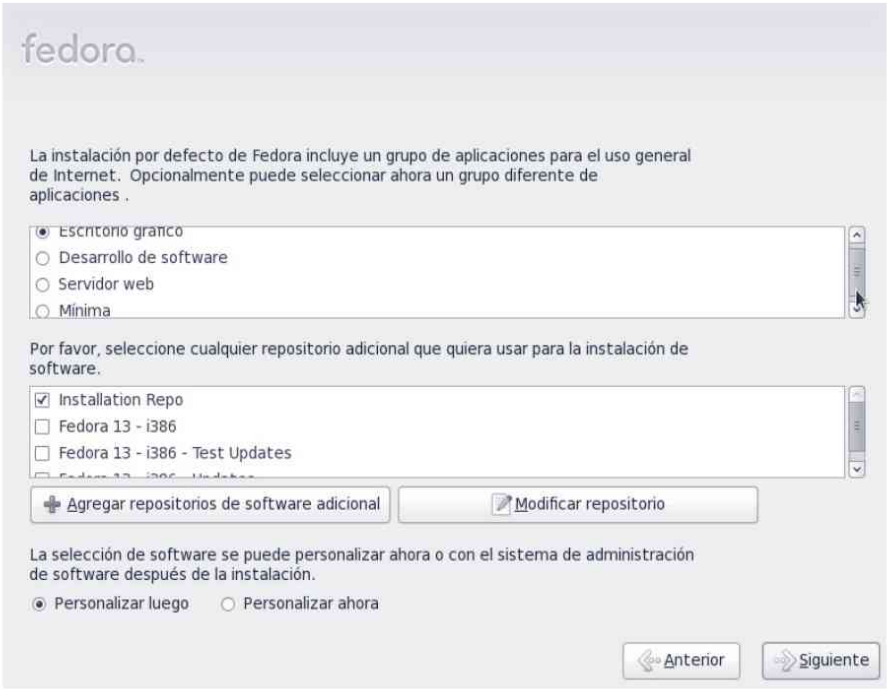


Figura 12-24. Personalizar aplicaciones a instalar

- Se inicia el proceso de instalación.

Figura 12-25. Proceso de instalación

Postinstalación

Ya se ha realizado la instalación del sistema y una vez reiniciado el equipo aparece un asistente que le guiará para realizar los últimos ajustes del sistema:

- Cuando finaliza la instalación se reinicia el sistema y aparece la pantalla de bienvenida de Fedora (véase la figura 12-26).

Figura 12-26. Pantalla de bienvenida

- Acepte los términos de la licencia del sistema.
- Para utilizar el sistema se recomienda utilizar la cuenta de root para tareas muy específicas (p. ej., instalar o configurar un servicio). Para trabajar normalmente con el sistema se recomienda utilizar una cuenta de usuario sin privilegios.

  En este punto de la instalación el sistema permite la creación de una cuenta sin privilegios (véase la figura 12-27). Introduzca los datos del usuario y pulse *Siguiente*.

Figura 12-27. Crear usuario

- Ajuste la fecha y la hora del sistema.
- Para colaborar con el proyecto Fedora puede enviar el perfil de hardware del sistema.
- Para finalizar, el sistema muestra la pantalla de inicio de sesión (véase la figura 12-28). Introduzca el nombre de usuario y contraseña creado en el paso anterior y ya puede utilizar el sistema (véase la figura 12-29).

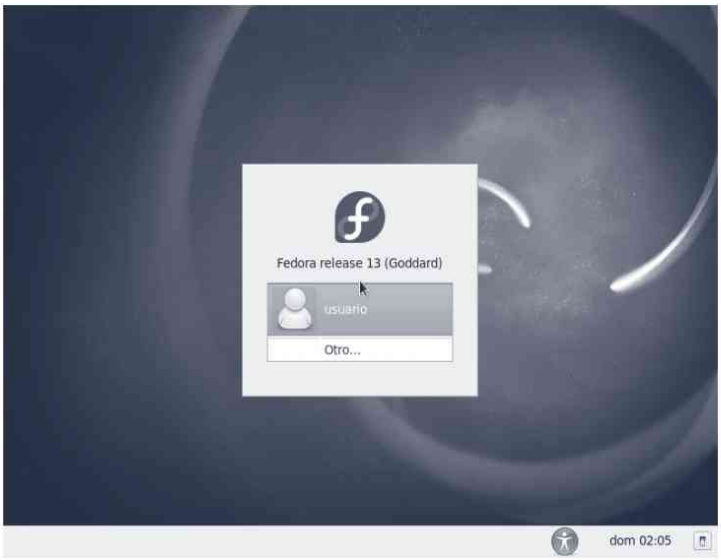


Figura 12-28. Inicio de sesión

Figura 12-29. Dentro del sistema

12.3 X-WINDOWS

Uno de los elementos que ha propiciado la gran expansión de los sistemas GNU/Linux en empresas y hogares es la utilización de entornos gráficos sencillos y amigables. Los sistemas GNU/Linux cuentan con diversos entornos gráficos, muy potentes, que permiten utilizar el sistema fácilmente.

x-Windows (o *sistema de ventanas X*, en castellano) es el nombre por el que se conoce al entorno gráfico usado por los sistemas Unix. Desarrollado desde mediados de la década de los ochenta en el MIT (Instituto Tecnológico de Massachussets) se encuentra actualmente en su versión 11, por lo que normalmente suele ser referenciado como X11. El grupo de desarrollo inicial ha ido dando lugar en el tiempo a diversos sucesores: X Consortion (desde 1994 a 1996), The Open Group (de 1997 a 1998), XFree86 (de 1992 a 2004) y X.org (desde 2004). X.org Fundation se fundó a partir de un grupo de desarrolladores y actualmente se encarga de desarrollar y coordinar el entorno X.

x-Windows proporciona una interfaz gráfica (GUI) al mundo de Linux. x-Windows, al igual que el sistema operativo Windows de Microsoft, ofrece una forma de manejo de algunos de los elementos de interacción más comunes como ventanas, cuadros de diálogo, botones y menús. x-Windows es quien proporciona las capacidades gráficas que hacen de las plataformas basadas en Linux la elección para el desarrollo de muchas aplicaciones de ingeniería y diseño, y es x-Windows el que hace posible que Linux sea un competidor serio en el mercado de los sistemas operativos para PC.

De forma simple, se puede decir que x-Windows es una interfaz gráfica completa para Linux y, por extensión, para Unix. Pero esto no es todo, x-Windows es un entorno muy configurable que proporciona un amplio abanico de opciones para el usuario y para el diseñador de aplicaciones.

x-Windows está compuesto por dos elementos principales: el **servidor X**, encargado de mostrar visualmente los elementos en la pantalla de forma totalmente independiente del sistema operativo, y el **gestor de ventanas**, cuyo objetivo es la gestión y administración de las ventanas mostradas para las aplicaciones, su apariencia, creación, colocación en la pantalla, etc. De esta forma x-Windows es capaz de distribuir el procesamiento de las aplicaciones siguiendo el paradigma cliente-servidor: el servidor provee los servicios para acceder a teclado, ratón y pantalla, mientras que los clientes son las aplicaciones que toman estos recursos para poder interactuar con los usuarios.

Esta forma de diseño *en dos partes* es lo que origina que existan diferentes implementaciones de gestores de ventanas, con diferentes características funcionales y visuales. El *servidor X*, como puede imaginar es altamente portable y en el caso de Ubuntu permite utilizar los tres principales **entornos de escritorio o GUI** (*Graphical User Interfaces* o *Interfaces gráficas de usuario*). GNOME está orientado a la simplicidad, KDE ofrece un mayor conjunto de aplicaciones así como posibilidades de caracterización por defecto, o Xfce está optimizado para su uso con requisitos hardware bajos. Aparte de los citados, Fedora permite usar otros entornos de escritorio como *Fluxbox*, *Sugar* o *LXDE*.

Tabla 12-2. Entornos gráficos más utilizados

	Nombre	URL
	GNOME	*http://www.gnome.org/*
	KDE	*http://www.kde.org/*
	Xfce	*http://www.xfce.org*

UBUNTU

Por defecto Ubuntu Server no utiliza modo gráfico. Si desea instalarlo debe ejecutar:

```
$ sudo apt-get update
$ sudo apt-get install x-window-system-core gnome-core
```

y para iniciar el entorno gráfico ejecute:

```
$ startx
```

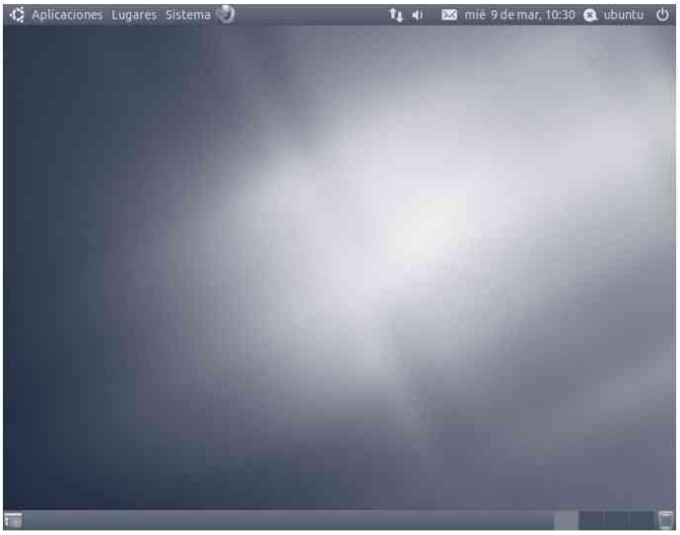


Figura 12-30. Entorno gráfico de Ubuntu

12.4 PRIMEROS PASOS

Una de las grandes ventajas de los sistemas GNU/Linux es que se adapta completamente al nivel de conocimientos del usuario. Hoy en día, a través de los asistentes y los entornos gráficos es posible utilizar fácilmente los sistemas GNU/Linux sin necesidad de tener amplios conocimientos sobre el sistema.

Por supuesto, cuantos más conocimientos tenga mejor puede aprovechar las prestaciones del sistema. A continuación se van a comentar las tareas más frecuentes en los sistemas GNU/Linux.

12.4.1 Intérprete de comandos

El intérprete de comandos o shell del sistema es la interfaz entre el usuario y el sistema operativo. La función del shell es recibir las órdenes del usuario a través de la línea de comandos, interpretarlas, ejecutarlas y mostrar su resultado.

Resulta muy útil aprender a utilizar el shell del sistema ya que aunque al principio puede parecer un poco difícil, resulta fundamental para obtener el máximo rendimiento del sistema. El shell permite interactuar directamente con el sistema y con sus ficheros de configuración.

Cuando se inicia el sistema aparece un terminal que le permite hacer "login" (figura 12-31). Para acceder al sistema hay que introducir su nombre de usuario y contraseña.

Figura 12-31. Login

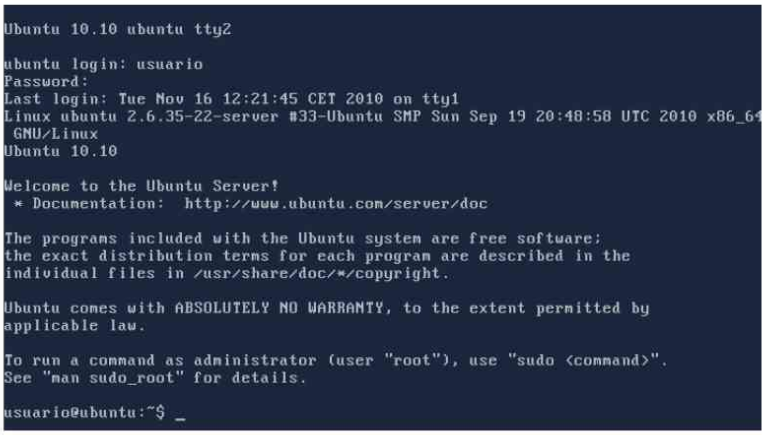


Figura 12-32. Terminal del sistema

Una vez que acceda al sistema se muestra un prompt con un aspecto parecido al siguiente:

```
usuario@ubuntu:~$
```

donde *usuario* es el nombre del usuario que está utilizando, *@ubuntu* indica el nombre del equipo. A continuación se muestra el directorio en el que se encuentra. En el caso de que se encuentre el carácter ~ es porque está en el directorio *home*. Por último, el símbolo $ o # indica si es un usuario normal ($) o es el administrador del sistema (#).

El usuario *root* es el administrador del sistema y puede realizar cualquier tarea de administración. En algunas distribuciones puede acceder directamente al sistema como usuario *root*, pero otras distribuciones, como Ubuntu, le obligan a

acceder al sistema con un usuario sin privilegios de administrador y luego cambiar de usuario.

Si desea ejecutar una tarea de forma puntual como *root* puede utilizar el comando *sudo* de la siguiente forma:

```
$ sudo <comando>
```

Si necesita ejecutar múltiples tareas puede obtener un shell de *root* ejecutando *sudo bash* o *su*:

```
$ sudo bash
#
```

Además, si lo desea, puede activar la cuenta de *root* al establecer su contraseña:

```
$ sudo passwd root
```

Nota

Si se ha iniciado el sistema en modo consola, puede cambiar entre los diferentes terminales pulsando las teclas ALT + F1 (primer terminal), ALT + F2 (segundo terminal), etc.

Aunque a lo largo del libro aprenderá a utilizar el shell del sistema, en la tabla 12-3 puede encontrar algunos de los comando más utilizados.

Tabla 12-3. Comandos más utilizados

Categoría	Comando	Descripción
Manipulación de directorios		
	cd <ruta>	Cambia de directorio.
	cp <origen> <destino>	Copia ficheros o directorios.
	mv <origen> <destino >	Mueve o cambia el nombre de un fichero o directorio.
	rm <fichero>	Borra un fichero o directorio.
	rmdir <directorio>	Borra un directorio.
	cd <directorio>	Cambia de directorio.
	pwd	Muestra el directorio actual de trabajo.
	mkdir <directorio>	Crea un directorio.
	tree	Muestra de forma gráfica la estructura de un directorio.
	find **locate**	Permite buscar ficheros en el sistema.
	ls	Muestra el contenido de un directorio.

Manipulación de ficheros	
touch <fichero>	Crea un fichero vacío.
less <fichero> **more <fichero>** **cat <fichero>**	Muestra el contenido de un fichero.
mv <origen> <destino>	Mueve o cambia el nombre de un fichero o directorio.
cp <origen> <destino>	Copia ficheros o directorios.
rm <fichero>	Borra un fichero o directorio.
locate <fichero>	Busca un fichero o directorio en nuestro equipo.

Particionamiento	
fdisk	Permite administrar las particiones del sistema.
fsck	Permite comprobar el estado de un sistema de ficheros.
mkfs	Permite formatear un sistema de ficheros.
df	Indica el espacio libre de un sistema de ficheros.
du	Indica el espacio utilizado por un usuario en el sistema de ficheros.
mount	Permite montar sistemas de ficheros.
umount	Permite desmontar sistemas de ficheros.

Comandos generales	
startx	Inicia el modo gráfico.
halt	Apaga el equipo.
reboot	Reinicia el equipo.
date	Muestra y permite cambiar la fecha del sistema.
clear	Borra la pantalla.
man	Permite obtener ayuda del sistema.

Procesos	
ps	Muestra los procesos activos del sistema.
top	Muestra los procesos del sistema y su rendimiento.
kill	Permite matar un proceso a partir de su PID.
pkill	Permite matar un proceso a partir de su nombre.

Permisos	
chmod <permisos> <fichero/directorio>	Establece los permisos de un fichero o directorio.
chown <usuario> <fichero/directorio>	Cambia el usuario propietario de un fichero o directorio.
chgrp <grupo> <fichero/directorio>	Cambia el grupo propietario de un fichero o directorio.

Redes	
ifconfig	Permite obtener información y configurar los adaptadores de red.
iwconfig	Permite obtener información y configurar los adaptadores de red inalámbrica.
ping <host>	Permite realizar un ping para comprobar la comunicación con un equipo.
route	Muestra y configura la tabla de enrutado del sistema.
iptables	Muestra y configura el cortafuegos del sistema.

service	Permite administrar los servicios del sistema.

Usuarios	
adduser <usuario>	Da de alta un usuario.
userdel <usuario>	Borra un usuario.
usermod	Permite modificar las propiedades de un usuario.
passwd	Cambia la contraseña de un usuario.
addgroup	Permite dar de alta un usuario dentro de un grupo.
su	Permite cambiar de usuario.
sudo	Permite ejecutar un comando como *root.*
id	Muestra el usuario que se está utilizando.

Grupos	
groups	Muestra los grupos a los que pertenece el usuario.
groupadd	Permite dar de alta a un grupo.
groupdel	Permite borrar un grupo de usuarios.

Consejo

Si desea volver a ejecutar un comando puede utilizar las fechas de los cursores arriba y abajo.

12.4.2 Estructura de directorios

Linux, al igual que UNIX, organiza la información del sistema en una estructura de árbol jerárquico de directorios compuesta de ficheros. Esta estructura se forma mediante un sistema de ficheros raíz (*file system root*) y un conjunto de sistemas de ficheros montables.

Un sistema de ficheros, o *file system*, es una estructura de directorios completa. Para poder utilizar un sistema de ficheros hay que montarlo; o sea, enlazarlo a la estructura de directorios ya existente. Los sistemas de ficheros se montan automáticamente cada vez que se inicia el sistema operativo. Cuando un usuario se conecta al sistema, se encuentra un único árbol de directorios formado por los distintos sistemas de ficheros que se encuentran montados en ese instante. La estructura que aparece al usuario será similar a la que se muestra, de forma abreviada, en la figura 12-33.

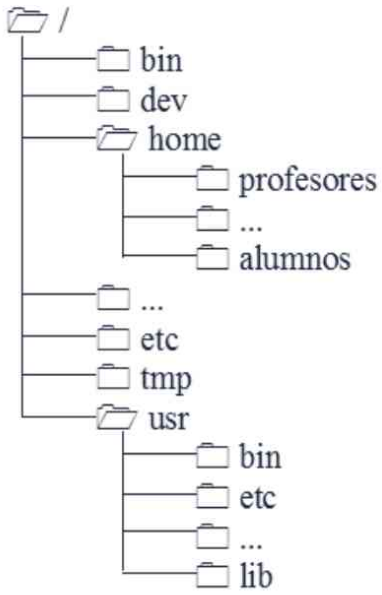


Figura 12-33. Estructura de directorios

Los directorios más importantes que tiene un sistema operativo GNU/Linux son los siguientes:

- ***/bin.*** Comandos y binarios del usuario.
- ***/boot.*** Archivos utilizados para el arranque del sistema.
- ***/dev.*** Dispositivos del sistema.
- ***/etc.*** Ficheros de configuración del sistema.
- ***/home.*** Directorios de trabajo de los usuarios.
- ***/lib.*** Bibliotecas compartidas y módulos del kernel necesarios para ejecutar los programas residentes en */bin* y */sbin*.
- ***/media.*** Directorio donde se suelen encontrar los dispositivos extraíbles como es el caso del CD-ROM.
- ***/mnt.*** Directorio donde se suelen montar los sistemas de archivos temporales.
- ***/proc.*** Es un directorio virtual y en él puede ver toda la información sobre el kernel y los procesos del sistema.
- ***/root.*** Directorio de trabajo del administrador del sistema.

- ***/sbin.*** Ficheros binarios del sistema que suele ejecutar el root.
- ***/tmp.*** Directorio donde se suelen encontrar los ficheros temporales del sistema.
- ***/usr.*** Utilidades, bibliotecas y aplicaciones del usuario.
- ***/var.*** Datos y archivos variables como logs, colas de correo, tareas de impresión, etc.

12.4.3 Instalar y quitar componentes

En GNU/Linux se puede realizar la instalación de una aplicación directamente a partir del código fuente o a través de la aplicación compilada (paquete). A las aplicaciones preempaquetadas se le denomina paquete y contienen los binarios, los archivos complementarios y archivos de configuración para poder ejecutarse.

Para facilitar el proceso de instalación se utilizan gestores de paquetes que facilitan la administración de los paquetes. A continuación va a aprender a instalar aplicaciones de todas las formas posibles: mediante *x-Windows*, mediante gestores de paquetes, directamente con el paquete o a partir del código fuente. Las dos primeras formas son las más fáciles de utilizar y, por tanto, las recomendadas.

12.4.3.1 Ubuntu

synaptic

synaptic es una herramienta de x-Windows que facilita las tareas de instalación y eliminación de software. Para instalarla debe ejecutar:

```
# apt-get install synaptic
```

Una vez completada la instalación para utilizar la herramienta ejecute *Gestor de paquetes Synaptic* que se encuentra en el submenú *Administration* dentro de *System.*

Una vez iniciada la herramienta (véase la figura 12-34) el menú de la izquierda muestra las diferentes categorías de aplicaciones. Si pulsa en una categoría aparecen sus diferentes aplicaciones. Si una aplicación ya se encuentra instalada en el sistema su campo de selección se encuentra activo. Si desea instalar o desinstalar una aplicación solo debe seleccionar o deseleccionar la aplicación y pulsar el botón *Aplicar.*

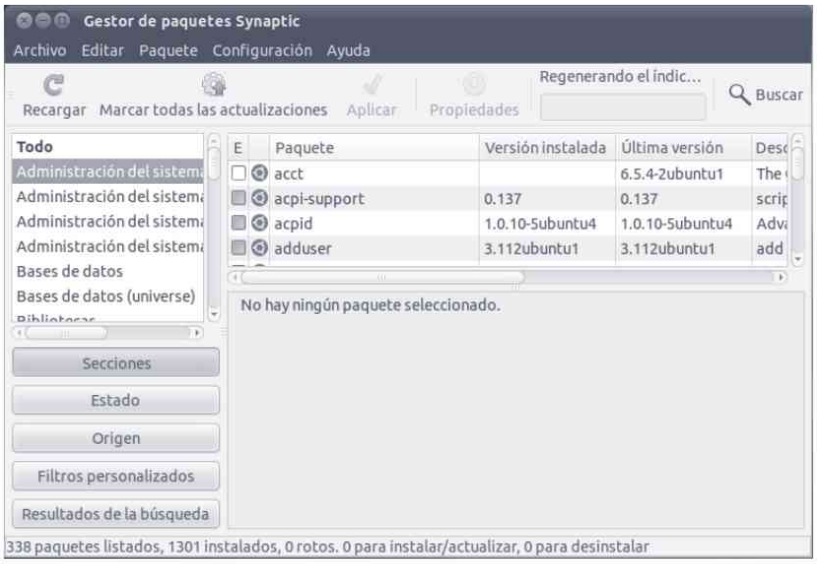


Figura 12-34. Añadir/Quitar software

aptitude

aptitude es un gestor de paquetes por línea de comandos muy cómodo y sencillo de utilizar. Para poder utilizar *aptitude* necesita acceder al sistema como *root*.

```
root@ubuntu ~ #aptitude
```

Una vez ejecutada la herramienta (véase la figura 12-35) puede acceder a las diferentes categorías e instalar o desinstalar el software.

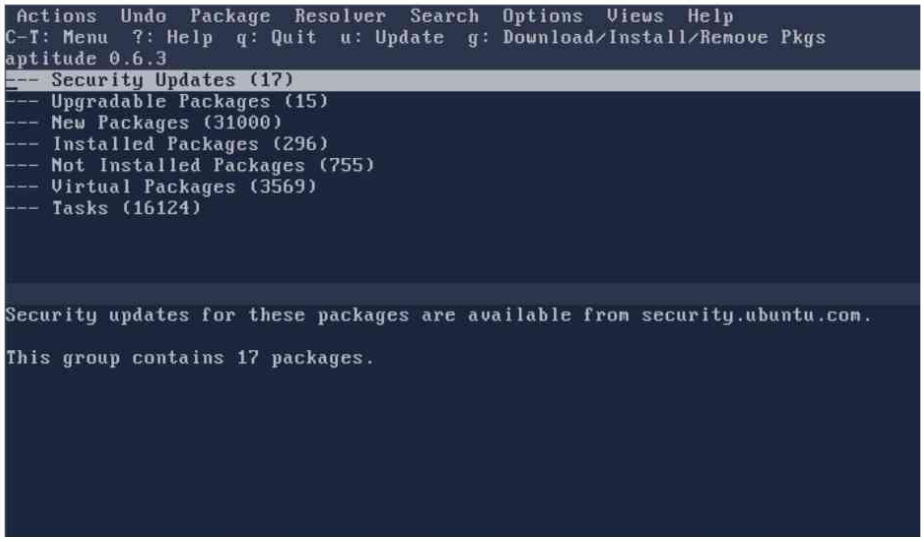


Figura 12-35. aptitude

apt-get

apt-get permite instalar o desinstalar por línea de comandos cualquier paquete. Para empezar, *apt-get* utiliza una serie de repositorios que se encuentran en el fichero */etc/apt/sources.list.* Si lo desea, puede modificar los repositorios del sistema y actualizar el sistema ejecutando:

```
# apt-get update
```

A continuación se van a ver los procedimientos más utilizados:

- **Actualizar el sistema.** Permite actualizar el sistema con todas las dependencias. Se utiliza:

```
# apt-get upgrade
```

- **Búsquedas.** Permite localizar un paquete o término en alguno de los repositorios. Se ejecuta:

```
# apt-cache search <nombre>
```

donde *nombre* indica el nombre del paquete que desea buscar.

- **Consulta de información.** Permite consultar información de un paquete.

```
# apt-cache show <paquete>
```

Por ejemplo si quiere información sobre el servidor web ejecute:

```
# apt-cache show apache2
```

- **Instalación de paquetes.** Permite realizar la instalación de paquetes con la resolución automática de dependencias.

```
# apt-get install <paquete>
```

Por ejemplo si desea instalar el servidor web ejecute:

```
# apt-get install apache2
```

- **Desinstalar un paquete.** Para desinstalar un paquete hay que ejecutar:

```
# apt-get remove <paquete>
```

Por ejemplo si desea desinstalar el servidor web ejecute:

```
# apt-get remove apache2
```

Nota

*A la hora de buscar o instalar un programa puede utilizar el carácter * para indicar cualquier carácter. Por ejemplo, si desea instalar cualquier aplicación que empiece por php entonces debe ejecutar apt-get install php-*.*

A modo de ejemplo, a continuación se va a proceder a la instalación de la aplicación *Writer* de la suite ofimática OpenOffice (*http://www.openoffice.org*) a través del gestor de paquetes *apt*. Si ejecuta:

```
# apt-cache search openoffice
```

puede ver un listado con todas las aplicaciones de *OpenOffice*. Por ejemplo, si desea instalar el procesador de textos *Writer* ejecute:

```
# apt-get install openoffice.org-writer
```

Una vez ejecutado el comando, el sistema busca el paquete *Writer* y resuelve todas las dependencias necesarias para completar el proceso de instalación. Tal y como muestra la figura 12-36, el sistema muestra un resumen de todos los paquetes que debe instalar o actualizar, y solicita que pulse la tecla *s* para iniciar el proceso de instalación.

```
Se instalarán los siguientes paquetes extras:
  libgraphite3 libhyphen0 libicu42 libneon27-gnutls libraptor1 librasqal2
  librdf0 libstlport4.6ldbl libwpd8c2a libwps-0.1-1 openoffice.org-base-core
  openoffice.org-common openoffice.org-core openoffice.org-emailmerge
  openoffice.org-math openoffice.org-style-galaxy python-uno ttf-opensymbol
  uno-libs3 ure xfonts-mathml
Paquetes sugeridos:
  raptor-utils librdf-storage-postgresql librdf-storage-mysql
  librdf-storage-sqlite redland-utils openoffice.org-base
  openoffice.org-style-industrial openoffice.org-style-hicontrast
  openoffice.org-style-tango openoffice.org-style-crystal
  openoffice.org-style-oxygen openoffice.org-gcj
  openoffice.org-filter-binfilter default-jre gcj-jre java-gcj-compat
  openjdk-6-jre sun-java5-jre sun-java6-jre java5-runtime jre
  openoffice.org-java-common cli-uno-bridge otf-stix ttf-lyx
Se instalarán los siguientes paquetes NUEVOS:
  libgraphite3 libhyphen0 libicu42 libneon27-gnutls libraptor1 librasqal2
  librdf0 libstlport4.6ldbl libwpd8c2a libwps-0.1-1 openoffice.org-base-core
  openoffice.org-common openoffice.org-core openoffice.org-emailmerge
  openoffice.org-math openoffice.org-style-galaxy openoffice.org-writer
  python-uno ttf-opensymbol uno-libs3 ure xfonts-mathml
0 actualizados, 22 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 70,0MB de archivos.
Se utilizarán 235MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? _
```

Figura 12-36. apt-get install openoffice.org-write

Una vez descargados todos los componentes, el sistema inicia automáticamente el proceso de instalación y al finalizar muestra un resumen del proceso.

Una vez completada la instalación ya tiene disponible la aplicación que se encuentra dentro del menú *Office* dentro de *Aplications.*

Figura 12-37. Write de OpenOffice instalado en el sistema

Nota

Puede definir repositorios adicionales para aumentar la disponibilidad de software del sistema. Un repositorio es una ubicación de red que almacena paquetes de software junto a los metadatos que los describe.

DEB

Si lo desea puede realizar la instalación o desinstalación directa de un paquete. Para realizar la instalación debe descargar previamente el paquete y ejecutar:

```
# dpkg -i nombre_paquete
```

Si por el contrario desea eliminar un paquete, primero debe conocer su nombre exacto. Para ello debe ejecutar:

```
# dpkg-query -s <nombre>
```

Una vez que conoce el nombre exacto se realiza la instalación ejecutando:

```
# dpkg -r <nombre_completo>
```

12.4.3.2 Fedora

Añadir/quitar software en GNOME

x-Windows ofrece la herramienta *Añadir/quitar software* que facilita las tareas de instalación y eliminación de software. Para utilizarla tan solo debe

ejecutar la herramienta *Añadir/quitar software* (véase la figura 12-38) que se encuentra dentro del menú *Sistema* en *Administración*.

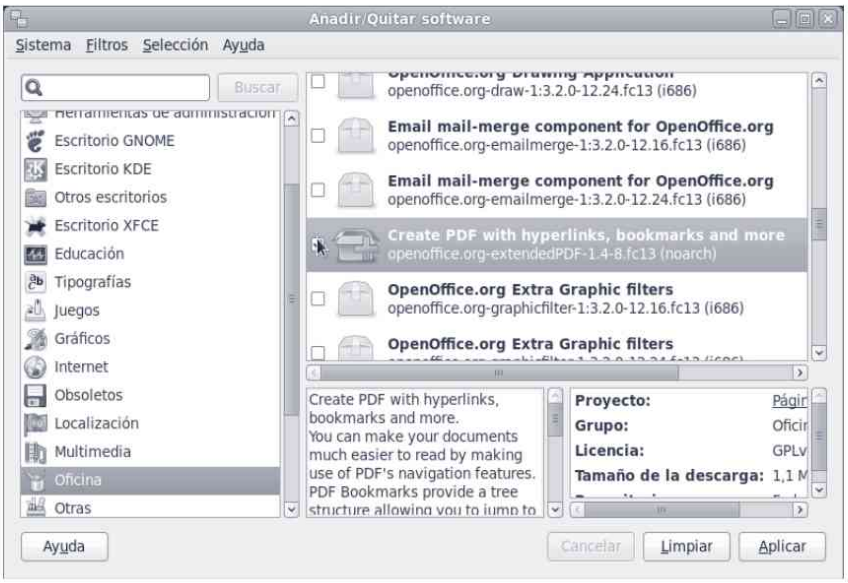


Figura 12-38. Añadir/quitar software

yum

yum (*Yellowdog Updater Modified*) es un gestor de paquetes por línea de comandos muy cómodo y sencillo de utilizar. Para poder utilizar *yum* necesita ser el administrador del sistema.

```
[root@localhost ~]  #
```

A continuación se van a ver los procedimientos más utilizados:

- **Actualizar el sistema.** Para actualizar el sistema ejecute:

```
# yum update
```

- **Búsquedas.** Si desea localizar algún paquete o término en alguno de los repositorios ejecute:

```
# yum search <nombre>
```

donde *nombre* indica el nombre del paquete que desea buscar.

- **Consulta de información.** Si desea consultar la información de un paquete ejecute:

```
# yum info <paquete>
```

Por ejemplo, si desea información sobre el servidor web ejecute:

```
# yum info httpd
```

- **Instalación de paquetes.** Para realizar la instalación de paquetes con la resolución automática de dependencias ejecute:

```
# yum install paquete
```

Por ejemplo si desea instalar el servidor web ejecute:

```
# yum install httpd
```

- **Desinstalar un paquete.** Para desinstalar un paquete ejecute:

```
# yum remove <paquete>
```

Por ejemplo, para desinstalar el servidor ejecute:

```
# yum remove httpd
```

Nota

*A la hora de buscar o instalar un programa puede utilizar el carácter * para indicar cualquier carácter. Por ejemplo, si desea instalar cualquier aplicación que empiece por php entonces debe ejecutar yum install php-**

RPM

El comando *rpm* permite realizar la instalación o desinstalación directa de un paquete. Para realizar la instalación debe descargar previamente el paquete y ejecutar:

```
# rpm -i <nombre_paquete>
```

Si por el contrario desea eliminar un paquete, primero debe conocer su nombre exacto. Para ello ejecute:

```
# rpm -q <nombre>
```

Una vez que conoce el nombre exacto ejecute:

```
# rpm -e <nombre_paquete completo>
```

Por ejemplo, a continuación se busca y desinstala el paquete del servidor apache (httpd):

```
[root|@localhost ~] # rpm -q httpd
httpd-2.2.15.1.fc12.2.i686
[root|@localhost ~] # rpm -e httpd
```

URL de interés

En http://rpmfind.net/ puede encontrar cualquier paquete rpm para instalarlo en el sistema.

12.4.3.3 Utilizando el código fuente

A veces se encuentran aplicaciones que no proporcionan paquetes de instalación, y hay que compilar a partir del código fuente. Para ello, lo primero que debe realizar es instalar las herramientas de compilación ejecutando:

UBUNTU

```
# apt-get install build-essential
```

FEDORA

```
# yum groupinstall build-essential
```

Al realizar la instalación directamente desde el código fuente, es posible que surja algún problema de dependencias. Si sucede esto, entonces debe resolver la dependencia y continuar con el proceso de instalación.

En general, los pasos a seguir para compilar una aplicación son los siguientes:

1. Descargue el código fuente.
2. Descomprima el código, generalmente está empaquetado con *tar* y comprimido con *gzip (*.tar.gz* o **.tgz*) o *bzip2* (**.tar.bz2*).
3. Acceda a la carpeta creada al descomprimir el código.

4. Ejecute el script *./configure* que permite comprobar las características del sistema que afectan a la compilación y crea el archivo *makefile*.

5. Compile el código ejecutando el comando *make.*

6. Instale la aplicación en el sistema ejecutando *make install*. Si desea desinstalar la aplicación entonces ejecute *make clean.*

12.4.4 Webmin

Webmin (*http://www.webmin.com*) es una interfaz web que permite administrar el sistema de una forma cómoda y sencilla a través de cualquier equipo utilizando un navegador web.

Figura 12-39. http://www.webmin.com

El proceso de instalación de *webmin* es muy sencillo, ya que una vez descargado el paquete de la web oficial, debe ejecutar el comando:

UBUNTU

```
# dpkg -i webmin-1.530_all.deb
```

FEDORA

```
# rpm -i webmin-1.530_all.rpm
```

Figura 12-40. Instalación de webmin

Tal y como puede ver en la figura 12-40 una vez finalizado el proceso de instalación, el sistema informa que hay que acceder a webmin a través de la dirección *https://localhost:10000*. Al acceder a webmin debe autenticarse en el sistema, por lo que debe introducir como nombre de usuario *root* y su contraseña.

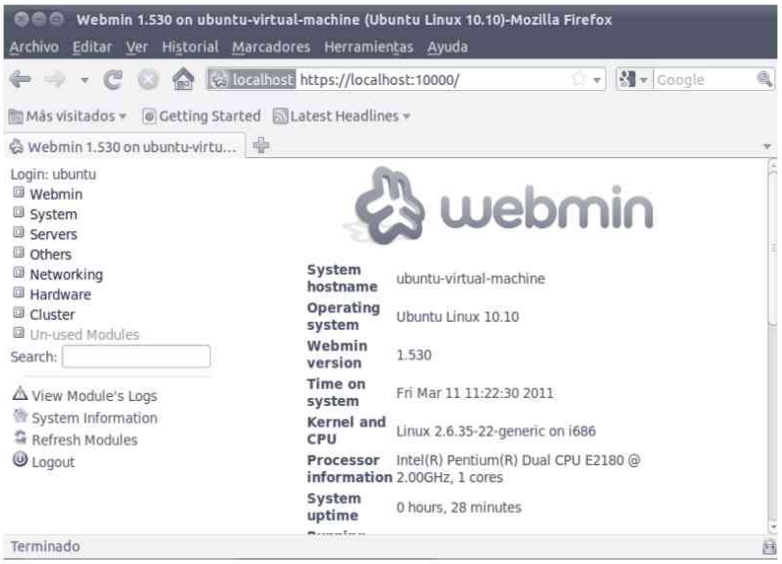


Figura 12-41. Página inicial de webmin

Una vez dentro en la página principal (figura 12-41) el sistema muestra un resumen del sistema y desde el menú de la derecha puede acceder a las diferentes herramientas de administración del sistema. Por ejemplo, en la figura 12-42 se muestra la herramienta *Users and Groups* que permite administrar los usuarios y grupos del sistema.

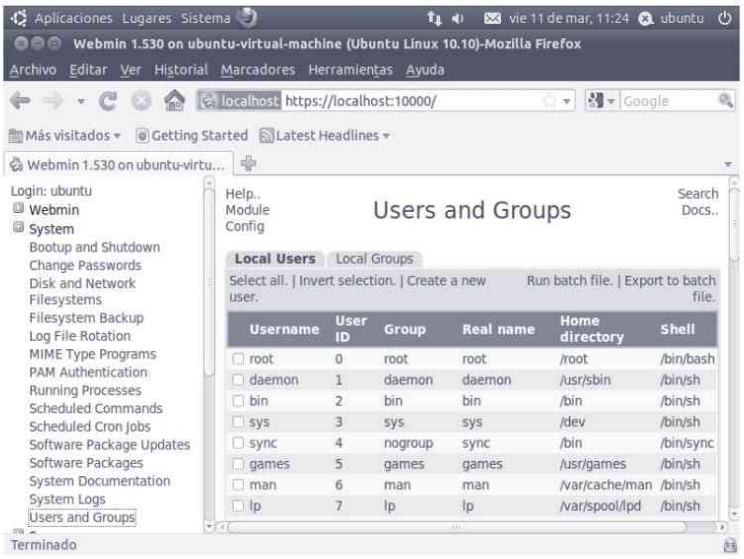


Figura 12-42. Administrando los usuarios y grupos del sistema con webmin

Capítulo 13

PUESTA EN MARCHA DEL SISTEMA

Existen varias formas de administrar el sistema que van variando dependiendo de su facilidad o control sobre el sistema. Básicamente, puede administrar el sistema a través de tres formas diferentes:

- **Interfaces gráficas.** Existen diferentes interfaces gráficas que permiten administrar el sistema de una forma fácil y sencilla. Puede utilizar la interfaz de administración de x-Windows o utilizar la web de administración (webmin). Este método es el más sencillo, pero es el que menos control proporciona sobre el sistema.
- **Terminal del sistema.** Una de las ventajas de los sistemas GNU/Linux es que puede administrarlo totalmente a través del intérprete de comandos o terminal del sistema. El terminal del sistema permite una gran flexibilidad a la hora de interactuar con el sistema pudiendo crear pequeños programas (*scripts*) para simplificar la administración del sistema.
- **Ficheros de configuración.** Por último, la modificación directa de los ficheros de configuración es el método que permite tener un mayor control del sistema. Como desventaja hay que destacar que para administrar el sistema de esta forma hay que conocer muy bien el sistema.

No se puede decir que un método sea el mejor siempre ya que el uso de un método u otro depende siempre de la tarea que desea realizar y de sus conocimientos. Lo mejor, como siempre, es conocer los tres métodos y utilizar el mejor en cada momento.

13.1 ADMINISTRACIÓN DE USUARIOS

Linux es un sistema operativo multiusuario. Esto significa que permite a varios usuarios que utilicen el sistema simultáneamente a través de la línea de comandos o conexiones remotas. Linux controla el acceso al equipo y a sus recursos a través de las cuentas de usuarios y grupos.

En los sistemas GNU/Linux existen tres tipos de usuarios:

- **Root.** Es el usuario más importante ya que es el administrador y dueño del sistema. Se aconseja utilizar la cuenta de *root* para las tareas específicas de administración y el resto del tiempo utilizar una cuenta de usuario normal.
- **Usuarios normales.** Son los usuarios que pueden iniciar sesión en el sistema y tienen una funcionalidad limitada tanto en los comandos que pueden ejecutar como a los ficheros a los que tiene acceso.
- **Usuarios asociados a servicios.** Este tipo de usuarios no pueden iniciar sesión en el sistema. Su utilización es muy útil ya que permiten establecer los privilegios que tiene un determinado servicio. Por ejemplo, el servidor de páginas Web tiene asociado un usuario para poder especificar a qué ficheros tiene acceso y, por tanto, qué ficheros son visibles a través de Internet.

Todos los usuarios del sistema tienen un identificador de usuario (UID) y un identificador de grupo (GID). El administrador del sistema *root* tiene los identificadores de usuario y grupo 0:0 y los demás usuarios tienen un valor mayor que 0.

13.1.1 Intérprete de comandos

La gestión de usuarios y grupos se puede realizar directamente a través del intérprete de comandos. En la tabla 13-1 se muestran los comandos más importantes para la gestión de usuarios y grupos.

Tabla 13-1. Comandos más utilizados (usuarios)

Categoría	Comando	Descripción
Usuarios		
	adduser <usuario>	Permite dar de alta a un usuario. Cuando da de alta un usuario el sistema solicita sus datos como nombre completo, dirección, contraseña, etc.
	addgroup	Permite dar de alta un usuario dentro de un grupo.
	chage	Permite establecer los períodos de vigencia de las contraseñas.
	id	Muestra el usuario que se está utilizando.

passwd	Permite cambiar la contraseña de un usuario. Si ejecuta *passwd* cambia la contraseña del usuario actual y si ejecuta *passwd nombre_usuario* cambia la contraseña del usuario indicado.
su	Permite cambiar de usuario.
sudo	Permite ejecutar un comando como *root*.
userdel <usuario>	Permite borrar un usuario.
usermod	Permite modificar las propiedades de un usuario.

Grupos

groups	Muestra los grupos a los que pertenece el usuario.
groupadd	Permite dar de alta a un grupo.
groupdel	Permite borrar un grupo de usuarios.
groupmod	Permite modificar las propiedades de un grupo.

Manipulación del fichero *letc/shadow*

pwconv	Crea y actualiza el fichero */etc/shadow*.
pwunconv	Desactiva el fichero */etc/shadow*.

Por ejemplo a continuación se va a dar de alta el usuario *javier* en el sistema.

UBUNTU

```
root@ubuntu:~# adduser javier
Añadiendo el usuario "javier" ...
Añdiendo el nuevo grupo "javier" (1003) ...
Añadiendo el nuevo usuario "Javier" (1002) con grupo
"Javier"...
Creando el directorio personal "/home/Javier" ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: password updated successfully
Changing the user information for javier
Enter the new value, or press ENTER for the default
        Full Name []: Javier
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
¿Es correcta la información? [S/n] S
root@ubuntu:~#
```

FEDORA

En el caso de utilizar Fedora primero hay que crear el usuario y luego establecer la contraseña ejecutando:

```
# adduser javier
# passwd javier
Cambiando la contraseña del usuario javier.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: todos los tokens de autenticación se
actualizaron exitosamente.
```

13.1.2 Ficheros utilizados

Siempre resulta muy útil conocer el funcionamiento interno del sistema operativo para poder tener un mayor control de las operaciones que realiza. Para conocer el funcionamiento interno debe conocer dos tipos de ficheros: aquellos ficheros que se utilizan para guardar la información de los usuarios y grupos, y los ficheros con los valores predeterminados que utiliza el sistema.

La información de las cuentas de usuario y grupos se encuentra en los siguientes ficheros:

- **/etc/passwd.** En este fichero se encuentra un listado de las cuentas de usuario que están dados de alta en el sistema.
- **/etc/shadow.** En este fichero se encuentran cifradas las contraseñas y sus períodos de vigencia.
- **/etc/group.** Listado de grupos activos en el sistema y usuarios que pertenecen a dichos grupos.

En el fichero */etc/passwd* se almacenan los datos de las cuentas de los usuarios. A continuación se muestra el fragmento de código de un usuario:

```
javier:x:1000:1000::/home/javier:/bin/bash
```

Como puede ver en el ejemplo anterior, para cada usuario se almacena la siguiente información:

```
Login:x:UID:GID:Descripción:Directorio de trabajo: Shell del
usuario
```

Nota

Es recomendable asignar a los servicios del sistema el shell /bin/false en Ubuntu y /sbin/nologin en Fedora para que no puedan iniciar sesión en el sistema.

Por motivos de seguridad, las contraseñas de los usuarios se almacenan en el fichero */etc/shadow* y no en el fichero */etc/passwd.* Por ejemplo, para el usuario anterior en el fichero */etc/password* en vez de almacenar la contraseña se guarda el carácter *x* y en el fichero */etc/shadow* se almacena la contraseña cifrada.

A continuación se muestra la estructura del fichero **/etc/shadow**:

```
nom:pass:changed:minlife:maxlife:warn:inactive:expired:unused
```

Los valores que se guardan en el fichero son:

- **nom.** Nombre del usuario.
- **pass.** Contraseña cifrada.
- **changad.** Fecha del último cambio del password.
- **minlife.** Número de días que han de pasar para poder cambiar la contraseña.
- **maxlife.** Número de días máximo que puede estar con la misma contraseña sin cambiarla.
- **warn.** El número de días que será avisado antes de que la contraseña expire (*maxlife*) y tenga que cambiarla.
- **inactive.** Número de días después de que la contraseña expire. La cuenta se deshabilitará de forma automática si no ha sido cambiada la contraseña.
- **expired.** Fecha en la que la cuenta expira y se deshabilita de forma automática.

A continuación puede ver un ejemplo de una entrada en el fichero */etc/shadow:*

```
javier:$1$h18Yvp9g$ezMH4yDWjHIv/l0R8042i/:12757:0:99999:7:::
```

El fichero ***/etc/group*** almacena los datos de los grupos que han sido dados de alta en el sistema. A continuación se muestra un fragmento del fichero:

```
root:x:0:root,javier
javier:x:1000:
```

Para cada grupo el sistema almacena el nombre del grupo, el identificador de grupo (GID) y los usuarios que pertenecen al grupo. En el ejemplo anterior se puede ver cómo los usuarios *root* y *javier* pertenecen al grupo *root.*

Al dar de alta un usuario si no especifica ningún parámetro el sistema utiliza los valores por defecto. El sistema guarda los valores por defecto en los siguientes ficheros:

- **/etc/default/useradd.** Permite establecer el *shell* que se va utilizar por defecto, el directorio *home* que van a tener los usuarios, etc.
- **/etc/login.defs**. Entre las opciones más importantes permite establecer los datos de expiración de las contraseñas, longitud mínima de las contraseñas, UID y GID mínimos y máximos, etc.

13.1.3 Configuración con asistentes

La administración de los usuarios del sistema se puede realizar gráficamente con la herramienta *Usuarios y grupos* en x-Windows o a través de webmin.

Para utilizar la herramienta de *Usuarios y grupos* antes hay que instalarla ejecutando:

UBUNTU

```
# apt-get install gnome-system-tools
```

FEDORA

```
# yum install system-config-users
```

Inicie la aplicación *Usuarios y grupos* que se encuentra en el submenú *Administración* dentro de *Sistema.* Aparece la ventana *Gestor de usuarios* (véase la figura 13-1) donde puede realizar la administración de los usuarios del sistema de una forma fácil y sencilla.

Figura 13-1. Gestor de usuarios

Para añadir un nuevo usuario pulse el botón *Añadir*, introduzca el nombre de usuario, pulse *Aceptar* y posteriormente introduzca la contraseña del usuario.

Otra forma de administrar los usuarios del sistema es utilizar Webmin. Para ello acceda con un navegador a la dirección *https://127.0.0.1:10000*. Una vez dentro en la página principal y dentro de menú *System* acceda a *Users and groups*.

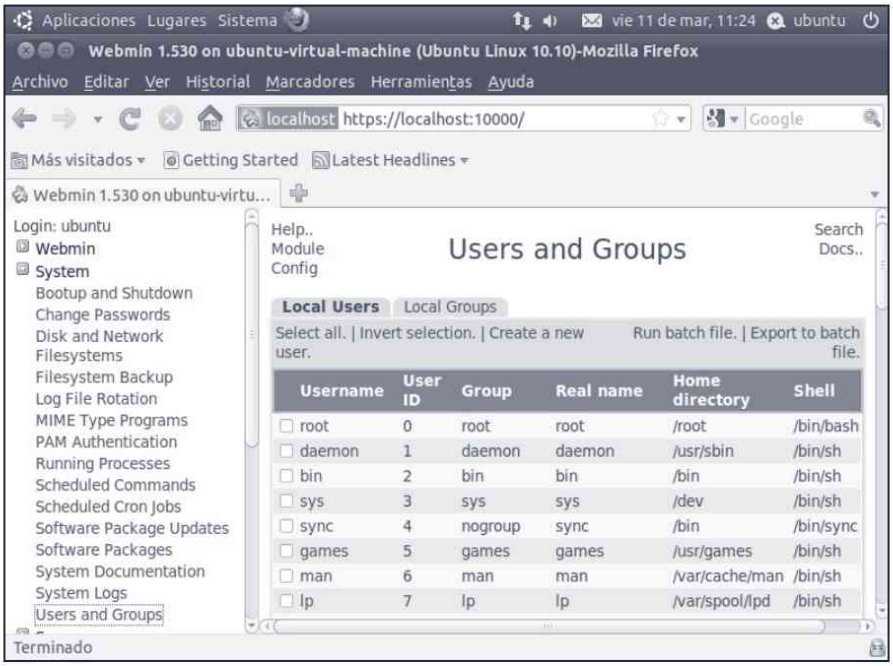


Figura 13-2. Administrando los usuarios del sistema con webmin

13.2 SISTEMA DE FICHEROS

Linux, al igual que UNIX, organiza la información del sistema en una estructura de árbol jerárquico de directorios compuesta de ficheros. Esta estructura se forma mediante un sistema de ficheros raíz (*file system root*) y un conjunto de sistemas de ficheros montables.

Existen diferentes formas de administrar el sistema de ficheros y cada una de ellas proporciona diferentes resultados dependiendo de si desea administrar el sistema utilizando particiones, volúmenes o sistemas RAID.

Nota

Para identificar los discos duros o particiones se utiliza la siguiente sintaxis: /dev/sda1.
Donde:

- ***s** indica el tipo de disco duro: s – discos duros SATA o SCSI; y h para discos IDE.*
- ***a** identifica el primer disco duro, b el segundo, etc.*
- ***1** indica el número de partición dentro del disco duro.*

Así, por ejemplo, /dev/sdb3 identifica la tercera partición del segundo disco duro y /dev/sdb identifica el segundo disco duro.

13.2.1 Particionamiento

La administración de las particiones de los sistemas de ficheros se puede realizar con herramientas gráficas como la *Herramienta de discos Palimpsest*, el *Administrador de volúmenes lógicos* o con el comando *fdisk.*

13.2.1.1 Herramientas gráficas

Las herramientas gráficas más utilizadas para administrar los sistemas de ficheros son: *Editor de particiones Gparted* y *Administrador de volúmenes lógicos.* Para instalar ambas herramientas hay que ejecutar:

UBUNTU

```
# apt-get install gnome-disk-utility
# apt-get install system-config-lvm
```

FEDORA

```
# yum install gparted
# yum install system-config-lvm
```

Si desea iniciar el *Editor de particiones* vaya al menú *System Administration* y ejecute la herramienta *GParted partition editor* (véase la figura 13-3). O si lo desea puede ejecutar la herramienta *Administración de volúmenes lógicos* que se encuentra en el submenú *System Tools* dentro del menú *Aplications* (véase la figura 13-4).

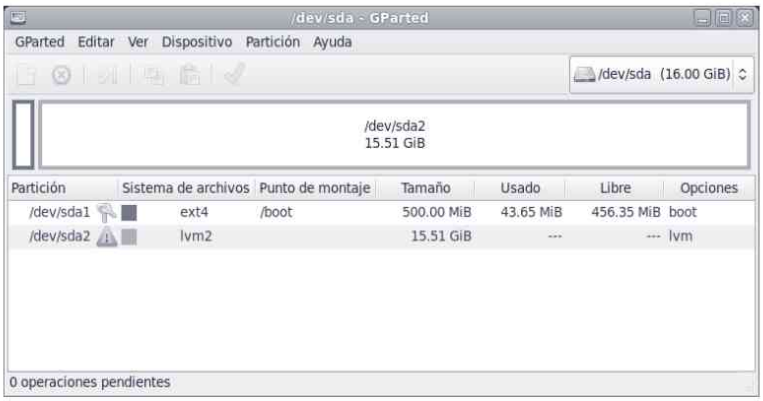


Figura 13-3. GParted partition editor

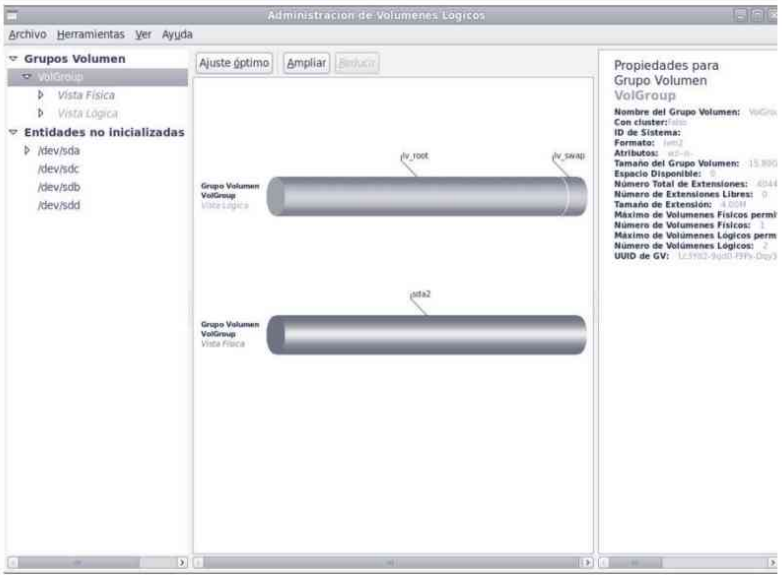


Figura 13-4. Administrador de volúmenes lógicos

13.2.1.2 fdisk

La utilidad *fdisk*, a pesar de que es un poco incómoda de utilizar porque no trabaja bajo una interfaz gráfica, es muy útil y potente. Para aprender mejor, se va a utilizar *fdisk* para crear una partición en uno de los discos duros que tiene libre en el sistema, se formatea y se monta para poder utilizarlo.

Crear la partición

El primer paso que debe realizar es conocer los discos duros y particiones que tiene el sistema. Para ello ejecute:

```
# fdisk -l
```

Tal y como puede ver en la figura 13-5, el equipo tiene dos discos duros (*/dev/sda* y */dev/sdb*). El primer disco duro (*/dev/sda*) tiene dos particiones donde está el sistema operativo (*/dev/sda1*) y la partición swap (*/dev/sda2*). Y el segundo disco duro no contiene ninguna tabla de particiones válida.

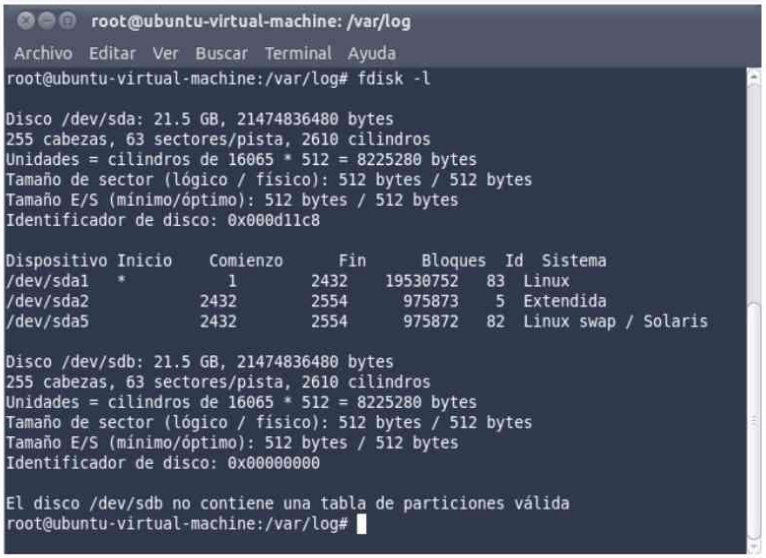


Figura 13-5. fdisk -l

Por ejemplo, si quiere utilizar *fdisk* en el segundo disco duro entonces hay que ejecutar:

```
# fdisk /dev/sdb
```

Una vez dentro del disco duro (véase la figura 13-6) el sistema informa que el disco duro no contiene ninguna tabla de particiones válida. Si desea conocer los comandos disponibles pulse *m*.

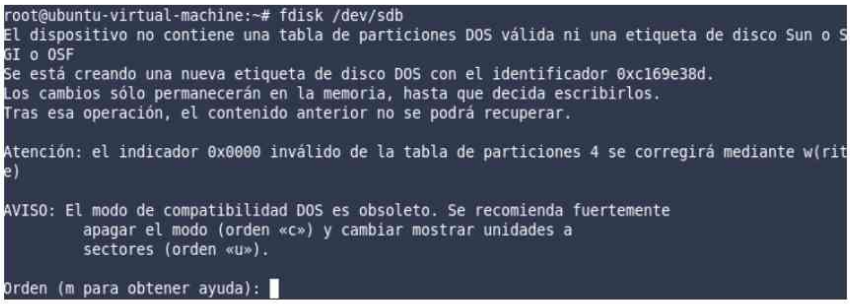


Figura 13-6. fdisk /dev/sdb

En la tabla 13-2 se muestran las opciones más interesantes que proporciona esta utilidad.

Para crear una partición en el sistema pulse *n* y realice los siguientes pasos:

- Seleccione el tipo de partición que quiere crear: (*p*) primaria y (*e*) extendida. Pulse *p*.
- Indique el número de la partición primaria. Como es la primera, pulse *1*.
- Ahora hay que indicar el tamaño de la partición. Para ello el sistema muestra una línea de texto de la siguiente forma:

```
Primer cilindro (1-1044, valor predeterminado 1):
```

Tabla 13-2. Principales parámetros de *fdisk*

Opción	Descripción
a	Permite establecer la partición activa.
d	Suprime una partición.
l	Lista tipos de particiones conocidas.
m	Imprime el menú de ayuda.
n	Agrega una nueva partición.
p	Imprime la tabla de particiones.
q	Salir sin guardar los cambios.
t	Permite cambiar el tipo de sistema de ficheros de una partición.
v	Verifica la tabla de particiones.
w	Guarda los cambios y sale de la aplicación

Pulse directamente *Enter* para que la partición empiece en el inicio del disco duro. A continuación indique el último cilindro. Para especificar el tamaño de la partición puede indicar el número del último cilindro o indicar el tamaño en MBytes que quiere asignarle a la partición de la forma *+tamañoM (p.e.: 1000M)*. Por ejemplo, pulse *Enter* para utilizar todo el disco duro.

Una vez creada la partición, pulse *p* para ver la tabla de particiones. Tal y como se muestra en la figura 13-7 el disco tiene la partición */dev/sdb1*.

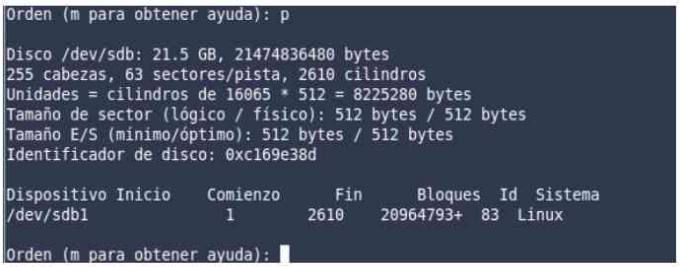


Figura 13-7. fdisk - partición creada

Una vez realizados todos los cambios hay que guardar la configuración y salir de la aplicación, utilizando *w*.

Formateo

Una vez creada la partición, el siguiente paso es formatearla con el comando *mkfs*. Para formatear la partición ejecute:

```
# mkfs /dev/sdb1
```

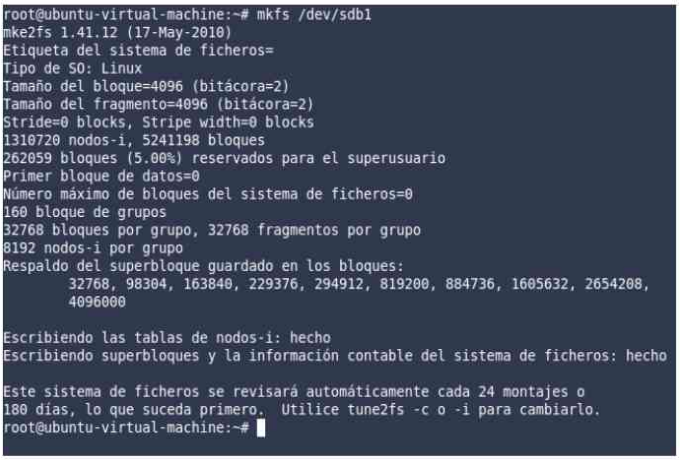


Figura 13-8. mkfs /dev/sdb1

Montar la unidad

Una vez lista la partición */dev/sdb1* para poder utilizarla hay que montarla en un directorio existente.

```
# mkdir /datos
```

Existen dos formas diferentes de montar una partición:

- **Manualmente con el comando *mount.*** Esta opción es la más sencilla y permite montar un sistema de ficheros de forma puntual ya que si se reinicia el ordenador se pierde el punto de montaje.

- **Automáticamente editando el fichero *letc/fstab.*** Esta opción permite montar de forma permanente un sistema de ficheros. Es la mejor opción en el caso de querer utilizar siempre el sistema de ficheros, o si quiere realizar en él acciones especiales como, por ejemplo, utilizar las cuotas de usuarios.

  Para montar manualmente la partición ejecute:

```
# mount /dev/sdb1 /datos
```

Si desea montar de forma definitiva el sistema de ficheros entonces hay que editar el fichero */etc/fstab* y añadir al final la siguiente línea de configuración.

```
/dev/sdb1  /datos ext2   defaults              0 0
```

Una vez modificado el fichero de configuración, la partición se monta automáticamente al reiniciar el equipo o puede montarla ahora ejecutando *mount /datos*.

Para finalizar, si quiere ver que la partición está correctamente montada puede ejecutar el comando *mount* o *df.*

Nota

Hay que tener mucho cuidado al modificar el fichero /etc/fstab ya que se puede dañar el sistema.

13.2.2 Sistemas RAID

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.

Para administrar los sistemas RAID en los sistemas GNU/Linux se utiliza la herramienta *mdadm.*

UBUNTU

En Ubuntu es necesario instalar la herramienta ejecutando:

```
# apt-get install mdadm
```

A modo de ejemplo para crear el sistema RAID hay que ejecutar el comando

```
# fdisk -l
```

y ver los discos duros disponibles en el sistema.

Como se dispone de dos discos duros (*/dev/hdb* y */dev/hdd*), a modo de ejemplo, se va a crear un sistema RAID 1 en espejo. Tal y como muestra la figura 13-9, la herramienta *mdadm* permite crear el raid en */dev/md0* que consta de los dos discos duros. De esta forma, se utiliza directamente */dev/md0* y de forma transparente, se guardan los datos en los dos discos duros.

Para crear el RAID ejecute el siguiente comando donde se especifica el dispositivo que se va a crear (*-C /dev/md0*), el nivel del RAID (*--level=raid1*) y los discos duros que quiere utilizar (*/dev/sdb* y */dev/sdc*):

```
# mdadm -C /dev/md0 --level=raid1 --raid-devices=2 /dev/sdb
/dev/sdc
```

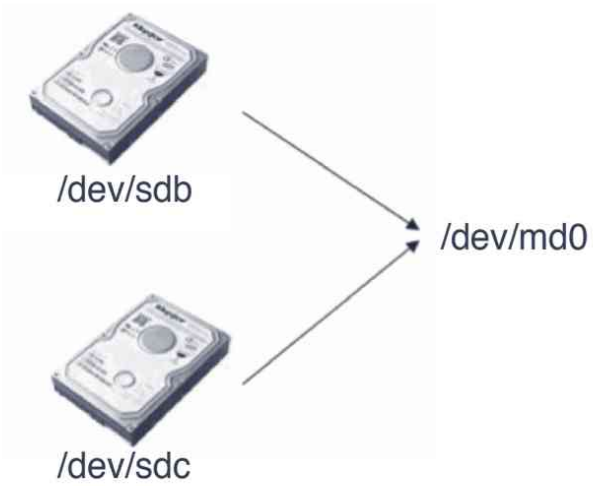


Figura 13-9. Esquema de un sistema RAID en GNU/Linux

```
root@ubuntu:~# mdadm -C /dev/md0 --level=raid1 --raid-devices=2 /dev/sdb /dev/sd
c
mdadm: array /dev/md0 started.
```

Figura 13-10. mdadm -C

Una vez creado el RAID guarde el fichero de configuración */etc/mdadm/mdadm.conf* ejecutando el comando:

```
# mdadm -Es > /etc/mdadm/mdadm.conf
```

```
root@ubuntu:~# mdadm -Es
ARRAY /dev/md0 level=raid1 num-devices=2 UUID=d4675699:9b36f8a4:e368bf24:bd0fce4
1
root@ubuntu:~# mdadm -Es >/etc/mdadm.conf
```

Figura 13-11. mdadm -Es

Otra opción muy útil que permite *mdadm* es obtener información sobre un sistema RAID. Como puede ver en la figura 13-12, el comando muestra

información detallada del sistema raid (tamaño, estado de los discos duros, fecha de creación, etc.).

```
# mdadm --detail /dev/md0
```

Una vez que se encuentra disponible el sistema RAID se puede utilizar como cualquier partición. Tal y como se ha visto en el apartado de particionamiento si quiere utilizar y montar el raid en la carpeta */copia* tiene que ejecutar los siguientes comandos:

```
# mkfs /dev/md0
# mkdir /copia
# mount /dev/md0 /copia
```

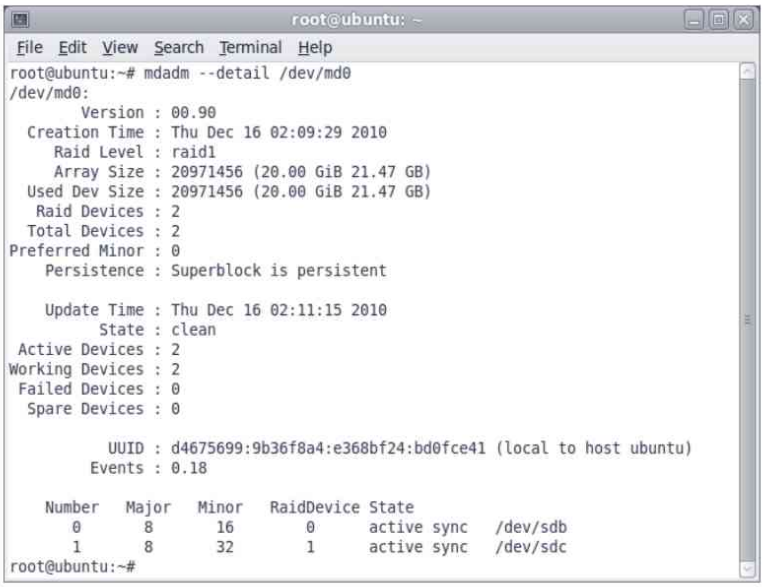


Figura 13-12. Información del RAID

13.2.3 Monitorización

Existen muchas herramientas que permiten monitorizar el sistema de ficheros entre las que destacan:

- **df.** Muestra un resumen sobre el espacio libre que queda en los discos duros del sistema (véase la figura 13-13).

- **du.** Muestra la cantidad de espacio que están utilizando los directorios o archivos específicos. Por ejemplo, si quiere ver el espacio que ocupa el directorio */datos* en MB ejecute:

```
$ du -ms /datos
```

- **fsck.** Permite comprobar el estado y reparar un sistema de ficheros.

```
root@ubuntu-virtual-machine:~# df
S.archivos         Bloques de 1K   Usado    Dispon Uso% Montado en
/dev/sda1            19222656   2711572  15534548  15% /
none                   248268       212    248056   1% /dev
none                   254244       252    253992   1% /dev/shm
none                   254244       104    254140   1% /var/run
none                   254244         0    254244   0% /var/lock
/dev/sda1            19222656   2711572  15534548  15% /prueba
root@ubuntu-virtual-machine:~#
```

Figura 13-13. df

13.2.4 Cuotas de disco

El almacenamiento en disco se puede restringir mediante la implementación de cuotas de disco. Las cuotas se pueden configurar para usuarios individuales o para grupos de usuarios. Las cuotas de disco se pueden establecer mediante tamaño (número de bloques) o mediante el número de archivos que pueden ser creados (inodos). Debido a que los inodos son usados para contener información relacionada a los archivos, estos permiten controlar el número de archivos que pueden ser creados.

En Fedora por defecto se instalan las herramientas de cuota, pero en Ubuntu es necesario instalar el paquete *quota.*

UBUNTU

En Ubuntu es necesario instalar la herramienta ejecutando:

```
# apt-get install quota
```

Para implementar cuotas de disco siga los siguientes pasos:

- Active las cuotas del sistema de archivos modificando el fichero */etc/fstab* y vuelva a montar el sistema de archivos.
- Cree los archivos de cuota y genere la tabla de uso de espacio en disco.
- Asigne las cuotas.

A continuación se describen cada uno de estos pasos en detalle.

13.2.4.1 Activar cuotas

Para activar las cuotas de usuario en un sistema de archivos hay que modificar el archivo */etc/fstab* añadiendo las opciones *usrquota* y/o *grpquota* al sistema de archivos donde se van a activar las cuotas. Por ejemplo, en el siguiente código se activan las cuotas en el directorio */datos*.

```
/dev/md0    /datos     ext2       defaults,usrquota,grpquota 0 0
```

Después de activar las cuotas en el fichero */etc/fstab* hay que volver a montar los sistemas de ficheros. Si el sistema de ficheros no se está utilizando por ningún proceso, use el comando *umount* para desmontar y *mount* para montar el sistema de archivos. Si el sistema de archivos está siendo utilizado, puede reiniciar el equipo o ejecutar la orden:

```
# mount -o remount filesystem
```

donde *filesystem* es el sistema de ficheros donde se aplican las cuotas.

13.2.4.2 Creación de los archivos de cuotas

Después de montar el sistema de archivos hay que prepararlo para soportar cuotas. El comando *quotacheck* examina el sistema de archivos y crea los ficheros necesarios para utilizar las cuotas de usuario.

Para crear los archivos de cuotas (*aguota.user* y *aguota.group*) en el sistema de archivos, use la opción *–c* del comando *quotacheck.* Por ejemplo, para activar las cuotas de usuario y grupo en el directorio */home* se ejecuta el comando:

```
# quotacheck -cug /datos
```

En la tabla 13-3, se muestran las opciones de la orden *quotacheck*.

Si no se especifica ninguna de las opciones *–u* ni *–g*, solo se crea el archivo de cuota de usuario.

Tabla 13-3. Opciones de la orden *quotacheck*

Opción	Acción realizada
a	Verifica todos los sistemas de archivos montados localmente con cuotas activadas.
v	Muestra información de verificación de cuotas.
u	Verifica la información de cuotas de usuario.
g	Verifica la información de cuotas de grupo.
m	Se utiliza si el sistema de ficheros está montado y en uso.

13.2.4.3 Asignación de cuotas

Para configurar las cuotas por usuario se utiliza el comando *edquota*.

Asignación de cuotas por usuario

Si la cuota esta activada en */etc/fstab* para la partición */datos* y ejecuta el comando *edquota usuario_prueba*, se muestra lo siguiente en el editor de cuotas predeterminado por su sistema.

```
Cuotas de disco para usuario javier (uid 1000)
Sist. arch.  Bloques  blando  duro    inodos  blando duro
/dev/md0     24     0        0       0       0      0
```

Filesystem es el nombre del sistema de archivos que tiene la cuota activada. *Blocks* muestra el número de bloques que está usando actualmente el usuario. *Inodes* muestra cuántos inodos está usando actualmente el usuario. *Hard* es el límite máximo absoluto que un usuario o grupo puede utilizar. Una vez que alcance el límite, no se puede utilizar más espacio. *Soft* es el límite máximo temporal que un usuario o grupo puede utilizar. A diferencia de *hard*, el límite definido por *soft* puede ser excedido durante un cierto tiempo. Este tiempo es conocido como período de gracia y puede ser expresado en diferentes unidades de tiempo (segundos, minutos, horas, días, etc.).

Si cualquiera de los valores *hard* o *soft* están especificados a 0, ese límite no está configurado.

Asignación de cuotas por grupo

Para asignar las cuotas por grupos de usuario ejecute el comando *edquota –g <nombre del grupo>* y se obtiene una salida con el siguiente formato:

```
Cuotas de disco para group javier (gid 1000)
Sist. arch.  bloques  blando  duro    inodos  blando duro
/dev/md0     24   0         0      0       0      0
```

Modifique los límites y guarde el archivo.

Advertencia

Si quiere utilizar las cuotas de usuario es muy recomendable montar una unidad para el directorio /home.

Asignación de cuotas por sistema de ficheros

Para asignar las cuotas del sistema de archivos se utiliza el comando *edquota –t*. Al igual que con los comandos anteriores, *edquota* abre el editor de texto con las cuotas actuales.

```
Grace period befor enforcing soft limits for users:
Time units may be: days, hours, minutes, or seocnds
Filesystem       Block grace period        Inode grace period
/dev/hda3        7 days                    7 days
```

13.2.4.4 Verificación de las cuotas de usuario

Para verificar que la cuota ha sido configurada se utiliza el comando *quota.* Y si quiere comprobar la cuota de un determinado usuario ejecute *quota <nombre de usuario>.* Por ejemplo:

```
Disk quotas for user usuario prueba (uid 502)
Filesystem blocks quota limit grace files quota limit grace
/dev/hda5  24      100    300     0      6      0      0      0
```

Para verificar la cuota de un grupo utilice *quota –g <nombre del grupo>*.

13.2.4.5 Generación de informes de cuota

El comando *repquota* genera un informe del uso de cuotas en el sistema de archivos. Por ejemplo, el comando *repquota /home* genera la siguiente salida:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
            Block limits                File limits
User  used  soft hard  grace        used  soft  hard  grace
----------------------------------------------------------
root  --    36      0       0              4     0     0
```

La marca - - que se muestra después del nombre del usuario es una forma rápida de indicar si se han superado los límites. Si el usuario ha superado el límite suave aparece el símbolo + en lugar de -. El primer - representa el límite de bloque, y el segundo el límite de inodo.

Para ver el informe sobre el uso de disco en todos los sistemas de archivos con cuotas, use *repquota –a*.

13.2.4.6 Activación y desactivación de cuotas

Para desactivar las cuotas en el sistema de archivos se utiliza el comando:

```
# quotaoff -aug
```

donde *–u* permite desactivar las cuotas de usuario, y *–g* permite desactivar las cuotas de grupo. Si no indica ninguna opción, por defecto, se desactivarán las cuotas de usuario.

Para activar nuevamente las cuotas, se utiliza el comando *quotaon* con las mismas opciones. Por ejemplo:

```
# quotaon -aug
```

13.3 PERMISOS

Es muy importante establecer correctamente los permisos en el sistema de ficheros para así evitar usos indebidos o pérdidas de datos en el sistema.

Si ejecuta en un directorio el comando *ls –la* puede ver los permisos del sistema de ficheros. Tal y como muestra la figura 13-14, para cada fichero o directorio se muestran los siguientes datos:

- **Permisos.** Indica los permisos que tiene el fichero o directorio.
- **Usuario propietario.**
- **Grupo propietario.**
- **Tamaño del fichero o directorio.**
- **Fecha de creación o de la última modificación.**

- **Nombre.**

Por ejemplo, los permisos para el directorio *documentos* son *drwxrwx---*. El carácter *d* indica que es un directorio. Luego se muestran tres grupos de caracteres (rwx) (rwx) (---) que permiten indicar los permisos del usuario propietario, del grupo propietario y de los demás usuarios.

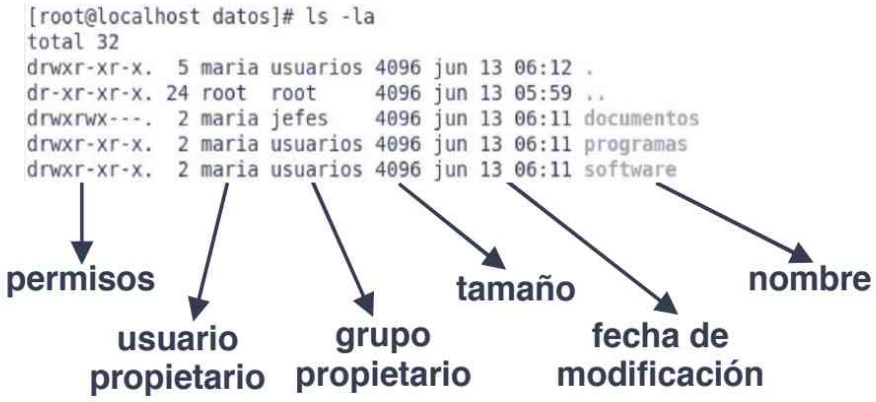


Figura 13-14. Permisos

El formato para establecer los permisos es (*rwx*) donde *r* indica lectura, *w* escritura y *x* indica ejecución. Si existe el permiso entonces se muestra su correspondiente letra y en el caso de que no exista ese permiso entonces aparece el carácter (-).

Por ejemplo, el directorio *documentos* tiene todos los permisos (*rwx*) para el usuario propietario, que es *maria*, el grupo propietario *jefes* también tiene todos los permisos (*rwx*), y el resto de los usuarios no tiene ningún permiso (---).

El directorio *programas* tiene todos los permisos para el usuario propietario *maria* (*rwx*) y tanto para el grupo propietario *usuarios* como el resto de los usuarios tiene permisos de lectura y ejecución (*r-x*).

Nota

En un fichero el permiso de ejecución permite ejecutar un programa y en el caso de los directorios el permiso permite indicar que es posible entrar en ese directorio.

13.3.1 Establecer los permisos

Para definir los permisos de un fichero o directorio se emplea el comando *chmod.* Su sintaxis es:

```
# chmod <modo> fichero
```

donde <*modo*> indica los permisos que le quiere asignar al fichero. Por ejemplo, si quiere establecer los permisos *rw-* para el propietario y *r--* para el resto, el comando que se debe utilizar es:

```
# chmod 644 fichero
```

Con *chmod* se puede establecer los permisos con tres valores numéricos (p. ej., 664): el primer valor corresponde al usuario propietario, el segundo al grupo propietario y el tercer valor corresponde a todos los demás usuarios del sistema.

Cada permiso tiene una equivalencia numérica donde *r* vale 4, *w* vale 2 y *x* vale 1. De esta forma si tiene el valor 7 corresponde a (*rwx*), el valor 6 corresponde a (*rw-*), etc.

13.3.2 Establecer el usuario y grupo propietario

El propietario de un fichero es aquel usuario que creó dicho fichero. Unix permite cambiar al propietario de cualquier fichero o directorio. Opcionalmente se puede cambiar también al grupo al que pertenece dicho fichero o directorio. Para ello se utiliza la orden *chown* que tiene la siguiente sintaxis:

```
chown <NombreUsuario> [.<NombreGrupo>] <fichero>...
```

donde <*NombreUsuario*> identifica el nuevo propietario de fichero o directorio, <*NombreGrupo*> el nuevo grupo y <*fichero*> identifica el fichero o directorio sobre el que se va a actuar.

Por otro lado, para cambiar el grupo al que pertenece un directorio se utiliza *chgrp*. Su sintaxis es:

```
# chgrp <NombreGrupo> <fichero>...
```

donde <*NombreGrupo*> identifica el nuevo nombre de grupo que se le va a asignar al fichero o directorio <*fichero*>. Se puede actuar sobre varios ficheros a la vez.

Nota

En los comandos chmod, chown y chgrp la opción –R significa que se establecen los permisos al directorio y a todos los datos que contiene. Por ejemplo, el comando

```
chmod 777 /datos -R
```

establece todos los permisos a la carpeta datos y a todo su contenido.

Capítulo 14

ADMINISTRACIÓN BÁSICA DEL SISTEMA

14.1 ARRANQUE Y PARADA

Una de las funciones de un administrador de sistemas es poder contestar en todo momento las siguientes preguntas: ¿qué sistema operativo se ejecuta en nuestro sistema?, ¿qué servicios o programas se ejecutan en el sistema?, ¿cuándo se ejecutan? Lógicamente, estos factores afectan muy estrechamente a la seguridad y al rendimiento del sistema.

En este capítulo se abordan los temas necesarios para poder tener control total sobre el proceso y arranque del sistema. Cuando se inicia el equipo primero inicia la BIOS que permite detectar y acceder al hardware del sistema. A partir de ahí, carga el gestor de arranque (que en Linux se llama GRUB) y en el caso de iniciar un sistema GNU/Linux accede al directorio */boot* donde carga el kernel o núcleo del sistema operativo y ejecuta el proceso *init* que es el encargado de iniciar todos los servicios para que el sistema funcione correctamente.

A continuación, se analizan cada uno de los elementos que intervienen en el arranque y apagado del sistema: gestor de arranque (GRUB), proceso de arranque, servicios del sistema, planificación de tareas y parada del sistema.

14.1.1 Gestor de arranque

El gestor de arranque es el encargado de iniciar cualquier sistema operativo que haya sido previamente instalado en el sistema (p. ej., Windows, GNU/Linux, FreeBSD). De forma tradicional el gestor de arranque utilizado en GNU/Linux era LILO, aunque actualmente el gestor de arranque más utilizado en la actualidad es GRUB.

GRUB (*Grand Unified Bootloader*) fue diseñado por Erich Stefan Boleyn y es un gestor de arranque que permite gestionar el inicio del equipo entre diferentes sistemas operativos.

El método que utiliza GRUB para la carga de sistemas operativos Linux es denominado carga directa, ya que el propio gestor de arranque es el encargado de hacerlo directamente y no existe ningún intermediario. Esto último puede ocurrir para la carga de otros sistemas operativos, como por ejemplo, Microsoft Windows. En este último caso el método de arranque es denominado de carga encadenada, en el que el MBR (Master Boot Record o Registro de arranque principal) indica el primer sector de la partición que contiene el sistema operativo.

Hay tres características fundamentales por las que GRUB destaca respecto a otros gestores de arranque:

- proporciona un entorno basado en comandos y previo al sistema operativo, para arquitecturas x86,
- soporta el modo de direccionamiento por bloques lógicos (LBA, Logical Block Addressing), lo que permite cargar sistemas operativos con sus ficheros más allá del cilindro 1.024,
- y puede leer particiones con sistemas de ficheros de tipo ext2 –esto permite al GRUB acceder a sus ficheros de configuración, por lo que la única vez en la que es necesario instalar GRUB en el MBR es al hacerlo por primera vez o si la partición /boot cambia de ubicación.

URL de interés

http://www.gnu.org/software/grub/

14.1.1.1 Instalación

GRUB normalmente se utiliza como gestor de arranque durante el proceso de instalación de prácticamente cualquier distribución GNU/Linux, como Debian o Fedora.

Siempre que realice operaciones sobre el gestor de arranque es muy importante estar seguros de las opciones y parámetros introducidos, ya que es posible dañar el arranque del sistema. Aún así, siempre es posible utilizar alguna utilidad de recuperación del arranque, como por ejemplo **Super GRUB Disk** (*http://www.supergrubdisk.org/*), de libre distribución. Esta herramienta además permite a usuarios avanzados realizar operaciones potencialmente peligrosas en el *MBR (Master Boot Record* o *Registro de arranque principal)* de forma segura.

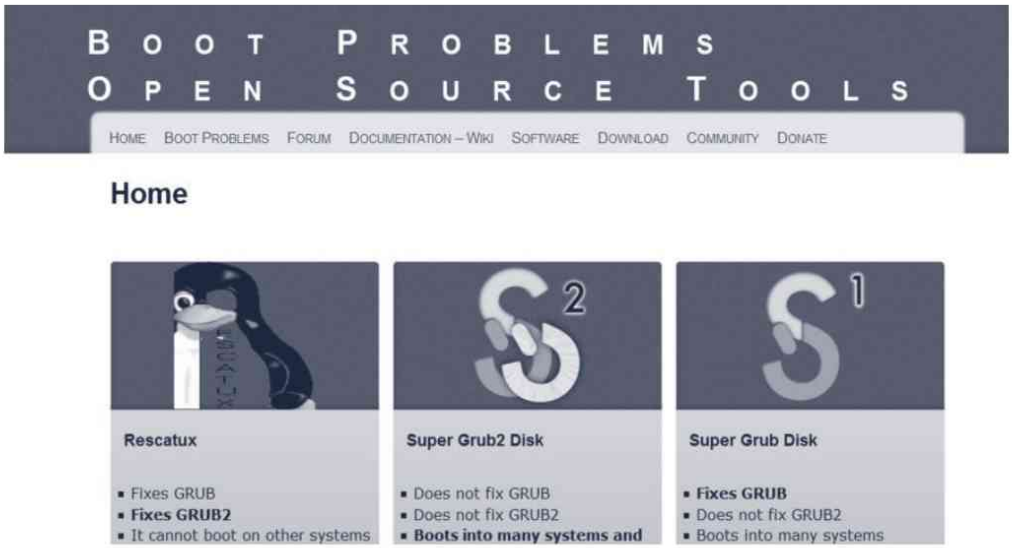


Figura 14-1. Web del proyecto Super GRUB Disk

Para instalar GRUB en el sistema hay que ejecutar:

UBUNTU

```
# apt-get install grub
```

FEDORA

```
# yum install grub
```

Una vez que se ha instalado el paquete *grub* debe sobrescribir el registro de arranque ejecutando:

```
# grub-install <localización>
```

donde <*localización*> se refiere al disco duro en el que se va a instalar el gestor de arranque. Por ejemplo, puede instalar GRUB en el MBR del dispositivo */dev/sda* ejecutando:

```
# grub-install /dev/sda
```

Nota

Para ver los discos duros y particiones del sistema se ejecuta fdisk –l.

Al finalizar, el comando *grub-install* muestra información sobre el éxito o no de la operación, dependiendo de la forma en que haya tenido lugar. De esta forma queda instalado el gestor de arranque GRUB, por lo que la próxima vez, al reiniciar el equipo, aparece el gestor de arranque gráfico GRUB pudiendo seleccionar el sistema operativo (véase la figura 14-2).

Figura 14-2. Gestor de arranque gráfico GRUB

14.1.1.2 Configuración en Fedora

Para realizar la configuración y automatización del menú del gestor de arranque GRUB, debe editar el fichero *grub.conf* o el fichero *menu.lst*, ubicados en el directorio */boot/grub* (*menu.lst* es un enlace a *grub.conf*, por lo que editarlo equivale a hacerlo directamente con el fichero *grub.conf*).

En estos ficheros se encuentra un conjunto de variables y opciones que permiten configurar el comportamiento del menú, cambiar la imagen de fondo para el menú, establecer una contraseña para su uso, cambiar el tiempo de arranque por defecto, etc., así como las diferentes entradas que forman parte del mismo para posibilitar así el arranque de nuevos sistemas operativos en nuestro equipo. En el siguiente listado puede ver un sencillo ejemplo del contenido de este fichero.

/etc/grub.conf

```
default=0
timeout=15
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
```

```
title Fedora (2.6.33.3-85.fc13.i686.PAE)
root (hd0,0)
kernel /boot/vmlinuz-2.6.33.3-85.fc13.i686.PAE ro
root=UUID=b2e88b6c-4b94-
   406d-8778-2ee814a03ed3 rd_NO_LUKS rd_NO_LVM rd_NO_MD rd_NO_DM
   LANG=es_ES.UTF-8 SYSFONT=latarcyrheb-sun16 KEYTABLE=es rhgb
quiet
initrd /boot/initramfs-2.6.33.3-85.fc13.i686.PAE.img

title WindowsXP
rootnoverify (hd0,1)
chainloader +1
```

Como se indica en el fichero anterior, para mostrar la partición raíz del sistema se realiza de la siguiente forma:

```
root (hd0,0)
```

Nota

El gestor de arranque GRUB nombra los discos duros como (hd0), (hd1),..,(hdN), siendo (hd0) el primer disco duro reconocido por la BIOS sin hacer distinciones entre discos de tipo SCSI o IDE.

Para hacer referencia a las particiones de un disco tiene que hacerlo respecto al disco al que pertenecen, comenzando a numerar también por cero. Por ejemplo, (hd0,0) es la primera partición del primer disco duro, (hd0,1) es la segunda partición del primer disco duro, etc.

En caso contrario, puede omitir parte de las rutas al ser éstas relativas al directorio */boot*. En la tabla 14-1 puede ver las opciones más comunes a la hora de configurar GRUB, su significado y un ejemplo con posibles valores que puede tomar. El contenido del fichero puede ser dividido en dos secciones: la primera, que comprende las cinco primeras opciones de la tabla, contiene opciones generales para el gestor de arranque y su modo de operar, sobre todo en lo que respecta a su visualización; la segunda sección, en cambio, recoge las opciones y características particulares que definen cada entrada del menú, por lo que se repiten para cada uno de los sistemas de los que quiere disponer al inicio. En función de nuestras necesidades puede comentar o descomentar algunas de las opciones para que sean obviadas por GRUB o no, respectivamente.

Tabla 14-1. Opciones de configuración para GRUB en *grub.conf*

Opción	Significado	Ejemplo
Opciones generales		
boot	Permite indicar la ruta de acceso al directorio *boot* si es que éste se encuentra en una partición independiente. Si el directorio se encuentra en la partición raíz, aparece comentada.	*#/boot=/dev/sda*
default	Contiene el identificador del sistema que se inicia por defecto.	*default=0*
timeout	Tiempo que se muestra el menú de arranque antes de iniciar el sistema operativo por defecto.	*timeout=15*
splashimage	Imagen que se muestra en el menú de arranque.	*splashimage=(hd0,0)/grub/splash.xpm.gz*
hiddenmenu	Permite ocultar la selección de los diferentes sistemas. En su lugar aparece un mensaje que sugiere presionar la tecla *escape* para mostrarlos.	*hiddenmenu*
password	Permite establecer la contraseña del menú de arranque.	*password contraseña*
Opciones de arranque para sistemas GNU/Linux		
title	Título identificativo del sistema operativo.	*title Fedora (2.6.33.3-85.fc13.i686.PAE)*
root	Permite indicar la ubicación para los ficheros de arranque.	*root (hd0,0)*
kernel	Permite indicar el fichero del núcleo del sistema operativo así como las características de su carga y parámetros en el arranque. También puede especificar la etiqueta o la partición en la que se encuentra el directorio raíz.	*kernel /boot/vmlinuz-2.6.33.3-85.fc13.i686.PAE ro root=UUID=b2e88b6c-4b94-406d-8778-2ee814a03ed3 rd_NO_LUKS rd_NO_LVM rd_NO_MD rd_NO_DM LANG=es_ES.UTF-8 SYSFONT=latarcyrheb-sun16 KEYTABLE=es rhgb quiet*
initrd	Indica la localización de la imagen de disco RAM utilizada en la carga del sistema: fichero comprimido que contiene una imagen del sistema de archivos temporal que es cargada en memoria y que es utilizada como disco RAM en el proceso de arranque.	*initrd /boot/initramfs-2.6.33.3-85.fc13.i686.PAE.img*
Opciones de arranque para otros sistemas		
rootnoverify	Similar a la opción root, es usada para no montar la partición ya que el sistema de ficheros es diferente al de Linux, como UFS para FreeBSD o NTFS para Windows.	*rootnoverify (hd0,1)*
chainloader +1	Para una determinada entrada permite cambiar al cargador del sistema operativo seleccionado (modo de carga encadenada).	*chainloader +1*

Para añadir una nueva entrada para sistemas operativos de tipo Windows o FreeBSD en el menú GRUB hay que hacerlo de la siguiente forma:

```
title WindowsXP
rootnoverify (hd0,1)
chainloader +1
```

Nota

Es importante saber que no es necesario, cada vez que se realiza una modificación en el fichero de configuración de GRUB, volver a grabar su configuración en el MBR, ya que GRUB tiene acceso directo a los ficheros de configuración.

Nota

Para establecer la contraseña en GRUB debes añadir la siguiente opción:

```
password contraseña_a_utilizar
```

14.1.1.3 Configuración en Ubuntu

En el caso de tratarse de Ubuntu el gestor de arranque por defecto es GRUB v2 por lo que cambia un poco la configuración del sistema.

Para empezar, para realizar los cambios generales del sistema de arranque (tiempo de espera, resolución, etc.) hay que modificar el fichero */etc/default/grub.* Por ejemplo, si quiere modificar el tiempo que se muestra el menú de arranque entonces hay que modificar la variable:

```
GRUB_TIMEOUT=10
```

Para configurar el menú de arranque hay que acceder a la carpeta */etc/grub.d* donde se encuentran los ficheros de configuración. Por ejemplo, para añadir en el menú de arranque una nueva opción para poder iniciar un sistema operativo Windows hay que añadir al final del fichero */etc/grub.d/40_custom* las siguientes líneas:

```
menuentry 'Windows XP'{
    insmod ntfs
    set root=(h0,1)
    chainloader +1
}
```

Finalmente, para aplicar los cambios en el sistema hay que ejecutar:

```
#update-grub2
```

14.1.2 Proceso de arranque y parada del sistema

14.1.2.1 Niveles de ejecución

Una vez que se ha encontrado el kernel y se ha iniciado. El sistema operativo comienza a cargarse, se inicia el hardware, los discos están preparados, se asignan direcciones IP, se inician servicios, y se realizan otras muchas tareas. Para ello, Linux ejecuta el programa *init*, cuya función es iniciar el sistema operativo y sus servicios. Las tareas que realiza el proceso *init* son:

- Comprueba los sistemas de ficheros.
- Monta los sistemas de ficheros permanentes.
- Activa la zona de memoria swap o de intercambio.
- Activa los demonios o servicios del sistema (p. ej., *atd*, *syslog*).
- Activa la red.
- Inicia los demonios o servicios de red del sistema (p. ej., *sendmail*, *httpd*).
- Limpia los sistemas de ficheros temporales.
- Finalmente, habilita el login a los usuarios del sistema.

El proceso *init* es el estándar para iniciar y apagar equipos Linux y Unix llamado *SysV*. *SysV* es un modo de definir qué estado debe tener el equipo en un momento determinado. Para ello se emplea un concepto denominado modo de ejecución (o *runlevels*).

SysV utiliza siete modos de ejecución que van del 0 al 6, y cada distribución utiliza los modos de ejecución para diferentes fines aunque hay varios niveles que son comunes. Los niveles que son comunes son: el 0 se utiliza para apagar el equipo; el 1 es el modo monousuario; y el 6 se utiliza para reiniciar el equipo.

Los demás modos de ejecución (del 2 al 5) difieren ligeramente en Ubuntu y Fedora. En Ubuntu los modos del 2 al 5 se ejecutan en modo multiusuario mientras que en los sistemas basados en RedHat, como es el caso de Fedora, cambian ligeramente. En la tabla 14-2 se muestran los modos de ejecución para las distribuciones Ubuntu y Fedora.

Tabla 14-2. Modos de ejecución

Modo	Ubuntu	Fedora
0	Apaga el equipo	Apaga el equipo
1	Modo monousuario	Modo monousuario (mantenimiento).
2	Modo multiusuario	Sin asignar
3	Modo multiusuario	Multiusuario en modo comandos
4	Modo multiusuario	Sin asignar
5	Modo multiusuario	Multiusuario con entorno gráfico
6	Reinicia el equipo	Reinicia el equipo

A continuación se van a ver las tareas más frecuentes sobre el nivel de ejecución del sistema:

- Si lo desea, puede **cambiar el nivel de ejecución del sistema por defecto** de la siguiente forma:

UBUNTU

Modifique el fichero /etc/init/rc-sysinit.conf de la siguiente forma:

```
env DEFAULT RUNLEVEL=2
```

FEDORA

Modifique el fichero /etc/inittab de la siguiente forma:

```
id:3:initdefault:
```

donde el 3 es el modo de ejecución del sistema.

- Para **ver el nivel de ejecución** que tiene actualmente el sistema debe ejecutar:

```
# runlevel
```

- Para **cambiar manualmente el nivel de ejecución del sistema** hay que ejecutar:

```
# telinit 3
```

o

```
# init 3
```

Cada nivel de ejecución, tiene asociado un directorio donde se especifican los servicios que se deben ejecutar o parar. Por ejemplo, el directorio */etc/rc0.d* corresponde al nivel 0, el directorio */etc/rc1.d* al nivel 1, etc.

Ahora bien, ¿cómo puedo ver los scripts que se ejecutan en un determinado nivel? Existen varias formas de ver los servicios asociados a un determinado nivel. Por ejemplo, si muestra el contenido del directorio:

```
$ cd /etc/rc3.d
$ls -l
```

Se obtiene una salida como la siguiente:

```
lrwxrwxrwx 1 root root 17 3:11 S10network -> ../init.d/network
lrwxrwxrwx 1 root root 16 3:11 S30syslog -> ../init.d/syslog
lrwxrwxrwx 1 root root 14 3:32 S40cron -> ../init.d/cron
lrwxrwxrwx 1 root root 14 3:11 S50inet -> ../init.d/inet
lrwxrwxrwx 1 root root 13 3:11 S60nfs -> ../init.d/nfs
lrwxrwxrwx 1 root root 15 3:11 S70nfsfs -> ../init.d/nfsfs
lrwxrwxrwx 1 root root 18 3:11 S90lpd -> ../init.d/lpd.init
lrwxrwxrwx 1 root root 11 3:11 S99local -> ../rc.local
```

Como se puede observar, el directorio contiene enlaces simbólicos a scripts del directorio */etc/init.d*. Cada enlace tiene una letra (*S* o *K*) y un número al principio. El número establece el orden en el que se van a ejecutar los servicios mientras que la letra "*S*" significa que se inicia y la "*K*" que se para el servicio correspondiente.

¿Cómo hace el proceso *Init* para arrancar y parar los servicios? Sencillo. Cada uno de los scripts se escribe para aceptar un argumento que suele ser *start*, *stop*, *status*, *restart* o *relaod.* Si lo desea puede ejecutar los scripts manualmente.

Por ejemplo, si quiere ver las opciones de un determinado servicio puede ejecutarlo directamente:

```
# /etc/init.d/apache2
Uso: ./apache2
{start|stop|restart|condrestart|reload|status|fullstatus|gracef
ul|help|configtest}
```

Por lo tanto, si quiere parar el servidor de páginas web manualmente ejecute:

```
# /etc/init.d/apache2 stop
```

También puede administrar los servicios utilizando el comando *service* de la siguiente forma:

```
# service apache2 stop
```

Una vez realizados todos los pasos que establece el nivel de ejecución, se procesa el fichero */etc/rc.local*. Este fichero es un "cajón desastre" donde se pueden escribir todos los comandos que el sistema ejecuta al iniciarse.

14.1.3 Servicios del sistema

Los servicios son aplicaciones que se ejecutan, en segundo plano, independientemente del usuario y ofrecen una determinada funcionalidad.

Normalmente se asocia el término "servicio" solo a servicios de red (p. ej., servidor web, servidor ftp) pero existen servicios que ofrecen todo tipo de funcionalidades (gestionan las conexiones de red, monitorizan el sistema, comprueban las actualizaciones y seguridad del sistema, permiten utilizar el hardware del equipo, etc.).

El administrador de servicios permite establecer los servicios que se van a ejecutar al iniciar el sistema, y permite parar, ejecutar o reanudar los servicios que se ejecutan actualmente en el sistema.

A continuación se van a ver varias formas de administrar los servicios en el sistema.

14.1.3.1 Herramientas gráficas

Ubuntu

En Ubuntu es posible administrar los servicios de modo gráfico utilizando *Boot Up Manager* o *sys-rc-conf* en el terminal del sistema.

Para ejecutar *Boot Up Manager* primero hay que instalarla ejecutando:

```
# apt-get install bup
```

A continuación, desde el entorno gráfico ejecute *Boot-up Manager* que se encuentra en *System/Administration* (véase la figura 14-3).

Figura 14-3. Boot-up Manager

Si desea administrar los servicios del sistema en modo terminal entonces debe instalar la herramienta *sysv-rc-config*:

```
# apt-get install sysv-rc-config
```

Una vez instalada ejecute en el terminal

```
# sysv-rc-config
```

y en la pantalla que se muestra en la figura 14-4 habilite o deshabilite los servicios que estime oportunos

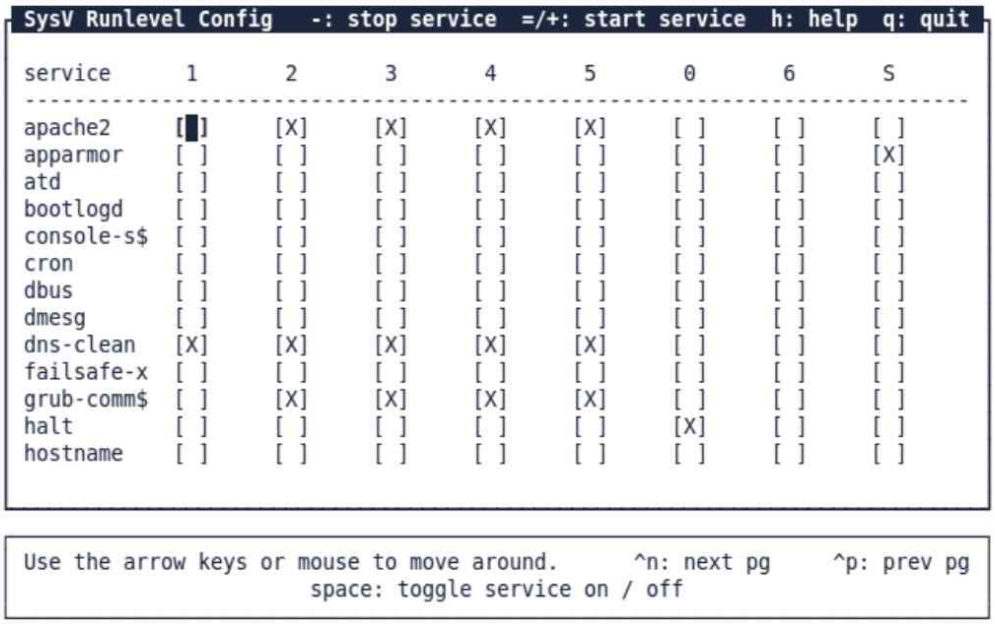


Figura 14-4. sysv-rc-conf

Fedora

En los sistemas Fedora es posible administrar los servicios del sistema a través de la herramienta *Configuración del servicio.* Si desea configurar los servicios de forma gráfica por terminal entonces debe ejecutar la herramienta *ntsysv.*

Para ejecutar el administrador de servicios (véase la figura 14-5) ejecute *system-config-services* desde un terminal o desde el entorno gráfico ejecute *servicios* que se encuentra en *Administración ->Servicios*.

ntsysv es una utilidad que se puede ejecutar desde la línea de comandos o desde el programa *setup*, opción *System services*. Para utilizarlo, tal y como muestra la figura 14-6, debe ir marcando los servicios que quiere que se ejecuten de forma automática.

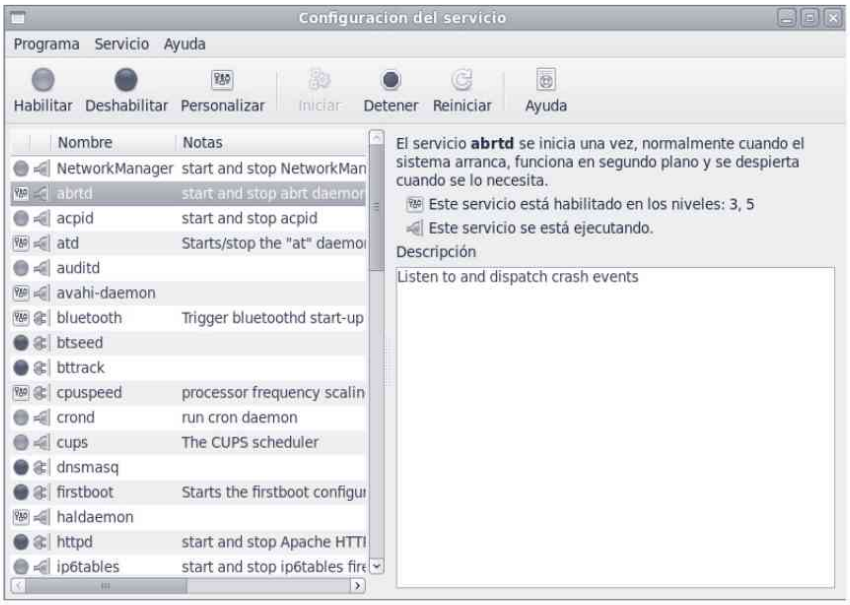


Figura 14-5. Administrador de servicios (x-Windows)

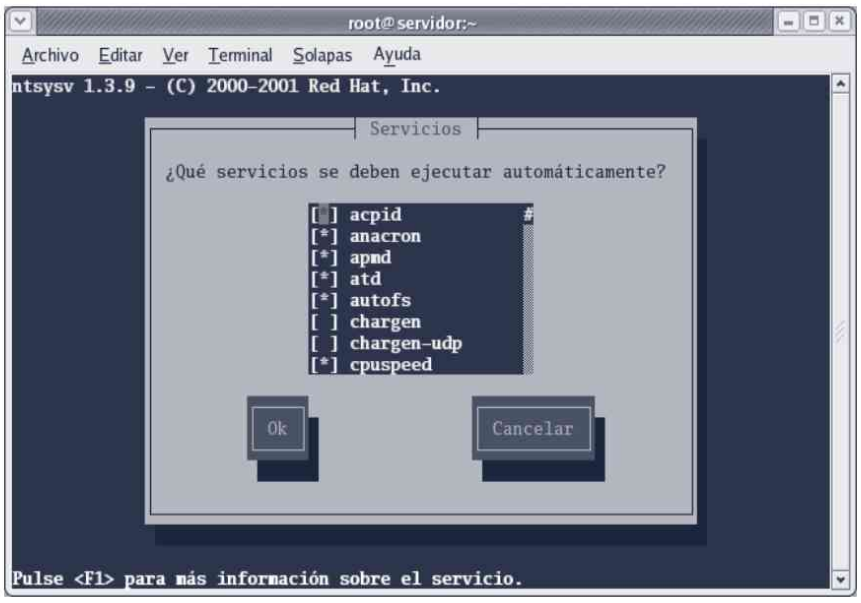


Figura 14-6. Administrador de servicios (ntsysv)

chkconfig

chkconfig permite administrar los servicios que se van a iniciar automáticamente cuando arranca el sistema.

UBUNTU

Para utilizar chkconfig en Ubuntu antes es necesario instalarlo ejecutando:

```
# apt-get install chkconfig
```

Para ver el estado de los diferentes servicios ejecute:

```
# chkconfig --list
```

Donde en cada fila se muestra un determinado servicio y en cada columna se indica si el servicio se inicia automáticamente en ese modo de ejecución (del modo 0 al 6).

Por ejemplo, si quiere que el servidor web se ejecute automáticamente ejecute:

```
# chkconfig apache2 on
```

Si desea activarlo en los niveles 235 ejecute:

```
# chkconfig –levels 235 apache2 on
```

Y si desea deshabilitarlo ejecute:

```
# chkconfig apache2 off
```

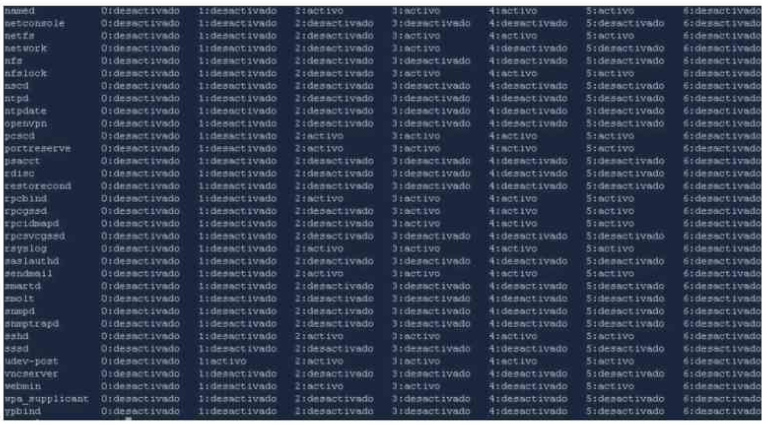


Figura 14-7. chkconfig –list

14.1.4 Procesos

En los sistemas GNU/Linux se ejecutan una gran cantidad de servicios que permiten realizar una determinada actividad en el sistema. Cada servicio o demonio consiste en uno o más procesos que se ejecutan en el equipo.

Además de los procesos vinculados a servicios, en el sistema se encuentran los procesos que ejecuta un usuario. Por ejemplo, un editor de textos, un navegador web, etc. A continuación, se van a ver las herramientas que permiten gestionar los procesos del sistema.

14.1.4.1 ps

El comando *ps* permite ver los procesos que se están ejecutando en el sistema. Tal y como se muestra en la figura 14-8, para cada proceso se muestra su identificador (PID), terminal donde se ejecuta (TTY), tiempo de uso de CPU (TIME) y el comando que ejecuta (CMD).

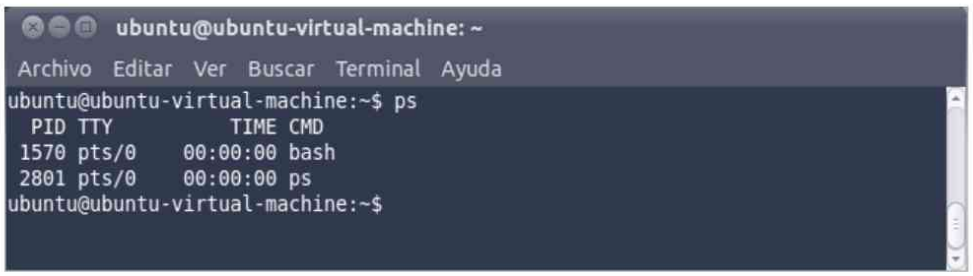


Figura 14-8. ps

Si desea ver todos los procesos que se ejecutan en el sistema utilice la opción *-A*:

```
# ps -A
```

Si desea eliminar un proceso que se está ejecutando en el sistema puede utilizar el comando *kill* de la siguiente forma:

```
# kill -9 <ID del proceso>
```

Otra forma de matar un proceso es con el comando *pkill.* El comando *pkill* permite matar un proceso utilizando el nombre del proceso. Por ejemplo, si quiere matar el editor de texto *nano* ejecute:

```
# pkill nano
```

14.1.4.2 top

Es una aplicación que, en tiempo real, informa sobre la actividad del sistema. Proporciona información sobre la carga del sistema operativo, grado de utilización de la CPU, memoria y swap, y los procesos que se encuentran en ejecución (véase la figura 14-9).

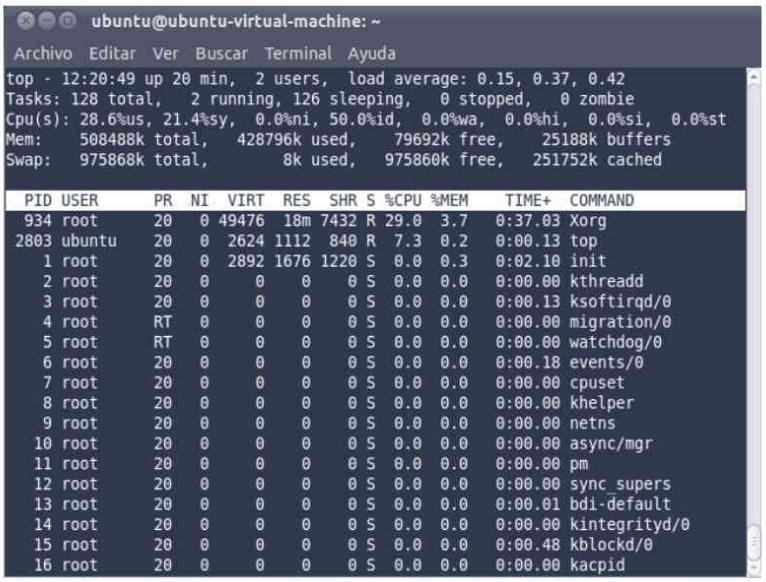


Figura 14-9. top

14.1.5 Programación de tareas

La programación de tareas permite programar la ejecución de un determinado programa en un momento determinado. Por ejemplo, se puede programar una copia de seguridad, enviar un fichero, comprobar la seguridad del sistema, enviar un informe, etc.

Antes de programar las tareas hay que comprobar que el servicio *crond* se encuentra en ejecución mediante el comando:

```
# service crond status
```

Para modificar el fichero de configuración de *crond,* ejecute el comando:

```
# crontab -e
```

y aparece un fichero con el siguiente formato:

```
PATH=/bin
0 0 * * * /root/comprobar_seguridad.sh
0 0 1 * * /root/copia_seguridad.sh
```

La sintaxis de las tareas programadas es:

```
# .---------------- minuto (0 - 59)
# |  .------------- hora (0 - 23)
# |  |  .---------- día del mes (1 - 31)
# |  |  |  .------- mes (1 - 12) o jan,feb,mar,apr ...
# |  |  |  |  .---- día de la semana (0 - 6) (Sunday=0 o 7) OR
# |  |  |  |  |
sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
  *  *  *  *  *  Comando a ejecutar
```

En el ejemplo anterior se ejecuta el script *comprobar_seguridad.sh* todos los días a las 0:00 h y se ejecuta *copia_seguridad.sh* el primer día de cada mes.

Otra forma de poder programar tareas es guardar el script que quiere ejecutar en las siguientes carpetas de configuración de *cron*:

```
/etc/cron.hourly        # Ejecuta el script cada hora
/etc/cron.daily         # Ejecuta el script diariamente
/etc/cron.weekly        # Ejecuta el script semanalmente
/etc/cron.monthly       # Ejecuta el script mensualmente
```

Nota

Para asegurar el sistema solo el usuario root puede modificar los scripts que ejecuta crontab.

Una ventaja muy interesante que permite *crontab* es que cada vez que se ejecuta la tarea se envía un e-mail con el resultado de la ejecución de dicha tarea.

14.1.6 Reinicio y parada del sistema

El proceso de parada y reinicio del sistema se puede realizar de forma gráfica o por terminal. Para hacerlo de forma gráfica tan solo hay que pulsar en el botón de apagar que se encuentra en la esquina superior derecha y en el menú que aparece (véase la figura 14-10) seleccione la operación a realizar.

Figura 14-10. Parada del sistema de forma gráfica

Además, puede utilizar comandos específicos para apagar el equipo como *halt* o *shutdown,* o se puede reiniciar el equipo ejecutando *reboot.*

Internamente, el proceso de parada y reinicio del sistema lo establecen los niveles de ejecución 0 y 6 respectivamente. De esta forma en los respectivos directorios */etc/rc0.d* y */etc/rc6.d* puede ver los pasos que realiza el sistema para apagar o reiniciar el equipo. Por tanto, si desea reiniciar el equipo puede llamar al proceso *init* de la siguiente forma:

```
# init 0
```

y si quiere reiniciarlo ejecute:

```
# init 6
```

14.2 MONITORIZACIÓN DEL SISTEMA

Para conocer el comportamiento del sistema es necesario obtener información sobre las prestaciones de los diferentes subsistemas que lo componen. En Linux se dispone, por una parte, de una serie de comandos que proporcionan datos sobre el rendimiento del hardware y del sistema operativo y, por otra parte, de una aplicación cliente-servidor que registra los eventos que suceden en el equipo (syslog).

14.2.1 Herramientas básicas

Según el tipo de información que presentan, los comandos se pueden clasificar en:

- **Procesos.** Muestran información sobre los procesos que se están ejecutando en el sistema.
- **Almacenamiento.** Proporcionan información sobre la entrada y salida al subsistema de almacenamiento.
- **Memoria.** Proporcionan información sobre el espacio de memoria real y *swap.*
- **Red.** Facilitan estadísticas de uso de las interfaces de red.
- **Polivalentes.** Muestran información sobre distintos subsistemas del equipo.

En la tabla 14-3 se muestra un resumen de las herramientas básicas de monitorización en GNU/Linux.

Tabla 14-3 Herramientas básicas de monitorización en GNU/Linux

Categoría	Comandos
Procesos	
ps	Muestra el estado de los procesos que se están ejecutando en el equipo.
Almacenamiento	
df	Muestra el espacio libre del sistema de ficheros (figura 14-11).
du	Muestra el espacio ocupado a partir de un determinado directorio.
Memoria	
free	Proporciona información relativa a la cantidad de memoria física, espacio de *swap* libre y usado por el sistema operativo, estado de los buffers y memoria caché utilizada por el núcleo.
pmap	Proporciona información referente a la utilización de la memoria por parte de un determinado proceso.
Red	
ifstat	Muestra la estadística de tráfico de entrada y salida de las interfaces de red.
iftop	Muestra las conexiones de red de un equipo.
iptraf	Es una completa herramienta que permite mostrar las estadísticas de red en tiempo real (véase la figura 14-12).
netstat	Proporciona estadísticas e información de estado sobre tablas de rutas, interfaces de red, conexiones establecidas, etc.
ping	Permite comprobar el estado de una conexión.
traceroute	Permite obtener el camino que sigue un paquete para establecer una comunicación con un destinatario, es decir, los routers que se atraviesan.
Polivalentes	
dstat	Permite realizar estadísticas de CPU, utilización de disco, red, paginación y estado del sistema.
iostat	Permite ver la carga de CPU y del disco duro.
top	Informa en tiempo real sobre la actividad del sistema. Proporciona información sobre la carga del sistema operativo, grado de utilización de la CPU, memoria y swap, y los procesos que se encuentran en ejecución.
vmstat	Muestra información sobre los procesos que se están ejecutando en el equipo, la memoria, las operaciones de E/S a disco y la utilización de la CPU. Es una aplicación clásica en los sistemas.
who	Permite ver de forma resumida el tiempo que lleva activo el sistema (*uptime*), la carga del sistema y la actividad de los usuarios que se encuentran conectados al sistema
xosview	Es una aplicación gráfica que proporciona información sobre el uso de CPU, memoria, cantidad de carga del sistema, red, interrupciones y swap en espacio de usuario.

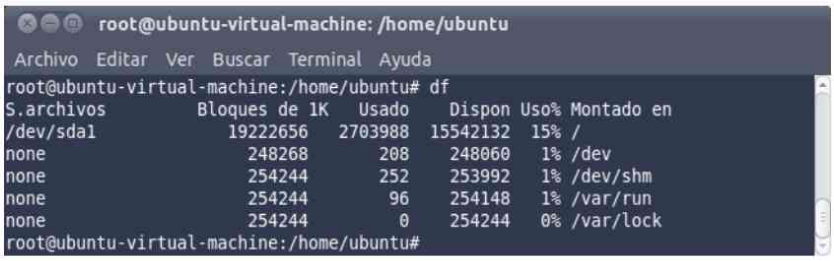


Figura 14-11 Salida del comando df.

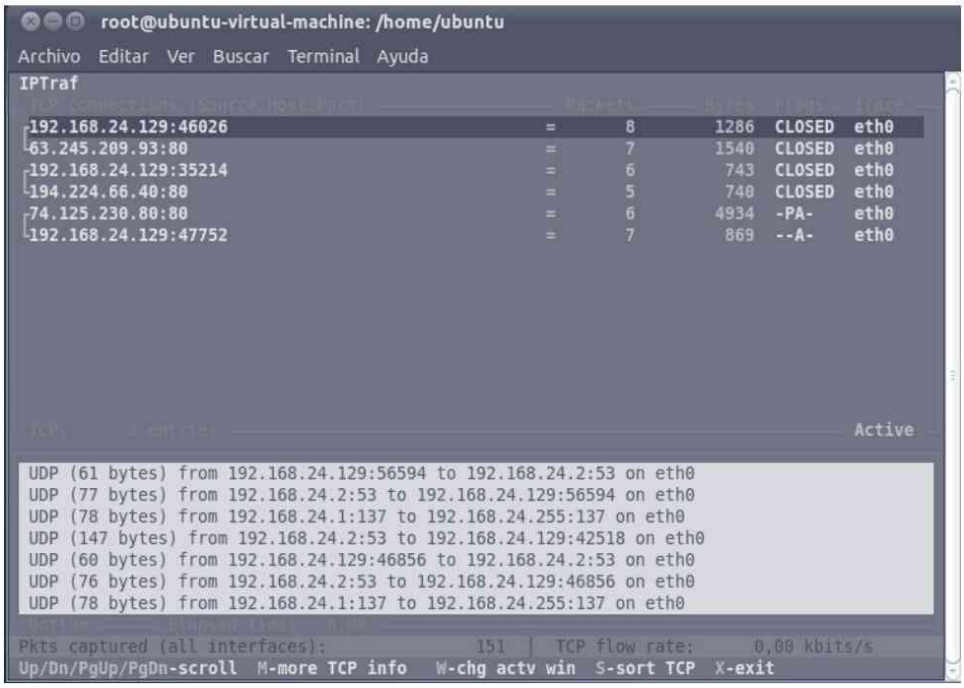


Figura 14-12 iptraf

14.2.2 Directorio /proc

El núcleo de Linux almacena información relativa a su funcionamiento en archivos situados en el directorio */proc*, de tal forma que, para analizar el comportamiento de un sistema, también se puede recurrir a la consulta de los archivos de este sistema de ficheros. De hecho, prácticamente todas las herramientas analizadas obtienen sus datos de esta fuente.

Un ejemplo de la información que reside en /proc es: **estado de la memoria** disponible en el fichero */proc/meminfo* (figura 14-13); **sistema de comunicaciones** en */proc/net*; o los **datos referentes a un proceso** que se encuentran en un subdirectorio del estilo */proc/pid_del_proceso*.

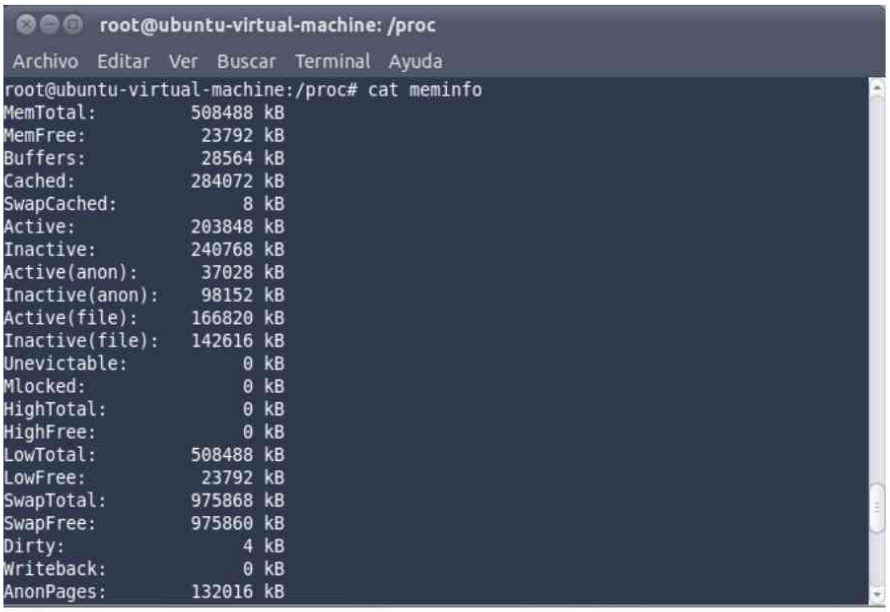


Figura 14-13. Contenido del fichero /proc/meminfo.

14.2.3 Archivos de registro (syslog)

Hasta ahora se ha visto cómo ver el estado actual del sistema. Pero sin duda es muy importante saber lo que ha pasado en el servidor.

Existen muchos motivos por los que se pueden generar mensajes. Entre los más frecuentes se encuentran los fallos del servidor (p. ej., problema de hardware, fallo en un servicio), de autenticación (p. ej., fallo en la autenticación de un usuario) o por la utilización de un servicio (p. ej., petición de un cliente de una página web). Estos mensajes se pueden encontrar en el directorio */var/log*. Por ejemplo, muchos mensajes se almacenan en los ficheros */var/log/syslog* o en el */var/log/messages.* Pero si un servicio genera muchos mensajes lo normal es utilizar un fichero o carpeta separada como lo hace Apache (*/var/log/httpd*) o el servidor de correo (*/var/log/mail*).

El registro de todos los mensajes del sistema lo realiza el servicio *syslogd* (o *rsyslogd*), el cual no es exclusivo de los servicios del sistema sino que nosotros también podemos registrar sus propios mensajes usando *syslog*.

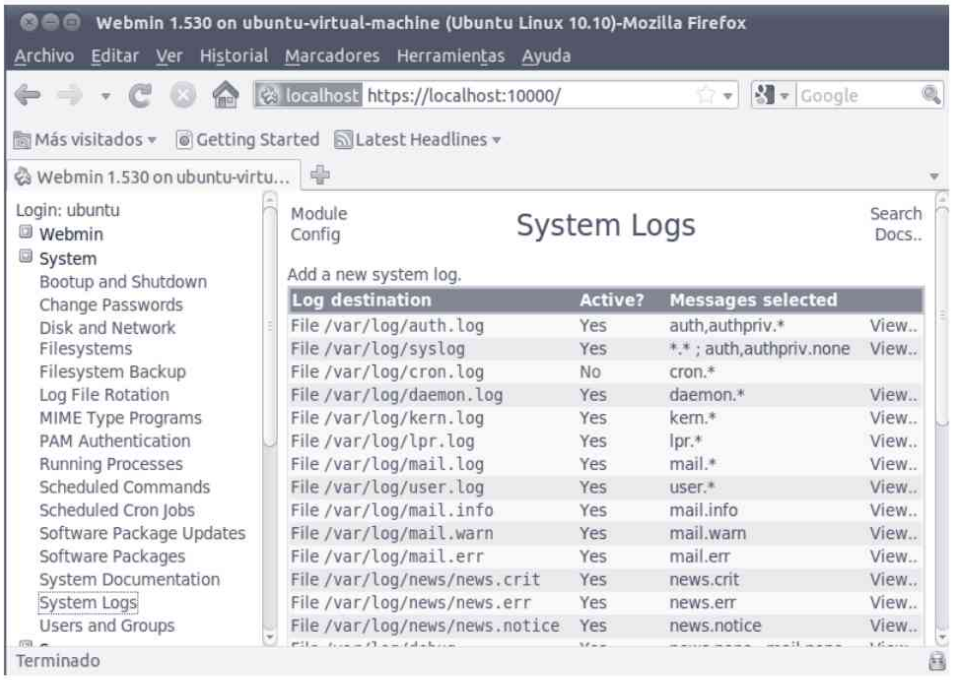


Figura 14-14. Webmin – syslog

Nota

Si quiere monitorizar de forma automática muchos equipos lo mejor es que utilice las herramientas Nagios (http://www.nagios.org) y Centreon (http://www.centreon.com/).

14.3 COPIAS DE SEGURIDAD

Existen muchas herramientas que permiten realizar copias de seguridad del sistema. Estas herramientas se pueden clasificar en tres categorías: herramientas o comandos básicos, herramientas avanzadas de copias de seguridad y herramientas de clonación de sistemas.

La forma más habitual de realizar las copias de seguridad es utilizando los comandos básicos que proporciona el sistema (p. ej., *dump*/*restore, tar, rsync*) y las herramientas existentes que permiten mejorar la funcionalidades de los comandos del sistema. En la tabla 14-4, se muestran las herramientas de copias de seguridad más utilizadas.

Con las herramientas básicas se pueden realizar copias de seguridad de un equipo de forma individual. Además, existen herramientas avanzadas que permiten centralizar y administrar todas las copias de seguridad de un sistema en único servidor. Un ejemplo de este tipo de herramientas es *amanda* (que permite

centralizar todas las copias de seguridad de los sistemas Windows y GNU/Linux de una empresa en un único servidor.

Tabla 14-4. Herramientas para realizar copias de seguridad de ficheros

Nombre	URL
Areca Backup	*http://www.areca-backup.org/*
Amanda	*http://www.amanda.org/*
Back in time	*http://backintime.le-web.org/*
Bacula	*http://www.bacula.org/en/*
BackupPC	*http://backuppc.sourceforge.net/index.html*
Déjà Dup	*http://mterry.name/deja-dup/*
Duplicity	*http://duplicity.nongnu.org/*
Flyback	*http://flyback-project.org/*
luckyBackup	*http://luckybackup.sourceforge.net/*
Remastersys	*http://www.remastersys.klikit-linux.com/*
Rsync	*http://rsync.samba.org/*
Time Vault	*https://launchpad.net/timevault*

Otra forma muy útil de realizar copias de seguridad de sistemas enteros es la clonación de discos duros. La clonación de discos duros permite realizar una copia exacta de un disco duro o partición para poder restaurarlo en otro equipo de características similares. Este tipo de herramientas es muy útil en el caso de que quiera realizar una copia exacta de un servidor o restaurar muchos equipos con la misma configuración como, por ejemplo, un aula de informática. En la tabla 14-5 se muestran las herramientas de clonación de sistemas más importantes, destacando la herramienta *Clonezilla* que se verá más adelante.

Tabla 14-5. Herramientas de clonación de discos

Nombre	URL
Clone Maxx	*http://www.pcinspector.de/clone-maxx/uk/welcome.htm*
Clonezilla	*http://www.clonezilla.org/*
Dubaron DiskImage	*http://www.dubaron.com/diskimage/*
g4U	*http://www.feyrer.de/g4u/*
NFGdump	*http://sourceforge.net/projects/nfgdump/*
Norton Ghost	*http://www.symantec.com/*
Partition Saving	*http://www.partition-saving.com/*
Partimage	*http://www.partimage.org*
WinDD	*http://sourceforge.net/projects/windd/*

14.3.1 Comandos básicos

Aunque muchas distribuciones de GNU/Linux ofrecen sus propias herramientas para realizar copias de seguridad de todo tipo, casi todas estas herramientas suelen presentar un grave problema a la hora de recuperar ficheros: se

trata de software propietario, por lo que si desea restaurar total o parcialmente ficheros necesita el propio programa para hacerlo. En determinadas situaciones, esto no es posible o es muy difícil. Imagine un departamento que dispone de solo una estación Silicon Graphics y pierde todos los datos del sistema. Si ha utilizado herramientas propias del sistema, necesitará otra estación con el mismo sistema operativo para poder restaurar estas copias, lo que obviamente puede ser problemático.

Por este motivo, muchos administradores utilizan herramientas estándar para realizar las copias de seguridad de sus máquinas. Estas herramientas suelen ser tan simples como: *dump/restore*, *tar*, *dd*, *gzip*, etc. Para mejorar las prestaciones de dichas herramientas se realizan y programan scripts para que se realicen las copias de forma automática.

A continuación se van a ver los comandos más utilizados para realizar copias de seguridad en sistemas GNU/Linux.

14.3.1.1 La orden *tar*

La utilidad *tar* (*Tape ARchiver*) es una herramienta de fácil manejo disponible en todas las versiones de UNIX/Linux que permite copiar ficheros individuales o directorios completos en un único fichero. Oficialmente fue diseñada para crear ficheros de cinta (esto es, para transferir ficheros de un disco a una cinta magnética y viceversa), aunque en la actualidad casi todas sus versiones pueden utilizarse para copiar a cualquier dispositivo o fichero, denominado *contenedor*.

En la tabla 14-6 se muestran las opciones de *tar* más habituales. Algunas de ellas no están disponibles en todas las versiones de *tar*, por lo que es recomendable consultar la página del manual de esta orden antes de utilizarla.

Tabla 14-6. Opciones de la orden *tar*

Opción	Acción
c	Crea un contenedor.
x	Extrae ficheros de un contenedor.
t	Testea los ficheros almacenados en un contenedor.
r	Añade ficheros al final de un contenedor.
v	Modo *verbose.*
f	Especifica el nombre del contenedor.
z	Comprime o descomprime el fichero.

En primer lugar debe saber cómo crear contenedores con los ficheros deseados. Por ejemplo, para copiar el directorio */home/* en el fichero */root/copia.tgz* hay que ejecutar el siguiente comando:

```
# tar cvf /root/copia.tgz /home/
```

La opción *v* no es necesaria, pero es útil para ver el proceso de empaquetamiento del fichero En muchas situaciones también resulta útil comprimir la información guardada (*tar* no comprime, solo empaqueta) por lo que hay que utilizar las opciones *cvfz*.

En lugar de indicar un único directorio con todos sus ficheros y subdirectorios es posible especificar múltiples ficheros (o directorios). Por ejemplo, la siguiente orden crea el fichero */tmp/backup.tar*, que contiene */etc/passwd* y */etc/hosts**.

```
# tar cvf /tmp/backup.tar /etc/passwd /etc/hosts*
```

Para recuperar los ficheros guardados en un fichero *tar* se utilizan las opciones *xvf* (o *xvzf* si se ha utilizado compresión con *gzip*). Puede indicar el fichero o ficheros a extraer; si no lo hace se extraerán todos los ficheros. A continuación puede ver un ejemplo:

```
# tar xvf /tmp/backup.tar /etc/passwd
```

En el ejemplo anterior, la restauración se ha realizado desde el directorio de trabajo, creando en él un subdirectorio */etc* con los ficheros correspondientes en su interior.

Nota

Un fichero con extensión tar se llama empaquetado ya que el fichero ocupa lo mismo que su contenido. Mientras que un fichero con extensión .tar.gz o .tgz está comprimido y ocupa menos espacio que su contenido.

14.3.1.2 El comando *dd*

El comando *dd* permite realizar copias exactas (bit a bit) de discos duros, particiones o ficheros. La sintaxis de *dd* es la siguiente:

```
# dd if=fichero_origen of=fichero_destino
```

Por ejemplo, tal como muestra la figura 14-15, si desea clonar el disco duro que se encuentra en */dev/sda* en el disco duro */dev/sdb* ejecute el comando:

```
# dd if=/dev/sda of=/dev/sdb
```

```
[root@redhatserver root]# fdisk -l

Disco /dev/sda: 4294 MB, 4294967296 bytes
255 cabezas, 63 sectores/pista, 522 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes

Disposit. Inicio  Principio   Fin    Bloques  Id  Sistema
/dev/sda1   *         1       382   3068383+  83  Linux
/dev/sda2           383       484    819315   83  Linux
/dev/sda3           485       522    305235   82  Linux swap

Disco /dev/sdb: 4294 MB, 4294967296 bytes
255 cabezas, 63 sectores/pista, 522 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes

Disposit. Inicio  Principio   Fin    Bloques  Id  Sistema
/dev/sdb1             1       522   4192933+  83  Linux
[root@redhatserver root]# dd if=/dev/sda /dev/sdb
dd: opción no reconocida `/dev/sdb'
Pruebe `dd --help' para más información.
[root@redhatserver root]# dd if=/dev/sda of=/dev/sdb
scsi0: Tagged Queuing now active for Target 1
8388608+0 registros leídos
8388608+0 registros escritos
[root@redhatserver root]# _
```

Figura 14-15. dd if=/dev/sda of=/dev/sdb

14.3.1.3 rsync

rsync es una aplicación para sistemas GNU/Linux que permite sincronizar carpetas de forma incremental y permite trabajar con datos comprimidos y cifrados. Mediante una técnica de delta encoding, permite sincronizar archivos y directorios entre dos máquinas de una red o entre dos ubicaciones en una misma máquina, minimizando el volumen de datos transferidos por la red.

Al sincronizar las carpetas de dos equipos los datos se envían a través de SSH por lo que es posible configurar el servidor SSH para que no solicite la contraseña a la hora de sincronizar las carpetas.

Si desea sincronizar dos carpetas locales ejecute:

```
$ rsync -avz /carpeta_origen /carpeta_destino
```

donde sincroniza el contenido de la */carpeta_origen* en la */carpeta_destino*. De forma análoga si quiere sincronizar las carpetas de dos equipos ejecute:

```
$ rsync -avz /carpeta_origen 192.168.0.9:/carpeta_destino
```

Lógicamente, tanto el origen como el destino puede ser un equipo remoto siguiendo la sintaxis anterior.

14.3.1.4 Backups sobre CD-ROM

Cada vez es más común realizar copias de seguridad sobre discos compactos. Para poder grabar datos en un CD o DVD primero es necesario crear la imagen ISO (el "molde" del futuro CD-ROM). Una vez creada la imagen se graba en el disco utilizando un software de grabación. Por ejemplo, puede utilizar el comando *cdrecord* que va incluido en Fedora.

Por ejemplo, si desea realizar una copia del directorio */home/*, en primer lugar ejecute *mkisofs* para crear una imagen con todos los ficheros y subdirectorios de los usuarios:

```
# mkisofs -o /root/imagen.iso /home/
```

Con esta orden se ha creado una imagen ISO denominada */root/imagen.iso* y que contiene toda la estructura de directorios de */home/.*

Una vez creada la imagen hay que grabarla en un CD-ROM, por ejemplo, mediante *cdrecord*:

```
# cdrecord /root/imagen.iso
```

Con esta orden el sistema detecta la grabadora de CD/DVD disponible en el sistema y realiza la grabación de la imagen ISO (véase la figura 14-16).

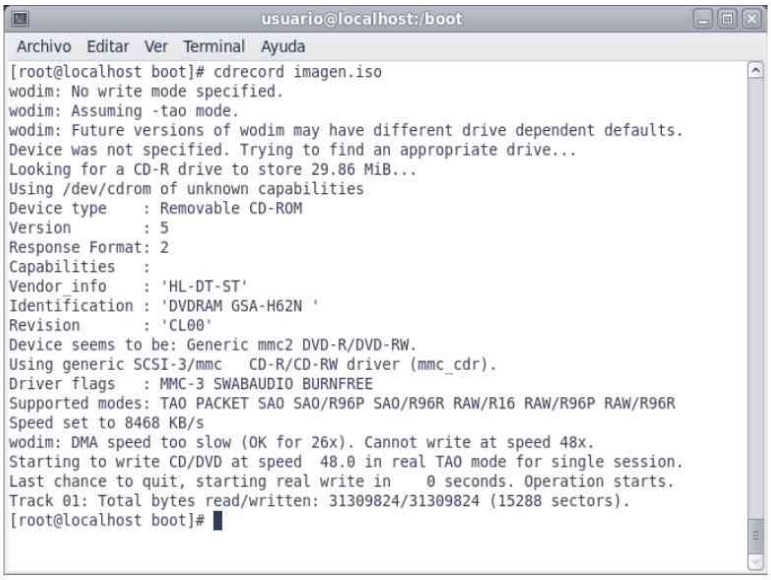


Figura 14-16. cdrecord /root/imagen.iso

Consejo

La mejor forma de automatizar una copia de seguridad es crear un script con todos los pasos de la copia de seguridad y programar su ejecución con crontab.

14.3.2 Herramientas gráficas

Además de realizar las copias de seguridad por comandos puede realizar la copia de seguridad del sistema mediante herramientas gráficas. Las herramientas más utilizadas son:

- **Déjà-Dup** es una aplicación para realizar copias de seguridad de forma sencilla e intuitiva. Entre sus características más importantes destaca la posibilidad de encriptar los datos para asegurar la privacidad, programación de las copias, permite almacenar las copias en diferentes destinos (p. ej., servidor externo, local, etc.).

  La instalación de Déjà-Dup se puede realizar a través de la herramienta *Agregar/quitar software* o ejecutando en el terminal el siguiente comando:

UBUNTU

```
# apt-get install deja-dup
```

FEDORA

```
# yum install deja-dup
```

Para iniciar la aplicación de copias de seguridad puede ejecutar el comando *deja-dup* en un terminal, o ir al menú *Aplicaciones ->Herramientas del sistema* y ejecutar *Herramienta de respaldo Déjà-Dup.*

Una vez iniciada la aplicación (figura 14-17) puede realizar dos acciones principales: *Respaldar* (*realizar*) o *Restaurar* copias de seguridad.

Figura 14-17. Déjà Dup

- **Brasero** es el software de grabación de CD/DVD en sistemas GNU/Linux más utilizado. Su interfaz es bastante sencilla e intuitiva y permite, entre otras opciones, la grabación de CD/DVD de datos, CD de audio, duplicación de CD/DVD, etc.

  Normalmente *Brasero* se instala automáticamente al realizar la instalación del sistema con entorno gráfico, pero si necesita instalarla hay que ejecutar:

UBUNTU

```
# apt-get install brasero
```

FEDORA

```
# yum install brasero
```

Para iniciar *Brasero* puede ejecutar en un terminal el comando *brasero* o ejecutar la aplicación *Grabador de discos Brasero* que se encuentra en el menú *Aplicaciones -> Sonido & Vídeo.*

Una vez iniciada la aplicación, véase la figura 14-18, puede utilizar la aplicación para realizar los diferentes proyectos de grabación.

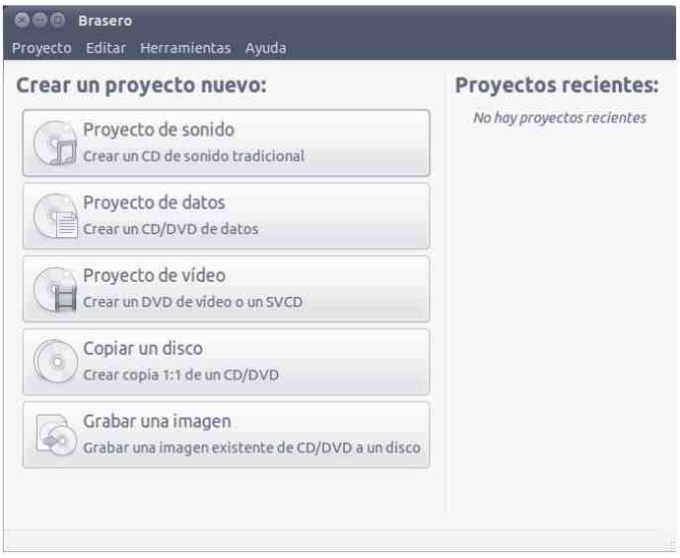


Figura 14-18. Brasero

- **Clonezilla** (*http://clonezilla.org/*) es la distribución LiveCD más potente y utilizada en la actualidad que permite realizar la clonación y restauración de sistemas. *Clonezilla* está licenciado bajo GPL y entre sus características más importantes destacan:
  - Permite la clonación y restauración de particiones o de discos duros completos.
  - Utiliza diferentes sistemas de ficheros como FAT32, NTFS y ext3 por lo que permite trabajar con cualquier instalación GNU/Linux o Windows.
  - Permite realizar y restaurar las copias de seguridad utilizando diferentes medios como, por ejemplo, discos duros locales, servidores Samba, servidores SSH, llaveros USB, etc.
  - Es fácil y sencilla de utilizar.

Para empezar a utilizar Clonezilla para clonar o restaurar un equipo tiene que descargar la imagen ISO de Clonezilla de su web oficial y la graba en un CD. Inicie el LiveCD en el equipo que desea clonar y en el menú de arranque (véase la figura 14-19) seleccione la opción cuya resolución se adapte mejor a sus necesidades. A continuación se inicia el asistente que le guía para poder clonar o restaurar una copia del equipo

Figura 14-19. Clonezilla – Inicio

Consejo

Para guardar una imagen ISO en un USB puede utilizar Unebootin (http://unetbootin.sourceforge.net/).

Capítulo 15

PROGRAMACIÓN SHELL

El shell es un intérprete de comandos que permite al administrador ejecutar determinadas tareas. Pero el shell no es únicamente eso, ya que los intérpretes de comandos son un auténtico lenguaje de programación que le permite al administrador automatizar y programar tareas. Como cualquier lenguaje de programación, el shell de GNU/Linux incorpora sentencias de control de flujo, sentencias de asignación, funciones, etc.

Los programas de shell no necesitan ser complicados, como ocurre en otros lenguajes, y son ejecutados línea a línea por lo que a estos programas se les conoce con el nombre de shell script.

Desde que en los años setenta se desarrollara UNIX, se han incluido con él varias variantes del lenguaje de shell. El más popular y común es el Bourne Shell, por su creador. En las variantes de UNIX de BSD se incluyó el C-Shell, una variante con sintaxis más parecida a C que el Bourne. También, el Korn shell incluyó funciones para controlar los trabajos en segundo plano, etc.

En el caso de Linux, se incluye el Bash (*Bourne-again shell*), que aglutina características de todas las variantes, pero que sigue la filosofía del Bourne. Se utilizará este intérprete por ser el que viene por defecto.

A continuación se va a realizar un pequeño resumen de programación en shell script para que pueda realizar sus propios scripts para automatizar las tareas del servidor.

15.1 CONCEPTOS BÁSICOS

15.1.1 Variables

Como en cualquier lenguaje de programación, las variables se utilizan para poder guardar información y a partir de ella poder tomar decisiones o realizar operaciones. Lógicamente, las variables no pueden tener el nombre de ninguna palabra reservada (p. ej., *echo*) y hay dos formas diferentes de utilizarlas dependiendo de si quiere asignarle un valor u operar con ellas. A continuación se va a ver un ejemplo en el que se le asigna a la variable *numero* un valor y luego se muestra por pantalla.

```
#!/bin/bash
numero=5
echo "el valor de la variable es "$numero
```

Como se puede ver en el ejemplo, cuando se quiere acceder al valor de la variable se utiliza el símbolo $.

15.1.2 Paso de parámetros

A menudo es necesario que los scripts reciban parámetros desde la línea de comandos para hacerlos más versátiles. Los parámetros se pueden usar dentro del script como cualquier otra variable de shell.

Los parámetros dentro del shell script son accesibles utilizando las variables: *$0* es el nombre del programa, *$1* es el primer parámetro, *$2* es el segundo parámetro, etc. Además, se utiliza la variable *$#* para obtener el número de parámetros que ha recibido el shell.

```
#!/bin/bash
echo "El nombre del programa es "$0
echo "El primer parámetro recibido es "$1
echo "El segundo parámetro recibido es "$2
echo "..."
echo "En total se han recibido "$#" parámetros"
```

15.2 ENTRADA Y SALIDA DE DATOS

15.2.1 E/S por consola

La salida de datos se realiza por pantalla con el comando *echo* y la entrada de datos, además de poder realizarla con el paso de parámetros se realiza con el comando *read*. A continuación se muestra un ejemplo:

```
#!/bin/bash
echo -n "Introduce el valor de la variable: "
#el parámetro -n se utiliza para evitar el salto de línea
read numero
echo "El valor introducido es: "$numero
```

La lectura de varios valores se puede realizar de dos formas:

```
read numero1
read numero2
read numero3
```

o

```
read numero1,numero2,numero3
```

Además, la entrada y salida de datos se puede realizar a través de ficheros o del resultado de la ejecución de un comando, pero eso se verá más adelante.

15.2.2 Redirección de la E/S

Cuando se ejecuta un programa en Linux se abren automáticamente tres archivos (flujos) de E/S para ellos. Estos son: la entrada estándar, la salida estándar y el error estándar. Aunque parezca confuso todos los sistemas UNIX utilizan este sistema, basado en el manejo de archivos.

Por defecto, la salida estándar está conectada a la pantalla, la entrada estándar al teclado, y el error estándar a la pantalla. Es posible reasignar estos destinos antes de ejecutar el programa, en lo que se conoce como redirección de E/S. Suponga que quiere crear una lista de archivos de configuración (**.conf*) del directorio */etc*. Una forma sencilla de hacer esto sería:

```
$ ls /etc/*.conf > ListaArchivos.txt
```

o lo que es lo mismo:

```
$ ls /etc/* | grep .conf >ListaArchivos.txt
```

En ambos casos, se realiza un listado de los archivos de la carpeta */etc* cuya extensión sea **.conf*. El carácter > es el que indica la redirección de salida, esto ocasiona que el shell redireccione la salida estándar al archivo *ListaArchivos.txt.*

Si por el contrario quiere que un determinado shell utilice el contenido de un fichero utilice el carácter "<". Por ejemplo:

```
$ grep host <ListaArchivos.txt
```

muestra las líneas de texto del fichero *ListaArchivos.txt* que contienen la palabra *host*.

15.2.3 Filtrado de textos

Para empezar debe conocer los comandos que permiten mostrar el contenido de un fichero. Los comandos más utilizados son *less* y *more.* Por ejemplo, para mostrar el contenido del fichero */etc/passwd* puede ejecutar:

```
$ less /etc/passwd
```

Se puede filtrar la salida del comando de las siguientes formas:

- Muestra las líneas que cumplen una determinada condición (*grep*).
- Muestra las *n* primeras líneas (*head*) o las *n* últimas líneas (*tail*).
- Muestra una determinada columna (*cut*).
- Además, puede ordenar la salida utilizando el comando *sort.*

A continuación se van a ver cada uno de los comandos:

15.2.3.1 grep

El comando *grep* permite filtrar la salida para que se muestren las líneas que cumplen una determinada condición. Su sintaxis es:

```
$ grep [expresión regular o palabra]
```

Por ejemplo, para mostrar las líneas del fichero */etc/passwd* que contienen la palabra *root* ejecute:

```
$ less /etc/passwd | grep root
```

15.2.3.2 head y tail

El comando *head* muestra las primeras *n* líneas de un fichero mientras que el comando *tail* muestra las *n* últimas líneas del fichero. Ambos comandos tienen la misma sintaxis:

```
$ head -n num lineas
$ tail -n num_lineas
```

Por ejemplo, si quiere mostrar las primeras 5 líneas del fichero */etc/passwd* ejecute:

```
$ less /etc/passwd | head -n 5
```

Y para ver las últimas 5 líneas ejecute:

```
$ less /etc/passwd | tail -n 5
```

15.2.3.3 cut

El comando *cut* permite obtener de una salida unas determinadas columnas de datos. Su sintaxis es:

```
$ cut -d "delimitador" -f filas
```

donde *delimitador* es el carácter que separa los datos entre filas y *filas* son los números de filas que desea mostrar. Puede mostrar una fila (p. ej., *-f2*) o varias filas (p.e., *-f2,3*).

Por ejemplo, para obtener el nombre de todos los usuarios del sistema hay que obtener la primera fila del fichero */etc/passwd* cuyo delimitador es el carácter ":". Por tanto, ejecute:

```
$ less /etc/passwd | cut -d ":" -f1
```

15.2.3.4 sort

El comando *sort* permite ordenar una salida de datos. Siguiendo el ejemplo anterior es posible ordenar los nombres de usuario del equipo ejecutando:

```
$ less /etc/passwd | cut -d ":" -f1 | sort
```

En el caso de querer ordenar valores numéricos hay que utilizar el operador *–n*. Por ejemplo, si quiere ordenar los identificadores de los usuarios del sistema ejecute:

```
$ less /etc/passwd | cut -d ":" -f3 | sort -n
```

15.3 OPERACIONES ARITMÉTICO LÓGICAS

Como cualquier lenguaje de programación se pueden realizar operaciones aritmético lógicas sobre las variables.

Para realizar operaciones se utiliza el comando *expr* y para realizar comparaciones se utiliza el comando *test*.

15.3.1 expr

El comando *expr* se utiliza principalmente para realizar operaciones aritméticas simples y, en menor medida para manipular cadenas. La sintaxis de *expr* es:

```
$ expr arg1 op arg2 [op arg3...]
```

En la tabla 15-1 se muestran las diferentes operaciones de *expr*.

A continuación puede ver un ejemplo de uso de operadores aritméticos:

```
#!/bin/bash
echo -n "Introduce un valor: "
read var1
echo -n "Introduce un valor: "
read var2
resultado=$(expr $var1 \* $var2)
echo "El resultado de la multiplicación es "$resultado
```

Tabla 15-1. Operadores de *expr*

Operador	Comentario
Operadores aritméticos	
+	Suma.
-	Resta.
*	Multiplicación. El operador * va precedido de \ porque * ya tiene un significado en GNU/Linux.
/	División.
%	Resto de la división.
Operadores relacionales	
=	Igualdad.
!=	Diferentes.
>	Mayor.
>=	Mayor o igual.
<	Menor.
<=	Menor o igual.
Operadores lógicos	
|	Or lógico.
&	And lógico.

Los operadores relacionales se utilizan para comparar dos argumentos.

```
#!/bin/bash
echo -n "Introduce un valor: "
read var1
echo -n "Introduce un valor: "
read var2
resultado=$(expr $var1 = $var2)
echo "El resultado es "$resultado
```

Otra funcionalidad adicional de la función *expr* y que resulta muy interesante a la hora de programar es la generación de números aleatorios:

```
#/bin/bash
numero=$(expr $RANDOM % 100)
echo $numero
```

15.3.2 test

El comando *test* permite evaluar tres tipos de elementos: archivos, cadenas y números. Su sintaxis es:

```
test - opcion archivo
test [expresión]
```

En la tabla 15-2 se muestran las diferentes opciones que permite utilizar el comando *test* según el tipo de datos.

Tabla 15-2. Opciones del comando *test*

Opción	Descripción
Archivos o directorios	
-f	Devuelve verdadero (0) si el archivo existe y es un archivo regular (no es un directorio ni un archivo de dispositivo).
-s	Devuelve verdadero (0) si el archivo existe y si su tamaño es mayor que 0.
-r	Devuelve verdadero (0) si el archivo existe y tiene permisos de lectura.
-w	Devuelve verdadero (0) si el archivo existe y tiene permisos de escritura.
-x	Devuelve verdadero (0) si el archivo existe y tiene permisos de ejecución.
-d	Devuelve verdadero (0) si existe y es un directorio.
Valores numéricos	
-lt	Menor que
-le	Menor o igual que
-qt	Mayor que
-qe	Menor o igual que
-eq	Igual a
-ne	No igual a
Conectores	
-o	OR
-a	AND
!	NOT

A continuación puede ver un ejemplo de cada tipo:

- Evaluación de ficheros o directorios:

```
test -f /etc/passwd
```

- Evaluación de cadenas:

```
test [cadena1 = cadena2]
test [cadena1 != cadena2]
```

- Evaluación numérica. Las evaluaciones numéricas son solo válidas para números enteros y su sintaxis es:

```
test numero operador numero
```

Por ejemplo:

```
test 20 -lt 40
```

15.4 ESTRUCTURAS DE CONTROL

Las estructuras de control permiten cambiar el flujo de programa, en función del estado de las variables.

15.4.1 Condición simple (if)

Las condiciones simples (*if*) permiten que en caso de cumplirse una determinada condición se ejecute un determinado código. La sintaxis de las sentencias *if* es:

```
if condición
then
      comandos
else
      comandos
fi
```

A continuación se muestra un ejemplo:

```
#!/bin/bash

echo -n "Introduce un valor: "
read var

if (( var < 10 ))
then
    echo "El valor es menor que 10"
else
    echo "El valor es mayor que 10"
fi
```

15.4.2 Condiciones múltiples (case)

Cuando se realizan muchas condiciones sobre un mismo valor (p. ej., en un menú) la mejor opción es utilizar *case.* Su estructura es:

```
case  $variable in
   valor1)   commando
             ..
             commando;;
   valor2)   commando
             ..
             commando;;
          ...
   *)        commando
             ..
             commando;;
esac
```

A continuación puede ver un ejemplo sencillo:

```
#!/bin/bash
echo -n "Introduce un valor: "
read var1

case $var1 in
 1) echo " uno ";;
 2) echo " dos ";;
 3) echo " tres ";;
 4) echo " cuatro ";;
 *) echo "opcion incorrecta ";;
esac
```

15.4.3 Bucle for

El bucle *for* se utiliza para ejecutar un código un determinado número de veces. Su sintaxis es:

```
for (( expr1; expr2; expr3 )) do
   ...
Done
```

A continuación puede ver un ejemplo que muestra los números del 0 al 5:

```
#!/bin/bash
for ((  i = 0 ;  i <= 5;  i++  ))
do
  echo " $i "
done
```

También puede utilizar el *for* para moverse en una lista de elementos:

```
for variabe in lista elementos
do
  echo " $variable "
done
```

15.4.4 Bucle while

El bucle *while* permite ejecutar un código hasta que no se cumpla una determinada condición de salida. Su sintaxis es:

```
while [ condición ]
do
    comando1
    comando2
    ...
done
```

A continuación se muestra un ejemplo sencillo:

```
#/bin/bash
limite=5
i=0;

while (test $limite -gt $i)
do
    echo "Valor $i"
    let i=$i+1
done
```

15.5 FUNCIONES

Una función es un bloque de código que permite su reutilización de una forma fácil y sencilla. Se recomienda que el nombre de la función sea lo más descriptivo posible y que describa lo más fielmente posible el funcionamiento de la función.

Para definir una función se hace a través de la palabra reservada *function*, seguida del nombre utilizado como identificador de la función. A continuación, se declara la instrucción o conjunto de instrucciones que se ejecutarán cada vez que se realiza la llamada a la función, como siempre entre llaves.

```
#!/bin/bash

function mostrar mensaje() {
        echo "Hola mundo!"
}

mostrar_mensaje;
```

Opcionalmente las funciones pueden aceptar uno o más valores de entrada, conocidos como parámetros de la función. A continuación se muestra la función suma que recibe dos variables y las suma.

```
#!/bin/bash
function suma (){
        resultado=$(expr $a + $b)
        echo "a + b =" $resultado
}

a=5
b=10
suma $a $b
```

Los parámetros de la función se pueden utilizar a través de su nombre o a través de *$1* (primera variable), *$2* (segunda variable),... El ejemplo anterior quedaría de la siguiente forma:

```
#!/bin/bash
function suma (){
        resultado=$(expr $1 + $2)
        echo "a + b =" $resultado
}

a=5
b=10
suma $a $b
```

Una función puede devolver uno o más valores. Si devuelve un valor entero se llama función y en cualquier otro caso se llama procedimiento.

Tal y como puede ver en el siguiente ejemplo, para devolver un valor entero se utiliza *return.*

```
#!/bin/bash
function suma (){
        c=$(expr $a + $b)
        return $c
}


a=5
b=10
suma $a $b
resultado=$?
```

```
echo $resultado
```

Y si desea devolver un valor string o más de un valor entonces se utiliza un procedimiento. A continuación, a modo de ejemplo, se muestra una función que cambia un número entero a hexadecimal:

```
#!/bin/bash

convertir en hex() {
  case $valor in
        0) valor="0";;
        1) valor="1";;
        2) valor="2";;
        3) valor="3";;
        4) valor="4";;
        5) valor="5";;
        6) valor="6";;
        7) valor="7";;
        8) valor="8";;
        9) valor="9";;
        10) valor="a";;
        11) valor="b";;
        12) valor="c";;
        13) valor="d";;
        14) valor="e";;
        15) valor=f;;
  esac
}

valor=2
convertir en hex $valor
echo "el resultado es $valor"
```

Capítulo 16

ADMINISTRACIÓN DE LA RED

Con la fuerte expansión que ha tenido Internet se ha generalizado la utilización de redes en las empresas y en los hogares. Hoy en día, para un empresa es totalmente necesario disponer de una red interna que le permita compartir información, conectarse a Internet o, incluso, ofrecer sus servicios en Internet.

En este capítulo aprenderá a configurar el sistema GNU/Linux para convertirlo en un potente router que provea a la red de los servicios necesarios: enrutamiento, DHCP y DNS. Para poder aprender mejor a administrar el sistema nuestro objetivo es configurar la infraestructura de red que se muestra en la figura 16-1. A la hora de configurar la red hay que tener en cuenta los siguientes objetivos:

- Configurar *iptables* para darle acceso a Internet a los clientes de la red interna.
- Configurar el servidor DHCP para que asigne de forma automática las direcciones que van desde la 10.0.0.100 a la 10.0.0.254. Las demás direcciones las asignará el administrador de la red de forma manual.

  Además, se dispone de una impresora de red que tiene la dirección MAC (AA:BB:CC:DD:EE:FF) a la que le quiere asignar siempre la dirección IP 10.0.0.254.
- Configurar el servidor de nombres para que administre el dominio *miempresa.com*. Además, se tiene que crear los siguientes registros: *www.miempresa.com* y *ftp.miempresa.com* apuntan a la IP 10.0.0.1; *mail.miempresa.com* es equivalente a *www.miempresa.com*; y el servidor de correo electrónico se encuentra en *mail.miempresa.com*.

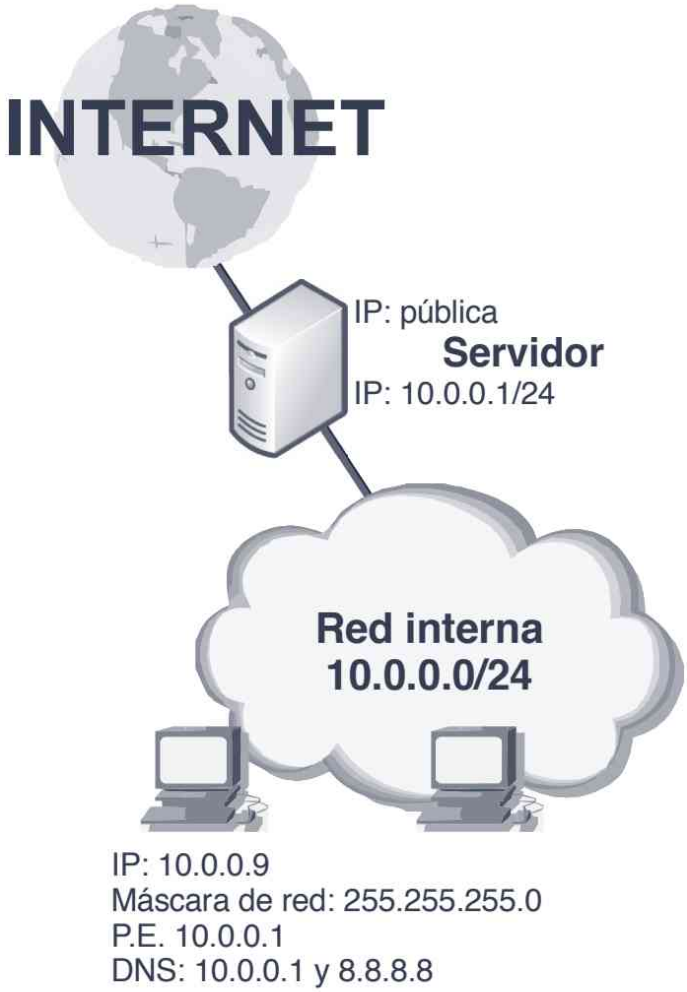


Figura 16-1. Esquema de red

16.1 ESQUEMA BÁSICO DE RED

16.1.1 Configuración de la red

Una vez que tiene claro el esquema de red que va a implementar, el primer paso que debe realizar es configurar correctamente las diferentes interfaces de red del servidor (que actuará como router) y de los clientes.

Básicamente existen dos formas de configurar las tarjetas de red: manualmente o dinámicamente a través de un servidor DHCP. A continuación se van a ver ambos métodos de configuración.

16.1.1.1 Configuración manual

Configurar las interfaces de red

En la mayoría de los casos los dispositivos hardware de red se crean automáticamente durante el proceso de instalación. Por ejemplo, el controlador Ethernet (para las tarjetas de red local) crea las interfaces eth0, eth1, etc. secuencialmente según las va encontrando en el sistema.

Este paso de detección lo realiza el kernel (núcleo del sistema) en el momento de arrancar si dispone del soporte para la tarjeta de red. En caso de que no encuentre soporte en el kernel para la tarjeta de red debe buscar un kernel que lo soporte, compilar el kernel, o tratar de cargar el controlador adecuado como módulo.

Para configurar una interfaz de red es necesario asignarle una dirección IP con su respectiva máscara de red. El comando más utilizado para configurar la red es *ifconfig (Interface Configuration)*. Por ejemplo:

```
# ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
```

En este caso, está configurando la interfaz eth0 (primera tarjeta de red detectada) con la dirección IP 192.168.1.2 y con máscara de red 255.255.255.0. El parámetro *up* indica que la tarjeta debe activarse, pero puede omitirse puesto que al asignarle los parámetros de red la tarjeta se activa por defecto. Para desactivar una interfaz de red ejecute:

```
# ifconfig eth0 down
```

Para activar una interfaz de red ejecute:

```
# ifconfig eth0 up
```

Consejo

Linux permite tener tarjetas de red virtuales sobre una tarjeta de red física. Por ejemplo, si tiene la interfaz física eth0, puede crear varias tarjetas de red virtuales (eth0:0 , eth0:1, ...).

Para comprobar la configuración de las interfaces de red ejecute el comando *ifconfig.* Tal y como puede ver en la figura 16-2 la interfaz *eth0* tiene la dirección 192.168.118.142 (la ha obtenido de forma automática) y la interfaz *eth1* tiene la dirección IP 10.0.0.1.

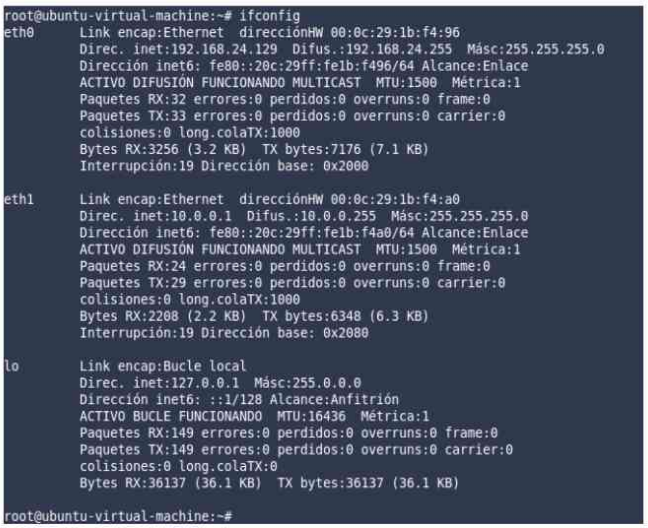


Figura 16-2. Comando ifconfig

Establecer la puerta de enlace

Para que el equipo pueda conectarse a una red diferente de la que se encuentra (p. ej., Internet) necesita establecer la puerta de enlace. La puerta de enlace es el equipo que permite comunicar varias redes. Para establecer la puerta de enlace ejecute:

```
# route add -net 0/0 gw IP_puerta_de_enlace interfaz
```

donde *IP_puerta_de_enlace* es la dirección IP donde se encuentra la puerta de enlace. *interfaz*, es la interfaz de red por donde se tiene acceso a dicha puerta de enlace.

Por ejemplo, si el equipo se encuentra conectado a la red 192.168.0.0/24 en la interfaz *eth0* y la puerta de enlace es 192.168.0.1, debe ejecutar el siguiente comando:

```
# route add -net 0/0 gw 192.168.0.1 eth0
```

16.1.1.2 Ficheros de configuración

El problema de configurar las interfaces de red con *ifconfig* es que no se guardan los datos de configuración en ningún fichero, al reiniciar el equipo se pierde la configuración. A continuación se van a ver los diferentes ficheros de configuración que intervienen en la configuración de la red del equipo.

La configuración de las interfaces de red cambia dependiendo del sistema operativo. En el caso de Ubuntu la configuración de todas las interfaces de red se encuentra en el fichero */etc/network/interfaces*. Y en Fedora la configuración se encuentra en el directorio */etc/sysconfig/network-scripts.* Por ejemplo, para la interfaz *eth0* la configuración se encuentra en el fichero */etc/sysconfig/network-*

scripts/ifcfg-eth0. De esta forma, si lo desea, puede modificar o verificar directamente los parámetros de la red.

Siguiendo el esquema de red propuesto en la figura 16-1 la interfaz de red *eth0* es la encargada de conectarse a Internet, mientras que la interfaz *eth1* pertenece a la red interna. Los parámetros de configuración de *eth0* los tiene que facilitar el proveedor de Internet o los puede obtener automáticamente utilizando DHCP.

UBUNTU

La configuración de las interfaces de red se encuentra en el fichero /etc/network/interfaces.

```
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 10.0.0.1
netmask 255.255.255.0
network 10.0.0.0
broadcast 10.0.0.255
# gateway 10.0.0.1
```

FEDORA

El fichero de configuración /etc/sysconfig/network-scripts/ifcfg-eth0 contiene:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Y el fichero de configuración de eth1 (/etc/sysconfig/network-script/ifcfg-eth1) tiene el siguiente contenido:

```
DEVICE=eth1
ONBOOT=yes
IPADDR=10.0.0.1
NETMASK=255.255.255.0
TYPE=Ethernet
```

donde DEVICE indica la interfaz de red, ONBOOT=yes indica que se cargue la configuración al iniciar el sistema, IPADDR indica la dirección IP y NETMASK la máscara de red.

Aunque lo normal es que eth0 obtenga la dirección IP de forma automática al iniciar el equipo puede hacerlo manualmente ejecutando:

```
# dhclient eth0
```

Configuración del nombre del equipo

Para configurar el nombre del equipo hay que:

UBUNTU

Modificar el fichero /etc/hostname e indicar el nombre del equipo

```
Nombre_equipo
```

FEDORA

Modifcar el fichero /etc/sysconfig/network y especificar en HOSTNAME el nombre del equipo

```
HOSTNAME=Nombre_equipo.dominio.com
```

Configuración del servidor DNS

Existen dos formas para la resolución de nombres: de forma local o a través de un servidor de nombres (DNS).

Para la resolución de nombres de forma local se utiliza el fichero */etc/hosts* donde se guarda el nombre y la dirección IP de las máquinas locales. Por ejemplo:

```
127.0.0.1         localhost.localdomain      localhost

150.214.156.62    www.ual.es
```

Para establecer los servidores de resolución de nombres (DNS) debe editar el fichero */etc/resolv.cof.* Por ejemplo:

```
nameserver 8.8.8.8

nameserver 150.214.156.2
```

Actualizar los cambios

Una vez realizada la configuración del sistema para que se apliquen los cambios en las interfaces de red hay que reiniciar el servicio o hacer un *reload* ejecutando:

UBUNTU

```
# /etc/init.d/networking force-reload
```

FEDORA

```
# service network reload
```

16.1.1.3 Configuración con asistentes

En Fedora es posible configurar la red, a través de la consola puede ejecutar el comando *setup* y acceder al submenú *network* o ejecutar directamente.

```
# system-config-network-tui
```

Tal y como puede ver en la figura 16-3, al acceder a la herramienta es posible configurar los dispositivos de red o establecer el servidor DNS que va a utilizar.

Figura 16-3. setup

Además, tanto en Ubuntu como en Fedora es posible realizar la configuración mediante el entorno gráfico x-Windows. Para ello en el menú *Sistema*, *Preferencias* ejecute la herramienta *Conexiones de red.* En la figura 16-4 se muestra la herramienta de configuración de Ubuntu y en la figura 13-5 la de Fedora.

Figura 16-4. Conexiones de red (Ubuntu)

UBUNTU

Por defecto, no se encuentra instalada la herramienta, por lo que hay que ejecutar:

```
# apt-get install gnome-network-admin
```

Figura 16-5. system-config-network (Fedora)

En ambas herramientas es posible configurar las interfaces de red, el nombre del equipo, los servidores de nombres y las entradas estáticas del fichero host.

16.1.1.4 Comprobación

Para comprobar la conexión a Internet puede ejecutar el comando *ping* indicando como parámetro cualquier dirección de Internet. Por ejemplo:

```
$ ping www.google.es
```

```
[root@localhost ~]# ping www.google.es
PING www.l.google.com (66.249.92.104) 56(84) bytes of data.
64 bytes from 66.249.92.104: icmp_seq=1 ttl=128 time=51.5 ms
64 bytes from 66.249.92.104: icmp_seq=2 ttl=128 time=39.7 ms
64 bytes from 66.249.92.104: icmp_seq=3 ttl=128 time=43.2 ms
64 bytes from 66.249.92.104: icmp_seq=4 ttl=128 time=39.7 ms
64 bytes from 66.249.92.104: icmp_seq=5 ttl=128 time=42.9 ms
^C
--- www.l.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4525ms
rtt min/avg/max/mdev = 39.729/43.451/51.527/4.310 ms
[root@localhost ~]#
```

Figura 16-6. Comando ping

Si al realizar el *ping* se recibe respuesta entonces la comunicación se está realizando correctamente. Si por el contrario indica que todos los paquetes se han perdido (100% *packet loss*) debe comprobar la configuración de red o los parámetros de configuración. En la figura 16-6 puede ver cómo el servidor *www.google.es* responde correctamente al comando *ping*.

Datos más importantes

Nombre del equipo:	*/etc/hostname (Ubuntu)* */etc/sysconfig/network (Fedora)*
Fichero de configuración de la interfaz de red:	*/etc/network/interfaces (Ubuntu)* */etc/sysconfig/network-scripts/ifcfg-eth0 (Fedora)*
Resolución estática de nombres:	*/etc/hosts*
Servidores DNS:	*/etc/resolv.conf*

FEDORA

Una vez configurada la red para que el servicio network se inicie automáticamente ejecute:

```
# chkconfig network on
```

16.1.2 iptables

16.1.2.1 Introducción

La tecnología de firewall de Linux ha evolucionado desde sencillos filtros de paquetes lineales hasta los motores actuales de inspección de paquetes de estado. Los núcleos de Linux 2.0 emplean una implementación de reglas de filtrado de paquetes que utilizan tres pilas: INPUT (tráfico de entrada), OUTPUT (tráfico de salida) y FORWARD (paquetes que se reenvían a otro equipo). Los paquetes llegan a la parte superior de las pilas y se filtran a través de las reglas hasta que exista una coincidencia. En este punto, cada paquete se puede aceptar, descartar, rechazar o reenviar. Si el paquete no coincide con ninguna de las reglas, pasa a la directiva predeterminada, que normalmente descarta el paquete.

Aunque la capacidad nativa de firewall de los núcleos de Linux 2.0 era más que adecuada para generar firewalls, en la siguiente versión del núcleo 2.2 apareció *Ipchains* que incorporó nuevas y eficaces características: permite la definición de nuevas pilas y mejora la administración de las reglas de una pila.

A partir del desarrollo del núcleo 2.3, los programadores de Linux comenzaron a trabajar en *iptables* (también llamado *netfilter*). *Iptables* mejoró las ventajas de administración de conjuntos de reglas al permitir la capacidad de crear y anular asociaciones de conjunto de reglas con sesiones existentes. Con *Iptables*, el firewall se puede programar para asociar el tráfico devuelto generado a partir de una regla INPUT anterior. El tráfico que entra correctamente en el host puede salir automáticamente del host al ser devuelto, indicando simplemente al firewall que genere dinámicamente una regla de devolución.

Las ventajas de la tecnología de inspección de paquetes de estado (*SPI, State Packet Inspection*) no se limitan a la eficacia de las reglas. *Ipchains* no permite diferenciar la "verdadera naturaleza" del tráfico de la red. Por ejemplo, un firewall *ipchains* programado para permitir el tráfico FTP de salida también tendrá una regla INPUT asociada para permitir la devolución de paquetes. Si un atacante puede fabricar paquetes FTP devueltos, *Ipchains* permite su entrada. Con SPI no existe ninguna sesión para asociar estos paquetes falsificados y, por tanto, el firewall los rechazaría.

16.1.2.2 Configuración

Iptables puede manejar varias tablas, pero las más importantes son:

- **Filter.** Es la tabla predeterminada que permite el filtrado de las comunicaciones. La tabla *Filter* está compuesta por tres pilas:
  - INPUT. Referencia el tráfico de entrada.
  - OUTPUT. Referencia el tráfico de salida.

  - FORWARD. Referencia el tráfico que el router reenvía a otros equipos.

- **NAT.** El servicio que permite dar acceso a Internet a una red interna. Esta tabla permite definir el tipo de comunicaciones entre la red externa y las redes internas. La tabla NAT tiene dos pilas:
  - POSTROUTING. Permite establecer las comunicaciones desde la red interna al exterior. Por ejemplo, para hacer que la red interna tenga Internet.
  - PREROUTING. Permite establecer las comunicaciones desde la red externa a la red interna. Por ejemplo, se utiliza para que desde el exterior se tenga acceso a un servidor interno.

Los comandos básicos de *iptables* son:

- *iptables –L.* Muestra el estado de la tabla predeterminada (*filter*). Si quiere ver el estado de la tabla NAT ejecute *iptables –t nat –L*.
- *iptables –A <parámetros> -j <acción>*. Permite añadir una regla para que el cortafuegos realice una acción sobre un tráfico determinado.
- *iptables –D <parámetros> -j <acción>*. Permite quitar una regla del cortafuegos.
- *iptables –F.* Limpia la tabla de cortafuegos. Si quiere limpiar la tabla NAT ejecute *iptables –t nat –F.*
- *iptables –P <cadena> <acción>*. Permite establecer por defecto una acción determinada sobre una pila. Por ejemplo, si quiere que por defecto el router deniegue todo el tráfico de la pila FORWARD ejecute el comando *iptables –P FORWARD DROP.*

Como se ha comentado antes, con el comando *iptables –A <parámetros> -j <acción>* puede definir la acción que quiere que realice el cortafuegos con un determinado tráfico. En la tabla 9-1 puede ver los parámetros que se utilizan para especificar el tráfico.

Las acciones que se pueden realizar en la tabla FILTER son:

- *-j ACCEPT.* Acepta el tráfico.
- *-j DROP.* Elimina el tráfico.
- *-j REJECT.* Rechaza el tráfico e informa al equipo de origen.
- *-j LOG –log-prefix "IPTABLES_L".* Registra el tráfico que cumple los criterios en */var/log.*

Las acciones que se pueden realizar en la tabla NAT son:

- *-j MASQUERADE.* Hace enmascaramiento del tráfico (NAT) de forma que la red interna sale al exterior con la dirección externa del router.
- *-j DNAT --to <ip>.* Se utiliza para que desde el exterior se tenga acceso a un servidor que se encuentra en la red interna.

De esta forma puede "jugar" con los parámetros de una determinada regla para poder especificar la acción que se aplica. A continuación puede ver tres reglas, para permitir el tráfico que reenvía el router, que van desde la más general a la más específica:

- *iptables -A FORWARD -j ACCEPT.* Permite todo el tráfico.
- *iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT.* Permite solo el tráfico de la red interna 192.168.0.0/24.
- *iptables -A FORWARD -s 192.168.0.0/24 -p TCP –dport 80 -j ACCEPT.* Permite solo el tráfico de la red interna 192.168.0.0/24 en el puerto 80.

Tabla 16-1. Parámetros para especificar las reglas de *iptables*

Elemento	Sintaxis	Ejemplo	Descripción
Interfaz			
	- i <interfaz>	-i eth0	Interfaz de entrada.
	-o <interfaz>	-o eth1	Interfaz de salida.
Dirección			
	-s <dir_red>	-s 10.0.0.0/24	Red de origen.
	-d <dir_red>	-d 0/0	Red de destino.
Puerto			
	-p <tipo>	-p TCP	Tipo de protocolo. Las opciones son: TCP, UDP o ICMP.
	--dport <puerto>	-p TCP --dport 80	Indica el puerto de destino. En el ejemplo se hace referencia al puerto de destino http (80/TCP).
	--sport <puerto>	-p UDP --sport 53	Indica el puerto de origen. En el ejemplo se hace referencia al puerto de destino DNS (53/UDP).
Estado			
	-m state --state <tipo>	-m state --state ESTABLISHED	Indica el estado de la conexión. Los posibles estados son: NEW, INVALID, RELATED y ESTABLISHED.
Acción			
	-j <acción>	-j ACCEPT	Indica la acción que se va a realizar con un determinado tráfico. Las posibles acciones son: ACCEPT, DROP, REJECT, LOG, DNAT y MASQUERADE.

Nota

Si desea bloquear comunicaciones por su país de origen le recomiendo que visite la web http://ipinfodb.com/ip_country_block.php

Una vez configurado el cortafuegos para guardar la configuración ejecute:

```
# iptables-save >/etc/iptables.rules
```

donde el fichero */etc//iptables.rules* guarda la configuración de *iptables* (en Fedora es el fichero */etc/sysconfig/iptables*). Si lo desea puede modificarlo directamente y cargar su configuración ejecutando:

```
# iptables-restore < etc/iptables.rules
```

UBUNTU

Finalmente, modifique el fichero /etc/network/interfaces y escriba:

```
pre-up iptables-restore </etc/iptables.rules
```

Además de configurar *iptables* mediante comandos o a través del fichero de configuración, existen interfaces gráficas que facilitan el proceso de configuración. En la tabla 16-2 se muestra un listado de las interfaces más utilizadas. A modo de ejemplo, en la figura 16-7 se muestra el módulo de configuración del firewall de Linux de Webmin.

Tabla 16-2. Interfaces gráficas para la configuración del firewall

GUI	URL
Dwall	*http://dag.wieers.com/home-made/dwall/*
FireHOL	*http://firehol.sourceforge.net/*
Firestarter	*http://www.fs-security.com/*
Firewall Builder	*http://www.fwbuilder.org/*
Guarddog	*http://www.simonzone.com/software/guarddog/*
KMyFirewall	*http://kmyfirewall.sourceforge.net/*
Shorewall	*http://shorewall.net/*
Webmin	*http://www.webmin.com*

Datos más importantes

Fichero de configuración:	*/etc/iptables.rules (Ubuntu)* */etc/sysconfig/iptables (Fedora)*
Comandos más utilizados:	*iptables iptables-save iptables-restore*

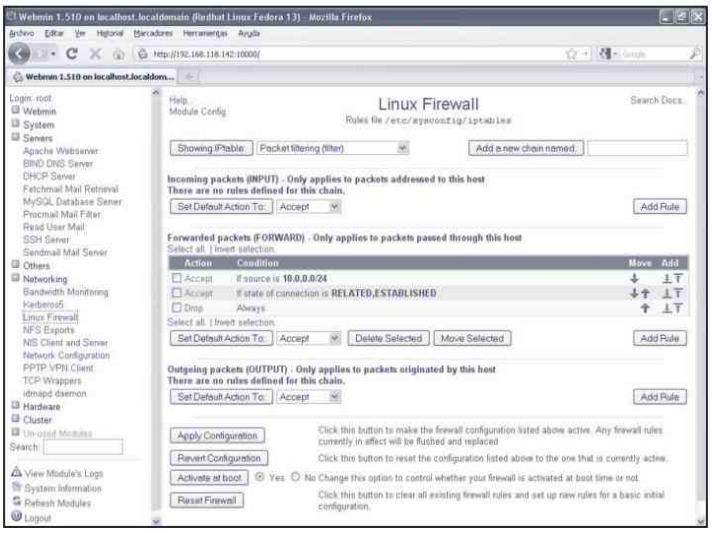


Figura 16-7. Administración del firewall con Webmin

16.1.2.3 Resolución del supuesto práctico

A continuación se va a configurar el cortafuegos para que permita que la red interna pueda conectarse a Internet:

- Establece que el sistema actúe como router:

```
# echo "1" >/proc/sys/net/ipv4/ip_forward
```

- Limpia la configuración del cortafuegos:

```
# iptables -F
# iptables -t nat -F
```

- Indica que la red interna tiene salida al exterior por NAT:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j
MASQUERADE
```

- Se permite todo el tráfico de la red interna y todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j
ACCEPT
# iptables -A FORWARD -j DROP
```

- Guarda la configuración del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```

- y modifica el fichero */etc/sysctl.conf* para establecer la variable *net.ipv4.ip_forward=1.*

Para comprender mejor iptables se va a realizar una mejora del supuesto en la que la red interna solo tiene acceso al exterior para ver páginas web (puerto

80/TCP) y para la resolución de nombres (53/UDP y 53/TCP). Además, se va a publicar un servidor web interno que se encuentra en la dirección 10.0.0.100.

- Limpia la configuración del cortafuegos:

```
# iptables -F
# iptables -t nat -F
```

- Indica que la red interna tiene salida al exterior por NAT.

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j
MASQUERADE
```

- Se permite solo el tráfico web (80/tcp) y DNS (53/udp y 53/tcp). Todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 80 -j
ACCEPT
# iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 53 -j
ACCEPT
# iptables -A FORWARD -s 10.0.0.0/24 -p UDP --dport 53 -j
ACCEPT
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j
ACCEPT
# iptables -A FORWARD -j DROP
```

- Redirige el tráfico web que entra por la interfaz externa (*eth0*) al servidor de la red interna:

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
DNAT -- to 10.0.0.100:80
```

- Guarda la configuración del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```

16.1.3 DHCP

El mantenimiento y la configuración de la red en los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IP así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace, etc., conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP: o se dispone de un sistema de asignación dinámica y flexible que permita

reutilizar las direcciones de tal forma que solo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente que tenemos, algo inviable con el número de usuarios conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

El servidor *dhcp* se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Para ello, necesita de un proceso (*dhcpd*) y un fichero de configuración (*/etc/dhcpd.conf*) que proporciona la información necesaria al proceso.

Los datos mínimos que un servidor de DHCP proporcionará a un cliente son: dirección IP, máscara de red, puerta de enlace (*gateway*) y servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- **Asignación dinámica.** Asigna direcciones IP libres de un rango de direcciones establecido por el administrador en el fichero */etc/dhcpd.conf*. Es el único método que permite la reutilización dinámica de las direcciones IP.
- **Asignación por reservas.** Si quiere que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración para una determinada dirección MAC se asignará una dirección IP.

  Este método es muy útil para aquellos dispositivos que no cambian de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP debe configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

En el fichero */etc/dhcpd.conf* se almacena toda la información referente a la asignación de direcciones IP a los clientes. Esta información incluye:

- Rango de direcciones IP a otorgar a los clientes.
- Asociación fija de direcciones IP a clientes, mediante el uso de la dirección MAC.
- Período de validez de las asignaciones.
- Servidores de nombres y *wins*.
- Si tienen o no autoridad para asignar direcciones IP.

16.1.3.1 Resolución del supuesto práctico

En primer lugar, es necesario realizar la instalación del servidor *DHCP ejecutando:*

UBUNTU

```
# apt-get install dhcp3-server
```

FEDORA

```
# yum install dhcp
```

Nota

Para utilizar el equipo como servidor es recomendable deshabitar SELinux (Security Enhanced Linux). Para ello edite el fichero /etc/selinux/config, modifique la variable SELINUX=disabled y reinicie el equipo.

Para configurar el servidor DHCP para la asignación dinámica de direcciones IP de tal forma que se preste servicio a la red 10.0.0.0/24 y, por otro lado, realizar una reserva al portátil con dirección MAC (AA.BB:CC:DD:EE:FF) para que se le asigne siempre la dirección IP 10.0.0.254.

Para comenzar con la configuración, debe indicar los parámetros generales del servidor y comunes a los equipos de la red, la información necesaria para que éste sepa cómo comportarse. Así, si el servidor *dhcp.ejemplo.es* es el que tiene la autoridad sobre la zona, se quiere que el tiempo máximo de asignación de una dirección IP sea de una semana (*max-lease-time*). Para ello, el fichero */etc/dhcp3/dhcpd.conf* (en Fedora */etc/dhcpd/dhcpd.conf*) debe tener el siguiente contenido:

```
authoritative;
one-lease-per-client on;
server-identifier 10.0.0.1;
default-lease-time 604800;
max-lease-time 604800;
ddns-update-style ad-hoc;
```

Posteriormente, se deben introducir los parámetros generales que se transmitirán a los clientes de la red. La red 10.0.0.0 con la máscara de red 255.255.255.0 tiene como puerta de enlace la dirección IP 10.0.0.1 y quiere utilizar los servidores de nombres 10.0.0.1 y 8.8.8.8. Además, hay que tener en cuenta el

rango de direcciones IP que desea asignar por DHCP que en el ejemplo es desde la dirección 10.0.0.100 a la 10.0.0.254.

A partir de estos parámetros de configuración debe escribir en el fichero la siguiente configuración:

```
subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.100 10.0.0.254;
    option subnet-mask 255.255.255.0;
    option broadcast-address 10.0.0.255;
    option routers 10.0.0.1;
    option domain-name-servers 10.0.0.1, 8.8.8.8;
    option domain-name "miempresa.com";
}
```

Como se desea realizar la reserva de la dirección IP 10.0.0.254 para el portátil con la dirección MAC AA:BB:CC:DD:EE:FF debe añadir las siguientes líneas:

```
host portatil {
    hardware ethernet AA:BB:CC:DD:EE:FF;
    fixed-address 10.0.0.254;
}
```

Para comprobar que la configuración del servidor *dhcpd* se ha realizado correctamente ejecute:

UBUNTU

```
# dhcpd3 eth1
```

FEDORA

```
# dhcpd eth1
```

siendo *eth1* la interfaz de red donde quiere que el servidor *dhcpd* ofrezca sus servicios.

UBUNTU

Una vez configurado correctamente el servidor inicie el servicio ejecutando:

```
# service dhcp3-server start
```

y configure el sistema para que se ejecute automáticamente:

```
# service dhcp3-server start
```

FEDORA

Una vez configurado correctamente el servidor inicie el servicio ejecutando:

```
# service dhcpd start
```

y configure el sistema para que se ejecute automáticamente:

```
# chkconfig dhcpd on
```

De esta forma el servidor *dhcpd* asigna automáticamente las direcciones IP a los equipos que se conecten a la red. Para comprobar las asignaciones que se han realizado puede consultar el fichero */var/lib/dhcp3/dhcpd.leases* (en Fedora */var/lib/dhcpd/dhcpd.leases*) donde, como puede ver a continuación, se muestran los datos de cada concesión de dirección IP:

```
server-duid "\000\001\000\001\023\375\362\001\000\014)\305#\377";
lease 10.0.0.100 {
  starts 3 2010/08/18 01:22:58;
  ends 3 2010/08/25 01:22:58;
  cltt 3 2010/08/18 01:22:58;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:24:2e:d0;
  uid "\001\000\014)$.\320";
  client-hostname "prueba-39a17d5a";
}
```

Datos más importantes

Nombre del servicio:	*dhcp3-server (Ubuntu)* *dhcpd (Fedora)*
Fichero de configuración:	*/etc/dhcp3/dhcpd.conf (Ubuntu)* */etc/dhcpd/dhcpd.conf (Fedora)*
Concesiones de direcciones:	*/var/lib/dhcp3/dhcpd.releases (Ubuntu)* */var/lib/dhcpd/dhcpd.releases (Fedora)*
Comandos más utilizados:	*dhcpd3 (Ubuntu)* *dhcpd (Fedora)* *dhclient*

16.2 SERVIDOR DNS

El servidor DNS más utilizado en los sistemas GNU/Linux es *bind* (*http://www.bind.com/*).

16.2.1 Instalación

Para prestar servicios de DNS en Linux es necesario instalar los paquetes *bind* y *bind-utils*, por lo que debe ejecutar:

UBUNTU

```
# apt-get install bind9 bind9utils
```

FEDORA

```
# yum install bind bind-utils
```

Si lo que se quiere es realizar la instalación con el entorno gráfico, acceda ir al menú *Sistema*, *Administración* y ejecutar la herramienta *Añadir y eliminar aplicaciones.* Una vez iniciada la herramienta seleccione el servidor de nombres y pulse el botón *Aplicar* para realizar la instalación.

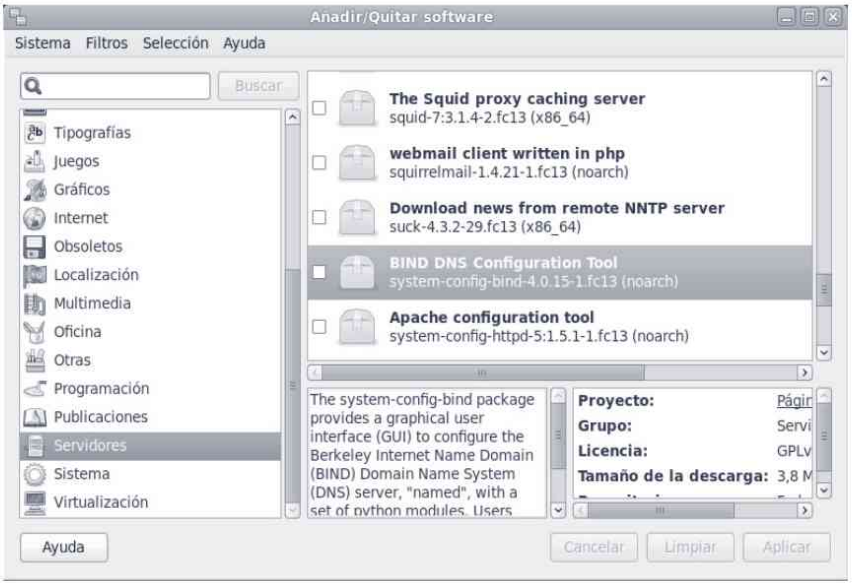


Figura 16-8. Aplicación gráfica para instalar el servidor de DNS

Nota

Para permitir el tráfico del servidor de nombres es necesario abrir los puertos 53/tcp y 53/udp.

16.2.2 Resolución del supuesto práctico

Para aprender a configurar el servidor de nombres se va a configurar el servidor que da acceso a la red interna 10.0.0.0/24 y que tiene la IP 10.0.0.1. El servidor gestiona la zona miempresa.com en la que hay que crear los siguientes registros: *www.miempresa.com* y *ftp.miempresa.com* apuntan a la IP 10.0.0.1; mail.miempresa.com es equivalente a *www.miempresa.com*; y el servidor de correo electrónico se encuentra en *mail.miempresa.com*.

Además, el servidor tiene la zona secundaria tuempresa.com que la administra el servidor DNS 20.0.0.1.

16.2.2.1 Configuración inicial

El fichero de configuración del servidor (*/etc/bind/named.conf* en Ubuntu y */etc/named.conf* en Fedora) es el encargado de proporcionar los datos necesarios para el funcionamiento del servidor DNS. En él se guardan las propiedades globales de las zonas donde el servidor actúa y el fichero donde se almacenan los datos de éstas.

Para empezar hay que configurar el servidor de nombres para que atienda las peticiones de la red interna (10.0.0.0/24) y si hay algún registro que no conozca le pregunte a otros servidores DNS externos (194.214.52.36 y 8.8.8.8).

Por tanto, el fichero de configuración */etc/bind/named.conf* tiene el siguiente contenido:

```
options {
        directory "/var/cache/bind";
        auth-nxdomain no ;  # Conform to RFC1035

        listen-on port 53 {
                127.0.0.1;
                10.0.0.1;
                };
        allow-query {
                localhost;
                10.0.0.0/24;
                };
        forwarders {
                194.214.52.36;
                8.8.8.8;
                };
};
```

UBUNTU

El fichero /etc/bind/named.cof hace un include a los ficheros named.conf.options, named.conf.local y named.conf.default.zones.

Los elementos de configuración que nos interesan están resaltados en negrita y permiten indicar los siguientes parámetros de configuración:

- **Interfaz donde el servidor DNS escucha las peticiones.** Para ello en la opción *liste-on port 53* indique las direcciones 127.0.0.1 y 10.0.0.1.
- **Red que puede realizar consultas al servidor DNS.** En la opción *allow-query* se establece que puede realizar consultas el equipo *localhost* y la red interna 10.0.0.0/24.
- **Servidores DNS reenviadores (*forwarders*).** La opción *forwarders* permite indicar los servidores DNS que van a actuar como reenviadores que en el ejemplo son los servidores 194.214.52.36 y 8.8.8.8.

Para que surtan efecto los cambios reinicie el servicio ejecutando:

UBUNTU

```
# service bind9 restart
```

FEDORA

```
# service named restart
```

16.2.2.2 Añadir zona primaria

Para añadir una zona de búsqueda primaria hay que modificar el fichero */etc/bind/named.conf.local* (en Fedora, */etc/bind/named.conf*) y añadir al final del fichero la zona miempresa.com que se encuentra en el fichero */var/lib/bind/miempresa.com.hosts*.

```
zone "miempresa.com" {
        type master;
        file "/var/lib/bind/miempresa.com.hosts";
        };
```

Y en el fichero de configuración de la zona */var/lib/bind//miempresa.com.hosts* se añaden los registros del dominio:

/var/lib/bind/miempresa.com.hosts

```
$ttl 38400
miempresa.com.  IN  SOA   localhost.localdomain. jgomez.ual.es. (
    1282101962
    86400         ; Refresh 24 hours
    3600          ; Retry   1 hour
    3600000       ; Expire  1000 hours
    86400         ; Minimum 24 hours
```

```
    )

miempresa.com.     IN      NS      localhost.localdomain.
www.miempresa.com.         IN      A       10.0.0.1
ftp.miempresa.com.         IN      A       10.0.0.1
mail.miempresa.com.        IN      CNAME   www.miempresa.com.
miempresa.com.     IN      MX      10 mail.miempresa.com.
miempresa.com.     IN      MX      20 mail.empresas.com.
```

Para comprender mejor el contenido del fichero a continuación se va a explicar el significado de cada registro:

- **Registro SOA.** Proporciona la información sobre la zona indicando el servidor de nombres primario, la dirección de correo del administrador de la zona y varios temporizadores útiles para los servidores secundarios. Un ejemplo de este registro es:

```
miempresa.com IN SOA localhost.localdomain. jgomez.ual.es. (
    1998072701      ; Serial
    86400           ; Refresh 24 hours
    3600            ; Retry   1 hour
    3600000         ; Expire  1000 hours
    86400           ; Minimum 24 hours
)
```

  Con este registro se indica que el dominio miempresa.com está controlado por el servidor local y que el correo del administrador es *jgomez@ual.es*. Los servidores secundarios se conectarán cada 24 horas al primario, si el número de serie es menor que el del primario, realizar una transferencia de zona para actualizarse (ya que el primario se habrá actualizado). Si el secundario no logra conectarse, se le indica que lo reintente dentro de una hora y si no es capaz de hacerlo en 1.000 horas, que deje de responder a consultas de resolución. El valor de 86.400 (24 horas) que se indica en el registro SOA es el valor por defecto usado para los registros en los que no se indica el TTL (*Time To Live*).

- **Registro NS.** Este tipo de registro indica el servidor de nombres encargado de la zona. Para los subdominios dependientes de otros servidores debe indicarse con una entrada para cada uno de los existentes y poder facilitar punteros a los servidores de más bajo nivel.

```
miempresa.com.     IN      NS      localhost.localdomain.
```

- **Registro A.** Asocia a un nombre una dirección IP. Si un host dispone de más de una interfaz de red debe tener un registro A por cada una de ellas.

```
www.miempresa.com.         IN      A       10.0.0.1
ftp.miempresa.com.         IN      A       10.0.0.1
```

- **Registro CNAME.** Permite crear alias para los nombres de equipos. En el siguiente ejemplo se indica que la dirección de mail.miempresa.com es la misma que *www.miempresa.com*.

```
mail.miempresa.com.        IN      CNAME   www.miempresa.com.
```

- **Registro MX.** Con el registro MX se indica la dirección IP y la prioridad del servidor de correo para el dominio especificado. En el siguiente ejemplo se indica que el servidor de correo principal es mail.miempresa.com y el secundario es mail.empresas.com.

```
empresa.com.     IN       MX       10 mail.miempresa.com.
empresa.com.     IN       MX       20 mail.empresas.com.
```

Una vez realizados los cambios reinicie el servicio ejecutando:

UBUNTU

```
# service bind9 restart
```

FEDORA

```
# service named restart
```

16.2.2.3 Añadir una zona secundaria

La creación de una zona secundaria es mucho más sencilla ya que tan solo hay que crear la zona e indicar la dirección IP del servidor DNS primario.

Por ejemplo, a continuación se crea la zona **tuempresa.com** que es gestionada por el servidor 20.0.0.1.

```
zone "tuempresa.com" {
        type slave;
        masters {
                20.0.0.1;
                };
        file "/var/lib/named/slaves/tuempresa.com.hosts";
        };
```

Una vez realizados los cambios reinicie el servicio.

Datos más importantes

Nombre del servicio:	*bind9 (Ubuntu)* *named (Fedora)*
Fichero de configuración:	*/etc/bind/named.conf (Ubuntu)* */etc/named.conf (Fedora)*
Fichero de configuración de una zona (p. ej., miempresa.com):	*/var/lib/named/miempresa.com.hosts*
Puertos utilizados:	*53/UDP y 53/TCP*

16.2.2.4 Configuración con asistentes

Además de configurar el servidor de nombres modificando directamente el fichero de configuración también puede configurarlo de forma gráfica a través de *webmin.*

FEDORA

También es posible utilizar la herramienta gráfica system-config-bind.

Para poder administrar el servidor de nombres con *webmin* escriba en el navegador la dirección del servidor (p. ej., *http://10.0.0.1:10000*) y en el menú *Servers*, pulse en *BIND DNS Sever* y aparece la ventana que se muestra en la figura 16-9.

Figura 16-9. system-config-bind

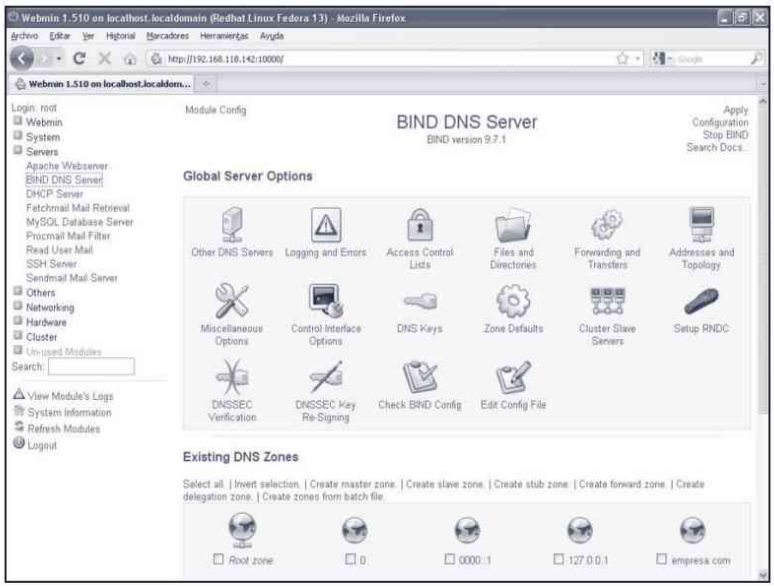


Figura 16-10. Configuración del servidor DNS con webmin

16.2.3 Utilidades de comprobación y prueba

Una vez configurado el servidor debe iniciarse el proceso que atiende las peticiones. Para ello basta con ejecutar:

```
# service bind start
```

Tras ello, si todo ha funcionado correctamente, el proceso *bind* escuchará las peticiones que le llegan por el puerto 53/UDP. En el caso de que no sea así, en el fichero */var/log/messages* aparecen los posibles errores que se han producido.

Una vez que el proceso servidor está ejecutándose, para comprobar que la configuración es la correcta, se puede utilizar uno de los siguientes comandos: *nslookup*, *dig*, *hosts* y *check-named-zone.*

16.2.3.1 nslookup

Herramienta que permite comprobar el funcionamiento de un servidor DNS mediante una interfaz que el cliente puede utilizar para realizar consultas de resolución al servidor indicado.

```
$ nslookup
> www.ual.es
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.ual.es
Address: 150.214.156.62
```

En el ejemplo anterior se realiza la consulta del registro *www.ual.es* y el servidor local 127.0.0.1 indica que el registro tiene la IP 150.214.156.62.

16.2.3.2 dig

Al igual que el comando *nslookup*, es una aplicación que actúa como cliente para interrogar a servidores DNS, devolviendo una detallada información sobre los servidores a los que se ha consultado. Por ejemplo, para consultar la dirección IP del servidor *www.ual.es* debe ejecutar:

```
$ dig www.ual.es
```

16.2.3.3 host

Host al igual que los anteriores comandos permite obtener la dirección IP que corresponde a un nombre y viceversa. A continuación puede ver cómo se ha utilizado el comando para obtener la dirección IP del registro *www.ual.es*:

```
$host www.ual.es
www.ual.es has address 150.214.156.62
```

16.2.3.4 named-checkconf/named-checkzone

named-checkconf es una utilidad que permite comprobar la sintaxis del fichero de configuración del servidor DNS. Para comprobar la configuración debe ejecutar:

```
# named-checkconf /etc/named.conf
```

Por otra parte, *named-checkzone* es una utilidad que se ejecuta en el servidor y comprueba la sintaxis e integridad de los ficheros de zona; realizando las mismas pruebas que realiza el proceso *named* cuando procesa los ficheros.

16.2.4 Seguridad

Los servidores de nombres, debido a su utilidad, juegan un papel muy importante en toda comunicación. Por un lado, un atacante puede aprovecharse de errores en el servicio para, ante la petición de resolución del nombre *www.ual.es*, asignar una dirección IP que no se corresponde con la real, permitiendo que las peticiones de servicio se dirijan a otro servidor. Este tipo de ataque se denomina *phising.*

Una buena costumbre consiste en limitar los equipos que pueden modificar datos de la siguiente forma:

```
allow-update { 10.0.0.1; };
```

Con esta orden, solo el servidor 10.0.0.1 puede actualizar los registros de la zona.

Nota

La configuración más habitual consiste en permitir solo las actualizaciones que provienen de servidores DHCP reconocidos.

Por otra parte, se debe ser muy cuidadoso con la configuración de un servidor de nombres para impedir que un atacante obtenga información sobre la red local. Para ello, un primer paso consiste en diferenciar la resolución local (nombres asociados a direcciones IP privadas) de la pública situando ambos servicios en servidores diferentes. Si no es posible, se puede configurar un único servicio DNS que diferencie la vista local de la pública:

```
acl internal { 10.0.0.0/24; };
View internal {
 math-clients { internal; };
 zone "ejemplo.es" {
        type master;
        files "db.data.ejemplo.interna";
              file "/var/named/miempresa.com.hosts.interna";

 };
};
View external {
 math-clients { any; };
 zone "ejemplo.es" {
        type master;
              file "/var/named/miempresa.com.hosts.externa";
 };
};
```

Además, se debe restringir los clientes a los que permite realizar consultas y los servidores a los que se les permiten peticiones de transferencia de zona. Este control se puede realizar a dos niveles, mediante:

- **Directivas apropiadas del servidor de nombres:**

```
allow-transfer { 10.0.0.2; };
allow-query { 10.0.0.0/24; };
```

Con la primera se permite la transferencia de zona exclusivamente al equipo 10.0.0.2, y con la segunda se permiten peticiones de resolución provenientes de la red 10.0.0.0/24.

- **Control del tráfico de red.** Otro aspecto muy importante es configurar el cortafuegos para permitir el tráfico de entrada al servidor (puerto 53/udp) de nuestra red interna.

Nota

Para que estas reglas sean efectivas, se deben incluir otras que denieguen por defecto todo el tráfico no permitido explícitamente.

16.3 ACCESO REMOTO AL SISTEMA

Los servicios más utilizados para acceder de forma remota a un sistema GNU/Linux son:

- **Telnet.** Permite acceder al sistema de forma remota de una manera no segura.
- **Open SSH.** Permite acceder al sistema por terminal pero de forma segura ya que se cifran las comunicaciones.
- **VNC.** Mientras que los servicios telnet y SSH permiten conectarse al servidor por medio de un terminal, el servidor VNC permite utilizar el servidor utilizando el escritorio instalado en el sistema: GNOME o KDE.

16.3.1 SSH

SSH es un protocolo que permite conectarse de forma segura a un servidor para poder administrarlo. En realidad, es más que eso, ya que se ofrecen más servicios, como la transmisión de ficheros, el protocolo *FTP* seguro e incluso se puede utilizar como transporte de otros servicios.

Figura 16-11. Página oficial openSSH (www.openssh.org)

El protocolo SSH garantiza que la conexión se realiza desde los equipos deseados (para lo que usa certificados) y establece una comunicación cifrada entre el cliente y el servidor, mediante un algoritmo de cifrado robusto (normalmente con 128 bits) que se utiliza para cualquier intercambio de datos.

A continuación va a ver cómo instalar y configurar el servicio *OpenSSH* (*www.openssh.org*) por ser el servidor *SSH* más utilizado.

16.3.1.1 Instalación

Al ser *ssh* el mecanismo más frecuente para acceder a un servidor, *OpenSSH* se instala por defecto al realizar la instalación del sistema. No obstante, si lo desea, para realizar la instalación de *OpenSSH* debe ejecutar:

UBUNTU

```
# apt-get install ssh
```

FEDORA

```
# yum install openssh
```

16.3.1.2 Configuración

El servidor *openSSH* utiliza el fichero de configuración */etc/ssh/sshd_config* y normalmente no es necesario modificarlo. Los parámetros más importantes son:

- **Port** y **ListenAdress.** Por defecto el servicio *ssh* trabaja en el puerto 22 y responde por todas las interfaces del sistema. Los siguientes parámetros permiten cambiar el puerto y la dirección, en las que atenderá peticiones:

```
Port 22
ListenAddress 0.0.0.0
```

- **PermitRootLogin.** Establece si se permite o no el acceso del usuario *root* al servidor.

```
PermitRootLogin no
```

- **AllowUsers.** Permite restringir el acceso a los usuarios del sistema. Al utilizar el parámetro *AllowUsers* indica los usuarios que pueden acceder al sistema.

```
AllowUsers cesar sonia
```

También es posible indicar el equipo anfitrión desde el que pueden conectarse. En el siguiente ejemplo solo los usuarios *cesar* y *sonia* pueden conectarse al servidor desde el equipo 10.0.0.2.

```
AllowUsers cesar@10.0.0.2 sonia@10.0.0.2
```

- Mensajes de entrada y conexión:

```
PrintMotd yes
Banner /etc/issue.net
```

- Configuración de seguridad y control de acceso:

```
IgnoreUserKnownHosts no
GatewayPorts no
AllowTcpForwarding yes
```

- Uso de subsistemas para otras aplicaciones, como por ejemplo, FTP.

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

Una vez configurado el servidor para que se apliquen los cambios ejecute:

UBUNTU

```
# /etc/init.d/ssh restart
```

FEDORA

```
# service sshd restart
```

16.3.1.3 Aplicaciones

Además de proporcionar servicio de sesiones remotas, el servidor SSH se puede utilizar para prestar otros servicios como la transferencia y copia segura de ficheros, ejecución remota de comandos, etc.

3.1.3.1 Cliente ssh

Cuando se trabaja con servidores lo normal es administrarlos de forma remota a través de *SSH* o *Webmin*. Si utiliza un equipo GNU/Linux y quiere conectarse al servidor tan solo hay que ejecutar:

```
$ ssh <equipo>
```

donde en *equipo* puede indicar el nombre del equipo o la dirección IP del mismo.

Si utiliza Windows y quiere conectarse al servidor en GNU/Linux lo mejor es utilizar la aplicación *PuTTY* (véase la figura 16-12).

Nota

En http://www.chiark.greenend.org.uk/~sgtatham/putty/ puede descargar PuTTY.

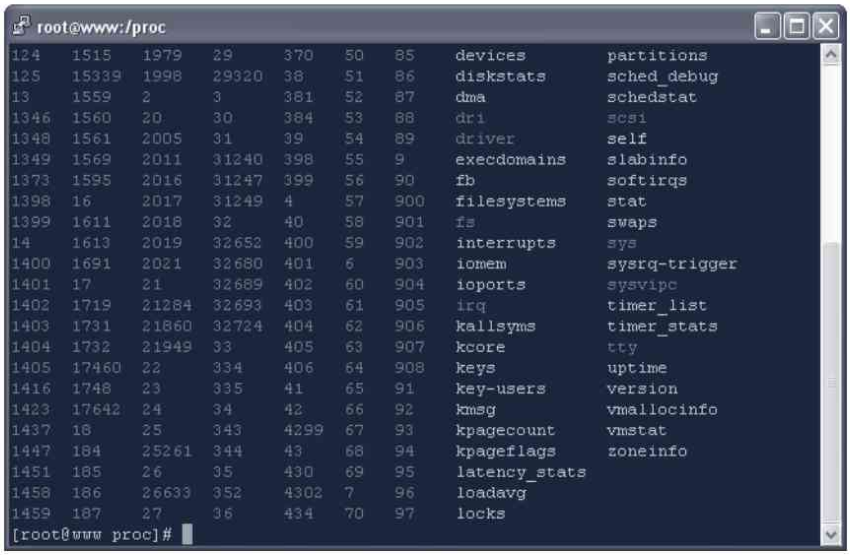


Figura 16-12. Conexión remota por SSH con PuTTY

3.1.3.2 scp

scp permite copiar ficheros entre dos equipos. Para poder copiar ficheros en un equipo remoto, éste debe tener instalado el servidor SHH. La sintaxis de *scp* es:

```
$ scp ficherolocal usuario@equipo_remoto:/directorio_remoto
```

donde:

- **fichero_local.** Especifica la fuente a copiar.
- **usuario.** Indica el usuario con el que va a acceder al sistema remoto.
- **equipo_remoto.** Indica a qué equipo se envía el fichero.
- **directorio_remoto.** Referencia al directorio destino del sistema de ficheros del equipo remoto.

Por ejemplo, para copiar el fichero local */etc/passwd* en la carpeta */root* en del servidor 10.0.0.2 ejecute:

```
$ scp /etc/passwd 10.0.0.2:/root
```

3.1.3.3 sftp

La utilidad *sftp* tiene la misma funcionalidad que *ftp* con la única diferencia que *sftp* establece una conexión segura utilizando el protocolo SSH como transporte. Su sintaxis es:

```
$ sftp usuario@equipo_remoto
```

Las opciones que admite el cliente sftp son: *get*, *put*, *mkdir*, *rm*, *cd*, *lcd*,..., similares a las opciones de los clientes ftp.

3.1.3.4 Montar por ssh

Es posible montar sistemas de ficheros remotos en el servidor a través de NFS y SAMBA. Pero si le resulta más cómodo, también puede montar sistemas de ficheros través del servicio SSH.

Para montar sistemas de ficheros por SSH hay que instalar el paquete *sshfs* ejecutando:

UBUNTU

```
# apt-get install ssh
```

FEDORA

```
# yum install sshfs
```

Para realizar el montaje hay que ejecutar:

```
# sshfs /mnt/fs 192.168.0.9:/datos /aux
```

Siendo */aux* la carpeta local donde se monta el directorio remoto */datos* del servidor 192.168.0.9.

3.1.3.5 scp y ssh sin contraseña

Dado el amplio uso que se realiza de los comandos *ssh* y *scp* para acceder a un servidor, copiar archivos (ya sea directamente por comando o con scripts) resulta muy práctico configurar el servidor para que un usuario pueda conectarse sin necesidad de escribir su contraseña.

Para que el servidor SSH no solicite la contraseña el cliente debe tener la clave pública en el fichero de claves autorizadas. Los pasos que debe realizar son:

Cliente

Desde del directorio *home* del usuario genere la clave privada y pública para el sistema RSA:

```
$ cd
$ ssh-keygen -b 4096 -t rsa
```

Copie la clave pública al servidor:

```
$ scp .ssh/id_rsa.pub root@servidor:.ssh/nueva_clave
```

Servidor

Acceda al servidor y copie la clave pública del cliente en *authorized_keys*:

```
$ ssh root@servidor
# cd .ssh/
# cat nueva_clave >> authorized_keys
```

Establezca los permisos de acceso al fichero:

```
# chmod 0700 $HOME/.ssh/
# chmod 0600 $HOME/.ssh/authorized_keys
```

La primera vez que se accede al servidor se almacena su *host_key* en el fichero *$HOME/.ssh/know_hosts* y a partir de ese momento puede conectarse al servidor sin necesidad de contraseña.

Nota

Evidentemente, se puede repetir este método para cualquier máquina y en ambos sentidos si se desea.

Datos más importantes

Nombre del servicio:	*sshd*
Fichero de configuración:	*/etc/ssh/sshd_config*
Host a los que se les permite el acceso:	*/etc/host.allow*
Equipos autorizados para acceder por SSH sin contraseña:	*$HOME/.ssh/authorized_keys*
Comandos más utilizados:	*ssh, scp* y *sftp*
Puerto utilizado:	*22/TCP*

16.3.1.4 Seguridad

3.1.4.1 Configuración básica de seguridad

Proporcionar sesiones de trabajo a un usuario en un equipo es arriesgado ya que éste puede aprovechar los diferentes *exploits* existentes para ejecutar comandos con privilegios de administrador. Por ello, se considera una buena política la

restricción de estos servicios, por una parte, a los equipos conocidos desde los que se desea utilizar este servicio y, por otra, a los usuarios que deban hacer uso de éste.

La restricción por clientes se puede realizar mediante:

- Reglas de control de tráfico de red:

```
# iptables -A INPUT -p tcp -dport 22 -s 172.20.41.0/24 -j
ACCEPT
# iptables -A OUTPUT-p tcp -sport 22 -d 172.20.41.0/24 -j
ACCEPT
```

- El fichero */etc/hosts.allow*:

```
sshd: 10.0.0.0/24
```

Por otra parte, el control de usuarios se debe realizar con opciones de configuración del servidor SSH:

```
AllowUsers javier cesar
```

Con esta directiva se permite el uso del servicio a los usuarios *javier* y *cesar*.

Además, también es recomendable no permitir el uso de las relaciones de confianza establecidas con los ficheros *.rhosts* y *.shosts*:

```
IgnoreRHosts  yes
```

Por último una buena costumbre es la de no permitir el acceso del usuario *root* directamente con el login:

```
PermitRootLogin  no
```

Nota

Con esta configuración, para acceder con el usuario root, primero debe acceder al sistema con otro usuario y, posteriormente, ejecutar el comando su para obtener el shell de root.

3.1.4.2 fail2ban

Cuando se administra un servidor público (con una dirección IP pública) es muy frecuente recibir ataques de fuerza bruta para acceder al sistema. Un ataque de fuerza bruta sobre *ssh* consiste en intentar iniciar sesión en el sistema con todas las combinaciones de nombres y contraseñas posibles.

Si no se toman las medidas adecuadas es posible que sea objeto de este tipo de ataque y si la contraseña no es segura, el atacante podrá acceder al sistema.

Para evitar los ataques de fuerza bruta, una de las mejores soluciones es utilizar *fail2ban* (*http://www.fail2ban.org*). Si utiliza *fail2ban* cuando se realizan 5 intentos fallidos de autenticación en el sistema *fail2ban* se comunica con el cortafuegos *iptables* y bloquea su dirección IP.

La instalación de *fail2ban* es muy sencilla ya que tan solo debe ejecutar:

UBUNTU

```
# apt-get install fail2ban
```

FEDORA

```
# yum install fai2ban
```

e iniciar el servicio en el sistema ejecutando:

```
# service fail2ban start
```

16.3.2 VNC

VNC es un programa con licencia GPL que utiliza el modelo cliente/servidor y permite acceder a un equipo remotamente utilizando su entorno gráfico.

16.3.2.1 Servidor

Para realizar la instalación del servidor *vnc* debe realizar los siguientes pasos:

- Instale el servidor de *vnc* ejecutando:

UBUNTU

```
# apt-get install tightvncserver
```

FEDORA

```
# yum install tigervnc-server
```

- Establezca la contraseña del servidor vnc ejecutando el comando:

```
# vncpasswd
```

- Ejecute el comando para crear automáticamente los ficheros de configuración e iniciar el servicio:

```
# vncserver
```

FEDORA

Si quiere que el servicio se ejecute automáticamente ejecute:

```
# chkconfig vncserver on
```

Nota

Para permitir el tráfico del servidor VNC es necesario abrir los puertos 6000/tcp, 6001/tcp, 6002/tcp y 6003/tcp.

Datos más importantes

Nombre del servicio:	*vncserver*
Fichero de configuración:	*/etc/sysconfig/vncservers*
Comandos más importantes:	*vncpasswd vncserver*
Puertos:	6000/tcp, 6001/tcp, 6002/tcp y 6003/tcp.

16.3.2.2 Cliente

Para acceder al servidor puede utilizar cualquier cliente VNC. Por ejemplo, en sistemas GNU/Linux puede utilizar *Vinagre* y en sistemas Windows puede utilizar *tightVNC*.

Vinagre (GNU/Linux)

Si desea acceder desde un equipo GNU/Linux a un servidor VNC, la mejor opción es utilizar el cliente *vinagre.* Para utilizar *vinagre* primero debe instalarlo ejecutando.

UBUNTU

```
# apt-get install vinagre
```

FEDORA

```
# yum install vinagre
```

Vaya al menú *Aplicaciones*, *Internet* y ejecute la aplicación *Remote Desktop Viewer*. Pulse el botón *Connect*, indique la dirección del servidor VNC (p. ej., 10.0.0.1:5901) y pulse *Connect* para acceder al servidor VNC (véase la figura 16-13).

Figura 16-13. Acceso al servidor por VNC con Vinagre (Linux)

tightVNC (Windows)

tightVNC es un cliente/servidor VNC que se encuentra licenciado bajo GPL. Para acceder desde Windows al servidor VNC debe realizar los siguientes pasos:

- Descargue *tightVNC* de la página oficial *http://www.tightvnc.com*.
- Instale en el equipo el visor *tightVNC*.
- Ejecute *tightVNC Viewer* que puede encontrar dentro del menú de aplicaciones *tightVNC.*
- *En TihgVNC Server* escriba la dirección IP del servidor y el puerto (p. ej., 10.0.0.1:5901).

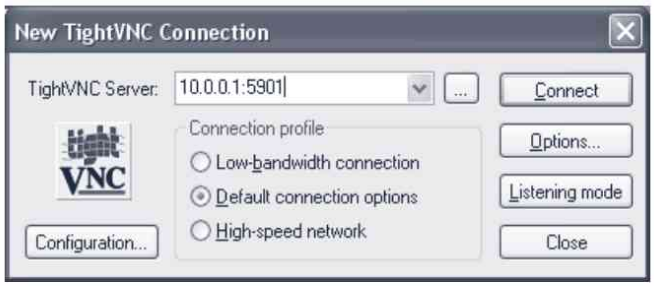


Figura 16-14. tightVNC conection

- Finalmente, pulse el botón *Connect*, introduzca la contraseña del servidor VNC establecida durante el proceso de instalación y tal como puede ver en la figura 16-15 ya tiene acceso al escritorio del servidor.

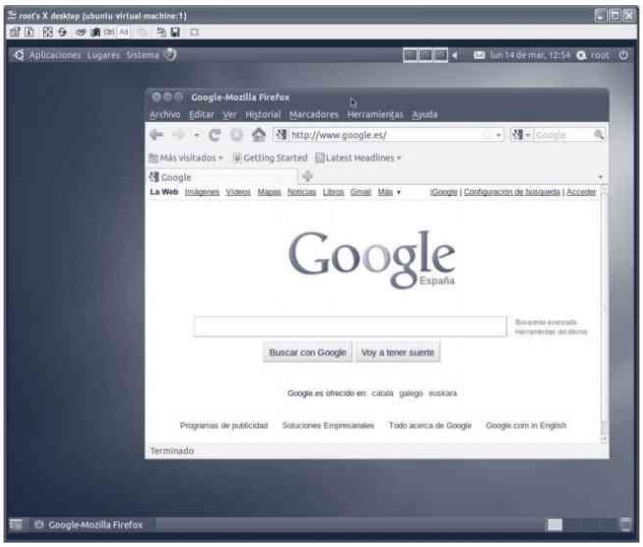


Figura 16-15. Acceso al servidor VNC con tightVNC viewer (Windows)

Capítulo 17

SERVIDORES DE IMPRESIÓN Y DE ARCHIVOS

En el capítulo anterior se ha creado la infraestructura de red y se han configurado los servicios más importantes para su correcto funcionamiento (enrutamiento, DHCP y acceso remoto). En esta ocasión el objetivo es aprender a configurar el servidor para compartir recursos entre sistemas GNU/Linux y Windows. Para poder compartir recursos entre otros equipos se pueden utilizar los siguientes servicios:

- **Compartir archivos e impresoras (Samba).** Este método se utiliza para compartir recursos entre equipos GNU/Linux y Windows.
- **NFS.** El servicio NFS es nativo de los sistemas GNU/Linux y permite compartir carpetas a través de la red. Este servicio es muy estable y se recomienda su uso para compartir información entre sistemas GNU/Linux.

17.1 COMPARTIR ARCHIVOS E IMPRESORAS (SAMBA)

Samba es el método más utilizado para permitir la integración entre sistemas ya que permite que los equipos Windows y GNU/Linux puedan compartir carpetas e impresoras entre sí.

Samba es una colección de programas que hacen que Linux sea capaz de utilizar el protocolo SMB (*Server Message Block*) que es la base para compartir ficheros e impresoras en una red Windows. Los posibles clientes para un servidor SMB incluyen LAN Manager, Windows NT, OS/2 y otros sistemas GNU/Linux.

17.1.1 Instalación

Samba está compuesto por tres paquetes: *samba-common* (archivos comunes), *samba-client* (cliente) y *samba* (que es el servidor). Por tanto, los paquetes que necesita instalar dependen del uso que quiera darle al equipo.

Para instalar el cliente y servidor de *Samba* es necesario ejecutar:

UBUNTU

```
# apt-get install samba4 smbclient
```

FEDORA

```
# yum install samba samba-client
```

A continuación, inicie el servicio ejecutando:

UBUNTU

```
# service samba4 start
```

FEDORA

```
# service smb start
```

17.1.2 Configuración

Para que *Samba* funcione correctamente primero debe dar de alta los usuarios del sistema y luego configurar los recursos a compartir.

17.1.2.1 Gestión de usuarios

Samba realiza una gestión de usuarios independiente a la del sistema operativo. Por esta razón necesita dar de alta los usuarios que vayan a utilizar S*amba.*

El comando *smbpasswd* se utiliza para administrar los usuarios de *Samba* y sus contraseñas. La sintaxis del comando es:

```
# smbpasswd -opcion usuario
```

donde *-opcion* es la opción a realizar y *usuario* es el nombre del usuario con el que quiere trabajar. En la tabla 17-1 puede ver las opciones más importantes del comando *smbpasswd.*

Tabla 17-1. Opciones más utilizadas de *smbpasswd*

Opción	Comentario
-a	Añade un usuario.
-x	Elimina un usuario.
-d	Deshabilita usuario.
-e	Habilita usuario.
-n	Establece la contraseña a NULL.

Así, por ejemplo, para añadir el usuario *juan* debe ejecutar el comando *smbpasswd –a juan* e introducir su contraseña:

```
# smbpasswd  -a juan
New SMB password:
Retype new SMB password:
Added user juan.
```

Y para eliminarlo hay que ejecutar:

```
# smbpasswd -x juan
Deleted user juan.
```

Nota

Para poder añadir un usuario en Samba éste tiene que existir en el sistema. Para dar de alta un usuario en el sistema utilice el comando adduser.

Para ver todos los usuarios de *Samba* en las primeras versiones bastaba con ver el contenido del fichero */etc/samba/smbpasswd* pero en las actuales versiones los usuarios y contraseñas se guardan en la base de datos SAM. Para ver los usuarios de *Samba* debe ejecutar el siguiente comando:

```
# pdbedit -w -L
juan:500:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:3527DA04C3D767E36C618
ED59764BD43:[U          ]:LCT-4B661D14:
eugenio:501:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:FA5664875FFADF0AF6
1ABF9B097FA46F:[U          ]:LCT-4C655E09:
encarni:503:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:0D7F1F2BDEAC6E574D
6E18CA85FB58A7:[U          ]:LCT-4C6569B6:
```

17.1.2.2 Compartir carpetas

Para compartir una carpeta hay que modificar el fichero de configuración de *Samba /etc/samba/smb.conf.* En la tabla 17-2 puede ver las opciones más importantes para compartir carpetas.

El ejemplo más sencillo que se puede realizar es compartir una carpeta de forma pública para todos los usuarios. Para ello añada:

```
[publico]
        path = /publico
        public = yes
        read only = yes
```

Tabla 17-2. Opciones más utilizadas de *smbpasswd*

Opción	Comentario
[recurso]	Nombre del recurso compartido.
browseable	Indica si se puede explorar dentro del recurso. Los posibles valores son *no* y *yes*.
comment	Proporciona información adicional sobre el recurso (no afecta a su forma de operar).
create mode	Especifica los permisos por defecto que tienen los ficheros creados.
directory mode	Especifica los permisos por defecto que tienen los directorios creados.
force user	Especifica el usuario propietario que tienen los ficheros y carpetas que se crean.
force group	Especifica el grupo propietario que tienen los ficheros y carpetas que se crean.
guest ok	Indica si se permite el acceso a usuarios anónimos. Los posibles valores son *no* y *yes*.
path	Carpeta a compartir.
public	Indica si el directorio permite el acceso público. Los posibles valores son *no* y *yes*.
read only	Indica que el directorio es solo lectura. Los posibles valores son *no* y *yes*.
valid users	Indica los usuarios que pueden acceder a la carpeta. Para añadir un grupo entonces hay que poner el nombre del grupo precedido de la @.
writable	Indica que se puede modificar el contenido de la carpeta.
write list	Indica los usuarios que pueden modificar el contenido.

O si lo prefiere, puede establecer que el recurso sea accesible solamente por unos determinados usuarios:

```
[miscosas]
        path = /datos/
        comment = "Datos y aplicaciones"
        valid users = juan,encarni,@master
```

Lógicamente los usuarios se han tenido que crear previamente y el grupo *master* debe existir en el fichero */etc/group.*

```
master:x:502:juan,encarni
```

A continuación se amplía el ejemplo pero estableciendo el permiso de escritura para el usuario *juan* y el permiso de lectura para el usuario *encarni* y el grupo *master.* Además, cuando un usuario crea un fichero o carpeta éste se crea en el sistema con un propietario (*juan:juan)* y unos determinados permisos (770).

```
[miscosas]
        path = /datos/
        comment = "Datos y aplicaciones"
```

```
        valid users = juan, encarni,@master

        writeable = yes
        write list = juan
        read list = juan,@master

        force user = juan
        force group = juan
        create mode = 770
        directory mode = 770
```

Nota

Cuando se comparte una carpeta es necesario establecer los permisos en el fichero de configuración y en el sistema de ficheros. Para ello puede utilizar los comandos: chmod, chown y chgrp.

Finalmente, para que se apliquen los cambios reinicie el servicio:

```
# service smb restart
```

17.1.2.3 Compartir impresora

Existen dos formas de compartir las impresoras que se encuentran conectadas al equipo para que las puedan utilizar todos los clientes de la red: a través de la herramienta gráfica *system-config-printer* o utilizando *samba.*

Nota

Existen impresoras con tarjeta de red que permiten a los clientes imprimir directamente sin necesidad de ningún servidor.

system-config-printer

Normalmente, en los sistemas Fedora, se encuentra instalada por defecto la herramienta *Imprimiendo*. No obstante, si desea realizar la instalación debe ejecutar:

UBUNTU

Dependiendo del entorno gráfico que utiliza debe ejecutar

```
# apt-get install system-config-printer-gnome
```

o

```
# apt-get install system-config-printer-kde
```

FEDORA

```
# yum install system-config-print
```

Una vez realizada la instalación vaya al menú *Administración* y seleccione *Imprimiendo.* Tal y como puede ver en la figura 17-1 el sistema muestra las impresoras activas en el sistema.

Figura 17-1. Imprimiendo

Las tareas más frecuentes que se pueden realizar son:

- **Compartir las impresoras a través de Internet.** Para que otros equipos puedan utilizar las impresoras del servidor vaya al menú *Servidor* y seleccione *Configuración.* En la ventana que se muestra en la figura 17-2 active la casilla *Publicar impresoras compartidas* y *Permitir la impresión desde Internet.*

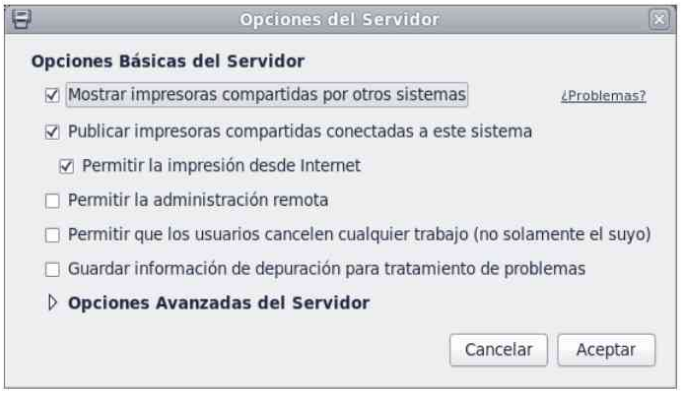


Figura 17-2. Opciones del servidor

- **Compartir una impresora.** Seleccione la impresora que desea compartir, pulse el botón derecho, seleccione *Propiedades* y en la pestaña *Control de acceso* indique los usuarios que pueden utilizar la impresora.
- **Administrar los grupos de impresión.** Permite que varias impresoras formen un mismo grupo de forma que cuando se envía un trabajo se procese en la impresora que se encuentre disponible.
- Para **gestionar los trabajos de la impresora** seleccione la impresora, pulse el botón derecho y selecciona *Ver la cola de impresión*. En la ventana que aparece puede ver y administrar todos los trabajos de la impresora.

Samba

Para compartir una impresora hay que añadir en el fichero de configuración de *Samba /etc/samba/smb.conf* un nuevo recurso siguiendo la siguiente estructura:

```
[printers]
    comment = All printers
    path = /var/spool/samba
    browseable = no
    printable = yes
    public = no
    writable = no
    create mode = 0700
```

El acceso a las impresoras Linux desde Windows funciona de la misma forma que los directorios. El nombre compartido es el nombre de la impresora Linux en el fichero *printtab*. Por ejemplo, para acceder a la impresora *HP_laserjet*, los usuarios de Windows deben acceder a *\\smbserv\HP_laserjet.*

A modo de resumen, en la tabla 17-3 se muestran los parámetros utilizados en la sección *[printers].*

Tabla 17-3. Parámetros de la sección *[printers]*

Parámetro	Comentario
comment	Proporciona información sobre la sección (no afecta a la operación).
path	Especifica la ruta de acceso al spool (que por defecto es */var/spool/samba*). Es posible crear un directorio de spool para Samba y hacer que apunte a él.
browseable	Como con los directorios raíz, si indica NO se asegura de que solo puedan ver las impresoras los usuarios autorizados.
printable	Se debe poner *YES*, si no se hace así no funcionarán las impresoras.
public	Si se pone *YES*, cualquier usuario podrá imprimir (en algunas redes se pone *NO* para evitar la impresión excesiva).
writable	Las impresoras no son escribibles, por tanto escriba NO.

17.1.2.4 Configuración con asistentes

Dado el gran uso que se realiza de *Samba* para compartir información entre sistemas Windows y GNU/Linux, existen varias interfaces que facilitan el proceso de configuración de sistema. Las interfaces más importantes son:

- **Swat.** Es una interfaz web específica para administrar *Samba*. Para realizar la instalación debe ejecutar:

UBUNTU

```
# apt-get install swat
```

FEDORA

```
# yum install samba-swat
```

Una vez instalado el servicio hay que modificar el fichero /etc/xinetd.d/swat, establecer la variable disabled=no y reiniciar el servicio xinetd ejecutando:

```
# service xinetd restart
```

Finalmente, inicie *el navegador* y escriba la dirección *http://127.0.0.1:901* y aparece la interfaz de administración de swat (véase la figura 17-3a).

- **Webmin.** Como siempre *webmin* permite configurar cualquier servicio del servidor. Para acceder al módulo de configuración pulse en *Servers. Samba Windows File Sharing* (véase la figura 17-3b).
- **system-config-samba.** Por último, también dispone de la herramienta de x-Windows para administrar *Samba* (véase la figura 17-4). Para instalarla ejecute:

UBUNTU

```
# apt-get install system-config-samba
```

Además, es necesario instalar las siguientes dependencias :

```
# apt-get install gksu python-gtk2 python-glade2
```

FEDORA

```
# yum install system-config-samba
```

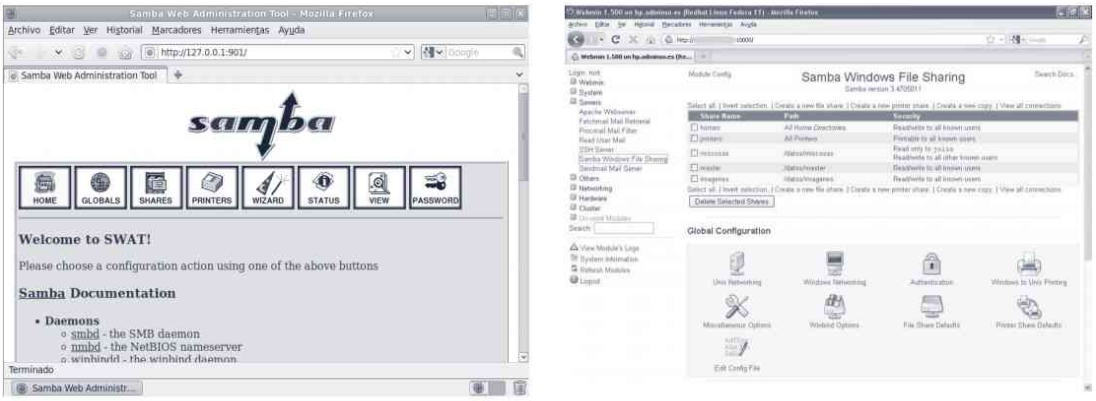


Figura 17-3. Administración de Samba utilizando a) swat y b) webmin

Figura 17-4. system-config-samba

17.1.3 Cliente

Además de actuar como servidor de ficheros, el equipo puede utilizarse como cliente para acceder a los recursos compartidos que hay en otros servidores.

Existen varias formas para acceder desde Linux a carpetas e impresoras compartidas. La forma más sencilla es mediante dos programas cliente que vienen en la instalación de *Samba*: *smbclient* y *smbprint*. Aunque esta solución funciona, está algo limitada, particularmente en el acceso a ficheros. *Smbclient* proporciona una forma similar a un servidor FTP para acceder a un recurso remoto compartido. No permite el uso de comandos normales de Unix como *cp* y *mv* para manipular los ficheros y, por tanto, no permite acceder a los recursos compartidos de otras aplicaciones (a diferencia de los sistemas de ficheros remotos montados con NFS, que aparecen para las aplicaciones Linux como sistemas de ficheros locales).

Este problema se puede evitar montando el sistema de ficheros compartidos SMB en Linux, como se hace con sistemas de ficheros NFS y locales.

17.1.3.1 smbclient

El programa *smbclient* permite conectarse a un servidor SMB y utilizar el sistema de ficheros utilizando una interfaz similar al FTP.

El primer paso para usar *smbclient* es conectarse al servidor para ver el listado de recursos disponibles. Para ver los recursos ejecutamos:

```
$ smbclient -L \\\\IP_servidor
```

Si quiere especificar directamente el usuario entonces ejecute:

```
$ smbclient -L \\\\IP_servidor r -U usuario
```

En la salida del comando puede ver un listado de todos los recursos que tiene el equipo:

```
[root@ubuntu samba]# smbclient -L \\\\10.0.0.1
Enter root's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.5.4-63.fc13]

        Sharename       Type      Comment
        ---------       ----      -------
        miscosas        Disk
        master          Disk
        IPC$            IPC       IPC Service (Samba Server
Version 3.5.4-63.fc13)
Anonymous login successful
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.5.4-63.fc13]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

Y si quiere conectarse al recurso entonces ejecute:

```
$ smbclient  \\\\10.0.0.1\\miscosas -U usuario
```

o si lo prefiere puede conectarse directamente indicando la contraseña:

```
$ smbclient  \\\\10.0.0.1\\miscosas -U usuario contraseña
smb: \>
```

Una vez conectado, aparece el shell de *Samba* (*smb:* \>) que permite interactuar con el sistema viendo el contenido de un directorio, copiando archivos, creando directorios, etc. En la tabla 17-4 se muestran los comandos más utilizados. Si desea más información puede utilizar el comando *help*.

Tabla 17-4. Comandos de operación con ficheros

Operación	Comentario
cd directorio	Cambia de directorio en el recurso compartido SMB.
del fichero rm fichero	Borra en el servidor el fichero especificado.
dir ls	Muestra el contenido del directorio actual del servidor.
get fichero	Obtiene el fichero especificado desde el servidor remoto y lo guarda con el mismo nombre en el directorio actual del sistema local. Opcionalmente se puede especificar un nombre diferente en el sistema local: *get fichero nombrelocal.*
help ?	Muestra los comandos del sistema. Para obtener información específica de un comando entonces ejecute: *help comando.*
lcd directorio	Cambia al directorio especificado en el sistema local.
mget fichero	Obtiene todos los ficheros del directorio especificado que contengan la máscara especificada.
mkdir directorio md directorio	Crea un directorio en el servidor remoto.
mput fichero	Copia los ficheros que coincidan con la máscara especificada, del directorio local al directorio actual del servidor remoto.
prompt	Realiza o no la pregunta por cada fichero copiado durante las operaciones *mput* y *mget.*
put fichero	Copia el fichero especificado desde el directorio local actual al servidor remoto y mantiene el nombre del fichero. Se puede cambiar el nombre del fichero en el servidor remoto: *put fichero nombreremoto*.
quit exit	Sale de *smbclient*.
recurse	Activa o desactiva la repetición en las operaciones de ficheros múltiples (*mput* y *mget*). Cuando está activado, el comando busca por todos los directorios que hay a partir del actual.
rmdir directorio rd directorio	Elimina el directorio especificado en el servidor remoto.

A continuación puede ver cómo el comando *ls* muestra el contenido del recurso compartido:

```
smb: \> ls
  .                   D        0  Fri Aug 13 17:48:58 2010
  ..                  D        0  Mon Jul 12 00:36:28 2010
  Software            D        0  Wed Jul 21 17:55:35 2010
  datos               D        0  Mon May 31 10:45:47 2010
  libro               D        0  Wed Jun 23 14:02:26 2010
  drivers             D        0  Wed Nov 18 10:03:53 2009

2513 blocks of size 8388608. 18307 blocks available
smb: \>
```

17.1.3.2 Montar el sistema de ficheros SMB

Otra forma más sencilla de acceder a un recurso compartido de *Samba* es montarlo en una carpeta y así poder acceder al contenido del recurso de la misma forma que lo hace con cualquier otra carpeta del sistema.

Para montar el recurso primero hay que crear la carpeta donde se va montar el recurso y luego ejecutar el comando *mount.*

```
$ mkdir /prueba
$ mount -t cifs -o user=usuario,pass=contrasena
//10.0.0.1/recurso /prueba
```

donde:

- **-t cifs.** Indica el tipo de fichero que se va a utilizar, que en este caso es *cifs.*
- **-o user=usuario,pass=contrasena.** Indica el nombre del usuario y la contraseña con la que se quiere acceder.
- **//10.0.0.1/recurso.** Indica la dirección IP y el nombre del recurso al que quiere acceder.
- **/prueba.** Es el directorio donde se va a montar el recurso compartido.

Nota

Para ver si se ha montado correctamente el recurso puede ejecutar el comando mount o entrar en la carpeta y ver su contenido.

Para que el recurso se monte automáticamente al iniciar el equipo hay que añadir al fichero */etc/fstab* la siguiente línea:

```
//10.0.0.1/recurso /prueba cifs rw,username=login,password=pass 0 0
```

donde *username* y *password* especifican el nombre y la contraseña del usuario con el que acceder al servidor.

Más información

Si desea más información sobre la utilización de sistemas de ficheros puede consultar el punto 13.2. Sistema de ficheros.

Datos más importantes

Nombre del servicio:	*samba4 (Ubuntu)* *smb (fedora)*
Fichero de configuración:	*/etc/samba/smb.conf*
Comandos más utilizados:	*smbpasswd smbclient pdbedit mount*
Puertos utilizados:	*137/UDP, 138/UDP, 139/TCP y 445/TCP*

17.2 NFS

Network File System (Sistema de archivos de red) es un servicio que permite que los equipos GNU/Linux puedan compartir carpetas entre sí. El servicio NFS se basa en el modelo cliente/servidor de forma que un servidor comparte una carpeta para que los clientes puedan utilizarla. De esta forma, una vez que un cliente monta una carpeta compartida puede utilizarla normalmente como si se tratara de una carpeta del sistema de ficheros local.

En Fedora el servicio se encuentra instalado por defecto, pero en Ubuntu es necesario instalarlo de la siguiente forma:

UBUNTU

```
# apt-get install nfs-kernel-server nfs-common portmap
```

17.2.1 Configuración del servidor

Antes de iniciar la configuración hay que iniciar el servicio ejecutando:

UBUNTU

```
# service nfs-kernel-service start
```

FEDORA

```
# service nfs start
```

17.2.1.1 Compartir una carpeta

Para indicar los directorios que se desea compartir hay que modificar el fichero */etc/exports* de la siguiente forma:

```
<directorio> <IP>(permisos) <IP>(permisos)...
```

Los permisos que se pueden establecer son: *rw* (lectura y escritura) y *ro* (lectura). Por ejemplo, para compartir la carpeta */datos* para que el equipo 192.168.20.9 pueda acceder en modo lectura y escritura, y el equipo 192.168.20.8 tan solo pueda acceder en modo lectura, se escribe:

```
/datos 192.168.20.9(rw) 192.168.20.8(ro)
```

Una vez compartida la carpeta, reinicie el servicio ejecutando:

UBUNTU

```
# service nfs-kernel-service restart
```

FEDORA

```
# service nfs restart
```

17.2.1.2 Permisos

La carpeta se comparte solamente a la IP establecida en el fichero */etc/exports* por el usuario *nfsnobody*.

De forma que la carpeta que está compartiendo tiene que tener los permisos para el usuario *nfsnobody*. Para establecer los permisos ejecute:

```
# chmod 660 /datos -R
# chown nfsnobody /datos -R
# chgrp nfsnobody /datos -R
```

Como el usuario *nfsnobody* tiene un UID y GUID diferente en cada equipo es recomendable asignarle el mismo identificador modificando los ficheros */etc/passwd* y */etc/groups* tanto en los equipos clientes como servidores.

17.2.2 Configuración del cliente

Para acceder al directorio que comparte el servidor hay que montarlo, ya sea manual o automáticamente, al iniciar el equipo.

17.2.2.1 Montar la unidad de forma manual

Para montar el sistema de ficheros en el cliente hay que ejecutar:

```
#  mount 192.168.20.100:/datos /prueba
```

donde:

- *192.168.20.100:/datos* es la carpeta que se ha compartido en el servidor en el fichero */etc/exports*.
- */mnt/trabajo* es la carpeta donde se monta la carpeta compartida.

17.2.2.2 Montar la unidad de forma automática

Para montar el sistema de ficheros de forma automática hay que modificar el fichero */etc/fstab* añadiendo la siguiente línea:

```
192.168.20.100:/datos    /prueba     nfs    rw,hard,intr     0 0
```

donde:

- *rw.* Indica que se monta el directorio en modo lectura/escritura. Para montarlo solo en modo lectura escriba *ro.*
- *hard.* Indica que si al copiar un fichero en la carpeta compartida se pierde la conexión con el servidor se vuelva a iniciar la copia del fichero cuando el servidor se encuentre activo.
- *intr.* Evita que las aplicaciones se queden "colgadas" al intentar escribir en la carpeta si no se encuentra activa.

Datos más importantes

Nombre del servicio:	*nfs*
Carpetas compartidas:	*/etc/exports*
Comandos más utilizados:	*mount*
Puertos:	*2049/TCP y 2049/UDP*

Capítulo 18

SERVICIOS DE INTERNET

Hoy en día Internet es una red de ámbito mundial que nos permite acceder a múltiples servicios. Por ejemplo, consultar una página web, enviar correos electrónicos, videoconferencia, etc. A pesar de que existen muchos servicios en Internet, los servicios que han permitido la gran difusión de Internet son:

- Servidor World Wide Web (WWW).
- Servidor de transferencia de ficheros (FTP).
- Servidor de correo electrónico.

18.1 SERVIDOR WEB (APACHE)

18.1.1 Instalación

Para instalar el servidor *Apache* fácilmente desde repositorios ejecute el comando:

UBUNTU

```
# apt-get install apache2
```

El servicio se inicia automáticamente:

```
# chkconfig apache2 on
```

E inicie ahora el servicio:

```
# service apache2 start
```

FEDORA

```
# yum install httpd
```

El servicio se inicia automáticamente:

```
# chkconfig httpd on
```

E inicie ahora el servicio:

```
# service httpd start
```

Una vez instalado, *Apache* publica automáticamente el contenido del directorio */var/www* en Ubuntu o */var/www/html* en Fedora. De esta forma, para publicar una página web debe crearla en dicho directorio.

Para acceder a la web principal de nuestro servidor escriba en la barra de direcciones *http://localhost/* o *http://dirección_ip/*:

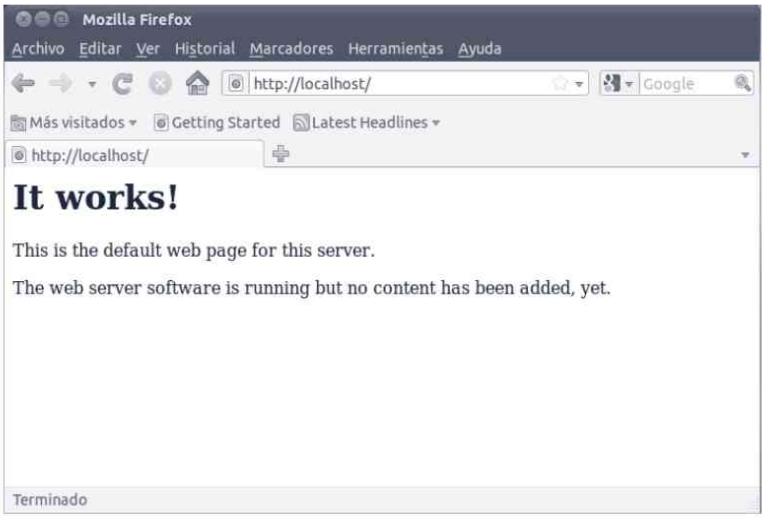


Figura 18-1. Página web de prueba de Apache

18.1.1.1 Instalar módulo de php

PHP (*Hypertext Pre-Processor*) es un lenguaje de programación interpretado por el servidor de páginas web de forma que éstas se pueden generar de forma dinámica. PHP no solo se utiliza para este propósito, sino que además se puede utilizar desde una interfaz de línea de comandos o para la creación de aplicaciones con interfaces gráficas.

En la dirección web oficial del proyecto (*http://php.net/*) puede encontrar una amplia documentación sobre el lenguaje: manuales, sintaxis utilizada, interfaz para la programación de las aplicaciones, etc.

Para instalar PHP automáticamente ejecute:

UBUNTU

```
# apt-get install php5
```

FEDORA

```
# yum install php
```

Para comprobar que PHP se ha instalado con éxito puede crear un fichero *php* y ubicarlo en el directorio raíz del servidor web. Por ejemplo, para mostrar toda la información útil disponible y detalles sobre la instalación actual de PHP, edite el fichero */var/www//info.php* (en Fedora, */var/www/html/info.php*).

```
# nano /var/www/info.php
```

El contenido del fichero incluye una sentencia para ejecutar la función *phpinfo()* que permite obtener la información sobre el módulo *php*.

```
<?php
   phpinfo();
?>
```

Así, al ejecutar el fichero en una petición HTTP el servidor lanza la sentencia y muestra el contenido solicitado, de forma dinámica. Antes de probar a ejecutar este fichero reinicie el servidor Apache:

UBUNTU

```
# service apache2 restart
```

FEDORA

```
# service httpd restart
```

Ahora sí, inicie un navegador web y escriba en la barra de direcciones *http://localhost/info.ph*p. Como puede ver en la figura 18-2, PHP se encuentra correctamente instalado. Si observa con detenimiento la información mostrada puede ver por ejemplo que trabaja a través de Apache, los módulos actualmente habilitados, etc.

Figura 18-2. PHP - Ejecución de phpinfo()

18.1.2 Configuración en Ubuntu

La configuración de Apache se almacena en el directorio de configuración */etc/apache2*. A continuación se van a ver las opciones de configuración más utilizadas para cada uno de los ficheros:

- ***/etc/apache2/ports.conf.*** Permite establecer los puertos de escucha para las comunicaciones normales (puerto 80) y las comunicaciones seguras https (puerto 443).

```
Listen *:80
Listen *:443
```

- ***/etc/apache2/apache2.conf.*** Una de las opciones más importantes es que se puede establecer el usuario y grupo al que pertenecen los procesos que ejecute el servidor:

```
User www-data
Group www-data
```

A continuación vamos a ver las tareas de administración más importantes:

18.1.2.1 Sitios

Apache almacena en la carpeta */etc/apache2/sites-available* la configuración de cada uno de los sitios web de Apache. Por defecto, se encuentran los sitios *default* y *default-ssl*. Cada sitio tiene la siguiente estructura:

```
<VirtualHost *:80>
        ServerAdmin servermaster@localhost
        # Servername www.miempresa.com # comentado en default
        DocumentRoot /var/www
        DirectoryIndex index.html default.html
</VirtualHost>
```

donde:

- *ServerrAdmin* es el correo electrónico del administrador del sitio web.
- *Servername* es el nombre FQDN del sitio web. Para el dominio *default* no se indica ningún nombre, pero para atender peticiones específicas de dominios (p. ej., *www.miempresa.com*) sí se debe establecer.
- *DocumentRoot*. Indica la ubicación donde se encuentran las páginas web del sitio.
- *DirectoryIndex*. Indica el nombre de los ficheros que envía por defecto el servidor web.

Nuevo sitio

Por defecto el servidor web publica el directorio */var/www/* para todos los dominios, pero es posible personalizar de forma independiente cada dominio. Por ejemplo, para añadir el dominio *www.miempresa.com* que se aloja en la carpeta */portales/miempresa* hay que crear el fichero */etc/apache2/sites-available/miempresa.com* con el siguiente contenido:

```
<virtualhost *:80>
    ServerName www.miempresa.com
    DocumentRoot /portales/miempresa
</virtualhost>
```

Active el sitio

```
# a2ensite miempresa.com
```

y reincie el servidor web

```
# service apache2 restart
```

Nota

Lógicamente para que el servidor web atienda un determinado dominio la entrada DNS (p. ej., www.miempresa.com) debe apuntar al servidor web.

Sitio seguro (https)

Con el auge de los negocios en Internet se ha popularizado el uso de comunicaciones cifradas entre los clientes y el servidor web, siendo la tecnología de encriptación más utilizada el Security Socket Layer (SSL).

Para poder utilizar una página segura bajo https hay que realizar los siguientes pasos:

- Active el módulo ssl:

```
a2enmod ssl
```

- Active el sitio default-ssl aunque si lo desea puede crear un nuevo sitio web:

```
# a2ensite default-ssl
```

- Reinicie el servidor web:

```
# service apache2 restart
```

Una vez finalizado el proceso, acceda a un navegador web y escriba *https://IP_Servidor* (véase la figura 18-3).

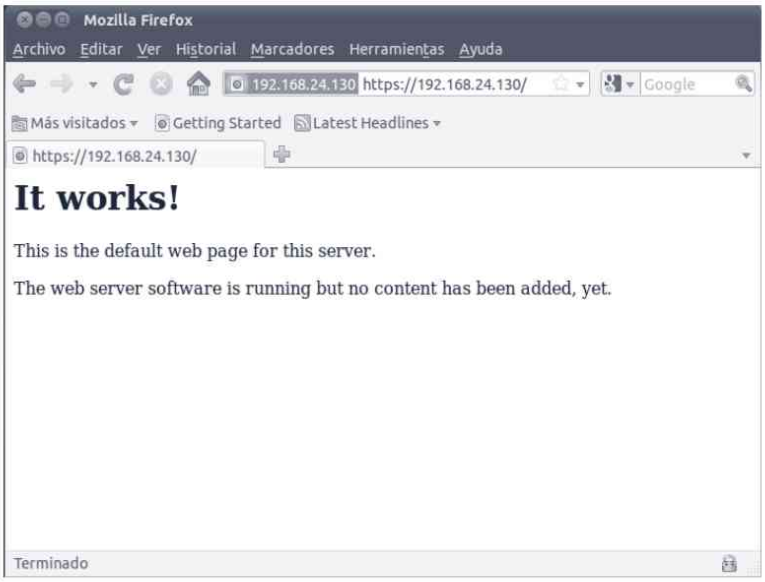


Figura 18-3. https

Nota

Puede generar su propio certificado de seguridad utilizando el comando open-ssl.

18.1.2.2 Directorios

Por defecto, la directiva *DocumentRoot* indica el directorio donde se almacenan las páginas del sitio web. Por ejemplo, en Ubuntu normalmente se publica siempre el directorio */var/www* lo que permite que el servidor web publique cualquier subdirectorio de la misma forma que se realiza en el directorio raíz.

En ocasiones resulta necesario indicar que un determinado directorio tiene unos permisos de acceso diferentes que el directorio raíz. Para ello es posible utilizar la directiva <*Directory*> para especificar los permisos de un determinado directorio.

A continuación se muestra un ejemplo básico de la utilización de dicha directiva:

```
<Directory /var/www/tienda>
    DirectoryIndex index.php
    Order allow,deny
    Allow from all
</Directory>
```

donde se indica que la web por defecto es *index.php* y que por defecto está permitido el acceso al recurso.

A continuación vamos a ver a través de unos sencillos ejemplos las opciones más utilizadas:

Hacer un directorio navegable

Cuando Apache recibe una determinada solicitud (p. ej., *www.miempresa.com/documentos/*) mira la directiva *DirectoryIndex* y sirve la página que esté establecida por defecto (normalmente, *index.htm* o *index.html*). Si lo desea, existe la posibilidad que en vez de mostrar la página por defecto muestre todo el contenido que tiene el directorio. Para configurar un directorio para que su contenido sea navegable hay que modificar el fichero de configuración y añadir el siguiente código:

```
<Directory /portales/miempresa/documentos>
        Options Indexes FollowSymLinks MultiViews
        Order allow,deny
        Allow from all
</Directory>
```

donde */portales/miempresa/documentos* es el directorio que desea que sea navegable.

Nota

Hay que tener cuidado al hacer un directorio navegable ya que los usuarios pueden ver todo su contenido. Para mejorar la seguridad puede configurar el directorio para que sea accesible por unos determinados usuarios o desde unas determinadas direcciones IP.

Restringir el acceso a usuarios auntenticados

Es posible restringir el acceso a un determinado directorio del sitio web para unos determinados usuarios. Para proteger un directorio hay que realizarlo de la siguiente forma:

```
<Directory /var/www/directorio protegido>
   AuthName "Directorio Protegido"
   AuthType Basic
   AuthUserFile /var/htpasswd
   Order  deny,allow
   require valid-user
</Directory>
```

Como puede ver en el código, la autenticación especificada es *Basic*. El fichero al que hace referencia mediante *AuthUserFile* es el que contiene los usuarios y contraseñas con acceso al directorio. Para generar este fichero se utiliza la utilidad *htpasswd*:

```
# htpasswd -c /var/htpasswd usuario
New password:
Re-type new password:
Adding password for user usuario
```

donde la opción *–c* permite crear el fichero de contraseñas en blanco y *usuario* es el nombre de usuario que se va a crear.

Restringir el acceso mediante direcciones IP

Apache permite restringir o permitir el acceso a un directorio a una determinada dirección de red. Por ejemplo, si desea restringir el acceso al directorio *protegido* de nuestra Intranet para permitir solamente la red 10.0.0.0/24 se incluye la siguiente directiva:

```
<Directory /var/www/intranet>
   Order Deny,Allow
   Deny from all
   Allow from 10.0.0.0/24
</Directory>
```

Si quiere permitir que un solo equipo acceda al sitio web escriba su dirección IP o nombre de host de la siguiente forma:

```
<Directory /var/www/intranet >
   Order Deny,Allow
   Deny from all
   Allow from 127.0.0.1
</Directory>
```

Redirección de URL

Cuando un cliente emite la solicitud de una página, lo que recibe como respuesta es una página HTML almacenada en el sistema de archivos del servidor bajo el directorio que marca la directiva *DocumentRoot*.

Si desea modificar este comportamiento de tal forma que, ante una petición, la página HTML servida resida en otro directorio del sistema de archivos del servidor o, incluso, en otro servidor diferente, debe configurar apropiadamente las directivas *Alias* (para la primera opción) y *Redirect* (para la segunda).

Con la directiva *Alias* puede conseguir que ante un requerimiento de un cliente la petición se redirija a otra página situada, incluso, fuera del directorio marcado por *DocumentRoot*.

```
Alias   /deseo/   /otro/directorio/
```

Con el ejemplo de configuración anterior, cuando un servidor reciba la URL *http://www.miempresa.com/deseo/mipagina.html*, el archivo que se devuelve es *http://www.miempresa.com/otro/directorio/mipagina.html*.

Cuando se redirecciona a directorios fuera del ámbito marcado por la directiva *DocumentRoot* se debe tener en cuenta que, por defecto, Apache está configurado para denegarlo y, por tanto, se debe añadir la siguiente directiva que permita el acceso al directorio */otro/directorio*:

```
<Directory   /otro/directorio>
    orden allow, deny
    allow from all
</directory>
```

Con la directiva *Redirect* se redirecciona la petición a otro servidor externo:

```
Redirect    /otro_sitio   http://www.otro.sitio.es
```

Con esta configuración, con la URL *http://www.miempresa.com/otro_sitio* el servidor web nos redirecciona al servidor *http://www.otro.sitio.es*.

18.1.3 Configuración en Fedora

La configuración de Fedora es práctica igual que Ubuntu salvo los siguientes detalles:

- En Fedora toda la configuración del servidor web, sitios web y directorios se encuentra en el fichero de configuración */etc/httpd/conf/httpd.conf*.
- Si desea utilizar varios sitios web en el mismo servidor de apache es necesario activar la siguiente variable en el fichero de configuración de Apache.

```
NameVirtualHost *:80
```

- En Fedora, el servidor se llama *httpd*, por lo que si desea reiniciar el servidor debe ejecutar el siguiente comando:

```
# service httpd restart
```

18.1.4 Arranque y parada del servidor

Para iniciar y parar el servidor web puede utilizar el comando *service* de forma que si quiere iniciar el servicio ejecute:

```
# service apache2 start
```

Además, puede parar el servicio (*stop*), reiniciarlo (*restart*) o volver a cargar la configuración (*reload*).

Datos más importantes

Nombre del servicio:	*apache2 (Ubuntu)* *httpd (Fedora)*
Fichero de configuración:	*/etc/httpd/conf/httpd.conf*
Directorio web:	*/var/www (Ubuntu)* */var/www/html (Fedora)*
Comandos más utilizados:	*htpasswd*
Puertos:	*80/tcp y 443/tcp*

18.2 SERVIDOR FTP

18.2.1 Instalación

Vsftpd (Very Secure FTP) es un servidor FTP muy pequeño y seguro. Para instalar el servidor FTP en el sistema debe instalar el paquete *vsftpd* (*Demonio FTP muy seguro*). Puede realizar la instalación a través de la línea de comandos o a través de *synaptic* (Ubuntu) o *Añadir/quitar software* (Fedora).

UBUNTU

```
# apt-get install vsfttpd
```

FEDORA

```
# yum install vsftpd
```

Una vez instalado el paquete debe iniciar el servicio ejecutando:

```
# service vsftpd start
```

Para comprobar que el servidor está funcionando correctamente puede conectarse al servidor:

```
$ ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.3.0)
Name (localhost:root): usuario
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV
150 Here comes the directory listing.
-rw-r--r--  1   1003   1003   179 Mar 15 18:00 examples.desktop
226 Directory send OK.
ftp> quit
221 Goodbye.
```

Nota

Si el servidor está correctamente instalado, pero no permite el acceso desde el exterior, es muy posible que no tenga el router configurado para dejar pasar el tráfico del servidor FTP.

18.2.2 Configuración

El fichero de configuración del servidor *vsftpd* en Ubuntu es */etc/vsftpd.conf* y en Fedora es */etc/vsftpd/vsftpd.conf*. Este archivo va a determinar cómo va a operar el servidor FTP. En la tabla 11-1 se detallan las opciones de configuración más importantes.

Las dos últimas opciones se utilizan para permitir o denegar el acceso a los usuarios en el sistema. Cuando la opción *userlist_enable=YES* los archivos funcionan como una lista de usuarios que están autorizados a conectarse al servidor FTP. Sin embargo, cuando se combina con la opción *userlist_deny=YES* estos archivos funcionan como una lista de usuarios que no están autorizados a conectarse al servidor FTP. Cuando utiliza la opción *userlist_deny* la naturaleza de la denegación de servicio FTP es diferente dependiendo del fichero en donde se encuentre.

18.2.3 Seguridad

Para mejorar la seguridad del servidor es recomendable limitar el uso del servidor en modo escritura solo para los usuarios autenticados y en el caso de permitir conexiones anónimas solo se permitirá el acceso en modo lectura. Para ello active el parámetro *anonymous_enable=YES* y *write_enable=NO.*

Tabla 11-1. Parámetros de configuración del fichero /etc/vsftpd/vsftpd.conf

Parámetros	Descripción
anonymous_enable=NO/YES	Activa o desactiva el acceso FTP anónimo.
local_enable=NO/YES	Permite que los usuarios se conecten de forma local.
write_enable=YES	Permite la escritura en el servidor.
xferlog_enable=YES	Registra en fichero (log) el tráfico de bajada y subida.
xferlog_std_format=YES	Establece el formato estándar para el fichero de registro.
Idle_session_timeout=600	Estable el tiempo máximo de inactividad de una sesión.
data_connection_timeout=120	Establece el tiempo máximo de inactividad en una transferencia de datos.
pam_service_name=vsftpd	Establece el nombre del servidor FTP.
ftpd_banner = Mensaje de bienvenida	Permite establecer un mensaje de bienvenida.
chroot_locar_user=NO/YES	Permite enjaular a los usuarios en su directorio home.
ftpd_banner=Bienvenido	Permite establecer el texto de bienvenida de los usuarios
userlist_enable=NO/YES	Indica a vsftpd que utilice los archivos *vsftpd.ftpusers* y vsftpd.user_list para permitir el acceso a los usuarios.
userlist_deny=NO/YES	Indica a vsftpd que utilice los archivos *vsftpd.ftpusers* y vsftpd.user_list para denegar el acceso a los usuarios.

Si decide activar la escritura tome las siguientes medidas:

- Registre toda la actividad del servidor. Para ello active el parámetro *Xferlog_enable=YES.*
- Establezca las listas de usuarios permitidos activando las opciones *userlist_enable* y *userlist_deny.*
- Enjaule a los usuarios en su directorio home a través de la opción *chroot_local_user=YES.*
- Active los tiempos de espera para evitar los ataques de denegación de servicios. Existen dos tiempos de espera: el tiempo de espera máximo de una sesión (definido por el parámetro *idle_session_timeout=600*) y el tiempo de espera máximo en una transferencia de datos (*data_connection_timeout=120*).

Nota

Nunca configure el servidor FTP para permitir el acceso anónimo y permita la escritura sin enjaular los usuarios del sistema.

Datos más importantes

Nombre del servicio:	*vsftpd*
Fichero de configuración:	*/etc/vsftpd.conf (Ubuntu)* */etc/vsftpd/vsftpd.conf (Fedora)*
Puerto utilizado:	*21/tcp*

18.3 SERVIDOR DE CORREO ELECTRÓNICO

18.3.1 Servidor de correo electrónico Postfix

Normalmente el servidor de correo electrónico que se instala por defecto en los sistemas GNU/Linux es *sendmail.* A continuación se va a realizar la instalación y configuración de *Postfix* porque es mucho más versátil, fácil de instalar y configurar.

Postfix (http://www.postfix.org/) es un agente de transporte de correo (MTA) de software libre que permite el enrutamiento y envío de correos electrónicos. Postfix fue desarrollado por IBM con el objetivo de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado *Sendmail*.

18.3.1.1 Instalación en Ubuntu

Para instalar el servidor de correo electrónico *Postfix* debe ejecutar:

```
# apt-get install postfix
```

Una vez realizada la instalación se inicia un asistente que le ayuda a configurar el servidor de correo (véase la figura 18-4) donde debe indicar el tipo de servicio que desea instalar (normalmente *Sitio de Internet*) e indique el nombre FQDN del sitio de Internet (p.ej., *miempresa.com*).

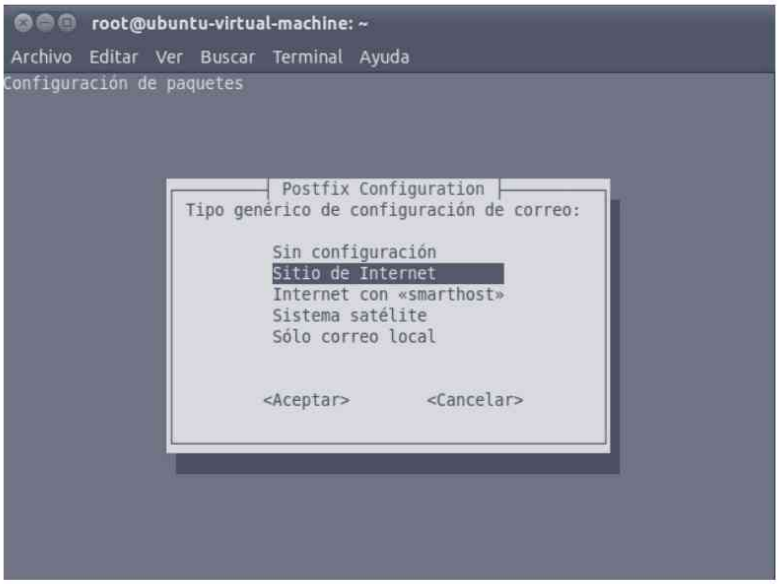


Figura 18-4. Instalación de Postfix en Ubuntu

18.3.1.2 Instalación en Fedora

Para instalar el servidor de correo electrónico *Postfix* debe instalar los paquetes *postfix*, *dovecot* y *system-switch-mail*. Para realizar la instalación ejecute:

```
# yum install postfix dovecot system-switch-mail
```

Una vez realizada la instalación debe indicarle al sistema quién es el servidor de correo electrónico por defecto. Para ello ejecute la herramienta *system-switch-mail* en la línea de comandos (véase la figura 18-5), seleccione el servidor de correo *Postfix* y pulse el botón de *Aceptar*.

Figura 18-5. system-switch-mail-nox

18.3.1.3 Inicio

Después de la instalación, puede iniciar el servicio ejecutando:

```
# service postfix start
```

o a través de la herramienta gráfica de administración de servicios.

Una vez iniciado *Postfix* puede comprobar que está funcionando correctamente examinando los ficheros de registro (*/var/log/maillog*, */var/log/mail.err* y */var/log/mail.warn*).

Cuando *Postfix* se inicia correctamente en el fichero */var/log/maillog* genera los siguientes mensajes:

```
Aug 26 10:50:49 localhost postfix/postfix-script[6305]:
starting the Postfix mail system
Aug 26 10:50:49 localhost postfix/master[6306]: fatal: bind
127.0.0.1 port 25: Address already in use
Aug 26 10:55:53 localhost postfix/postfix-script[6928]:
starting the Postfix mail system
Aug 26 10:55:53 localhost postfix/master[6930]: daemon started
-- version 2.7.0, configuration /etc/postfix
```

18.3.1.4 Configuración

Los ficheros de configuración de *Postfix* se encuentran en el directorio */etc/postfix.* Los ficheros más importantes de configuración son:

- **main.cf.** Contiene las opciones generales de configuración del servidor de correo.
- **master.cf.** Controla cómo se conectan los clientes al servidor y cómo están configurados los servicios para que el servidor funcione correctamente. Las opciones más importares del fichero de configuración *main.cf* son:
  - **Directorios de trabajo.** En los directorios de trabajo indique el directorio donde se almacenan los mensajes (*queue_directory*), donde se encuentran los comandos de root (*command_directory*), el servidor (*daemon_directory*) y dónde se guardan los datos del servidor (*data_directory*).

    ```
    queue directory = /var/spool/postfix
    command directory = /usr/sbin
    daemon directory = /usr/libexec/postfix
    data_directory = /var/lib/postfix
    ```

  - **mydestination.** Permite indicar qué dominios debe utilizar para administrar el correo. Por ejemplo, si desea gestionar el dominio *miempresa.com* escriba:

    ```
    mydestination= miempresa.com, localhost.localdomain,
    localhost
    ```

- **inet_interfaces.** Indica las interfaces por donde el servidor recibe los correos electrónicos.

```
inet_interfaces = eth0
```

  Para recibir los correos por cualquier interfaz de red escriba:

```
inet_interfaces = all
```

- **mynetworks.** Permite indicar nuestra dirección de red local.

```
mynetworks = 127.0.0.0/8, 10.0.0.0/24
```

En el archivo *master.cf* puede ver una lista estructurada de los dominios, servicios y procesos que pueden activarse y configurarse en *Postfix.* A continuación, a modo de ejemplo, puede ver las líneas referentes al proceso *smtp*.

```
#
==========================================================================
#service type private unpriv chroot wakeup  maxproc command + args
#              (yes)   (yes)   (yes)   (never)   (100)
#
==========================================================================
smtp      inet  n       -       n       -       -       smtpd
```

En este caso, el servicio *smtp* es el servicio SMTP básico que recibe correos por el puerto 25/tcp.

Nota

En http://postfix.wiki.xs4all.nl/ puede encontrar más información sobre la configuración de Postfix.

Existen varias formas de configurar *Postfix*, mediante un editor de textos (p. ej., *nano*), mediante el comando *postconf* o mediante Webmin (véase la figura 18-6).

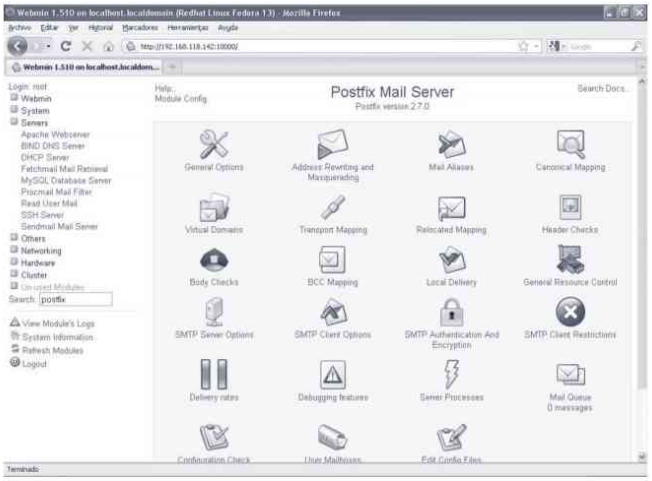


Figura 18-6. Configuración de Postfix con Webmin

Una vez configurado reinicie el servidor ejecutando:

```
# service postfix restart
```

18.3.1.5 Seguridad

Para evitar que nuestro servidor de correo electrónico se utilice de forma indebida es recomendable configurar el servidor para que lo utilicen los usuarios autorizados y evitar el correo span.

Listas de bloqueo basadas en DNS

Las listas de bloqueo son unas listas de servidores que supuestamente envían spam. Al configurar *Postfix* para que use estas listas significa que cada vez que llega un correo al servidor, *Postfix* comprueba que la IP del servidor que envía el mensaje no se encuentra en esas listas.

A continuación puede ver un ejemplo de lista de bloqueo que se especifica en el fichero *main.cf:*

```
maps rbl domains =
        relays.ordb.org
        list.dsbl.org
        blackholes.mail-abuse.org
        dialups.mail-abuse.org
        relays.mail-abuse.org

smtpd client restrictions =
        permit mynetworks
        reject_maps_rbl
        check_relay_domains
```

Nota

En http://www.declude.com/JunkMail/Support/ip4r.htm puede obtener un completo listado de bloqueo.

Control de envíos

Para indicar a *Postfix* los equipos o redes que pueden enviar correos a través del servidor se utiliza la directiva *mynetworks.* Por ejemplo, a continuación se indica que la red interna 10.0.0.0/24 puede enviar correos:

```
mynetworks = 127.0.0.0/8, 10.0.0.0/24
```

18.3.2 Simple SMTP

SSMTP (*Simple SMTP*) es un servidor ligero de correo electrónico, muy útil, que permite retransmitir los correos a otra cuenta de correo en otro servidor. Por ejemplo, puede utilizar *ssmtp* para reenviar todos los correos del servidor a otro servidor (p. ej., *gmail*).

Para realizar la instalación hay que realizar los siguientes pasos:

- Instale el servidor:

UBUNTU

```
# apt-get install ssmtp
```

FEDORA

```
# yum install ssmtp
```

- Edite el fichero */etc/ssmtp/ssmtp.conf* con el siguiente contenido:

```
root=usuario@gmail.com
mailhub=smtp.gmail.com:587
rewriteDomain=
hostname=usuario@gmail.com
UseSTARTTLS=YES
AuthUser=usuario
AuthPass=tu password
FromLineOverride=YES
```

- Deshabilite *sendmail* ejecutando:

```
service sendmail stop
chkconfig sendmail off
```

- y finalmente, cambie *sendmail* por *ssmtp*:

```
# mv /usr/sbin/sendmail /usr/sbin/sendmail backup
# ln -s /usr/sbin/ssmtp /usr/sbin/sendmail
```

Capítulo 19

LDAP

19.1 INTRODUCCIÓN

LDAP (*Lightweight Directory Access Protocol*) es un protocolo de aplicación que permite el acceso a un servicio de directorio (dominio). Los directorios con los que trabaja LDAP son de propósito general aunque se suele utilizar para almacenar información referente a organizaciones, usuarios, redes, etc.

Los servidores LDAP utilizan sistemas de bases de datos como *backend* donde almacenar y gestionar las entradas del directorio. Se puede dividir el árbol de directorios en subárboles de tal manera que cada servidor LDAP controla un subárbol por los siguientes casos:

- **Rendimiento.** Al distribuir el directorio entre varios servidores se distribuye la carga individual de cada uno de ellos y, por lo tanto, se obtiene un mayor rendimiento global.
- **Localización geográfica.** Cada servidor puede dar servicio a una zona geográfica diferente.
- **Cuestiones administrativas.** Cada servidor es gestionado por administradores diferentes.

En LDAP se pueden distinguir cuatro modelos que representan los servicios que proporciona un servidor LDAP vistos por el cliente.

- El **modelo de información** establece la estructura y los tipos de datos que tiene el directorio: esquemas, entradas, atributos, etc. Según este modelo un directorio está formado por entradas estructuradas en forma de árbol.

Cada entrada estará definida por un conjunto de atributos y cada atributo está compuesto por un nombre y su valor.

- El **modelo de asignación** de nombres define cómo referenciar de forma única las entradas y los datos en el árbol de directorios. Cada entrada tendrá un identificador único llamado DN (*Distinguished Name*). El DN se construye a partir de un RDN (*Relative Distinguished Name*) que se compone de varios atributos de la entrada, seguido de los DN de sus ancestros.
- El **modelo funcional** establece las operaciones para acceder al árbol de directorio: autenticación, solicitudes y actualizaciones.
- Por último el **modelo de seguridad** establece los mecanismos que garantizan para el cliente cómo probar su identidad (autenticación) y para el servidor cómo controlar el acceso (autorización).

19.2 OPENLDAP

OpenLDAP es una implementación de código abierto de LDAP desarrollada por OpenLDAP Project. Las características más destacadas de OpenLDAP son:

- Se distribuye bajo licencia libre.
- Es multiplataforma.
- Tiene una buena integración con multitud de aplicaciones, principalmente en el mundo Linux.
- Soporta IPv6 y LDAPv3.
- Soporte de *Referrals* (esquema distribuido).
- Permite operaciones de publicación de esquemas antes de realizar búsquedas.
- Internacionalización mediante caracteres UTF-8 y atributos de lenguaje.
- Soporta multitud de bases de datos como almacén de datos.
- Soporta extensiones en el protocolo (modificación y creación de nuevas operaciones).
- Contiene un esquema de mapeo entre Radius y OpenLDAP.
- Tiene mecanismos avanzados de búsqueda.

OpenLDAP se puede descargar de la página web oficial, *http://www.openldap.org/*. Los principales componentes de OpenLDAP son:

- **slapd.** El servidor (demonio) principal de LDAP
- **slurpd.** El servidor de replicación de LDAP. Permite sincronizar varias réplicas de un servidor LDAP.
- El conjunto de librerías que implementa el protocolo LDAP.
- Un conjunto de herramientas, utilidades y clientes de ejemplo (*http://asg.web.cmu.edu/sasl/sasl-library.html*).

19.2.1 Instalación

Para instalar OpenLDAP debe disponer de los paquetes *slapd* y *ldap-utils*, el demonio servidor del directorio activo y las utilidades para la administración de LDAP, respectivamente. Por defecto, se configura *slapd* con un conjunto de opciones mínimas que garantizan el correcto funcionamiento del servidor. Sin embargo, es importante tener en cuenta que la mayoría de aplicaciones y scripts requieren la carga de *schemas* específicos o configuración adicional.

Puede instalar *openladap* a través del gestor de paquetes o utilizando directamente el terminal ejecutando:

UBUNTU

```
# apt-get install slapd ldap-utils
```

FEDORA

```
# yum install openldap-servers openldap-clients
openldap-devel
```

A continuación se va a realizar la configuración básica de *OpenLDAP* (sus dos lados fundamentales –*Backend* y *Frontend*–) así como empezar a poblar el *Frontend* con información.

19.2.2 Configuración

Una vez instalado *OpenLDAP* es importante observar que en el directorio */etc/ldap/* (en Fedora, */etc/openldap*) se encuentran disponibles los ficheros de configuración del directorio activo así como los diferentes *schemas* y otra información aplicable al funcionamiento y dinámica del mismo.

También es importante recordar que puede iniciar, detener, o reiniciar el servicio, de la siguiente forma:

```
# service slapd start | stop | restart
```

A continuación se va a configurar tanto del *Backend* (parte que implica las directivas para dinámicamente configurar el demonio servidor *slapd* y las opciones para poblar con información el directorio -*Frontend*) como del *Frontend* de OpenLDAP, desarrollando al mismo tiempo un ejemplo que permita conocer de forma sencilla en qué consiste.

19.2.2.1 Creación del dominio: configuración del Backend

Toda la información en el directorio activo se almacena con estructura de árbol. Gracias a OpenLDAP dispone de libertad total para implementar el *Árbol de información del directorio* o *DIT* (*Directory Information Tree*). En la configuración básica que se va a presentar a continuación se crean dos nodos bajo la raíz del árbol: usuarios (para almacenar usuarios del dominio) y grupos (para almacenar grupos de usuarios).

Lo primero que debe hacer es determinar la raíz del árbol para el directorio LDAP, normalmente el FQDN (*Fully Qualified Domain Name*) del dominio. Por ejemplo, para el dominio miempresa.com, el nodo raíz es *dc=miempresa,dc=com*.

OpenLDAP utiliza un directorio independiente que almacena el DIT *cn=config*, que permite determinar de forma dinámica el comportamiento del servidor *slapd*, lo que permite realizar modificaciones en las definiciones de los esquemas, índices, listas de control de acceso… sin la necesidad de detener el servicio. Este directorio *backend* inicialmente dispone de una configuración mínima, por lo que es necesario ampliar su funcionalidad con opciones, módulos, esquemas… adicionales para sentar la base para la población del directorio con información (*frontend*) –así, para determinadas aplicaciones, lo recomendable es consultar la documentación específica de las mismas. A continuación se va poblar el directorio con usuarios y grupos de usuarios, en un formato compatible con aplicaciones de libretas de direcciones o cuentas Unix Posix. Este tipo de cuentas permiten a varias aplicaciones implementar autenticación, tales como aplicaciones Web, agentes de correo electrónico, y otras.

Por tanto, se realiza la carga de los ficheros *schema* para la estructura del directorio, disponibles en este caso en el directorio creado en la instalación de OpenLDAP */etc/ldap/schema/*, ejecutando los siguientes comandos como *root*:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/ldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/ldap/schema/inetorgperson.ldif
```

FEDORA

Los schemas se encuentran en el directorio /etc/openldap/schema/.

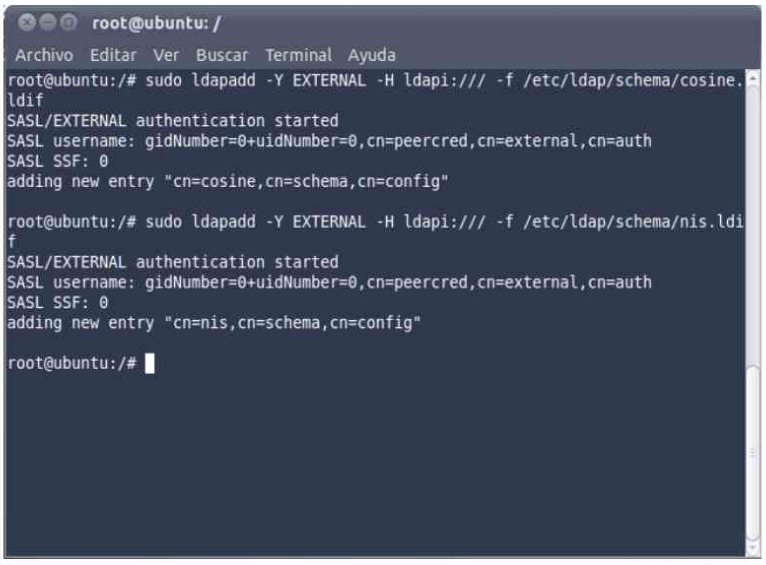


Figura 19-1. Carga de ficheros schema

Una vez añadidos los esquemas a LDAP debe crear el fichero LDIF de configuración para la carga dinámica de los módulos en el *backend* y la base de datos para el directorio. A continuación puede ver un ejemplo de este fichero, en el que es fundamental especificar el directorio con la ubicación para los módulos así como el sufijo de nuestro dominio, identificador y contraseña para el usuario privilegiado o la ubicación y permisos de acceso para la base de datos:

Listado 1. Ejemplo de fichero LDIF para la configuración del backend: backend.miempresa.com.ldif

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=miempresa,dc=com
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=miempresa,dc=com
olcRootPW: hola00==
```

```
olcDbConfig: set cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set lk max locks 1500
olcDbConfig: set lk max lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by
dn="cn=admin,dc=miempresa,dc=com" write by anonymous auth by self
write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=miempresa,dc=com" write by *
read
```

Nota

Las opciones especificadas en el fichero de configuración del backend y su sintaxis dependen del tipo de base de datos utilizada para el mismo. En el ejemplo anterior se trata de una base de datos BDB, aunque otros tipos pueden instanciarse, como por ejemplo LBDM. De esta forma recomendamos la consulta de la documentación OpenLDAP para su correcta configuración cuando necesitemos escenarios más complejos.

Una vez creado el fichero LDIF debe cargarlo en el directorio, haciéndolo de forma similar al caso de los *schemas* necesarios:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f backend.miempresa.com.ldif
```

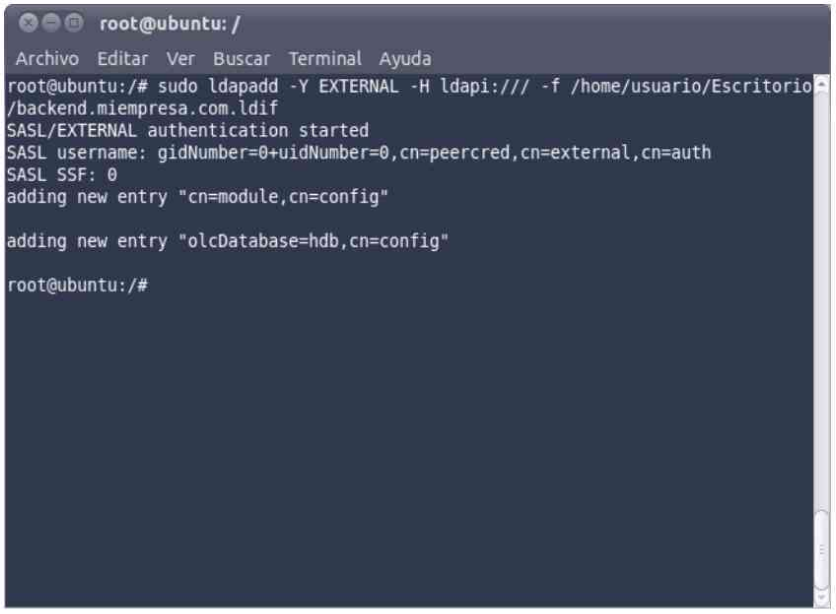


Figura 19-2. Carga del fichero LDIF para la configuración del backend

Como puede observar en la figura 19-2, se han creado con éxito dos entradas; una para la carga dinámica de módulos en el directorio y otra para la base de datos. Desde este momento es posible comenzar a poblar el directorio *frontend* con información.

19.2.2.2 Poblar el directorio: configuración del frontend

Una vez que dispone, al menos, de una configuración mínima del comportamiento del proceso servidor puede comenzar a poblar el *frontend* de OpenLDAP con información, atendiendo a los *schemas* utilizados para almacenar la misma. Para ello hay que crear un fichero LDIF en el que se añaden los diferentes nodos que desea registrar en el árbol del directorio activo.

Como puede ver en el siguiente ejemplo, se crea el objeto de primer nivel del dominio (*dc=miempresa,dc=com*), unidades organizacionales para usuarios y grupos, y un ejemplo de usuario y grupo de usuarios especificando, fundamentalmente, identificadores, clases de objeto y atributos correspondientes a cada caso.

Listado 2. Ejemplo de fichero LDIF para la población del frontend: frontend.miempresa.com.ldif

```
# Creamos el objeto del nivel superior del dominio
dn: dc=miempresa,dc=com
objectClass: top
objectClass: dcObject
objectclass: organization
o: Ejemplo de Organizacion
dc: miempresa
description: LDAP Ejemplo

# Usuario Administrador (admin)
dn: cn=admin,dc=miempresa,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: hola00==

# Unidad Organizacional usuarios
dn: ou=usuarios,dc=miempresa,dc=com
objectClass: organizationalUnit
ou: usuarios

# Unidad Organizacional grupos
dn: ou=grupos,dc=miempresa,dc=com
objectClass: organizationalUnit
ou: grupos

# Usuario Juan López
dn: uid=juan,ou=usuarios,dc=miempresa,dc=com
```

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: juan
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory: /home/juan
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@miempresa.com
postalCode: 31000
l: Almeria
o: Ejemplo
mobile: +34 (0)6 xx xx xx xx
homePhone: +34 (0)5 xx xx xx xx
title: Administrador del Sistema
postalAddress:
initials: JL

# Grupo Ejemplo
dn: cn=ejemplo,ou=grupos,dc=miempresa,dc=com
objectClass: posixGroup
cn: ejemplo
gidNumber: 10000
```

Se realiza la carga de las entradas en el directorio LDAP ejecutando:

```
# ldapadd -x -D cn=admin,dc=miempresa,dc=com -W -f
frontend.miempresa.com.ldif
```

En la figura 19-3 se puede ver el resultado de aplicar dichos cambios.

Como se puede apreciar, para realizar la carga de nuevas entradas en el directorio LDAP es necesario introducir la contraseña del usuario administrador LDAP. Si quiere comprobar que las entradas han sido añadidas correctamente puede consultar el contenido del directorio LDAP con la utilidad *ldapsearch* de la siguiente forma:

```
# ldapsearch -xLLL -b "dc=miempresa,dc=com" uid=juan sn givenName
cn
```

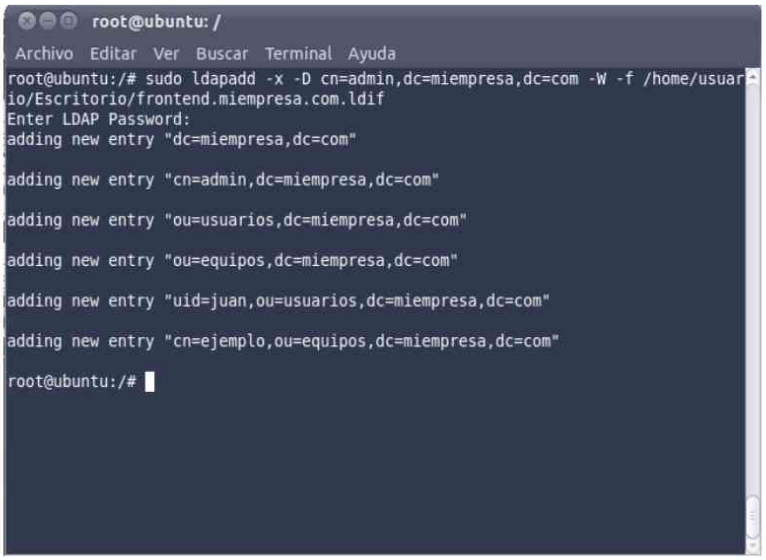


Figura 19-3. Carga del fichero LDIF para la población del frontend

En la figura 19-4 puede ver cómo efectivamente la ejecución del comando de búsqueda devuelve la información solicitada (*sn, givenName, cn*) para el usuario con *uid=juan*.

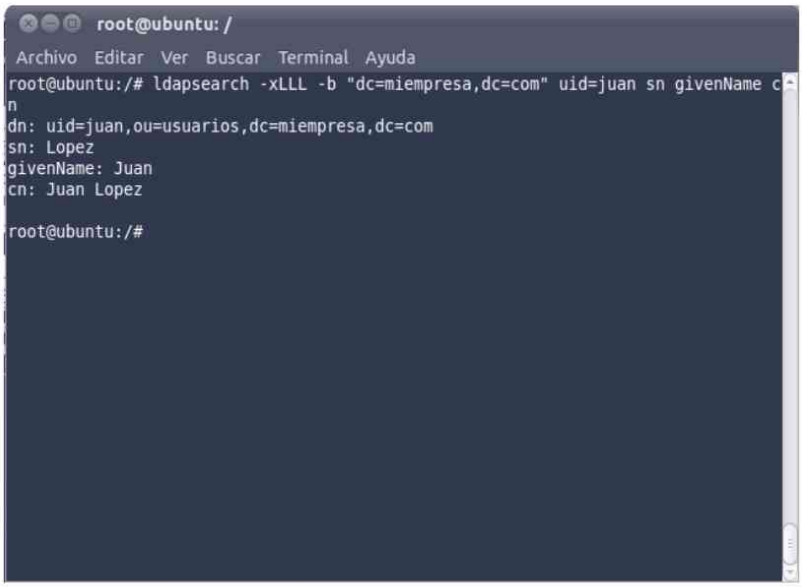


Figura 19-4. Ejemplo de utilización de ldapsearch

En ella se han incluido parámetros para no utilizar autenticación simple SASL (*Simple Authentication Security Layer*), ya que es aplicada de forma predeterminada (*-x*) y para deshabilitar la muestra de información sobre el *schema* LDIF (*-LLL*).

En ocasiones, y como resulta en este caso, para llevar a cabo operaciones sobre el directorio activo resulta más cómodo o incluso eficiente trabajar con alguna aplicación o herramienta que ofrezca una interfaz gráfica para el acceso al mismo.

Datos más importantes

Nombre del servicio:	*slapd*
Fichero de configuración:	*/etc/ldap/ldap.conf (Ubuntu)* */etc/ldap.conf (Fedora)*
Directorio de configuración:	*/etc/ldap/ (Ubuntu)* */etc/openldap (Fedora)*
Comandos más utilizados:	*ldapadd, ldapsearch ldapmodify, ldapdelete, slapadd, slapcat, slapindex y slappaswd.*
Puertos utilizados:	*389/TCP*

19.3 HERRAMIENTAS Y UTILIDADES

OpenLDAP tiene dos tipos de utilidades. Por un lado están las denominadas *herramientas de cliente* que permiten modificar, borrar, añadir entradas en el servidor LDAP de una forma remota. Para usar dichas herramientas debe estar activo el servidor LDAP. El otro conjunto de herramientas trabajan sobre la base de datos o *backend* directamente por lo que no necesitan que *slapd* esté ejecutándose. Estas son más útiles cuando se producen inconsistencias en la base de datos porque varias personas han actuado sobre el servidor LDAP. A continuación se describen las principales herramientas existentes en cada uno de los grupos con sus opciones más características.

19.3.1 Herramientas de cliente

A continuación se describen algunas de las denominadas *herramientas de cliente* que permiten modificar, borrar, añadir entradas en el servidor LDAP de una forma remota. Para usar dichas herramientas debe estar activo el servidor LDAP.

- **ldapmodify.** Permite modificar entradas de un directorio LDAP aceptando la introducción de datos a través de un fichero o de la línea de comandos si no se especifica. Sintaxis:

```
# ldapmodify [-a] [-r] [-n] [-w passwd] [-H ldapuri] [-D
binddn] [-p ldapport] [-f file]
```

  donde *-a* añade nuevas entradas; *-r* remplaza los valores existentes; *-n* simula la operación pero no realiza el cambio; *-f* lee la entrada del fichero LDIF especificado; *-H* especifica la URI del servidor LDAP; y *-D* utiliza el *dn* que permite realizar la operación.

En ocasiones, y como resulta en este caso, para llevar a cabo operaciones sobre el directorio activo resulta más cómodo o incluso eficiente trabajar con alguna aplicación o herramienta que ofrezca una interfaz gráfica para el acceso al mismo.

Datos más importantes

Nombre del servicio:	*slapd*
Fichero de configuración:	*/etc/ldap/ldap.conf (Ubuntu)* */etc/ldap.conf (Fedora)*
Directorio de configuración:	*/etc/ldap/ (Ubuntu)* */etc/openldap (Fedora)*
Comandos más utilizados:	*ldapadd, ldapsearch ldapmodify, ldapdelete, slapadd, slapcat, slapindex y slappaswd.*
Puertos utilizados:	*389/TCP*

19.3 HERRAMIENTAS Y UTILIDADES

OpenLDAP tiene dos tipos de utilidades. Por un lado están las denominadas *herramientas de cliente* que permiten modificar, borrar, añadir entradas en el servidor LDAP de una forma remota. Para usar dichas herramientas debe estar activo el servidor LDAP. El otro conjunto de herramientas trabajan sobre la base de datos o *backend* directamente por lo que no necesitan que *slapd* esté ejecutándose. Estas son más útiles cuando se producen inconsistencias en la base de datos porque varias personas han actuado sobre el servidor LDAP. A continuación se describen las principales herramientas existentes en cada uno de los grupos con sus opciones más características.

19.3.1 Herramientas de cliente

A continuación se describen algunas de las denominadas *herramientas de cliente* que permiten modificar, borrar, añadir entradas en el servidor LDAP de una forma remota. Para usar dichas herramientas debe estar activo el servidor LDAP.

- **ldapmodify.** Permite modificar entradas de un directorio LDAP aceptando la introducción de datos a través de un fichero o de la línea de comandos si no se especifica. Sintaxis:

```
# ldapmodify [-a] [-r] [-n] [-w passwd] [-H ldapuri] [-D
binddn] [-p ldapport] [-f file]
```

  donde *-a* añade nuevas entradas; *-r* remplaza los valores existentes; *-n* simula la operación pero no realiza el cambio; *-f* lee la entrada del fichero LDIF especificado; *-H* especifica la URI del servidor LDAP; y *-D* utiliza el *dn* que permite realizar la operación.

El fichero debe tener como primera línea el *dn* sobre el que se trabaja. A continuación aparece el atributo *changetype* con el valor *add*, *delete*, *modify* o *modrdn* según lo que se quiera hacer.

Ejemplos de *ldapmodify*:

```
dn : cn=Alex Garcia Perez, ou=usuarios, dc=miempresa,dc=com
changetype : modify
replace : sn
sn : Lopez Alegria
-
add : title
titl e: Grand Poobah
-
add: postalCode
postalCode : 04120
-
delete : street
-
```

- **ldapadd.** Añade entradas al directorio aceptando dichos datos a través de un fichero LDIF o de la línea de comando. En realidad, se trata de un enlace fijo a *ldapmodify –a*. La sintaxis y opciones son las mismas que *ldapmodify*.

- **ldapsearch.** Permite buscar entradas en el directorio LDAP. Su sintaxis es:

```
# ldapsearch [opciones] filtro [atributos]
```

Las posibles opciones del comando son: *-b base* indica el punto base de la búsqueda; *-f fichero* lee la entrada de búsqueda del fichero especificado; *-H ldapuri* especifica la URI del servidor LDAP; y *-D dn* utiliza el *dn* que permite realizar la operación.

Con *filtro* establece los patrones que tienen que cumplir los registros a buscar (se permiten los comodines) y en *atributos* se indica opcionalmente los atributos que se muestran de los registros encontrados.

Por ejemplo, a continuación se muestran todas las entradas del directorio *miempresa.com.*

```
ldapsearch -b "dc=miempresa,dc=com" "objectclass=*"
```

O las entradas de tipo persona del directorio:

```
# ldapsearch -b "dc=miempresa,dc=com" "objectclass=person" sn
```

- **ldapdelete.** Permite eliminar entradas del directorio mediante un fichero o desde línea de comando. Donde *-f fichero* permite leer la entrada del fichero LDIF especificado; *-H ldapuri* especifica la URI del servidor LDAP y *-D dn* utiliza el *dn* que permite realizar la operación.

A continuación, a modo de ejemplo, se va a borrar la entrada de *Juan Perez Garcia.*

```
# ldapdelete –D "cn=root,dc=miempresa,dc=com"
> cn=Juan Perez Garcia, ou=usuarios, dc=miempresa,dc=com
```

19.3.2 Configuración del servidor

Las herramientas para la manipulación de bases de datos o *backends* son las siguientes:

- **slapadd.** Permite añadir entradas desde un fichero LDIF a una base de datos *SLAPD*. Actúa sobre la base de datos indicada y le añade las entradas descritas en el LDIF. Si no se especifica un fichero LDIF la información se lee de la entrada estándar.

Listado 3. Creación de entradas básicas para miempresa.com

```
 # cat /tmp/top.ldif

## Construye el nodo raíz
dn: dc=miempresa,dc=com
dc: dtic
objectclass: dcObject
objectclass: organizationalUnit
ou: Dtic Dot Ua Dot Es

## Construye el ou profesores
dn: ou=profesores,dc=miempresa,dc=com
ou: profesores
objectclass: organizationalUnit

 # slapadd –v –l /tmp/top.ldif
added: "dc=miempresa,dc=com"
added: "ou=profesores,dc=miempresa,dc=com"
```

Sintaxis:

```
# slapadd [-l <inputfile>] [-f <slapdconfigfile>] [-d
<debuglevel>] [-n <integer>|-b <suffix>]
```

donde *-d* indica el nivel de depuración; *-n* indica qué base de datos se modifica en función de un número que indica la posición (primera, segunda, tercera,…) en el fichero de configuración; *-b* indica qué base de datos se modifica en función del sufijo de la misma; *-f* especifica un fichero de configuración alternativo y si no se indica se utiliza el fichero por defecto de *slapd*; y *-l* especifica el LDIF de donde obtendrá la(s) entrada(s) a insertar. Por ejemplo:

```
# slapadd -l alumnos.ldif
```

- **slapcat.** Permite extraer de una base de datos LDAP en formato LDIF. Si no se especifica un fichero se muestran por la salida estándar. Su sintaxis es:

```
# slapcat -l <filename> [-f <slapdconfigfile>] [-d
<debuglevel>] [-n <databasenumber>|-b <suffix>]
```

donde *-d* indica el nivel de depuración; *-n* indica qué base de datos se modifica en función de un número que indica la posición (primera, segunda, tercera,…) en el fichero de configuración; *-b* indica qué base de datos se modifica en función del sufijo de la misma; *-f* especifica un fichero de configuración alternativo; y *-l* especifica el fichero LDIF donde se insertan las entradas extraídas. Por ejemplo:

```
# slapcat –l salida.ldif
```

- **slapindex.** Se utiliza para la regeneración de índices de la base de datos.

```
# slapindex [-f <slapdconfigfile>] [-d <debuglevel>] [-n
<databasenumber>|-b <suffix>]
```

donde -d indica el nivel de depuración; *-n* indica qué base de datos se modificada en función de un número que indica la posición (primera, segunda, tercera,…) en el *fichero de configuración*; *-b* indica qué base de datos será modificada en función del sufijo de la misma; y *-f* especifica un fichero de configuración alternativo.

- **slappaswd.** Genera una contraseña de usuario cifrada para usar con *ldapmodify* o el valor *rootpw* para el fichero de configuración *slapd.conf*.

```
# slappasswd [-h schema]
```

Nota

Si desea más información sobre cualquier comando consulte las páginas man.

19.3.3 Herramientas gráficas

Las herramientas gráficas de apoyo a la administración del directorio activo LDAP son de especial utilidad sobre todo en nuestra primera toma de contacto con este servicio. De esta forma se va a ver en este apartado las dos herramientas más utilizadas que permiten llevar a cabo las operaciones habituales sobre el directorio (población del mismo, importación y exportación de ficheros LDIF, exploración de las bases de datos y *schemas*, etc.) de forma sencilla.

19.3.3.1 Herramienta de administración LDAP

Quizás la herramienta de administración LDAP sea la aplicación gráfica más intuitiva para la manipulación del directorio activo LDAP. Para su puesta en marcha hay que realizar la instalación del paquete *LAT* (*LDAP Administration Tool*) ejecutando:

UBUNTU

```
# apt-get install lat
```

FEDORA

```
# yum install lat
```

Una vez realizada la instalación puede iniciar la herramienta a través del menú *Aplicaciones/Internet/LDAP Administration Tool*.

Lo primero que debe hacer es especificar los parámetros de la conexión con el servidor de directorio LDAP. De forma simplificada tan solo es necesario introducir el nombre del *host* o dirección de red del servidor y el puerto de escucha, aunque si pulsa sobre el botón *Show more options* puede incluir más parámetros como el identificador de la base de datos, nombre de usuario y contraseña, si quiere utilizar encriptación, o el tipo de servidor (es posible conectar esta herramienta con otros servidores de directorio activo que no sean OpenLDAP).

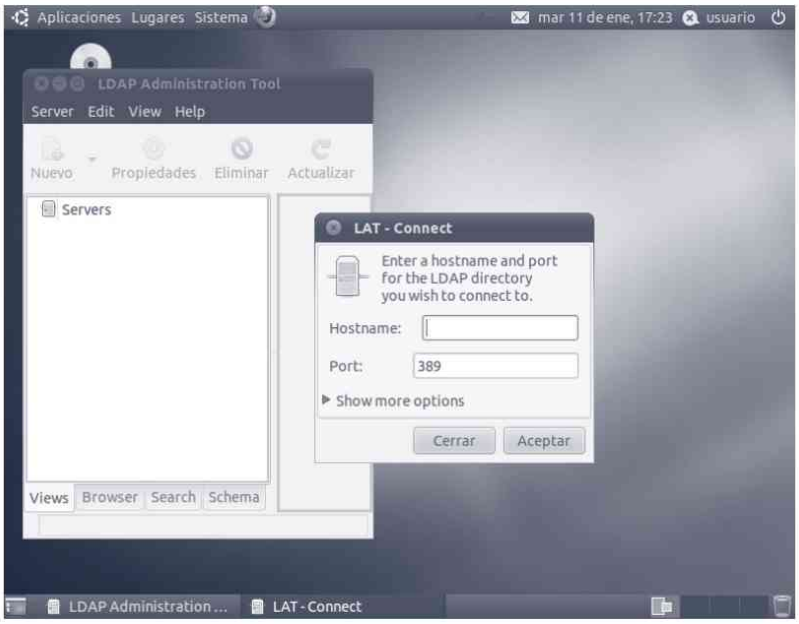


Figura 19-5. Conexión con el servidor LDAP en la herramienta de administración LDAP

En la figura 19-6 puede ver el aspecto inicial de la herramienta de administración LDAP una vez establecida la conexión con el servidor.

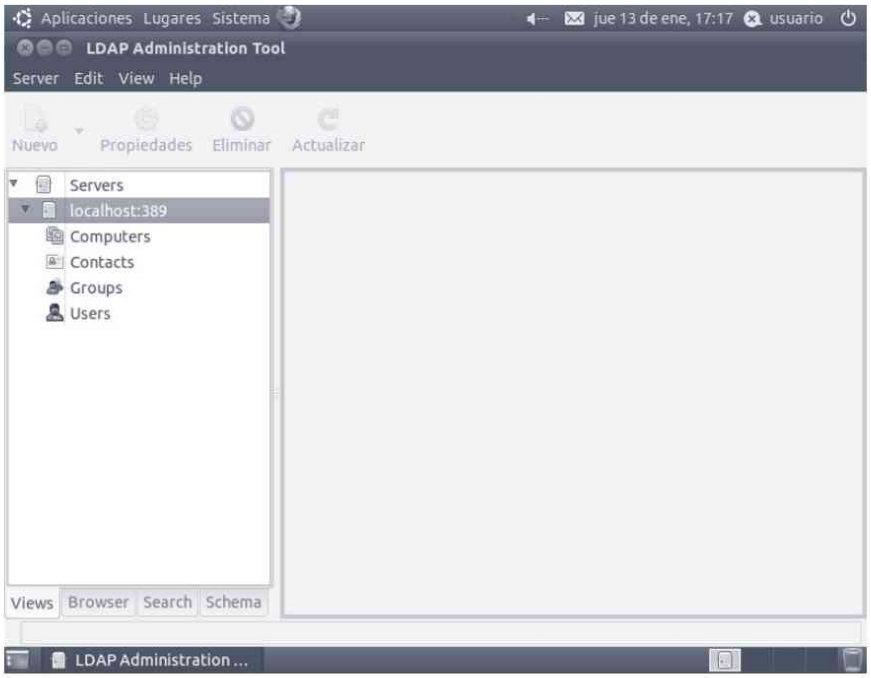


Figura 19-6. Aspecto general de la herramienta de administración LDAP

La herramienta de administración tiene tres zonas principales:

- **Barra de menús.** Contiene los menús principales de la aplicación a través de los que puede configurar las opciones y preferencias para trabajar con ella así como la manipulación de los datos, objetos, esquemas… del directorio activo.
- **Barra de herramientas.** Permite el acceso, dependiendo del componente, atributo u objeto del directorio activo que se está visualizando, a botones que permiten ejecutar de forma rápida las operaciones asociadas más habituales: *Nuevo*, *Eliminar*, *Templates* (Plantillas), *Propiedades*, *Actualizar*.
- **Panel principal.** En el panel de control se realizan las tareas principales en la manipulación del directorio activo sobre la vista o aspecto que se encuentre seleccionado. Dependiendo de la vista seleccionada las operaciones disponibles son diferentes, mostrando en la mayoría de los casos en la parte derecha los atributos correspondientes al objeto seleccionado en la exploración.

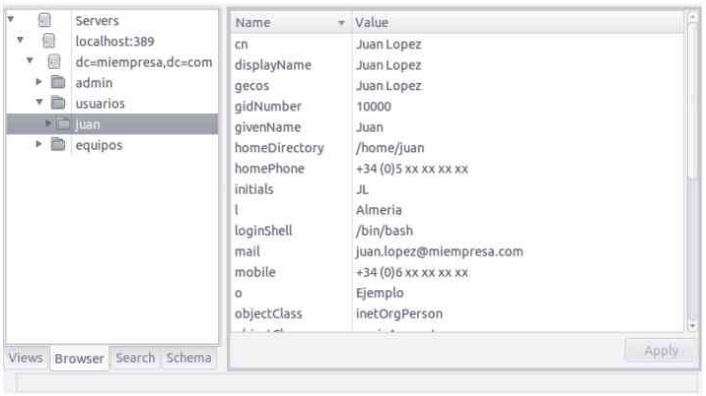


Figura 19-7. Panel principal de la herramienta de administración LDAP

A continuación se va a ver de forma breve qué es posible realizar en cada una de estas *vistas*:

- ***Views* (Vistas).** Permite ver los diferentes objetos incluidos en el directorio desde un punto de vista con nivel de abstracción alto, mostrando fundamentalmente datos clasificados en los distintos tipos de objetos incluidos en el *schema*. Se pueden introducir nuevos datos.
- ***Browser* (Explorador).** Permite navegar por la estructura en árbol para el directorio LDAP. Como en el resto de vistas, hay que conectarse a un servidor para ver los dominios y la información distribuida y almacenada en ellos. Para cada nodo puede ver los atributos que lo definen así como los valores asociados.
- ***Search* (Búsqueda).** Permite realizar búsquedas especificando cualquier filtro para la misma sobre los diferentes servidores y bases de datos a los que tiene acceso.

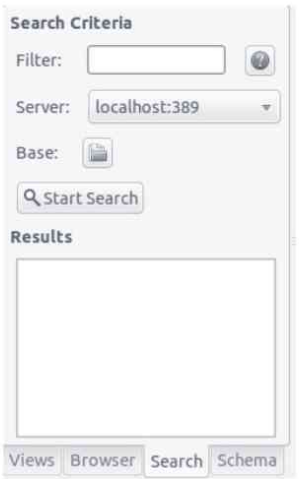


Figura 19-8. Vista Search de la herramienta de administración LDAP

- ***Schema* (Esquema).** Permite explorar *por el servidor* las clases de objetos, tipos de atributos, reglas de coincidencia y sintaxis LDAP que componen su *schema* o esquema. Puede ver y editar los detalles de cada uno de estos elementos seleccionándolos en el explorador con doble clic sobre su nombre tal y como muestra la figura 19-9.

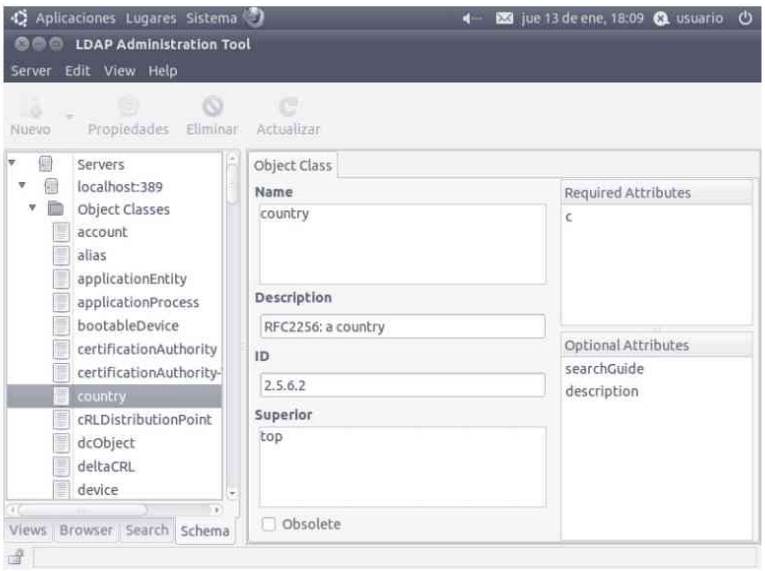


Figura 19-9. Vista Schema de la herramienta de administración LDAP

19.3.3.2 PhpLadpAdmin

PhpLdapAdmin es una interfaz web que permite la puesta en marcha y mantenimiento de directorios activos OpenLDAP. Para instalar *PhpLdapAdmin* puede utilizar el gestor de paquetes o ejecutando:

UBUNTU

```
# apt-get install phpldapadmin
```

FEDORA

```
# yum install phpldapadmin
```

Una vez finalizado el proceso, puede acceder a la página de inicio de *PhpLdapAdmin* (*http://localhost/phpldapadmin*) y conectarse al servidor de directorio activo.

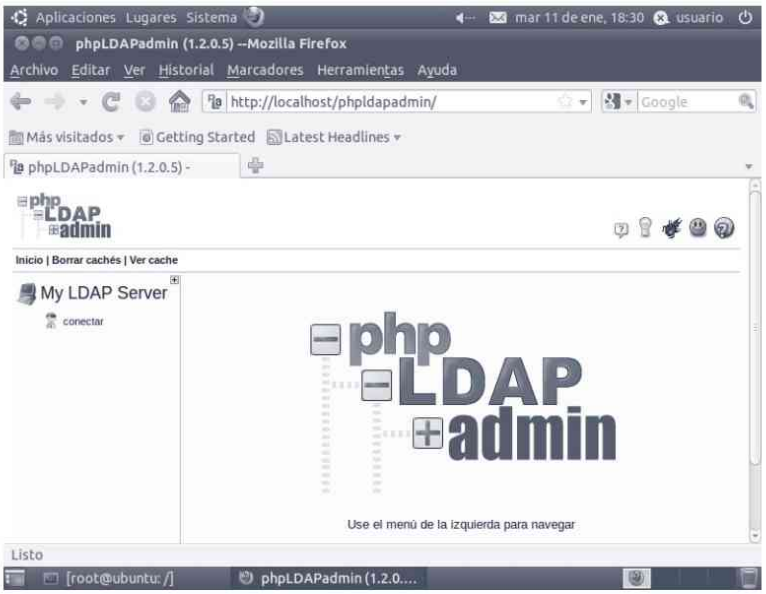


Figura 19-10. Página inicial de PhpLdapAdmin

Para conectarse a un servidor pulse en el vínculo *Conectar* situado en el menú izquierdo de la página y aparece la pantalla de autenticación (véase la figura 19-10).

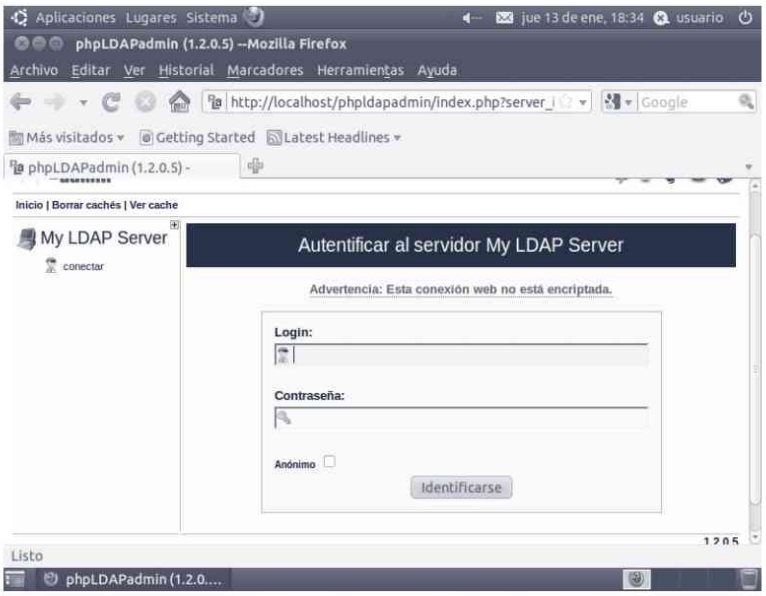


Figura 19-11. Inicio de conexión en PhpLdapAdmin

Una vez identificado en la página se cargan los diferentes menús y opciones en la parte izquierda de la página (véase la figura 19-12).

Figura 19-12. Menús con las opciones de PhpLdapAdmin

A través de ellos puede consultar las propiedades y características de las diferentes clases de objetos, tipos de atributo, reglas de coincidencia y sintaxis LDAP (esquema) que componen el *schema* del directorio activo, ejecutar detalladas y precisas búsquedas sobre los elementos e información disponible (buscar), mostrar información sobre la instalación y estado actual del servidor LDAP (info) así como exportar a diversos formatos los resultados obtenidos en una búsqueda o el contenido o valores de objetos y nodos del árbol del directorio.

En la figura 19-13 se muestra como ejemplo el resultado de la búsqueda en el dominio *miempresa.com.*

Figura 19-13. Ejemplo de resultado mostrado en una búsqueda con PhpLdapAdmin

Más información

Para más información puede consultar la siguiente dirección http://phpldapadmin.sourceforge.net./

PÁGINA WEB

Este libro dispone de su propia página web que complementa la obra, le permite ampliar sus conocimientos a través de software referenciado a lo largo de la obra, presentaciones, herramientas de autoevaluación para evaluar sus conocimientos, etc.

http://www.adminso.es

A través de esta página web los usuarios que se registren, podrán acceder a un curso virtual realizado con moodle. Para poder acceder al curso, el sistema le pedirá la contraseña:

INFORMACIÓN

ÍNDICE ALFABÉTICO

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Administración de Sistemas Operativos

Un enfoque práctico 2ª EDICIÓN ACTUALIZADA

Administre su servidor de una forma fácil y segura

Los conocimientos que se abordan en esta obra son fundamentales para cualquier persona cuya labor profesional sea administrar un sistema informático. Por ello, va dirigida a dos tipos de usuarios: por un lado, al profesional que desea actualizar sus conocimientos y, por otro lado, al estudiante que cursa materias que abarcan estos contenidos.

El libro cubre los aspectos teóricos de Administración de Sistemas Operativos, como los conocimientos prácticos en los sistemas más utilizados: Windows 2008 R2 y las distribuciones GNU/Linux, Ubuntu y Fedora.

Temas incluidos:

- Instalación y configuración del sistema. Hardware del servidor, configuración RAID, características de los sistemas operativos, proceso de instalación y configuración.
- Gestión de usuarios. Administración de usuarios, perfiles y permisos de usuarios.
- El sistema de archivos. Tabla de particiones, unidades RAID, permisos y cuotas de usuarios.
- Arranque y parada del sistema. Gestor de arranque, procesos, servicios, archivos de configuración y de inicio.
- Monitorización del sistema. Monitorizar el rendimiento de los recursos del sistema y gestión de las alertas del sistema.
- Copias de seguridad. Tipos de copias de seguridad, realizar, restaurar y planificar copias de seguridad.
- Administración de la red. Configuración de la red, configuración de routers, compartir archivos e impresoras y filtrado de puertos.
- Servicios básicos de red. Servidores DNS, servidores DHCP y servidores de acceso remoto.
- Servicios de Internet. Servidores web, Servidores FTP y servidores de correo electrónico.
- Servicios de directorio. Conceptos generales, instalación y configuración del Active Directory y de LDAP.

El libro cuenta con la web *http://www.adminso.es* donde, una vez registrado, tendrá acceso a diferente material electrónico como: presentaciones, animaciones, ficheros de configuración, etc.

9 788499 640822

ra-ma.es

Ra-Ma®