USERS

INCLUYE VERSIÓN DIGITAL GRATIS

REDES

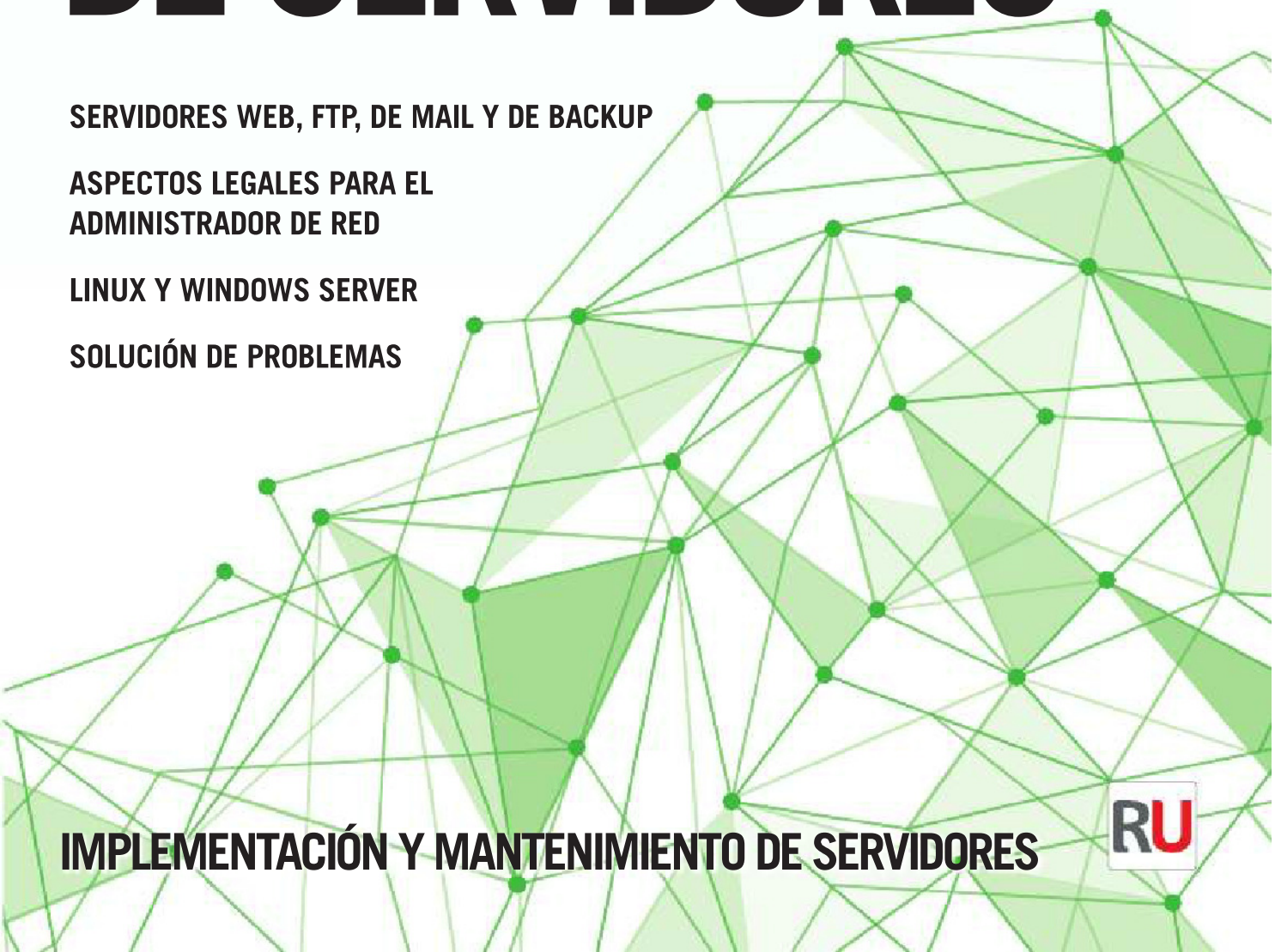
ADMINISTRACIÓN DE SERVIDORES

SERVIDORES WEB, FTP, DE MAIL Y DE BACKUP

ASPECTOS LEGALES PARA EL ADMINISTRADOR DE RED

LINUX Y WINDOWS SERVER

SOLUCIÓN DE PROBLEMAS



IMPLEMENTACIÓN Y MANTENIMIENTO DE SERVIDORES

RU

REDES: ADMINISTRACIÓN DE SERVIDORES

IMPLEMENTACIÓN
Y MANTENIMIENTO
DE SERVIDORES DE RED

RedUSERS

TÍTULO: REDES: ADMINISTRACIÓN DE SERVIDORES
COLECCIÓN: Manuales USERS
FORMATO: 24 x 17 cm
PÁGINAS: 320

ISBN 978-987-1949-48-9

Redes: Administración de servidores / Valentín Almirón ... [et.al.]. - 1a ed. - Ciudad Autónoma de Buenos Aires : Fox Andina; Buenos Aires: Dalaga, 2014.
320 p. ; 24x17 cm. - (Manual users; 264)
ISBN 978-987-1949-48-9
1. Informática. I. Almirón, Valentín
CDD 005.3

VISITE NUESTRA WEB

EN NUESTRO SITIO PODRÁ ACCEDER A UNA PREVIEW DIGITAL DE CADA LIBRO Y TAMBIÉN OBTENER, DE MANERA GRATUITA, UN CAPÍTULO EN VERSIÓN PDF, EL SUMARIO COMPLETO E IMÁGENES AMPLIADAS DE TAPA Y CONTRATAPA.

RedUSERS
COMUNIDAD DE TECNOLOGÍA

redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios y todos los elementos necesarios para asegurar un aprendizaje exitoso.

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com | usershop@redusers.com | + 54 (011) 4110-8700

RedUSERS
COMUNIDAD DE TECNOLOGÍA

La red de productos sobre tecnología más importante del mundo de habla hispana

Libros
Desarrollos temáticos en profundidad

Coleccionables
Cursos intensivos con gran despliegue visual

Revistas
Las últimas tecnologías explicadas por expertos

RedUSERS
Noticias actualizadas minuto a minuto, reviews, entrevistas y trucos

Newsletters
Regístrese en redusers.com para recibir un resumen con las últimas noticias

Re...m
Nuestros productos e...n contenido adicional y...s

Usershop
usershop.redusers.com

Revistas, libros y fascículos a un clic de distancia y con entregas a todo el mundo

Prólogo

Cada vez más, los sistemas se multiplican y abarcan todos los órdenes de la vida. Desde un simple kiosco hasta una gran multinacional, todo es regido por los sistemas. Esto lleva a que los data centers crezcan en forma exponencial, y que los administradores cada vez tengan que trabajar con más y más equipos. La administración artesanal y dedicada para cada servidor va quedando en el pasado, y cada vez está más automatizada y requiere menor intervención por parte de los técnicos.

Los servidores no suelen ser fácilmente accesibles ni configurables para los administradores novatos, por esta razón, en esta obra reunimos los consejos y datos que necesitamos para iniciarnos en la implementación y administración de servidores.

Sabemos que las redes de cómputo constituyen un elemento predominante en el saber informático y que, sin duda alguna, han proliferado por todo el mundo. Además, día a día, somos cada vez más los que nos dedicamos a estudiar y diagnosticar las redes. Por tal razón, debemos estar bien preparados y a la vanguardia con respecto a las redes en general y al manejo de servidores en particular.

En este libro se proponen diferentes acercamientos a los servidores de red más comunes, se describen sus características principales, cómo debemos configurarlos y también se entregan consejos para enfrentarse a los problemas que pueden surgir al trabajar con ellos, problemas que deambulan pero que, finalmente, no llegan más allá cuando se ha dado lugar a un conjunto de estrategias de solución.

Los invitamos a formar parte de esta obra, en la que juntos descubriremos cómo aprovechar al máximo los servidores de red.

El libro de un vistazo

Este libro reúne los conceptos y procedimientos que necesitamos conocer para efectuar la correcta administración de servidores de red. En cada uno de los capítulos que componen esta obra encontraremos información que nos ayudará a implementar y sacar el máximo provecho de distintos tipos de servidores en nuestra red de datos.

*01 HARDWARE DE SERVIDORES

En este capítulo se entregan las características del hardware de un servidor de red, describiendo cada uno de los componentes físicos más importantes que corresponden a un servidor y considerando sus particularidades.

*02 WINDOWS SERVER

Veremos las características de Windows Server y revisaremos la asignación de derechos y las restricciones. También veremos qué es Active Directory y la administración de las Directivas de Grupo.

*03 SISTEMAS GNU/LINUX

Aquí revisaremos la administración de un sistema de servidor GNU/Linux. Conoceremos los comandos básicos y realizaremos diagnósticos de red y procesos; también conoceremos la seguridad en el kernel.

*04 SERVIDORES WEB Y FTP

Nos enfocaremos en conocer los servidores web y FTP, veremos qué ventajas nos entregan y revisaremos las consideraciones que debemos tener en cuenta para administrarlos. También analizaremos los conceptos de seguridad en este tipo de servidores.

*05 SERVIDOR DE CORREO ELECTRÓNICO

Aquí analizaremos qué es un servidor de correo electrónico y aprenderemos a instalarlo y a configurarlo en sistemas Windows y GNU/Linux. También conoceremos los peligros del SPAM y de qué forma enfrentarlo.

*06 SERVIDORES DE ARCHIVOS E IMPRESIÓN

En este capítulo conoceremos las funciones que desempeña un servidor de archivos y de impresión. Luego aprenderemos a administrarlo en un sistema Windows y también en un sistema GNU/Linux.

*07 SERVIDORES ADICIONALES

Revisaremos alternativas de servidores adicionales, conoceremos el funcionamiento de los servidores de backup y entregaremos consejos para administrarlos. Veremos el funcionamiento de los servidores de actualización y de los servidores de antivirus. También aprenderemos a instalar un servidor proxy.

*08 ASPECTOS LEGALES PARA EL ADMINISTRADOR

Aquí podremos conocer los aspectos legales, los alcances y también las formas de atenuar la responsabilidad civil de un administrador de redes. También entregaremos consejos para enfrentar situaciones cotidianas en la administración de una red.

INFORMACIÓN COMPLEMENTARIA

A lo largo de este manual podrá encontrar una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados. Para que pueda distinguirlos en forma más sencilla, cada recuadro está identificado con diferentes iconos:


CURIOSIDADES E IDEAS

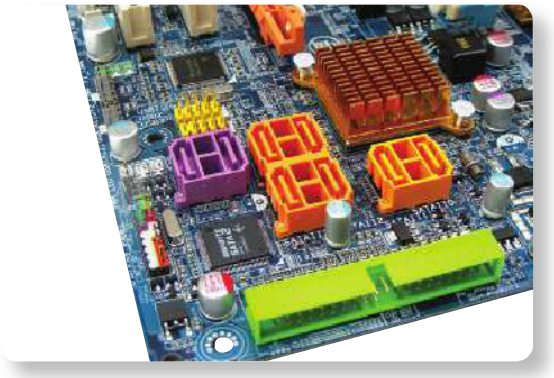

ATENCIÓN


DATOS ÚTILES Y NOVEDADES


SITIOS WEB

Contenido

*01 Hardware de servidores



*02 Windows Server

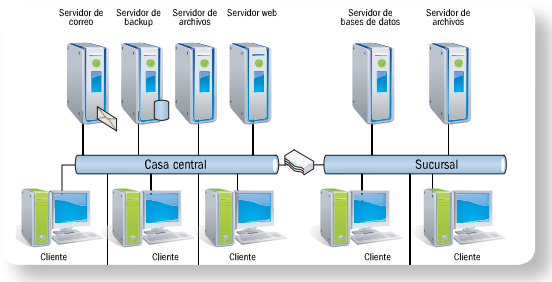
*03 Sistemas GNU/Linux

*04 Servidores web y FTP

*05 Servidor de correo electrónico

*06 Servidores de archivos e impresión

*07 Servidores adicionales



*08 Aspectos legales para el administrador

Introducción

En el ámbito de los servidores reinan los procesadores, las memorias y discos duros fabricados en forma especial para este tipo de equipos. En líneas generales, el hardware interno de los servidores de red no difiere tanto del hardware de un equipo de escritorio aunque posee mayores capacidades de proceso y almacenamiento.

A través de los capítulos que conforman esta obra conoceremos los componentes internos que podemos encontrar en un servidor de red pero también aprenderemos a implementar y configurar diversos sistemas operativos especialmente preparados para obtener el máximo provecho del hardware de un servidor.

Una vez que hayamos analizado en detalle el funcionamiento del hardware y que hayamos seleccionado el sistema operativo adecuado para cubrir nuestras necesidades nos daremos a la tarea de implementar diversos servidores de red, cada uno adecuado para tareas específicas. Conoceremos los servidores web y FTP, los servidores de correo electrónico y también los servidores de backup, entre otras alternativas.

La información que reúne este libro se presenta como un cúmulo de conocimientos que permite profundizar los datos entregados en los anteriores números de esta colección, cerrando el círculo que nos convierte en expertos administradores de una red informática.

En este sentido, el objetivo de este libro es simplificar la tarea de un administrador de red, entregándole los conocimientos que necesita para implementar y configurar los servidores que le permitirán entregar la información adecuada a cada uno de los clientes.

*01 –

Hardware de servidores

En este capítulo veremos las características del hardware de un servidor de red. Conoceremos cada uno de los componentes físicos que corresponden a un servidor y consideraremos sus particularidades.

Componentes internos

Cuando hablamos de los componentes de un servidor, nos referimos a los mismos componentes básicos que encontramos en un equipo de escritorio, pero especializados para brindar mayor poder de cómputo y, por sobre todo, mayor fiabilidad. La razón de ser de un servidor es, justamente, dar un servicio a los usuarios en forma continua y predecible. Lo normal es que los servidores den **servicio 24x7**, es decir, las 24 horas, los 7 días de la semana.

Esta característica **non-stop** es, sin dudas, uno de los principales requerimientos, sobre el que tienen que trabajar los ingenieros que diseñan servidores comerciales. En el mercado podemos encontrar servidores con distintos tipos de prestaciones, pero la **robustez** y la **confiabilidad** deben estar entre las principales.

El espacio en los **data centers** suele ser costoso y, por lo tanto, escaso, motivo por el cual los servidores se diseñan para poder ahorrar lugar en los racks. Dependiendo de la función que cumpla el servidor, ocupará más o menos unidades (U) de un rack. El diseño de gabinete condiciona la disposición y el tamaño que deben tener los componentes internos.

Figura 1. Proliant DL360. Podemos apreciar todos los componentes dispuestos en bloques.

Motherboard

El **motherboard** es el principal componente de un servidor, y su misión es dar soporte a los demás elementos. Puede contener más de un socket, para así poder conectar más de un procesador y varias memorias.

Microprocesador

Los procesadores para servidor se caracterizan por tener mayor capacidad y velocidad de cómputo, pero también, por la mayor cantidad de memoria caché. La capacidad de cómputo está dada por la cantidad de procesadores que posee el system board y por la cantidad de cores que tiene cada procesador.

La **memoria caché**, que se encuentra dentro del procesador, permite realizar operaciones con más velocidad. La gran diferencia que tienen los procesadores para servidores es, justamente, la cantidad de memoria caché con que cuentan. Poseen, típicamente, tres niveles de memoria. La L1 se encuentra dentro del procesador y es la más veloz, la más cara y, en consecuencia, la de menor capacidad. Es del tipo SDRAM y se utiliza, principalmente, para almacenar las instrucciones; suele tener menos de 150 KB. La L2 suele utilizarse para instrucciones y datos, y oscila entre 256 y 512 KB por core. Por último, la L3 está fuera del DIE y es compartida por todos los cores. Su capacidad varía considerablemente y su beneficio se percibe en aplicaciones que utilizan ciertas instrucciones o datos en forma repetitiva.

> LA MEMORIA CACHÉ PERMITE REALIZAR OPERACIONES CON UNA MAYOR VELOCIDAD

EL BACKUP A DISCO

El **backup** a disco está ganando mercado por ser un económico y muy efectivo método para reducir las ventanas de backup y mejorar los tiempos de restauración. La velocidad de los discos aumenta permanentemente, y las tecnologías SAS y SATA han reducido sus costos. Los discos permiten acceso aleatorio, lo que posibilita varias sesiones concurrentes de backup. Pero la cinta aún no puede ser completamente reemplazada cuando se trata de retención y archivo offsite.

Figura 2. El **Intel Server Board S2400SC2** soporta 2 procesadores Xeon E5, 8 módulos DDR3, 14 discos, 4 slots PCI Express y 1 slot PCI.

Los procesadores que Intel comercializa para servidores son el Xeon y el Itanium (también conocido como IA64). Los **Xeon** son, típicamente, x86, pero también tienen soporte para direccionamiento de 64 bits; son utilizados en servidores que van desde la gama inicial hasta los de misión crítica. Presentan algunas características especiales, como la posibilidad de detectar errores y corregirlos. En cuanto a la seguridad, se encargan de implementar un set de instrucciones AES-NI que permiten acelerar la encriptación de datos y reducir la cantidad de ciclos utilizados por el algoritmo.

Por su parte, los procesadores **Itanium** fueron desarrollados en conjunto entre HP e Intel, y se orientan a competir con los

FACEBOOK OPEN COMPUTE SERVER

Facebook ha desarrollado un estándar de servidor adaptado a sus necesidades, y en 2011 creó el proyecto Open Compute Server. La iniciativa tiene como objetivo contribuir a la madurez de la industria proveyendo los diseños de los componentes de servidores y otros elementos del data center. Es así que se diseñaron equipos de bajo costo y eficientes en términos energéticos. Cada componente ha sido revisado y adaptado. El motherboard fue simplificado al quitar los componentes innecesarios.

procesadores IBM Power y SPARC. Últimamente, se han visto envueltos en una gran controversia, luego de que Microsoft, Oracle y otras grandes empresas anunciaron sus intenciones de discontinuar el desarrollo y soporte de sus productos para esta plataforma. El sistema operativo que mejor ha recibido a esta familia de procesadores es HP-UX, así como otros sistemas Linux.

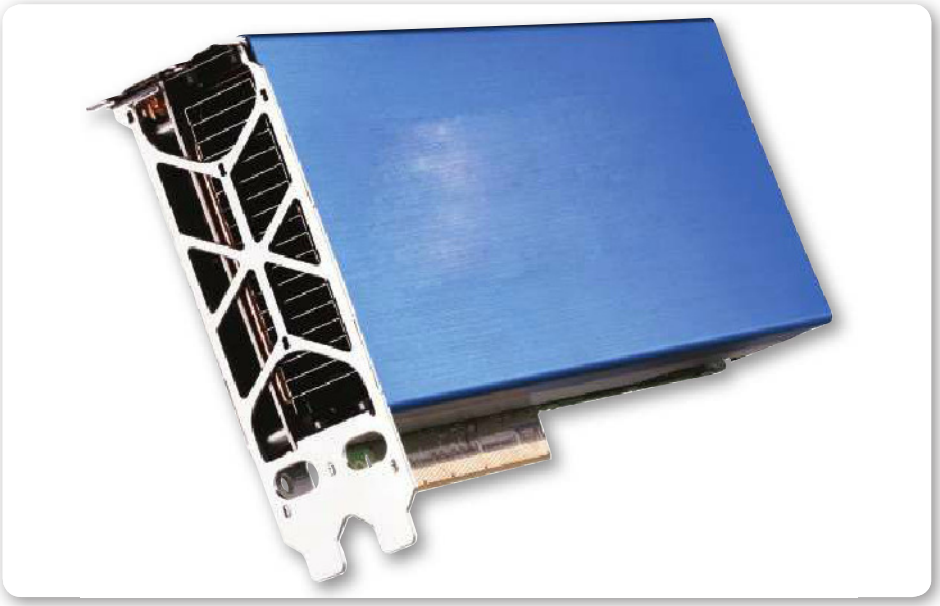


Figura 3. Procesador **Intel Xeon-Phi**. Realiza procesamiento altamente paralelo para ayudar a las supercomputadoras.

Por su parte, AMD produce la línea de procesadores **Opteron**, que ofrecen una excelente relación precio/prestaciones. Utilizan la arquitectura de instrucciones AMD64, pero ofrecen soporte nativo para 32 bits. La tecnología de Opteron conocida como **Hyper Transport** permite que un procesador acceda a la memoria principal de otro en el mismo motherboard, lo cual incrementa la velocidad de acceso. Existen numerosos sistemas operativos con soporte para estos procesadores, entre los que se destacan Windows, Solaris y Red Hat.

> LOS PROCESADORES OPTERON OFRECEN UNA EXCELENTE RELACIÓN PRECIO/ PRESTACIONES

Los **procesadores SPARC**, desarrollados por Sun Microsystems, son ampliamente conocidos en el mundo Solaris y BSD. Están basados en la arquitectura RISC, que es completamente abierta. En la actualidad,

Oracle, que adquirió a Sun Microsystems, utiliza procesadores Intel para su sistema operativo Solaris, pero reserva el procesador SPARC para sus equipos de gama alta, como la línea M.

Otro procesador que no podemos dejar de nombrar es el **IBM Power**, también basado en la arquitectura RISC, y soportado por los sistemas operativos AIX, Linux y OS/400 (I Series).

Memoria

Al igual que en el mundo de los procesadores, la memoria RAM utilizada en servidores tiene características propias que la diferencian de los módulos típicamente utilizados en computadoras de escritorio. Por ejemplo, los módulos de memoria RAM conocidos como **Fully Buffered**, los cuales son empleados por los procesadores Xeon y SPARC, entre otros, utilizan comunicación serie en vez de comunicación paralela con el controlador de la memoria, lo que incrementa el bus sin necesidad de aumentar la cantidad de pines.

Por otra parte, es necesario mencionar que la arquitectura utilizada en este tipo de memorias implementa un buffer que permite detectar y corregir errores (ECC), sin generar sobrecarga en el procesador ni en el controlador de la memoria.

Figura 4. Samsung Green Solution. Módulo RAM de 16 GB DDR3 y disco SSD de 512 GB con interfaz SATA de 6 Gbps.

Controlador de discos

El controlador de discos (HDC) está compuesto, esencialmente, por un chip y un circuito que es responsable de la administración de los discos. También puede controlar unidades ópticas (tales como unidades CD/DVD), unidades de cinta, etcétera.

La controladora es la que define qué tipo de disco puede usarse según la interfaz que soporte. Las interfaces típicas de servidores son IDE (prácticamente discontinuada), SATA (típicamente, para **servidores entry level**), Fiber Channel o SCSI, y sus derivados.

El **controlador de discos** puede estar integrado al motherboard o puede consistir en una placa de expansión (PCI, PCI-X). Una placa madre puede contar con distintos tipos de controladores de disco conectados en simultáneo, ya sea onboard o mediante placas externas.

El de un servidor suele incluir la funcionalidad RAID mediante hardware. El controlador RAID permite realizar un arreglo de discos con la finalidad de brindar mayor fiabilidad y/o performance. La ventaja de que el arreglo de disco se realice mediante un controlador de hardware dedicado es que libera ciclos de procesamiento de la CPU. Existen distintos tipos de RAID, que van del 0 al 6, y permiten que el sistema operativo vea los discos dentro del arreglo como una sola unidad.

> EL CONTROLADOR DE DISCOS PUEDE ESTAR INTEGRADO O TAMBIÉN EN UNA PLACA DE EXPANSIÓN

El RAID 0 brinda mayor performance, pero no otorga redundancia. EL RAID 1 se conoce comúnmente como espejado, porque mantiene dos discos con la misma información. En caso de que uno de ellos falle, el RAID puede seguir dando servicio con el disco espejado. El RAID 10 o 1+0 combina el RAID 0 con el 1, y otorga fiabilidad y performance. Los arreglos que van del 2 al 6 proveen distintos niveles de confiabilidad y rendimiento.

MEMORIAS FULLY BUFFERED

Uno de los puntos fuertes de este tipo de memorias es su casi nulo margen de error: se estima un error de lectura en 1.142.000 años. Los **módulos FB-DIMM** usan pistas bidireccionales en serie, que pasan por cada módulo, en vez de tener canales individuales que envían información a los módulos.

Discos duros

Los discos duros para servidores más utilizados hoy en día son SAS (Serial Attached SCSI), SATA (Serial ATA) y SSD (Solid State Drive). Los SAS se utilizan en un rango de servidores que va de gama media a alta o misión crítica. Poseen gran capacidad de almacenamiento: un solo disco puede almacenar entre 1 y 4 TB (4096 GB).

La velocidad de rotación del disco puede llegar hasta 15.000 rpm, y la velocidad de transferencia se establece en 6 GB/seg. Los discos SATA se utilizan en servidores entry o de gama media, pero no en los de misión crítica, ya que su tasa de I/O es menor que la de los discos SAS. Su capacidad oscila entre 250 GB y 4 TB. Por último, los discos SSD tienen una capacidad limitada, cuyo tope oscila en los 400 GB, y un altísimo precio, por lo que su uso se restringe a propósitos específicos.

Figura 5. Disco **SATA Samsung F1 RAID LG** con interfaz SATA, ampliamente difundida en servidores de gama baja y media.

La caché de disco permite optimizar la velocidad de acceso a la información, y así evitar la necesidad de acceder al disco cuando los datos están en la memoria de la controladora. El uso de este tipo de memoria caché es muy beneficioso para aplicaciones con manejo intensivo de disco, como las bases de datos. Al contar con este componente activo, cualquier base de datos funciona más eficientemente, tanto para leer como para escribir.

El problema potencial de este tipo de memoria si se usa para escritura es que, frente a un apagado inesperado del sistema, puede haber información que se pierda, y esto genere posibles problemas de consistencia en la base de datos. Otra característica particular que presentan los discos para servidores es que son hot swap, es decir, pueden intercambiarse en caliente, sin necesidad de apagar el equipo.

Módulo TPM

Como comentamos anteriormente, los procesadores modernos incorporan instrucciones especializadas para gestionar con mayor eficiencia las tareas de encriptación. Pero también existe un módulo denominado **TPM** (*Trusted Platform Module*), que permite almacenar llaves de encriptación, generar números aleatorios (no pseudoaleatorios, como puede hacer el software), calcular hashes, y también realizar otras funciones similares.

Los módulos TPM permiten tener un mayor nivel de seguridad y reducir la carga de trabajo de la CPU. Su arquitectura es abierta y está definida en el estándar ISO/IEC 11889. Actualmente, existen numerosos fabricantes que los comercializan, lo que implica que podemos encontrar estos módulos en casi todos los equipos modernos.

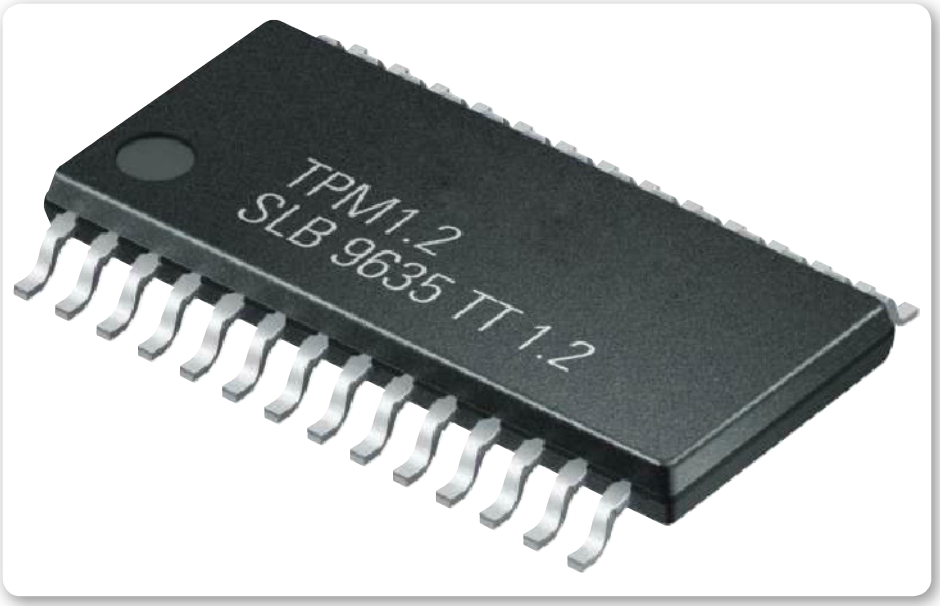


Figura 6. Módulo TPM Infineon. Permite ejecutar una gran variedad de algoritmos para asegurar la información en descanso y en tránsito.

Fuente de poder

Otra de las características distintivas en los servidores es la fuente de alimentación eléctrica. En general, estos poseen fuentes redundantes, es decir que, ante la falla de una de ellas, la otra continúa brindando energía al motherboard y sus componentes.

Además, las fuentes son **hot swap**, lo que permite retirar una defectuosa y colocar otra nueva sin necesidad de apagar el equipo o interrumpir el servicio. El hecho de contar con dos fuentes de poder distintas permite enchufarlas a distintos tomas o fases eléctricas. Las fuentes utilizadas en servidores entry level implementan una variante de ATX llamada **EPS** (*Entry-Level Power Supply Specification*).

El estándar EPS ofrece mayor estabilidad y poder eléctrico. La potencia que brindan va desde 550 W hasta 800 W, y tiene 8 voltajes de salida (3.3 V, 5 V, 12 V1, 12 V2, 12 V3, 12 V4, -12 V, y 5 VSB). Este estándar fue desarrollado en conjunto por Intel, Dell, Hewlett Packard, Silicon e IBM.

Figura 7. Fuente de poder silenciosa, especial para usar en servidores.

Tarjeta de red

Como muchos de los componentes presentes en un servidor, la placa de red posee características significativamente distintas de las de una terminal de usuario. Existen dos tipos de placas: las que utilizan cables de cobre y las que usan fibra óptica. Los cables de cobre emplean un

conector RJ-45, y el estándar empleado es CAT5 o CAT6, según las velocidades deseadas; CAT6 permite acceder a velocidades de hasta 10 Gigabit. Los enlaces de fibra óptica se usan, principalmente, para conectarse con **SAN** (*Storage Area Network*) utilizando el estándar *Fiber Channel* (FCP), un protocolo de transporte comparable con el protocolo TCP, que transporta comandos SCSI.

Existe una gran variedad de conectores para fibra óptica. Los más comunes son **LC** (*Lucent Connector*) y **SC** (*Subscriber Connector*). Otra arquitectura de comunicaciones utilizada en servidores de altas prestaciones es InfiniBand, que provee de una gran capacidad de transporte, baja latencia y **QoS** (*Quality of Service*). Esta arquitectura se encarga de establecer una conexión entre el servidor y los nodos de alta performance, como un storage.

Figura 8. El **Cisco Nexus 5000** provee de capacidad **Fiber Channel Over Ethernet** de 10 Gigabits.

Tarjeta de video

A diferencia de lo que sucede en equipos de escritorio, la placa de video pasa casi inadvertida en un servidor, donde raramente es utilizada, ya que estos equipos cuentan con mínimos requisitos gráficos. Estas placas suelen estar embebidas en el **system board** y representan uno de los componentes más baratos.

Ahora bien, desde hace tiempo existen iniciativas en súper computadoras que utilizan el poder de cómputo de las **GPU** (*Graphics Processing Unit*). Si bien esta es una tendencia que aún no se encuentra explotada comercialmente, puede que lo sea en algún tiempo.

Administración remota

Dado que los servidores no suelen ser fácilmente accesibles para los administradores, cuentan con facilidades para administrarlos en forma remota. Para este fin existen las herramientas conocidas como *Remote Management Support*.

ILO (*Integrated Lights Out*) es una tecnología desarrollada por HP, y una de las más difundidas, que permite ver los eventos que acontecieron en el servidor, como el reinicio del equipo, el cambio de partes, etc. También da la posibilidad de ver e interactuar con la pantalla como si estuviéramos delante del servidor. A su vez, es posible forzar el reinicio o apagado de este, de la misma manera que si lo hiciéramos oprimiendo los botones correspondientes. Esta funcionalidad puede usarse independientemente de si el servidor tiene o no un sistema operativo instalado o si el equipo está apagado. De manera genérica, esta capacidad se denomina *Out of Band Management* o *Lights-Out Management* (**LOM**).

Tecnología RAID

Un **sistema RAID** es un conjunto de dos o más discos cuya finalidad es obtener ciertos beneficios, como mayor velocidad y/o seguridad, dependiendo de la cantidad de componentes utilizados y su configuración. Esta tecnología se volvió más popular en los últimos años gracias a la inclusión de interfaces Serial ATA en las placas madre de línea baja, media y alta. Anteriormente, era necesario tener hardware especial para montar un conjunto RAID, como controladoras SCSI o Parallel-ATA compatibles.

Hoy en día, esas placas especiales no son necesarias, ya que prácticamente todo motherboard incorpora varios puertos Serial ATA con posibilidad de montar un set RAID. Sin embargo, la primera

versión de RAID data del año 1987, cuando se lo implementó por primera vez en una universidad estadounidense con el único fin de que dos o más discos conformaran una unidad que sumara la capacidad de todos como un único volumen. En 1988, se definieron los niveles de RAID del 1 al 5. Pero la primera patente que trata sobre combinar discos duros para tener mayor tolerancia a fallos es del año 1978, y aunque el método era similar, no se llamaba RAID.

> EN EL AÑO 1988 SE REALIZÓ LA DEFINICIÓN DE LOS NIVELES DE RAID DEL 1 AL 5

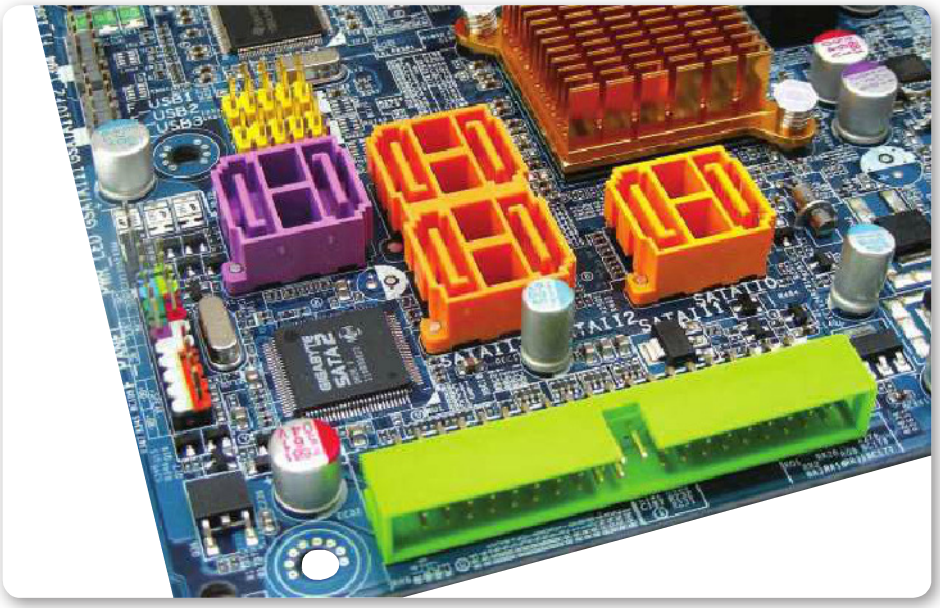


Figura 9. Los motherboards de gama alta, media y baja incorporan puertos **Serial ATA** con soporte para montar matrices RAID.

Tipos de RAID

Es necesario considerar que la elección de los diferentes niveles de RAID dependerá de las necesidades del usuario en lo que respecta a diversos factores, tales como seguridad, velocidad, capacidad, costos, etcétera. Cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y costos, desarrollados para brindar soluciones a los diferentes requisitos de almacenamiento.

La mayoría de los niveles RAID pueden satisfacer de manera efectiva solo uno o dos de estos criterios. No hay un nivel de RAID mejor que

otro, sino que cada uno es apropiado para determinadas aplicaciones y ámbitos. Resulta frecuente el uso de varios niveles de RAID para distintas aplicaciones del mismo servidor. Oficialmente, existen siete niveles (del 0 al 6), definidos y aprobados por el **RAID Advisory Board** (**RAB**). Luego están las posibles combinaciones de estos niveles (1+0, 5+0, etc.). Los niveles RAID 0, 1, 0+1 y 5 son los más usados.

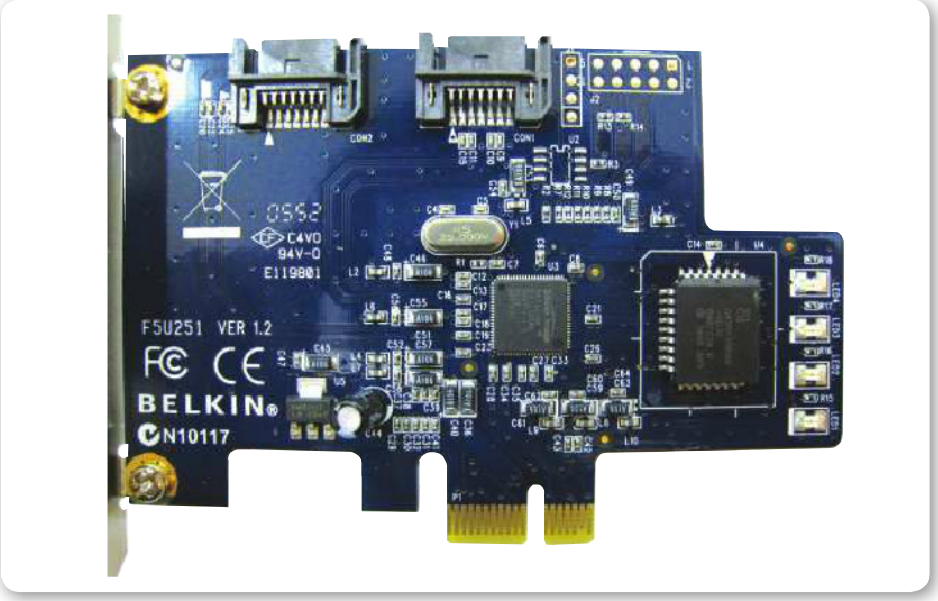


Figura 10. Controladora **Serial ATA RAID** en formato PCI Express 1x, ideal si no tenemos una incorporada en nuestro motherboard o si esta se encuentra dañada.

RAID 0

Se usa para obtener altas velocidades de transferencia, pero sin tolerancia a fallos. Es conocido como **stripping**, que significa "separación" o "fraccionamiento", pues los datos se dividen en segmentos que se distribuyen entre dos o más unidades físicas.

Este nivel de array o matriz no ofrece tolerancia a fallos. Como no posee redundancia, RAID 0 no ofrece ninguna protección de los datos. Si uno de los discos físicos de la matriz tiene problemas, el resultado es la pérdida de los datos. Por lo tanto, RAID 0 no se ajusta realmente a la sigla RAID, ya que no hay redundancia. Simplemente, se trata de una serie de unidades de disco conectadas en paralelo que permiten una transferencia simultánea de datos a todos ellos, con lo cual se

obtiene una gran velocidad en las operaciones de lectura y escritura. Consideremos que la velocidad de transferencia de datos aumenta en relación al número de discos que forman el conjunto.

Esto representa una gran ventaja en operaciones secuenciales con archivos de gran tamaño. Así, este método es aconsejable cuando se trabaja con aplicaciones de retoque fotográfico, audio, video o CAD; es decir, es una buena solución para cualquier aplicación que necesite un almacenamiento a gran velocidad pero que no requiera tolerancia a fallos.

> LA VELOCIDAD DE TRANSFERENCIA AUMENTA EN RELACIÓN AL NÚMERO DE DISCOS

Tengamos en cuenta que para implementar una solución RAID 0 se requiere un mínimo de dos unidades de disco.

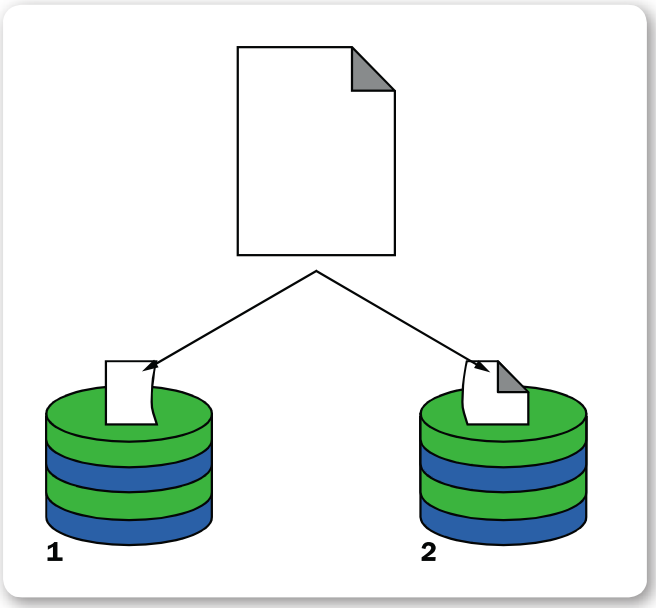


Figura 11. En RAID 0, cada archivo es dividido en segmentos que se distribuyen en los discos físicos que conforman el volumen. Así, se reparten las tareas, y los datos se responden, leen y escriben más rápidamente.

Es importante mencionar que un sistema RAID en stripping se encarga de aumentar considerablemente la velocidad de transferencia, sobre todo, la lineal, no muy presente en la práctica, pero sí en la lectura aleatoria y la que insume buffer de disco. En general, el incremento en el rendimiento en este tipo de matriz RAID suele ser del 50%. En todos los casos, y como un factor que juega en contra,

se nota un leve aumento en el consumo de CPU, pero los valores no son alarmantes en absoluto. Otro factor en el que se aprecia una gran mejora en el rendimiento es en el tiempo de carga del sistema operativo, y lo mismo sucede al iniciar aplicaciones pesadas.

JBOD

Si bien la concatenación de discos, también llamada **JBOD** (*Just a Bunch Of Drives*, sólo un montón de discos) no es uno de los niveles RAID numerados, sí es un método popular de combinar múltiples discos duros físicos en un solo disco virtual. Como su nombre lo indica, los discos son meramente concatenados entre sí, de manera que se comportan como un único disco. De esta forma, la concatenación es como el proceso contrario al de particionar: mientras este toma un disco físico y crea dos o más unidades lógicas, JBOD usa dos o más discos físicos para crear una unidad lógica.

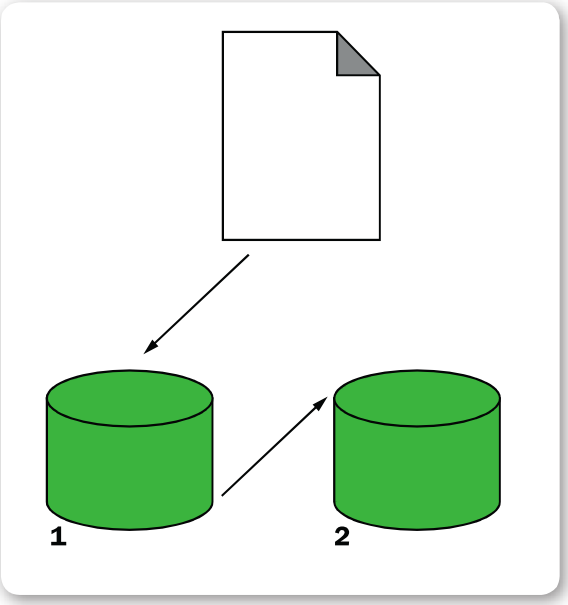


Figura 12. Diagrama de un array JBOD, donde dos unidades forman un solo volumen, una a continuación de la otra.

Al tratarse de un conjunto de discos independientes sin redundancia, puede ser visto como un método similar al de RAID 0. JBOD es usado a veces para combinar varias unidades pequeñas (obsoletas) en una unidad mayor con un tamaño útil. Una ventaja de JBOD sobre RAID 0 es que, en

caso de que un disco falle, en RAID 0 suele producirse la pérdida de todos los datos del conjunto por estar la información distribuida en "rodajas" por las unidades que conforman la matriz, mientras que en JBOD solo se pierden los datos del disco afectado, pero se conservan los de los restantes. Sin embargo, JBOD no supone ninguna mejora de rendimiento.

RAID 1

Este método también se denomina **mirroring**, que significa "espejado", porque cada disco que conforma el conjunto funciona como un espejo del otro. Se basa en el uso de discos adicionales, sobre los cuales se realiza una copia, en todo momento, de los datos que se están modificando.

RAID 1 ofrece una excelente disponibilidad de los datos mediante la redundancia total de estos. Para lograrlo, se duplican todos los datos de una unidad o matriz en otra; así, se asegura la integridad de los datos y la tolerancia a fallos, ya que ante un problema, la controladora sigue trabajando con los discos no dañados sin detener el sistema. Los datos se pueden leer desde la unidad duplicada sin que se produzcan interrupciones.

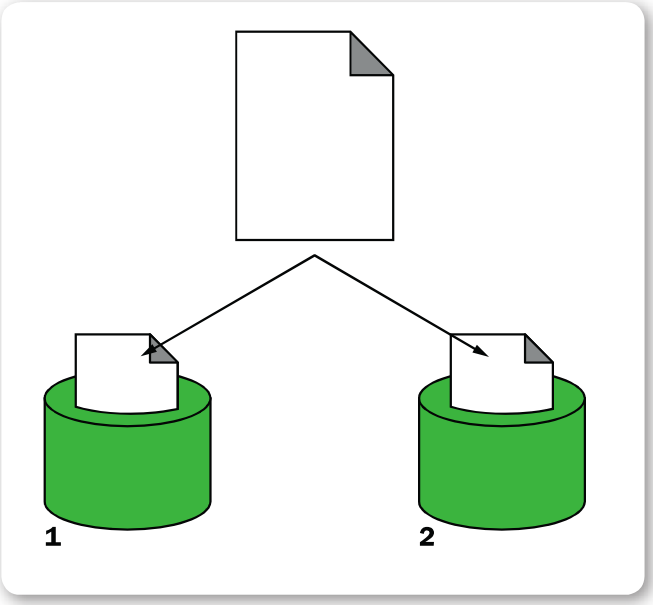


Figura 13. Esquema que representa un sistema RAID 1. Cada bit que se escribe en el disco se replica en el resto de las unidades; si uno falla, toda la información permanecerá intacta en otra unidad.

RAID 1 es una alternativa costosa para los grandes sistemas, porque las unidades se deben añadir en pares con el fin de aumentar la capacidad de almacenamiento. Pero es una buena solución para las aplicaciones que requieren redundancia cuando hay solo dos unidades disponibles. Los servidores de archivos son un buen ejemplo. Al igual que en RAID 0, se necesita un mínimo de dos unidades para implementar una solución de este tipo.

RAID 0+1

También llamado RAID 0/1 o RAID 10, es una combinación de los arrays vistos anteriormente, que ofrece velocidad y tolerancia a fallos al mismo tiempo. El nivel de RAID 0+1 segmenta la información para mejorar el rendimiento y, además, utiliza un conjunto de discos espejados para lograr la redundancia de datos.

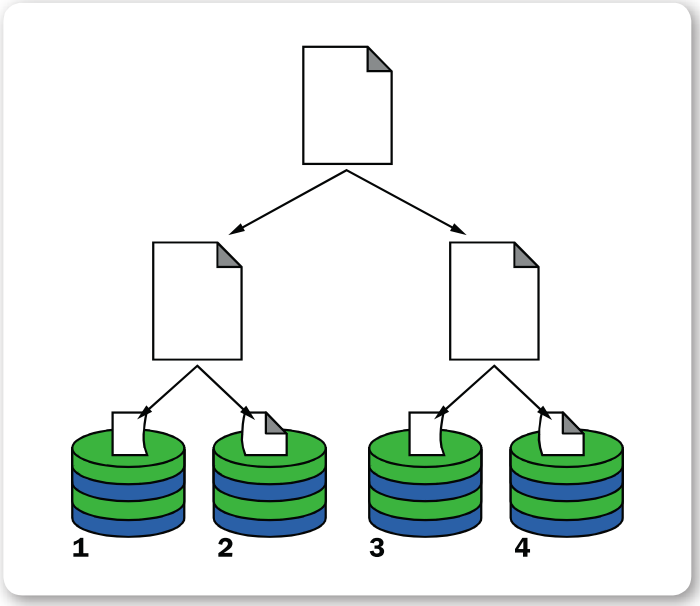


Figura 14. Diagrama de un RAID combinado (0+1), donde se gana en velocidad y en seguridad de los datos. La desventaja es lo costoso de su implementación debido a la cantidad de discos necesarios.

Al ser una variedad RAID híbrida, unifica las ventajas de rendimiento que brinda RAID 0 con la redundancia que aporta RAID 1. Sin embargo, la principal desventaja es que se necesita un mínimo de cuatro unidades, y solo dos de ellas se utilizan para el almacenamiento

efectivo de información. RAID 0+1 es la solución ideal para cualquier uso que requiera alto desempeño y tolerancia a fallos, pero no una gran capacidad. Normalmente, se lo implementa en entornos como servidores de aplicaciones, que permiten a los usuarios acceder a una aplicación en el servidor y almacenar datos en sus discos duros locales, o como los servidores web, que permiten a los usuarios entrar en el sistema para localizar y consultar información. Consideremos que este nivel de RAID es el más rápido y el más seguro, pero, como desventaja, el más costoso de implementar.

> RAID 0+1 OFRECE UNA SOLUCIÓN DE ALTO DESEMPEÑO Y TOLERANCIA A FALLOS

RAID 2

El nivel 2 de RAID adapta la técnica comúnmente empleada para detectar y corregir errores en memorias de estado sólido. De esta forma el código **ECC** (*Error Correction Code*) se intercala a través de varios discos a nivel de bit. El sistema empleado se conoce como **hamming**, ya que se utiliza tanto para la detección como para la corrección de errores (*Error Detection and Correction*).

Si bien RAID 2 no hace uso completo de las amplias capacidades de detección de errores contenidas en los discos, las características del código hamming también restringen las configuraciones posibles de matrices para RAID 2, particularmente, el cálculo de paridad de los discos. Está orientado a aplicaciones que requieran una alta tasa de transferencia, y resulta menos conveniente para aquellas otras que tienen una alta tasa de demanda de accesos.

CAPACIDAD DE LOS DISCOS

Otro aspecto importante para señalar es que es posible utilizar discos de diferentes capacidades; es decir, no es preciso que sean del mismo tamaño para conformar un set RAID. Pero, como regla, no se suman las capacidades de ellos, sino que se duplica la capacidad del disco más chico. Con respecto a la velocidad de transferencia, también es posible emplear discos de distintas velocidades, aunque para no perder sincronismo, las dos unidades operarán según la norma de transferencia del disco más lento.

RAID 3

Destina un único disco del conjunto al almacenamiento de información de paridad. La información de **ECC** (*Error Checking and Correction*) se emplea para detectar errores. La recuperación de datos se consigue mediante cálculos, gracias a la información registrada en los otros discos.

Este método ofrece altas tasas de transferencia, alta fiabilidad y alta disponibilidad, a un costo ligeramente inferior a un RAID 1 (espejado). Sin embargo, su rendimiento de transacciones es deficiente porque todos los discos del conjunto operan al mismo tiempo. Para implementar una solución RAID 3, se necesita un mínimo de tres discos duros.

RAID 4

La tolerancia a fallos se basa en el uso de un disco dedicado a guardar la información de paridad calculada a partir de los datos guardados en los otros discos. Ante una falla de cualquiera de los discos, la información se puede reconstruir en tiempo real mediante una operación manejada por la controladora. Debido a su organización interna, este RAID es especialmente indicado para el almacenamiento de archivos de gran tamaño, lo cual lo vuelve ideal para aplicaciones de video, sonido o gráficas donde se requiera, además, seguridad de los datos.

> ES NECESARIO UN MÍNIMO DE TRES UNIDADES DE DISCO PARA IMPLEMENTAR RAID 4

Debemos recordar que se necesita un mínimo de tres unidades para que podamos implementar una solución RAID 4. La ventaja sobre RAID 3 radica en que se puede acceder a los discos de manera individual.

RAID EN WINDOWS SERVER

Ni bien comienza la instalación de Windows Server 2003, en la parte inferior de la pantalla aparece un mensaje que nos advierte que, para instalar el sistema en unidades conectadas a controladoras SCSI o RAID, debemos pulsar la tecla F6. Al hacerlo, más adelante, se nos solicitará un disquete para cargar esos controladores y hacer que Windows reconozca el volumen donde instalarse. En Windows Server 2008 y 2012, estos drivers se pueden cargar vía pen drive o CD.

RAID 5

Ofrece tolerancia a fallos y optimiza la capacidad del sistema al permitir el uso de hasta el 80% de la capacidad total de los discos. Esto se logra mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques distribuidos en todos los discos del conjunto. La información se graba en forma de bloques, alternativamente, en todos ellos. Así, si cualquiera de las unidades de disco falla, se puede recuperar la información sobre la marcha, sin que el servidor deje de funcionar.

El RAID 5 es el nivel de RAID más eficiente y el de uso obligado para las aplicaciones de servidor básicas en una empresa. En comparación con otros niveles de RAID con tolerancia a fallos, RAID 5 ofrece la mejor relación costo-rendimiento en un entorno con varias unidades. Gracias a la combinación del fraccionamiento de datos y a la paridad como método para recuperar datos en caso de fallas, es una solución ideal para los entornos de servidores en los que gran parte del acceso a disco es aleatoria, la protección y disponibilidad de los datos es fundamental, y el costo es un factor importante. Este nivel de array es especialmente indicado para trabajar con sistemas operativos multiusuario, como Linux, UNIX o Windows Server. Se requiere un mínimo de tres unidades para implementar una solución de esta clase.

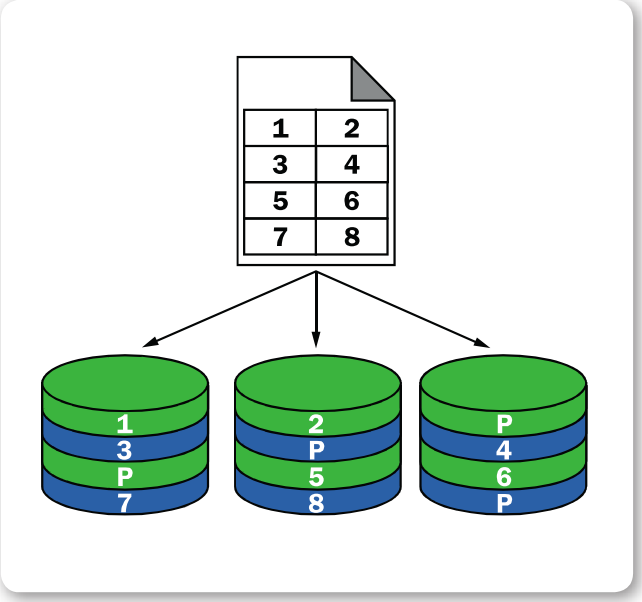


Figura 15. RAID 5: rápido, confiable y costoso.
Se requieren al menos tres discos duros para montar un RAID 5.

El BIOS Setup de un servidor

El **BIOS** o *Basic Input/Output System* es el software encargado de inicializar la computadora y administrar los periféricos. Entre sus varias funciones, se encarga de testear los componentes principales del equipo e inicializar el sistema operativo.

El BIOS es el primer software que ejecuta el equipo. Construye una capa de software que independiza al hardware del sistema operativo, lo que permite que este interactúe de una manera estandarizada con los distintos periféricos, sin importar su modelo o fabricante.

Los dispositivos se catalogan como de entrada o de salida. Entre los más comunes encontramos teclado y mouse, como dispositivos de entrada; y monitor, de salida.

Funcionamiento

Uno de los errores más comunes es confundir al utilitario o menú que se utiliza para configurar el BIOS con el BIOS en sí. De hecho, los primeros equipos IBM que implementaron la funcionalidad BIOS no contaban con un menú de configuración, pero naturalmente sí tenían un BIOS para controlar los dispositivos e inicializar el equipo.

La primera acción que realiza el BIOS es chequear el correcto funcionamiento de los dispositivos y periféricos; esta acción se denomina Power-OnSelf-Test (POST). Algunos de los dispositivos que testea son la CPU, la memoria RAM, las interrupciones, el chipset y los periféricos básicos (video, teclado, disco duro y lector de CD/DVD). En caso de detectar algún problema en ellos, lo informa al usuario, ya sea por pantalla, por medio de sonidos o a través de los LEDs del equipo.

Software

El software se almacena en un chip **EEPROM** (*Electrically Erasable Programmable Read-Only Memory*) que tiene la característica principal de ser no volátil, es decir que no se borra al desconectarle la energía, sin importar cuánto tiempo permanezca apagado.

La pila (habitualmente una CR2032) que poseen los motherboards tiene la función de mantener las configuraciones y la hora del sistema

almacenadas en el CMOS, pero no es necesaria para mantener el BIOS en sí mismo, ya que, como mencionamos anteriormente, este no se borra por la falta de energía.

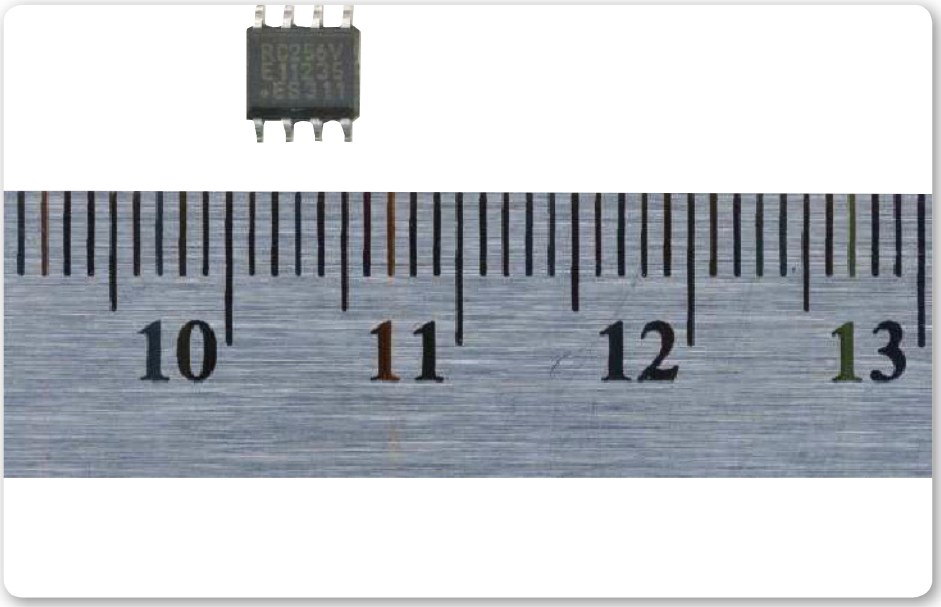


Figura 16. Fujitsu FRAM mejora el desempeño y el consumo eléctrico de las tradicionales memorias EEPROM

CMOS

El **CMOS** (*Complementary Metal Oxide Semiconductor*) es una antigua tecnología utilizada en la construcción de circuitos integrados. Se usa para almacenar las configuraciones del BIOS, ya que su simple diseño consume poca energía, emite poco calor y es inmune al ruido. La manera tradicional de restablecer la configuración predefinida del BIOS es, justamente, desconectando la pila o utilizando un jumper destinado a tal fin.

> EL CMOS ES UNA ANTIGUA TECNOLOGÍA UTILIZADA EN CIRCUITOS INTEGRADOS

La memoria EEPROM permite que el software sea fácilmente actualizado, sin necesidad de abrir el gabinete del equipo o retirar el chip. Los fabricantes de servidores recomiendan mantener actualizado el BIOS porque periódicamente se aplican mejoras o se corrigen errores. Incluso, en algunos casos, se pueden realizar mejoras que influyen en la performance del servidor de modo significativo.

Figura 17. Tradicional pila **CR2032** usada para mantener las configuraciones del BIOS en la memoria CMOS.

Servidores

El BIOS presente en un servidor posee funcionalidades más amplias que las de una estación de trabajo. Debido a su criticidad y al hecho que debe permanecer encendido durante la mayor parte de su vida útil, el BIOS monitorea todos los dispositivos a fin de resguardar información útil. Así como las computadoras de a bordo de los automóviles miden el consumo y las velocidades desarrolladas, el BIOS almacena información histórica sobre uso de la CPU y memoria, eventos de apagado y encendido, temperatura, fallas y más. Definitivamente, esta funcionalidad afecta en cierta medida la performance del equipo,

INTEFAZ ACPI

Advanced Configuration and Power Interface es el estándar que permite que el sistema operativo controle el consumo eléctrico. Fue desarrollado por Intel y otras empresas, y da la posibilidad de administrar el consumo del equipo, el procesador y los dispositivos. Esto permite que el SO encienda, apague, suspenda o hiberne, y que controle la performance y el consumo eléctrico. Tanto Intel como AMD han desarrollado distintas tecnologías para reducir el consumo eléctrico del procesador.

porque genera interrupciones en el trabajo del procesador. Según la funcionalidad que se habilite, por ejemplo, para monitorear el uso y consumo del procesador, puede generar 8 interrupciones por segundo. Los sistemas operativos modernos operan en modo protegido, y no utilizan el BIOS ni las interrupciones que este genera para acceder a los dispositivos, ya que implementan sus propios mecanismos de acceso al hardware.

> LOS SISTEMAS MODERNOS NO USAN EL BIOS PARA ACCEDER A LOS DISPOSITIVOS

Si bien el BIOS de los equipos x86 es un estándar de hecho que se mantuvo y fue evolucionando a lo largo de los años, algunos fabricantes de servidores desarrollaron otros estándares que tienen la misma funcionalidad, pero de forma diferente. Es el caso de los equipos Sun (actualmente, Oracle), que implementan el sistema **Open Boot**, también aplicado por IBM y Apple.

Otra alternativa al BIOS, pero compatible con él, es la iniciativa **UEFI**. Esta interfaz elimina algunas de las limitaciones del antiguo BIOS, como el modo de 16 bits de arranque y la limitación de 1 MB de direccionamiento, entre otras. Su desarrollo fue iniciado por Intel y HP para dar soporte a los procesadores Itanium, pero actualmente se utiliza, incluso, con otros procesadores.

Figura 18. La implementación del menú de configuración UEFI de ASUS permite tener una mejor visualización del estado del equipo.

En un principio, la configuración del BIOS y el hardware se realizaba mediante jumpers, pero en la actualidad se lleva a cabo por software desde un menú de configuración.

Debemos tener en cuenta que para acceder a este menú podemos hacerlo localmente por teclado y video, o en forma remota utilizando ILOM. Es importante considerar que la combinación de teclas para acceder al menú puede ser diferente si accedemos de uno u otro modo. Una vez que hayamos accedido al menú de configuración, podremos visualizar o modificar la información general del sistema (fecha y hora), la configuración del hardware (CPU, IDE, I/O, ACPI, USB, LAN, PnP, chipset, etcétera), las funciones de **Event log** y **Remote Access**, el orden de booteo de los discos, la contraseña de inicio o la de acceso al menú, y muchas otras opciones más.

Seguridad aplicada a servidores de red

Teniendo acceso físico a un servidor, es posible, por ejemplo, bootear con un CD, DVD o USB drive, y forzar una nueva contraseña de administrador para acceder al sistema. Este es uno de los motivos por los cuales la seguridad física de los servidores resulta casi tan importante como la seguridad lógica.

Algunas herramientas que realizan esta tarea en ambientes Windows son **Offline NT Contraseña &Registry Editor**, **ERD Commander** y **MS-DaRT** (Microsoft Diagnostics and Recovery Toolset), entre otras.

TIPOS DE CONTROL DE ACCESO

El método **DAC** (**Discretionary Access Control**) otorga al dueño del objeto el poder de permitir el acceso a otros individuos. El método **NDAC** (**Nondiscretionary Access Control**) establece reglas que no son implementadas por el usuario, sino por una entidad administrativa. En **MAC** (**Mandatory Access Control**) las reglas son establecidas por una entidad centralizada. Según **RBAC** (**Role Based Access Control**), las decisiones sobre niveles de acceso se basan en roles que los usuarios individuales tienen.

Para Linux, por ejemplo, booteando en modo single user, es posible resetear la contraseña de root. Muchas de estas herramientas fueron pensadas en un principio para ser utilizadas por administradores que necesitaban resolver un problema. Pero, naturalmente, también pueden ser utilizadas por usuarios malintencionados, con el fin de realizar "hacking". Es importante conocer estas herramientas, porque de esta manera podremos proteger los activos de un modo más consciente.

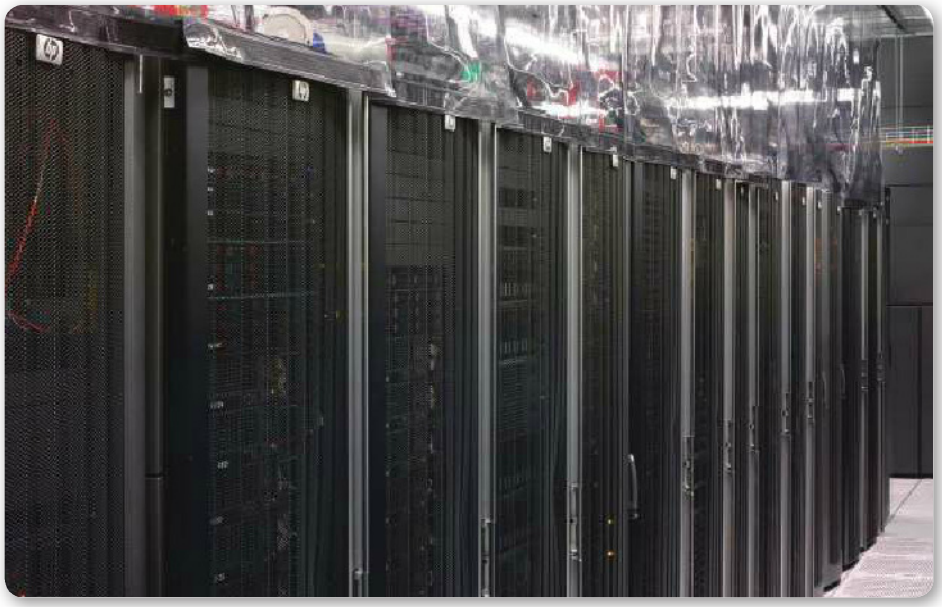


Figura 19. Data center con separación de pasillos fríos y calientes; el uso de la refrigeración se encuentra optimizado.

Seguridad perimetral

La primera medida que debemos considerar es la seguridad perimetral de los servidores. Es recomendable que estos se encuentren en un cuarto exclusivo de acceso restringido, al que denominaremos **server room.**

Este lugar no debe tener ventanas que puedan abrirse, ni tampoco paredes lindantes con el exterior. Es preciso llevar un registro de las personas que acceden a este recinto, ya sean empleados, visitas, proveedores o terceros en general. Para hacerlo, existen distintas herramientas de control de acceso que podemos usar, como las tradicionales cerraduras de llave, tarjetas magnéticas, de proximidad o autenticación biométrica. Seleccionemos el método que mejor se adecue a nuestras posibilidades y necesidades.

Figura 20. Con servidores cerrados, tenemos seguridad de acceso granular.

Infraestructura necesaria

El estándar **TIA-942** (del año 2005), ampliamente aceptado en el mercado, define la infraestructura necesaria para un data center: establece la organización del espacio y la disposición de los distintos elementos, la infraestructura del cableado, los niveles de confiabilidad y redundancia, y las consideraciones ambientales que deben tenerse en cuenta.

Existen cuatro tipos básicos de data centers: TIER-1, TIER-2, TIER-3 y TIER-4. La principal diferencia entre ellos radica en el nivel de

IBM HARDWARE MANAGEMENT CONSOLE

HMC es una tecnología desarrollada por IBM para permitir la configuración de LPARs (máquinas virtuales) en sistemas IBM p5, i5 y OpenPower. Se basa en un simple kernel Linux, un entorno gráfico X y aplicaciones Java. Un administrador, utilizando IBM HMC, puede identificar problemas de hardware, monitorear y configurar las LPARs. También puede asignar hardware (memoria, procesadores, etc.) a una LPAR dinámicamente. La administración puede realizarse desde la interfaz gráfica o por línea de comandos.

redundancia. Un data center TIER-1 carece de redundancia, en tanto que uno TIER-4 es completamente redundante. Un data center TIER-4 requiere de un edificio completamente independiente y no conectado con otras estructuras; tampoco puede lindar con la vía pública.

Figura 21. UPS Eaton 9390IT para data centers de tres fases. Utiliza procesos de doble conversión.

Racks

Una vez dentro del server room o data center, debemos considerar que los servidores estén instalados en racks con puerta y cerradura, con los tres paneles (los dos laterales y el posterior) instalados y asegurados; solo deberían abrirse los racks sobre los cuales se va a trabajar. Existen dos tipos básicos de racks: abiertos (bastidores) y cerrados. En caso de que un tercero deba realizar una instalación o tarea específica sobre un equipo dentro del server room, podremos asegurar que el resto de los equipos y su información permanezcan protegidos.

A su vez, cada servidor puede tener un cierre propio que protege el acceso al frente del equipo, para impedir el apagado no autorizado o el acceso a la lectora de CD/DVD o puertos USB. En el caso de equipos que estén fuera de un cuarto restringido, ya sean servidores o estaciones

de trabajo, es recomendable utilizar tornillos de seguridad o candado para proteger los componentes internos de robo o alteración. Cuando los equipos no están rackeados, también se recomienda utilizar una linga de seguridad, con el fin de anclar el equipo a un punto fijo y, así, dificultar su robo. Aun cuando los servidores se encuentren en racks cerrados, deben requerir autenticación para el acceso a la consola, así como también bloqueo por inactividad.

Detección de intrusión

Como medida adicional de seguridad, es posible habilitar la detección de intrusión de chasis desde la configuración del BIOS. En caso de que el chasis sea abierto, se generará un evento DMI, que se registrará en el CMOS, y alertará cada vez que el equipo se encienda, hasta que el evento sea borrado. Este tipo de eventos también puede ser monitoreado en forma remota. Es recomendable definir un proceso que recopile los eventos y notifique a los administradores para su revisión.

> LOS CCTV DISUADEN EL VANDALISMO Y EVIDENCIAN LOS ROBOS QUE SON REALIZADOS

Los switches y patcheras, ya sea dentro o fuera del data center, también deben protegerse dentro de gabinetes cerrados, para evitar que usuarios malintencionados se conecten a los puertos de administración y alteren la configuración o ganen acceso a segmentos de red restringidos. La implementación de NAC (Network Access Control) permite detectar, evaluar y remediar la configuración de los equipos que se conectan a la red. Es posible validar si poseen antivirus actualizado, fixes de seguridad y otros requisitos necesarios para garantizar el estado de la red. Si no se llega a cumplir alguno de estos requisitos, puede denegarse el privilegio de conexión a la red o corregir en forma automatizada, según las políticas definidas.

Dado el caso de proceder a la remediación del equipo, el proceso se realiza en una red independiente para tal fin, hasta que se corrijan todos los desvíos y pueda conectarse a la red correspondiente.

Los servidores en ambientes inseguros (sucursales, áreas de tránsito, pequeños negocios u oficinas) deben contar con *Full Disk Encryption*. De esta forma, y en caso de robo del equipo, podremos garantizar la

confidencialidad de la información contenida. Para esto existen distintas tecnologías, como Bitlocker para Windows Server, o dm-crypt para Linux.

CCTV

Los **CCTV** (circuito cerrado de TV) cumplen una doble función. Por un lado, disuaden el vandalismo o el robo del equipamiento; y por otro, lo evidencian una vez realizado. Existen equipos especialmente diseñados para el data center que tienen sensores para medición de temperatura, humedad y capacidad infrarroja para visión en la oscuridad, cuando las luces están apagadas.

Algunas aplicaciones de CCTV incluyen la funcionalidad de detección facial, para permitir el acceso a áreas restringidas. Estas requieren cámaras de mayor fidelidad de imagen, pero brindan una funcionalidad que puede ser complementaria a las tarjetas tradicionales, con lo cual otorgan un nivel de seguridad adicional.

> LA NORMA TIA-942 SE ENCARGA DE DEFINIR CÓMO DEBE SER LA CIRCULACIÓN DEL AIRE

Es posible integrar el CCTV con el sistema de control de acceso. Esto permite asociar una imagen de una persona con la información de la tarjeta o huella digital presentada ante el lector de esa zona. Habitualmente, la grabación se realiza cuando hay detección de movimiento, así se reduce el espacio total de almacenamiento utilizado, y esto aumenta la cantidad de horas de grabación disponible.

HVAC

Los circuitos HVAC (*Heating, Ventilation and Air Conditioning*) de data centers tienen la particularidad de que, además de enfriar

HP ILO MOBILE APP

Hewlett Packard ha desarrollado una aplicación para smartphones y tablets con iOS y Android que permite administrar servidores ProLiant. Algunas de las tareas que realiza son: operar el encendido y apagado de los servidores, interactuar con el sistema operativo y el BIOS.

el aire, regulan la humedad del ambiente y filtran las partículas de polvo. La **ASHRAE** (*American Society of Heating, Refrigerating and Air-Conditioning Engineers*) recomienda un rango de temperatura de entre 16 y 24° C, con una humedad de entre 40 y 55%. La humedad por encima de estos valores puede generar condensación, y por debajo de ellos, producir estática en los componentes electrónicos.

La norma TIA-942 define cómo debe ser la circulación del aire: pasillos fríos por donde los servidores toman el aire y pasillos calientes por donde lo expulsan. El aire frío circula por debajo del piso técnico y sale por los orificios frente a los racks. El aire caliente sube por detrás de los racks y es succionado por el aire acondicionado, que lo enfría y envía otra vez por debajo del piso técnico. Esta forma de separar los pasillos fríos y los calientes optimiza el flujo de aire, y así genera un ahorro en la energía necesaria para mantener las temperaturas recomendadas.

Figura 23. Los HVAC para data centers succionan el aire caliente por el techo, lo enfrían y lo envían por debajo del piso técnico.

Incendios

La detección temprana de humo es clave para reducir los daños al equipamiento. Por lo tanto, es importante colocar sensores debajo del piso técnico, en los racks y en el techo. En este sentido, si solo existieran sensores en el techo y el fuego se originara debajo del piso

técnico, donde existe gran cantidad de cableado, este sería detectado una vez que estuviera en una etapa muy avanzada, y entonces habrá dañado gran parte del equipamiento.

Figura 22. Tubos de **gas Inergen** para extinción de incendios en data centers. No daña los equipos ni afecta a las personas.

La metodología de supresión de incendios utilizando **gas Inergen** es la preferida. Este gas es un compuesto de nitrógeno, argón y dióxido de carbono que extingue el fuego al suprimir el oxígeno, uno de los tres elementos necesarios para que exista combustión. La ventaja es que no causa ningún tipo de daño en los equipos, como sí ocurre con el agua o el polvo. Así, no es necesario realizar una limpieza luego de utilizarlo, por lo que permite retornar rápidamente a la actividad normal. El compuesto Inergen no es nocivo para los humanos, y por este motivo reemplazó al CO2, que sí lo es.

Alimentación eléctrica

Los data centers deben contar con circuitos de alimentación independientes para poder energizar de manera correcta a los equipos que poseen fuentes redundantes. Dado el caso de que exista un corto o salte una térmica en un circuito, el servicio no se interrumpirá. Los sistemas **UPS** (*Uninterruptible Power Supply*) proveen energía de

emergencia. Su objetivo es mantener el suministro eléctrico luego de un corte de la energía de la red hasta que los generadores entran en funcionamiento. Típicamente, las baterías soportan algunos minutos, que son los necesarios para que la corriente generada por los motores sea estable y, por lo tanto, apropiada para los equipos.

Figura 24. General Electric Spectra Series Power Panel otorga protección eléctrica y permite intercambiar las líneas.

Respaldos

Las cintas o medios que contienen los backups no deben permanecer en el mismo recinto que los servidores, ni en forma contigua. El BCRA (Banco Central de la República Argentina) establece en la comunicación "A" 4609:

"Los procedimientos para el resguardo de datos, programas y todo otro componente de información deben prever, como mínimo, la generación de 2 (dos) copias de resguardo sincronizadas, manteniendo el almacenamiento de una de ellas en una localización distinta a la primaria, ubicada a una distancia determinada de acuerdo con el análisis de riesgos simultáneos que la entidad haya formalmente realizado".

> LOS MEDIOS DE RESPALDO NO DEBEN PERMANECER EN EL MISMO RECINTO QUE LOS SERVIDORES

El atentado a las Torres Gemelas producido el 11-S resulta un caso de estudio muy interesante. La firma **Morgan Stanley** estuvo en condiciones de volver a operar al día siguiente del atentado, ya que poseían un sistema de espejado en línea desde sus servidores del **World Trade Center** a otros en New Jersey. Este tipo de facilidades se conocen como **hotsite**, en contraposición a los **coldsites**, que necesitan que los backups sean restaurados antes de poder entrar en servicio. Muchas otras empresas tenían sus backups en la misma torre o en la torre vecina, por lo que no pudieron recuperar la información y, en muchos casos, quebraron.

En caso de tener que transportar cintas o medios ópticos, es sumamente recomendable que estos se encuentren encriptados, para evitar que la información pueda ser visualizada o alterada por terceros. Es el caso del hurto que sufrió Petrobras en 2008, cuando transportaba computadoras y discos con información sobre la exploración de un pozo petrolero muy importante. La información no estaba encriptada, y se sospecha que pudo ser aprovechada por alguna firma de la competencia.

> DEBEMOS ALMACENAR LOS MEDIOS DE RESPALDO EN CAJAS DE SEGURIDAD

Por último, es también recomendable que los medios utilizados para resguardar información sean almacenados en cajas de seguridad ignífugas, para que no se vean afectados en casos de calor excesivo o incendio.

EPO

En circunstancias extremas, puede ser necesario realizar un **EPO** (*Emergency Power Off*) de un data center. Si bien es un recurso útil, implica que es un único punto de falla. Este debe ser protegido de manera de evitar que una persona malintencionada pueda accionarlo.

Por otro lado, existen situaciones críticas en las que se cuenta con una ventana de tiempo que permite el apagado ordenado de los equipos, por lo que es necesario contar con un plan de apagado de emergencia detallado y actualizado. Este tiene que estar organizado, de forma que un operador pueda ejecutarlo paso por paso sin necesidad de tener que recurrir a su memoria o su juicio. Un ejemplo simple consiste en apagar primero las bases de datos, luego las aplicaciones y,

por último, los DNS y LDAP, que permiten autenticarnos en los equipos. Después de apagar los servidores, continuamos con los dispositivos de comunicación y, al final, con los HVAC. Es posible desarrollar un script que permita el apagado ordenado de todo el equipamiento en el data center en forma veloz. El objetivo final siempre debe ser minimizar los riesgos de corrupción de datos.

Figura 25. Emergency Power Off, o **EPO**, nos permite un rápido apagado frente a emergencias.

Monitoreo

El monitoreo activo de los componentes necesarios para el buen funcionamiento de los servicios es fundamental. Para determinar qué debemos monitorear y qué tipo de monitoreo utilizar, se aconseja aplicar el método **Whatif?**, es decir, preguntarnos **¿Qué pasa si...?** sucesivas veces, hasta recabar la información necesaria.

Por ejemplo: Pregunta 1: ¿Qué pasa si se descompone el aire acondicionado del data center? Respuesta 1: Todo el ambiente se recalienta. Pregunta 2: ¿Qué pasa si el ambiente se recalienta? Respuesta 2: Los servidores podrían fallar o reiniciarse. Pregunta 3: ¿Qué pasa si los servidores se apagan? Respuesta 3: Gran parte de la operatoria de la empresa se demoraría o paralizaría.

Conclusión: el mal funcionamiento del aire acondicionado del data

center puede afectar de manera significativa al negocio. Por lo tanto, utilizando esta metodología de análisis podemos:

1. Identificar riesgos.
2. Evaluarlos y valorarlos.
3. Desarrollar controles o implementar salvaguardas.

Figura 26. Tape Library Quantum Scalar i500.
Permite almacenar hasta 643 TB de datos en cintas LTO-6.

RESUMEN

En este capítulo conocimos las principales características del hardware que encontraremos en un servidor de red. También vimos qué es la tecnología RAID, analizamos el BIOS Setup de un servidor y detallamos las ventajas de la tecnología UEFI. Para terminar, dimos diversos consejos de seguridad aplicada a los servidores de red y describimos los recursos y tecnologías del hardware management.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice un microprocesador para servidores.
2. ¿Qué es la memoria caché?
3. Describa un controlador de discos.
4. ¿Para qué sirve un módulo TPM?
5. ¿Qué es un sistema RAID?
6. Describa el BIOS Setup de un servidor.
7. ¿Cómo funciona el BIOS?
8. ¿Para qué sirve la detección de intrusión?
9. ¿Qué es un CCTV?
10. ¿Para qué sirve un EPO?

EJERCICIOS PRÁCTICOS

1. Identifique los componentes internos en un servidor de red.
2. Ubique un sistema RAID en funcionamiento y describa sus componentes.
3. Acceda al BIOS Setup de un servidor.
4. Configure las opciones del BIOS Setup.
5. Identifique las falencias de seguridad en un servidor en funcionamiento.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*02

Windows Server

En este capítulo conoceremos las principales características de Windows Server y revisaremos los conceptos asociados con la asignación de derechos y las restricciones. También veremos qué es Active Directory y aprenderemos cómo administrar las Directivas de Grupo en forma avanzada.

Características

Dentro del amplio abanico de sistemas operativos que podemos instalar en nuestros equipos, encontramos que existen diferentes versiones y características asociadas a ellos. Entre las distintas empresas desarrolladoras, hay familias de sistemas operativos dedicadas a diversas tareas, principalmente, hogareñas y empresariales.

Casi el 90% de los equipos hogareños de escritorio cuentan con sistemas operativos de la empresa Microsoft, de la familia Windows. A lo largo de los años, estos fueron modificados según las necesidades de los diversos clientes, y hoy, una de las ramas principales son los sistemas dedicados a servidores (empresas y redes informáticas grandes), conocidos como Windows Server.

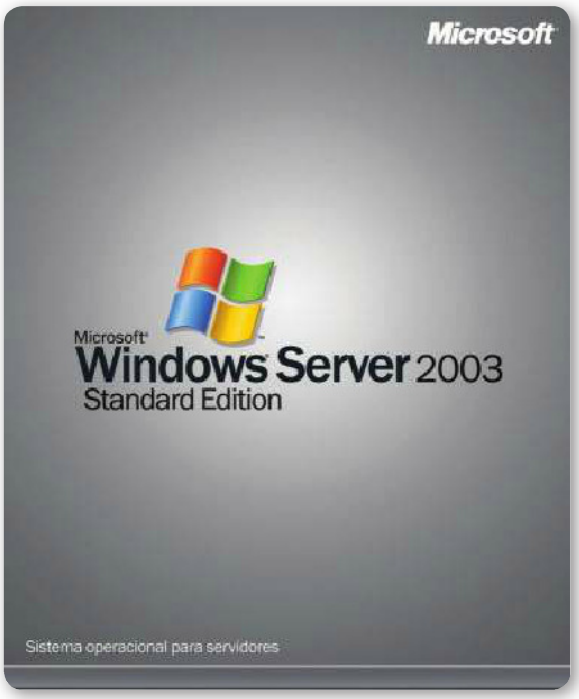


Figura 1. Windows Server presenta diversas alternativas para sus versiones de sistemas operativos adaptados a cada necesidad.

Se puede considerar que las diversas versiones de Windows Server corresponden a los sistemas operativos comerciales destinados al consumidor promedio, pero centrados en aplicaciones y rendimiento

para empresas y organizaciones. La primera versión de ellos destinada a las organizaciones fue Windows NT (que, a partir de entonces, fue conocido como Windows NT 3.5, 3.51, 4.0), y se correspondía con Windows 95; y así sucesivamente para Windows 2000 (Windows NT 2000), Windows XP (se integraron muchos programas, procesos y aplicaciones, y se conoció el nuevo Windows Server 2003, que salió a la venta casi dos años después que XP), Windows Vista (con su versión dedicada a servidores Windows Server 2008), Windows 7 (se actualizó la versión Windows Server 2008 R2), hasta la última versión disponible de Windows 8 con su administrador de servidores Windows Server 2012.

> LOS SISTEMAS OPERATIVOS WINDOWS SERVER ESTÁN DEDICADOS AL USO EMPRESARIAL

Los Windows Server están basados en las tecnología NT y, a diferencia de sus homólogos para computadoras de escritorio, están optimizados para labores empresariales, porque deshabilitan funciones innecesarias con el fin de mejorar el rendimiento (la interfaz gráfica, por ejemplo, está desactivada para disminuir el uso de memoria).

Características principales

Entre las características principales aplicadas a partir del lanzamiento de la familia Windows Server se encuentran las siguientes:

- Establece cuentas de usuario gestionadas, personalizadas y organizadas. Cada usuario es identificado y se le hace corresponder un perfil con permisos y delegaciones. Los datos, redes, servidores y cuentas de usuario quedan protegidos de intrusiones.

SAMBA

Samba es una implementación de código abierto del protocolo de archivos compartidos de Windows, denominado SMB en sus inicios y renombrado como sistema de archivos común de Internet o CIFS (Common Internet File System) en la actualidad, para sistemas operativos de la familia UNIX. Samba hace posible que computadoras Linux, Mac OS X o UNIX, actúen como PC Windows dentro de una red.

- Se establece el sistema de archivos NTFS, que permite establecer cuotas, ampliar la capacidad de almacenamiento y cifrar información. Se habilita la compresión de archivos y se permite el montaje de unidades de almacenamiento sobre sistemas de archivos de otros dispositivos.
- Gestiona el almacenamiento, de modo que los archivos menos utilizados son desplazados a unidades de almacenamiento más lentas o menos frecuentadas y, de esta manera, el disco las busca solo cuando las precisa.
- Se implementa Windows Driver Model, que según los dispositivos más utilizados, estandariza determinadas características; así, los fabricantes de hardware solo especifican algunas características especiales en sus dispositivos.
- Se gestiona la seguridad de manera centralizada localmente, gracias al uso de Active Directory, que relaciona distintos componentes de la red tales como: usuarios, grupos de usuarios y políticas de seguridad, entre otros. Utiliza protocolos tales como DNS, DHC, LDAP, etcétera.
- Emplea autenticación Kerberos, basada en la identificación de los terminales cliente/servidor, donde ambos se identifican mutuamente y, luego, la transferencia de información es encriptada y genera conexiones seguras.

Los servidores que podemos manejar son los siguientes:

- Servidor de archivos
- Servidor de impresiones e impresoras
- Servidor de aplicaciones de red
- Servidor de terminal

NÚCLEO NT

Todos los sistemas operativos de la familia Windows Server están basados en el núcleo NT. Esto significa que son modulares y se basan en dos capas: modo usuario y modo núcleo. En modo usuario, están limitados y restringidos a los recursos del sistema que tiene acceso. En modo núcleo, se tiene total acceso a la memoria del sistema y a los dispositivos externos. Dentro del núcleo se controla y dirige al modo usuario, delimitando las áreas a las cuales este puede acceder.

- Servidor de correo (SMTP/POP) mediante aplicaciones tales como Microsoft Outlook, integrada en la suite Office.
- Servidor de redes privadas virtuales (VPN)
- Controlador de dominios
- Servidor DNS
- Servidor DHCP
- Servidor WINS
- Servidor RIS (Remote Installation Services, que nos ofrece servicios de instalación remota de aplicaciones)

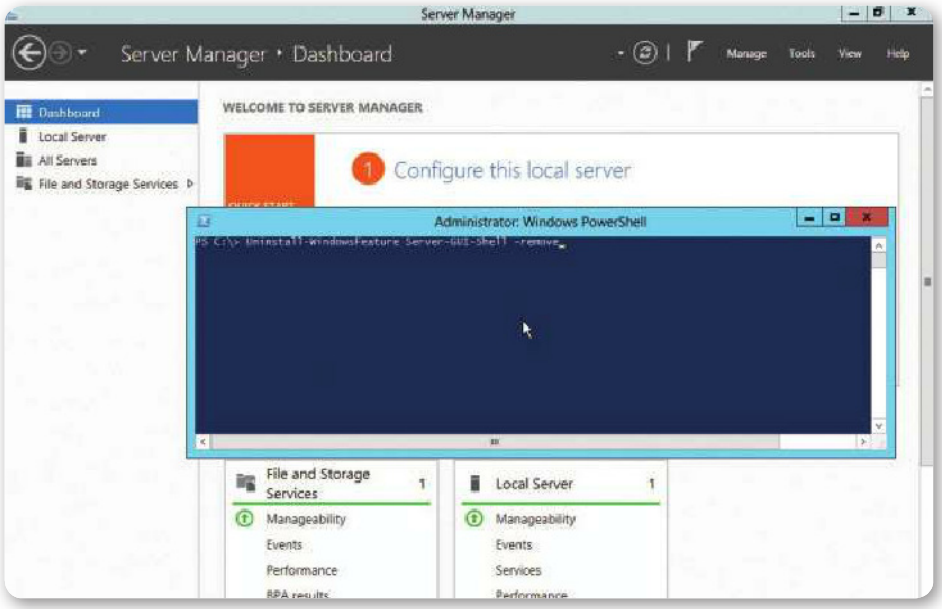


Figura 2. Dentro de Windows Server, podemos utilizar la consola de comandos para realizar numerosas actividades, al igual que en la interfaz gráfica.

Características adicionales

Algunas de las características adicionales se dividen según la versión del sistema operativo. Comercialmente salieron las versiones Web Edition (destinada a servicios y hospedaje Wew), Estandard Edition (cumple con la mayoría de los requerimientos de servicios para servidores), Enterprise Edition (destinada a empresas grandes con numerosos terminales), Data Center Edition (para servidores con grandes flujos de datos) y Small Business Edition (creada para redes con no más de 25 estaciones de trabajo).

Al tratarse de sistemas operativos dedicados a funcionar como servidores o como clientes, en los que la seguridad es primordial y las conexiones deben autenticarse permanentemente, las vulnerabilidades tienen que reducirse al mínimo. Es por esta razón que Microsoft realiza actualizaciones para corregir parches, optimizar funciones o agregar otras nuevas. Para estos sistemas operativos se liberaron distintos Service Packs, que reúnen actualizaciones críticas descargables y aplicables en cualquier momento.

Integración

En líneas generales, la implementación de Windows Server permite una fácil integración con otros sistemas operativos. Es simple de implementar, administrar y usar, genera una infraestructura de datos segura, con información confiable y de fácil acceso; y ofrece fiabilidad, disponibilidad, escalabilidad y rendimiento. Entre las herramientas de administración está presente la consola de comandos, cuyo fin es gestionar las cuentas más ágilmente que usando la interfaz gráfica.

El soporte del sistema operativo está respaldado por el gigante informático de Microsoft, que asegura el desempeño óptimo y la permanente corrección de errores.

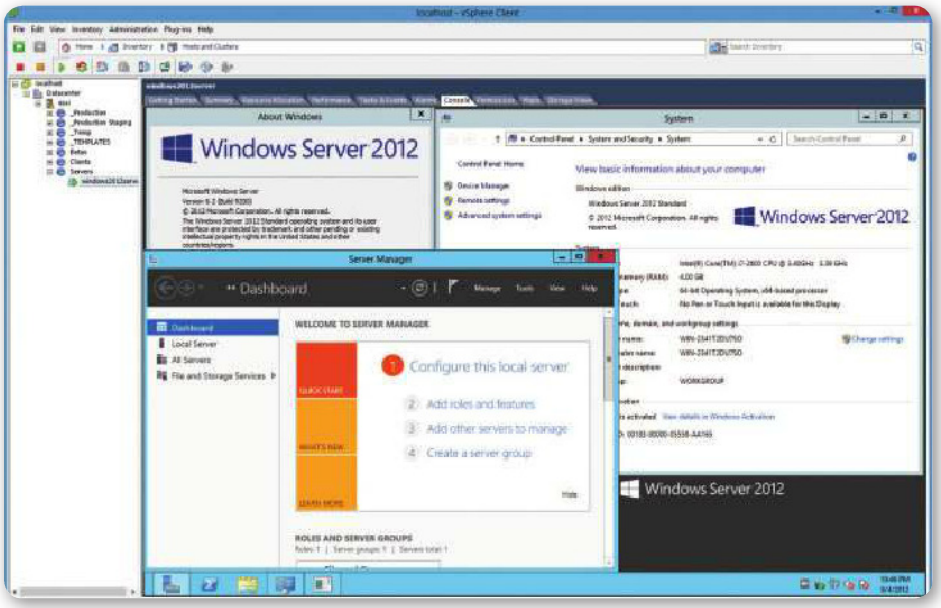


Figura 3. Windows Server 2012 presenta muchas mejoras con respecto al rendimiento, la gestión y la apariencia gráfica.

Active Directory

Active Directory es el nombre comercial que utiliza la empresa de desarrollo Microsoft para referirse a su solución informática o implementación propia de un servicio de directorio para una red distribuida de computadoras. Un servicio de directorio es un componente importante dentro de una red. Los usuarios y administradores, con frecuencia, no saben el nombre exacto de los objetos en los que están interesados. Quizá conozcan uno o más atributos de los objetos y, de esta manera, pueden consultar al servicio de directorio para obtener una lista de aquellos que concuerden con los atributos conocidos. Un servicio de directorio permite que un usuario encuentre cualquier objeto sabiendo solo uno de sus atributos.

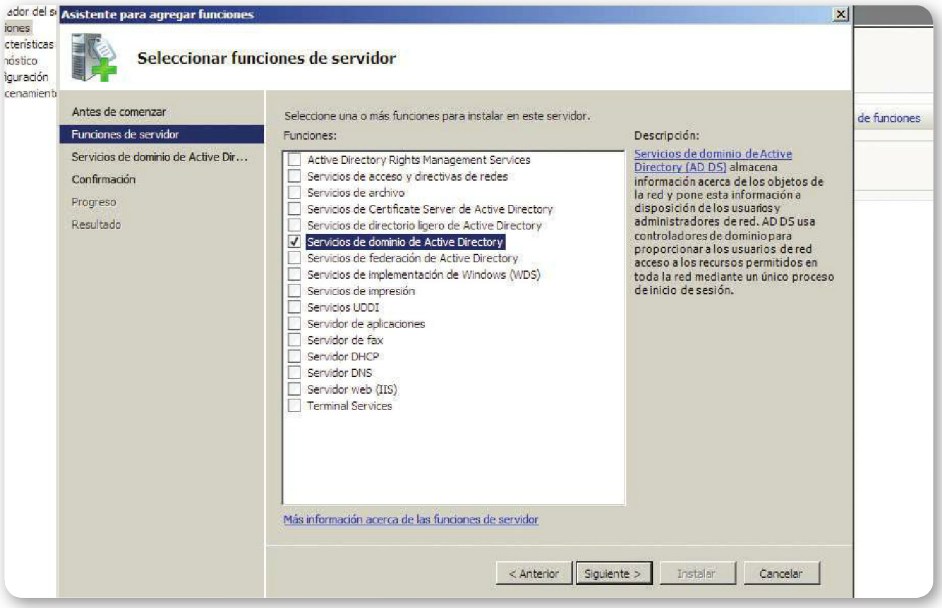


Figura 4. Los servicios de Active Directory deben ser instalados en el servidor. No se encuentran activos por defecto.

Protocolos y estructura

Este producto utiliza un conjunto de protocolos diferentes, entre los que podemos resaltar **LDAP** (*Lightweight Directory Access Protocol*, protocolo ligero de acceso a directorios), **DNS** (*Domain Name System*, sistema de nombres de dominio), **DHCP** (*Dynamic Host Configuration*

Protocol, protocolo de configuración dinámica de host, entendiendo como host al nodo huésped o computadora local que consume el servicio) y **Kerberos** (protocolo de autenticación de nodos de una red).

Suele referirse a Active Directory con el diminutivo **AD**. Posee una estructura jerárquica que nos permite mantener un conjunto de objetos relacionados con componentes de una red. Cuando mencionamos componentes, queremos decir usuarios, grupos de usuarios, permisos, y asignación de recursos y políticas de acceso.

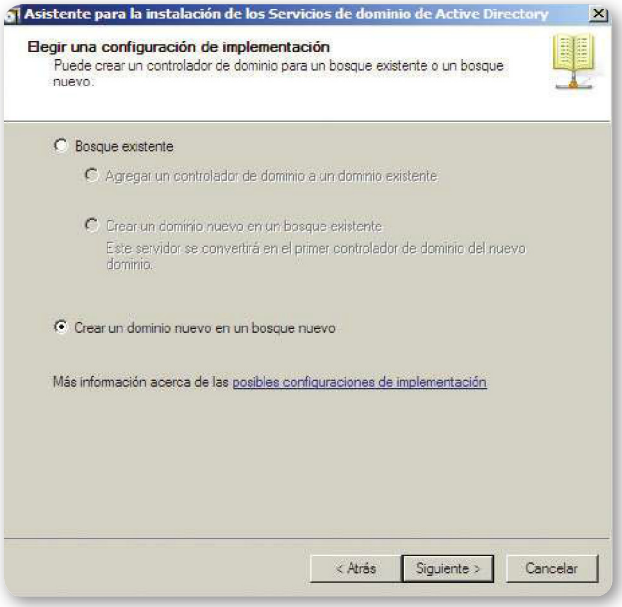


Figura 5. Para poder consumir los servicios de Active Directory es necesario crear un nuevo dominio o agregar un controlador de dominio a uno existente.

Como administradores, con Active Directory podemos definir políticas a nivel de empresa, ejecutar programas en una serie

AUDITORÍA

En los casos en los que, por cumplimiento de alguna normativa o por necesidad, tengamos que llevar un control de las modificaciones que se realizan en las políticas de grupo, podemos habilitar las opciones de auditoría, mediante la cual se registrarán las acciones que llevan a cabo los administradores para que, luego, tengamos la posibilidad de controlarlas mediante alguna herramienta de generación de informes.

de computadoras e implementar actualizaciones para toda una organización. AD posee una base de datos centralizada en donde se almacena la información de la organización: desde directorios con cientos de objetos hasta directorios con millones de ellos.

Arquitectura

Estructuralmente hablando, **AD** está conformado por un conjunto de dominios y subdominios (en organizaciones pequeñas, por lo general, los objetos se aglutinan en un único dominio), que se definen a través del protocolo **DNS**. Es por eso que para utilizar Active Directory necesitamos uno o más servidores DNS en línea dentro de la red. AD está basado en un conjunto de estándares den ominados X.500.

Los dominios y subdominios están dispuestos en una estructura jerárquica en forma de árbol. Si un usuario pertenece a un dominio particular, este será reconocido por los subdominios que descienden de él, sin necesidad de definirlo para cada uno de ellos.

> LOS DOMINIOS Y SUBDOMINIOS SE DISPONEN EN UNA ESTRUCTURA JERÁRQUICA

Además, distintos árboles (no comparten el nombre de zona DNS) pueden agruparse para conformar un bosque y establecer una relación de confianza (trust) entre ellos, de manera tal que los usuarios y los recursos de los distintos árboles sean visibles entre sí. AD es el que mantiene cada estructura de árbol en forma individual.

Active Directory, como mencionamos con anterioridad, utiliza un sistema común de resolución de nombres (**DNS**) y un catálogo común que contiene una réplica completa de todos los objetos del directorio del dominio en que se aloja, además de una réplica parcial de todos los objetos del directorio de cada dominio del bosque. Podemos clasificar dichos objetos en tres grandes categorías: recursos (por ejemplo, impresoras), servicios (como correo electrónico) y usuarios (por ejemplo, cuentas y grupos). Gracias a que los objetos se encuentran catalogados, AD puede brindar información sobre ellos, organizarlos, controlar su acceso y establecer la seguridad. Los objetos se encuentran dentro de los directorios que poseen un dominio o subdominio.

Cada objeto es una representación abstracta de una entidad única e indivisible (que puede ser un usuario, un nodo de la red, un recurso

como una impresora, una aplicación o una fuente compartida de datos). Esta representación contiene todos los atributos de la entidad. Los objetos pueden contener otros objetos. Cada uno de los atributos, que son la estructura interna básica de un objeto, se define por un objeto esquema o metadato, que también define la clase de objetos que se pueden almacenar en un directorio. Cada atributo se puede utilizar en diferentes esquemas de clase de objeto.

Cada objeto esquema se utiliza para definir los atributos de un conjunto de objetos y, por lo tanto, se integra con ellos. Por lo tanto, modificar o eliminar un objeto esquema puede volverse una acción tediosa y compleja, ya que la modificación o eliminación se propagará a través de todos los objetos con los que se encuentre integrado.

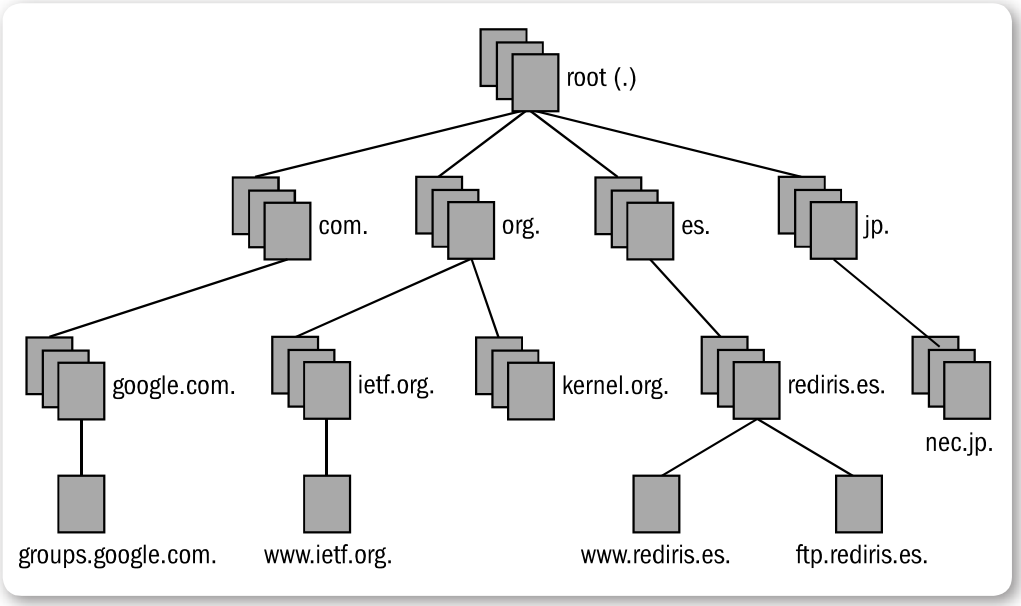


Figura 6. Los dominios y subdominios de Active Directory respetan una estructura jerárquica de árbol.

Funcionamiento

Active Directory posee una base de datos centralizada en donde se almacena toda la información relacionada a un dominio de autenticación. La sincronización entre los distintos servidores de autenticación del dominio es un punto fuerte de esta implementación.

Cada objeto posee atributos que lo identifican de forma unívoca (por ejemplo, un usuario puede tener los campos **<<Nombre>>**,

<<E-mail>>, etc.; y una impresora puede incluir los campos **<<Nombre>>**, **<<Fabricante>>**, **<<Modelo>>**, **<<Usuarios Autorizados>>**, etc.). Toda esta información se encuentra centralizada y se replica de manera automática entre todos los servidores que controlan el acceso al dominio.

> LA INFORMACIÓN SE REPLICA EN FORMA AUTOMÁTICA ENTRE TODOS LOS SERVIDORES

De esta manera, es factible crear recursos (como carpetas compartidas, impresoras de red, etc.) y conceder autorización de acceso a ellos a usuarios, con la ventaja de que todos estos objetos se encuentran memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito. Para decirlo en otras palabras, Active Directory es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

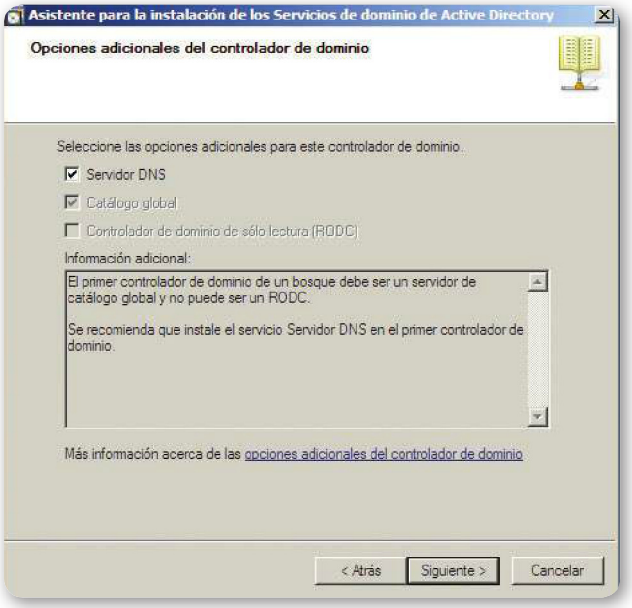


Figura 7. En una red de computadoras que implementan Active Directory es necesaria la presencia de uno o más servidores DNS.

Las relaciones de confianza entre dominios (*trust* en inglés) permiten que usuarios de un dominio particular accedan y consuman recursos presentes en otro dominio diferente del primero. Estas relaciones son

creadas en forma automática cuando se generan nuevos dominios. Los límites de las relaciones de confianza no son marcados por dominio, sino por el bosque al cual pertenecen los dominios implicados.

Existen diferentes tipos de relaciones de confianza:

- Confianza transitiva: estas relaciones son automáticas y de dos sentidos entre dominios gestionados por Active Directory.
- Confianza explícita: son aquellas relaciones que se establecen de forma manual para especificar una ruta de acceso con propósitos de autenticación. Este tipo de relación puede ser de uno o dos sentidos (de ida y/o de vuelta), dependiendo de la aplicación. Se utiliza con frecuencia para acceder a dominios integrados por computadoras con Windows NT 4.0.
- Confianza de Acceso Directo: es esencialmente una relación de confianza explícita que crea accesos directos entre dos dominios en la estructura de dominios. Este tipo de relaciones permite incrementar la conectividad entre dos dominios, y así reduce las consultas y los tiempos de espera para la autenticación.
- Confianza entre bosques: estas relaciones permiten la interconexión entre bosques de dominios, creando relaciones transitivas de doble sentido. En Windows 2000, las relaciones de confianza entre bosques son del tipo explícito, a diferencia de lo que sucede en Windows Server 2003.

ACTIVE DIRECTORY IMPLEMENTA UN SERVICIO DE DIRECTORIO PARA REDES DISTRIBUIDAS

Para conectarse a otros bosques o dominios que no son de Active Directory, AD usa el protocolo Kerberos 5, aunque también soporta NTLM y usuarios web mediante autenticación SSL/TLS.

Los direccionamientos a recursos están definidos por los estándares **UNC** (convención universal de nombramiento), URL (localizador uniforme de recursos) y las definiciones de direcciones definidas en el protocolo LDAP.

Cada objeto que forma parte de la red posee un nombre distintivo o **DN** (*Distinguished Name*). Así, por ejemplo, una impresora denominada **Imprimir**, que se encuentra dentro de una unidad organizativa u **OU** (*Organizational Unit*) denominada **Administración**, perteneciente al dominio **organizacion.org**, puede especificarse de dos modos:

- En notación DN, CN=Imprimir, OU=Administración, DC=organización, DC=org; donde CN (Common Name) es el nombre común, y DC (Domain Class Object) es la clase de objeto de dominio.
- En forma canónica podemos especificar la dirección como: **organización.org/Administración/Imprimir**

También podemos emplear métodos para individualizar un recurso en forma local:

- Empleando una distinción de nombre relativo o **RDN** (*Relative Distinguished Name*), que se caracteriza por buscar un recurso a través del nombre común (CN) solamente.
- Empleando un identificador global único o **GUID** (*Globally Unique Identifier*), que genera una cadena de caracteres de 128 bits de la cual se vale AD para buscar y replicar información.

> ES POSIBLE USAR DIVERSOS MÉTODOS PARA IDENTIFICAR UN RECURSO EN FORMA LOCAL

Algunos tipos de objetos poseen un nombre de usuario principal o **UPN** (*User Principal Name*), que posibilita el acceso de forma abreviada a un recurso o directorio dentro de una red de computadoras. La notación es **nombredeobjeto@dominio.**

Active Directory, a diferencia de Windows NT Server, permite generar la creación de estructuras jerárquicas conformadas por dominios y subdominios, una manera más sencilla y ágil de representar los recursos de una red según su ubicación o función dentro de una organización o empresa. Además, se basa en estándares como X.500 y LDAP para acceder a la información.

KERBEROS

Kerberos es un protocolo de autenticación que se utiliza en redes de computadoras. Fue creado por Gerard Kominek y permite que dos computadoras presentes en una red insegura demuestren su identidad de modo seguro. En sus comienzos, utilizaba una arquitectura de cliente/servidor para que ambos verifiquen la identidad del otro. Se basa en criptografía de clave simétrica y requiere de un tercero de confianza. En la actualidad, existen extensiones que hacen posible el uso de claves asimétricas.

Personalización

Otra característica peculiar que ofrece Active Directory son las interfaces de servicio o **ADSI** (*Active Directory Service Interface*), que brindan a los programadores la posibilidad orientada a objetos de crear programas que interactúen con AD, y aprovechen sus capacidades mediante lenguajes de desarrollo de alto nivel, como Visual Basic, sin tener que lidiar con los diferentes espacios de nombres.

Es posible desarrollar software que realice un acceso único a diferentes recursos de la red sin importar si están basados en LDAP o en algún otro protocolo. También es posible generar secuencias de comandos que puedan ser ejecutadas por los administradores.

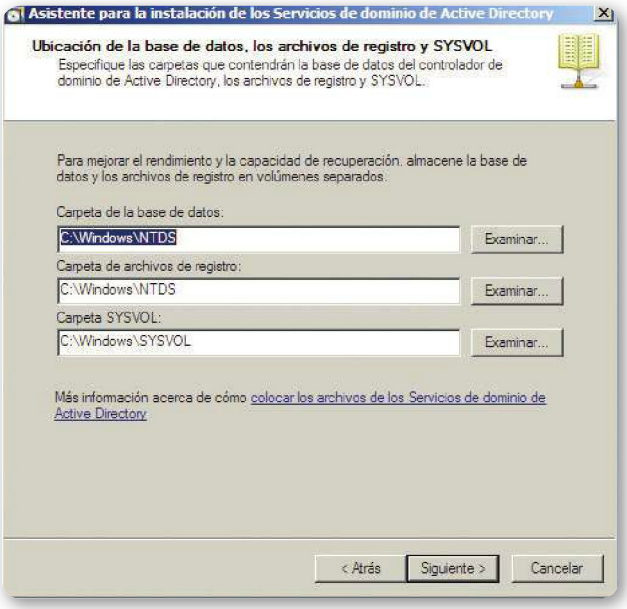


Figura 8. Active Directory posee una base de datos centralizada en donde se guarda la información de los objetos que pertenecen a un dominio.

NOVELL EDIRECTORY

Una eficiente alternativa para Active Directory es Novell eDirectory, un sistema multiplataforma que se puede correr sobre cualquier sistema operativo Linux, AIX, Solaris, Novell Netware, UNIX, y además integra LDAP v.3 en forma nativo. Se trata del precursor en materia de estructuras de directorio, ya que fue introducido en 1990 con la versión de Novell Netware 4.0.

Requisitos para la instalación

Antes de instalar Active Directory, debemos asegurarnos de que la computadora que va a ser configurada como controlador de dominio (*Domain Controller*) cumple con los requisitos de hardware y de sistema operativo necesarios para su correcto funcionamiento. Además, el controlador de dominio debe tener acceso al servidor DNS, y el software de este debe soportar la integración con Active Directory. Por lo general, se instala la solución DNS de Microsoft.

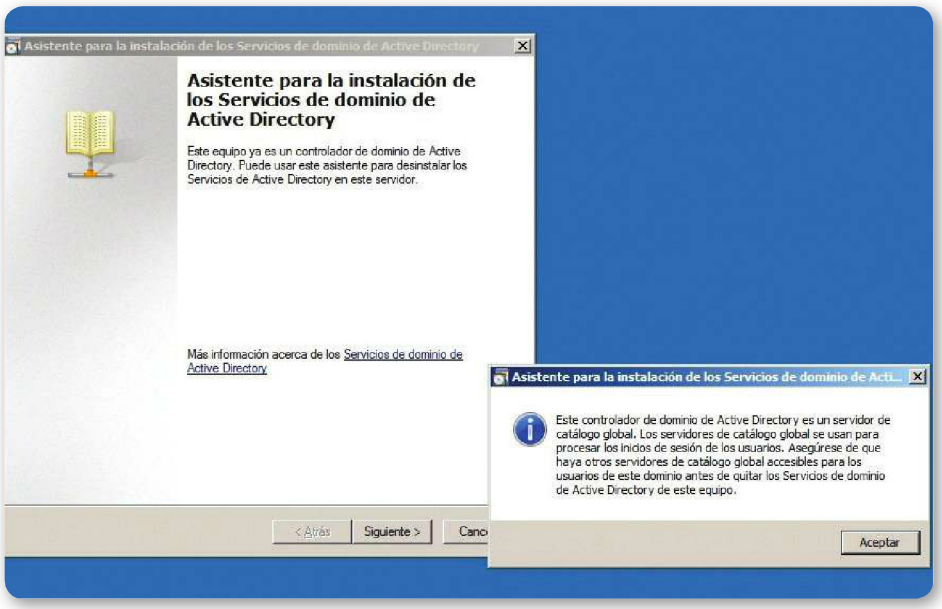


Figura 9. Los servidores de Active Directory pueden ser configurados como servidores de catálogo global para procesar los inicios de sesión de los usuarios.

- Es necesario contar con cualquier versión de servidor de Windows instalado, como Windows 2000 Server, Windows 2003 Server en sus diferentes versiones o Windows 2008. Para Windows 2003 Server hay que tener instalado el Service Pack 1.
- Se requiere la instalación del protocolo TCP/IP configurado de forma manual en lo que se refiere a los parámetros de la interfaz o placa de red, es decir que dichos parámetros no sean asignados de manera dinámica por un servidor DHCP.
- Tiene que haber uno o más servidores DNS dentro de la red donde se desea implementar AD, para resolver la dirección de los distintos recursos presentes en los dominios.

- Se necesita un mínimo de 250 MB de espacio en disco, 200 MB para la base de datos de Active Directory y 50 MB para los archivos logs de transacciones de Active Directory. Los requisitos del tamaño del archivo para la base de Active Directory y los archivos log dependen del número y del tipo de objetos en el dominio. Se requiere espacio adicional si el controlador es un servidor de catálogo global.
- Se precisa una partición o volumen con formato NTFS como sistema de archivos. La partición NTFS se requiere para la carpeta SYSVOL.

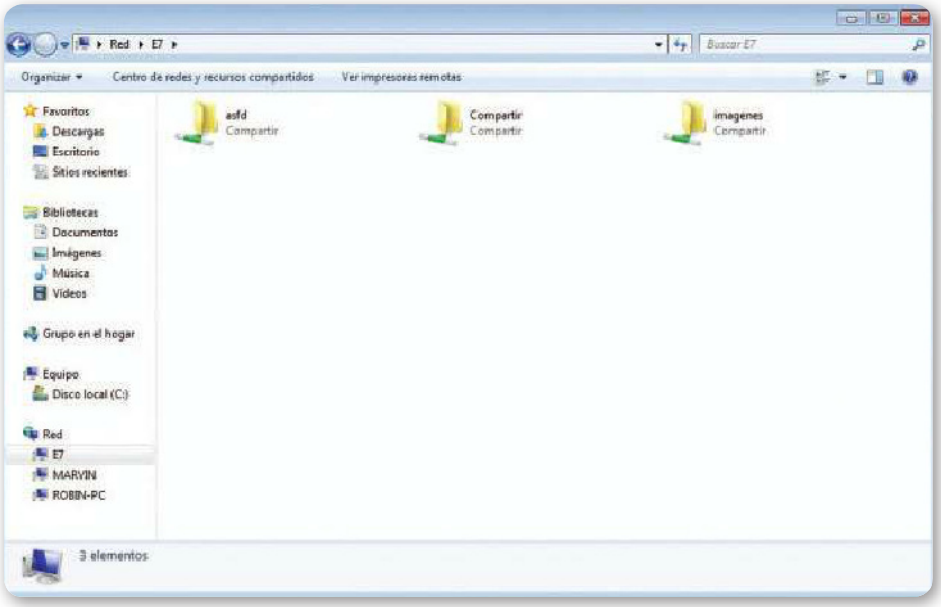


Figura 10. Samba es una alternativa de código abierto mediante la cual las computadoras basadas en UNIX puedan compartir recursos con computadoras Windows de forma transparente.

Derechos y restricciones

Una vez que hayamos implementado el dominio Active Directory, ¿cómo configuramos nuestro dominio de manera que cada usuario posea los permisos para realizar solo las tareas que necesita y se eliminen los riesgos de efectuar acciones no deseadas? Antes de adentrarnos en las opciones de seguridad del dominio Active Directory, es necesario conocer, desde el punto de vista de la seguridad, los distintos tipos de objetos que utilizaremos.

Usuarios

Este tipo de objetos representa a una persona que emplea algún servicio en los equipos del dominio. Siempre tenemos que tratar de que cada persona que ingrese en alguno de ellos tenga su propio usuario, ya que esto facilita la asignación de políticas personalizadas y el seguimiento de las acciones de cada uno.

> ES NECESARIO QUE CADA PERSONA INGRESE O UTILICE LOS EQUIPOS CON SU PROPIO USUARIO

Los usuarios de un dominio Active Directory se administran mediante el complemento **Usuarios y Equipos** de Active Directory, desde donde podemos realizar todas las tareas relacionadas con los objetos de tipo usuario, como crear, modificar y borrar cuentas, así como también modificar las contraseñas en caso de que alguna persona olvide sus datos de ingreso.

Grupos

Si bien tenemos que asignar una cuenta de usuario a cada persona para poder establecer políticas personalizadas, esto no quiere decir que las opciones del dominio vayan a asignarse a cada uno de manera individual.

Los grupos permiten asignar políticas o permisos a un conjunto de usuarios; de este modo, evitamos problemas en muchas situaciones. Un ejemplo sería cuando un usuario cambia de sector en una empresa; si tenemos los permisos y políticas definidos por usuario, deberemos modificar, en la cuenta de la persona, los permisos y políticas para que concuerden con su nuevo rol. En cambio, si organizamos nuestra política de seguridad utilizando grupos, bastará con cambiar el usuario al grupo que representa el sector al que fue asignado.

ALTERNATIVAS A ACTIVE DIRECTORY

Entre las otras alternativas a Active Directory existentes encontramos a Sun Java ES Directory Server y OpenDS; el primero está basado en java y el segundo fue desarrollado en C. Es importante mencionar que Sun Java ES Directory Server es un producto de Sun Microsystems y OpenDS se presenta como una eficiente alternativa de código abierto.

Los grupos se administran desde el complemento Usuarios y Equipos de Active Directory, donde podremos cambiar todos los parámetros de los objetos del tipo grupo, como nombre, miembros y subgrupos.

Equipos

Para que una PC o servidor forme parte del dominio Active Directory, debe existir un canal seguro mediante el cual se realicen las tareas de gestión centralizada de la seguridad, como la autenticación de usuarios o la autorización de acceso a un recurso compartido.

Con el fin de establecer el mencionado canal seguro, tenemos que "unir" los equipos al dominio. Esta acción se realiza mediante un usuario del dominio Active Directory que posea los privilegios apropiados, y tiene como finalidad delegar la gestión de la seguridad en el dominio.

> ES NECESARIO UNIR CADA UNO DE LOS EQUIPOS DESEADOS AL DOMINIO DE ACTIVE DIRECTORY

Una vez unidos al dominio, se crea una cuenta que identifica a cada equipo; esta cuenta es un objeto del tipo **Equipo**. Las cuentas de equipo se administran del mismo modo que las de usuario, desde el complemento **Usuarios y Equipos**.

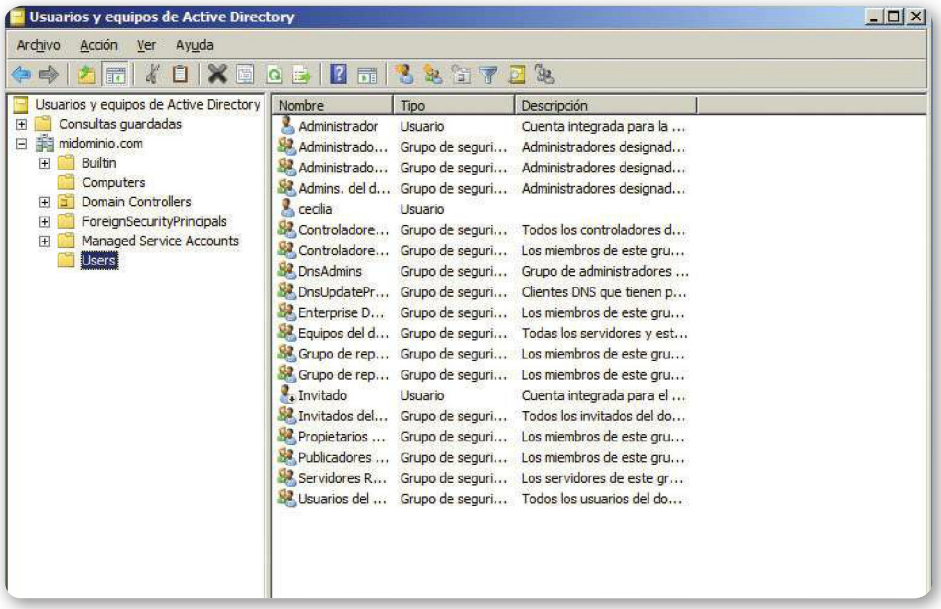


Figura 11. Mediante el administrador de usuarios y equipos de Active Directory, se gestionan los grupos, las cuentas de Usuario y las de Equipo.

Unidades organizativas

Las unidades organizativas son contenedores que nos permiten organizar el resto de los objetos (por ejemplo, usuarios, grupos y equipos) y, a la vez, vincularlos a las políticas de grupo, a fin de modificar las opciones de configuración que creamos necesarias, incluidas las referidas a la seguridad. Al igual que los usuarios, grupos y equipos, las unidades organizativas se administran desde el complemento Usuarios y Equipos de Active Directory.

Políticas de grupo

Existe una gran cantidad de opciones relacionadas con los usuarios y equipos de nuestro dominio Active Directory; en este caso, nos interesan las que se refieren a la seguridad. Las opciones de los usuarios y equipos se gestionan mediante la herramienta Políticas de Grupo.

A través del uso de políticas de grupo, administraremos de forma centralizada, eficiente y escalable los parámetros de los miembros de nuestro dominio Active Directory.

> MEDIANTE LAS POLÍTICAS DE GRUPO ADMINISTRAREMOS LA RED EN FORMA CENTRALIZADA

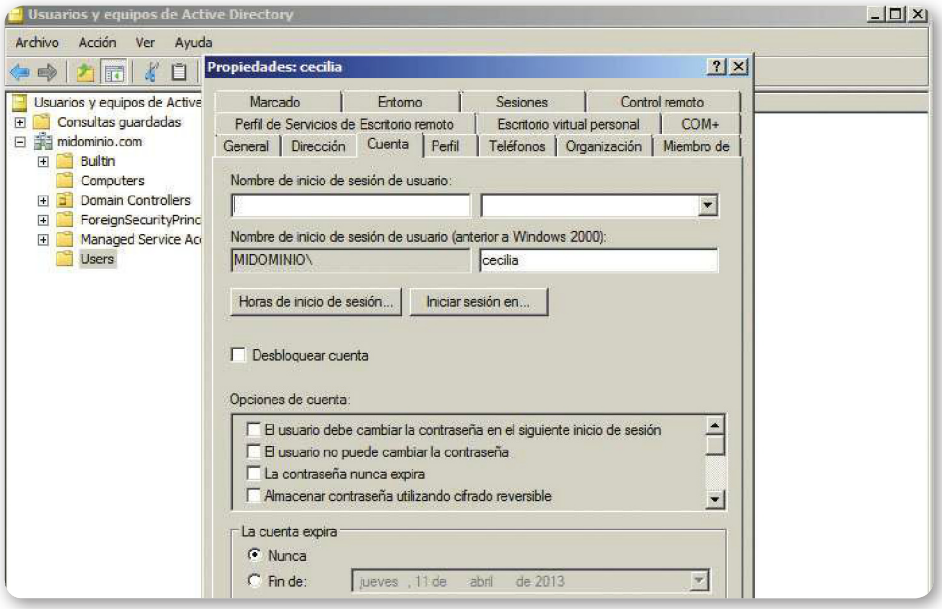


Figura 12. En el dominio Active Directory hay una gran cantidad de parámetros para establecer en los objetos de tipo Usuario.

Clasificación de las políticas de grupo

El número de opciones de configuración que podemos administrar mediante políticas de grupo es enorme. A medida que evoluciona la plataforma Microsoft Windows, se incorporan otras funcionalidades que aprovechan las características de las nuevas versiones de Windows, tanto en las versiones cliente (Windows XP, Windows Vista, Windows 7 y Windows 8) como en las versiones para servidor (Windows Server 2000, 2003, 2008 y 2012).

Existen 18 categorías de políticas de grupo:

- **Plantillas administrativas**: son directivas que tienen el objetivo de configurar el Registro de Windows, donde se almacenan las opciones de funcionamiento de una gran cantidad de aplicaciones, servicios y componentes.

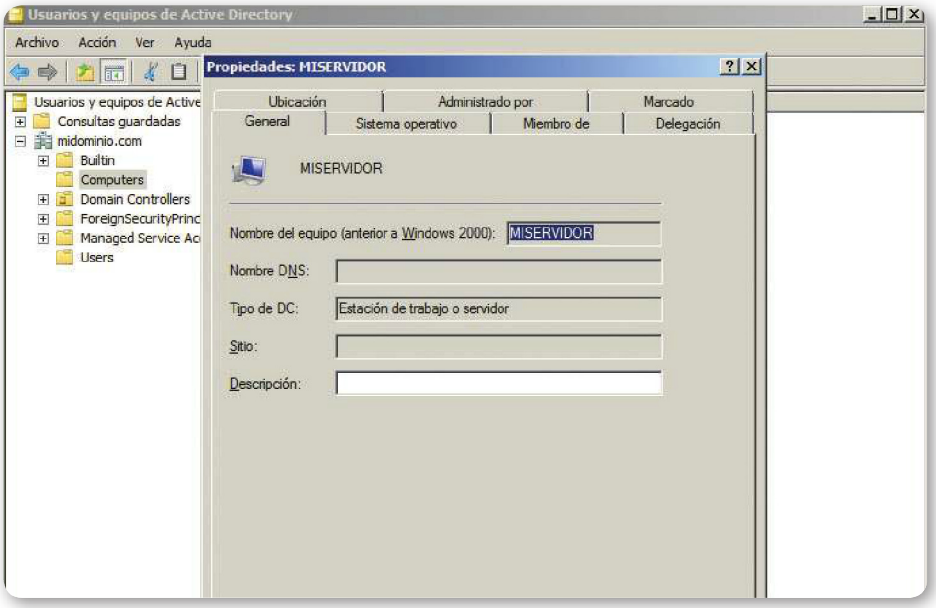


Figura 13. Cada equipo que forma parte del dominio Active Directory está representado por una cuenta de Equipo.

- **Opciones de seguridad**: abarca las opciones destinadas a establecer los parámetros de seguridad de los equipos y usuarios miembros del dominio; por ejemplo, mediante una política de seguridad de esta categoría, podemos establecer el máximo número de intentos en que un usuario puede ingresar incorrectamente la contraseña, luego de los cuales la cuenta se bloquea.

- **Configuración de red cableada**: abarca las opciones relacionadas con las redes cableadas, como los parámetros vinculados a la protección de acceso por red (NAP).
- **Configuración de red inalámbrica**: en esta categoría se encuentran las opciones referidas a las redes inalámbricas, como los tipos de encriptación soportados (WPA, WPA2 etc.).
- **Scripts**: mediante políticas de grupo, podemos establecer pequeños programas para que se ejecuten en algún instante específico, por ejemplo, cuando un usuario ingrese a un equipo mediante su usuario y contraseña.

> ES POSIBLE EJECUTAR LOS SCRIPTS MEDIANTE LAS POLÍTICAS DE GRUPO

- **Políticas de grupo de instalación de software**: permiten la instalación de software en las PCs o servidores desde los controladores de dominio.
- **Redirección de carpetas**: es posible redireccionar carpetas de los perfiles de los usuarios a los fines de cambiar su ubicación original. Una finalidad de este tipo de políticas es centralizar las carpetas **Mis documentos** de los usuarios en un servidor central.
- **Cuotas de disco**: existen políticas para regular el uso en las carpetas que consideremos críticas; de este modo, logramos controlar el uso del espacio en disco.
- **Opciones del sistema de archivos encriptado**: permiten establecer los parámetros en caso de que necesitemos encriptar alguna partición en los servidores o PCs de nuestro dominio.
- **Mantenimiento de Internet Explorer**: dado que muchas de las amenazas de seguridad informática provienen de Internet, conviene centralizar las opciones de configuración de Internet Explorer.
- **Políticas de restricción de software**: por medio de estas

DIRECTIVAS DE GRUPO

Directiva de grupo se presenta como un conjunto de reglas que se encargan de controlar el entorno de trabajo de cuentas de usuario y cuentas de equipo en sistemas Windows. Esta opción proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y también la configuración de los usuarios que se encuentren en un entorno de Active Directory.

políticas, controlamos los paquetes que pueden ejecutarse en los equipos de nuestro dominio.

- **Calidad de servicio basado en políticas**: configura la prioridad de los servicios a nivel de red.
- **Políticas IPSec**: permiten establecer parámetros relacionados con la red segura por Internet.
- **Búsqueda de Windows**: cambian opciones vinculadas a la búsqueda dentro de las PCs y servidores de nuestro dominio.
- **Distribución de conexiones a impresoras**: distribuye a los clientes del dominio las conexiones a las impresoras; estas políticas son especialmente útiles en redes donde existen muchos dispositivos de impresión.
- **Archivos sin conexión**: especifican los parámetros para la sincronización de archivos para los clientes que en algún momento se desconectan del dominio para funcionar en redes distintas. Un ejemplo de la aplicación de estas políticas son los equipos portátiles.
- **Preferencias - Extensiones de Políticas de grupo**: a partir de Windows 7 y Windows Server 2003, se incluye una serie de preferencias que nos permiten afinar la configuración de los equipos miembro de nuestro dominio.
- **Aceleradores de Internet Explorer**: estas políticas permiten establecer los parámetros de los aceleradores de Internet Explorer, una característica introducida a partir de Windows 7.

Descripción

Cada política de grupo tiene dos nodos o partes: la parte relacionada al usuario y la parte relacionada al equipo. Ambas abarcan las opciones que afectan a los objetos de tipo Usuario y de tipo Equipo,

SITIOS DE INTERÉS

Las políticas de grupo abarcan una infinidad de parámetros de seguridad y de aplicación general, a la vez que van evolucionando de la mano de los sistemas operativos Windows. Resulta indispensable tener una lista de sitios de referencia. Uno de los más importantes es, sin lugar a dudas, el sitio de Microsoft TechNet (**http://technet.microsoft.com**) y otro es el de **GroupPolicy Central** (**www.grouppolicy.biz**).

respectivamente, los cuales deben estar contenidos en la Unidad Organizativa a la que se vincula la política de grupo. Las políticas de grupo pueden establecerse a nivel local (en cada equipo), a nivel de sitio, a nivel de dominio o a nivel de unidad organizativa.

Administración de políticas de grupo

Para administrar las políticas de grupo utilizaremos la herramienta denominada **gpedit.msc**, esta aplicación proporciona una forma sencilla para editar las políticas de grupo a nivel local en cada equipo, mientras que, para trabajar con las políticas de grupo a nivel de dominio, recurriremos a la herramienta **Consola de Administración de Políticas de Grupo** (**GPMC**). Mediante la Consola GPMC podremos crear, modificar y borrar políticas de grupo, así como también vincularlas a las unidades organizativas, sitios y dominios.

Aplicación

Dependiendo del nivel en el que establecemos las políticas de grupo, será la prioridad de ejecución. Como es lógico, las políticas que definamos a nivel local son las que tienen menos prioridad de ejecución, ya que la finalidad del dominio es que los equipos deleguen la gestión de la seguridad en los controladores de dominio.

El orden en el que se aplicarán las políticas de grupo es el siguiente: primero se aplican las vinculadas a nivel de sitio, luego se cargan las que están vinculadas al dominio, después las relacionadas a la unidad organizativa a la que pertenezca el usuario o el equipo y, finalmente, las políticas de grupo definidas de manera local.

> EN PRIMER LUGAR SE APLICAN LAS POLÍTICAS VINCULADAS AL NIVEL DEL SITIO

Debemos tener en cuenta que siempre que existan conflictos entre dos o más políticas de grupo, tendrán precedencia aquellas vinculadas al nivel de mayor prioridad. Por ejemplo, ante un conflicto en una opción definida en una política de grupo vinculada a nivel de dominio y otra vinculada a nivel de unidad organizativa, tendrá precedencia la opción configurada en la política de grupo vinculada a nivel de dominio.

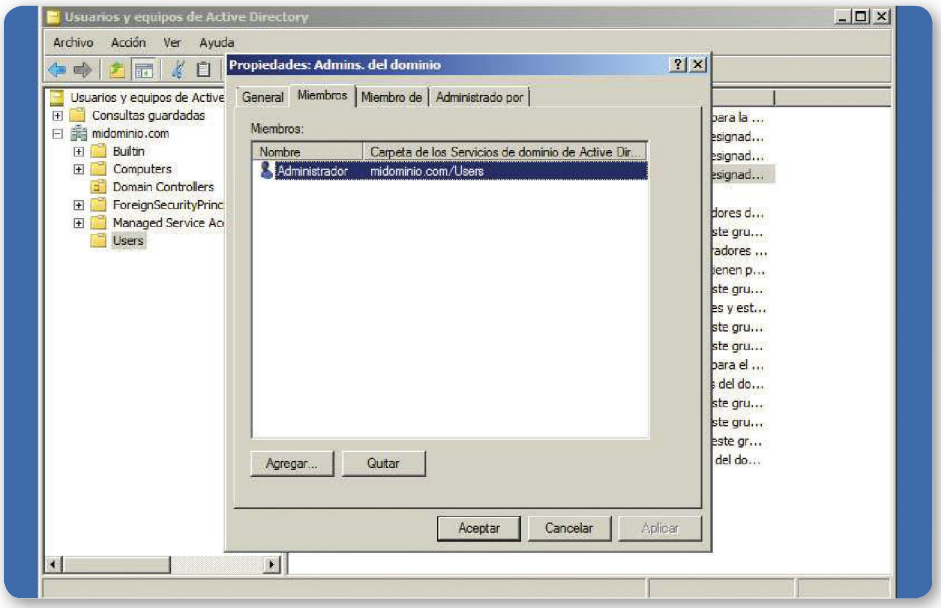


Figura 14. Los objetos del tipo Grupo nos permiten organizar los objetos de nuestro dominio y administrarlo de manera más eficiente.

Herencia

Las políticas de grupo se heredan desde un contenedor hacia los elementos que contiene. Por ejemplo, si definimos una OU con nombre Sistemas y, dentro de ella, definimos otra OU llamada Desarrollo, las políticas de grupo vinculadas a la OU Sistemas serán heredadas por la OU Desarrollo, ya que la primera contiene a la segunda.

La herencia puede bloquearse mediante los parámetros de configuración de las políticas de grupo.

Herramientas para la resolución de problemas

Debemos considerar que existen numerosas herramientas para ayudarnos a resolver los inconvenientes que puedan surgir durante la implementación de las políticas de grupo.

Una de las herramientas que no nos puede faltar es **gpresult**, que nos permite calcular el resultado de las políticas de grupo aplicadas a un equipo teniendo en cuenta las distintas políticas de grupo y los diferentes niveles a los cuales se vinculan.

Otra herramienta para tener en cuenta es **gpupdate**, mediante el cual actualizamos inmediatamente las políticas de grupo aplicadas a un equipo, visualizando en detalle los niveles y políticas que se aplican.

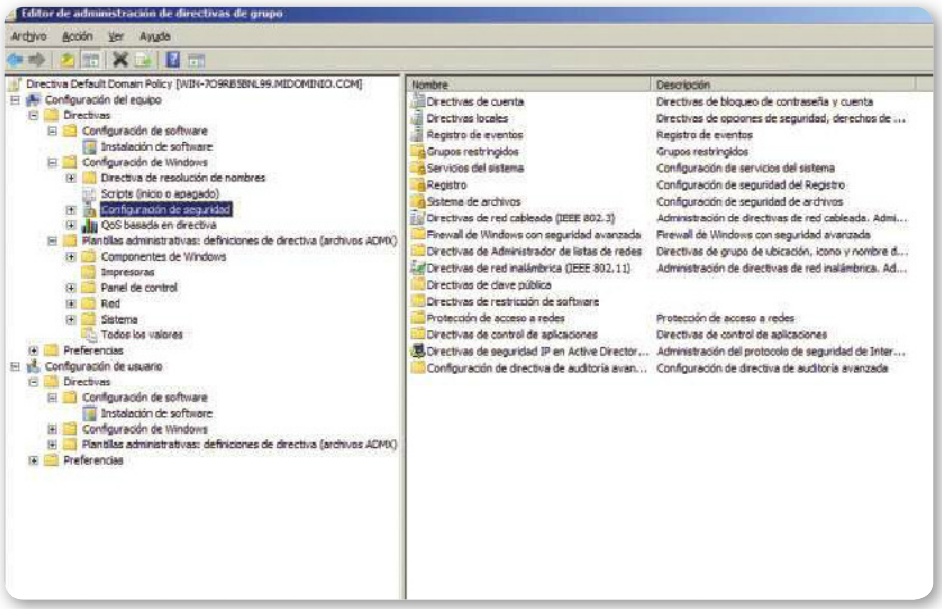


Figura 15. Las políticas de grupo permiten gestionar las opciones de configuración de los equipos que forman parte del dominio.

Administración avanzada (AGPM)

Entre todas las herramientas que el sistema operativo nos brinda para controlar y dirigir los permisos dentro de la red, encontramos una que nos permite delegar acciones conteniéndolas en un mismo lugar, y nos permite revisar, editar, aprobar y generar nuevas políticas en un mismo aplicativo. La herramienta que se encarga del control de las políticas de grupo funciona como el manager de estas dentro del sistema operativo.

Esta aplicación funciona como cliente/servidor, y permite realizar la administración avanzada de las Directivas de Grupo (**AGPM**, **Advanced Group Policy Managment**), que brinda un control de cambios integral y edición sin conexión. Es un componente principal dentro del paquete de optimización de Microsoft Desktop (**MDOP**, **Microsoft Desktop**

Optimization Pack). MDOP ayuda a las organizaciones a reducir el costo de desarrollo de aplicaciones, utilizar aplicaciones como servicios y mejorar la administración de configuraciones de escritorio.

La aplicación **AGPM** flexibiliza la administración de las políticas de grupos, principalmente, cuando estas se encuentran en entornos de red complejos. Una de las principales características es la posibilidad de realizar cambios en los objetos de las políticas de grupos (**Group Policy Objects**, **GPO**) de manera offline, auditar los cambios y encontrar variaciones entre las distintas versiones de los GPO. Nos otorga informes detallados para controlar cambios en las versiones, capturas en el historial y restauración de versiones antiguas velozmente.

> LA ADMINISTRACIÓN AVANZADA DE LAS GPO PERMITE REALIZAR CAMBIOS DE MANERA OFFLINE

Edición offline

Los archivos de AGPM permiten el almacenamiento offline de los GPO, y esto habilita que los cambios realizados en los GPO no afecten el área de trabajo hasta que terminemos su desarrollo. De esta manera, editaremos los objetos libremente, bajo nuestras normativas, sin afectar los procesos que estén funcionando en ese momento. Una vez que finalicemos los cambios, estos GPO sustituirán a los antiguos mediante una sincronización. Si estas actualizaciones no resultan favorables, es posible restituir los cambios realizados fácil y rápidamente.

Integración GPMC

El AGPM tiene un componente de cliente/servidor que se instala de manera independiente. Primero instalamos el componente servidor en

APLICAR POLÍTICAS

Una vez que hayamos definido nuevas políticas podremos reiniciar el servidor o equipo para que se aplique la nueva configuracion de políticas. Pero también es posible ejecutar el siguiente comando para no tener que reiniciar el equipo: **gpupdate.exe /force /boot /logoff**.

un sistema que tenga acceso a las políticas que queremos administrar y, luego, instalamos el componente de cliente en un sistema que posea administradores de las políticas de grupo que tengan permitido revisar, editar y desarrollar las GPO.

El componente del cliente se entrega con la consola de administración de las políticas de grupo (*Group Policy Managment Console*, GPMC). Entre sus opciones encontramos la posibilidad de realizar numerosas modificaciones e, incluso, tomar control de los GPO sin dominio (GPO que no estén en archivo). A través de la consola podremos delegar dominios y roles a los usuarios AGPM.

> EL COMPONENTE CLIENTE SE ENTREGA CON LA CONSOLA DE ADMINISTRACIÓN DE POLÍTICAS DE GRUPO

Control de cambios

El control de cambios nos brinda un detallado listado de la historia de los GPO durante su ciclo de vida y los cambios que han sufrido. La interfaz es amigable con el usuario y con los administradores experimentados con este tipo de herramientas. De esta manera, si los GPO nos presentan errores o no obtenemos los resultados esperados, podemos revisar los puntos clave donde fueron modificados y, así, corregir los posibles incidentes. Además de controlar el historial de los GPO, obtenemos a su vez un listado de las actividades relacionadas con él.

Delegaciones basadas en roles

Podemos delegar tareas y permisos a administradores y sectores especializados; esto quiere decir, asignar usuarios que puedan realizar

VALORES POSIBLES

Es importante recordar que la mayoría de las opciones que corresponden a las Directivas de Grupo presentan tres valores posibles: **Activado**, la cual indica que esta opción ha sido configurada; **Desactivado**, que se encarga de indicar que esta opción ha sido desactivada y **Sin configurar**, que informa que esta opción no ha sido activada ni desactivada. Al elegir Sin configurar, no especificaremos ninguna opción.

determinadas tareas para que ellos hagan sus propios cambios. Las modificaciones que hagamos en AGPM luego serán establecidas en un modelo de revisión, aprobación y edición.

Un administrador AGPM tiene control completo de los archivos de AGPM, mientras que un Administrador de rol AGPM define tres roles especiales para sostener el modelo de delegación: revisor, que pueden ver y comparar los GPO pero no pueden editarlos ni desarrollarlos; editor, que puede ver y comprarlos, chequearlos desde archivo, editarlos y levantarlos al archivo, a la vez que solicitar el desarrollo de GPOs nuevos; y aprobador, que aprueba la creación del desarrollo de los GPO (si un aprobador crea o desarrolla un GPO, este es aprobado de inmediato).

> EL ADMINISTRADOR AGPM POSEERÁ EL CONTROL COMPLETO DE LOS ARCHIVOS DE AGPM

Búsqueda y filtro

Es importante mencionar que hay una característica que permite filtrar la lista de los GPO existentes mediante nombres, estado o comentarios; incluso, se puede filtrar la lista para mostrar los GPO que fueron cambiados por un usuario particular en una fecha específica. Los resultados pueden ser precisos o parciales.

La versión más utilizada de AGPM es la 4.0, y se aplica a los sistemas Windows 7, Server 2008, Server 2008 R2 y Vista. En estas versiones se incluyen herramientas para un manejo más limpio a través de la búsqueda y filtrado de GPO, que nos permite encontrarlos por medio de atributos específicos en la lista completa. La integración con otros árboles se realiza gracias a la exportación e importación de un bosque

INTEGRACIÓN

En todas las versiones de sistemas operativos orientados a servidores, muchas herramientas fueron integrándose unas a otras, de modo que la gestión y la administración de permisos y usuarios sean más eficientes. El **AGPM** incluye muchas soluciones en un mismo paquete, lo cual permite tener un control de cambios integral, y hacer un rastreo más eficiente y preciso de cambios, errores y mejoras. Se ha puesto a disposición el AGPM como parte del pack de optimización de **Microsoft Desktop**.

al dominio de un segundo mediante archivos de tipo CAB, y levantando en el nuevo dominio directamente de archivo en archivo.

Con respecto a otras versiones de sistemas operativos, existen algunos limitantes, principalmente, entre Windows 7 y Vista, debido a que algunos parámetros son incompatibles porque algunas características fueron solo detalladas para el primero, y no, para el segundo.

> LA INTEGRACIÓN SE REALIZA MEDIANTE LA EXPORTACIÓN E IMPORTACIÓN DEL BOSQUE

RESUMEN

En este capítulo pudimos analizar en detalle las características y opciones que nos ofrece Windows Server, también revisamos la asignación de derechos y la aplicación de restricciones. Por otra parte profundizamos en las ventajas de Active Directory y aprendimos cómo es posible administrar las Directivas de Grupo en forma avanzada.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice a Windows Server.
2. ¿De qué forma Windows Server gestiona la seguridad?
3. Mencione las características adicionales de Windows Server.
4. ¿Cómo se integra Windows Server con otros sistemas operativos?
5. ¿Qué es Active Directory?
6. ¿Qué protocolos utiliza Active Directory?
7. ¿Cómo funciona Active Directory?
8. Caracterice a los usuarios como objetos de Active Directory.
9. ¿Qué son los grupos?
10. ¿Para qué sirve una política de grupo?

EJERCICIOS PRÁCTICOS

1. En una implementación de Active Directory identifique algunos objetos.
2. Utilice una interfaz de servicio o ADSI.
3. Efectúe una instalación de Active Directory.
4. Agregue usuarios a su dominio.
5. Administre las políticas de grupo en Windows Server.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*03

Sistemas GNU/Linux

En este capítulo revisaremos la administración de un sistema Linux. Conoceremos los comandos de consola básicos y realizaremos diagnósticos de red y procesos. También detallaremos la seguridad a nivel de kernel.

↗↗↗

Servidores basados en GNU/Linux

GNU/ Linux es un sistema perteneciente a la familia UNIX, que se distribuye en forma libre, es posible acceder a su código y modificarlo. Una de las grandes ventajas de la implementación de servidores GNU/Linux es el ahorro en los costos de instalación, pero también se requiere una mayor especialización por parte del personal informático.

PARA INSTALAR LINUX LO PRIMERO ES ELEGIR UNA DE LAS DISTRIBUCIONES DISPONIBLES

La puesta en marcha de un servidor basado en GNU/Linux demanda dividir el proceso en varias etapas, de las cuales las más importantes son: **instalación**, **servicios básicos** y **servicios avanzados**. Para realizar la instalación tenemos que elegir una distribución, de modo que será importante comparar las opciones que nos ofrece el mercado, luego de lo cual iniciamos la instalación mínima y, posteriormente, realizamos el trabajo de configuración.

Figura 1. Suse Linux Enterprise es una de las opciones recomendadas para implementar un servidor.

Servicios

La habilitación y configuración de los **servicios básicos** nos permitirá realizar las tareas más importantes según las necesidades de la red. Por ejemplo, precisamos integrar el equipo en una red,

ofrecer un servidor web con Apache o configurar un servidor FTP; también podemos necesitar funciones como proxy para controlar las conexiones y acelerar la navegación de los equipos que se conectan como clientes.

Los **servicios secundarios** son aquellos que nos permiten, por ejemplo, hacer que el servidor web acepte conexiones internas y también desde Internet, entregue soporte para PHP y CGI, y acepte conexiones por SSH con el fin de administrar la computadora desde cualquier lugar.

> PUEDE SER NECESARIO CONTAR CON PROXY PARA CONTROLAR LAS CONEXIONES

Figura 2. La conexión y administración de una impresora puede realizarse mediante asistentes gráficos.

Distribuciones

La elección de la distribución que utilizaremos es una tarea que nos demandará algo de tiempo, ya que existen muchas opciones disponibles. En este punto debemos tener en cuenta diversas características que nos permitirán comparar las ventajas y desventajas de cada una de ellas, hasta tomar la decisión según nuestras necesidades.

Los puntos que compararemos en las diversas distribuciones GNU/Linux disponibles son los siguientes:

- **Precio**: tengamos en cuenta que, aunque las distribuciones GNU/Linux son libres, no todas se distribuyen en forma gratuita, si bien el precio suele ser menor al que encontramos en otros sistemas operativos, por ejemplo, de la familia Windows. Las distribuciones incluyen un gran número de soportes, los cuales abarcan todos los programas necesarios. Para la mayoría de ellas, como Debian, podemos acceder a su sitio web y descargar todos los CDs o DVDs que corresponden al sistema.

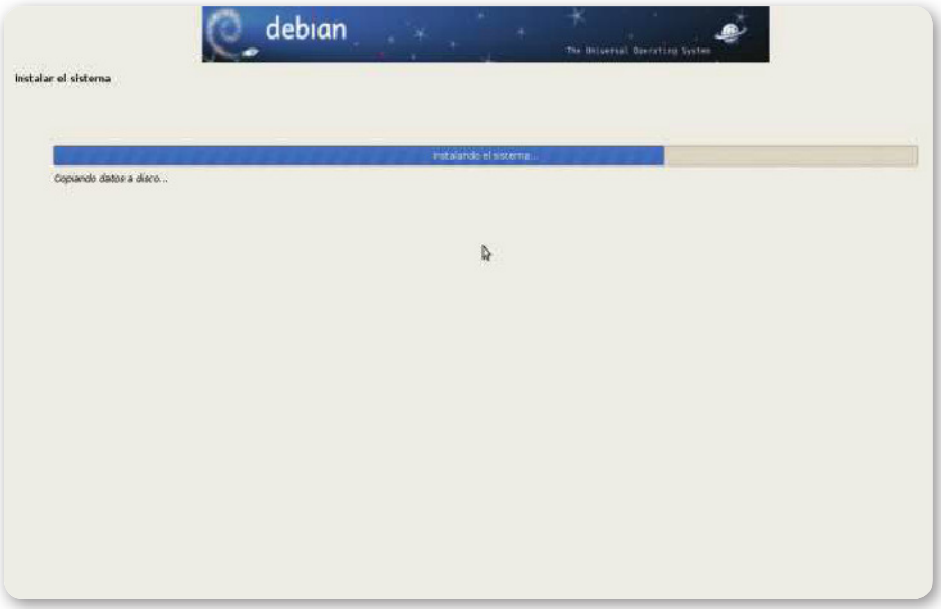


Figura 3. La instalación de Debian puede hacerse mediante un modo gráfico o de texto.

- **Soporte técnico**: en general, las distribuciones Linux ofrecen un soporte técnico para los usuarios que adquieran el sistema. Si optamos por descargar las imágenes de los discos, tendremos que buscar soporte y ayuda en foros o grupos de usuarios.

DEBIAN

Debian, más conocido como **Proyecto Debian** se presenta como una distribución Linux y una comunidad conformada por desarrolladores y usuarios que se encargan de mantener un sistema operativo GNU basado completamente en software libre.

- **Versión del kernel**: la versión del kernel o del núcleo del sistema operativo es importante para enfrentar problemas de compatibilidad o de seguridad. Siempre es necesario contar con la última versión disponible. Si elegimos una distribución que no posee un kernel actualizado, tendremos que actualizarlo en forma manual, un procedimiento bastante tedioso y no exento de problemas.
- **Tipo de instalación**: no todas las distribuciones ofrecen ambientes gráficos para realizar la instalación; en algunas de ellas, tendremos que utilizar la consola, razón por la cual, si no somos usuarios expertos, será una buena idea seleccionar una distribución que simplifique el proceso.
- **Gestor de ventanas**: en implementaciones de servidor no utilizaremos mucho el entorno gráfico, pero también puede ser una buena idea instalar algún gestor de ventanas sencillo, de esta forma estaremos preparados para enfrentar cualquier eventualidad.
- **Tipo de paquetes**: para instalar aplicaciones, según la distribución, podemos usar distintos tipos de paquetes: tar.gz (comprimidos llamados Tarball, contienen el código fuente del programa), RPM (se utiliza en forma original para RedHat, pero se ha implementado en otras distribuciones) y también paquetes DEB (formato propio de Debian, también usado por Ubuntu).
- **Otras opciones**: cada distribución se encuentra orientada a un público específico, por lo que debemos buscar las opciones adecuadas para implementar un servidor.

> NO TODAS LAS DISTRIBUCIONES GNU/LINUX SE INSTALAN DESDE UN AMBIENTE GRÁFICO

La elección de la distribución para nuestro servidor es una tarea personal, pero algunas opciones recomendadas son: **Debian**, **RedHat Enterprise** y **SUSE Linux Enterprise Server.**

Gestión de usuarios

Una de las tareas más básicas que tendremos que realizar es la gestión de usuarios, para lo cual recurriremos a la consola de comandos.

Debemos tener presente que existen dos tipos de usuarios: el administrador, o root; y los usuarios comunes.

Es necesario considerar que para realizar las tareas de administración, necesitaremos poseer un perfil de administrador o root. Para realizar la administración de usuarios será necesario que realicemos la creación y posterior gestión de las cuentas de usuarios, grupos y la asignación de permisos.

Esta gestión se realizará cuando debamos establecer políticas de seguridad en el equipo o en la red, o cuando deseemos gestionar servidores NFS, FTP o web.

Para comenzar, vamos a gestionar los permisos, mediante el comando **ls -l**, tal como vemos a continuación:

```
$ ls -l
total 284
drwxr-xr-x 5 usuario usuario4096 2007-11-26 17:38 2006r3
drwxr-xr-x 5 root root 4096 2007-09-17 15:48 AlberTUX_LIVE
drwxr-xr-x 3 usuario usuario4096 2007-04-02 11:38 Beryl
drwxr-xr-x 2 usuariousuario4096 2007-12-14 15:05 bin
```

Las líneas poseen el siguiente formato del estilo:

{T} {rwx} {rwx} {rwx} {N} {usuario} {grupo} {tamaño} {fecha de creación} {nombre}

Campo **T**: indica qué tipo de archivo es.
Campo **{rwx}**: permisos que tiene el propietario.
Campo **{rwx}**: permisos que tiene el grupo.
Campo **{rwx}**: permisos del resto de usuarios.
Campo **{N}**: número de archivos/directorios que contiene.
Campo **{usuario}**: nombre del usuario al que pertenece el archivo.
Campo **{grupo}**: nombre del grupo al que pertenece.
Campo **{tamaño}**: tamaño.
Campo **{fecha}**: fecha de creación.
Campo **{nombre}**: nombre.

La administración de permisos se realiza mediante la siguiente estructura de comandos:

[chmod] [modo] [permisos] [fichero/s]

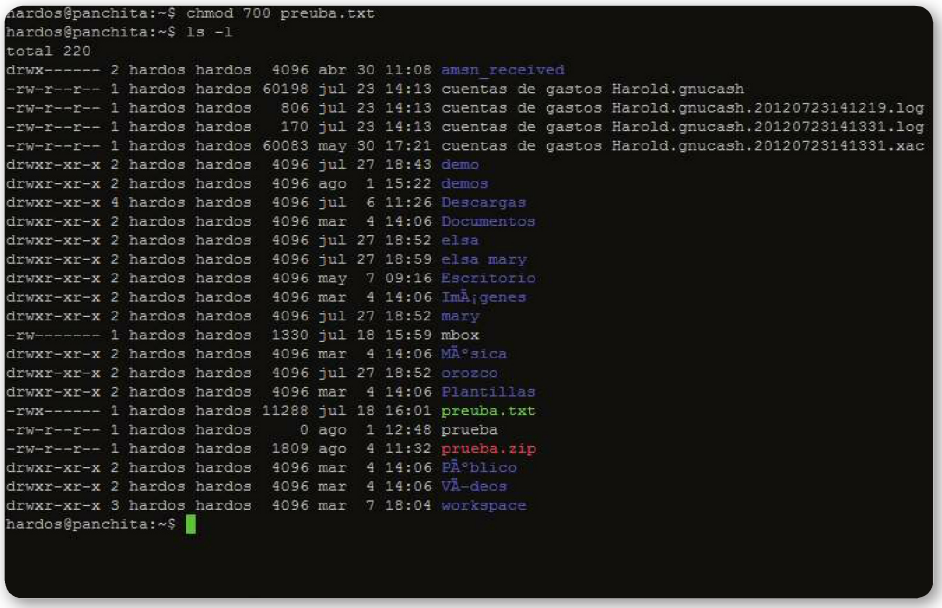


Figura 4. Aquí vemos un ejemplo de uso del comando **chmod**, para definir permisos en carpetas y archivos.

Un ejemplo de su uso es el siguiente:

$ chmod -R 755 mi_directorio
$ ls -l
$drwxr-xr-x 2 usuariousuario 4096 2007-07-13 13:57 mi_directorio

También podemos usar los siguientes modos para asignar permisos:

a: se aplicará a todos (all)
u: se aplicará al usuario (user)
g: se aplicará al grupo (group)
o: se aplicará a otros (other)
+: se añade el permiso
-: se quita el permiso
r: indica permiso de lectura
w: indica permiso de escritura
x: indica permiso de ejecución

Por ejemplo:

$ chmod -R o-rxmi_directorio

Para agregar un usuario usamos:

```
# addusernombre_usuario
Adding user 'pepito' ...
Adding new group 'pepito' (1001) ...
Adding new user 'pepito' (1001) with group 'pepito' ...
Creating home directory '/home/pepito' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
```

Luego de completar la serie de comandos que hemos mencionado, solo será necesario que ingresemos la contraseña que se asociará al usuario recién creado. Tengamos en cuenta que la sintaxis completa para la gestión de usuarios es la siguiente:

```
addusr [-c comentario] [-d home] [-e fecha] [-f dias] [-g grupo] [-G lista de grupos] [-m [-k template] | -M] [-n] [-o] [-p passwd] [-r][-s shell] [-u uid] usuario
```

Para eliminar un usuario utilizamos:

```
# deluser -R nombre_usuario
```

La opción **-R** eliminará el directorio home del usuario; sin ella, se eliminará la cuenta de usuario, y quedará el home.

Para crear un grupo y asignarle un usuario utilizamos:

```
# groupadd -r NuevoGrupo
# gpasswd –a nombre_usuarioNuevoGrupo
```

PERMISOS

Linux es un sistema operativo multiusuario, por lo que debemos ser muy cuidadosos al establecer los permisos para los recursos y usuarios. Los permisos que asignamos a cualquier archivo se componen de tres partes: los permisos del propietario, los permisos del grupo y los permisos del resto. De esta forma, podemos ver que un archivo pertenece a un determinado propietario, a un determinado grupo y, dependiendo de estos permisos, podremos o no acceder a él.

Figura 5. La gestión de usuario puede realizarse mediante la consola o utilizando la interfaz gráfica, en caso de que hayamos instalado un entorno de escritorio.

Recursos y unidades

Sin depender de la distribución de Linux que utilicemos, la gestión de recursos se realiza en forma similar. Es necesario considerar que entre las tareas que debemos tener en cuenta para administrar los recursos del sistema se encuentran mantener las unidades de disco, efectuar la gestión del sistema de archivos y también realizar el completo control de los recursos disponibles.

> PODEMOS UTILIZAR LA HERRAMIENTA FDISK PARA GESTIONAR LAS PARTICIONES

Como sabemos, las unidades de disco están divididas en particiones, las cuales almacenan el sistema que entrega la estructura en la cual se grabarán los archivos. Por ejemplo, el directorio root de un sistema de archivos puede ser montado en cualquier punto del sistema global, aunque generalmente se ubicará en /usr.

Una buena idea a la hora de gestionar particiones es utilizar la herramienta **fdisk**, cuya sintaxis es la siguiente:

```
fdisk [opciones] dispositivo
```

Se trata de una herramienta que se utiliza mediante un menú en modo texto, por lo que debemos seguir una serie de pasos tendientes a crear una partición; a continuación conoceremos un completo ejemplo de los comandos necesarios para usar **fdisk**:

```
Command (m for help): n
Command action
e  extended
p  primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-20805, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-20805, default 20805): +5G
Command (m for help): p
Disk /dev/hdb: 10.7 GB, 10737418240 bytes
16 heads, 63 sectors/track, 20805 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Device Boot   Start     End   Blocks  Id System
/dev/hdb1       1    9689   4883224+ 83 Linux
```

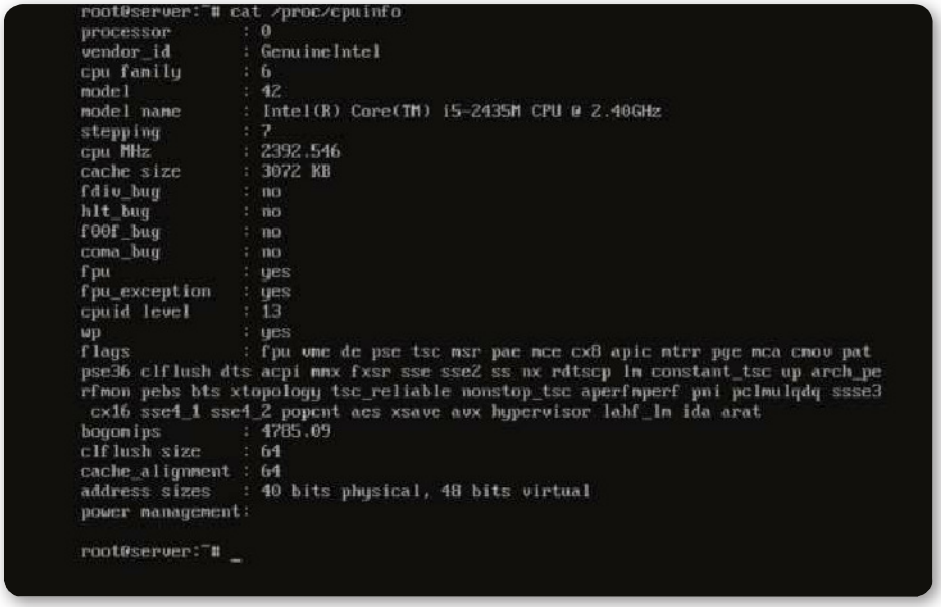


Figura 6. Visualización de las características de un procesador, muy utilizado en distribuciones como Gentoo, ya que usaremos estas variables obtenidas para la compilación de aplicaciones.

Otras opciones para gestionar las particiones son las siguientes:

- **cfdisk**: interfaz gráfica para la herramienta fdisk.
- **parted**: programa para crear, destruir, cambiar el tamaño, chequear y copiar particiones en forma sencilla.
- **qtparted**: programa gráfico para manejar particiones.

Las tareas de gestión del sistema de archivos son algo complejas y muy extensas, por lo que abordaremos un ejemplo sencillo para crear un sistema de archivos, utilizando el comando **mkfs.**

mkfs [-V] [-t filesystem] dispositivo [n_bloques]

Sus opciones son las siguientes:

-t filesystem: tipo de sistema de archivos que crearemos.
n_bloques: número de bloques usados para el sistema de archivos.

A continuación, vemos algunos ejemplos del uso de mkfs:

mkfs.ext2 o **mke2fs**: crea sistemas ext2.
mkfs.ext3: crea sistemas ext3.
mkfs.jfs, **mkfs.reiserfs**, **mkfs.xfs**: crea sistemas JFS, ReiserFS y XFS.
mkfs.msdos, **mkfs.vfat**: crea sistemas MS-DOS.
mkswap: crea un sistema de ficheros de intercambio o swap.

> MEDIANTE LA CONSOLA PODREMOS CONTROLAR LOS PROCESOS Y ADMINISTRAR TAREAS

Para terminar, es posible realizar el control de los procesos que se ejecutan en el servidor, así como otras tareas de administración importantes. Ahora veremos un listado de las opciones de consola que nos servirán en estas tareas:

$ free -m -s 3
Muestra el uso de memoria.

$ psaux
Muestra información de los procesos que están siendo ejecutados.

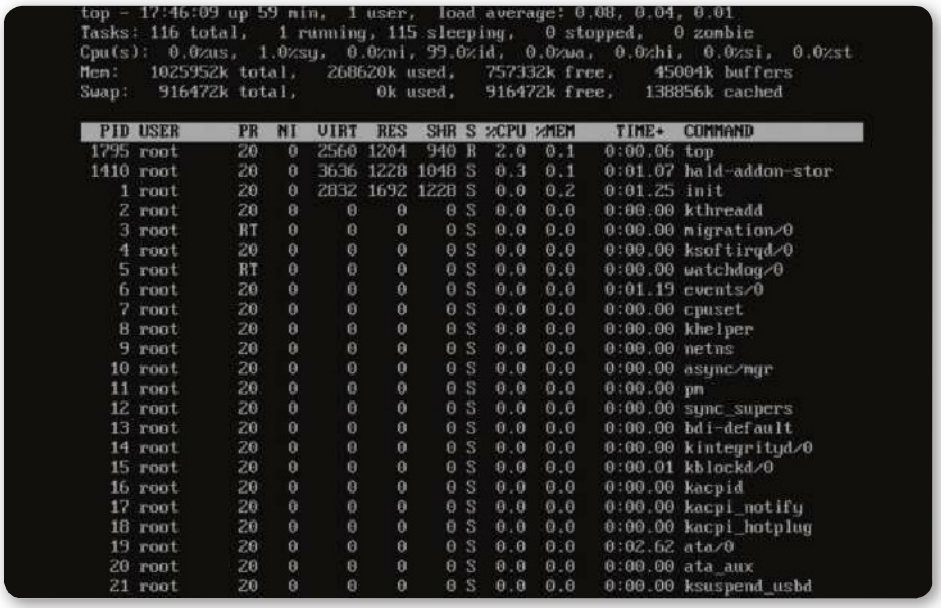


Figura 7. **Top** es una analogía del **Monitor de Recursos** de Windows, con la diferencia de que aquí podremos realizar modificaciones como un **`re-nice`** o reasignar prioridades.

$ top

Muestra información de los procesos ejecutados.

$ pstree

Muestra los procesos, en una estructura de árbol.

$ killall proceso

Se encarga de detener un proceso.

$ strace comando

Muestra las llamadas que un proceso ha realizado al sistema.

PING

El conocido **ping** (**Packet Internet Groper**) está presente en todos los sistemas operativos y plataformas. Envía paquetes **echo_request** a la dirección IP especificada, para comprobar que la conexión funciona. A diferencia de Windows, en Linux, por defecto, la cantidad de pings es infinita. La variable para limitarlos es **-c**, con la cantidad de paquetes **echo_request** que queremos enviar.

$ fuser -v archivo

Muestra los procesos que se encargan de usar un archivo o directorio.

$ lsof | less

Nos muestra el listado de los archivos abiertos por los procesos.

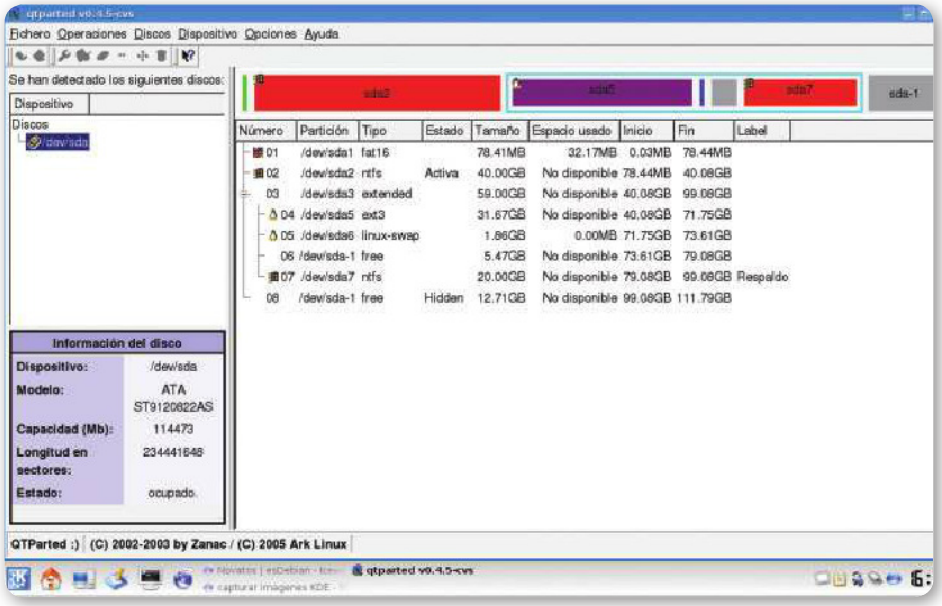


Figura 8. Qtparted es una interfaz gráfica que nos permite administrar las particiones de manera sencilla.

Comandos de consola

Una vez instalado el sistema operativo (sin interfaz gráfica), vamos a iniciar sesión como **superusuario** o **root**, ingresando la contraseña definida en la instalación; así ya tendremos listo el prompt para ejecutar comandos. En primera instancia, navegamos con nuestra consola ingresando en directorios del sistema base sobre la partición raíz "**/**", y listando los archivos y directorios que tenemos dentro. Los comandos son los siguientes:

Para ingresar a la raíz del sistema operativo y a sus carpetas:

root@server:~# cd /

Para listar contenido (directorios o archivos) en este caso, la raíz:

```
root@server:~# ls
```

Con respecto a **ls** para listar, podemos usar **flags** o argumentos que permitan visualizar el contenido; por ejemplo, vamos a ejecutar:

```
root@server:~# ls –ltr
```

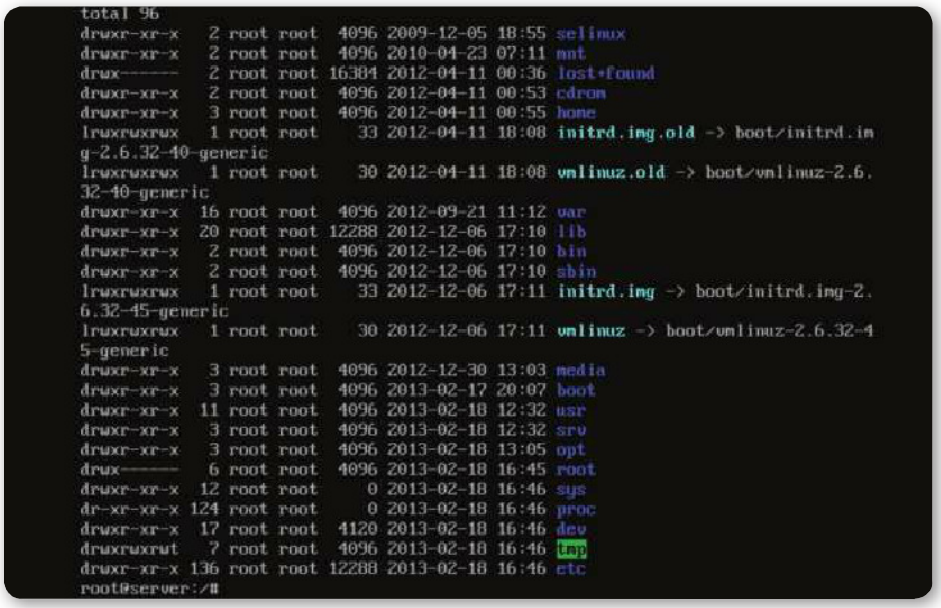


Figura 9. En la imagen podemos visualizar el listado personalizado con los argumentos que nos brinda el comando `ls –ltr`.

Donde **l** es listado extenso, **t** es ordenar por tiempo de modificación y **r** es ordenar en forma reversa.

Para visualizar todas las opciones de un comando, podemos ayudarnos con el manual incorporado, ejecutándolo de la siguiente manera, en este caso, para **ls**:

```
root@server:~# man ls
```

Una vez visualizado, salimos con **:q**.

Luego, para ir ingresando en los demás directorios, también lo hacemos con “cd”, Cabe recordar que podemos utilizar la tecla TAB para sugerir comandos o completar el contenido:

```
root@server:~# cd home
```

Para volver un nivel:

```
root@server:~# cd ..
```

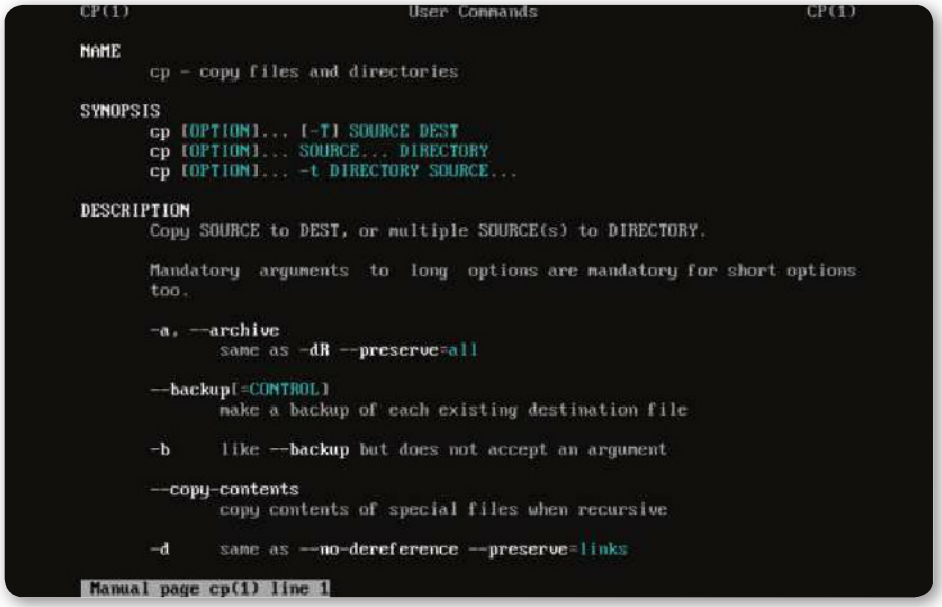


Figura 10. Un ejemplo de la información detallada bajo el comando **man** de una aplicación. Los administradores de red la usan a diario.

Comandos de visualización de contenido

Una vez que estemos configurando un servidor, realizando modificaciones o editando algún servicio, debemos listar las configuraciones en cada caso, que se encuentran alojadas, por lo general, en los archivos **.conf**. Por ejemplo, para el demonio **syslog**, que administra los registros del sistema en la distribución Debian, lo ubicamos en **/etc/rsyslog.conf.**

Ejecutando el comando **cat** (proveniente de concatenar), utilizado para concatenar archivos e imprimirlos por salida estándar (por ejemplo, pantalla). Su sintaxis es muy simple y podemos observarla con **man**:

```
root@server:~# man cat
root@server:~# cd /etc
root@server:~# cat rsyslog.conf
```

En el caso particular de este archivo, contiene 116 líneas, por lo cual en una pantalla convencional solo podremos visualizar las últimas, y el inicio quedará sin verse. Para esto, utilizamos el comando **less**, que nos permite paginar un archivo extenso haciendo que podamos continuar o retroceder tan solo con las flechas del cursor.

```
root@server:~# less /etc/rsyslog.conf
root@server:~# manless
```

Figura 11. **Les** nos ayudará a visualizar contenido muy extenso en la consola, ya que con las flechas del cursor podremos subir y bajar.

Por último, vamos a estudiar el comando **tail**, que proviene de la palabra **cola**. Este comando es de mucha utilidad porque nos permite visualizar, de manera estándar, las últimas 10 líneas de un archivo. Muchas veces, esto sucede cuando debemos hacer análisis de un log o evento de un servicio y solo nos interesan las últimas líneas, y no queremos utilizar toda la pantalla, ya que puede generar confusión por la gran cantidad de información que genera un log. Además, con el argumento **–f** (de follow), nos arroja en forma instantánea lo que está sucediendo. Por lo tanto, además de ser un visualizador, también es una herramienta de monitoreo. De aquí nacen otras aplicaciones externas como **multitail**, que permite ordenar un log por columnas y colores.

```
root@server:~# tail /etc/rsyslog.conf
```

Vamos al ejemplo con argumento incorporado:

```
root@server:~# tail –f /var/log/syslog
root@server:~# mantail
```

Manipulación de contenido

En este ítem veremos cómo crear, modificar, copiar y borrar contenido desde la consola de un servidor GNU/Linux.

Para crear un directorio en la raíz usaremos el comando **mkdir.** Primero observamos las características con:

```
root@server:~# man mkdir
```

Luego:

```
root@server:~# mdkir /directorio
```

Ahora, vamos a crear uno dentro de nuestra carpeta de usuario:

```
root@server:~# cd /home/usuario
root@server:~# mkdir directorio
```

Creamos un archivo:

```
root@server: ~# touch archivo01
```

Un comando útil para tener en cuenta es **pwd**, que nos devuelve en pantalla la ruta en donde estamos ubicados:

```
root@server: ~# pwd
/home/usuario
```

Luego, vamos a modificar este último archivo creado, con **mv** (abreviatura de move, en inglés):

```
root@server:~# mv archivo01 archivo02
```

> GIT ES USADA PARA DESCARGAR CÓDIGO FUENTE O SINCRONIZAR EL VERSIONADO

Renombramos un directorio o carpeta:

```
root@server:~# mv directorio/ directorio2
```

Podemos verificarlo si realizamos un listado de contenido, y veremos la falta del **archivo01**. Ahora, para poder tener ambos, vamos a copiarlo con **copy**:

```
root@server:~# cp archivo02 archivo01
```

Para copiar un directorio usamos el flag **–r**, es decir, copia directorios recursivamente:

```
root@server:~# cp –r /tmp /home/usuario/
```

Es muy útil prestar atención al manual, ya que si aprovechamos el potencial de esta herramienta, ganaremos velocidad en la copia de recursos y también nos será más sencillo programar scripts, donde, por ejemplo, podemos listar el nombre de los recursos copiados en un registro con **--verbose.**

Para eliminar contenido, seguimos la misma metodología anterior, pero con **rm** de **remove** y **-r** para directorios:

```
root@server:~# rm/home/usuario/archivo01
```

Y carpetas con:

```
root@server:~# rm–r / /home/usuario/tmp
```

Aquí eliminamos la carpeta **tmp.**

Empaquetado y compresión

Llamamos empaquetado a la agrupación de archivos y directorios dentro de un archivo, lo que da como resultado un archivo sin estar comprimido. La herramienta que tenemos en nuestro sistema GNU/Linux es **tar**. Para usarla, combinamos argumentos con el fin de indicarle qué es lo que queremos como resultado:

- **c**: crear un nuevo archivo.
- **x**: extraer contenido en lugar que estemos situado en consola.
- **v**: indicar que haga una salida de los archivos en el procedimiento.
- **f**: indicar que el argumento es el nombre del archivo **.tar.**
- **t**: argumento para listar contenido y visualizarlo.

Por lo tanto, para realizar un empaquetado de nuestro directorio de usuario, es imprescindible no estar situados en consola dentro del directorio por empaquetar; por lo tanto, vamos a la raíz:

```
root@server:~# cd /
root@server:~# tar –cvf backup1.tar /home/usuario
```

Ahora vamos a listar el contenido de **backup.tar**:

```
root@server:~# tar –tf backup1.tar
```

Por último, vamos a extraer los elementos del archivo **backup.tar**:

```
root@server:~# tar –xvf backup1.tar
```

Luego, tenemos los mecanismos de compresión, que se usan para reducir el tamaño de los archivos. Aquí usamos **gzip**, que no comprime directorios, sino archivos y ficheros creados previamente. La sintaxis es **gzip+ archivo**, pero podremos incorporar un factor de compresión que va desde 1 a 9, siendo 1 el menor factor de compresión:

```
root@server:~# gzip -9 backup1.tar
```

Obtendremos el archivo comprimido **backup.tar.gz.**

Para descomprimir, utilizaremos el argumento **-d** y volveremos al archivo de tamaño original:

```
root@server:~# gzip –d backup1.tar.gz
```

Para finalizar, vamos a utilizar una combinación de empaquetado (tar) y compresión (gzip) dentro de un mismo comando, agregando el argumento **-z** a la sintaxis, como vemos a continuación:

```
root@server:~# tar –czfv backup2.tar.gz /home/usuario
```

Hacemos el proceso inverso para desempaquetar y descomprimir:

```
root@server:~# tar –xzfv backup2.tar.gz
```

Debemos considerar que estas herramientas son utilizadas, entre otras funciones, para efectuar la manipulación de backups o copias de seguridad y para hacer traslados de estos, ya que nos permite facilitar la manipulación de volúmenes de información en un solo archivo y reduce su espacio. Además, mediante scripts, podemos agregarles valores del tipo fecha a los archivos creados y, así, mantener un orden es nuestra estructura de respaldos.

Utilidades para volúmenes, dispositivos y hardware

En esta sección vamos a revisar algunos de los comandos que nos permitirán visualizar e interpretar los volúmenes, ya sean discos duros, medios extraíbles o unidades de CD-ROM. Gracias a estas opciones usaremos la consola para gestionar diversos dispositivos.

```
root@server:~# fdisk -l

Disco /dev/sda: 21.5 GB, 21474836480 bytes
255 cabezas, 63 sectores/pista, 2610 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
Identificador de disco: 0x000f095a

Disposit. Inicio    Comienzo       Fin      Bloques  Id  Sistema
/dev/sda1   *           1        2497    20051968   83  Linux
/dev/sda2            2497        2611      916481    5  Extendida
/dev/sda5            2497        2611      916480   82  Linux swap / Solaris

Disco /dev/sdb: 1000.2 GB, 1000170586112 bytes
255 cabezas, 63 sectores/pista, 121597 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
Identificador de disco: 0x564f7512

Disposit. Inicio    Comienzo       Fin      Bloques  Id  Sistema
/dev/sdb1               1      121598   976734911    7  HPFS/NTFS
root@server:~#
```

Figura 12. Información proporcionada por la herramienta **`fdisk`** en un servidor de producción Debian GNU/Linux.

Df se presenta como una utilidad de reporte sobre el espacio libre en nuestro sistema de archivos, la cual nos brinda información como espacio total, espacio libre y utilizado, uso en porcentaje y, por último, lugar donde está montado este volumen de datos.

Los argumentos básicos o más utilizados son:

- **h**: se encarga de mostrar una visualización sencilla del volumen de datos, expresada en Megabytes y Gigabytes.
- **l**: brinda la misma información que el argumento anterior, pero expresado en bloques de disco.

> AL EJECUTAR EL MANUAL DE TOP, PODREMOS OBTENER INFORMACIÓN ACERCA DE SU USO

```
[root@virtual-XS ~]# df -h
S.ficheros          Tamaño Usado  Disp Uso% Montado en
/dev/sda1             4,0G  2,2G  1,7G  57% /
none                  373M  4,0K  373M   1% /dev/shm
/dev/sdb1             1,8T  518G  1,2T  30% /backup
/opt/xensource/packages/iso/XenCenter.iso
                       52M   52M     0 100% /var/xen/xc-install
[root@virtual-XS ~]#
```

Figura 13. Ejemplo de la aplicación **df** para visualizar el contenido de nuestras particiones montadas en el sistema; en este caso, un servidor de producción en CentOS.

Comandos de instalación

En los sistemas GNU/Linux, tenemos diferentes maneras de realizar instalaciones de paquetes, todo depende de qué distribución estemos usando, en qué formato se encuentren o si tan solo están en los repositorios de la distribución en uso.

HERRAMIENTAS PARA INSTALAR PAQUETES

NOMBRE	DISTRIBUCIÓN	COMANDO
Deb	Debian GNU/Linux	# dpkg
Apt (*)	Debian GNU/Linux	# apt-get
Rpm	RedHat y derivados	# rpm
Yum (*)	RedHat y derivados	# yum instsall
Ebuild	Gentoo	Compilación del archivo fuente
Emerge (*)	Gentoo	# emerge
Tar.gz	Todas	Compilación del archivo fuente

Tabla 1. Herramientas utilizadas para la instalación de paquetes desde los repositorios asignados de cada distribución.

Edición de archivos de configuración

Para modificar archivos de configuración, realizar scripts y hacer tareas de mantenimiento, necesitamos los editores. Distribuciones como Debian GNU/Linux incorporan a **nano** como editor por defecto, pero la realidad es que el navegador predefinido, presente en la gran mayoría de servidores que estemos configurando, es **vi**:

```
root@server:~# vi /etc/rsyslog
```

i: para ingresar en modo inserción de texto y realizar modificaciones.
o: inserta una línea debajo de la actual.
q: salir sin haber hecho cambios.

NAVEGADORES

Los sitios web de la mayoría de los proyectos en GNU/Linux están diseñados para ser visualizados a través de navegadores por consola. Uno de los proyectos más difundidos se llama **elinks**, y podemos obtenerlo por medio de los repositorios de la distribución Debian o bien del sitio **http://elinks.or.cz/download.html**, para acceder a los archivos fuentes y compilar. Luego, desde la consola ejecutamos, por ejemplo, **elinks www.debian.org** y ya estaremos listos para navegar desde nuestra shell por el proyecto Debian.

q!:salir sin guardar cambios.
x: salir guardando los cambios.

Luego, podemos instalar, de manera opcional, la evolución de **vi** llamada **vim**, que presenta grandes funcionalidades, como apertura de varios archivos y detección de sintaxis.

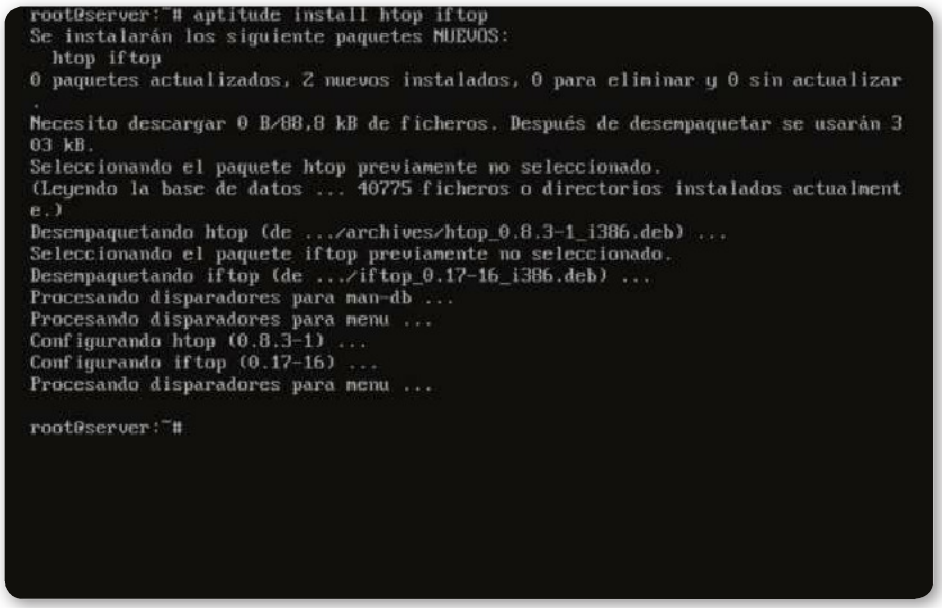


Figura 14. Ejemplo de búsqueda e instalación de un paquete como SSH con APT, en Debian GNU/Linux.

Diagnóstico de red y procesos

Dentro del directorio **init.d**, ubicado en **/etc** o en **/etc/rc.d** (dependiendo de la distribución), encontraremos una serie de scripts que nos permitirán manipular los servicios instalados en el equipo. La mayoría de ellos reconoce los argumentos **start**, **stop**, **restart** y **status.**

Los nombres de los argumentos describen su función (iniciar, detener, reiniciar y condición) y tienen permisos de ejecución. Si estamos identificados como un usuario root, podremos iniciar un servicio tal como mostramos a continuación:

networking: servicio que controla la tarjeta de red.
/etc/init.d/networkingstart: inicia los servicios de red.
/etc/init.d/networkingrestart: reinicia los servicios de red.
/etc/init.d/networking stop: detiene los servicios de red.

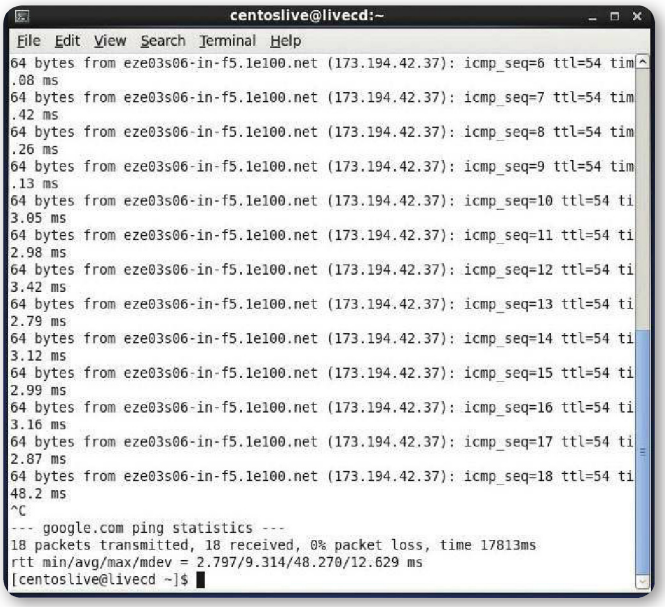


Figura 15. A diferencia de Windows, en sistemas Linux, la cantidad de **`ping`** es infinita.

ifconfig

Este comando nos muestra información sobre la configuración TCP/IP de nuestra PC: dirección IP, MAC Address, gateway, DNS, etc. Lo utilizamos de la siguiente forma:

Ifconfig: muestra el estado de las interfaces activas.
ifconfig–a: muestra el estado de todas las interfaces, activas o no.
ifconfig ppp0: muestra el estado del ppp0.
ifconfig eth0 up: activa eth0.
ifconfig eth0 down: desactiva eth0.

Para cambiar la IP manualmente, debemos ingresar lo siguiente:

ifconfig eth0 [Dirección IP] netmask [máscara subred]
Por ejemplo: **ifconfig eth0 192.168.1.102 netmask 255.255.255.0**

Si nuestra máquina tiene dos placas de red, entonces les asignaremos distintas IP a los diferentes ethX. Por ejemplo:

```
ifconfig eth0 192.168.1.102 netmask 255.255.255.0
ifconfig eth1 10.100.0.10 netmask 255.255.0.0
```

En algunas oportunidades, también tendremos que asignarle la dirección de broadcast con la IP del router:

```
ifconfig eth0 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.100
```

Es recomendable que, después cambiar una dirección IP, se baje y se suba (reset) la interfaz con los comandos **down** y **up**:

```
ifconfigdown
ifconfig up
```

Otra variante con el mismo resultado es usando los comandos:

```
ifdown
ifup
```

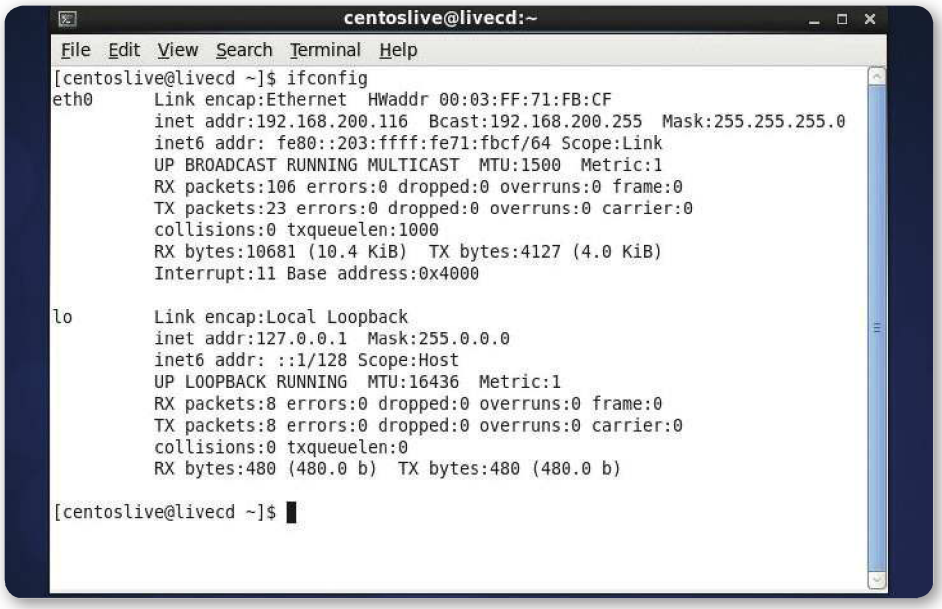


Figura 16. Con **`ifconfig`** podemos obtener datos básicos de nuestra interfaz de red y cambiar la dirección IP.

iwconfig

Es similar al comando **ifconfig**, pero para las interfaces wireless. Lo utilizamos de la siguiente forma:

iwconfig: muestra el estado de las interfaces activas.

iwconfig eth0: muestra cómo está configurada la placa inalámbrica.

iwconfig ath0: muestra información de la red inalámbrica (nombre de la red, canal, nivel de señal, velocidad, potencia, cifrado de WEP, punto de acceso, etc.).

iwconfig ath0 essid "Red_WiFI": para configurar el nombre de nuestra red Wi-Fi o ESSID (*Extended Service Set IDentifier*), con el nombre que queremos asociarnos.

dhclient

Dynamic Host Client se encarga de iniciar la conexión DHCP mediante el cliente **dhcp-client**. Usando el parámetro **-r**, liberamos la IP actual; se usa de la siguiente manera:

dhclient eth0 –r: libera la IP actual.

dhclient eth0: renueva la IP.

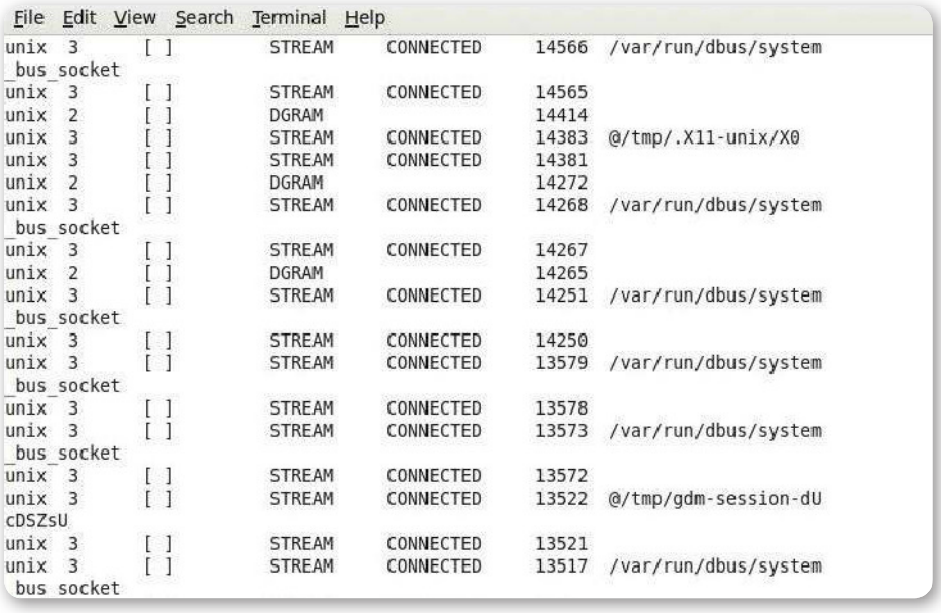


Figura 17. Listado de las conexiones activas, tanto internas (localhost) como externas.

netstat

Network Statistics muestra un listado de las conexiones activas, tanto internas (localhost) como externas, los sockets abiertos y las tablas de enrutamiento. Lo usamos de la siguiente forma:

netstat–p: muestra los programas asociados a los sockets abiertos.
netstat–l: muestra los server sockets que están en modo escucha.
netstat–s: muestra información sobre todos los puertos.

host

Sobre un nombre de dominio, el comando **host** nos devuelve la IP asociada a él, y viceversa. Sobre una dirección IP, nos devuelve el dominio asociado (DNS lookup).

host google.com: muestra la IP de Google (varía según el ISP, zona, etcétera).
host 8.8.8.8: muestra los DNS públicos de Google.

dig

Domain Information Groper o **dig** es una de las mejores opciones a la hora de hacer troubleshooting o debug de problemas DNS. Esta herramienta se utiliza para obtener una dirección IP a partir del nombre del host (y viceversa), para proveernos de la información de una ruta. Nos será muy útil, por ejemplo, para comprobar si el DNS se encuentra correctamente configurado en nuestra computadora.

> DIG SE PRESENTA COMO UNA DE LAS MEJORES OPCIONES A LA HORA DE HACER TROUBLESHOOTING

También muestra el mapeo de nombres a IP, así como el mapeo inverso de IP a nombres, pero solo sirve para Internet y no, dentro de nuestra red LAN. Su uso es el siguiente:

dig: realiza una consulta de los NS (Name Servers) raíz.
dig google.com: muestra un registro al DNS de Google.
diglocalhost: muestra una respuesta 0; solo consulta a los DNS del ISP. Lo mismo ocurre con cualquier otra PC de nuestra red.

```
File  Edit  View  Search  Terminal  Help
[centoslive@livecd ~]$ dig google.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3993
;; flags: qr rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             121     IN      A       173.194.42.7
google.com.             121     IN      A       173.194.42.8
google.com.             121     IN      A       173.194.42.9
google.com.             121     IN      A       173.194.42.14
google.com.             121     IN      A       173.194.42.0
google.com.             121     IN      A       173.194.42.1
google.com.             121     IN      A       173.194.42.2
google.com.             121     IN      A       173.194.42.3
google.com.             121     IN      A       173.194.42.4
google.com.             121     IN      A       173.194.42.5
google.com.             121     IN      A       173.194.42.6
```

Figura 18. **`Dig`**, junto a **`hostname`**, nos ayudarán a resolver cualquier problema de DNS.

tcpdump

Es uno de los analizadores de paquetes de red más conocidos, al estilo de **Wireshark** (**www.wireshark.org**). Se trata de un sniffer que monitorea toda la actividad de la red, capaz de "escuchar" el tráfico de la LAN y capturar datos para su posterior análisis. Podremos detectar problemas de red e intrusiones, conocer y monitorizar el tráfico que se está generando, y controlar el ancho de banda.

Tengamos en cuenta que nuestra placa de red se encargará de trabajar en modo promiscuo, lo cual nos permitirá no solo escuchar los paquetes que vienen destinados a nuestra computadora, sino también escuchar todo el tráfico que se genera en la red de datos. Por esta razón, es importante la ubicación de la computadora para no quedar fuera del umbral de audición del sistema.

Las múltiples opciones de parámetros y filtros nos dan una infinidad de combinaciones. En primer lugar debemos verificar sobre qué placas podemos empezar a escuchar tráfico; a continuación revisaremos las opciones que debemos tener en cuenta para utilizarlo:

tcpdump–D: muestra la lista de interfaces disponibles.

tcpdump –i wlan0: inicia la captura. La detenemos con **CTRL+C.**

hostname

Junto con **dig**, nos ayudará a resolver problemas de DNS. El nombre almacenado que identifica cada máquina se encuentra en **/etc/hostname** y podemos consultarlo con el comando **hostname.**

Con la variable **files dns**, busca primero en el archivo **/etc/hosts**, y luego, en el servidor DNS (en el archivo **/etc/resolv.conf**). Su uso es el siguiente:

hostname files DNS: muestra un listado de los servicios que se usarán para resolver un nombre.

hostname–f: muestra el nombre y dominio de nuestra PC.

hostname–i: muestra la dirección IP de nuestro nodo.

hostname–a: muestra los alias para nuestro nodo.

Seguridad a nivel de kernel

Quienes no estén familiarizados con las plataformas **GNU/Linux** o derivadas de **UNIX** quizás encuentren esta sección algo difícil de comprender, pero es importante para todo especialista en informática saber un poco sobre cada uno de los distintos sistemas operativos principales: la rama **Microsoft Windows** y la rama GNU/Linux.

> LOS SISTEMAS GNU/LINUX SIEMPRE FUERON BIEN VISTOS EN CUANTO A SU NIVEL DE SEGURIDAD

Si bien los sistemas del tipo Linux siempre fueron bien vistos en cuanto a la seguridad, lo cierto es que esta seguridad puede dividirse en lo que respecta a sus distintas capas, es decir, desde la que se encuentra más cercana al usuario hasta la más cercana al **hardware.**

En la capa donde operan las aplicaciones, Linux provee todo tipo de software orientado a que pueda darse mayor seguridad al sistema desde un uso administrativo, es decir, configurando de distintas formas sus características en cuanto a usuarios y contraseñas, controles de acceso, sistema de archivos, inicio y parada, administración general, y demás. Debemos considerar que, en este nivel, el usuario administrador deberá ajustar todo haciendo uso de comandos incluidos o no en el sistema, de modo tal que pueda mejorarse la confiabilidad y seguridad total.

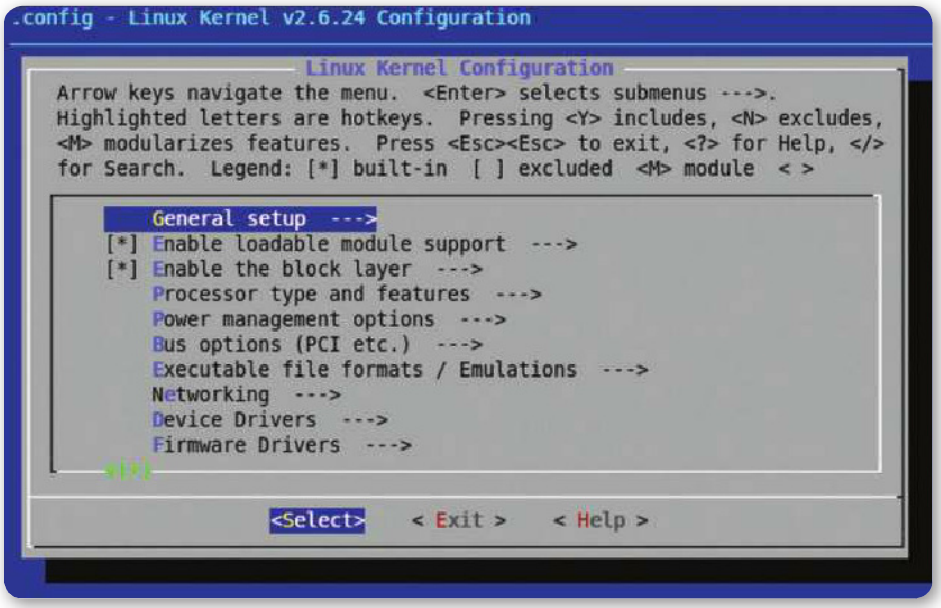


Figura 19. Interfaz que permite la configuración de las características del núcleo de Linux.

Hardening

Si nos encontráramos en sistemas Microsoft Windows, esto sería lo máximo que podríamos hacer como administradores: usar software o comandos y herramientas del propio sistema que permitan mejorar sus características, o bien adicionarle medidas de control y seguridad para elevar incluso más el nivel de seguridad.

> PARA AUMENTAR LA SEGURIDAD DE UN SISTEMA LINUX, NO BASTA CON AJUSTAR LAS APLICACIONES

Este proceso, en líneas generales, es al que nos referimos cuando hablamos de **hardening**, aunque algunos prefieren considerar hardening solo a los ajustes provenientes de los propios comandos y herramientas internas del sistema.

En caso de que sea necesario realizar algunos ajustes a un mayor nivel de profundidad, no será posible hacerlo en estas plataformas, dado que el sistema se encuentra compilado y funcionando, y no se puede modificar su núcleo ni tampoco sus características internas, por ejemplo el manejo de la memoria, el soporte de algunas características específicas de sistemas de archivos, la forma en que se gestiona el registro, el uso del disco rígido y el procesador, etcétera.

Figura 20. Menú de configuración en modo gráfico que muestra la selección de opciones para **ASLR**.

Mejorar la seguridad

En el caso de sistemas Linux, sí es posible mejorar la seguridad en el nivel del **kernel**, lo cual, por cierto, nos obliga a comprender en mayor profundidad los distintos aspectos de éste. Para modificar características del núcleo, por empezar, deberemos utilizar alguna herramienta que nos permita gestionar todas las posibles funcionalidades que se pueden cambiar, y luego, pasar por un proceso de recompilación de dicho núcleo a partir del **código fuente**, que nos dará como resultado un nuevo núcleo, pero modificado de la manera en que nosotros queríamos.

> EN GNU/LINUX ES POSIBLE MEJORAR LA SEGURIDAD A NIVEL DEL KERNEL DEL SISTEMA

Por ejemplo, al instalar el sistema, nuestro núcleo viene preconfigurado de forma estándar para soportar una serie de componentes generales, placas de video, **motherboards** y protocolos, y todo lo que necesita el sistema operativo para entenderse con el exterior (usuario) y el interior (hardware). Si quisiéramos agregarle el soporte para nuevos protocolos de cifrado, o producir cambios en el manejo

de la memoria, o en la compilación, o en la gestión de los procesos, deberíamos recompilar el núcleo en función de esto.

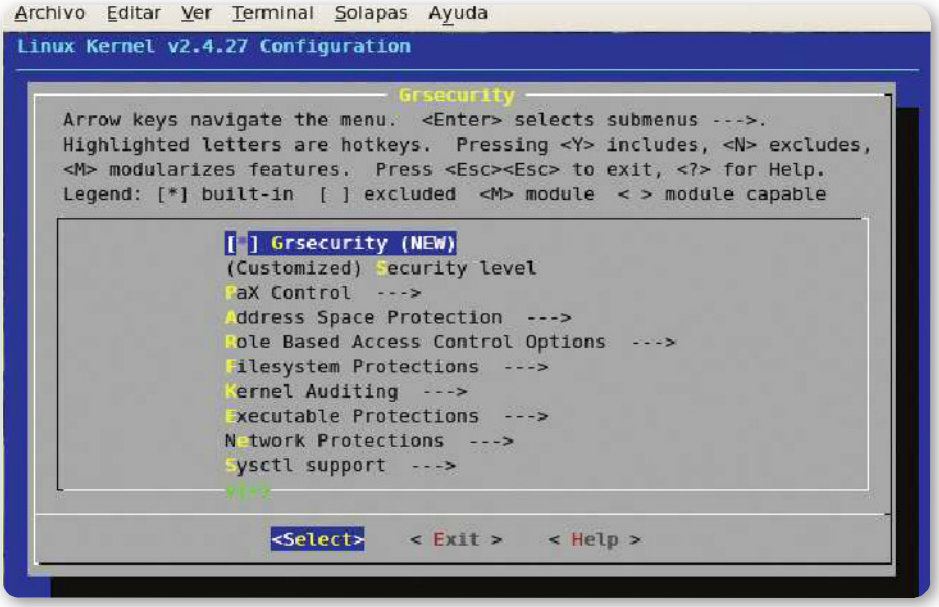


Figura 21. Menú específico de **GRSecurity**, agregado mediante la aplicación de dicho parche al kernel.

Para realizar esta tarea, debemos contar, como dijimos, con el código fuente del núcleo, que obtenemos del sitio oficial **www.kernel.org** o descargándolo mediante el sistema de gestión de paquetes de la distribución que tengamos. Una vez bajado el núcleo sin compilar, debemos bajar alguna interfaz de administración de características para facilitar el acceso a las opciones. Luego, ya podemos navegar por el menú en las diferentes opciones, tanto de funcionalidad como de seguridad, modificar el parámetro al valor que queramos y, finalmente,

¿NÚCLEO MONOLÍTICO O MODULAR?

El sistema GNU/Linux cuenta con un núcleo monolítico, es decir que todas las funciones necesarias para él están incluidas en un solo núcleo único en el que basa su funcionamiento. Su creador en 1991, Linus Torvalds, dio el nombre al núcleo (kernel) y a la plataforma (Linux). A partir de esto, se conoció como GNU/Linux a la combinación de software libre con licencia GNU y un núcleo de Linux. Existen también núcleos que no son monolíticos, y se conocen como micronúcleos.

generar un archivo que corresponda a esos cambios, que luego se aplicarán al código fuente y se volverá a compilar teniendo en cuenta las modificaciones efectuadas.

Características de seguridad

Más allá de las características de seguridad que ya vienen incluidas para cambiar en el núcleo de Linux, también podemos incluir características especiales, que se incorporan de manera directa mediante parches de kernel al código fuente, y agregan más elementos modificables de los que permite en el menú de configuración original con el código original (llamado también **Vanilla**). Un ejemplo de este tipo de parches es el bien conocido **GRSecurity** (**http://grsecurity.net**), creado por **Brad Spegler** (**Spender**) en 2001 para el kernel en su versión 2.4.1, tomando prestados algunos conceptos de **LIDS** (**Linux Intrusion Detection System**) y agregando decenas de funciones, como restricción de recursos con alta granularidad, **ACLs** basadas en tiempo y **Role-Based Access Control** (**RBAC**).

Figura 22. Desde el sitio web de **GRSecurity** se puede descargar la última versión del parche para el núcleo.

Otro sistema de parches para el núcleo de Linux destinado a agregar elementos de configuración de seguridad es el conocido **Openwall**

(**Owl**), nacido también en 2001 y no tan actualizado como el anterior, y creado por el hacker ruso **Alexander Peslyak**.

Una de las funcionalidades generales agregadas normalmente por estos parches es el soporte para sistema **PaX**, que refuerza, entre otras cosas, las llamadas al sistema (**syscalls**) e implementa páginas no ejecutables de memoria, además de aleatorizar el espacio de memoria (**Address Space Layout Randomization**, o **ASLR**) para **binarios ELF**. También se incluye entre las mejoras la eliminación de la clásica problemática de la predecibilidad en el manejo de los servicios, demonios, procesos, direcciones, y todo lo que pueda ser enumerable e identificable dentro del sistema, y el soporte para **TPE** (**Trusted Path Execution**) o rutas de ejecución segura, que evita que los usuarios ejecuten binarios no confiables, que no están en directorios cuyo dueño es **root**.

EL SOPORTE PARA SISTEMAS PAX SE AGREGA MEDIANTE EL USO DE DIVERSOS PARCHES

Sistemas de verificación de integridad

Sabemos que no existen sistemas completamente invulnerables, razón por la cual es necesario tener en cuenta que siempre estaremos expuestos a la ejecución de diversos ataques. Es cierto que podemos contar con algunas medidas altamente efectivas, tales como firewalls, parches o políticas de control, pero aun en su conjunto, estas no son capaces de brindarnos una seguridad total.

Ahora bien, la ejecución de ataques a la red busca ejecutar acciones malintencionadas, tales como modificar en forma parcial los archivos del sistema mediante la alteración o reemplazo de ciertos archivos. Luego, estas modificaciones pueden ser la base para que el atacante tome el control del sistema.

Es en este punto donde los sistemas de verificación de integridad cobran una importancia crucial, ya que nos permitirán monitorear los archivos del sistema para asegurar que no sean modificados.

A continuación, conoceremos dos de los sistemas de verificación de integridad más utilizados: **Tripwire** y **AFICK**.

Tripwire

Es una aplicación para entornos Linux, que funciona monitoreando la integridad de aquellos archivos del sistema que son el blanco de ataques. Este sistema de verificación de integridad es capaz de comparar los archivos en los intervalos que configuremos, aunque debemos tener en cuenta que, cuanto más reducidos sean estos intervalos, más recursos del sistema se utilizarán.

Podemos obtener una copia de esta aplicación Open Source visitando el sitio web oficial en **www.tripwire.org**. Para instalarlo, abrimos una consola de comandos y escribimos los siguientes comandos, presionando **ENTER** después de cada uno.

Para descomprimir el archivo:

```
# tarxvzf tripwire.tar.gz
```

Para instalar la aplicación:

```
# rpm -ivh tripwire-2.3-47.i386.rpm
```

Figura 23. Cada vez que realicemos un cambio en el archivo de configuración, deberemos regenerar la base de datos de Tripwire.

Consideremos que, en algunas distribuciones GNU/Linux, Tripwire podría encontrarse instalado, por lo que los pasos que mencionamos anteriormente no serán necesarios.

> DEBEMOS CONSTRUIR LA BASE PARA QUE TRIPWIRE ALMACENE EL ESTADO DE LOS ARCHIVOS

Una vez que hayamos instalado Tripwire, comenzaremos con el proceso de configuración, para lo cual será necesario definir las claves con el siguiente comando:

```
# /etc/tripwire/twinstall.sh
```

Luego de hacerlo, configuramos los archivos del sistema que serán monitoreados por Tripwire. Estos se mantienen en un fichero conocido como **archivo de políticas**. Por suerte para nosotros, Tripwire nos proporciona un archivo que podemos utilizar como plantilla, que se ubica en **/etc/tripwire/twpol.txt**. Lo abrimos con un editor de texto, como Vi, y buscamos la sección denominada **File System and Disk AdministratonPrograms**. En ella encontraremos un listado de las ubicaciones que serán monitoreadas; un ejemplo de esta sección es el siguiente:

```
(
rulename = "File System and Disk AdministratonPrograms",
severity = $(SIG_HI)
)
{
 /sbin/accton              -> $(SEC_CRIT) ;
 /sbin/badblocks                   -> $(SEC_CRIT) ;
 /sbin/dosfsck             -> $(SEC_CRIT) ;
 /sbin/e2fsck              -> $(SEC_CRIT) ;
 /sbin/debugfs              -> $(SEC_CRIT) ;
```

Aquí debemos ingresar o eliminar las ubicaciones deseadas. Es importante constatar que la llave de cierre, **}**, se encuentre al final de las ubicaciones que se monitorearán. Guardamos el archivo y lo instalamos con el comando:

```
# twadmin -m P /etc/tripwire/twpol.txt
```

A continuación, vamos a construir la base de datos en la que Tripwire almacenará el estado actual de los archivos, para lo cual necesitamos ejecutar el comando:

```
# tripwire -m i 2> /tmp/msj
```

Con esto redirigimos los errores a **/tmp/msj**; así podremos revisar los problemas encontrados y corregirlos en el archivo de políticas, para luego instalarlo otra vez y generar la base de datos. Cuando todo se realice sin errores, eliminamos **/tmp/msj**. Cuando terminemos el proceso de configuración de Tripwire, verificamos con el comando:

```
# tripwire -m c
```

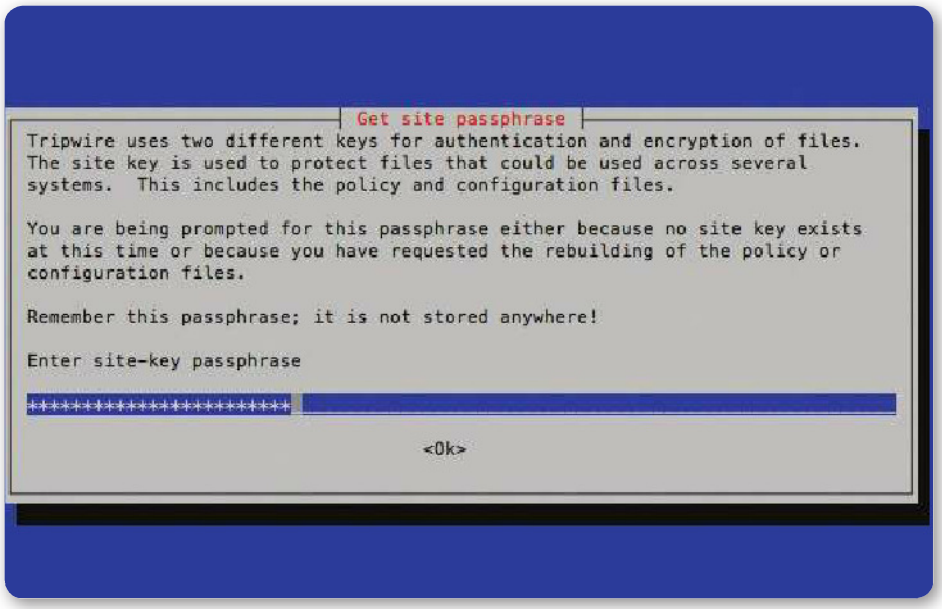


Figura 24. En esta ventana ingresamos la contraseña que utilizará Tripwire para autenticar y encriptar los archivos.

AFICK

Afick (**http://afick.sourceforge.net**) es una aplicación que se encarga de supervisar los cambios que se produzcan en el sistema de archivos del equipo, de forma de mantenernos alertados sobre cualquier modificación, lo que podría significar la presencia de una intrusión.

Entre las principales características de AFICK están las siguientes:

- Se presenta como una aplicación portátil y multiplataforma, por lo que podremos utilizarla en diversos sistemas operativos, tales como Microsoft Windows o distribuciones GNU/Linux.

- El proceso de instalación de esta herramienta es una tarea sencilla, y su posterior ejecución, muy rápida.
- Nos permite acceder a los datos sobre los archivos que han sido creados, eliminados o cambiados.
- El archivo de configuración de la herramienta permite utilizar excepciones y, también, comodines.

En líneas generales, para utilizar Afick debemos realizar una serie de pasos similares a Tripwire, los cuales incluyen la descarga y ejecución, la edición del archivo de configuración y la creación de la base de datos para comparar en análisis posteriores; luego, hacemos un chequeo del sistema de archivos.

> LA MEJOR FORMA DE DETECTAR ROOTKITS ES BOOTEANDO CON UN LIVE DVD DE UN SISTEMA GNU/LINUX

A continuación, conoceremos y comentaremos algunos ejemplos del archivo de configuración que necesitamos para AFICK.

Para definir la ruta de la base de datos, usamos el comando:

```
base de datos: = / var / lib / Afick / Afick
```

Para ignorar la estructura del directorio **/ dev**:

```
! / Dev
```

Para excluir todos los archivos o directorios con nombre **tmp**:

```
exclude_re: = / tmp $
```

CONFIGURACIÓN DE AFICK

Para editar el archivo de configuración de AFICK, debemos tener en cuenta algunas cuestiones importantes. En primer lugar, distingue entre mayúsculas y minúsculas. Para continuar, tanto en las líneas iniciales como en las finales los espacios en blanco se ignoran. Finalmente, las líneas en blanco o las líneas que comienzan con # serán ignoradas, ya que se consideran comentarios.

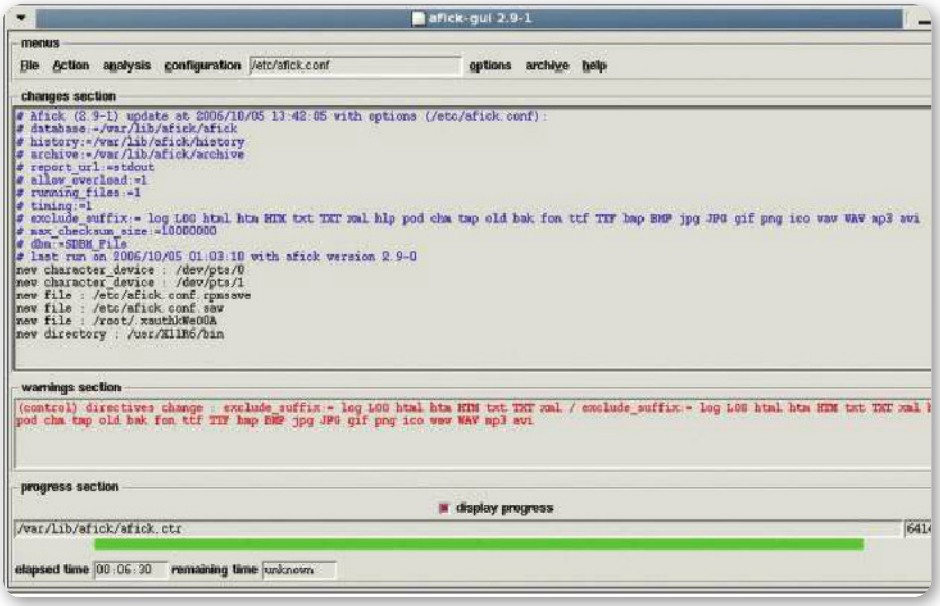


Figura 25. Ventana de ejecución de la aplicación AFICK.

Protección ante rootkits

Un **rootkit** es un tipo de malware, es decir, un programa malicioso que se ejecuta sin ser percibido por el usuario o administrador del sistema. Si bien en general se utiliza en servidores, puede afectar cualquier tipo de dispositivo, como computadoras de escritorio, tablets o teléfonos.

Implementa un funcionamiento de bajo nivel, haciéndose pasar, por ejemplo, por drivers o componentes del S.O. Su instalación puede ser realizada por un atacante que utiliza una vulnerabilidad o que engaña al usuario por medio de técnicas de **ingeniería social** o **phishing**. De esta manera, puede ejecutarse durante largos períodos de tiempo sin ser advertido, ya que su objetivo principal no es perjudicar al sistema operativo usurpado, sino servir para otros fines.

Los rootkits suelen incluir un backdoor, que permite establecer una conexión remota al sistema. Se los emplea para monitorear el uso del sistema, alterar programas, realizar ataques del tipo DDoS e IRC, y enviar spam. Facilitan la formación de botnets, ya que resulta sencillo instalar nuevos programas en equipos que tengan un rootkit instalado.

Su nombre proviene de los términos *root* (usuario privilegiado en Linux/UNIX) y *kit* (ya que suelen incluir varias herramientas).

Es importante mencionar que, en un principio, se asociaban solo a sistemas operativos del tipo UNIX, pero también han incursionado en equipos **Windows**, **Mac OSX**, routers Cisco, controladores PLC e, incluso, en **Android**, **iOS** y **Symbian**.

Recomendaciones

Es necesario tener en cuenta que utilizando buenas prácticas de seguridad, se reduce drásticamente la posibilidad de ser infectado por un rootkit. A continuación detallaremos las recomendaciones más importantes, las cuales consisten en:

- **Utilizar antivirus**: si bien parece obvio, muchos usuarios y empresas no lo usan o no controlan adecuadamente su correcto funcionamiento y actualización. En grandes ambientes corporativos, es común encontrar equipos cuyo antivirus no fue instalado o no está funcionando como corresponde. Es preciso desarrollar un proceso que permita detectar con rapidez estas situaciones y corregirlas. A pesar de no ser muy utilizados, también hay antivirus para ambientes UNIX/Linux. Los antivirus más completos permiten detectar rootkits.

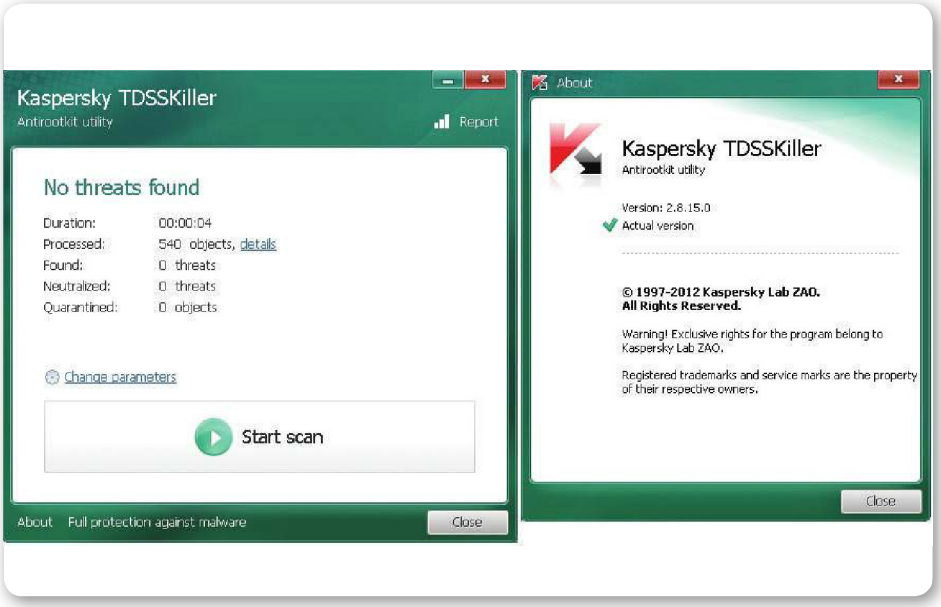


Figura 26. Kaspersky TDSS Killer detecta y elimina rootkits conocidos en Windows analizando archivos del sistema operativo.

- **Utilizar firewalls**: los firewalls correctamente configurados pueden restringir el tráfico malicioso que genera el malware. Existen dos tipos básicos de firewalls: los de red y los que se ejecutan a nivel del sistema operativo. La adecuada segregación de redes permite tener una administración mejor y más flexible. Por ejemplo, es recomendable que los administradores y los usuarios finales utilicen distintos segmentos de red.
- **Políticas de password**: la política de password debe requerir contraseñas complejas. Exigir a los usuarios y administradores cambios de contraseña permanentemente puede ser perjudicial: es mejor una clave compleja, que una simple que cambia todos los meses. Cuanto mayor es la cantidad de caracteres y requisitos de complejidad, más difícil es utilizar técnicas de 'fuerza bruta' o ataques por diccionario.

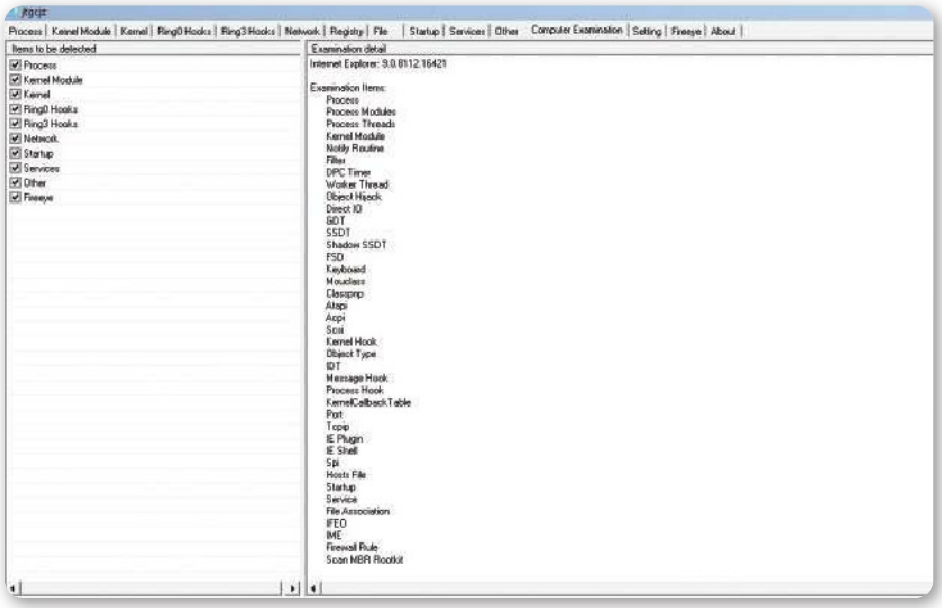


Figura 27. XueTr examina los procesos, el kernel y demás configuraciones del sistema en busca de rootkits conocidos.

- **Mantener el software actualizado**: las actualizaciones de seguridad corrigen fallas de diseño que, muchas veces, son conocidas y poseen métodos de explotación disponibles públicamente. Es común ver en las empresas que se actualizan solo los equipos con sistema operativo Windows, y no, el resto, como UNIX/Linux. Las aplicaciones también deben ser actualizadas con frecuencia.

- **Realizar hardening**: los sistemas operativos suelen incluir muchas herramientas y funcionalidades que posiblemente nunca se utilicen. Es recomendable desactivar todo el software que no va a ser usado y adoptar parámetros seguros para el que sí emplearemos. Por ejemplo, en sistemas UNIX es aconsejable quitar el conjunto de demonios y utilitarios **rlogin**, y configurar **sshd** para que solo utilice la versión 2 del protocolo.

Niveles de ejecución

Existen distintos niveles en los cuales un rootkit puede ejecutarse. Por ejemplo, los que se ejecutan en el nivel 3 o **ring 3** (modo usuario) corren como una aplicación más. Pueden ocupar el espacio de memoria de otra aplicación para ejecutarse cuando esta es llamada. Los que lo hacen en el **ring 0** (modo kernel) usan drivers o modifican el sistema operativo para correr de forma privilegiada. Estos son propensos a generar inestabilidad en el sistema operativo como consecuencia de una programación de muy bajo nivel. Debemos considerar que al ejecutarse a nivel del kernel, su detección y remoción resultan más complicadas.

EXISTEN DIFERENTES NIVELES O RING EN LOS CUALES UN ROOTKIT ES CAPAZ DE EJECUTARSE

Utilidades

Además de los antivirus tradicionales, existen utilidades especializadas en detectar y remover rootkits conocidos. En la gran mayoría de los casos, estos pueden revertir las modificaciones que fueron realizadas para pasar inadvertidos:

- **chkrootkit**: es una herramienta de origen brasileño que permite detectar rootkits instalados en sistemas UNIX/Linux. Consiste en un shell script que utiliza herramientas del sistema para detectar modificaciones realizadas por un rootkit. Puede utilizarse desde un Live CD, que resulta lo más conveniente, ya que de esta manera no utiliza componentes del sistema operativo que puedan estar alterados por la acción de algún malware.

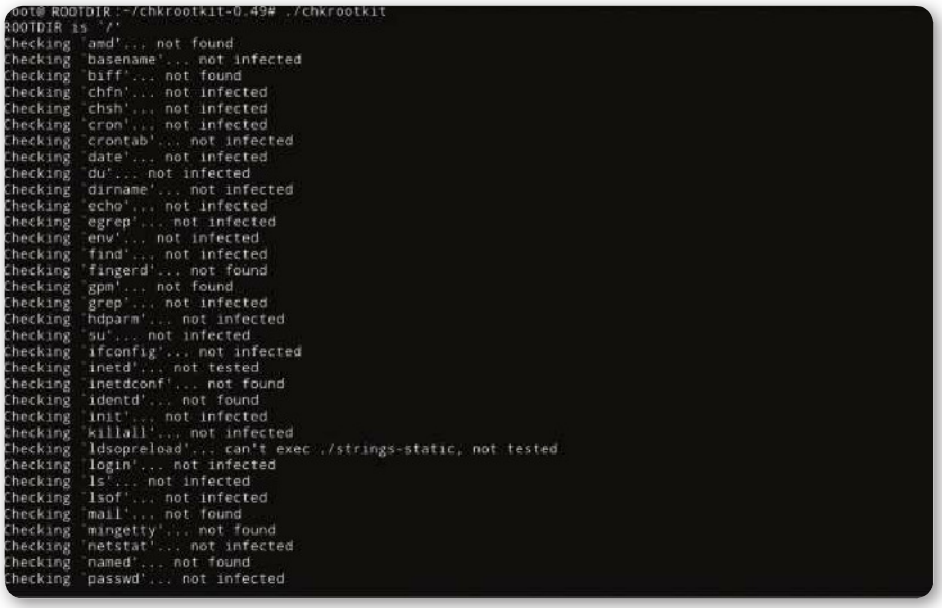


Figura 28. **Chkrootkit** chequea los archivos del sistema operativo en busca de alteraciones.

- **rkhunter**: permite identificar rootkits, backdoors y malware en general, comparando el hash de los archivos más importantes del sistema con una base de datos en Internet. Identifica archivos ocultos, permisos incorrectos y cadenas sospechosas en el kernel. Requiere la presencia de comandos como **cat**, **sed**, **head**, **tail**, **stat**, **readlink**, **md5/md5sum** o **sha1/sha1sum** para realizar las comprobaciones. **Rootkit Hunter** solo corre en el equipo donde se ejecuta; es pasivo, porque requiere de una ejecución manual o automática; es **post-incidente**, ya que detecta las amenazas una vez que fueron realizadas y, por último, es **path-based**, dado que controla nombres de archivos pero no posee heurística o firmas, como los antivirus.

RESUMEN

En este capítulo aprendimos a protegernos a revisar en detalle la manera en que debemos administrar un sistema Linux. Vimos los comandos de consola básicos y realizamos diagnósticos de red y procesos a través de una consola de comandos, además detallamos la seguridad a nivel de kernel. Conocimos los sistemas de verificación de integridad y aprendimos a protegernos contra rootkits.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice a los sistemas GNU/Linux.
2. Describa los servicios básicos.
3. ¿Qué son los servicios secundarios?
4. ¿Cómo se gestionan los usuarios mediante una consola de comandos?
5. ¿Para qué sirve el comando **ls**?
6. ¿Qué entrega el comando **man**?
7. Mencione las herramientas que podemos usar para instalar paquetes.
8. ¿Para qué sirve el comando **ifconfig**?
9. ¿Cómo se utiliza el comando **iwconfig**?
10. ¿De qué forma podemos protegernos ante rootkits?

EJERCICIOS PRÁCTICOS

1. Realice una comparación de diversas distribuciones GNU/Linux.
2. Establezca los permisos para un directorio mediante una consola de comandos.
3. Utilice la herramienta **fdisk**.
4. Utilice el comando **cat**.
5. Realice un diagnóstico de red.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*04

Servidores web y FTP

En este capítulo revisaremos las características de los servidores web y FTP, conoceremos qué son y qué ventajas nos entregan. Además detallaremos las consideraciones que debemos tener en cuenta para administrarlos.

Qué es un servidor web

Un **servidor web**, también denominado servidor **HTTP**, es una aplicación o software que se ejecuta en una computadora que cumple con el rol de servidor en una arquitectura cliente-servidor. Esta aplicación se encarga de realizar conexiones bidireccionales o unidireccionales, sincronizadas o no, con uno o varios clientes, recibiendo peticiones y posteriormente respondiendo a dichas solicitudes utilizando un lenguaje de programación determinado del lado del cliente.

> LAS RESPUESTAS RECIBIDAS POR EL CLIENTE SON EJECUTADAS EN UN NAVEGADOR WEB

Las respuestas recibidas por el cliente son compiladas y ejecutadas por un navegador web. Para la transmisión de datos entre el servidor y el cliente, por lo general, se utiliza el protocolo de red HTTP que emplea el puerto TCP 80 y se encuentra en la capa de aplicación del modelo OSI. El término servidor web también es utilizado para referirse a la computadora que ejecuta la aplicación o software de servidor web.

Figura 1. Sitios web populares como Google o Facebook poseen grandes clústeres de servidores que se utilizan para satisfacer el número de peticiones diarias que se producen.

Funcionamiento

La aplicación de servidor web se ejecuta en una computadora servidor, a la espera de peticiones de clientes (navegadores web que se ejecutan en los clientes). Las peticiones al servidor suelen realizarse mediante HTTP utilizando el método de petición GET, en la que una página o un sitio se solicita, a través de la **URL** (*Uniform Resource Locator* o localizador uniforme de recursos) al servidor web. Por ejemplo, cuando ingresamos la dirección **www.organizacion.com/index.html** en la barra de direcciones del navegador, estamos ejecutando la siguiente petición GET:

> LOS NAVEGADORES WEB OFRECEN UNA INTERFAZ PARA PODER REALIZAR SOLICITUDES WEB

GET / index.html HTTP / 1.1 HOST: www.organizacion.com

Figura 2. HTML es el lenguaje por excelencia utilizado para el desarrollo de páginas web.

Las peticiones **POST** son el segundo tipo de petición HTTP más utilizado; su objetivo es el envío de datos. Los datos por enviar al servidor se incluyen en el cuerpo de la misma petición con las cabeceras HTTP asignadas correspondientes respecto al tipo de petición. Casi siempre se asocia con los formularios web en los que los datos suelen

ser cifrados para ser enviados de manera segura al servidor. Todo navegador web provee a sus usuarios de una interfaz para poder realizar una o varias solicitudes web. La interfaz está conformada por aquellos elementos del navegador que permiten realizar la petición de forma activa. Estas peticiones pueden ser realizadas también por aplicaciones que no sean un navegador web.

Aplicaciones

Además de la transferencia de código HTML, los servidores web pueden entregar aplicaciones web. Estas son porciones de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- **Aplicaciones en el lado del cliente**: el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java applets o JavaScript: el servidor proporciona el código de las aplicaciones al cliente, y este, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts).

Figura 3. Los formularios presentes en una página web se usan para el envío de datos desde el cliente al servidor. Por lo general, utilizan peticiones del tipo POST.

Comúnmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje JavaScript y Java, aunque pueden añadirse más lenguajes mediante el uso de plugin.

- **Aplicaciones en el lado del servidor**: el servidor web ejecuta la aplicación; esta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP. Por lo general, es más práctico que las aplicaciones se encuentren del lado del servidor ya que, al ejecutarse en el servidor y no en los clientes, estos últimos no requieren de ningún agregado para poder interpretar Java o JavaScript. Solo es necesario un navegador web básico.

Figura 4. Los hipervínculos, como los que devuelve Google después de una búsqueda, se utilizan para solicitar la URL al servidor web que la aloja.

HTML

HTML (**Hyper Text Markup Language**) o lenguaje de marcado de hipertexto, es un lenguaje de desarrollo que se utiliza para la elaboración de páginas web. Cumple con la función de describir y traducir la estructura y la información de una web, en forma de texto. También permite complementar el texto antes mencionado con otros objetos, como imágenes o videos. Además, puede ser utilizado, de forma limitada, para definir la apariencia de un documento y permite la introducción de scripts.

Qué es un servidor FTP

Antes de comenzar con la definición de un servidor FTP, debemos recordar qué es **FTP** (*File Transfer Protocol*) o protocolo de transferencia de archivos. Como bien lo especifica su nombre, consiste en un protocolo de red que se utiliza para el intercambio de archivos entre dos o más computadoras. Un servidor FTP es una aplicación o software que se ejecuta en una computadora que cumple con el rol de servidor en una arquitectura cliente–servidor, que utiliza el protocolo antes mencionado y que se encuentra conectada generalmente a Internet (puede que se encuentre conectada a otros tipos de redes, como redes LAN, MAN, etc.). Esta realiza conexiones bidireccionales o unidireccionales entre uno o varios clientes para intercambiar archivos.

Figura 5. Con el surgimiento de internet, es muy común la utilización de servidores FTP web, es decir, fuera del entorno local, a los cuales podemos acceder a través del navegador.

Las computadoras dispuestas a intercambiar archivos deben encontrarse conectadas a una red **TCP** (*Transmission Control Protocol*) o protocolo de control de transmisión. Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario casi siempre utilizará el FTP para conectarse

remotamente a uno y, así, intercambiar información con él. Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes; o como **servidor de backup** (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (*Secure File Transfer Protocol*) o protocolo de transferencia de archivos seguro.

> LA APLICACIÓN MÁS COMÚN DE UN SERVIDOR FTP SUELE SER EL ALOJAMIENTO DE ELEMENTOS WEB

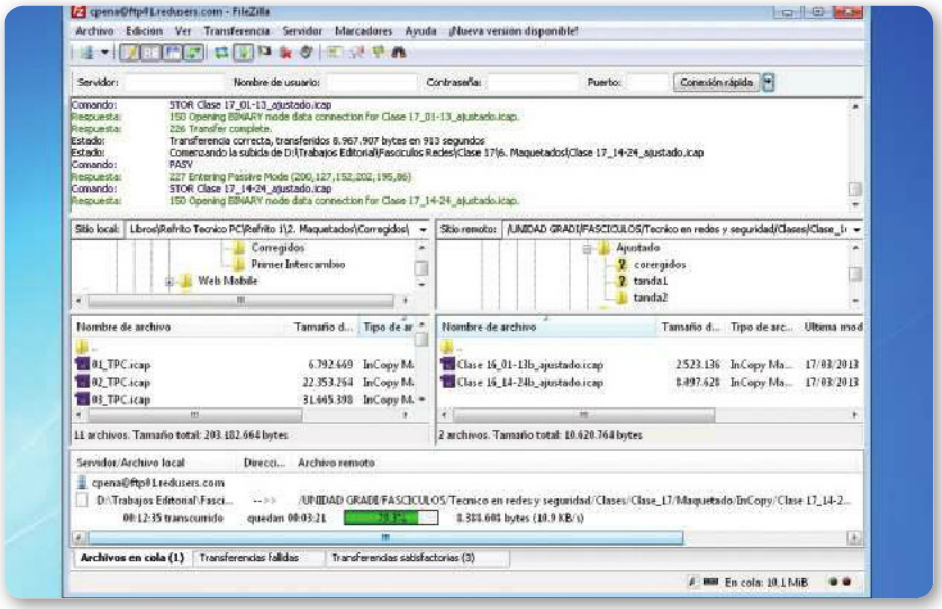


Figura 6. FileZilla es un cliente FTP muy popular a la hora de acceder a un servidor FTP dejando de lado el navegador web.

FILEZILLA

FileZilla es una aplicación cliente FTP multiplataforma, de código abierto y libre, licenciada bajo la Licencia Pública General de GNU. Soporta los protocolos de transferencia de archivos FTP, **SFTP** (**Secure FTP**) y **FTP sobre SSL/TLS**. Como características principales podemos resaltar que posee un administrador de sitios, permite crear y almacenar listados de sitios FTP con la información de conexión, registro de mensajes y, también, muestra en modo consola las instrucciones enviadas al servidor.

Una computadora cliente puede conectarse a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada nodo.

Funcionamiento

El servicio FTP se encuentra dentro de la capa de aplicación del modelo de red TCP/IP y utiliza los puertos TCP 20 y 21. Debemos tener en cuenta que la principal desventaja que presenta es que está pensado para ofrecer la máxima velocidad, pero no la máxima seguridad, ya que todo el intercambio de información, desde el *login* y *password* del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede realizar la captura de este tráfico, acceder al servidor y luego apropiarse de los archivos transferidos.

> EL SERVICIO FTP SE ENCUENTRA DENTRO DE LA CAPA DE APLICACIÓN DEL MODELO TCP/IP

Para solucionar este problema, son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos, pero cifrando todo el tráfico.

Figura 7. Para acceder a un servidor FTP, es necesario ingresar un usuario y una contraseña válidos.

Tipos de usuarios

Ahora veremos los tipos de usuarios en un servicio de FTP.

- **Usuario anónimo**: se trata del tipo de usuario que permite que cualquier persona pueda acceder a un servicio FTP sin que su administrador deba intervenir para realizar la creación de la cuenta correspondiente. Para poder acceder a un servidor FTP como usuario anónimo, solo basta con ingresar la palabra **anonymous** cuando este pregunte por la cuenta.
- **Usuario común**: si deseamos poseer privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes y también la posibilidad de subir nuestros propios archivos al servidor, por lo general, se suele necesitar de este tipo de cuenta.
- **Usuario invitado**: se trata de un tipo de usuario que se utiliza para permitir el acceso a entornos restringidos, como ocurre con el usuario anónimo, pero con más privilegios.

> EXISTEN DIFERENTES TIPOS DE USUARIOS PARA ACCEDER Y UTILIZAR UN SERVICIO DE FTP

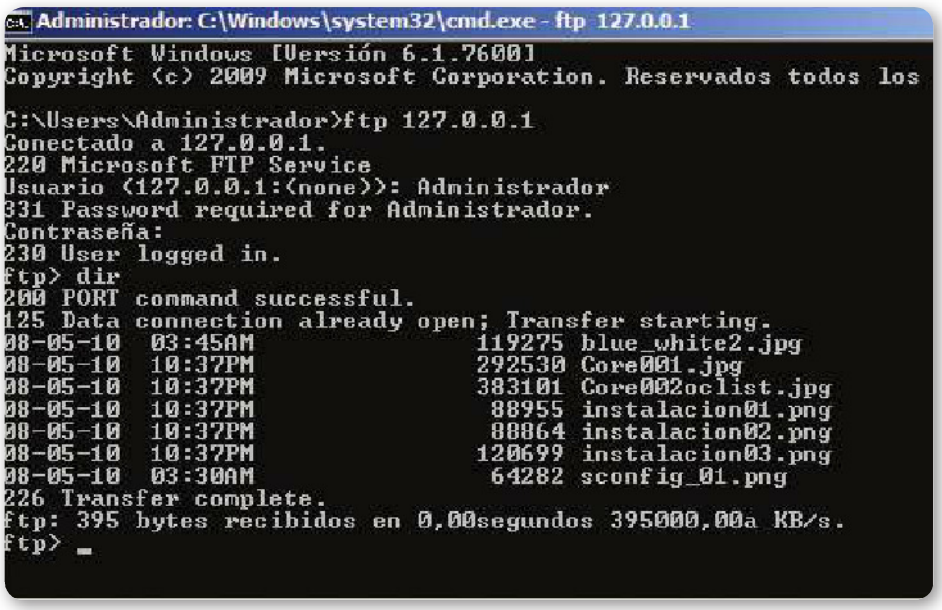


Figura 8. La consola de comandos de Windows posee el comando **FTP**. Con él podemos, de forma básica, conectarnos a un servidor FTP, autenticarnos e intercambiar archivos.

Administración de un servidor web

En la actualidad, instalar y poner en línea un **servidor web** no posee una complejidad alta asociada. Puede ser un trabajo que consuma solo algunas horas de nuestro tiempo, incluso para personas inexpertas, dada la gran cantidad de información que se encuentra circulando en Internet al respecto. Además, existen empresas y organizaciones que se dedican a alquilar espacio en servidores dedicados, lo que simplifica la necesidad de montar nuestro propio servidor web.

Figura 9. **QtdSync** es excelente cliente–servidor para poder implementar la utilización de **rsync** en la sincronización de archivos y directorios.

A diferencia de la instalación y puesta en línea, el **mantenimiento y monitoreo** de nuestro servidor es una tarea ardua que implica prevención, configuración, actualización del software relacionado, escalado del hardware y de los medios de conexión a medida que el tráfico aumenta, etc. La estabilidad de un servidor web (entendiendo como *estabilidad* el brindar un servicio continuo en el tiempo, libre

de cuelgues y fallos) va a depender de la calidad de las actividades de mantenimiento y monitoreo que se realizan de manera periódica. El éxito de mantener un servidor activo y en línea depende directamente de la previsión que tengamos por adelantado.

Previsión

Aunque la falta de previsión es un problema difícil de detectar en etapas tempranas, puede que sea visible luego de meses o, incluso, de años de la instalación y puesta en línea del servidor web, cuando ya sea demasiado tarde para realizar acciones correctivas con el objetivo de restablecer el servicio en el corto plazo. Puede salir a la luz en momentos críticos cuando se produce un tráfico elevado repentino, cuando falla un disco duro o al sufrir un ataque informático (**hackeo**).

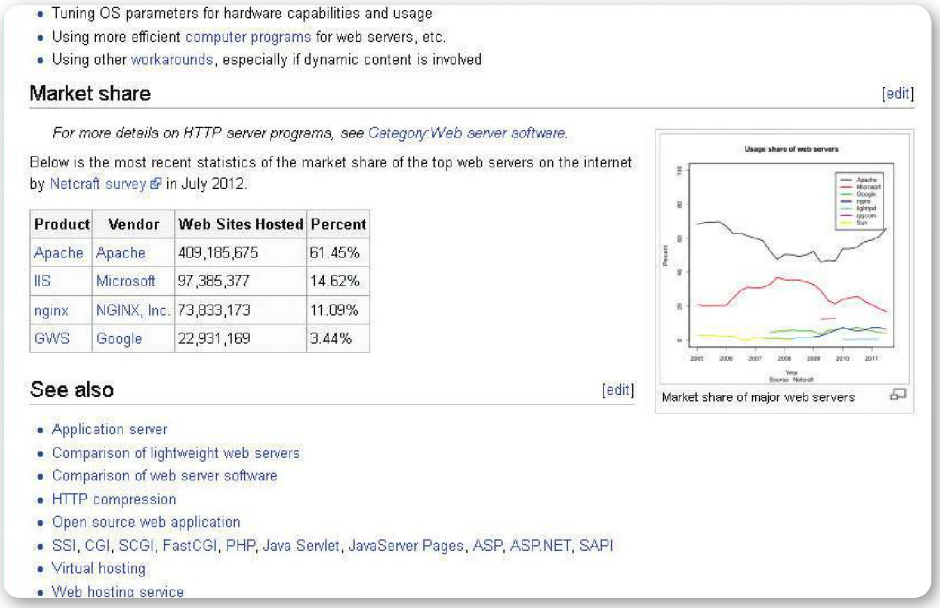


Figura 10. Apache Web Server es la aplicación líder en el mercado de servidores web según un estudio que menciona el sitio Wikipedia, realizado hasta julio de 2012.

Cabe aclarar que la previsión tiene sus límites, y resulta imposible tener en cuenta todos los escenarios posibles; lo saludable es proyectar una evolución del servicio para poder ir escalando el servidor a medida que el tráfico aumenta, estar al tanto de fallos de seguridad y actualizaciones de software para corregir defectos en los sistemas,

implementar políticas de respaldo y restauración de la información y de las aplicaciones, y monitorear el ecosistema en busca de fallos de hardware y ataques, para aplicar acciones correctivas lo antes posible.

Consideraciones

A continuación, analizaremos algunos aspectos importantes para tener en cuenta en la administración de un servidor web:

- **Implementación de políticas de respaldos (backups)**: si bien este aspecto resulta un poco obvio, en la práctica no se le suele asignar la importancia que requiere. Si carecemos de un plan de respaldo concreto, es hora de que nos sentemos cuanto antes a delinearlo y a ponerlo en práctica. No hay otra forma de asegurarnos de que la información perteneciente a nuestro servidor web, la que se genera como resultado de la operatoria cotidiana, esté a salvo si se produce una caída del servicio por fallos de hardware o software.
  Cuando hablamos de respaldos, tenemos dos objetos genéricos que requieren de nuestra atención: los directorios y archivos físicos, y las bases de datos, si es que nuestro servidor web las posee.
  Para respaldar los directorios y archivos, podemos utilizar software como **rsync**, **tar**, y similares. Este tipo de software se encarga de replicar y sincronizar cambios en directorios y archivos en una computadora remota.
  Para respaldar bases de datos, debemos utilizar las herramientas específicas que ofrecen los distintos motores de bases de datos.
  En ambos casos, lo ideal es que implementemos un proceso automático o semiautomático de backup para estar seguros de que los respaldos se van a realizar independientemente de nuestra disponibilidad para llevarlos a cabo.

ALTERNATIVA LIBRE

La aplicación **rsync** es una alternativa libre desarrollada para sistemas de tipo Unix y Microsoft Windows; esta herramienta nos ofrece una transmisión eficiente de datos incrementales, que opera también en forma eficiente con datos comprimidos y cifrados.

- **Verificación de los respaldos realizados**: una vez que el proceso de respaldo de información se encuentra operativo, es decir, en funcionamiento, es necesario que validemos, con periodicidad, que los archivos de respaldo generados estén correctamente conformados (no se encuentren corruptos) y se puedan restaurar con éxito. Es muy posible que necesitemos de un entorno de prueba, es decir, una infraestructura similar a la principal en donde restaurar los backups y verificar que nuestro servidor funcione en forma correcta. Además, frente a una eventualidad real, sabremos cómo proceder gracias a las restauraciones de prueba realizadas.
- **Limpieza de archivos de auditoría (logs)**: otro punto para tener en cuenta es la limpieza periódica de archivos logs generados que posean una antigüedad definida con anterioridad. Estos deberían ser limpiados de forma automática cada cierto período de tiempo para optimizar la utilización del espacio físico. Cuando la cantidad de transacciones que se ejecutan contra el servidor asciende a un número considerablemente alto, puede que los archivos logs generados terminen por utilizar todo el espacio en disco disponible para nuestro servidor y produzcan una caída del servicio.
- **Monitoreo de la utilización de los recursos**: así como es importante implementar una política de respaldos, monitorear la utilización de los recursos también es clave. Debemos verificar periódicamente la carga de procesos a la que es sometida la CPU, el uso de memoria RAM, el espacio disponible en disco y el ancho de banda de la conexión a Internet que se consume. De esta manera, vamos a poder determinar con antelación cuándo realizar una actualización (upgrade) de hardware. Cuando mencionamos upgrade de hardware, nos referimos a instalar más memoria RAM, agregar un disco duro nuevo, contratar un ancho de banda mayor, etc. Tengamos en cuenta que si no tomamos este tipo de precauciones, puede que un día el crecimiento en la demanda del servicio termine haciendo colapsar nuestro servidor.
- **Monitoreo de procesos y servicios**: mantener en ejecución software como Apache, Internet Information Server (IIS), MySQL,

> ES NECESARIO CONSIDERAR LA LIMPIEZA DE LOS ARCHIVOS LOGS EN FORMA PERIÓDICA

servicios de correo electrónico (pop, smtp, imap) y demás puede ser crucial para mantener a nuestros usuarios satisfechos. Deberíamos utilizar alguna herramienta de software que se encargue de automatizar el proceso de monitoreo de los servicios para que nos informe en caso de que se produzca algún fallo y nos evite enterarnos de este a través de la queja de un usuario.

- **Endurecer nuestro servidor (hardening)**: el proceso de hardening o endurecimiento consiste en mantener nuestro servidor seguro frente a las diferentes amenazas que se encuentran en la Web, tanto las conocidas como las futuras. Por eso, resulta importante que conozcamos qué procesos se ejecutan en nuestro servidor para detectar procesos anormales, qué puertos tenemos abiertos para interiorizarnos de los peligros que ello conlleva, mantenernos informados sobre los distintos síntomas que producen las principales amenazas, para poder actuar con celeridad frente a un ataque, etcétera. El mantenernos informados sobre las novedades en materia de seguridad nos va a permitir aplicar nuevas tecnologías a nuestro sistema y reducir los riesgos.
- **Actualizaciones de seguridad**: ningún software se encuentra ciento por ciento libre de fallos y errores que pueden aprovechar las amenazas para vulnerar nuestro servidor. Partiendo de esta regla, debemos estar al tanto sobre las actualizaciones que se liberan con el fin de solucionar estos defectos, para descargarlas e instalarlas lo antes posible. No aplicar las actualizaciones a nuestro sistema es definitivamente un comportamiento negligente, ya que las vulnerabilidades de las distintas aplicaciones se divulgan muy rápido por Internet y, a medida que pasa el tiempo, más atacantes se ponen al tanto de ellas. Debemos considerar que los riesgos crecen exponencialmente con el tiempo.

ENDURECIMIENTO

El **hardening** o **endurecimiento** es el proceso que nos permite asegurar un sistema de datos mediante la reducción de las vulnerabilidades que presenta; esto se logra eliminando aplicaciones, servicios, usuarios, entre otros elementos que son innecesarios en el sistema; además podemos cerrar puertos que tampoco estén en uso por el sistema operativo.

Alternativas

Dos de los servidores web más conocidos en la actualidad,hablando de software, son **Apache Web Server**, de **Apache Foundation**, e **Internet Information Server (IIS)**, de **Microsoft**. Dado que el primero es la solución más popular, a continuación vamos a describir algunas consideraciones para tener en cuenta y configurarlo correctamente.

> APACHE WEB SERVER ES UNO DE LOS SERVIDORES WEB MÁS UTILIZADOS EN LA ACTUALIDAD

Partiendo del hecho de que poseemos una capacidad de hardware limitada y que Apache Web Server está diseñado para soportar múltiples peticiones simultáneas de decenas o centenares de usuarios (si nuestro sitio es popular), es fácil darse cuenta de que el hardware existente puede no ser suficiente para que el software de servidor web funcione a su máxima capacidad. Nuestro servidor permanecerá expectante, a la espera de peticiones de conexión realizadas por usuarios y, a medida que vayan llegando, destinará a un proceso (o un hilo de ejecución) a atenderlas.

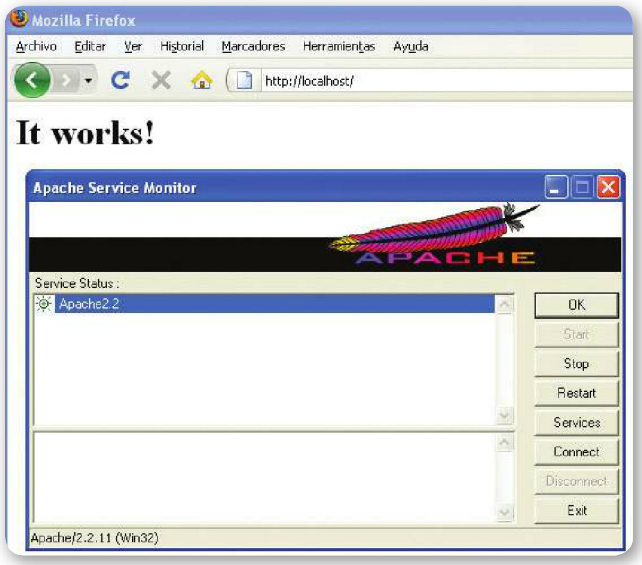


Figura 11. La aplicación **Apache Service Monitor** nos permite administrar nuestro servidor web de manera centralizada, gráfica e intuitiva.

Mientras mayor sea la cantidad de peticiones que se formulen de manera simultánea, más procesos/hilos necesitaremos para satisfacer

la demanda, y consumiremos más recursos del servidor, sobre todo memoria. Un servidor web consume mucha memoria RAM cuando se encuentra en funcionamiento y a medida que el tráfico aumenta. Este va a ser el recurso clave que debemos aprender a gestionar: la RAM que no se utiliza se desperdicia y provoca que perdamos visitantes o que estos sean atendidos con mayor lentitud. Pero, si no controlamos el consumo y el servidor la agota, comenzará a hacer swapping a disco, y evitar esto es la regla de oro: si llegamos a esta instancia, se habrá caído y, posiblemente, deberemos reiniciar el servicio.

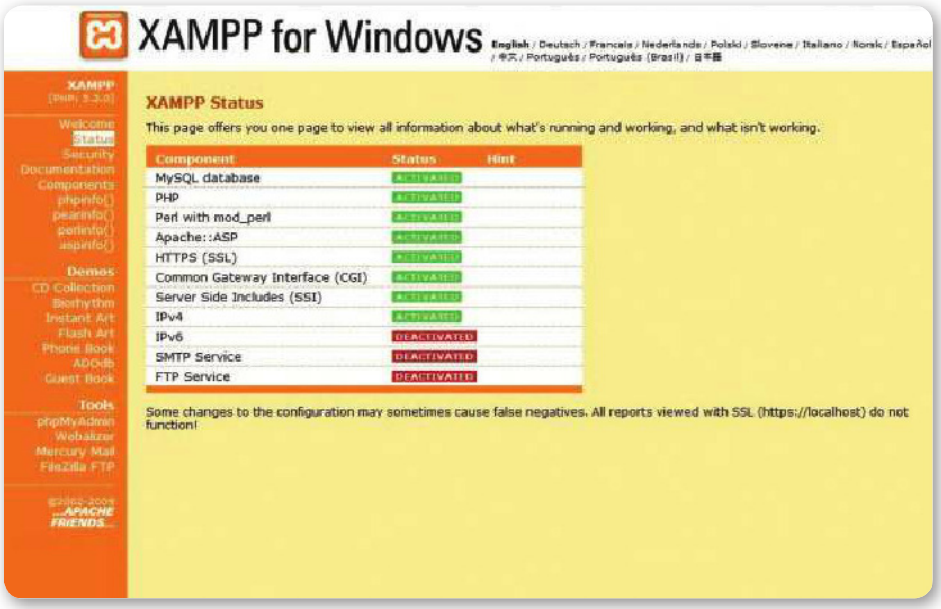


Figura 12. La aplicación **Xampp** es una solución de software más completa para implementar un servidor web y cuenta con Apache entre sus componentes.

Los principales ajustes que necesitamos realizar se encuentran en los siguientes parámetros del archivo de configuración **httpd.conf** que se halla en la ruta **C:\Apache\conf.**

- **Timeout** establece la cantidad de tiempo medido en segundos que Apache esperará a determinados eventos antes de cerrar o abortar una conexión. En servidores con pocos recursos, 300 segundos puede ser una cantidad bastante elevada. Reducir ese tiempo sustancialmente ayudará a gestionar mejor la memoria del servidor. Valores de 30 o 40 son óptimos en servidores

con pocos recursos. Un valor de 10, incluso, podría mejorar el rendimiento en determinados contextos.

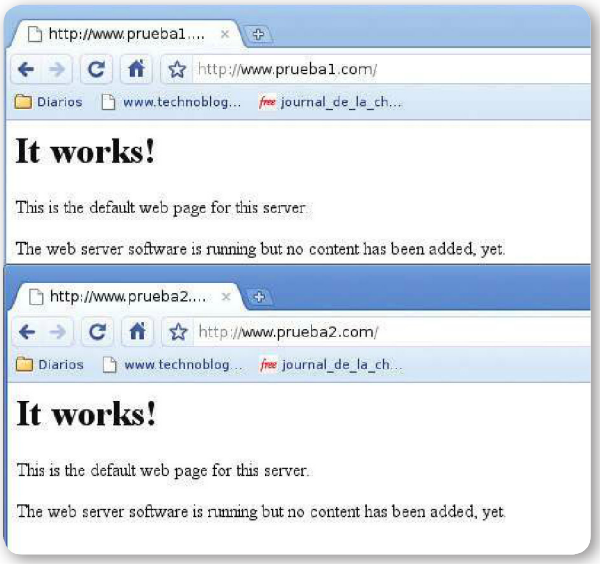


Figura 13. Otra de las características de **Apache Web Server** es que permite definir hosts virtuales para alojar más de un sitio en una misma instalación física.

- Los tres parámetros, **KeepAlive**, **KeepAliveTimeout** y **MaxKeepAliveRequest**, definen la posibilidad de usar conexiones persistentes y la forma de tratarlas. En concreto, el número de solicitudes que se permitirán sobre cada conexión (**MaxKeepAliveRequest**) y el tiempo de espera sin solicitudes antes de abortarlas. Tener habilitadas este tipo de conexiones reduce en gran medida la carga del servidor y los tiempos de respuesta, y el número de solicitudes se puede mantener alrededor de 100 en casi cualquier entorno. Es, de nuevo, el Timeout por defecto de 15 segundos el que puede resultar demasiado elevado en servidores con poca RAM, y podríamos reducirlo a un valor de 5 segundos o incluso menos.

> A DIFERENCIA DE LA INSTALACIÓN, EL MANTENIMIENTO Y MONITOREO ES UNA TAREA ARDUA

- Los parámetros restantes, **StartServers**, **MinSpareServers** y **MaxSpareServers**, ajustan, respectivamente, la cantidad de procesos Apache que se crearan al inicio, y el mínimo y máximo de estos que mantendremos inactivos a la espera de que lleguen solicitudes

de posibles usuarios. Los procesos inactivos definidos por estos parámetros consumirán memoria, pero nos permitirán dar una respuesta más rápida a los usuarios (los procesos están ya listos para usarse cuando llegan peticiones y no hay que perder tiempo en crearlos), así que, en un servidor con grandes recursos y que espera cargas elevadas, querríamos tener valores más elevados de los que vienen por defecto, mientras que, en un servidor pequeño, podríamos reducirlos todos a, por ejemplo, 3 o 4.

```
# be kept in a single file for simplicity.  The commented-out values
# below are the built-in defaults.  You can have the server ignore
# these files altogether by using "/dev/null" (for Unix) or
# "nul" (for Win32) for the arguments to the directives.
#
#ResourceConfig conf/srm.conf
#AccessConfig conf/access.conf

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
```

Figura 14. Para configurar la aplicación Apache Web Server, es necesario editar el archivo de configuración **`httpd.conf`**.

- **MaxClients** es, quizás, el parámetro más importante. Define la cantidad máxima de procesos simultáneos que nuestro servidor podrá crear para atender solicitudes. Un número más pequeño del

FUNCIONAMIENTO DE RSYNC

Es una aplicación de código abierto para sistemas basados en Unix y Windows, que permite sincronizar archivos y directorios entre dos computadoras conectadas a una red o entre dos ubicaciones dentro del equipo local minimizando el volumen de los datos transferidos. Es muy útil para satisfacer políticas de respaldo. Actúa como un proceso demonio en el servidor y utiliza el puerto **TCP 873**.

que podemos permitirnos desperdiciará memoria y ralentizará las solicitudes de muchos usuarios (que permanecerán a la espera de que uno de estos procesos se libere para atenderlo) mientras que un número demasiado elevado agotará la memoria del servidor y lo obligará a hacer swapping a disco. Lo primero que se nos puede ocurrir es que, dividiendo la memoria que tenemos disponible entre lo que ocupa cada proceso de Apache, obtendríamos la cantidad que necesitamos, pero el problema es que la memoria disponible resulta difícil de calcular de forma exacta (ya que, posiblemente, tendremos también un servidor **MYSQL**, servicios de correo, etc.). Además, los procesos de Apache no consumen todos la misma cantidad de memoria. Si tenemos distintas instancias de Apache con características muy diferentes, la diversidad será aún mayor.

- Tenemos todavía un parámetro más, **MaxRequestsPerChild**, que define la cantidad de solicitudes que atenderá cada proceso antes de reciclarse. El valor por defecto es cero, que indica un número ilimitado. Definir un valor elevado pero no ilimitado ayudará también a que nuestro servidor libere y limpie su memoria de forma regular. Un valor de entre 500 y 1000 podría ser adecuado para nuestra pequeña computadora.

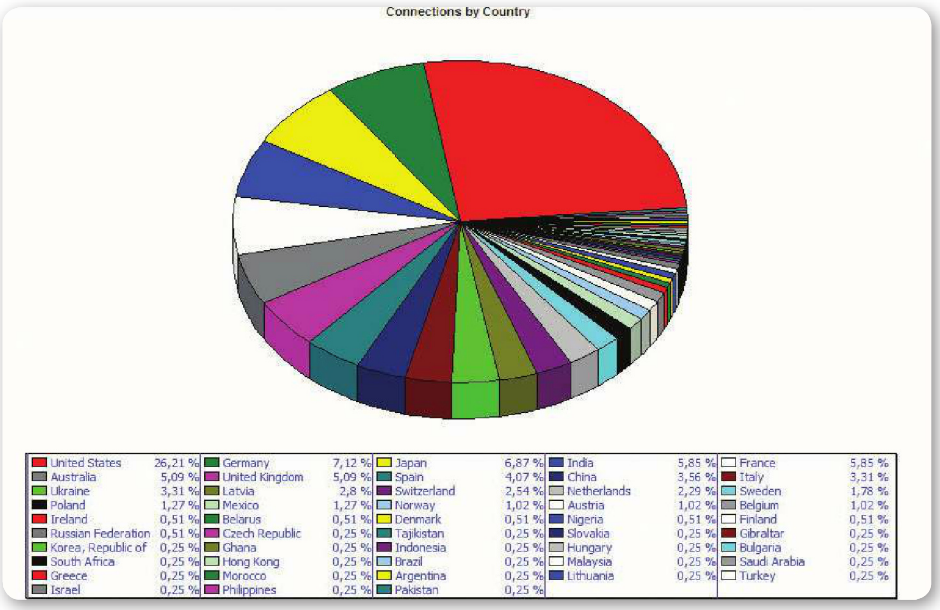


Figura 15. Existen en el mercado varias herramientas de software para generar y poder consultar estadísticas de funcionamiento de un servidor web. **HSLAB HTTP Monitor** es una de ellas.

Administración de un servidor FTP

Un **servidor FTP** es un programa de software que se ejecuta sobre una computadora que cumple el rol de servidor y generalmente conectado a Internet (existe la posibilidad de que esté conectado a otros tipos de redes como redes LAN, MAN, etc.). Su función es la de proveer un servicio de intercambio de archivos. Las aplicaciones de servidor FTP no suelen instalarse en computadoras personales. Casi siempre, un usuario de un servicio FTP se conecta a un servidor FTP que aloja el servicio a través de un software cliente FTP instalado en una computadora cliente. Una aplicación ampliamente extendida del servicio FTP es el alojamiento de páginas web; se utiliza para actualizar y agregar archivos en sitios de Internet y realizar respaldos.

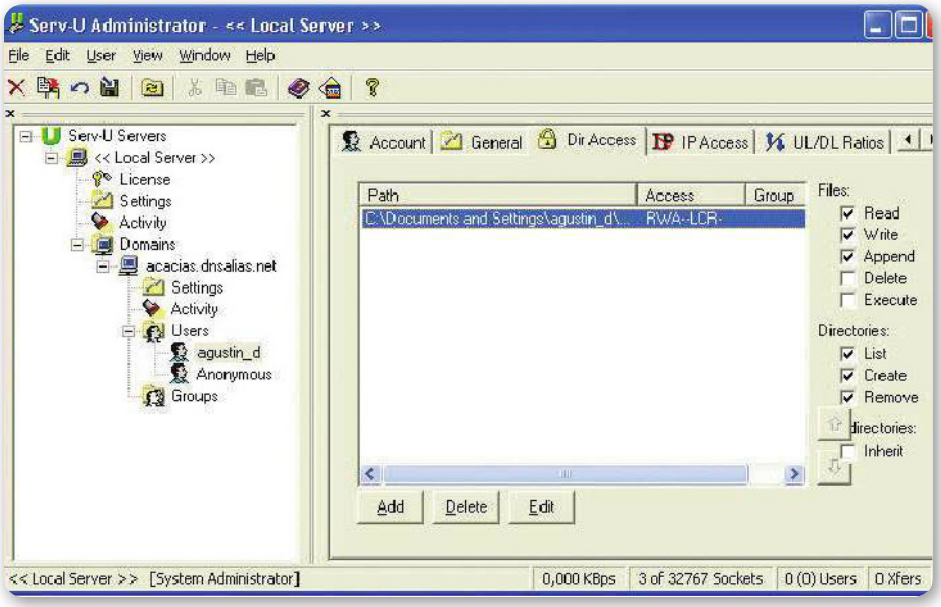


Figura 16. Los privilegios asignados a los usuarios de un servicio FTP delimitan las acciones que pueden realizar dentro del servidor.

En la actualidad, instalar un servidor FTP resulta bastante sencillo dada la gran cantidad de información que se encuentra en Internet al respecto. Tutoriales paso a paso, guías visuales con capturas de pantalla y muchas opciones gratuitas o pagas en lo que se refiere al

software. No obstante, el administrar un servidor FTP no resulta tan sencillo, ya que debemos tener una serie de consideraciones para poder mantener el servicio en línea y saludable a lo largo del tiempo.

A continuación, vamos a destacar algunos de los objetos que un administrador debe administrar en su labor diaria.

Usuarios

Antes que nada, debemos definir a quién vamos a dirigir el servicio; si a un conjunto de usuarios bien definidos, al público en general, a usuarios ocasionales, etc. Esta elección va a delimitar y a encuadrar la administración futura de usuarios.

Acceso anónimo (Anonymous): los servidores FTP anónimos ofrecen sus servicios de forma libre y gratuita a todos los usuarios (público en general), les permiten acceder a los archivos alojados en ellos sin la necesidad de poseer una cuenta de usuario definida. Es una forma práctica de permitir que todos los usuarios asiduos y potenciales tengan acceso con privilegios definidos sin que para ello el administrador del servidor deba crear una cuenta para cada usuario y asignarle los permisos correspondientes (la administración no requiere de la intervención del administrador).

> ES NECESARIO DEFINIR A QUÉ TIPO DE USUARIOS VAMOS A DIRIGIR EL SERVICIO DE FTP

Debemos considerar que si un servidor posee un servicio **FTP anonymous**, solo debemos ingresar **anonymous** cuando este solicite el usuario durante el proceso de autenticación. No se requiere de ninguna contraseña preestablecida, aunque tendremos que ingresar una contraseña durante el logeo, la cual no será sometida a proceso de

ACCESO DE USUARIO

Es importante considerar que si deseamos tener privilegios de acceso a cualquier parte del sistema de archivos que ofrece un servidor FTP, o los permisos para realizar la modificación de los archivos que se encuentren en sus carpetas, y también la posibilidad de subir nuestros propios archivos, generalmente se suele realizar mediante una cuenta de usuario que debe ser creada por el administrador del servicio.

> UN ACCESO ANÓNIMO, GENERALMENTE NOS PERMITE LEER Y COPIAR ARCHIVOS

validación alguno. Por lo general, se suele utilizar la dirección de correo electrónico propia.

Solamente con eso se consigue acceso a los archivos del FTP, aunque con menos privilegios que un usuario normal. Casi siempre, solo tendremos privilegios de lectura y copia sobre los archivos que sean públicos, estos serán indicados por el administrador del servidor al que nos estemos conectando.

Debemos considerar que en la mayoría de los casos se utiliza un servicio FTP anónimo para proceder a almacenar archivos de gran tamaño, los cuales no tienen utilidad si no son transferidos a la máquina del usuario, como por ejemplo programas, y se reservan los servidores de páginas web (HTTP) para almacenar información textual destinada a la lectura en línea.

Acceso de usuario común: si vamos a interactuar con usuarios que necesitan contar con privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes y la posibilidad de subir archivos propios, es común que se establezcan usuarios de este tipo. En el servidor se almacena la información de las distintas cuentas de usuario que pueden acceder a él con sus privilegios correspondientes, de manera que, para iniciar una sesión FTP, debemos introducir una cuenta de usuario (**login**) y una contraseña (**password**) válidas que nos identifiquen unívocamente. La administración de este tipo de usuarios requiere de la intervención del administrador. Consideremos que para simplificar la gestión de usuarios, cuando el grupo de estos se encuentra bien delimitado al igual que sus permisos, podemos heredarlos de un dominio dependiendo de la aplicación servidor que utilicemos.

Acceso de invitado (Guest): este tercer tipo de usuario es una combinación de los dos anteriores. El objetivo de esta clasificación o tipificación es permitir que cada usuario se conecte al servidor utilizando su cuenta y contraseña, pero evitar de forma general que tengan acceso a partes del sistema y directorios que no necesitan para realizar su labor. De esta manera, estamos realizando la creación de un entorno restringido genérico que se puede aplicar a un conjunto de cuentas y, con esto, nos encargamos de realizar la disminución de la intervención requerida del administrador.

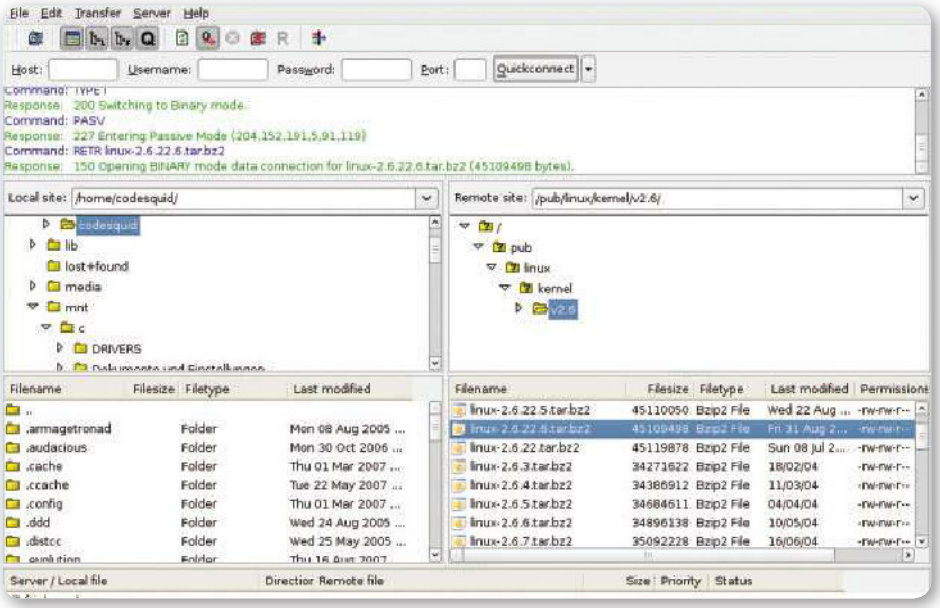


Figura 17. Mediante un cliente podremos utilizar nuestro usuario y contraseña para acceder a los archivos a través del protocolo FTP.

Privilegios

Una vez definidos los usuarios, debemos asignarles los privilegios que tendrá. Es necesario que asociemos los directorios con los que va a trabajar al usuario. Y luego definir los permisos con los que contará por cada directorio y para los archivos contenidos.

Los permisos para los directorios pueden ser:

- **Listar**: para poder listar el contenido de los directorios.
- **Crear**: para crear directorios dentro del directorio asociado.
- **Remover**: para eliminar directorios dentro del directorio asociado.

Estos permisos se asignan por cada directorio que se asocia al usuario. Los permisos que se pueden asignar para el conjunto de archivos contenidos en un directorio son:

- **Lectura**: para descargar archivos existentes dentro del directorio remoto a la computadora local.
- **Escritura**: para poder subir archivos nuevos dentro del directorio.
- **Eliminación**: este permiso es necesario para poder eliminar archivos dentro del directorio especificado.

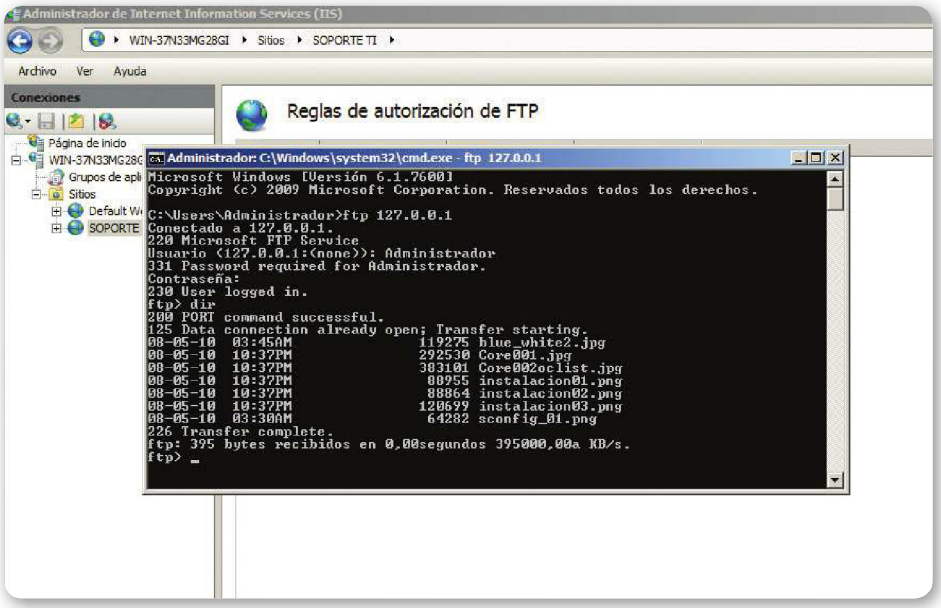


Figura 18. No es necesario acceder a un servidor FTP a través de una GUI. Podemos utilizar instrucciones básicas a través de una ventana de comandos.

Cabe aclarar que los privilegios se pueden asignar para grupos de usuarios, por lo que la actividad del administrador se simplifica.

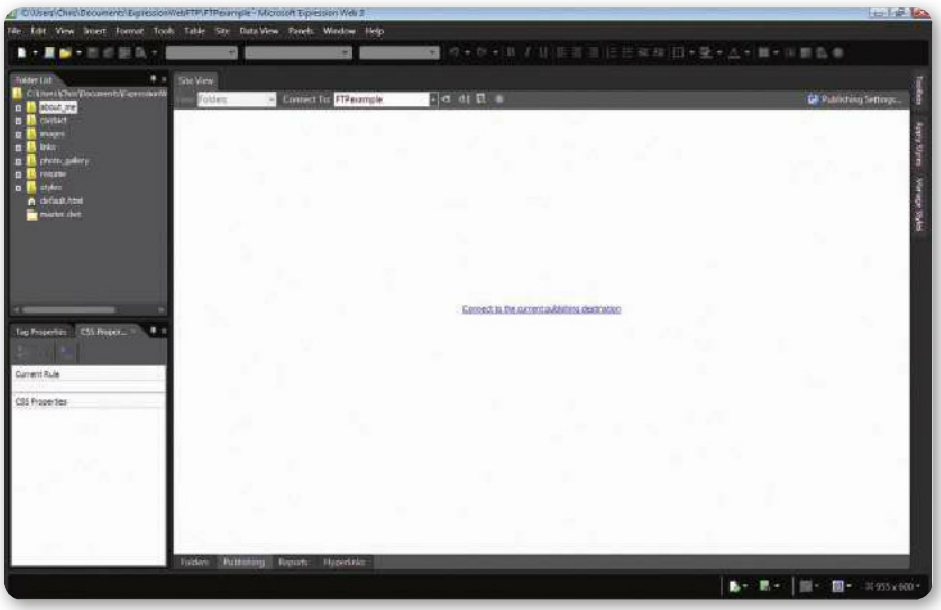


Figura 19. Además de aplicaciones cliente, también existen clientes web para poder consumir los servicios de un servidor FTP.

Cuota de disco

Mediante el establecimiento de cuotas de disco, podemos limitar el espacio de disco disponible para utilizar por los usuarios, de manera de prevenir un posible colapso del sistema en caso de que estos agoten el total de espacio en disco que posee el servidor. De esta manera, cuando un usuario agota su cuota de disco, debe o bien eliminar archivos existentes para ganar espacio libre o bien solicitarle al administrador que amplíe su cuota.

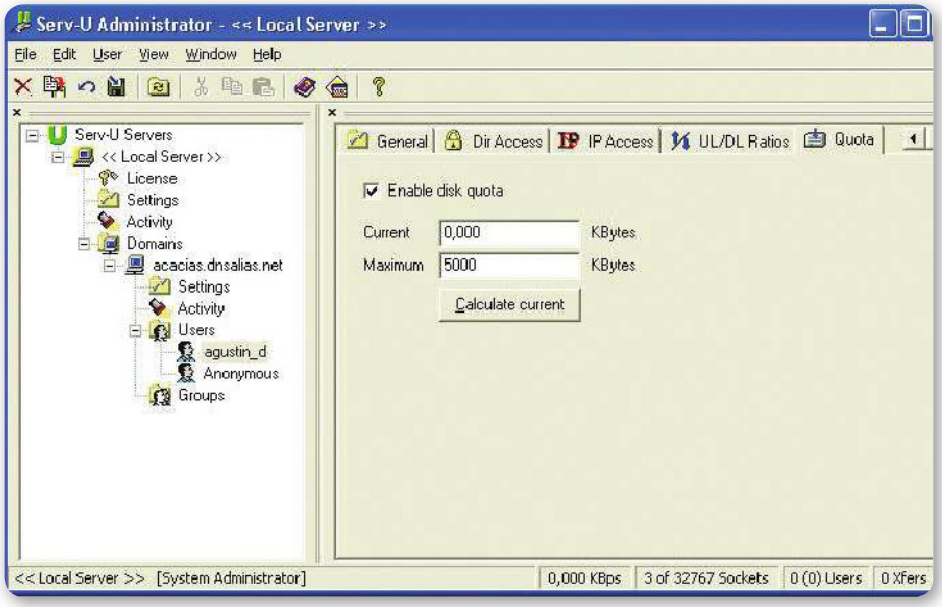


Figura 20. Las cuotas de disco son una herramienta útil para los administradores de sitios FTP debido a que contribuyen a una gestión eficiente del espacio físico.

Ratios UL/DL

Este parámetro se utiliza para definir el ancho de banda de la conexión para la subida de archivos y para la descarga de archivos de forma separada, por cada usuario. De esta manera, podemos limitar el consumo de ancho de banda a un máximo en horarios pico para asegurar que el servidor no se colapse como ocurriría si el ancho de banda fuera ilimitado para cada usuario. También permite asegurar una cierta calidad de conexión. Como desventaja, puede suceder que un usuario posea ancho de banda ocioso, es decir, que no lo esté utilizando, y otro usuario necesite más ancho de banda del asignado.

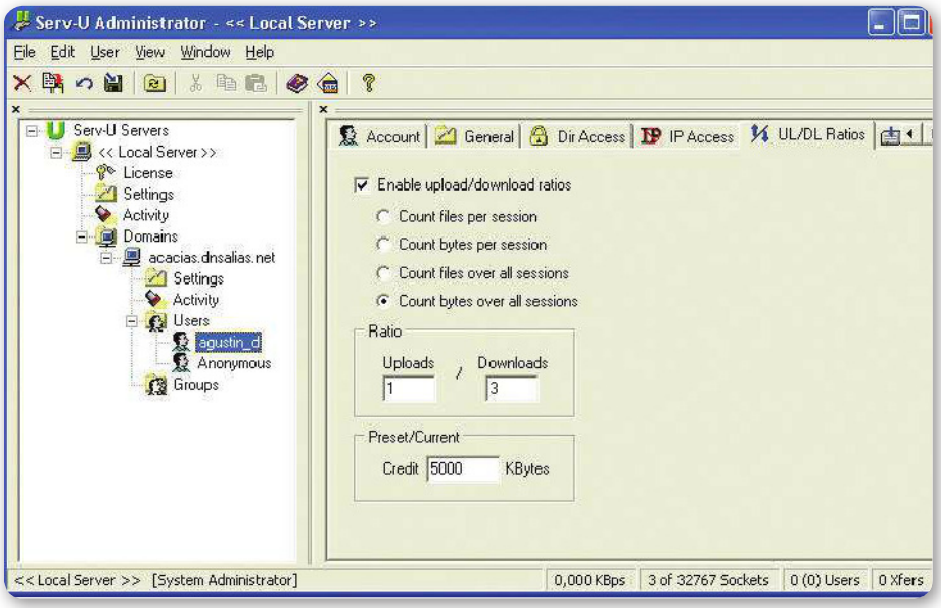


Figura 21. Los ratios de subida y descarga contribuyen a una gestión eficiente de los anchos de banda que posee un servidor FTP.

Modos de Conexión

Es necesario especificar con qué modo de conexión va a trabajar nuestro servidor. En este sentido FTP soporta dos modos de conexión: el modo activo y el modo pasivo.

Modo activo: en el modo activo, el servidor siempre crea la conexión en su propio puerto TCP 20, mientras que del lado del cliente la conexión se asocia a un puerto aleatorio mayor al puerto TCP 1024. Para ello, el cliente le envía un mensaje al servidor indicándole el número de puerto, de forma tal que el servidor pueda abrir una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado. La principal desventaja que presenta este modo es que el cliente debe estar dispuesto a aceptar cualquier conexión entrante a un puerto TCP superior al puerto TCP 1024 con los riesgos que esto trae aparejado si consideramos que estamos conectados a una red insegura como lo es Internet. Además, por lo general, los cortafuegos o firewalls rechazan las conexiones aleatorias. La solución a esta desventaja es el modo pasivo.

> ADMINISTRAR UN FTP NO ES SENCILLO, PUES DEBEMOS CONSIDERAR MUCHAS OPCIONES

Modo pasivo: cuando un cliente envía una solicitud de conexión, el servidor FTP le indica un puerto TCP específico (mayor al puerto TCP 1023 del servidor) al que debe conectarse. El cliente inicia una conexión hacia el puerto TCP del servidor especificado anteriormente.

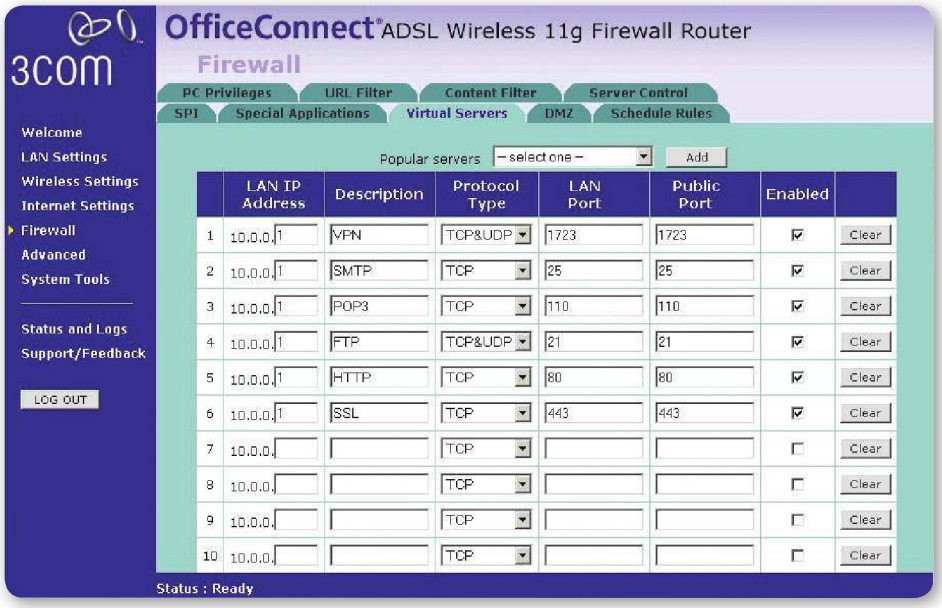


Figura 22. Para poder montar un servidor FTP hogareño, es necesario mapear el puerto **TCP 21** en la puerta de enlace a internet.

Para finalizar, podemos mencionar como soluciones concretas de servidor FTP el servicio FTP que se ofrece como parte integrante de la suite **Internet Information Services (IIS)** y **FileZilla Server**. La primera opción viene integrada con los sistemas operativos de Microsoft, y la segunda opción se puede descargar desde el sitio que encontramos en la dirección **http://filezilla-project.org**.

FTPS

También conocido como **FTP sobre SSL**, es un protocolo de transferencia de archivos basado en FTP que le agrega seguridad al encriptar las conexiones de transferencia utilizando el protocolo SSL. De esta manera, se solucionan las falencias o carencias que posee el protocolo FTP original en este aspecto. Existe otra variante del protocolo FTP, denominada **SFTP**, que también aumenta la seguridad encriptando las conexiones de transferencia, pero, a diferencia de FTPS, utiliza el protocolo SSH para realizar dicha tarea.

Figura 23. La solución del servidor FTP de Microsoft forma parte de la suite de servicios **Internet Information Services (IIS)**.

Seguridad en servidores web

Al considerar la seguridad de un servidor web, debemos tener en cuenta todos los componentes que forman parte del servicio. Es necesario considerar: la seguridad física del servidor, la seguridad lógica en el sistema operativo, los componentes de infraestructura que permiten el acceso a este, como por ejemplo: firewall, router y switch. Una vez analizados estos, debemos considerar la seguridad de la aplicación y el gestor web.

> LA SEGURIDAD DE UN SERVIDOR WEB DEBE CONSIDERAR TODOS LOS COMPONENTES DEL SERVICIO

En cuanto a la aplicación, hace falta que la codificación sea realizada considerando las cuestiones de seguridad. Para este fin, pueden utilizarse las guías y aplicaciones del proyecto **OWASP** para orientar el desarrollo seguro. El gestor web consiste en la aplicación que sirve el contenido a los usuarios; los más comunes son **Apache**, **IIS** y **WebSphere Host Publisher**. Debemos definir las configuraciones que permitan una menor superficie de contacto, lo que puede ser

logrado deshabilitando los servicios no requeridos y restringiendo los permisos de los servicios que sí son requeridos.

IIS

Comenzando con IIS (el gestor web integrado en Windows), es recomendable deshabilitar los servicios del sistema operativo no requeridos, por ejemplo, deberían deshabilitarse: **Alerter**, **Computer Browser**, **DHCP Client**, etc. El producto Internet Information Server puede instalarse en el directorio por defecto, pero la información para ser publicada (por ejemplo las páginas HTML) deben ubicarse en una partición NTFS distinta a la del sistema operativo. Dentro del IIS, debemos deshabilitar todos los componentes que no sean utilizados, como por ejemplo: **FTP Server**, **SMTP Server**, **Internet Printing**, etcétera.

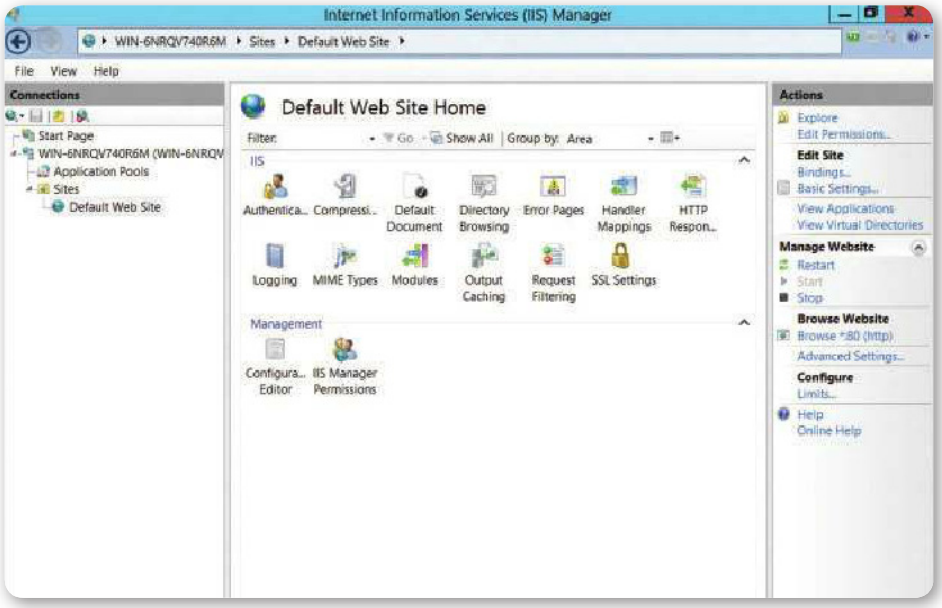


Figura 24. Microsoft Internet Information Services (IIS) Manager. Concentra todas las configuraciones necesarias para administrar las aplicaciones web.

En la configuración de la aplicación, debemos deshabilitar la opción **ParentPaths** ya que podría permitir el acceso no autorizado al directorio inmediato superior. Se debe verificar que no se visualice la dirección IP en el campo **Content-Location** de la información devuelta vía HTTP (puerto 80) del servidor. Para ello debemos:

(1) Realizar telnet al puerto 80 del servidor.

(2) Ejecutar el comando **GET/HTTP/1.0<CR><CR>.**

(3) Verificar que, en el campo denominado **Content-Location**, no se visualice la dirección IP de la computadora.

Para deshabilitarlo, usamos este comando: **cscript.exe c:\inetpub\adminscripts\adsutil.vbs set w3svc/UseHostName True** y reiniciamos el servicio denominado **w3svc**. Sobre los directorios virtuales que contenga la web App, debemos deshabilitar los siguientes permisos: **Script sourceaccess**, **Write** y **Directorybrowsing.**

Los mensajes de error generados por los sitios web suelen ser fuente de mucha información útil para un atacante. Por eso, los mensajes de error en servidores productivos deben indicar solamente un texto genérico sin dar detalles. De esta forma, evitamos revelar información propia del servidor, como rutas de ciertos archivos, o nombres de tablas o bases de datos.

Figura 25. El proyecto Open Source **OWASP Live CD**, basado en Linux, permite realizar verificaciones de seguridad sobre aplicaciones web.

Tomcat

En cuanto a **Apache Tomcat**, al momento de instalarlo se debe utilizar la última versión estable disponible. En servidores productivos,

no se deben instalar los componentes **native**, **documentation**, **examples**, **webapps**, etc. Consideremos que se debe crear un usuario y grupo no privilegiado que iniciará el servicio (por ejemplo: **tomctusr** y **tomctgrp**). Posteriormente modificar el **ownership** de **USUARIO_HOME** al usuario y grupo definido. Modificar los archivos en **USUARIO_HOME/conf** a **readonly**. Verificar que **tomctusr** tenga permisos **rw** en **/tmp** y solo **wx (300)** en **USUARIO_HOME/logs.**

Asignar los permisos mínimos necesarios (**rx**) sobre la aplicación por utilizar. Se debe analizar si la aplicación requiere permisos de escritura sobre el sistema de archivos, lo cual no es aconsejable.

> ES NECESARIO CREAR UN USUARIO Y GRUPO NO PRIVILEGIADO, EL CUAL INICIARÁ EL SERVICIO

Por otra parte, se recomienda intercambiar los archivos de configuración de Tomcat, para simplificar y reducir los componentes innecesariamente habilitados por defecto. Para esto, renombrar (mv): **USUARIO_HOME/conf/server.xml** a **USUARIO_HOME/conf/server-original.xml** y **USUARIO_HOME/conf/server-minimal.xml** a **USUARIO_HOME/conf/server.xml**. Se debe evitar el uso de los puertos inferiores a **1024** ya que, en sistemas Unix, estos requieren ejecutarse con privilegios de **root.**

Por defecto, Tomcat se instala configurado para escuchar en el puerto **8080**. La modificación del puerto de escucha se hace desde el archivo de configuración **USUARIO_HOME/conf/server.xml**. Luego de modificar el puerto de escucha, es necesario reiniciar el servicio.

Debemos considerar que el puerto **8005** nos permite detener el servicio Tomcat y también sus aplicaciones. Recordemos que el script necesario para detener el servicio provisto por Tomcat realiza una conexión a este puerto, enviando un **string** que indica el **shutdown.**

URL SCAN

Es una herramienta gratuita ofrecida por Microsoft, que permite restringir los HTTP request que procesará el servidor. Para esto, escucha los requerimientos y realiza filtros basados en reglas. Estos filtros minimizan las posibilidades de ser víctima de diversos ataques como: denegación de servicio, **SQL Inyections**, **Cross-site scripting**, etc. En la instalación por defecto, se generan reglas que pueden ser modificadas en el archivo: **C:\Windows\system32\inetsrv\urlscan\UrlScan.ini.**

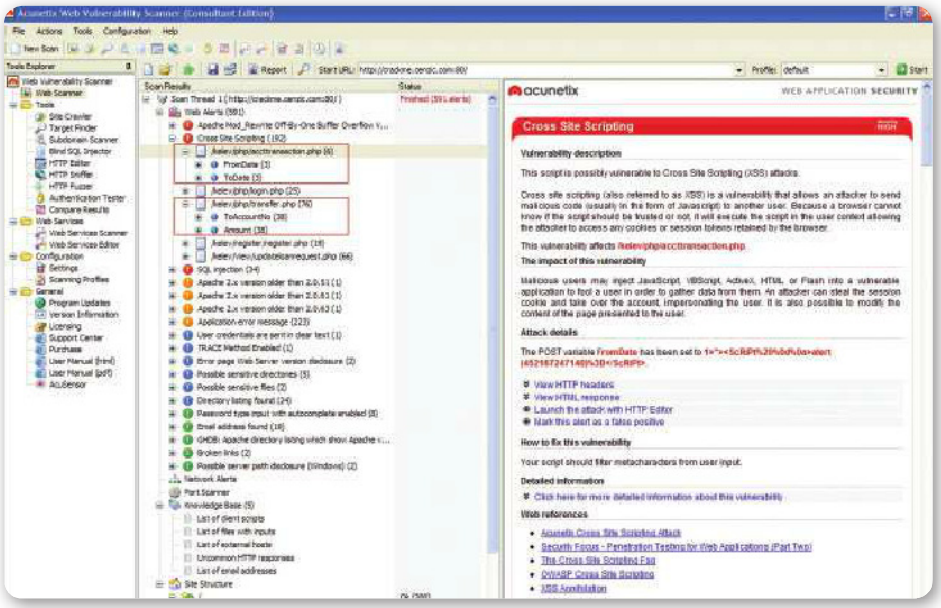


Figura 26. Acunetix Web Vulnerability Scanner permite identificar gran cantidad de vulnerabilidades en forma automática.

Es recomendable modificar este string en el archivo **USUARIO_HOME/conf/server.xml** para evitar apagados no autorizados. Asimismo, es necesario que todos los puertos (salvo los usados por el servicio, ej.: **8080**, **8443**) estén filtrados por un firewall.

> DEBEMOS OCULTAR LAS VERSIONES DE LOS PRODUCTOS EXPUESTOS PÚBLICAMENTE

Por defecto, Tomcat tiene ciertos conectores definidos en el archivo **server.xml**. Algunos están habilitados, y otros deshabilitados. Se recomienda deshabilitar todos los conectores no utilizados por la aplicación. Es preciso tener en cuenta que se requiere por lo menos un conector que esté escuchando algún tipo de tráfico, de lo contrario, Tomcat no podrá servir ninguna petición. Si no deshabilitamos los conectores no usados, estamos permitiendo que Tomcat reciba peticiones en ese puerto. Es altamente recomendable que se use conector HTTPS para toda la información sensible que genere la aplicación.

Para ocultar la versión del servidor, se debe reempaquetar **USUARIO_HOME/server/lib/catalina.jar** con una versión actualizada del archivo **ServerInfo.properties**; desempaquetar catalina.jar y modificar la **default error page** para evitar que muestre el **stacktrace** ante errores y, luego, será necesario volver a empaquetar.

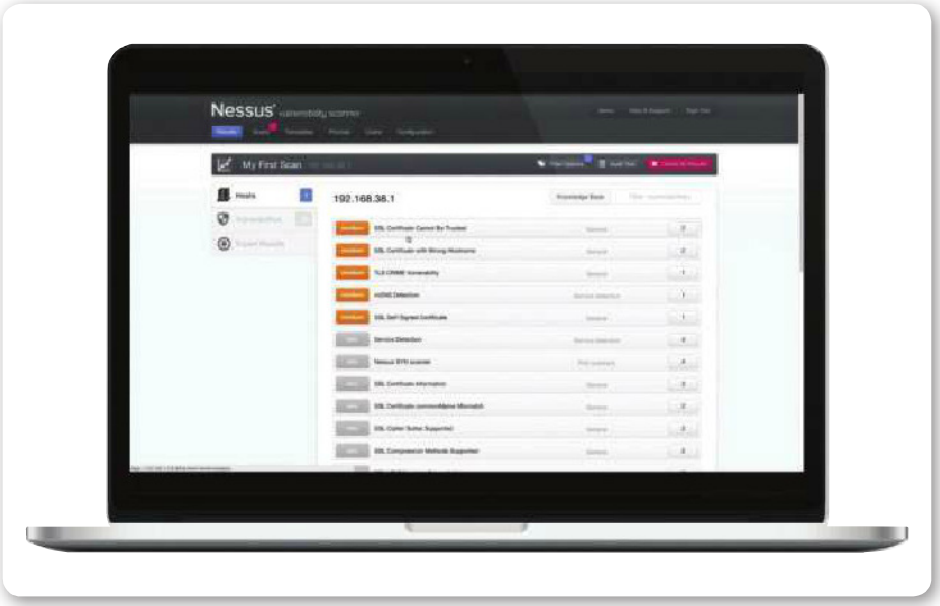


Figura 27. **Nessus**, el escáner de vulnerabilidades desarrollado por **Tenable**, permite identificar vulnerabilidades en numerosos productos web.

Seguridad en servidores FTP

Al planear los elementos de seguridad que integran un servidor FTP, debemos tener en cuenta todos los componentes que hacen a la seguridad del servicio. Es muy importante que consideremos el entorno físico del servidor, la seguridad en el sistema operativo y los componentes de infraestructura que permiten el acceso, como por ejemplo: firewalls, routers y switches. Una vez asegurados estos componentes, debemos verificar la configuración del servicio FTP.

> LOS SERVIDORES FTP IMPLEMENTAN EL RFC 114, CUYO ORIGEN DATA DEL AÑO 1971

Consideremos que los servidores FTP implementan el **RFC 114** de IETF, cuyo origen data del año 1971 con sucesivas modificaciones hasta la actualidad. Originalmente, el protocolo FTP no consideraba mayores cuestiones de seguridad, pero, en sus sucesivas actualizaciones, se agregó soporte para **TLS/SSL** (**FTPS**), autenticación fuerte, integridad y confidencialidad, entre otros elementos de seguridad esenciales.

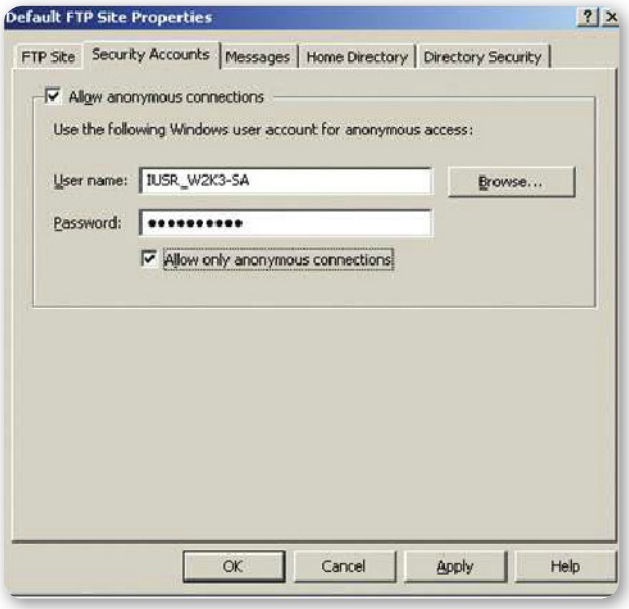


Figura 28. La configuración por defecto del IIS 6.0 permite el acceso anónimo al servidor FTP.

Seguridad del sistema

En cuanto a la seguridad del sistema operativo en general, debemos definir las configuraciones que permitan una menor superficie de contacto, lo que puede ser logrado deshabilitando los servicios no requeridos y restringiendo los permisos de los servicios requeridos.

Uno de los servidores FTP más comúnmente utilizados en Microsoft Windows es el **Internet Information Server (IIS)**, que se encuentra integrado a este. Solo debería habilitarse el servicio de FTP cuando fuera necesario y no pudiera ser reemplazado con algún otro servicio seguro como SSH, SFTP o similar.

Es recomendable habilitar la encriptación SSL/TLS siempre que sea posible, lo que generará que el servicio se comporte como FTPS, garantizando la confidencialidad e integridad de la información.

Carpetas y permisos

La carpeta que se publique en el FTP deberá ser distinta de las que pertenecen al sistema operativo y, en lo posible, diferentes de cualquier sitio web publicado. Nunca se debería compartir un disco entero del sistema operativo; es recomendable utilizar una unidad completamente

separada del SO. Los permisos para lectura/publicación de archivos deben otorgarse a los usuarios mediante utilización de grupos, de esa manera se facilita la administración y es posible definir roles (RBAC). Para el caso del acceso de lectura a recursos FTP públicos, no es necesario autenticar a los usuarios, por lo que es recomendable que el acceso sea con el usuario anónimo **IUSR_Servername** que posee ciertas restricciones.

Cabe mencionar que, independientemente de los permisos que se asignen a nivel del servicio FTP, se deben configurar las ACL necesarias a nivel del sistema de archivos (NTFS) para cada uno de los grupos/usuarios. Para el acceso a recursos FTP públicos, no es obligatorio restringir el acceso a nivel de direcciones IP. Pero sí puede realizarse en intranets para restringir los segmentos de red no autorizados o en caso de detectarse ataques de fuerza bruta.

Restricciones

Es posible configurar las restricciones por equipos (**Single computer**) o grupos de equipos (**Group of computers**). Es necesario que implementemos una política de auditoría a fin de registrar los logins exitosos y fallidos. Es recomendable definir un tamaño máximo de log para no comprometer el espacio en disco.

Si el servidor cuenta con distintas placas de red, es aconsejable definir una por la cual se aceptarán las conexiones FTP. Muchos servidores permiten bloquear las transferencias FXP, potencialmente peligrosas, pero hacerlo puede implicar que los usuarios que utilicen un proxy no podrán descargar contenido.

Debemos considerar que el mecanismo de control que impide las transferencias FXP consiste en controlar que la IP que inicia la transferencia sea la misma que descarga el contenido.

USO DEL NAVEGADOR

Es importante saber que para iniciar sesión en un servidor FTP que requiere una contraseña podemos utilizar un navegador web como cliente. Para realizar esta acción escribimos la URL de esta forma: **ftp://<usuario>:<contraseña>@<servidor ftp>/<url-ruta>**, donde **<usuario>** es el nombre de usuario, **<servidor ftp>** es el servidor FTP, **<contraseña>** es la contraseña de acceso, y **<url-ruta>** el directorio donde iniciamos sesión.

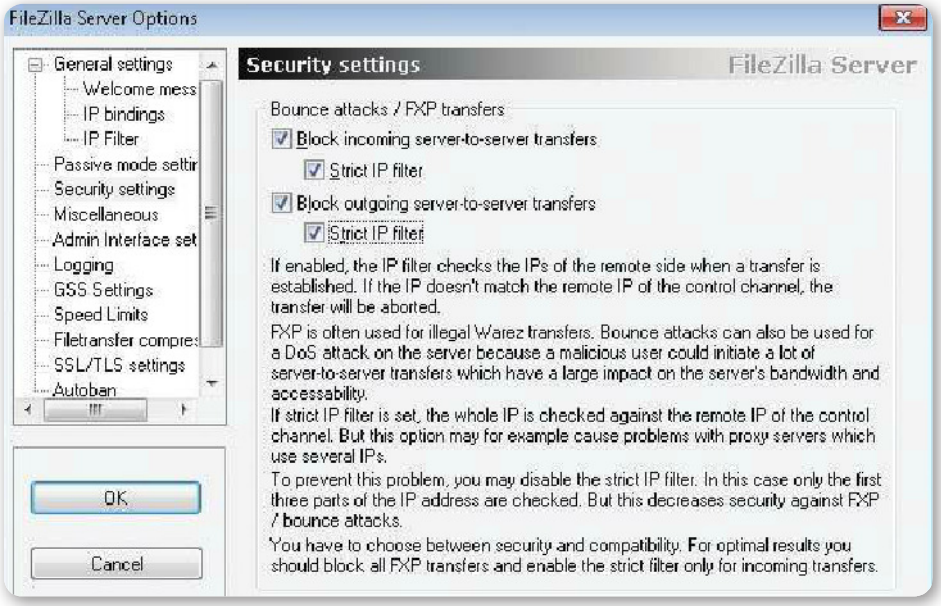


Figura 29. Protección contra **Bounce Attack** presente en **FileZilla** Server. Previene el escaneo de puertos y ataques **DoS**.

Algunos servidores como **FileZilla** y **Gene6**, soportan **MODE Z**, que permite comprimir el tráfico **onthefly** para ahorrar ancho de banda. Esta función podría limitar la capacidad de un proxy o IPS de detectar malware. Una vez descomprimido podrá escanearse en busca de virus.

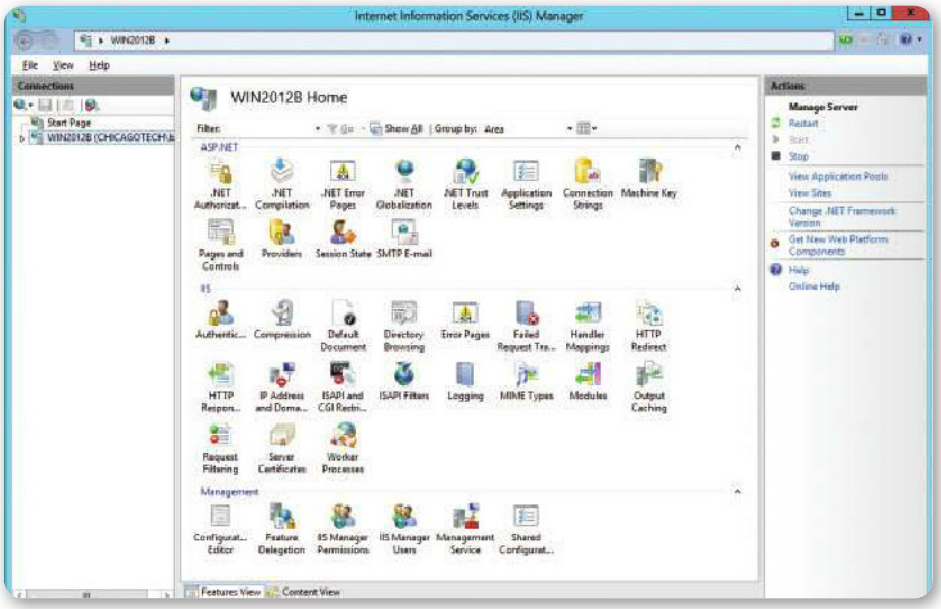


Figura 30. Las configuraciones de **Internet Information Services** presentes en Windows 2012 Server.

Ya sea que esta funcionalidad esté o no habilitada, es recomendable instalar un antivirus completo y mantenerlo actualizado en el servidor FTP para evitar la distribución de contenido malicioso, aun cuando el servidor no sea Windows.

Sea cual fuere el servidor FTP que instalemos, es necesario revisar las configuraciones iniciales. Por ejemplo, IIS permite por defecto el acceso anónimo al servidor.

Si mantenemos acceso anónimo al servidor, es recomendable crear un directorio para solo escritura y un directorio para solo lectura. De esa forma, garantizamos que los archivos presentes en la carpeta de solo lectura no sean alterados con fines maléficos.

Una solución intermedia para poder enviar información confidencial por la red usando un FTP convencional es encriptar la información antes de transferirla. Para esto, pueden utilizarse diversa técnicas / herramientas. Otra opción es forzar el tráfico FTP a través de una VPN, que otorga altos niveles de confidencialidad e integridad.

RESUMEN

En este capítulo nos encargamos de detallar las características de los servidores web y FTP, y pudimos conocer cuáles son sus ventajas. También aprendimos a configurarlos y revisamos las consideraciones que debemos tener en cuenta para administrarlos. Posteriormente, vimos conceptos importantes sobre la seguridad en los servidores web y FTP.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es un servidor web?
2. ¿Cómo funciona un servidor web?
3. ¿Qué es un servidor FTP?
4. ¿Cómo funciona un servidor FTP?
5. ¿Para qué sirve FileZilla?
6. ¿Qué significa endurecer un servidor?
7. ¿Para qué sirve el archivo **httpd.conf**?
8. ¿Qué son las cuotas de disco?
9. Caracterice el modo de conexión activo.
10. ¿Qué es MODE Z?

EJERCICIOS PRÁCTICOS

1. Administre un servidor web.
2. Administre un servidor FTP.
3. Implemente una política de respaldos.
4. Edite el contenido de **httpd.conf**.
5. Establezca restricciones en un servidor FTP.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*05

Servidor de correo electrónico

En este capítulo analizaremos qué es un servidor de correo electrónico y aprenderemos a instalarlo y a configurarlo en sistemas operativos Windows y GNU/Linux.
Para continuar, conoceremos los peligros del SPAM y de qué forma se filtra en el servidor.

Qué es un servidor de correo

En líneas generales, decimos que un servidor de correo electrónico hace las veces de una casilla de **correo postal**, a la que una persona nos puede enviar algo físico, ya sea una carta o una encomienda, y que hasta que no nos acercamos a retirarla seguirá ahí guardada. En caso de que el envío sea más grande que el espacio disponible en la casilla (que es literalmente una especie de casillero, semejante a un **locker** de seguridad), la puerta no cerrará y no se podrán guardar más elementos.

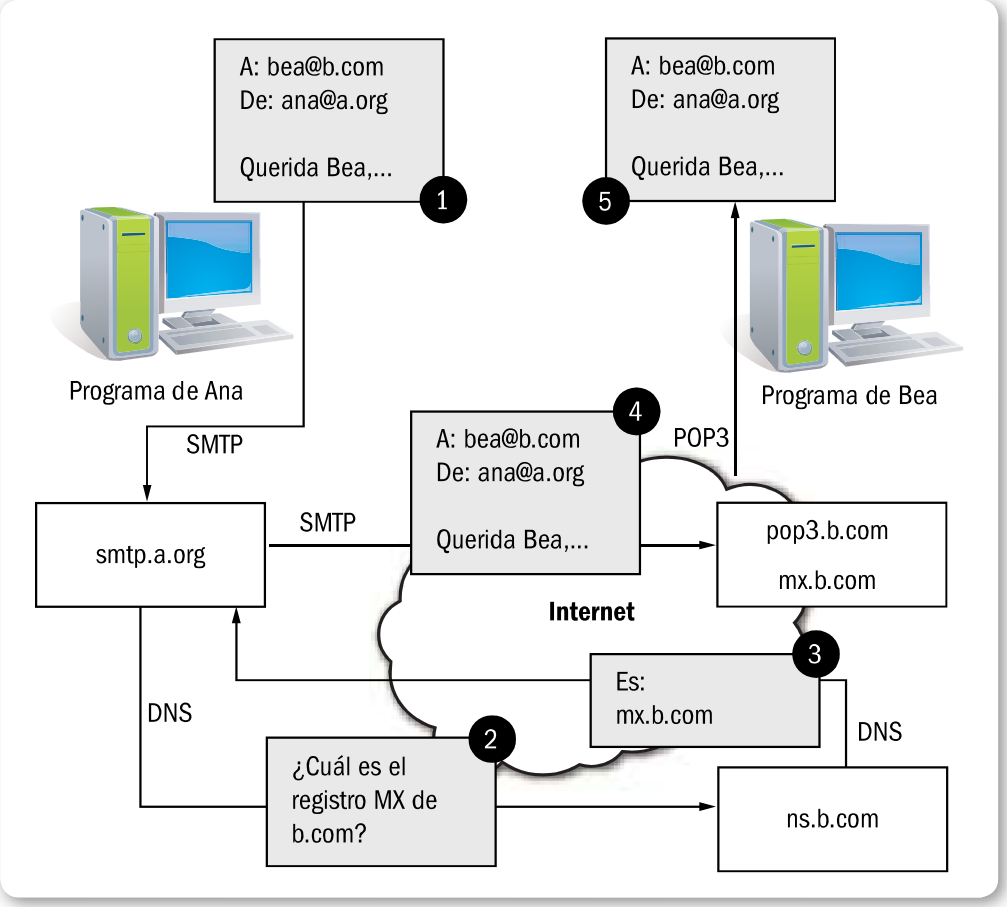


Figura 1. Esquema de funcionamiento del correo electrónico para envío y recepción de mensajes.

En el correo electrónico ocurre algo similar. En este caso, existe un servidor que provee el espacio virtual en términos de una determinada cantidad de **gigabytes**, que será utilizado para recibir mensajes y sus

archivos adjuntos. En caso de que se llene, no podremos continuar recibiendo más envíos de correos.

El servidor de correo electrónico, entonces, presta en principio el **espacio de almacenamiento**, pero esto no es suficiente, ya que resulta necesario, además, establecer un mecanismo por el cual un usuario logre recibir los mensajes y otro para que pueda enviarlos. En términos físicos, ese trabajo lo hará la **empresa de correo**, que se encargará de proveer el espacio físico, las oficinas, los empleados, etc. En términos técnicos, ese trabajo es organizado por las empresas proveedoras del servicio, por medio de **protocolos de comunicación**.

Protocolo

En el caso del correo electrónico, el protocolo que se utiliza para realizar envíos es el llamado **SMTP** (*Simple Mail Transfer Protocol*) o protocolo de transferencia simple de correo, que está definido en el **RFC 2821** y trabaja en el puerto **25/TCP**. Esta comunicación se basa en el **modelo cliente-servidor** para el envío y recepción de mensajes, y supone la existencia de un software cliente que realice la tarea de conexión en forma activa.

Para la recepción del correo, es necesario contar con otro protocolo de comunicaciones, de los cuales el más importante es el llamado **POP** (*Post Office Protocol*) o protocolo de oficina de correo, definido como estándar en el **RFC 1939**, y que suele utilizarse en la versión 3, por lo que también se lo refiere como **POP3**. Otro protocolo muy utilizado para la recepción de mensajes de correo es el llamado **IMAP** (*Internet Message Access Protocol*) o protocolo de acceso a mensajes de Internet, que utiliza principalmente el puerto **143/TCP**.

DNS Y CORREO ELECTRÓNICO

El sistema **DNS** (**Domain Name System**) también suele ser utilizado para enviar y recibir correo electrónico, ya que lo que se provee generalmente no es una dirección IP, sino su nombre, como por ejemplo, smtp.servidor.com o pop3.servidor.com. De esta forma, se resuelve primero el nombre y, luego, se realiza la conexión. El sistema DNS incluye, de hecho, un registro especial para identificar los servidores de correo electrónico, que es el denominado **MX**.

Figura 2. Sendmail es uno de los servidores de correo electrónico más difundido del mundo, originario de plataformas UNIX.

La nube

Si bien los servidores de e-mail son fundamentales en toda infraestructura tecnológica que implique la comunicación entre usuarios, con la masificación de Internet se dio un fenómeno particular que implicó que el e-mail se transformara naturalmente en el primer servicio **en la nube** por medio del uso de los **webmails**, o servidores de correo a los que se puede acceder directamente desde una página web a través de Internet. Estos no requieren el uso de un cliente de software instalado localmente en un sistema. Esta característica promovió el uso del correo electrónico desde **cualquier ubicación**, e independizó al servicio de toda plataforma operativa. Los webmails son, entonces, servidores que incluyen además el propio cliente, de modo que el usuario solo debe acceder con usuario y contraseña, o con algún otro sistema de acceso más seguro, para visualizar la interfaz.

Un aspecto por el que siempre se ha tenido especial cuidado con el correo electrónico es su **seguridad**, ya que tanto el SMTP como el POP y el IMAP son protocolos que funcionan normalmente sobre la base de la comunicación en **texto plano**, es decir, no cifran los datos que transfieren, y pueden ser objeto de ataques, como falsificación de remitente, escucha de protocolo (**sniffing**) y otros. Por tal motivo,

también existen versiones seguras, que, en el caso del POP corresponde al uso del puerto **995/TCP**, en el caso de IMAP es el puerto **993/TCP**, y en el caso de SMTP es el **465/TCP.**

En cuanto a la **intercompatibilidad**, es importante mencionar que las distintas implementaciones de software suelen tener algunas diferencias en el uso de los estándares, por lo que muchas veces se recomienda que el par cliente-servidor se base en sistemas del mismo fabricante, como por ejemplo, el cliente **Microsoft Outlook** y el servidor **Microsoft Exchange Server**, o el cliente **Lotus Notes** (**IBM**) y el servidor **Lotus Domino**. Esto suele darse cuando los fabricantes agregan funcionalidades especiales a sus sistemas, que implican la modificación de los protocolos, en detrimento de la compatibilidad con otros sistemas no propios.

Figura 3. Outlook.com es el servicio de Microsoft que reemplazó a Hotmail, el más popular de los webmails.

Plataformas

Si bien existen servidores de correo para cada una de las distintas plataformas y sistemas operativos modernos, históricamente han sido **GNU/Linux** y los derivados de **Unix** los preferidos de las grandes infraestructuras. Este hecho se basa, quizás, en su alta estabilidad en años en los que no había muchas opciones extras. Las ventajas

ES POSIBLE AGREGAR SEGURIDAD SI HACEMOS USO DE PROTOCOLOS EN VERSIONES SEGURAS

incorporadas por Microsoft a su sistema de correo, por ejemplo, no han tenido especial relación con la eficiencia, sino más bien con las funcionalidades, ya que se encargaron de proveer interfaces de administraciones muy poderosas e intuitivas para los administradores, y mayor comodidad para los usuarios.

En suma, consideremos que como centro de gran parte de las comunicaciones mundiales, los servidores de correo electrónico deben ser considerados en todo su espectro cuando de redes se trata.

Figura 4. Thunderbird es uno de los clientes de correo más utilizados, y se distribuye como software libre.

BREVE HISTORIA DE LAS MLMS

A mediados de los 80, internet aún no existía, pero sí ARPANET, que interconectaba universidades y agencias gubernamentales. BITNET permitía el envío y recepción de mensajes por vía telefónica. BITNIC tenía una central (NIC) que poseía unas listas de distribución. Cada dirección debía agregarse y quitarse en forma manual. Para suscribirse a las listas, era necesario contactar al personal de BITNIC para que estos agregaran manualmente la dirección a la lista de distribución.

Servidor de correo en Windows Server

Un **servidor de correo electrónico** es una aplicación que se aloja en una computadora servidor (con un sistema operativo servidor en la mayoría de los casos), por lo general dentro de Internet (podemos montar un servidor de correos dentro de una red tipo LAN, MAN, etc.). El objetivo de dicha aplicación es simular el correo postal tradicional, pero de manera electrónica sobre una red de transmisión de datos. Se intercambian correos electrónicos en lugar de cartas y paquetes físicos. Los correos electrónicos permiten el envío no solo de mensajes, sino también de archivos adjuntos, como documentos de Word e imágenes.

> ES POSIBLE MONTAR UN SERVIDOR DE CORREO ELECTRÓNICO SOBRE UNA RED LAN

Para instalar **Microsoft Exchange 2010 Server**, debemos ejecutar el archivo **setup.exe**, que se encuentra dentro de la carpeta del instalador. A continuación, el instalador nos muestra una serie de pasos por seguir para poder hacer efectiva la instalación de la aplicación:

- Paso 1: instalar .NET Framework 3.5 SP1.
- Paso 2: instalar Windows PowerShell v2.
- Paso 3: seleccionar la opción de idioma de Exchange.
- Paso 4: instalar Microsoft Exchange.
- Paso 5: obtener actualizaciones críticas para Microsoft Exchange.

Se recomienda no instalar el servidor de correo sobre un controlador de dominio por razones de seguridad.

Es importante mencionar que para iniciar el proceso de instalación, debemos hacer un clic sobre el primer paso que se encuentra activo. En ocasiones, no es necesario ejecutar los pasos 1, 2 o 3 porque los componentes ya se encuentran instalados; en esos casos, el instalador desactiva estos pasos (aparecen en gris y finalizan con el mensaje **Instalado**). Recordemos que solo desde el paso 4 comienza la instalación de Exchange propiamente dicha.

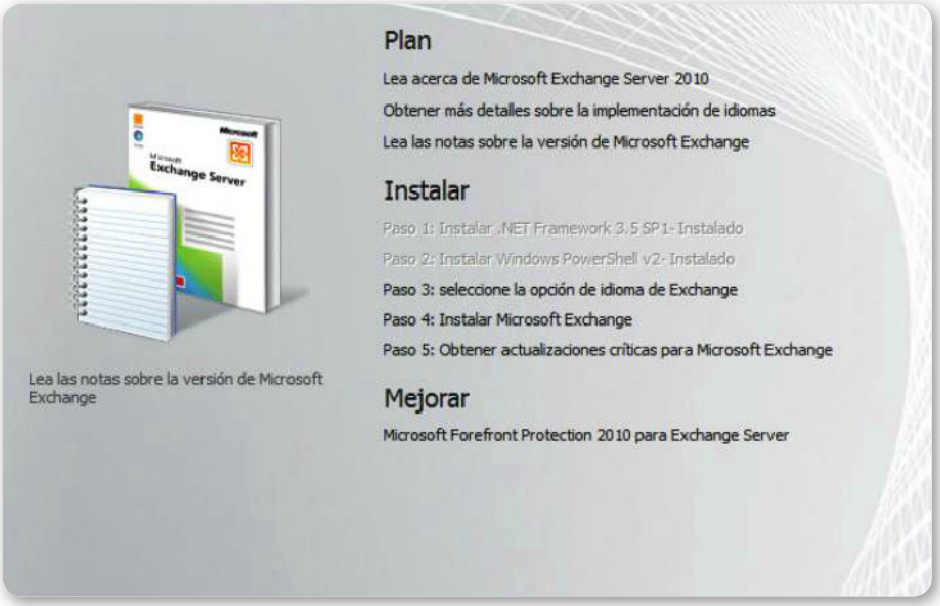


Figura 5. La aplicación de servidor de correos electrónicos Microsoft Exchange es muy utilizada en el ambiente empresarial.

PODEMOS EFECTUAR UNA INSTALACIÓN TÍPICA O TAMBIÉN PERSONALIZAR LAS OPCIONES

A continuación, el instalador nos va a mostrar una introducción; en este punto presionamos el botón **Siguiente**. Luego, nos ofrecerá el contrato de licencia, y lo aceptamos. Siguiendo con la instalación, debemos optar entre realizar una instalación típica o una instalación personalizada, y especificar la ruta de instalación en el sistema.

Las diferencias principales entre ambas opciones de instalación son las siguientes:

- **Instalación típica de Exchange Server**: implica la instalación de los componentes Concentrador de transporte, Acceso de cliente, Buzón y Herramientas de administración de Exchange.
- **Instalación personalizada de Exchange Server**: además de comprender los componentes mencionados en el tipo de instalación anterior, se anexan Mensajería unificada y Transporte perimetral.

Una vez seleccionado el tipo de instalación, debemos introducir el nombre de la organización e indicar si existen equipos con clientes de correo anteriores. Siguiendo con la instalación, el instalador realiza las comprobaciones necesarias. Al finalizar estas, se muestran los

mensajes de error de configuración y de no aptitud de la computadora huésped en caso de que existan. Si no se produce ningún mensaje de error, nos encontramos en condiciones de comenzar la instalación. Para ello, presionamos el botón **Instalar.**

Figura 6. Los correos basura o spam incrementan los costos de mantenimiento de una red. Los productos actuales de servidor de correos ofrecen opciones de filtrado.

Una vez que haya finalizado la instalación, solo debemos presionar el botón **Finalizar**. Por último, se va a iniciar la **Consola de administración Exchange**. En este momento se recomienda reiniciar el servidor, de ser posible, para terminar con la instalación.

Para configurar nuestro servidor de correo, vamos a utilizar la **Consola de administración de Exchange** para realizar

CONSOLA DE ADMINISTRACIÓN

Debemos considerar que la **Consola de administración** de Exchange se presenta como una herramienta basada en Microsoft Management Console 3.0 que ofrece a los administradores de Exchange una interfaz gráfica de usuario (GUI) para administrar la configuración de Exchange. Consideremos que también es posible agregar el complemento para personalizar herramientas que están basadas en MMC.

configuraciones generales y **Active Directory** para efectuar configuraciones puntuales sobre los usuarios (modificar las propiedades de una cuenta de correo por ejemplo).

Figura 7. Para acceder a una cuenta de correo en Exchange, podemos utilizar un cliente de escritorio o acceder vía web a través de un navegador.

Consola de administración de Exchange

Consideremos que para comenzar a configurar Microsoft Exchange, debemos tener en cuenta la estructura que presenta la organización en donde va a funcionar el servidor de correos, en lo que respecta a usuarios o servidores externos con los que debe interactuar, caso contrario Exchange no va a intercambiar información con ellos.

> LA CONSOLA DE ADMINISTRACIÓN PERMITE CONFIGURAR DIVERSOS ASPECTOS

Como mencionamos en apartados anteriores, es completamente necesario asignarle un nombre a la organización durante la instalación de la presente aplicación. En este sentido, recordemos que la consola de administración nos permite configurar los aspectos que mencionamos a continuación.

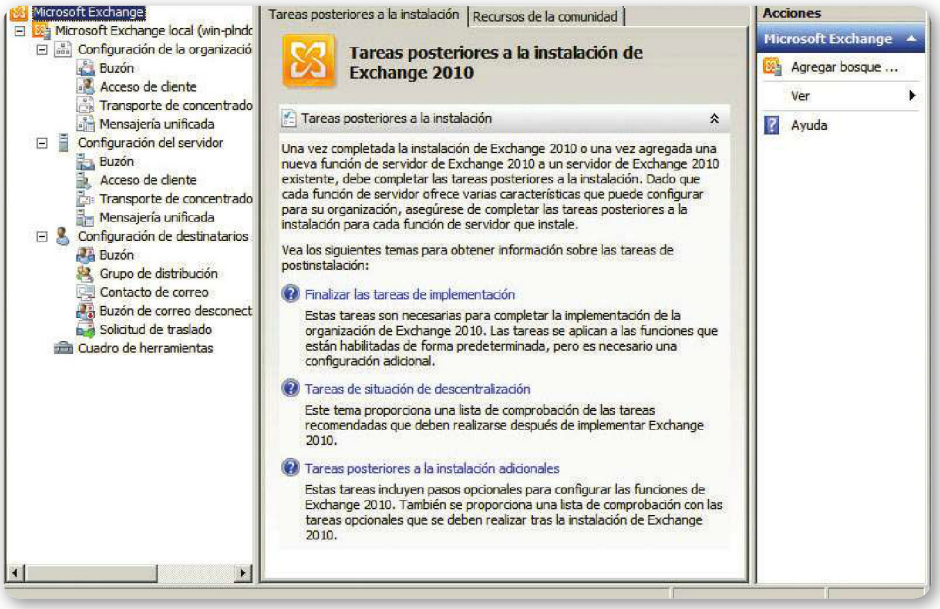


Figura 8. Exchange está fuertemente integrada con Active Directory. La primera permite la configuración de los servicios, y la segunda, de los usuarios.

Configuración de la organización

La Consola de administración nos permite configurar opciones globales de la organización de Exchange, como por ejemplo, funciones de acceso administrativo para usuarios y grupos. Esta configuración está compuesta por las siguientes secciones:

- **Buzón**: engloba la configuración de las funciones de servidor de buzón, como listas de direcciones, carpetas personalizadas administradas, directivas de buzón de administración de registros de mensajería (MRM) y libretas de direcciones sin conexión.
- **Acceso de cliente**: nos 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 por Active Directory dentro de la organización. Permite administrar todo el flujo de correo interno, aplica las directivas de enrutamiento de mensajes de la organización y es la responsable de la entrega de mensajes a un buzón de un destinatario particular. En esta sección, se define cómo y cuándo se envían los mensajes.

- **Mensajería unificada**: alcanza a toda la organización; permite la administración de los planes de marcado, IP de puertas de enlace y operadores automáticos de mensajería unificada.

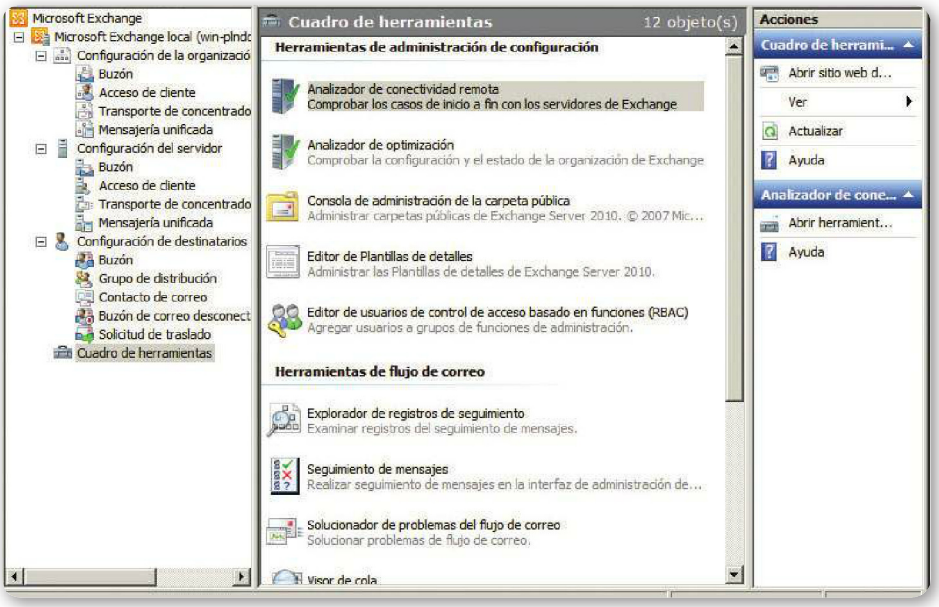


Figura 9. Por lo general, un servicio de correo electrónico utiliza el protocolo SMTP para los correos entrantes y POP3 para los correos salientes.

Configuración de servidores

Nos permite configurar los servidores Exchange y los componentes de los que disponen (bases de datos, protocolos y administración de registro de mensajería, por ejemplo). Dentro de esta opción de menú podemos definir los servicios activos (POP3, SMTP, etc.) y los grupos de almacenamiento de los servidores. Un grupo de almacenamiento es un contenedor para buzones y carpetas públicas.

Por ejemplo, para modificar los parámetros de un servidor, debemos seleccionar el servidor, seleccionar las propiedades y establecer los parámetros de configuración que consideremos apropiados. Para un servidor de correo saliente (SMTP) podemos configurar parámetros como la forma de autenticación, el límite de los mensajes, etc.

- **Buzón**: administra las bases de datos de los buzones de los servidores con esta función instalada.
- **Acceso de cliente**: gestiona las libretas de direcciones sin

conexión, la función Microsoft Outlook Web Access y también el acceso desde dispositivos móviles con Active Sync.

- **Transporte de concentradores**: permite listar todos los servidores con esta función y configurar los conectores de recepción SMTP de Exchange que no son la puerta de enlace por la cual reciben los mensajes.
- **Mensajería unificada**: nos permite configurar aspectos relacionados con mensajes de voz, de fax, correos electrónicos, etc., a los que tienen acceso los usuarios.

> PODEMOS LISTAR LOS SERVIDORES CON LA FUNCIÓN DE TRANSPORTE DE CONCENTRADORES

Configuración de destinatarios

En esta sección, debemos definir y gestionar los destinatarios de correos electrónicos dentro de la organización. Un destinario es un objeto o entidad que puede recibir un correo electrónico desde Exchange. Incluye usuarios, contactos, grupos y otros elementos. Desde aquí podemos administrar grupos de distribución de Exchange, por ejemplo. Esta opción de menú posee las siguientes secciones:

- **Buzón**: permite administrar los usuarios de los buzones y los buzones de los recursos (salas y equipos). Dentro de esta sección podemos habilitar la mensajería unificada y los dispositivos móviles.
- **Grupo de distribución**: gestiona los grupos de distribución.
- **Contacto de correo**: se trata de la opción que nos permite gestionar todo lo relacionado con contactos de correo.
- **Buzón desconectado**: desde este punto podemos ver y habilitar buzones que se encuentren deshabilitados.

ÁRBOL DE LA CONSOLA

Entre los elementos que encontramos en la **Consola de administración** de Exchange se encuentra el árbol de la consola. Esta sección está ubicada en el lado izquierdo de la consola de administración y presenta la organización de los nodos que se basan en los roles del servidor que ha instalado. Consideremos que estos nodos están basados en funciones del servidor.

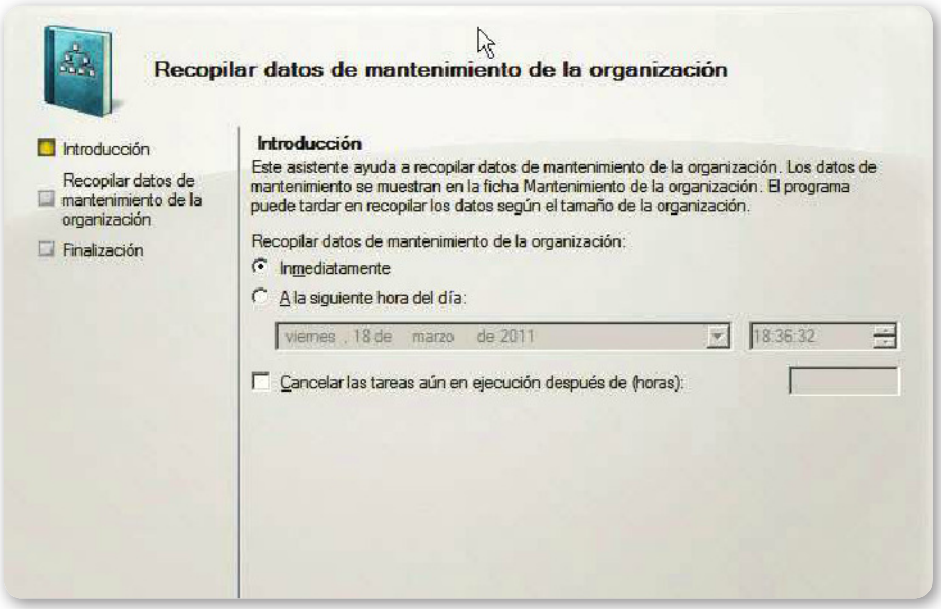


Figura 10. Las listas Robinson o ficheros de exclusión son registros de personas que no desean recibir publicidades de terceros por ningún medio, incluidos los e-mails.

Cuadro de herramientas

Además, Exchange cuenta con un conjunto extra de herramientas para optimizar su funcionamiento.

Para comenzar a utilizar Exchange, es necesario recopilar información acerca de la organización huésped. Primero, debemos seleccionar la opción de menú **Microsoft Exchange Local**, presionamos el botón derecho del mouse y, luego, seleccionamos la opción **Recopilar datos de mantenimiento**, de la organización del menú que se despliega. A continuación, presionamos el botón **Siguiente** y, por último, el botón **Recopilar**. De ahora en adelante, en el menú de administración de Exchange se debería reconocer el servidor junto a las bases de datos.

Active Directory

Cuando instalamos Exchange, este se integra totalmente con Active Directory. Luego de la instalación, cuando creamos un usuario nuevo, su cuenta de correo electrónico se crea en forma automática.

Desde **Configuración de destinatarios**, si seleccionamos la opción **Propiedades** podemos acceder a los siguientes ítems de configuración:

- **Direcciones de correo electrónico**: nos permite consultar las direcciones electrónicas del usuario, agregar nuevas direcciones o modificar las existentes.
- **Configuración del buzón**: realiza la administración de los registros de mensajería y las cuotas de almacenamiento de un usuario (advertencias, período de tiempo que se almacenan los mensajes eliminados, etc.).
- **Características del buzón**: podremos habilitar o deshabilitar servicios y características del buzón de un usuario, como por ejemplo, protocolos que utiliza, Outlook Web Access, Exchange ActiveSync, POP3, etc.; y consultar sus propiedades.
- **Configuración de flujo de correo**: nos permite configurar opciones relacionadas con la entrega de mensajes (permisos delegados y dirección de reenvíos), restricciones de tamaño de mensajes y restricciones de entrega (por ejemplo, destinatarios prohibidos).
- **General**: permite asociar nombres simples a cuentas de correo, ocultar usuarios de listas de distribución, y consultar y editar permisos de acceso de buzón, entre otras cosas.

> UN SERVIDOR DE CORREO SIMULA EL CORREO POSTAL TRADICIONAL EN FORMA ELECTRÓNICA

Webmail

Otra opción muy útil de configuración consiste en configurar Exchange para que los usuarios puedan acceder a sus cuentas de correo a través de la Web, utilizando un navegador. Primero, debemos corroborar si el servicio se encuentra activo (si no, debemos activarlo). Dentro de la Consola de administración de Exchange ingresamos a la **Configuración de servidor**, seleccionamos la opción de menú **Acceso de cliente** y luego el servidor que utiliza (se encuentra listado). Solo nos resta consultar la pestaña **Outlook Web Access.**

Si el servicio se encuentra activo, debería existir el directorio virtual OWA (Outlook Web Access). Podemos comprobar lo antes mencionado utilizando el **Administrador de Internet InformationServices (IIS).** Para hacer uso de la funcionalidad de webmail, abrimos el explorador web y escribimos la dirección del servidor web. Para finalizar, solo resta que ingresemos un nombre de usuario y una contraseña.

Figura 11. Es recomendable que un servidor de correos trabaje en conjunto con un antivirus para que las amenazas sean eliminadas antes de llegar al buzón.

Filtrado inteligente

Para evitar que ingresen mensajes no deseados, por lo general spam, podemos utilizar la herramienta **Content Filter Agent**. Esta nos ayudará a determinar la probabilidad de que los correos entrantes sean o no deseados. Utilizando esta probabilidad, podemos elegir bloquear los correos en la puerta de enlace, en el almacén de correos o en el buzón. Si no se encuentra instalada, debemos posicionarnos en la opción de menú **Inicio/Programas/Exchange** y ejecutar la aplicación Exchange Management Shell. Luego, dentro de la aplicación antes mencionada,

ZIMBRA

Zimbra es la solución de servidor de correo y cliente que provee VMware. Existen varias versiones disponibles de Zimbra, algunas de código abierto soportadas por comunidades de desarrolladores independientes, y otras que poseen partes de código cerrado. La aplicación servidor hace uso de proyectos de código abierto existentes como **Postfix**, **MySQL**, **OpenLDAP** y **Lucene**. Cuenta con una interfaz de programación de aplicaciones basada en SOAP y puede actuar como servidor IMAP y POP3.

nos posicionamos en la ruta **C:\Archivos de programa\Microsoft\Exchange Server\V14\Scripts** y ejecutamos la sentencia **install-AntispamAgents.ps1** para instalar una serie de componentes que nos permiten lidiar con el spam. Entre estos componentes, se encuentra Content Filter Agent.

Luego de la instalación del componente, reiniciamos el servicio de transporte de **Microsoft Exchange**. Content Filter Agent se encuentra disponible para configurar en la Consola de administración de Exchange en las secciones **Configuración de la organización** y **Transporte de concentradores.** Para acceder a dicho componente, seleccionamos la herramienta **Filtro de correo no deseado** dentro de alguna de las secciones antes mencionadas. Podemos filtrar correos según 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 listas de direcciones IP bloqueadas
- Proveedores de listas de direcciones IP permitidas
- Reputación del remitente

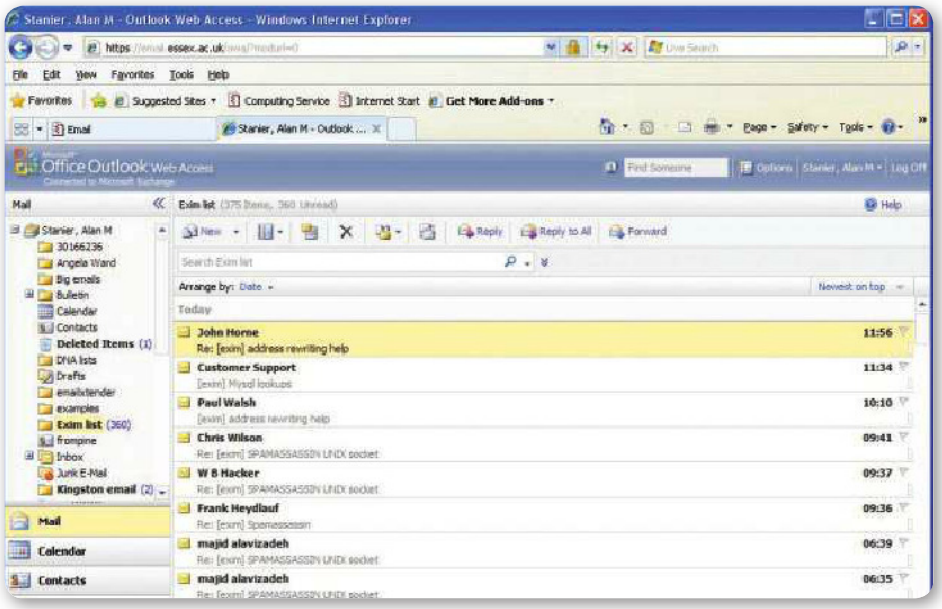


Figura 12. Mantener un buzón libre de spam requiere también que, como usuarios, reportemos los remitentes que nos invaden con publicidades.

Servidor de correo en Linux

Existen numerosas soluciones que integran las distintas funcionalidades requeridas en un servidor de correo moderno. Algunas de estas funcionalidades son: transferencia de e-mails (**MTA**, **Message Transfer Agent**), recupero de e-mails (**MRA**, **Mail Retrieval Agent**), procesamiento de e-mails y listas (**MLM**, **Mail List Manager**), antispam, antivirus, webmail y, por último, interfaz de administración.

Todos estos componentes, cuando son comercializados, suelen integrarse como un único producto y ser mostrados a través de una única interfaz. En el mundo Linux debemos ser nosotros quienes instalemos e integremos todos estos servicios.

En estas páginas nos centraremos en las tecnologías disponibles en ambientes Linux; veremos las características de cada producto, su instalación y su configuración.

MTA

Los **MTA** más comúnmente utilizados en Linux son **Postfix**, **Qmail** y **Sendmail**. Sendmail (**sendmail.com/sm/open_source**) es un ruteador de e-mails que soporta numerosos protocolos para envío de e-mails, como por ejemplo SMTP. Fue desarrollado por Eric Allman en los años 80. Actualmente, Sendmail cuenta con una versión open source mantenida por la comunidad y una versión propietaria mantenida por Sendmail Inc. Para instalarlo, descargamos el código fuente en un directorio y ejecutamos:

```
/buildinstall
```

Esto deberá crear los binarios en **/usr/sbin** y crear links desde **/usr/bin/newaliases y/usr/bin/mailq** a **/usr/sbin/sendmail.**

Luego de la instalación, es necesario configurar **/etc/mail/sendmail.cf** y el resto de los archivos requeridos. La configuración de Sendmail es compleja, por lo que será necesario utilizar la guía de instalación.

Postfix (**postfix.org**) fue desarrollado originalmente en 1997 por Wietse Venema en los laboratorios de IBM como un reemplazo de Sendmail. Se distribuye bajo licencia IBM Public License. Postfix posee una limitada cantidad de funciones, por lo que deben utilizarse otros productos que completan la funcionalidad del servicio. Posee soporte

para los estándares SMTP, LMTP, encriptación STARTTLS, autenticación SASL, encapsulamiento MIME, notificaciones DSN, IPv4 e IPv6.

Para la instalación, utiliza GCC como compilador por defecto. Desde el directorio fuente, simplemente ejecutamos **make**. Si este es exitoso, debemos proceder con el resto de la instalación. Si el SO cuenta con una versión de Sendmail instalada, debemos realizar algunas modificaciones para que Postfix sea el servidor por defecto.
Creamos el usuario en **/etc/passwd**

postfix:*:12345:12345:postfix:/no/where:/no/shell

Y los grupos en **/etc/group**

postfix:*:12345:

postdrop:*:54321:

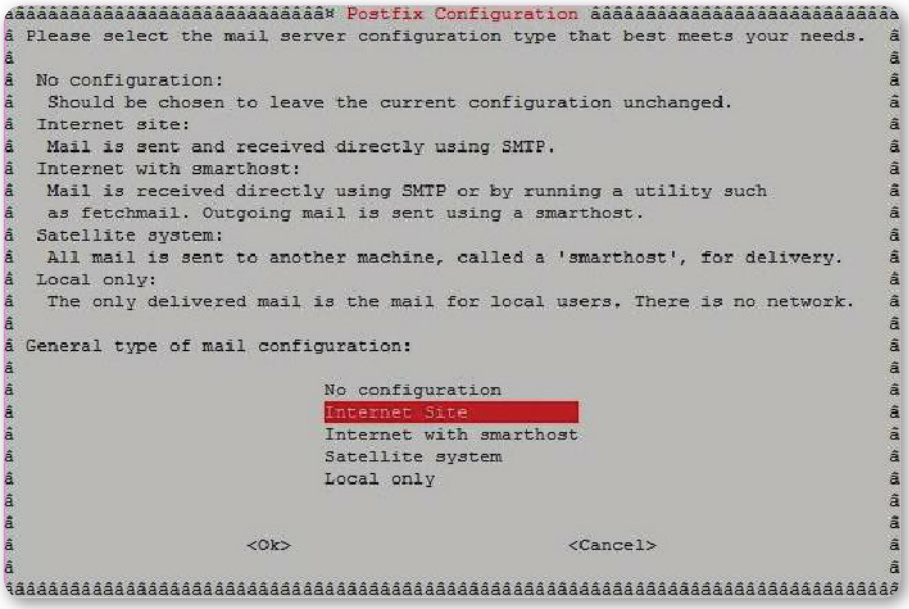


Figura 13. La interfaz de configuración interactiva de **Postfix**. Permite configurar el servicio rápida y fácilmente.

A continuación, ejecutamos **makeinstall** desde root, que, en forma interactiva, nos guiará por la instalación.

Por defecto, los archivos de configuración de Postfix se encuentran en **/etc/postfix**. Los archivos más importantes son **main.cf** y **master.cf**; root debe ser dueño de estos archivos.

Qmail (**qmail.org**), escrito por Dan Bernstein, es tal vez el segundo MTA más utilizado en Internet. Es considerado un servicio pequeño, rápido y seguro.

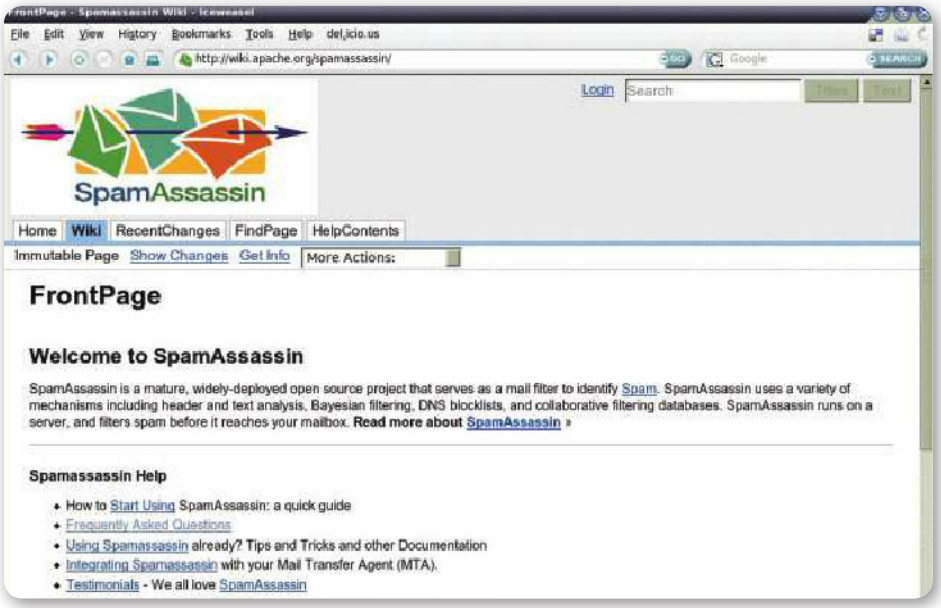


Figura 14. SpamAssassin es un proyecto open source maduro que realiza con eficacia el filtrado del correo basura.

Para su instalación, debemos ejecutar los siguientes comandos, reemplazando **x.yy** por la versión utilizada:

```
mkdir -p /usr/local/src
mv netqmail-x.yy.tar.gz ucspi-tcp-x.yy.tar.gz /usr/local/src
mkdir -p /package
mv daemontools-x.yy.tar.gz /package
chmod 1755 /package
```

Luego, desempacar y compilar (es necesario un compilador C) ejecutando **makesetupchecky ./config**

Para información detallada de instalación, podemos recurrir a **lifewithqmail.org**.

Tengamos en cuenta que los agentes más populares para búsqueda de e-mails en un servidor remoto son fetchmail, getmail y fdm. Originalmente, **fetchmail** (**fetchmail.berlios.de**) fue desarrollado por Eric Raymond en 1996, tomando como base a popclient. Soporta todos los protocolos disponibles: POP2, POP3, RPOP, APOP, KPOP, IMAP, ETRN y ODMR. Incluso soporta IPv6 e IPSEC. En cuanto a la autenticación de los clientes, soporta APOP, KPOP, OTP, CompuServe RPA y Microsoft NTLM, entre otros. Consideremos que se puede configurar para soportar encriptación end-to-end vía túneles SSH.

Figura 15. Interfaz gráfica de **Fetchmail** para configuración y pruebas. Facilita la administración del servicio.

Para instalar fetchmail desde una terminal ejecutamos desde el usuario root:

apt-getinstallfetchmail (Debian y Ubuntu)

yuminstallfetchmail (CentOS y Fedora)

pacman -S fetchmail (Arch Linux)

emergefetchmail (Gentoo)

Una vez instalado es posible configurarlo utilizando el entorno gráfico con el comando **fetchmailconf.**

Esta herramienta fue desarrollada por Charles Cazabon en 1998, **getmail** (**pyropus.ca/software/getmail**) se presenta como un reemplazo de fetchmail por ser flexible, seguro y confiabilidad, y por su facilidad de uso e instalación. Soporta POP3, POP3-sobre-SSL, IMAP4, IMAP4-sobre-SSL, SDPS (extensión de POP3).

Para instalarlo, debemos instalar Python, luego descargar el tarball, desempacarlo en el directorio deseado y ejecutar el comando:

python setup.py install

La ruta por defecto de instalación es **/usr/local/ o /usr/.**

No es necesario realizar ninguna configuración sobre MTA, ya que getmail escribe sobre los archivos maildir, mboxrd o MDA.

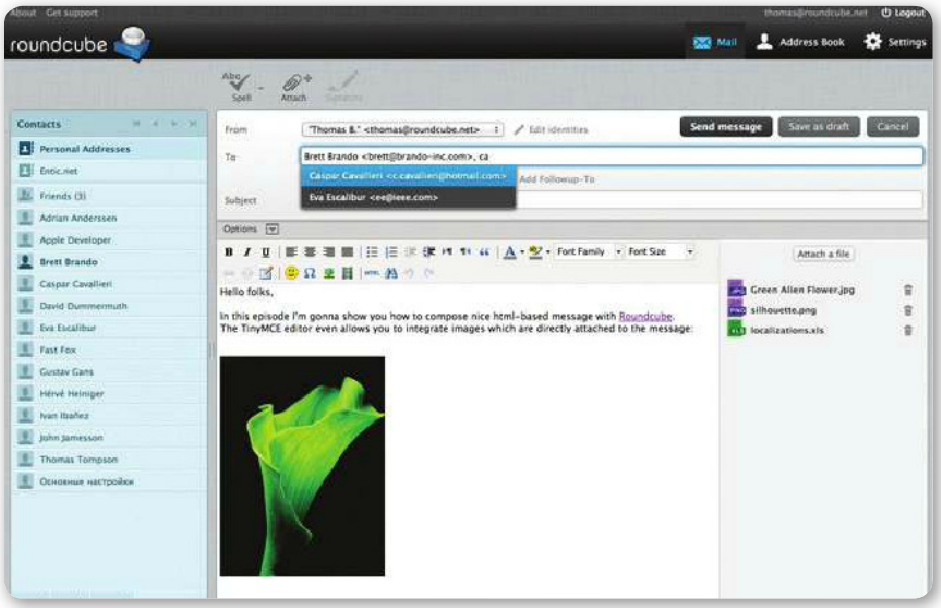


Figura 16. Roundcube presenta una interfaz muy atractiva y amigable. Los controles Ajax facilitan su uso.

Fdm (**fdm.sourceforge.net**) entrega e-mails de diversas formas dependiendo de las reglas definidas por el usuario. El e-mail puede ser recuperado desde el standard input (stdin), IMAP, POP3 o desde maildirs. Puede ser filtrado basado en expresiones regulares, tamaño, fecha, o la salida de un comando de consola.

SE UTILIZA SEGREGACIÓN DE PERMISOS PARA MINIMIZAR LA CANTIDAD DE CÓDIGO

Cada correo puede ser reescrito por un proceso externo, dropeado, dejado en el servidor o entregado a buzones con formato maildir, mbox, a un archivo o tubería (pipe), o a cualquier combinación de estos. Está diseñado para ser liviano y con una configuración compacta. Originalmente, se pensó para usuarios individuales, pero puede ser configurado para un entorno multiusuario. En estos casos, usa segregación de permisos para minimizar la cantidad de código ejecutándose como root.

Para su instalación, descargamos el tarball, lo descompactamos y ejecutamos **make**. Luego, ejecutamos **makeinstall** para que sea instalado en la ubicación por defecto (**/usr/local**). Para no utilizar root, es recomendable crear un usuario:

```
useradd -u 999 -s /bin/nologin -d /var/empty -g=uid _fdm
```

Debemos examinar el archivo de configuración que encontramos en **/etc/fdm.conf** y editarlo según nuestras necesidades.

Figura 17. Funcionalidades del webmail **Atmail**. Integra funcionalidades de antivirus, antispam y dispositivos móviles.

MLM

Debemos considerar que los **list managers** se encargan de recibir un correo y distribuirlo a un número determinado de receptores. Este tipo de servicios permite que las personas se suscriban y desuscriban a distintas listas de interés. Los más populares son Ecartis, Mailman, Majordomo, Procmail SmartList.

Majordomo (**greatcircle.com/majordomo**) es tal vez el más popular de todos. Está desarrollado en lenguaje de scripting Perl, lo que lo hace algo ineficiente. Pero Perl es muy poderoso sobre todo para procesamiento de texto. El hecho de que esté desarrollado utilizando scripting permite que el código sea extendido en cada implementación. Para su instalación, debemos desempacar el tarball, crear el usuario y grupo (reemplazar **x.yy** por la versión descargada):

```
majordomo:x:16:16:Majordomo LM:/usr/local/majordomo-x.yy:
majordomo:*:10883:0:88888:7:::
```

Luego, ejecutamos **makewrapper**, **makeinstall** y **makeinstall-wrapper.**

Ecartis (**ecartis.org**) fue desarrollado por Rachel Blackman en 1997, pero antes se conocía como Listar. Posee algunas funcionalidades no encontradas en majordomo. Una de sus características sobresalientes es que se carga en el sistema como un módulo. Posee una interfaz web para administración de las listas y los miembros.

EL SERVICIO MTA ES EL ENCARGADO DE RECIBIR CORREO Y ALMACENARLO EN EL BUZÓN CORRECTO

Para instalarlo, debemos compilarlo utilizando GCC o EGCC; para esto descompactamos el tarball. En el directorio elegido, ingresamos al directorio src y copiamos **Makefile.dist** a **Makefile**. Editamos su contenido para customizar lo necesario y lo salvamos. Luego, ejecutamos el comando **make**, en BSD tal vez sea necesario realizar **gmake**. Una vez instalado, debemos integrarlo con el MTA. Para Sendmail, la forma más sencilla es copiar la salida del script newlist.pl de Eclair en el subdirectorio **/etc/aliases** de Sendmail y, luego, ejecutar el programa newaliases de Sendmail. Para Postfix, también es posible copiar la salida de alias de Eclair en el archivo **default aliases** y luego ejecutar el comando **postaliases.**

En qmail, el método para agregar alias es completamente diferente a los otros dos. Debemos crear un archivo **.qmail-miLista** en el home directory del usuario qmail. Para esto, una vez posicionados en el homedir de qmail, ejecutamos el comando

```
echo "|/home/ecartis/ecartis -s miLista" > .qmail- miLista
```

No es necesario ejecutar un comando para recrear los aliases de qmail.

Mailman (**gnu.org/software/mailman**), desarrollado

MAILMAN

GNU Mailman se presenta como una eficiente aplicación del proyecto GNU; este programa es capaz de manejar complejas listas de correo electrónico. Este interesante programa se compone principalmente de código desarrollado con el lenguaje de programación Python y en la actualidad es mantenido por Barry Warsaw. GNU Mailman se ofrece como software libre y, por lo tanto, se distribuye acompañado por la licencia GNU General Public License.

principalmente en Python por Barry Warsaw, soporta almacenamiento, procesamiento automático, entrega, filtrado de contenido, spam, y más. Para su instalación, se requiere un compilador C (GCC) y el intérprete de Python. Debemos crear el usuario y grupo con los siguientes comandos:

```
groupaddmailman
useradd -c"GNUMailman" -s /no/shell -d /no/home -g mailmanmailman
```

El directorio de instalación por defecto es **/usr/local/mailman**. Una vez descompactado el paquete, ejecutamos:

```
cdmailman-x.yy
./configure
makeinstall
```

Para más detalles consultamos la guía de instalación.

Procmail y **SmartList** (**procmail.org**) integran una misma suite para administración de listas. Procmail puede ser utilizado para crear servidores de mail, listas, organizar el correo entrante en carpetas/archivos, preprocesar el correo, iniciar programas al recibir nuevos e-mails (por ejemplo para hacer un sonido) o reenviar algunos correos a alguien más en forma automática.

SmartList se ejecuta sobre Procmail, y permite la creación y administración de listas, incluyendo la gestión automatizada de las suscripciones, desuscripciones, solicitud de ayuda, autoremoción de direcciones que generan mucho tráfico (spamers), un servidor de archivado (con soporte MIME), y más funcionalidades. Para su instalación, descompactamos y ejecutamos los comandos **make** y **makeinstall.**

Otro componente fundamental de nuestro servidor es el webmail. Algunos de los más reconocidos son: Roundcube, Zimbra Collaboration Suite, phpGroupWare, Squirrelmail y Atmail.

Administración

Para facilitar la tarea del administrador existen diversas interfaces para administrar el servicio de correo. Algunas de las más reconocidas son Korreio, RavenCore Hosting Control Panel, Webmin y Tequila.

Korreio (**korreio.sf.net**) posee una interfaz gráfica para administración de sistemas de e-mail. Posee varios módulos independientes para administrar Postfix, LDAP, Cyrus-IMAP y Cyrus-Sieve.

RavenCore Hosting Control Panel (**sourceforge.net/projects/ravencore**) posee interfaz web y utiliza dovecot para descargar correo POP3/IMAP; permite configurar sistemas multiusuario y multidominio con autenticación SASL. También, puede integrarse con SpamAssassin y ClamAV para escaneo de spam y virus.

Webmin (que encontramos en la dirección **webmin.com**) posee una interfaz web para administración de servidores Linux. Permite administrar bases de datos, usuarios, DNS, compartir archivos, y mucho más. Posee un módulo de configuración para Postfix.

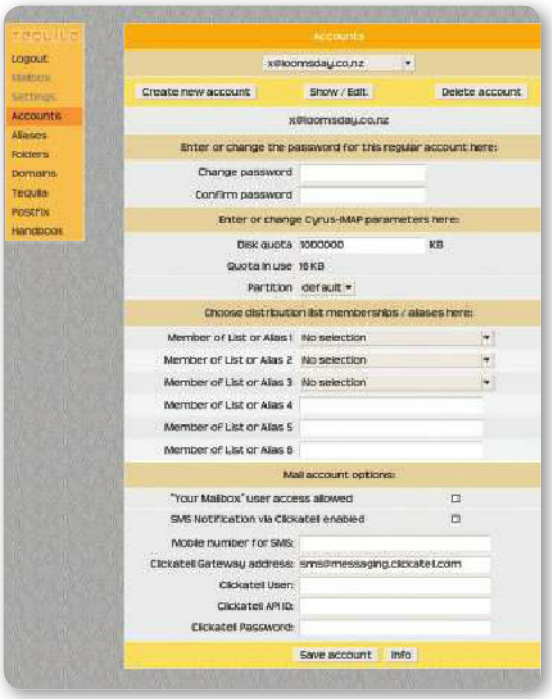


Figura 18. Tequila: interfaz web para administración de servidores Postfix.

INSTALACIÓN BÁSICA DE SENDMAIL

Hay dos pasos básicos para instalar **Sendmail**. Primero compilar y, luego, instalar los binarios. Si Sendmail se encuentra portado al SO que usamos es más simple. Segundo, debemos construir un archivo de configuración. Este es un archivo que se lee al inicio del servicio y contiene los dominios, cómo parsear las direcciones, cómo reescribir las cabeceras, y más opciones. El archivo es realmente complejo, pero puede construirse utilizando el lenguaje basado en M4.

Tequila (**loomsday.co.nz/development?id=tequila**) es una interfaz web que permite administrar sistemas Postfix incluyendo reenvío de e-mails y autorespuesta.

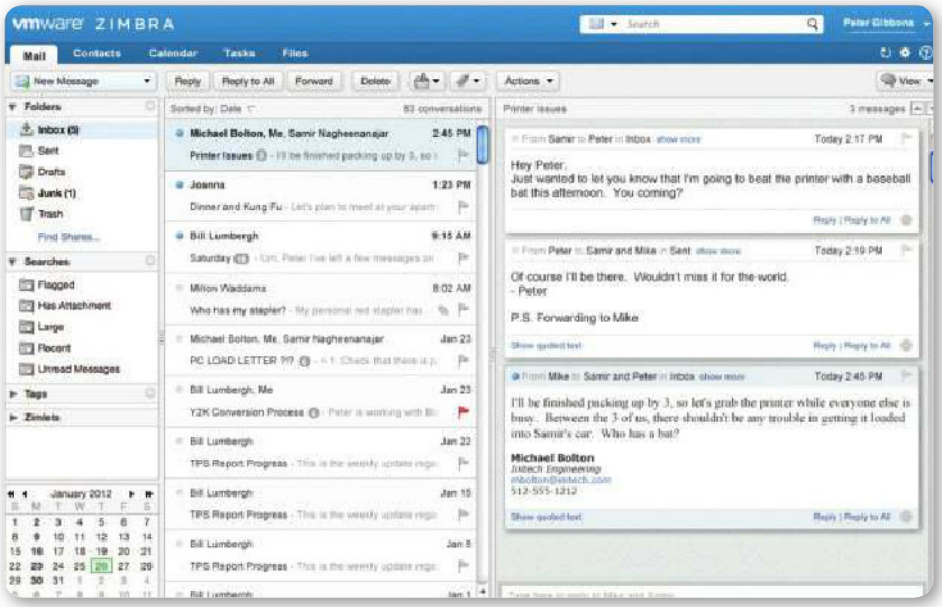


Figura 19. La completa interfaz de **Zimbra** permite administrar el correo, los contactos, calendarios y más.

SPAM

Pocas palabras hemos visto tantas veces en nuestro buzón de correo electrónico como **spam**. Ya sea en los encabezados del e-mail, en la carpeta donde se almacenan y se filtran, en las opciones del cliente de correo, el spam, o correo basura, nos acompaña hace más de una década, habiendo pasado por varias etapas.

Figura 20. Spamhaus es un proyecto que recopila y ofrece información sobre el estado del spam en el mundo.

EL SPAM CORRESPONDE A MENSAJES DE E-MAIL MASIVOS Y NO SOLICITADOS

Podemos definir spam específicamente como mensajes de correo electrónico que se han enviado de manera **masiva** y se han recibido además **sin haber sido solicitados**. Estas dos cualidades simultáneas son las que permiten determinar si un mensaje se trata de spam o no. De hecho, en caso de que la definición permita la duda, se puede contrastar un correo con el hecho de que la identidad personal del receptor y el contexto sean irrelevantes, lo cual determinará definitivamente que se trata de correo basura. Estos mensajes se envían en general a modo de **publicidad** de productos y servicios que, muchas veces, son **ilegales**.

SPAM Y DEC

Existen diversas versiones sobre el origen del Spam, una de ellas cuenta que data del 3 de mayo de 1978, cuando un total de 393 empleados de ARPANET recibieron un correo de la compañía de computadoras DEC, el cual les invitaba al lanzamiento de un nuevo producto.

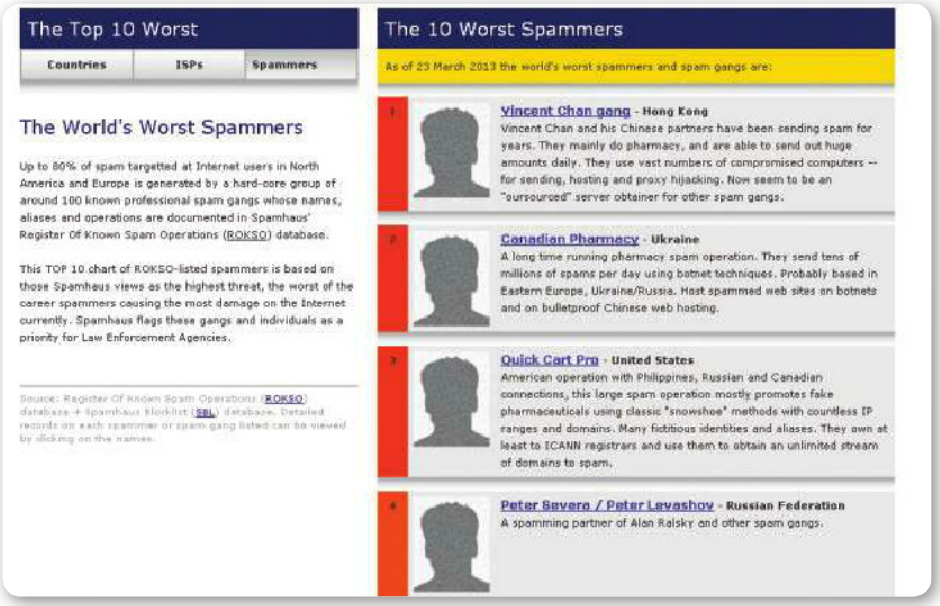


Figura 21. En **www.spamhaus.org** vemos un ranking de los spammers más temidos en el mundo.

Origen

El origen de la palabra aplicada al mundo de la informática es un tanto incierto, pero de todas las versiones la que pareciera más real es la que cuenta la siguiente historia. Una empresa norteamericana, llamada **Hormel Foods**, tenía un producto denominado **Spiced Ham** (algo así como 'jamón con especias') lanzado al mercado en el año 1937; se trataba básicamente de carne enlatada, que contaba con conservantes y especias, y podía mantenerse por mucho tiempo antes de ser consumido. Durante la Segunda Guerra Mundial, el Spiced Ham se utilizó para alimentar a las tropas soviéticas y también británicas, dada su versatilidad y duración. Tal fue su éxito que, desde el año 1957, comenzó a venderse en latas con sistemas de apertura fácil para evitar el uso de los abrelatas tradicionales.

Es interesante mencionar que años más tarde, el grupo cómico inglés **Monty Python** utilizó el nombre en un sketch que realizaba en el programa **Flying Circus**, en el que una pareja en un bar pedía comida y, en el menú, encontraba que todos los platos que había tenían spam, desde huevos con spam, hasta salchichas con spam, jamón con spam, y así todo. De esta forma, el mozo les leía el menú mientras ellos escuchaban repetidamente la palabra **spam**.

Figura 22. Ranking de los 10 ISPs más generadores de spam en el mundo.

Ya en los años 80, se adoptó el término para describir el comportamiento abusivo de algunos usuarios que frecuentaban los primeros **BBSs**, que repetían "spam" una gran cantidad de veces para lograr que el texto de otros usuarios saliera de la pantalla por medio del **scrolling** del texto. De hecho, en los primeros servicios de chat, como **PeopleLink** y **Online America** (posteriormente **America Online**) lo que se repetía eran directamente frases del mencionado sketch de Monty Python.

Más allá de la historia, lo cierto es que **no representa una sigla**, y que ha pasado por diferentes etapas, comenzando por ser un verdadero flagelo, hasta casi estar resuelto en determinados niveles.

Funcionamiento

Una de las primeras preguntas que surgen cuando se habla de spam es cómo los spammers (quienes envían spam) obtienen las direcciones de e-mail para enviarles sus correos basura. Los spammers consiguen armar grandes bases de datos de distintas maneras, a saber: la primera es utilizando algún tipo de **malware** que, al infectar un sistema, se replica **enviándose por e-mail** a los contactos de la **libreta de direcciones** de la persona afectada (ya sea en servicios de webmail como en correo recibido en la PC). Cuando las demás personas están

infectadas, repite el proceso y va recopilando direcciones en los sistemas infectados.

Otra manera es mediante el **engaño** a los usuarios, utilizando **cadenas de correo** referidas a alguna causa noble, como la lucha contra el cáncer, pedidos de solidaridad, supersticiones varias, onomásticos y demás. En estos correos, se incita al usuario a **reenviar voluntariamente** el e-mail a sus contactos, de modo que entre dichos contactos aparezca quién envía el e-mail originalmente, y este pueda ver todos los reenvíos que se realizan, obteniendo así direcciones de contactos de los contactos. Esto se podría evitar si quienes desean reenviar cadenas de e-mails utilizaran la opción de envío con copia oculta (**BCC** o **Blind Carbon Copy**) para que los receptores no puedan ver a quién más se le está enviando la cadena en cuestión.

> ES POSIBLE RECOPILAR DIRECCIONES AL COMPRAR LISTAS COMERCIALES

Otra forma de recopilar direcciones es por medio de la compra de **listas comerciales**, que son **bases de datos** provistas por las empresas y organizaciones que de por sí recaban los datos por otra cuestión, ya sea por motivos de marketing, estudios de mercado, etcétera. Estas bases de datos suelen filtrarse desde dentro de las organizaciones, por medio de empleados que, al tener acceso, las utilizan para comercializar, en tanto que dicho comportamiento por supuesto no está aprobado por la empresa.

Una manera bastante más evidente de obtener direcciones de correo electrónico es la simple **búsqueda en Internet**. Tanto en foros como en blogs, redes sociales y otros sitios, la gente coloca sus direcciones de e-mail como parte de la información personal de contacto, sin

SPAM E IRC

El spam es tan antiguo como el IRC. Este tipo de mensajes basura se encontraba en las redes de conversación en línea toma, presentó auge gracias a la masificación de este medio de comunicación. En estas redes se podía observar que los mensajes más habituales solían presentar como único objetivo lograr la visita de otros canales de chat, la visita de sitios webs y también la difusión de diversos contenidos que se distribuían en forma comercial.

saber que muchas veces los spammers recolectan esa información con programas robot que recorren la red en su búsqueda. Una forma sencilla de evitar esto es simplemente no dejando nuestra dirección de e-mail, pero en caso de que sea necesario, existen escrituras alternativas como **nombre [at] dominio.com** o algo similar para representar la arroba, que es el carácter que normalmente los robots virtuales intentan detectar a la hora de determinar si se ha encontrado una dirección de e-mail. Otros, especialmente en sitios personales, lo evitan colocando el e-mail **en forma de gráfico**.

Figura 23. La empresa Barracuda Networks provee **Appliances antispam** para combatir el problema.

La última de las técnicas clásicas del spammer para obtener direcciones válidas es tomar los dominios más importantes de los correos gratuitos, como **Hotmail** (**Outlook**), **Gmail**, **Yahoo!**, **AOL**, **GMX** y otros, y generar nombres de usuario que se comprobarán contra el servidor de correo solicitando el envío a esa dirección. El servidor responderá afirmativamente en caso de que la cuenta exista, y el spammer no le enviará la cuenta, sino que guardará la información en la base de datos como cuenta válida. De esta forma, se explota la posibilidad de que, en dominios muy numerosos, utilizados por millones de usuarios, existan **nombres comunes** y sus combinaciones con números, apellidos, etc. Esta probabilidad es fácil de comprobar

al querer sacarnos una nueva cuenta de correo, cuando casi todos los nombres que escribimos ya están previamente registrados y no podemos utilizarlos por tal razón. El spammer aprovechará eso para deducir direcciones válidas y crear más listas de usuarios.

Infraestructura

Por otra parte, el spammer requiere de una infraestructura en particular para el envío de miles de millones de mensajes, ya que no puede realizarlo desde una conexión hogareña o comercial, pues el **ISP** la detectaría y la bloquearía justamente por envío de spam. Aquí es donde entran en juego los mecanismos de envío. Uno de los más básicos es **utilizar conexiones hasta saturarlas** y que sean bloqueadas para luego pasar a otra y saturarla, y así de manera sucesiva. Esto puede realizarse en especial desde conexiones **inalámbricas públicas o robadas** en sectores donde se encuentran accesibles físicamente. En forma adicional, se puede utilizar el máximo potencial de las **direcciones IP** y las conexiones de banda ancha sin que se lleguen a bloquear por saturación del uso del servicio, pero es más complejo para el spammer.

> UN SPAMMER REQUIERE UTILIZAR UNA INFRAESTRUCTURA PARTICULAR

Otra técnica consiste en escanear grandes rangos de direcciones IP de Internet en busca de servidores de correo electrónico mal configurados, que permitan realizar lo que se llama **Open Relay**, o envío de correo sin necesidad de autenticación por parte del usuario, es decir, sin que se precise una cuenta en ese dominio o sistema. Si bien este problema en los servidores de correo ha disminuido con el tiempo, muchas veces ocurre que, por algún descuido, queda alguno mal configurado y, por el tiempo que se le permite hasta su bloqueo, será utilizado por el spammer desde el momento inmediato en que lo detecte.

Enfrentar el spam

Existen una serie de contramedidas que se pueden tomar para enfrentar el spam, y todas dependerán del nivel en el que se quieran aplicar. Por ejemplo, una buena idea es contar con una **dirección**

válida personal, pero **especial para recibir spam**, la cual sabemos que podemos utilizar para registrarnos en sitios sin preocuparnos de que nos la llenen de publicidad, pero que a la vez podamos acceder en el caso de que nos envíen algún link para registración o similar. También podemos contar con direcciones temporales, pero nos encargaremos de ese tema más adelante.

Una contramedida más técnica y de implementación a gran escala es el uso de **listas negras** de direcciones. Estas listas deben actualizarse con alta frecuencia, dado que las direcciones pueden variar constantemente, y constituyen uno de los mecanismos principales sobre los cuales se basa el filtrado de spam actual a nivel de ISPs y de grandes proveedores de servicios de correo. Esta técnica, sin embargo, no suele ser muy implementada por el usuario final, ya que existen otras más eficientes para ello.

> LOS FILTROS BAYESIANOS ESTÁN ENTRE LAS TÉCNICAS PARA ENFRENTAR EL SPAM

Entre las técnicas que pueden ser implementadas por el usuario en su software cliente, se encuentra el uso de **filtros bayesianos**. Estos filtros implican el uso del **teorema de Bayes**, utilizado ampliamente en estudios de **probabilidad y estadística**, para deducir qué probabilidad hay de que un mensaje sea spam considerando que posee una cierta cantidad de palabras que aumentan o disminuyen dicha probabilidad. Entonces, existirá una lista de **palabras prohibidas** o de alto nivel de probabilidad de que representen un spam o se encuentren en él, y se analizará contra ella cada mensaje que arribe. Cuando llegue un nuevo correo, se analiza el contexto y se calcula la probabilidad de que sea spam, teniendo en

EVOLUCIÓN DE LA SOLUCIÓN

Durante los primeros años del siglo XXI, el spam representaba un gran problema debido al enorme consumo de ancho de banda que demandaba su descarga, especialmente cuando las conexiones promedio eran de línea telefónica (Dial-Up). Con el tiempo, las conexiones de banda ancha hicieron que solo fuera una molestia por mezclarse entre los mensajes reales. Hoy en día, con una buena configuración de filtrado, un buen tiempo "entrenándolo" y un buen servicio de e-mail, ya casi podemos considerarlo un problema menos.

consideración tanto lo bueno como lo malo. Algunas palabras reducirán mucho la probabilidad, y otras la incrementarán.

Otras técnicas más específicas incluyen la recepción con **autorización explícita**, ya sea mediante el uso de firma digital o algún otro sistema de autenticación, con el problema inherente de que también reduce la funcionalidad del sistema, por quedar fuertemente restringido.

Por último, debemos mencionar que prácticamente todo el software y hardware comercial **antispam** (basado en especial en el análisis bayesiano) suele permitir al usuario tomar decisiones sobre mensajes dudosos, o quitar del filtrado los **mensajes válidos**, de manera que el sistema puede ir aprendiendo a medida que se utiliza, en función de las preferencias particulares de cada usuario. Esto nos lleva a concluir que no existen dos sistemas de filtrado iguales, ya que lo que es spam para una persona, quizás no lo es para otra, y viceversa.

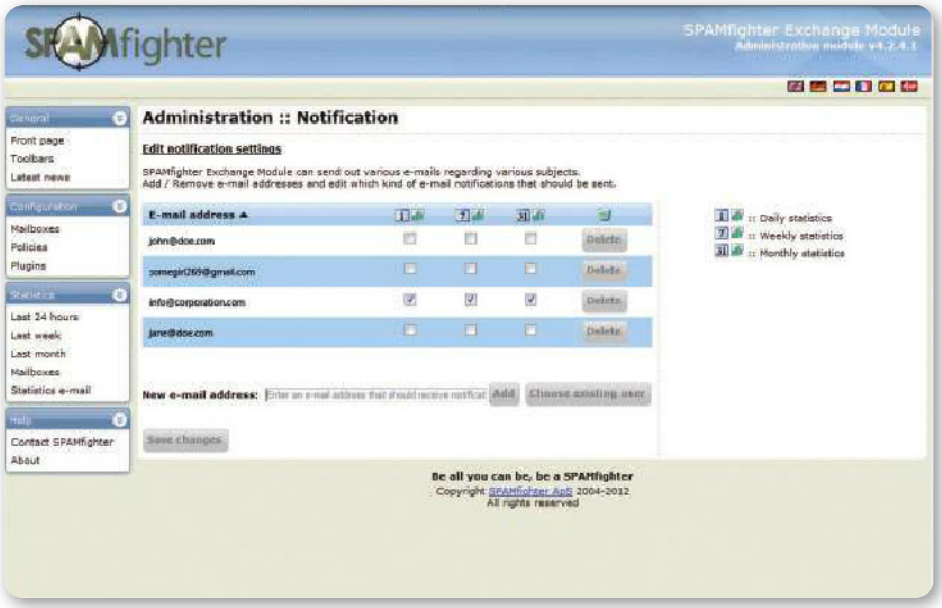


Figura 24. Spamfighter es un potente antispam gratuito para **Mozilla Thunderbird** y **Microsoft Outlook**.

El spammer, por supuesto, contará con una serie de contratécnicas y trucos para evitar que los mecanismos utilizados por los filtros antispam sean efectivos, y estas técnicas son de lo más variadas. Un ejemplo es el uso del **idioma nativo** del receptor, lo cual puede deducirse a veces por el país en el que está alojado el dominio, o colocar datos aleatorios (o específicos quizás) en el campo **From** (de)

de manera que pueda ir variando, o contar con un **Subject** (asunto) **amigable** para que tiente al usuario a abrirlo. Además, aprovechando las características comunes de los correos actuales, cuya gran mayoría admite (salvo configuración explícita) el uso del **lenguaje HTML**, se puede manipular dicho lenguaje para que muestre o no muestre ciertas cosas, o que incluya imágenes en vez de palabras para que no puedan ser fácilmente detectadas por el filtro de texto —basado en principio en texto escrito en alguna codificación (**encoding**) como **ASCII**, **UNICODE**, etcétera—. Por supuesto que siempre se intentará codificar también las URL a las que apunte el mensaje, para que no puedan ser leídas y bloqueadas con facilidad.

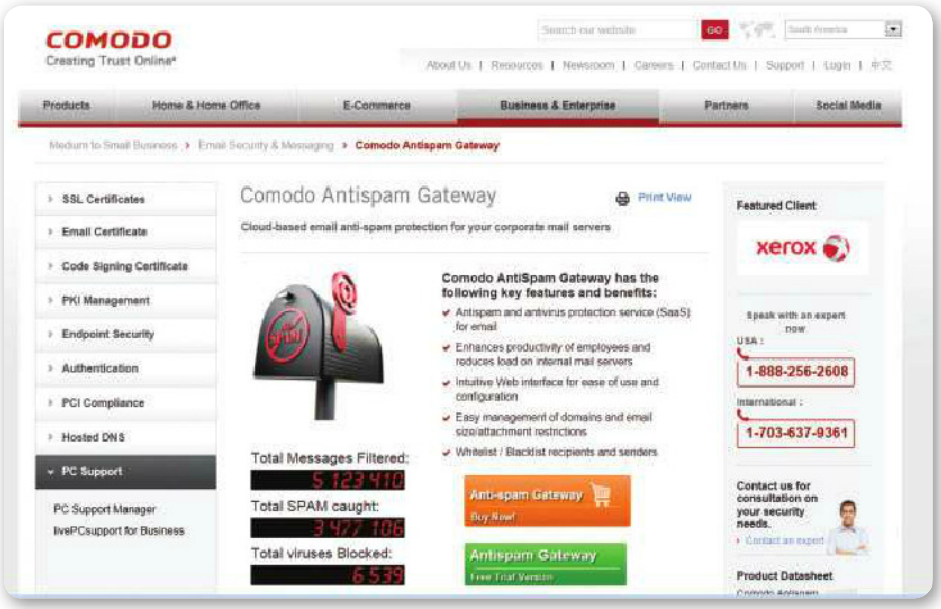


Figura 25. Comodo Antispam Gateway ofrece una solución antispam por software basada en la nube.

En cuanto a los métodos más alternativos, el spammer utiliza algunos **trucos visuales** o **patrones**, como por ejemplo la escritura con un espacio entre letras, o con un punto entre letras de una palabra, de modo que para el filtro la palabra **s.e.x.o** no significaría lo mismo que **sexo** y tal vez lo engañaría, pero el usuario que lo lee podría entender de qué se trata sin problemas. La idea en todos los casos es **engañar al filtro**, pero que la información permanezca visible y comprensible para el usuario.

Una técnica algo más sofisticada es el agregado en el mensaje de **palabras válidas** para confundir al filtro, que reduzcan la posibilidad

de que sea considerado spam al ser analizado, como ser el nombre de la persona, o datos aleatorios que no contengan las palabras clave que suelen ser las que aumentan la probabilidad de que lo sea.

Figura 26. Existen muchas soluciones de software que incorporan sistemas antispam para proteger al usuario.

RESUMEN

En este capítulo pudimos analizar en detalle el funcionamiento de un servidor de correo electrónico; a continuación aprendimos a instalarlo y también a efectuar su correcta configuración en sistemas operativos Windows y en distribuciones GNU/Linux. Además conocimos los peligros del spam y mencionamos algunos consejos mediante los cuales podemos enfrentarlo.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es un servidor de correo?
2. ¿Para qué sirve el protocolo SMTP?
3. ¿Qué hace el protocolo POP?
4. Describa las ventajas del correo en la nube.
5. ¿Qué es Thunderbird?
6. ¿Cómo funciona Microsoft Exchange Server?
7. ¿Qué encontramos en la configuración del buzón de Exchange?
8. Mencione los MTA más comunes en GNU/Linux.
9. ¿Qué es una MLM?
10. ¿Qué es el SPAM?

EJERCICIOS PRÁCTICOS

1. Instale Microsoft Exchange.
2. Acceda a la consola de administración de Exchange.
3. Realice la configuración de la organización.
4. Configure el filtrado inteligente.
5. Instale y utilice Fdm.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*06

Servidores de archivos e impresión

En este capítulo conoceremos las funciones que desempeña un servidor de archivos, luego aprenderemos a administrarlo en un sistema Windows y también en un sistema GNU/Linux. Para continuar veremos los servidores de impresión y detallaremos sus características.

Servidor de archivos

Un **servidor de archivos** es un equipo que cumple la función de almacenar archivos en una red y convertirse en el repositorio para los clientes que acceden a los recursos allí almacenados. Esta función puede cumplirla cualquier PC de escritorio con un software acorde, o equipos dedicados, de mayor potencia y capacidad para este fin.

Cuando hacemos mención a software acorde, nos referimos al que permite administrar el protocolo de red para compartir archivos. Veamos, a continuación, los más usados.

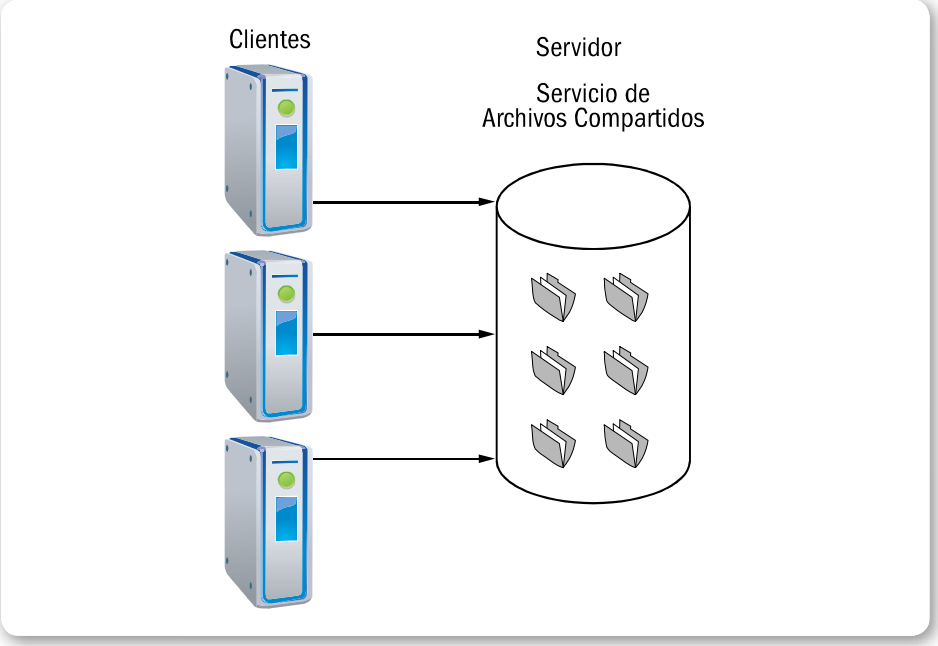


Figura 1. En este esquema podemos visualizar un servidor de archivos y sus clientes.

SMB (Server Message Block)

Es un protocolo de capa de aplicación en el modelo OSI, que nos permite compartir archivos e impresoras. **SMB** es un servidor de clientes; funciona con un protocolo de petición-respuesta. La única excepción a la naturaleza de solicitud y respuesta de SMB (cuando el cliente realiza peticiones y el servidor envía respuestas) se da cuando el cliente ha solicitado bloqueos oportunistas (oplocks), y el

servidor posteriormente tiene que romper un bloqueo operativo ya concedido por otro cliente, ya que ha solicitado un archivo abierto con un modo que es incompatible con la operación de bloqueo concedida. En este caso, el servidor envía al cliente un mensaje no solicitado de señalización de la ruptura de operación de bloqueo.

Los clientes se conectan a los servidores mediante TCP/IP (en realidad NetBIOS sobre TCP/IP como se especifica en el RFC1001 y RFC1002), NetBEUI o IPX/SPX. Una vez que se haya establecido la conexión, el cliente puede enviar comandos (SMBs) en el servidor que les permite acceder a recursos compartidos, archivos abiertos, leer y escribir archivos y, en general, hacer todo el tipo de cosas que queremos realizar con un sistema de archivos. Sin embargo, en el caso de las SMB, estas actividades se efectúan a través de la red.

Figura 2. Samba en una distribución Ubuntu, nos permite compartir archivos; a estos se puede acceder desde clientes Windows y Mac OS X.

SAMBA

Es un software de licencia GNU, una implementación de SMB que, desde el año 1992, permite la interoperabilidad de compartición de archivos e impresoras entre equipos con sistemas operativos Windows (SMB/CIFS), Linux, Mac OS o UNIX.

SMB/CIFS (Common Internet File System)

Es la modificación realizada por Microsoft al protocolo SMB creado por IBM, usado a partir de Windows 2000; este trae notables mejoras en materia de seguridad (aunque en la actualidad se le han encontrado múltiples vulnerabilidades) y estabilidad en el uso, entre otros.

Las características que ofrece CIFS son las siguientes:

- **Integridad y concurrencia**: permite a varios clientes acceder y actualizar el mismo archivo, mientras que la prevención de conflictos proporciona el intercambio y bloqueo de archivos.
- **Uso compartido y bloqueo de archivos**: es el proceso de permitir a un usuario acceder a un archivo a la vez y bloquear el acceso a todos los demás usuarios. Estos mecanismos de distribución y de fijación se pueden utilizar a través de Internet e intranet. También, permiten el almacenamiento en la caché, para lectura anticipada y escritura en segundo lugar, sin pérdida de integridad. Estas capacidades aseguran que solo una copia de un archivo puede estar activo por vez, y evitan la corrupción de datos.
- **Optimización de vínculos lentos**: el protocolo CIFS ha sido adaptado para funcionar con la más baja velocidad.
- **Seguridad en servidores**: admiten tanto las transferencias anónimas como el acceso seguro y autenticado de archivos con nombre de usuario y contraseña. Las políticas de seguridad de archivos y directorios son fáciles de administrar.
- **Nombres de archivo Unicode**: los nombres de archivos pueden estar en cualquier conjunto de caracteres, no solo con juegos de caracteres diseñados para los idiomas europeos inglés u occidental.

COPIAS DE SEGURIDAD

Un servidor de archivos nos brindará muchos beneficios, como los ya mencionados, pero debemos tener en cuenta que la disponibilidad de esos archivos debe encontrarse resguardada por un backup periódico (según la criticidad de la información almacenada). En caso de que el servidor dejara de funcionar ante cualquier tipo de contingencia, debemos disponer de un plan de recuperación de la información.

- **Nombres de archivo global**: los usuarios no tienen que montar sistemas de archivos remotos, pero puede referirse directamente a ellos con nombres de importancia mundial (nombres que se pueden encontrar en cualquier sitio de Internet), en lugar de los que tienen solo importancia local (en un equipo local o LAN). El sistema de archivos distribuidos (DFS) permite a los usuarios construir un espacio de nombres en toda la empresa.
- **Convención de nomenclatura uniforme (UNC)**: los nombres de archivo son compatibles, por lo que una letra de unidad no necesita ser creada antes de que los archivos remotos sean accesibles.

> PODEMOS CREAR UNA LISTA DE CONTROL DE ACCESO Y RESGUARDAR LA INFORMACIÓN

NFS (Network File System)

Consideremos que se ubica en la capa de aplicación según el modelo OSI, desarrollado por la empresa Sun Microsystems, con el fin de fomentar el uso de archivos en equipos. Se ha desarrollado para permitir que las máquinas monten una partición de disco en un equipo remoto como si fuera un disco local.

Viene incluido de manera predeterminada en sistemas operativos UNIX y en la mayoría de las distribuciones GNU/Linux.

Ventajas de un servidor de archivos

Un servidor de archivos nos proporciona múltiples ventajas, las cuales enumeraremos a continuación:

- **Centralización de archivos**: ya que nos permite almacenar todos los archivos en una sola ubicación física, y que estos se encuentren disponibles para todos los clientes sin la necesidad de que cada uno disponga del archivo de forma local.
- **Disponibilidad**: al utilizar un servidor de archivos, estamos dedicando un equipo a esta función que se encontrará disponible en la red durante las horas del día necesarias; en caso de necesitar acceder al recurso, podríamos hacerlo desde cualquier equipo de la red (con las credenciales de usuario autorizadas).

- **Integridad**: nos permite mantener la integridad de los archivos debido a que, al trabajar muchas personas con un documento, siempre se encontrará disponible la última versión de este en el servidor de archivos; en el caso de que muchas personas trabajen de manera local con un documento, es muy difícil mantener su integridad.
- **Control de acceso a la información**: nos permite crear ACLs (listas de control de acceso) para darles seguridad a los archivos que utilizamos, asegurarnos de que accedan a ellos solo personas autorizadas y, además, auditar las acciones realizadas por los usuarios.
- **Centralización de backups**: al disponer de un almacenamiento centralizado, la tarea de backup se concentra en un solo equipo, evitando así que perdamos tiempo en realizar, a diario, backups de los equipos personales, ya que la información valiosa se almacenará en el servidor de archivos.

En la actualidad, existen servidores de archivos de hardware que permiten la compartición de archivos de forma nativa, conocidos como **NAS** (*Network Attached Storage* o almacenamiento conectado en red), que son dispositivos dedicados a cumplir esta función con soporte a los protocolos de compartición de archivos más usados.

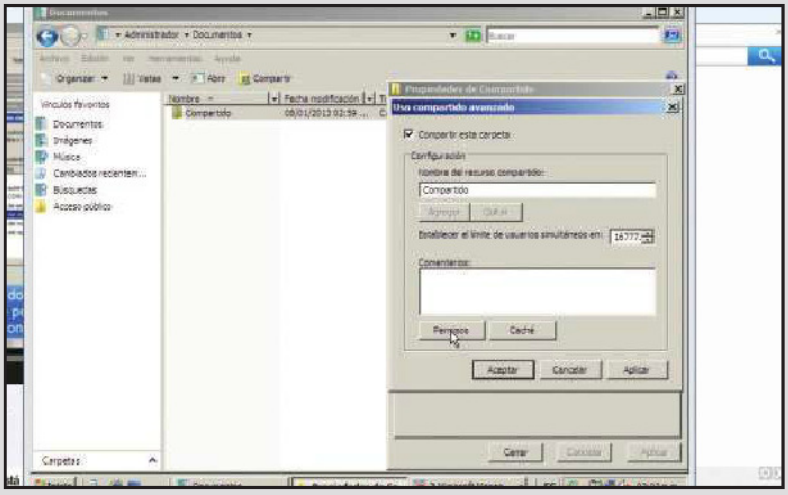
Figura 3. Dispositivo NAS que soporta 12 discos, dispone de 2 puertos Ethernet de 1 GB, procesador Dual Core de 3.3 GHz y memoria RAM de 4 GB expandible a 8 GB.

Administración en Windows

La administración básica de un servidor de archivos o file server en sistemas Windows requiere que tengamos en cuenta algunos consejos importantes. En el siguiente **Paso a paso** mencionaremos cada uno de los detalles que es necesario considerar.

PAP: SERVIDOR DE ARCHIVOS EN WINDOWS

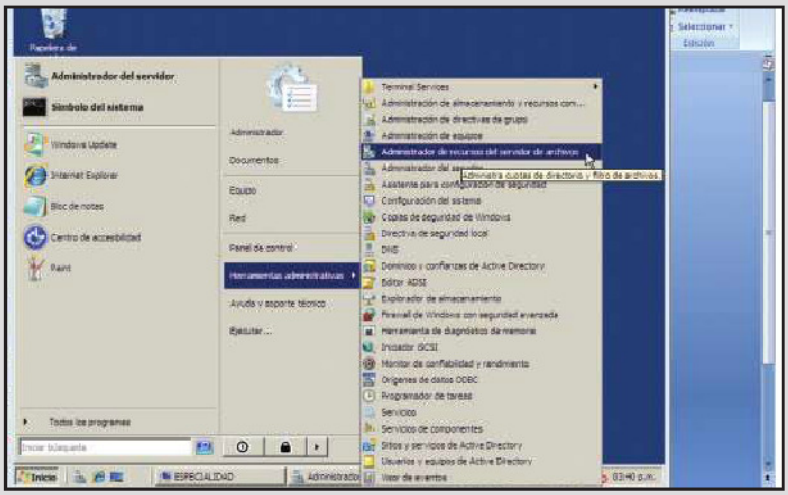
01 Inicie compartiendo un archivo desde el servidor de Windows. Para ello, es necesario crear una carpeta, por ejemplo, con el nombre `Compartido`, la cual puede estar ubicada en: `C:\Usuarios\Administrador\Documentos\Compartido`. Finalice asignando los permisos correspondientes.



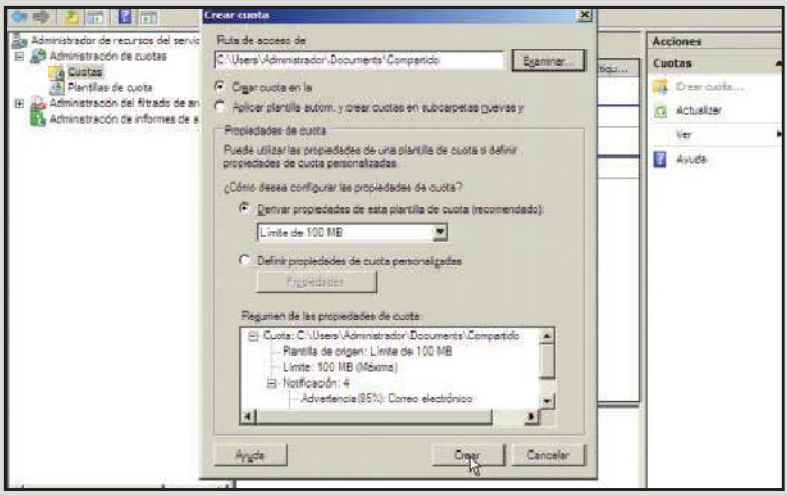
FUNCIONAMIENTO

El funcionamiento de un servidor de archivos es sencillo. Una vez que se haya configurado correctamente y se haya publicado en la red, será posible utilizar el espacio de almacenamiento que se encuentra disponible en el servidor de archivos, para ello se realiza la asignación de las unidades correspondientes. Cuando se asigna como una unidad, el sistema operativo podrá leerlo y tratarlo como una unidad adicional presente en cada computadora que se conecte al servidor.

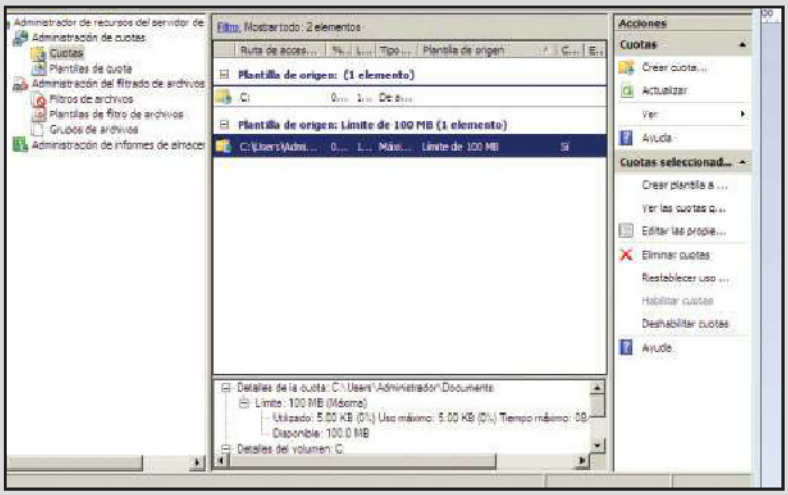
02 Ahora, desde el botón `Inicio/ Herramientas administrativas`, ingrese a la opción `Administrador de recursos del servidor de archivos`. Desde aquí, comenzará con la administración básica del servidor.



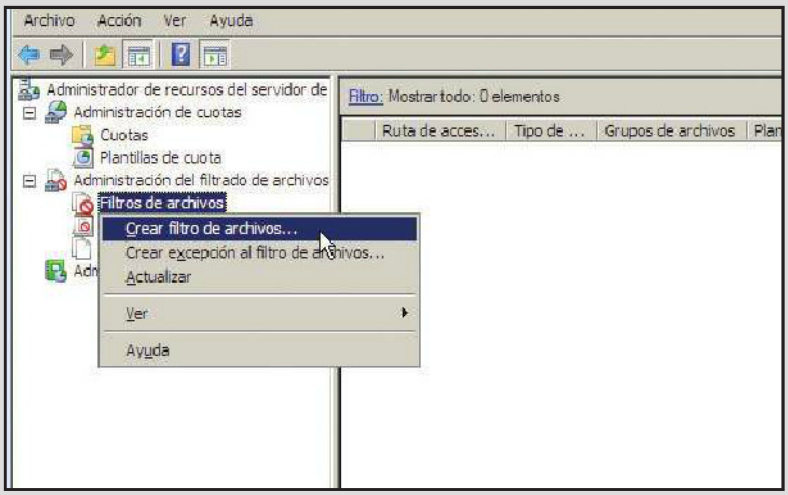
03 Para crear una cuota, presione clic derecho y elija `Crear cuota`. En la nueva ventana, coloque la ruta donde se halla almacenada la carpeta (`Compartido`). Luego, asigne un límite (por ejemplo: 100 MB), y presione `Crear`.



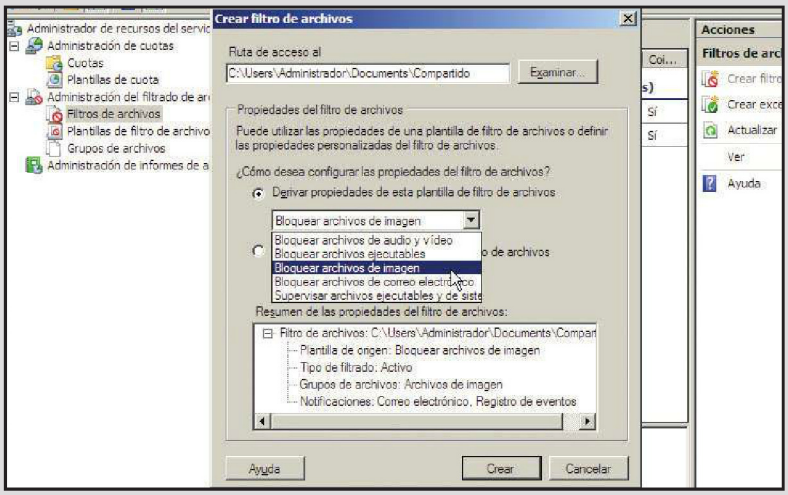
04 Para comprobar que se ha llevado a cabo la creación y configuración adecuada de la cuota, seleccione la opción `Cuota` y verifique su configuración, desde la sección denominada `Mostrar todo`.



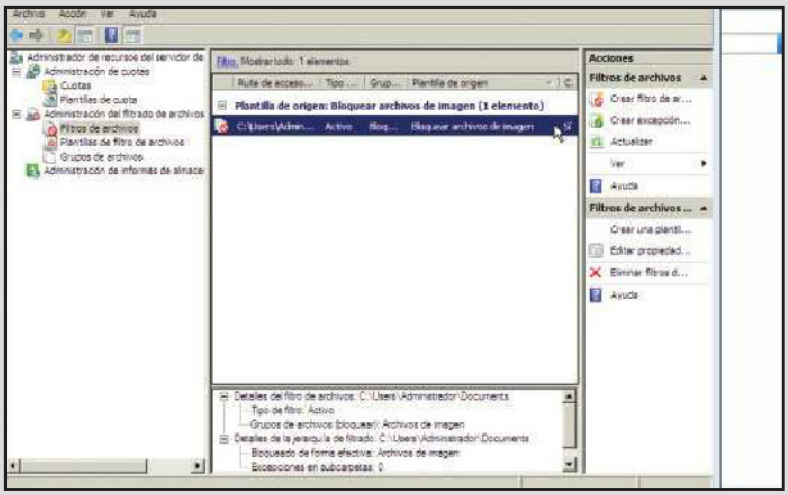
05 Para continuar, proceda a crear un filtro de archivos. Para ello, seleccione la opción `Administración del filtrado de archivos`, ubicada en el panel izquierdo de la ventana `Administrador de recursos` del servidor de archivos.



06 Ahora, coloque la ruta donde se halla almacenada la carpeta compartida. Después, presione `Propiedades`, para definir las características del filtro de archivos. Una vez allí, elija del combo `Bloquear archivos de imagen`, y presione `Crear`.



07 Verifique si se ha llevado a cabo la creación del filtro. Seleccione `Filtros de archivos`, ubicada en el panel izquierdo de la pantalla. Los datos de alta se pueden apreciar en la sección `Filtro`, ubicada en el centro de la ventana.



Es importante considerar que para tener acceso a la opción llamada **Administrador de recursos del servidor de archivos**, será necesario realizar la instalación de la función **Servicios de archivos.**

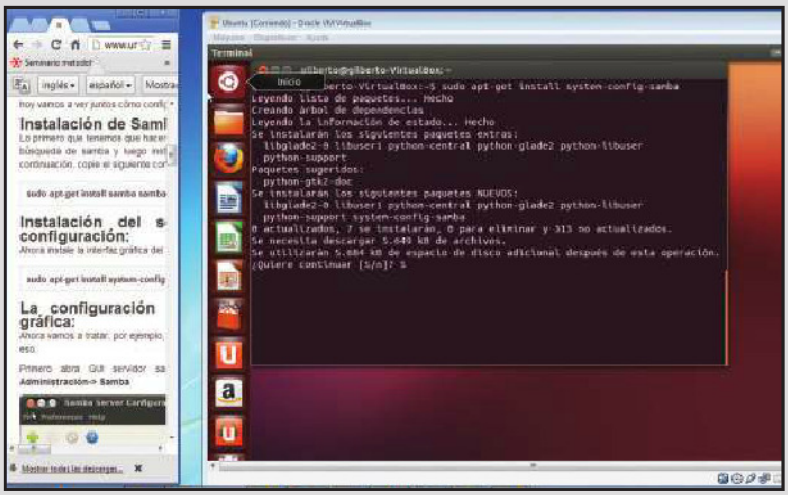
Si no completamos el proceso de instalación de la función que ya comentamos, esta no estará visible desde las herramientas administrativas ofrecidas por el servidor.

Administrar un servidor de archivos en Linux

En esta sección realizaremos la administración de un servidor de archivos desde un sistema GNU/Linux. Como en el caso anterior, completar esta tarea requiere que prestemos atención a los detalles que mencionamos en el siguiente **Paso a paso**.

PAP: SERVIDOR DE ARCHIVOS EN LINUX

01 Encienda su PC y cargue el escritorio de Ubuntu 12.10. Abra la terminal e instale el paquete Samba. Esto se logra mediante el comando `#sudo apt-get install samba samba-common`, luego pulse ENTER. Ahora instale la interfaz gráfica del sistema de configuración de Samba como se ve a continuación:



02 Desde el botón `Inicio` de Ubuntu escriba `Terminal` y seleccione la funcionalidad Samba instalada. Aparece `Configuración del servidor Samba`, donde debe presionar el icono en forma de cruz para comenzar a compartir archivos.

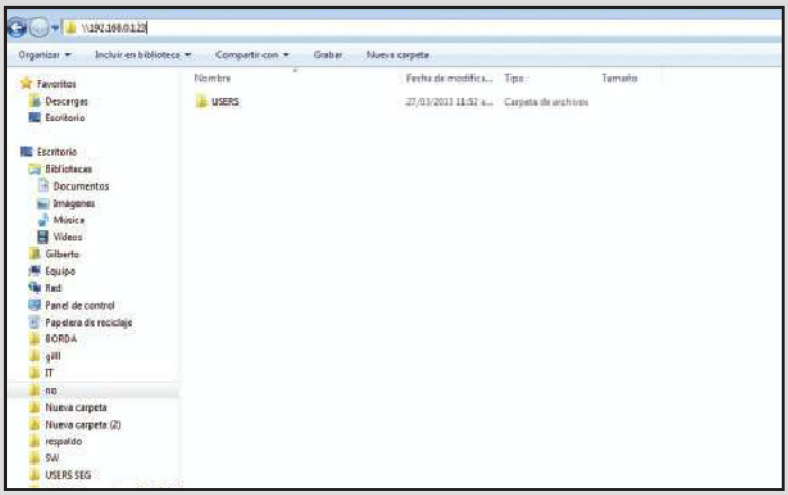
03 Proceda a compartir un archivo seleccionando el botón `Examinar` del campo `Directorio`. Agregue una descripción y delegue los permisos de acceso. Esto último se logra haciendo clic en la pestaña `Acceso`. Pulse `Aceptar`.

04 Note que ha sido dada de alta la ruta del archivo por compartir en el servidor. En este caso, lo que desea compartirse es un directorio ubicado en el escritorio del sistema. Cierre la ventana para continuar con la compartición de los archivos.

05 Ubique el archivo que se va a compartir. Luego, presione el botón derecho del mouse sobre la carpeta y seleccione `Opciones de compartición`. Asigne un nombre y delegue el acceso a los usuarios de su preferencia.

06 Abra las propiedades del archivo para asignar parámetros de acceso, políticas de seguridad y permisos. Seleccione el fichero por compartir y despliegue sus propiedades. Navegue por las fichas `Básico`, `Permisos` y `Compartir`.

07 Los equipos pueden estar usando un mismo sistema operativo en la red, sin embargo, existe la posibilidad de que no sea así. Si este fuera el caso, abra Windows y coloque la dirección IP del server, y acceda al archivo compartido.



Es posible que, durante la inspección o apertura de algunas ventanas de configuración del sistema, por ejemplo para el acceso a Samba, se le haya solicitado escribir una contraseña. Esta es la misma que utilizó en el momento de instalar su sistema Linux Server.

Seguridad en servidores de archivos

La protección de los archivos en la red corporativa de una organización es un factor crítico que tiene a bien asegurar la continuidad de sus operaciones.

Por eso, hoy en día existen incontables soluciones informáticas que cumplen con la tarea de brindar seguridad e integridad a los archivos, aplicaciones y servicios compartidos en el entorno corporativo.

En la actualidad, muchas compañías han vislumbrado la necesidad de contar con una plataforma que garantice la seguridad total del servidor de archivos manejada en la red informática. Para ello, se han dado a la tarea de implementar una interesante opción incluida en sus antivirus, mejor conocida como *Security Solution for File Servers* (solución de seguridad para servidores de archivos).

Soluciones

Las soluciones **Security for File Servers**, representan hoy en día una utilidad altamente demandada que garantiza, desde luego, la seguridad de la información. Se trata de un servicio dedicado a servidores.

AVAST FILE SERVER SECURITY

La solución de seguridad para servidores de archivos propuesta por Avast (**Avast File Server Security, www.avast.com/es-cl/file-server-security**), se presenta como una opción para la protección de servidores de alto rendimiento. Es compatible con los sistemas operativos más utilizados, como Windows 2012/2008/R2 y 2003 Server, y además ofrece un complemento para SharePoint Server.

UTILIDADES DE SEGURIDAD EN FILE SERVERS	
▼ NOMBRE DE LA UTILIDAD	▼ DESCRIPCIÓN
Panda Security for File Servers	Ofrece una eficaz protección preventiva contra malware e intrusos para servidores Windows. Para mayor información, puede consultar en **www.pandasecurity.com/mexico/enterprise/solutions/fileservers**.
ESET File Security para Windows	Incluye un administrador remoto. Además, integra un sistema de detección de virus con el mínimo consumo de recursos. Para más información, ingrese en **www.eset.es/empresas/productos/file-windows**.
AVG File Server Business Edition	Brinda un control completo de sus archivos, protegiéndolos ante amenazas en línea, y mantiene un máximo rendimiento del servidor de Windows. Puede consultar en **www.avg.com/ww-es/avg-file-server-edition**.
Avast File Server Security	Analiza el tráfico de sus servidores, proporcionando una protección eficaz contra infecciones. Más información en **www.avastmexico.com.mx/avast/html/file.html**.
Kaspersky Antivirus Windows Server Enterprise	Ofrece una potente protección para los servidores. Es una completa solución para mantener la seguridad en redes corporativas. Puede consultar en **www.kaspersky.com/products/business/applications/anti-virus-windows-server-enterprise**.
Bitdefender for File Severs	Se trata de una solución de seguridad de datos especialmente dedicada a servidores Windows. Puede consultar en **www.bitdefender.es/business/security-for-file-servers.html**.

Tabla 1. Los antivirus más famosos y su infraestructura Security File Servers.

LOS ANTIVIRUS ACTUALES PUEDEN RASTREAR VIRUS OCULTOS EN EJECUTABLES

Muchos antivirus modernos incluyen un novedoso y potente sistema, capaz de identificar patrones sospechosos en aplicaciones maliciosas y ataques dirigidos. Cumplen también con rastrear virus que pudieran permanecer ocultos en archivos ejecutables protegidos o comprimidos, utilerías, bases de datos, ficheros de sistema y, desde luego, en documentos, además de estar especialmente diseñados con el propósito de mantener nuestros equipos (y por consiguiente una corporativa) con un rendimiento óptimo.

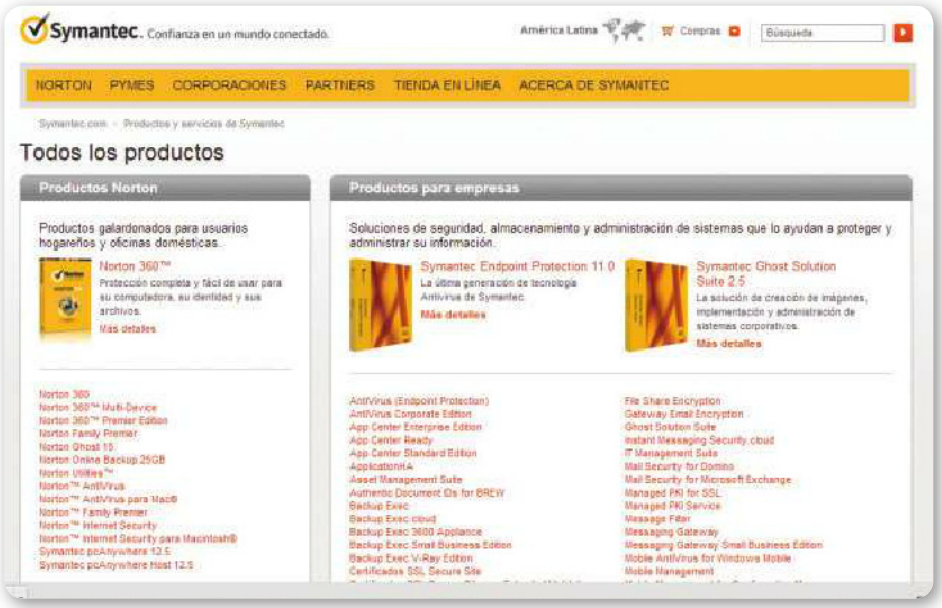


Figura 4. Algunas firmas, como Symantec, ofrecen a través de la Web un mundo de soluciones de seguridad en File Servers para redes corporativas.

Instalación

Es importante considerar que si deseamos realizar la instalación de funcionalidades File Server sobre plataformas Microsoft Windows, debemos considerar algunos requerimientos técnicos: un procesador Intel o AMD x86/x64, compatible con sistemas de Microsoft (Windows Server 2000, 2003, 2008, 2008 R2, 2012) y un espacio en el disco 230 MB (espacio en el disco requerido después de la instalación y aplicación de las correspondientes actualizaciones).

> NECESITAMOS AL MENOS 230 MB DE ESPACIO PARA LA FUNCIONALIDAD FILE SERVER

SET FILE SECURITY

ESET File Security (**www.eset-la.com/empresas/server-security/windows-file**), desarrollado para funcionar sobre servidores de archivos Microsoft Windows, es una herramienta poderosa que proporciona altos niveles de protección para servidores de archivos. Sus características son similares a ESET NOD32 Antivirus, pues está basado en el motor ThreatSense®.

Figura 5. En la página principal de Bitdefender, encontraremos una versión de prueba descargable de productos Security File Servers.

Sistemas Linux

Hasta ahora, mucho se ha hablado de la seguridad en File Servers para sistemas de Microsoft, pero ¿qué hay de la seguridad en File Servers basados en Linux? ¿Qué tipo de soluciones existen para el ya conocido sistema operativo del pingüino?

Se sabe que GNU-Linux es más seguro en comparación con los sistemas Windows. Sin embargo, lo que muchos no saben es que las grandes redes corporativas (que por lo regular hacen uso de servidores de archivos) que se ejecutan en distintas plataformas (Windows y GNU-Linux) pueden presentar problemas por infección. La razón de ello se debe no solo a la convivencia entre sistemas operativos distintos, sino al frecuente y masivo intercambio de información entre una terminal y otra.

> DEBEMOS CONTAR CON LAS APLICACIONES DE SEGURIDAD ACTUALIZADAS

Cada vez es más común encontrarnos con compañías que basan sus actividades en servidores de archivos Linux y Unix (BSD, FreeBSD), por lo que recomendamos que, a medida que veamos crecer el volumen de datos en nuestra red, incrementemos también la necesidad de protegerla del malware.

Es importante considerar que en la actualidad, las empresas creadoras de antivirus para Windows han incluido una versión totalmente dedicada al sistema operativo del pingüino. Tal es el caso de las empresas **AVG**, **Kaspersky** y también **ESET**, solo por mencionar algunas.

Los servidores de archivos basados en GNU-Linux, por lo general, cuentan con una sólida y segura plataforma de almacenamiento. Debemos saber que lo anterior se debe a que el kernel es mucho más estable y se halla protegido a una escala mayor en comparación con el que encontramos en la plataforma Microsoft Windows. Esto es impoprtante, pues se encarga de impedir definitivamente el daño en cualquiera de los módulos que conforman el sistema.

> EXISTEN APLICACIONES ANTIVIRUS DESARROLLADAS PARA GNU/LINUX

Es interesante saber que los File Servers Linux incluyen, además, un completo conjunto de interfaces gráficas de configuración tanto local como remota protegidas en su totalidad contra amenazas en comparación con el sistema operativo de Microsoft. De esta forma encontramos que este tipo de sistemas se convierte en el número uno en cuanto a inmunidad y seguridad.

Figura 6. Ciertas compañías han desarrollado antivirus capaces de proteger la red corporativa basada en sistemas Linux y Unix.

Auditoría en servidores de archivo

Antes de entrar de lleno en el tema de auditoría en File Servers, vamos a analizar el término *auditoría* desde el punto de vista informático. De ese modo, podremos comprender el contexto del presente apartado.

> SE PODRÁN AUDITAR LOS EVENTOS QUE OCURREN DESPUÉS DE HABILITAR LA AUDITORÍA

El término **auditoría** es concebido en informática como un proceso de inspección, recopilación, agrupación y evaluación de evidencias, con el fin de determinar si un sistema de información es capaz de mantener la integridad de los datos basándose en el uso de los recursos existentes.

Si tratamos de readaptar dicha definición al ámbito de los File Servers, concluiremos que no se trata más que de un análisis detallado de la actividad sobre los archivos que se comparten en un servidor. La finalidad de esta tarea se centra básicamente en la protección y control de la información con el fin de evitar que esta pueda ser rastreada, modificada, robada e, incluso, eliminada.

Integridad de los archivos

Con seguridad, muchos nos hemos preguntado alguna vez qué hacer cuando notamos que los archivos almacenados en el servidor de archivos sorpresivamente han desaparecido o han sido modificado y, derivado de ello, quién es el causante de todo esto.

En estos casos, consideremos que el presunto causante del intercambio o eliminación de los datos es, sin duda, algún usuario de la red corporativa, el cual pudo haber intervenido en la manipulación de los archivos de manera accidental o de manera intencional. La forma óptima de mitigar estos daños es, desde luego, mediante una inspección minuciosa del servidor de archivos.

Los servidores modernos de Microsoft incluyen una funcionalidad conocida como **Event Viewer** (visor de eventos), que tiene como objetivo

mostrarnos un reporte de los sucesos presentes durante la ejecución de tareas en el servidor. A menudo, arroja notificaciones de error o datos relevantes, como posibles problemas de configuración o de seguridad.

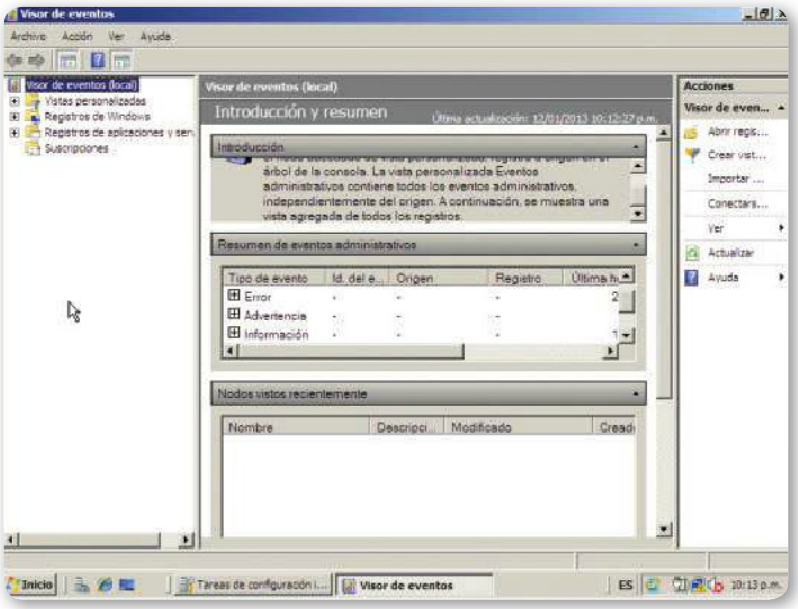


Figura 7. En la imagen, se muestra la interfaz del **Event Viewer** residente en servidores Windows.

Auditar eventos

Siempre hay que tener en cuenta que, en un server, solo se podrán auditar los eventos que ocurren después de habilitar la auditoría, de lo contrario no será posible saber quién ha manipulado con anterioridad algún archivo.

Antes de activar la auditoría del file server, debemos tener claros algunos conceptos:

> LOS SERVIDORES CUENTAN CON ENTORNOS PARA EDITAR DIRECTIVAS O ESTATUTOS

- **Políticas de seguridad locales del servidor**: por lo general, todo servidor cuenta con un entorno en el que se puede editar una serie de estatutos o directivas que el administrador tiene a bien asignar a su conjunto de objetos existentes, conocido como **Editor GPO** (**Group Policy Object Editor** o editor de objetos y políticas de grupo). Conseguiremos la entrada a dicha ventana para configurar algunas políticas o directivas desde

Windows Server de la siguiente forma: pulsamos **Inicio** y, luego, procedemos a teclear la palabra **gpedit.msc**. Notaremos que aparece una ventana con el nombre: **Editor de directivas de grupo local.**

- **Directivas de auditoría**: estas pueden estar enfocadas a diversas tareas, tales como: auditar sucesos de inicio de sesión de cuentas, auditar el acceso del servicio de directorio, auditar el acceso a objetos, auditar el uso de privilegios, etc. Por lo general, es posible encontrar estos estatutos en la ventana principal del **Editor de objetos y políticas de grupo**, en la opción **Directiva de auditoría**. Para más información sobre este apartado, recomendamos consultar la siguiente página de Microsoft: **www.microsoft.com/spain/technet/recursos/articulos/secmod50.mspx**.

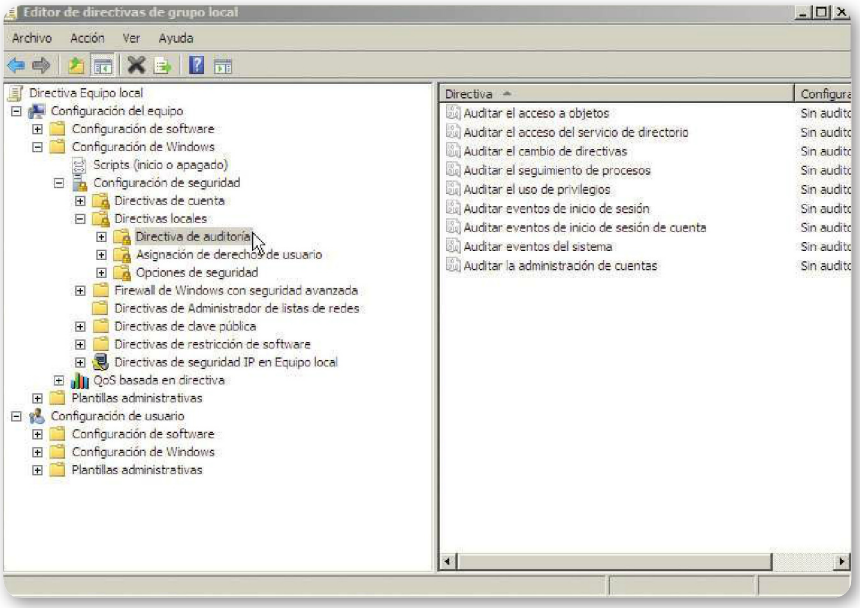


Figura 8. A través del editor de directivas de grupo local, es posible configurar las directivas de auditoría.

- **Valores de auditoría**: no olvidemos que, durante el proceso de auditoría en un file Server de Windows, es muy común encontrar patrones de vulnerabilidad, los cuales deben mitigarse para evitar amenazas o riesgos. Seamos siempre cautelosos a la hora de analizar el contexto, con el fin de evitar la omisión de evidencias que pudieran servirnos para determinar la causa de ciertos problemas. Las opciones para los valores de configuración comunes para la auditoría son: correcto, erróneo, sin auditoría.

Supervisión

Hoy por hoy, la supervisión de los diversos elementos que pertenecen a la estructura organizativa, la infraestructura de datos y los servicios de correo electrónico son los puntos más críticos en cuanto a seguridad informática se refiere, por lo que su alteración puede generar un sinnúmero de conflictos a nivel organizativo.

Consideremos que con el paso del tiempo, es habitual encontrar, en muchas organizaciones, un conjunto de serios inconvenientes derivados de la pérdida de datos, accesos no autorizados a la información personal, cambio de perfiles de los usuarios de la empresa, alteración en los correos, etc.

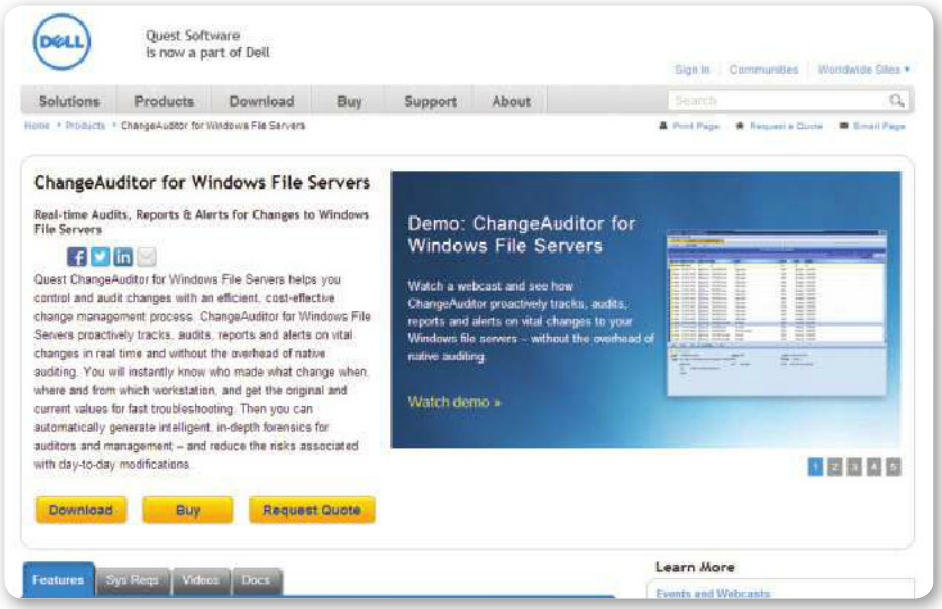


Figura 9. En el portal de **Quest** de Dell, podemos encontrar una demo de la utilidad **Quest ChangeAuditor**.

Por lo general, este tipo de aspectos justifican por sí mismos la necesidad de hacer uso de herramientas de seguridad como apoyo a las tareas de los administradores de seguridad de las empresas. A menudo, se requieren soluciones que aseguren un adecuado resguardo de la información y monitorización de procesos. Algunas utilerías de software (posibles de instalarse y configurarse de manera adicional en un file server) que pueden ser una excelente opción para auditar un servidor de archivos son: **File System Auditor**, **NetWrix File Server Change Reporter** y **Quest ChangeAuditor**.

Con el fin de establecer un marco de gestión en la seguridad de la información para cualquier tipo de compañía, se ha determinado un conjunto de reglas que no podemos echar por la borda. Sobre todo, las establecidas por la Organización Internacional para la Estandarización **ISO** (*International Organization for Standardization*) y la **IEC** (*International Electrotechnical Commission*). Hacemos una especial mención del estándar **ISO 27001**, el cual especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un **Sistema de Gestión de la Seguridad de la Información** (**SGSI**).

Servidor de impresión

Los servidores de impresión son también conocidos como **Print Servers**. Se trata de servidores especiales que, conectados a un dispositivo de impresión, permiten imprimir desde cualquier equipo que se encuentre enlazado a la red.

Los Print Servers a menudo son implementados para utilizarse tanto a nivel software como a nivel hardware según las necesidades de la red corporativa o de la misma compañía.

Los servidores de impresión a nivel hardware se clasifican en dos: internos y externos. El primero hace referencia al mecanismo que incluyen muchas impresoras actuales, capaces tanto de cumplir con tareas de gestión, control y automatización de impresiones, como de compartir archivos y recursos físicos en la red. Como es habitual, este tipo de dispositivos integra una conexión de red cableada o inalámbrica (Wi-Fi). Un Print Server externo, por lo general, consiste en

ORGANIZACIONES

La auditoría de File Servers es un requisito indispensable para las organizaciones basadas en servidores de archivos, que tienen a bien almacenar sus documentos y aplicaciones en la red corporativa. Los cambios no autorizados o accidentales en ficheros, como carpetas o recursos compartidos, pueden llegar a afectar significativamente a los usuarios y a la infraestructura misma, facilitando así el robo de datos y cediendo el paso a posibles amenazas de seguridad en el futuro.

un dispositivo que se conecta al puerto de la impresora (USB) con una salida hacia un dispositivo concentrador (switch o AP) residente en la red. Este tipo de equipos pueden ser alambrados o inalámbricos.

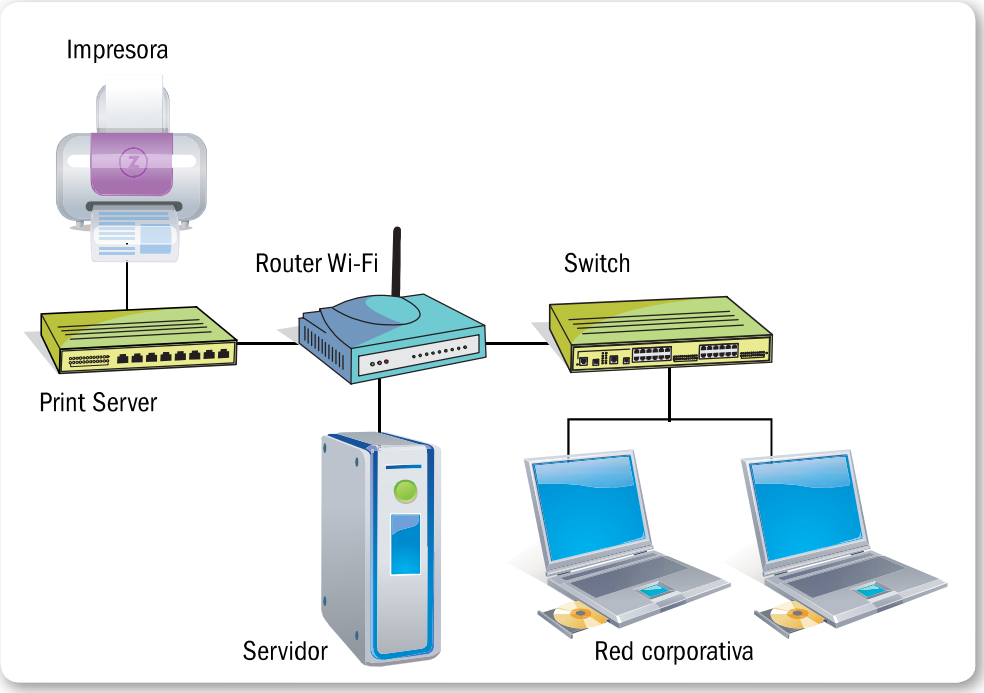


Figura 10. En el presente esquema se muestra la forma de conectar un servidor de impresión a la red de datos de una organización.

Características

Los servidores de impresión (cualquiera que sea su tipo) cumplen prácticamente con las mismas características, entre las cuales podemos destacar las que mencionamos a continuación:

- **Funcionan como un servidor dedicado**: cumple con un propósito específico, el de recibir datos procedentes de una red informática y prepararlos para su impresión a través de un dispositivo de impresión específico.
- **Hacen uso del protocolo IPP**: los servidores de impresión, por lo regular, incluyen una funcionalidad que permite la impresión a través de Internet mediante IPP (protocolo de impresión de Internet).
- **Hacen un resguardo por contraseña**: el Print Server nos permite encolar las impresiones que se envían al dispositivo de impresión y

guardarlas con una contraseña. Así evitaremos que otros usuarios impriman nuestros trabajos por error.

- **Son administrados desde una PC**: cualquier equipo en la red puede ser capaz de administrar un servidor de impresión. Para ello, es necesaria la instalación de un SO para servidores.
- **Servicio sin interrupción**: la red no debe presentar ningún problema por interrupción del servicio. A menudo, este se halla publicado en el directorio activo del servidor de red, lo que garantiza un uso accesible para todos los usuarios conectados.
- **Servicio de impresoras virtuales**: permite la configuración de impresoras virtuales, además del uso del servicio de manera remota.
- **Permite la asignación de políticas de seguridad**: se delegan permisos y prioridades de impresión a los usuarios de la red.

Ventajas

Los Print Servers a menudo cumplen con una serie de ventajas que los convierten en los preferidos de muchas compañías. A continuación, vamos a describir algunas de ellas:

- **Ahorro de espacio y costes de mantenimiento**: al no contar con una impresora por cada PC, existe un ahorro significativo en espacio, costos para el mantenimiento y, desde luego, la optimización de energía.
- **Rápida instalación**: no es necesario intervenir en procesos complejos para la puesta en marcha y configuración de la impresora en la red.
- **Flexibilidad**: con la implementación de Print Server, a menudo se evitan colas o retrasos en los procesos de impresión.

IMPRESIÓN DESDE WINDOWS 2008 SERVER

Existen dos herramientas principales que se pueden usar para administrar un servidor de impresión en Windows Server 2008: el Administrador del servidor y el Administrador de impresión. El primero es comúnmente usado para instalar la función del servidor: servicios de impresión, funciones opcionales y características. Desde aquí se muestran también los eventos relacionados con la impresión desde el **Event Viewer** (**visor de eventos**) del servidor. La opción Administración de impresión se administra únicamente en el servidor local.

- **Conexión heterogénea**: algunas compañías implementan redes heterogéneas, en las que conviven ambos medios de transmisión de datos. Las conexiones inalámbricas, en convivencia con las tecnologías Ethernet, facilitan la portabilidad y flexibilidad.
- **Manejo de puertos USB**: la elección de los modelos con puertos USB son una buena opción para el Print Server. Recomendamos el uso de modelos multipuerto para garantizar una futura expansión.

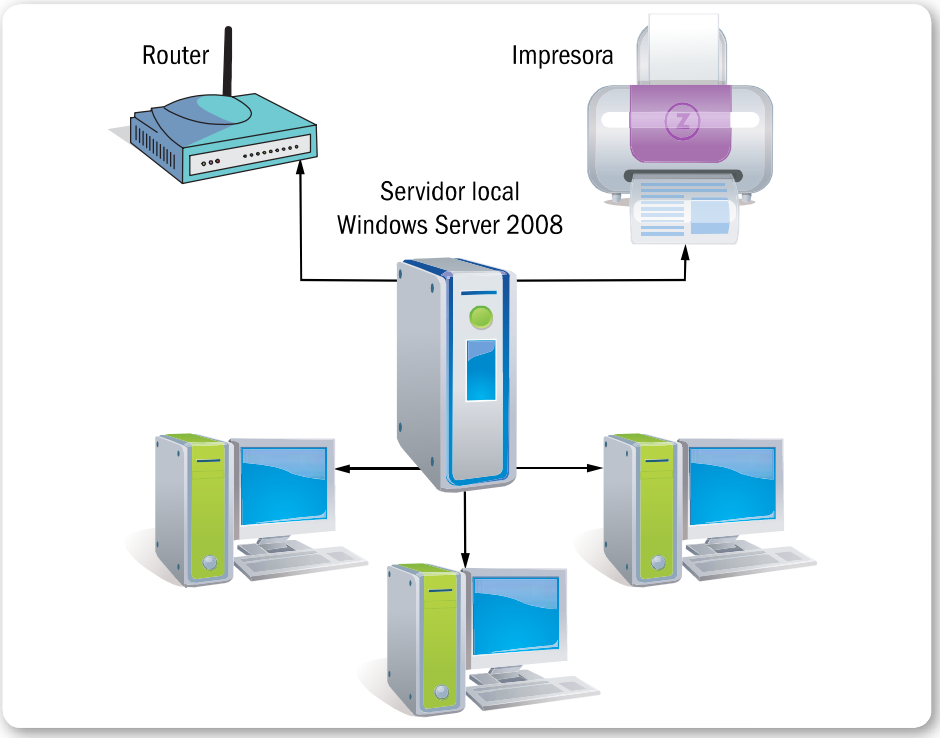


Figura 11. Los servidores locales hacen posible compartir los dispositivos de impresión en la red. Son preparados con un SO Server especial.

Servidores de impresión en Windows Server

Los Print Servers casi siempre son configurados sobre equipos que funcionan como servidores en la red de datos (servidores locales). Esto quiere decir que pueden ser gestionados desde cualquier computadora que se encuentre configurada con algún sistema operativo Server (como Windows Server o Linux servidor), aunque muchas compañías pequeñas hacen uso de Windows 7 y Windows 8.

A menudo, se recurre también a la ejecución de utilerías incluidas en prácticamente todos los Print Servers. Tomemos siempre en cuenta que este software tiene que ser configurado con suma cautela, ya que de no ser así, el sistema nos arrojará un conjunto de errores en el momento en que realicemos la prueba de conectividad.

WINDOWS SERVER DEBE EJECUTARSE EN UN EQUIPO CON CARACTERÍSTICAS ESPECIALES

Windows Server es un sistema operativo robusto que requiere ser ejecutado en un equipo con características especiales; por ejemplo recomendamos para realizar esta instalación un microprocesador de 2 GHz, 1 GB de memoria RAM, y un disco duro de, al menos, 40 GB de almacenamiento. Una vez completados dichos requerimientos, se sugiere la instalación del sistema operativo para la configuración del servidor de impresión.

La instalación y la configuración de un servidor de impresión bajo Windows 2008 Server son sencillas, solo hace falta tener paciencia y conocimientos elementales para ponerlas en marcha.

Servidores de impresión para Linux

Los servidores de impresión desarrollados para sistemas GNU/Linux poseen prácticamente las mismas ventajas que un Print Server para Windows, solo que son acreedores a un nivel de seguridad mayor por la plataforma en la que se ejecutan.

Los servidores Linux, a menudo, hacen uso de un conjunto de herramientas, mejor conocidas como CUPS (Sistema de Impresión Común de UNIX o Common Unix Printing System). Este sistema consiste

DESARROLLO DE CUPS

CUPS se comenzó a desarrollar por Michael Sweet en el año 1997. Es interesante considerar que las primeras versiones públicas beta de esta aplicación estuvieron a disposición del público en el año 1999. El diseño original del sistema de impresión CUPS se encargaba de utilizar el protocolo denominado **Line Printer Daemon** (LPD), pero debido a las limitaciones que existían en este protocolo y también a las incompatibilidades entre algunas marcas de impresoras, se optó por cambiar al protocolo **Internet Printing Protocol** (IPP).

en un nuevo estándar de impresión vigente en la mayoría de las distribuciones de GNU-Linux.

Debemos considerar que CUPS utiliza de igual modo el protocolo denominado IPP para efectuar la gestión de las tareas de impresión y también las colas de impresión a través de internet. De esta forma se encarga de proveer las instrucciones de impresión tradicionales ofrecidas por los sistemas de la familia Unix, además de entregar un completo soporte de operaciones bajo el Bloque de Mensajes del Servidor (SMB), protocolo que permite compartir archivos e impresoras desde un servidor.

> LOS SERVIDORES DE IMPRESIÓN SUELEN IMPLEMENTARSE A NIVEL SOFTWARE Y A NIVEL HARDWARE

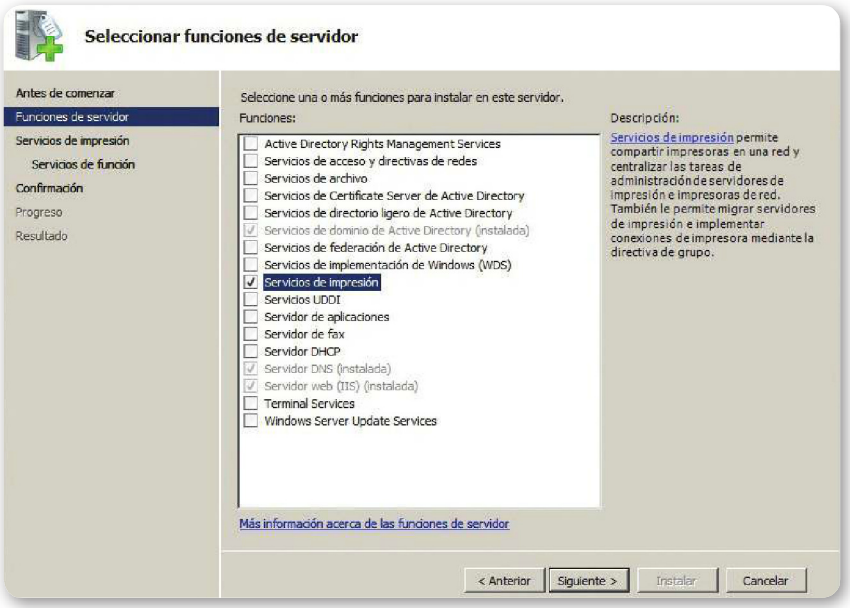


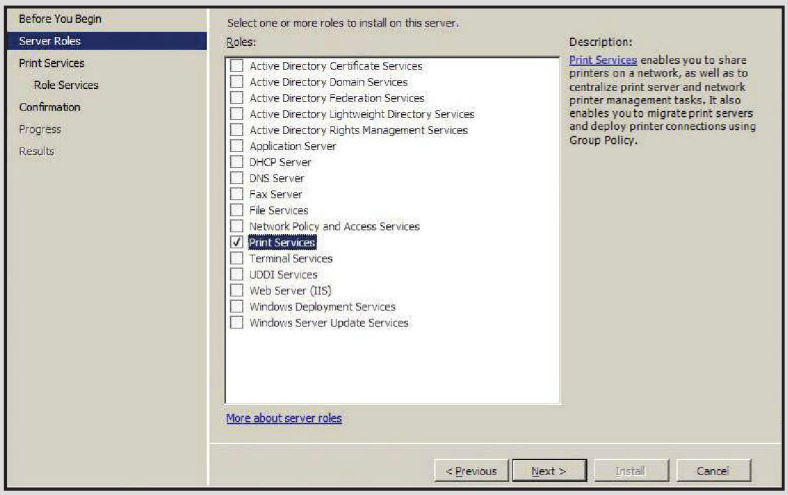
Figura 12. El rol **Servicios de impresión** debe darse de alta desde el **Administrador** del servidor de Windows 2008 para configurar un Print Server.

Administración de un Print Server en Windows

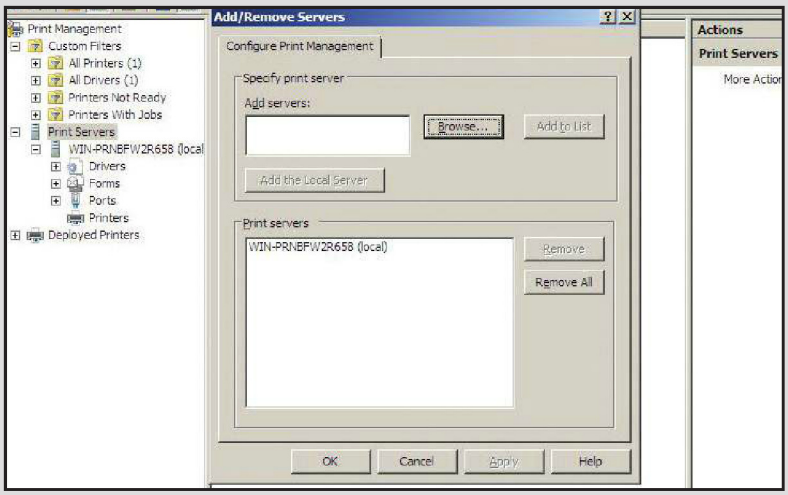
La administración de las impresoras en forma centralizada utilizando Windows Server debe ser realizada en forma cuidadosa. En este sentido, las recomendaciones que entregamos en el siguiente **Paso a paso** pueden facilitarnos la tarea.

PAP: SERVIDOR DE IMPRESIÓN EN WINDOWS

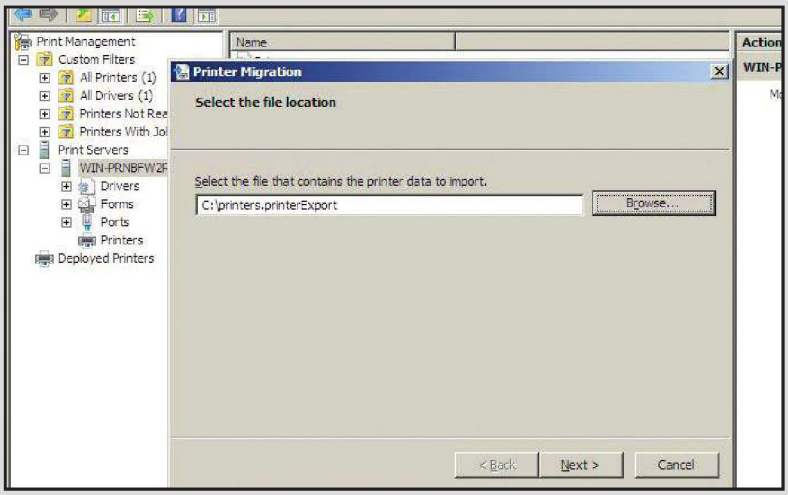
01 Puede instalar Print Management desde el Administrador de servidores, abra el asistente para agregar funciones y seleccione Print Services.



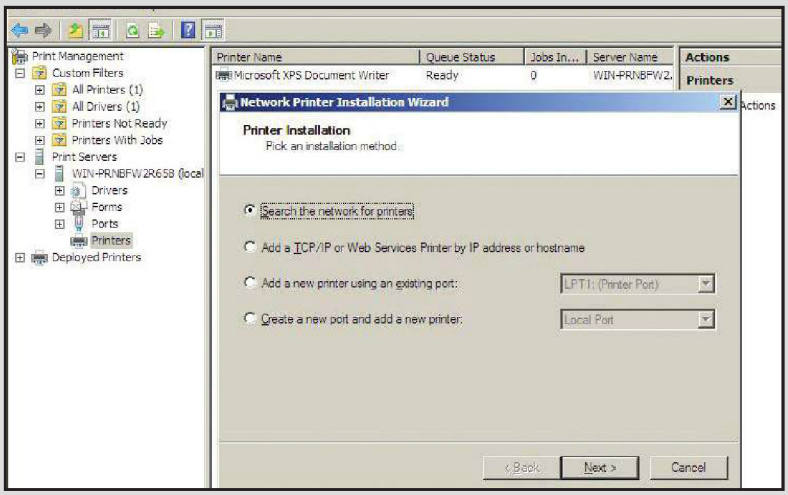
02 Para agregar Print Servers al Print Management vaya a Administrative Tools y, luego, a Print Management. Una vez allí, presione Add/Remove Servers, e ingrese el nombre adecuado. Presione Add to List.



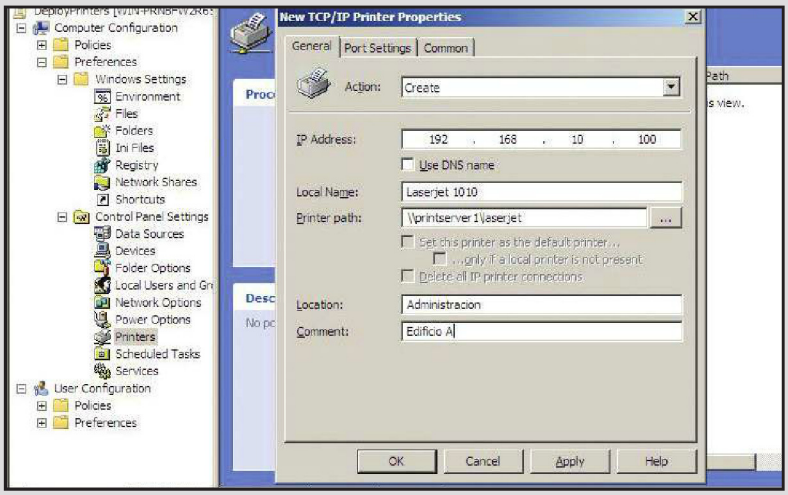
03 Para Windows Vista en adelante, es posible migrar las colas de impresión junto con las configuraciones de las impresoras de un servidor a otro utilizando el `Printer Migration Wizard` o el comando `Printbrm.exe`.



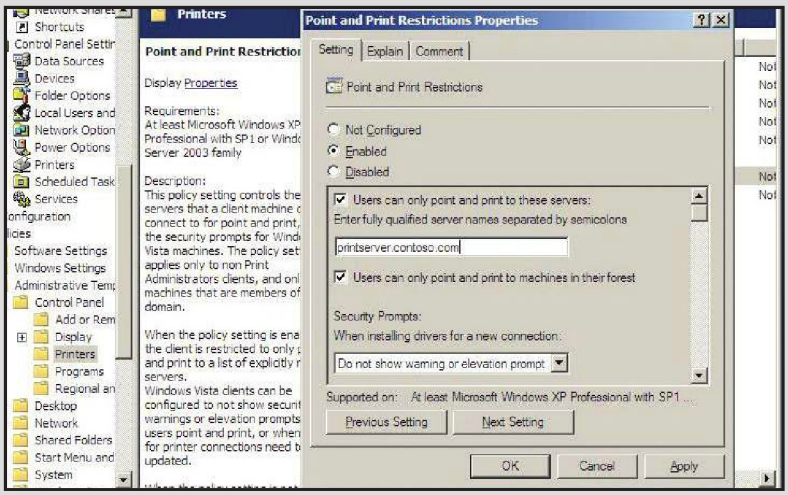
04 `Print Management` puede detectar las impresoras que se encuentran en la misma red. Presione Add `Printer` y haga clic en `Search the Network for Printers`. Es posible que solicite los drivers.



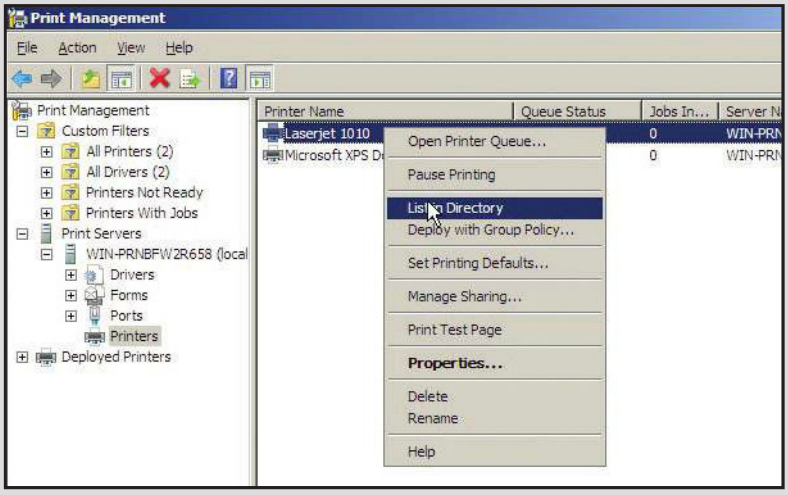
05 Una vez instaladas las impresoras en el Print Server, puede instalar en forma centralizada las impresoras en las estaciones de trabajo, utilizando `Group Policy`. Se requiere como mínimo Windows Server 2003 R2.



06 La configuración de Windows Vista en adelante permite a no administradores instalar solo drivers firmados. Para usar drivers no firmados, se debe configurar la opción `Point and Print Restrictions` en la GPO.



07 Listar las impresoras en `Active Directory Domain Services` (AD DS) facilita que los usuarios encuentren e instalen impresoras. Para listar las impresoras en AD DS, se debe buscar y seleccionar la impresora en la consola `Print Management` y hacer clic en `List in Directory`.



Tengamos en cuenta que si el firewall está activo, las impresoras no se mostrarán desde la red. En este caso, debemos agregar **Print Management** a la lista de excepciones en el firewall. Al instalar los drivers de las impresoras en el Print Server, debemos considerar las versiones de Windows en nuestra red.

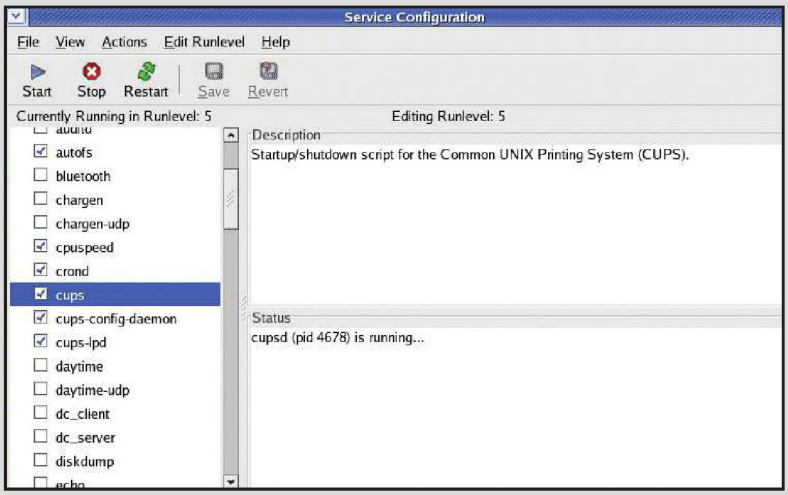
> CON EL FIREWALL ACTIVO LAS IMPRESORAS NO SE MOSTRARÁN EN LA RED

Administración de un Print Server en Linux

En esta oportunidad, conoceremos algunos consejos para instalar y administrar las impresoras de forma centralizada utilizando CUPS. Para administrar un servidor de impresión en GNU/Linux solo debemos seguir las indicaciones que mencionamos en el siguiente **Paso a paso**.

PAP: SERVIDOR DE IMPRESIÓN EN GNU/LINUX

01 Como primera acción, debe verificar que posea el servicio CUPS instalado y habilitado en el sistema; use el comando `/etc/init.d/cups start`.



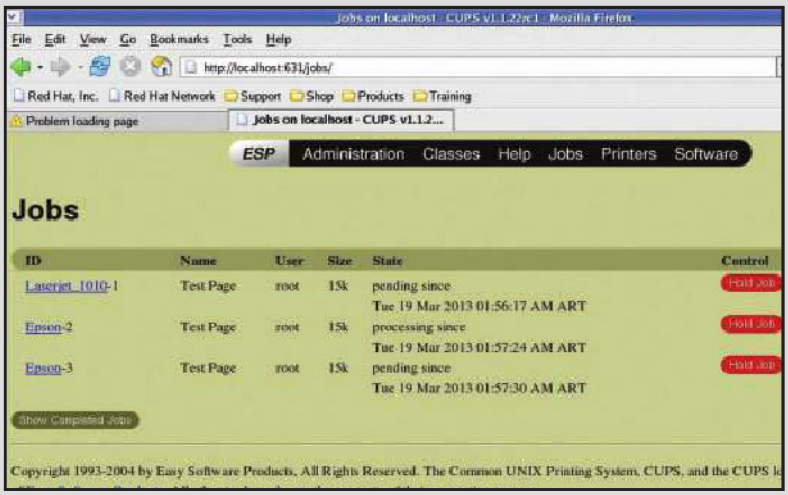
02 En caso de contar con una infraestructura Active Directory, es recomendable que Samba se convierta en un miembro, utilizando el modo de autenticación ADS. La hora debe estar sincronizada con Active Directory usando NTP.

03

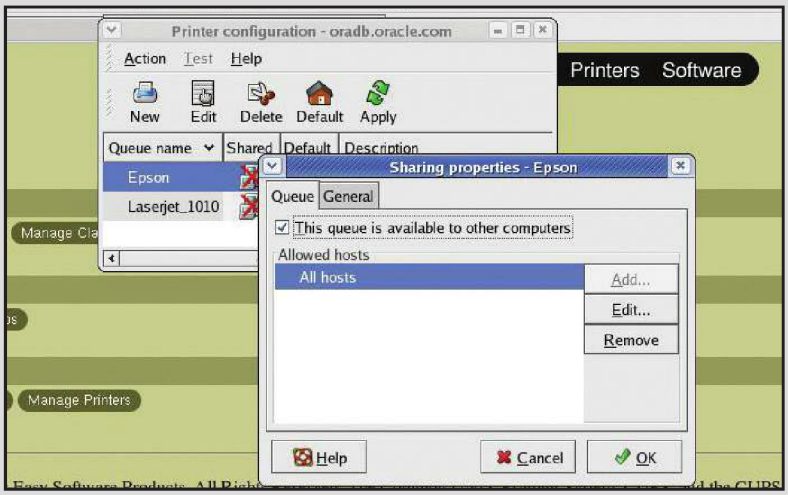
Para acceder a CUPS mediante un browser, ingrese a **http://localhost:631**. Allí podrá crear y testear las impresoras definidas. CUPS posee gran cantidad de drivers. Desde **www.cups.org/ppd.php**, es posible consultar el listado.

04

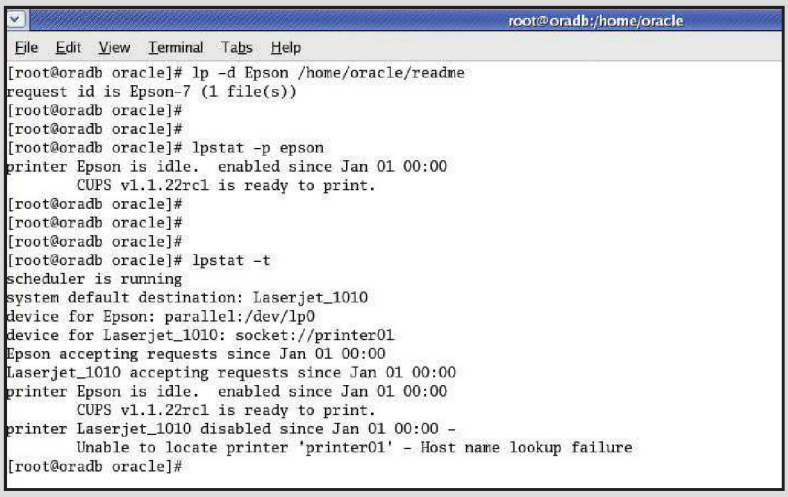
Es posible visualizar los trabajos activos y suspenderlos o cancelarlos. También se puede consultar la lista de los trabajos finalizados. Desde la consola, es posible consultar los logs en el directorio `/var/log/cups`.



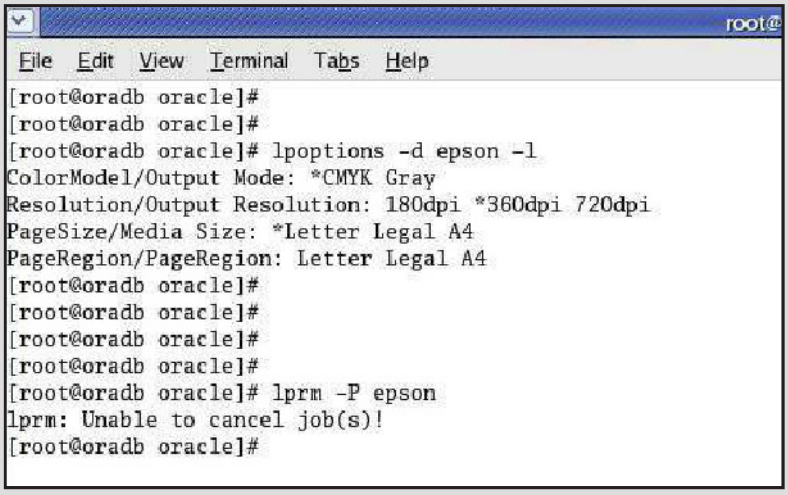
05 Las impresoras agregadas en CUPS no se comparten, por lo que es necesario habilitar esta posibilidad. En RedHat, se debe ejecutar `system-config-printer` y, luego, tildar `This queue is available to other computers`.



06 Para imprimir desde la línea de comandos, es posible utilizar el comando `lp -d Nombre Queue archivo`. Por ejemplo, para imprimir el archivo readme, en la impresora Epson, escribimos lo siguiente: `lp -d Epson /home/Oracle/readme`.



07 El comando `lpoptions` permite visualizar las características principales de cada impresora. Si direcciona la salida a un archivo, podrá genera un inventario de ellas. Por otra parte, gracias al comando `lprm -P impresora`, podrá cancelar los trabajos activos que desee anular.



Es necesario recordar que para poder acceder en forma remota a CUPS, tendremos que habilitar el puerto **631** (TCP y UDP) en el firewall local. Para realizar esta acción, en la distribución Red Hat ejecutamos el comando **system-config-firewall** en un terminal de comandos y se abrirá la interfaz de configuración gráfica. Debemos además habilitar los puertos requeridos por Samba (Kerberos, netbios, etc.).

PRINT MANAGER PLUS

El software **Print Manager Plus** para Microsoft Windows se licencia por Print Server. El producto no realiza instalaciones especiales, ya que utiliza la información provista por el subsistema de impresión de Windows. Soporta cluster de Windows y Citrix. Esta aplicación permite almacenar la información en una base de datos centralizada cada vez que una impresión se realiza, y mantiene el registro de las propiedades: fecha y hora de impresión, usuario, nombre del documento, páginas, copias y el costo de cada impresión.

Print Servers y políticas de uso

Los usuarios y las empresas cada vez más se preocupan por el consumo de papel gracias a la puesta en práctica de iniciativas de Responsabilidad Social Empresaria (RSE), pero también debido a los costos que implica el papel, el tóner y otros insumos requeridos por las impresoras. Con la popularización de las tablets y los e-readers todo tiende a digitalizarse, sin embargo, aún así es necesario contar con información sobre el uso de las impresoras. Existen diversas formas de controlar la utilización según las características de nuestro equipamiento.

Impresiones

Las impresiones realizadas por los usuarios pueden ser registradas en el eventlog, si así se lo ha definido en cada impresora. Una vez registrados los eventos, es posible generar reportes extrayendo la información deseada. El informe típico por extraer indica la cantidad de páginas impresas por usuario o impresora. Los reportes pueden generarse simplemente filtrando en forma manual los eventos deseados o mediante scripts. Es posible generar scripts WMI que utilizan el objeto Win32_Printer o mediante **Powershell**.

Los **Group Policy Objects** (**GPO**) generados a nivel de dominio permiten hacer deploy de impresoras, definir restricciones y propiedades en los equipos cliente. Por ejemplo, es posible impedir el agregado o borrado manual de las impresoras. También, se puede definir soporte para impresión a través de la Web, publicación en Active Directory, URL de soporte para las impresoras, entre otras opciones.

ANTIVIRUS PARA GNU/LINUX

eScan para Linux es un software antivirus confiable, utilizado a menudo en estaciones de trabajo y servidores que se ejecutan en GNU/Linux. Ofrece una completa y segura solución de seguridad capaz de detectar y eliminar más de 12.000 virus, troyanos y amenazas.

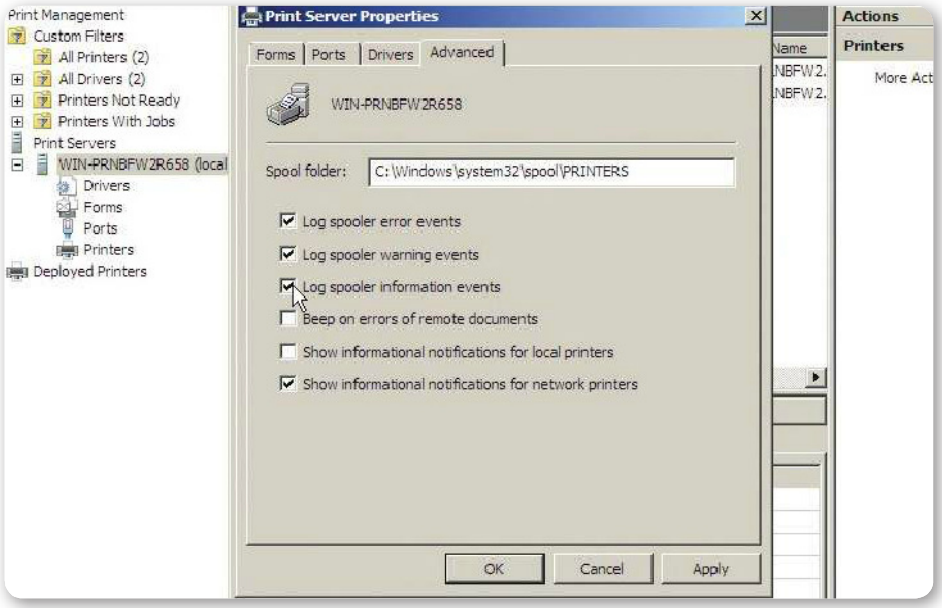


Figura 13. Configuración de la consola **Print Manager** de **Windows Server 2008 R2** para guardar todos los eventos del spool.

GNU/Linux

En la plataforma Linux, el estándar actual para Print Server es CUPS (*Common Unix Printing System*). Desarrollado originalmente por Michael Sweet y, luego, adquirido por Apple, se ejecuta en sistemas Unix, BSD y más. Permite una variedad de esquemas de contabilización, por tamaño, por páginas, y soporta el uso de cuotas. Que CUPS se ejecute en un servidor Linux no implica que los usuarios también deban usar Linux; es posible usar CUPS como Print Server de Windows sin mayor complejidad, solo debemos configurar Samba para exportar impresoras mediante **smb.conf.**

> EN SISTEMAS LINUX, EL ESTÁNDAR ACTUAL PARA IMPLEMENTAR PRINT SERVER ES CUPS

El rol de Samba en el proceso de impresión consiste en tomar el archivo por imprimir y enviarlo a CUPS. Todo lo que Samba informa respecto a impresoras lo hace a través de CUPS. Pero debemos tener en cuenta que los clientes también pueden imprimir de manera directa en CUPS utilizando el protocolo IPP (*Internet Printing Protocol*), por esto es importante considerar que cualquier control implementado en Samba puede ser salteado si se imprime directamente en CUPS.

CUPS PUEDE INTEGRARSE CON SISTEMAS UNIX, LINUX, MAC OS X Y WINDOWS

Para evitar que usuarios anónimos impriman, debemos indicar **guest ok = no** en la sección **[printers]** de Samba; de esta manera, podremos identificar a quienes imprimen y llevar el control. CUPS genera logs por cada página que se imprime en el archivo **page_log**. El logging por página solo está disponible para los drivers que soportan accounting. Casi siempre, los drivers PostScript y CUPS soportan la contabilización de impresión. Las queues raw, por lo general, no permiten el accounting de impresión.

Al imprimir, CUPS, y no Samba, es el encargado de hacer el trabajo de accounting. Es posible setear una cuota en CUPS de la siguiente manera:

```
lpadmin -p Impresora01 -o job-cuota-period=604800 -o job-page-limit=100
job-k-limit=500000
```

Esto establece tres opciones de la **Impresora01**. La primera es el período de la cuota, que son 604,800 segundos (1 semana). La segunda es el límite de páginas en ese período, 100 páginas. Y, por último, el tamaño de impresión se define en 500 MB. Para verificar la cuota ingresada a una impresora, debemos visualizar el archivo **/etc/cups/printers.conf**. La limitación que presenta esta cuota es que no puede definirse por usuario, sino solamente por impresora.

Cada impresión realizada se almacena en el archivo **/var/log/cups/page.log** y tiene este formato:

```
Impresora01755 juan [26/Feb/2013:15:02:27 -0500] 1 1 - localhost
smbprn.0019.FWqosE
```

PYKOTA

PyKota posee varios proyectos para control y contabilización de las impresiones realizadas por los usuarios. Tea4CUPS es un wrapper para el backend de CUPS, que permite reemplazar o complementar las funcionalidades de CUPS. Algunas de las funcionalidades de Tea4CUPS son: automatizar el archivo de las impresiones en PDF, impedir impresión de trabajos duplicados, crear soluciones de contabilización con rapidez. PyKota soporta cualquier impresora física o virtual.

Los campos son: **nombre de la impresora**, **número de trabajo**, **usuario**, **fecha**, **número de páginas impresas**, **número de copias solicitadas.**

Debemos tener en cuenta que es posible integrar Samba con un Dominio de Active Directory, de forma que sea posible efectuar la autenticación a los usuarios que se conectan para imprimir o utilizar carpetas compartidas. De esta manera, no será necesario que generemos un usuario especial en el sistema GNU/Linux solo para imprimir o acceder a los archivos.

Herramientas propias

Dispositivos específicos pueden tener sus propias herramientas para control de impresiones. Por ejemplo, Xerox dispone del software **Xerox Standing Accounting** (**XSA**) embebido en sus dispositivos de alta gama (**ColorQube**, **Phaser** y **WorkCentre**). Para utilizar este software, basta con acceder mediante un browser a la IP de la impresora. Es posible generar usuarios individuales y definir, para cada uno, cuotas para impresiones color, blanco y negro, escaneos y faxes. Si se habilita esta función en la impresora, cada usuario deberá ingresar su nombre de usuario y contraseña en el driver a fin de poder imprimir en ella.

Figura 14. Impresora **Xerox WorkCentre 7346** con soporte para **Xerox Standing Accounting** (XSA), que registra detalladamente la utilización del equipo.

Por su parte, Hewlett-Packard posee la solución **HP Access Control Printing Solutions**, que permite autenticar los usuarios que utilizan las impresoras. De esta manera, impide que usuarios no autorizados impriman material confidencial o restringido. También, es posible llevar un control de qué se imprime y quién lo hace. De esta forma, es posible analizar el uso de los consumibles y el comportamiento de los usuarios.

La firma **Papercut** ofrece un producto centrado principalmente en el control de impresiones y sus costos asociados. Permite monitorear el uso de las impresoras, el consumo de papel, medir el impacto ambiental, definir cuotas y generar todo tipo de reportes. Las aplicaciones poseen soporte multiplataforma (Windows, Mac, Linux y Novell).

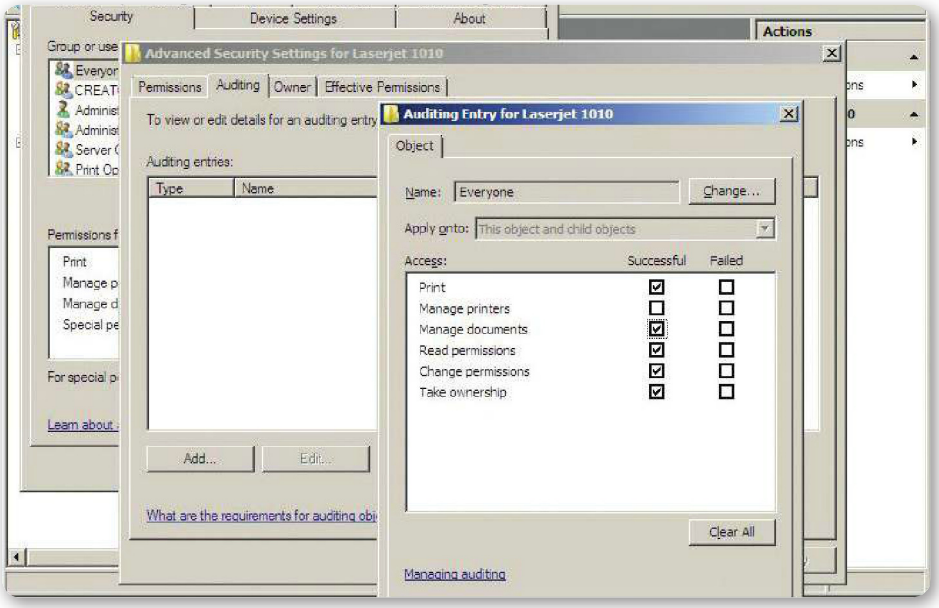


Figura 15. Configuración de seguridad sobre una impresora. Desde la solapa **Security**, con el botón **Advanced** es posible definir los eventos por auditar.

XEROX Y MCAFEE

Xerox y **McAfee** desarrollaron una serie de multifunciones que protegen contra el malware y los virus. El software McAfee embebido posee un sistema de filtrado que permite que solo los programas autorizados se conecten con la impresora. Cuando una multifunción recibe datos y los procesa para imprimir, copiar, escanear o faxear, se vuelve vulnerable a los ataques de malware.

Seguridad en Print Servers

Para lograr una efectiva separación de roles, los permisos para los administradores y para los usuarios deben ser otorgados mediante grupos. Los administradores deben ser los únicos con privilegios para administrar las impresoras y el Print Server. Las impresiones realizadas por los usuarios pueden ser registradas en el **Visor de eventos**, si así se lo ha definido en cada impresora. De esta manera, se puede auditar el uso de las impresoras y de los privilegios.

Figura 16. Interfaz de administración CUPS. Puede ser accedida remotamente utilizando un web browser.

Existe gran cantidad de malware embebido en drivers de impresoras, por lo que controlarlos es crucial en un entorno corporativo. De esta manera, se supervisa qué impresoras y drivers se instalarán en el equipo. Esto nos permite establecer conexiones con Print Servers del bosque, pero un administrador puede agregar servidores adicionales o deshabilitar este seteo para conectarse a cualquier servidor.

Dado el caso que nuestro servidor esté expuesto en la red ya sea interna o de cara a Internet mediante IPP (*Internet Printing Protocol*), es aconsejable restringir mediante un firewall el acceso a los puertos de administración. El puerto utilizado para imprimir es TCP 9100, pero,

dependiendo del sistema operativo que utilicemos, es posible que se necesiten otros puertos adicionales para autenticación u otras finalidades.

Herramientas de seguridad

Dispositivos específicos pueden tener sus propias herramientas de seguridad. Por ejemplo, Xerox dispone de una serie de funcionalidades de seguridad como ser:

- **Sobrescritura de datos**: en forma periódica se escribe el disco con sucesivas pasadas de forma de evitar que el contenido almacenado en el disco pueda ser copiado.
- **Encriptación de datos**: los datos en tránsito pueden ser encriptados utilizando SSL o IPSec.
- **Control de acceso**: las impresoras multifunción pueden ser integradas con lectores de tarjetas de proximidad para autenticar a los usuarios.
- **Xrox Standard Accounting (XSA)**: permite control y logueo granular de las impresiones y copias realizadas por un usuario.
- **ConnectKey**: integra la suite de seguridad de McAfee para reducir las amenazas del malware.

Figura 17. Autenticación biométrica para impresoras **HP LaserJet**. Permite limitar el uso del dispositivo a usuarios habilitados.

Contraseñas

Las impresoras y Print Servers que poseen interfaces de administración deben ser protegidas con contraseñas fuertes para evitar el acceso no autorizado o el snifeo de las impresiones generadas.

Es recomendable deshabilitar los protocolos no utilizados en nuestra red, por ejemplo, IPX/SPX, DLC o EtherTalk. También se aconseja deshabilitar las funcionalidades de administración no utilizadas, como ser FTP, Service Location Protocol, SNMP o IPP entre otros.

Hewlett-Packard posee la solución HP Access Control Printing Solutions, que permite autenticar los usuarios que utilizan las impresoras. Por esta vía, se controlan las impresiones de los usuarios. Además, permite realizar control sobre lo que se imprime y quien lo imprime.

> ES NECESARIO QUE CONSIDEREMOS ENCRIPTAR LOS DATOS QUE SE IMPRIMEN

Los Print Servers y las impresoras utilizan gran cantidad de software y, como todo, debe ser actualizado con los últimos firmware disponibles. Por ejemplo, el firmware de los Jetdirects de HP puede ser actualizado utilizando **Download Manager** o mediante el software de **HP Web Jetadmin**.

Figura 18. Print Server Wireless con soporte para WPA. Transmite la información sobre una conexión Wi-Fi robusta y segura.

Auditoría de Print Servers

La auditoría permite controlar el uso de las impresoras. Las principales finalidades por las que podemos estar interesados en habilitar la auditoría de impresoras son: controlar y supervisar los gastos de impresión y analizar lo que se imprime, de manera de detectar posibles brechas en la confidencialidad de la información sensible. Es posible definir, a partir de grupos de usuarios, qué acciones deben ser registradas para cada impresora.

Windows

En Windows, podemos almacenar, visualizar y publicar información en varios formatos utilizando el Event Viewer. Para definir las acciones por auditar, se deben modificar las propiedades de cada impresora.

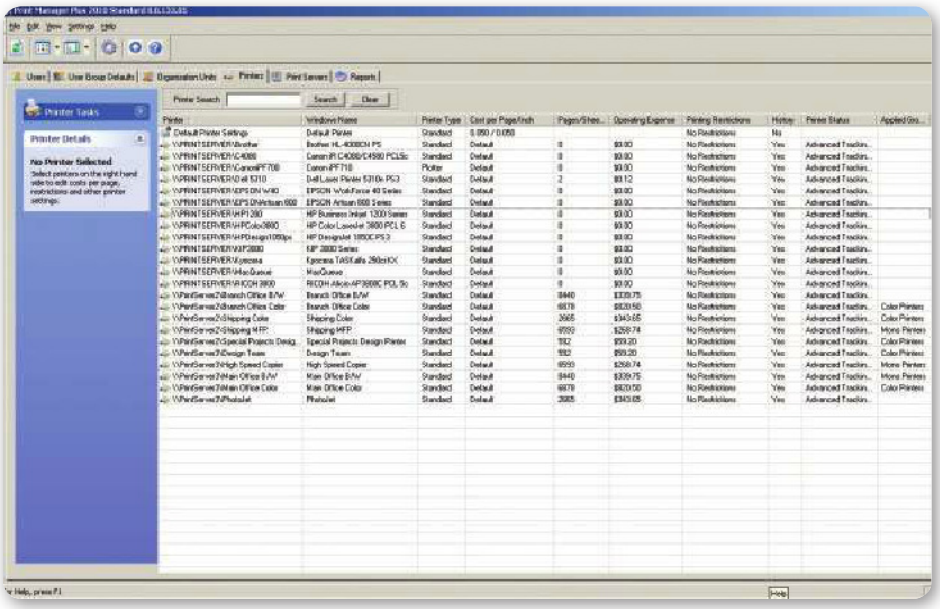


Figura 19. Información de costo detallada provista por el complemento **Print Manager Plus**.

Para agregar, remover o ver las entradas de auditoría de una impresora, es necesario acceder a sus **Propiedades**, vamos a la solapa **Security** (**Seguridad**) y luego hacer clic en **Advanced** (**Avanzado**).

Hacemos clic en la solapa **Auditing** (**Auditoría**). Si no está visible,

significa que se carece de permisos de Administrador para el servidor, y no es posible continuar hasta no contar con estos privilegios.

Utilizamos el botón **Add and Remove** (**Agregar y quitar**) para definir un nombre de usuario o grupos que serán auditados. En la pantalla **Audit Entry**, es posible especificar si la auditoría se realizará por impresora, por documento o por ambos.

En la sección **Access**, seleccionamos los eventos que se auditarán para los usuarios o grupos definidos. Para finalizar y guardar la configuración, presionamos **OK.**

Cada objeto posee un set de información de seguridad relacionado. Parte del descriptor de seguridad especifica los usuarios o grupos con permisos para acceder al objeto. Esta parte es conocida como **DACL** (*Discretionary Access Control List*).

Un descriptor de seguridad para un objeto contiene información de auditoría. Esta información es conocida como **SACL** (*System Access Control List*). Específicamente, SACL define lo siguiente:

- El grupo o usuario por auditar cuando el objeto es accedido.
- Las operaciones que serán auditadas por cada grupo o usuario.
- El atributo de éxito o fracaso para ejecutar cada evento, basado en el permiso otorgado (DACL).

Debemos notar que el log de eventos puede llenarse de eventos inútiles si tildamos todas las opciones. Debemos seleccionar solo los eventos que arrojen información relevante según nuestras necesidades.

Es importante tener en cuenta para qué funciones debe estar habilitada la **Auditoría de Acceso a Objetos** (*Audit Object Access*) en las políticas de seguridad local.

RESUMEN

En este capítulo pudimos conocer las características y las funciones que desempeña un servidor de archivos o File Server, además aprendimos a administrarlo en un sistema Windows y también en una distribución GNU/Linux. También vimos las opciones de seguridad y las alternativas de auditoría que es necesario tener en cuenta. Para continuar analizamos el funcionamiento de un servidor de impresión, la forma correcta de administrarlo, vimos cómo aumentar su nivel de seguridad y realizar tareas de auditoría.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice a un servidor de archivos.
2. ¿Qué es SMB?
3. Mencione las características de CIFS.
4. ¿Qué es NFS?
5. Enumere las ventajas de un servidor de archivos.
6. Describa las soluciones de seguridad para un servidor de archivos.
7. ¿Qué es un servidor de impresión?
8. Mencione las ventajas de un servidor de impresión.
9. ¿Cómo podemos administrar un servidor de impresión en GNU/Linux?
10. ¿Qué debemos tener en cuenta para auditar un servidor de impresión?

EJERCICIOS PRÁCTICOS

1. Administre un servidor de archivos en Windows.
2. Administre un servidor de archivos en GNU/Linux.
3. Audite un servidor de archivos.
4. Administre un servidor de impresión en Windows.
5. Audite un servidor de impresión.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*07

Servidores adicionales

En este capítulo revisaremos diversas alternativas de servidores adicionales, conoceremos el funcionamiento de los servidores de backup y entregaremos algunas recomendaciones de aplicaciones y consejos para administrarlos. Veremos el funcionamiento de los servidores de actualización y de los servidores de antivirus. También aprenderemos a instalar y a configurar un servidor proxy.

Servidor de backup

A medida que nuestra plataforma tecnológica crece, debemos contar con una estrategia de copia de seguridad que acompañe el crecimiento.

Existe una gran cantidad de eventos que pueden afectar la continuidad de los sistemas de nuestra red y requieren que recuperemos información desde una copia de seguridad, desde errores humanos, problemas de integridad de sistemas operativos y bases de datos, hasta fallas físicas en nuestros servidores y desastres naturales, como inundaciones o incendios.

Cuando los sistemas implementados en nuestra red se vuelven críticos, la estrategia de copia de seguridad juega un papel fundamental para poder recuperarnos en el menor tiempo posible ante algún evento que afecte la continuidad de nuestros servicios.

Los servidores de backup son los equipos a los que asignamos el rol de implementar nuestra estrategia de copias de seguridad.

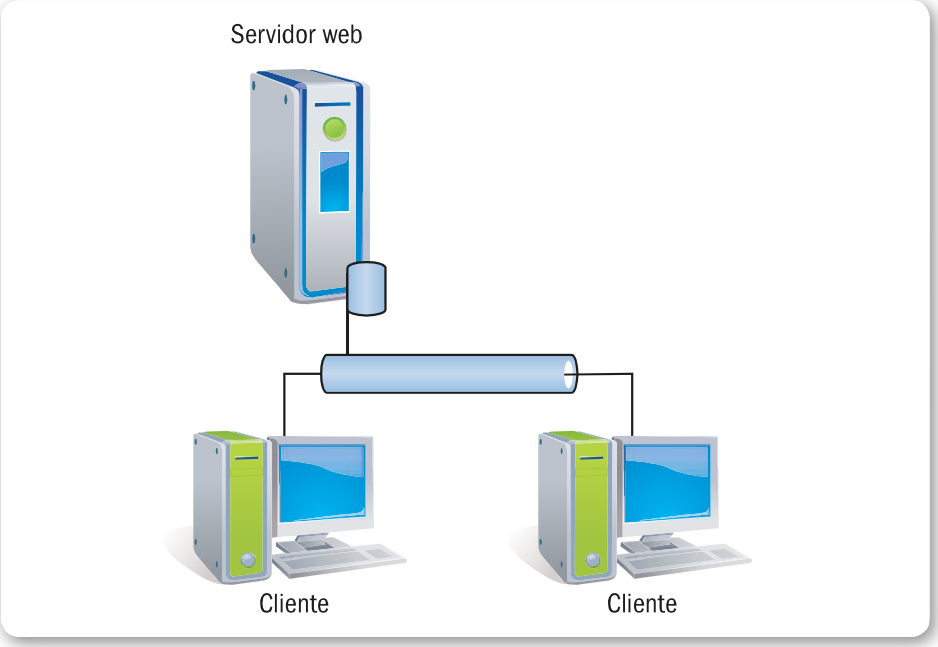


Figura 1. Una red con un solo servidor, en la que se realiza el backup en forma manual, almacenado de manera local.

La evolución de la estrategia de copias de seguridad a medida que nuestra infraestructura tecnológica crece se puede resumir en tres etapas:

Primera etapa: copias manuales y locales

Si el número de servidores con los que contamos lo permite y cuando los servicios que ofrecemos no tienen una criticidad relevante para nuestra red, es suficiente con realizar una copia de nuestros sistemas cuando lo consideremos necesario; por ejemplo, cada vez que se realiza una modificación importante en nuestro sitio web o sobre nuestra base de datos, llevamos a cabo una copia de respaldo en forma manual, la cual almacenamos en el mismo servidor.

> LAS COPIAS MANUALES PUEDEN REALIZARSE CUANDO LO CONSIDEREMOS NECESARIO

Segunda etapa: copias locales y automáticas

Cuando la cantidad de servicios y servidores en nuestra red aumenta, la estrategia de copias de seguridad realizadas en forma manual deja de ser la óptima, ya que debemos ingresar a cada servidor en el momento en que necesitamos realizar una copia de respaldo.

Para sobrellevar los inconvenientes de la administración del backup en forma manual, ejecutamos las tareas de copia de seguridad mediante el administrador de tareas del sistema operativo; un ejemplo sería realizar el backup mediante archivos de proceso por lotes (.BAT) desde el administrador de tareas de Windows en todos los servidores en los que necesitemos realizar copias de respaldo.

Tercera etapa: copias centralizadas y automáticas

A medida que aumenta la cantidad de servidores en nuestra red y los servicios que brindamos incrementan su criticidad, es necesario contar con una estrategia de backup automática y centralizada; en los casos en los que tengamos que prever recuperaciones ante desastres naturales, necesitamos incluso que las copias de respaldo se almacenen

en medios extraíbles, como cintas de backup, las que debemos resguardar en un sitio distinto del que aloja a nuestros servidores.

Al llegar a esta etapa, necesitamos contar en nuestra red con equipos dedicados a implementar nuestra estrategia de backup; a estos equipos los denominamos **servidores de backup**.

Para que nuestro servidor de backup lleve a cabo de forma óptima la estrategia de copias de seguridad, debe implementar al menos cuatro funciones básicas:

Concentrar las copias de seguridad

Nuestro servidor de backup debe ser el centro especializado en recibir las copias de seguridad de los distintos servidores la red, los cuales pueden estar ubicados en diferentes puntos geográficos.

Para implementar esta funcionalidad, debemos instalar, en cada servidor de nuestra red, el software necesario para integrarlo a nuestra estrategia de backup y, de ese modo, poder extraer la información que necesitamos copiar.

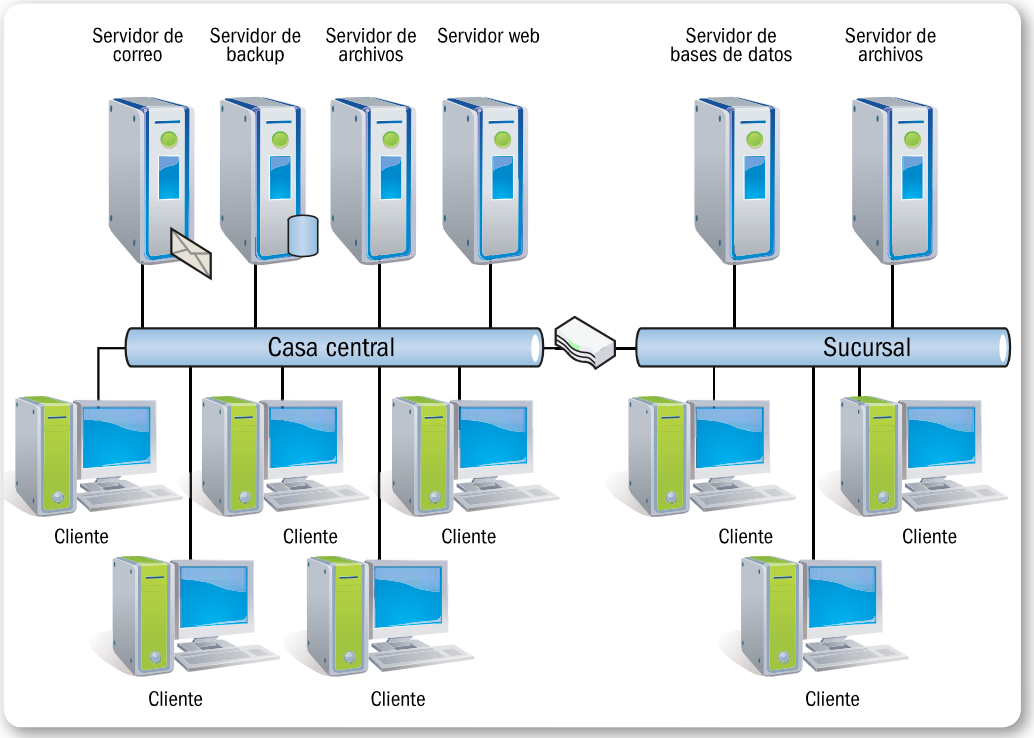


Figura 2. Esta es una red con dos sitios, en la cual se implementó la estrategia de copia de seguridad centralizada en un servidor de backup.

Almacenar

A medida que nuestro servidor de backup recibe las copias de seguridad desde los distintos orígenes, debe almacenarla en los medios que correspondan; para esto tiene que agrupar los medios según la estrategia definida. Por ejemplo, podemos definir un grupo de cintas de backup para cada día de la semana, según esta configuración nuestro servidor de backup debe solicitarnos la cinta de acuerdo al día en el que se ejecutan las copias de respaldo.

Catalogar las copias de seguridad

En el momento menos pensado, tendremos que recurrir a nuestras copias de seguridad. En ese instante, lo que menos deseamos es tener incertidumbre acerca del medio en que se encuentra la información que necesitamos recuperar.

El servidor de backup debe llevar un catálogo detallado en el que se registre qué información se halla en cada medio de almacenamiento y a qué fecha corresponde; de ese modo nos permite localizar la información que necesitamos restaurar en el menor tiempo posible.

> LOS SERVIDORES DE BACKUP IMPLEMENTAN LAS COPIAS DE SEGURIDAD

Dirigir la ejecución del proceso

Nuestra red puede contar con múltiples sitios y una gran cantidad de servidores con sistemas operativos distintos.

Es necesario que nuestro servidor de backup coordine las tareas de copias de respaldo entre los distintos orígenes de datos y los

HARDWARE PARA REALIZAR BACKUP

Existen muchas opciones para nuestro servidor de backup y los dispositivos que usaremos para almacenar la información. En el caso del hardware para el servidor, debemos tener en cuenta principalmente la capacidad de los discos duros si necesitamos realizar copias a disco; si deseamos usar cintas, existen dispositivos para grabación que nos permiten usar una cinta a la vez.

dispositivos que tienen la finalidad de transferir las copias a los medios de almacenamiento correspondientes.

Para definir los parámetros que necesita nuestro servidor de backup para coordinar las tareas de copia de seguridad en nuestra red, es necesario que configuremos la programación de las tareas, indicando al menos la periodicidad en las que se realizan las copias, el tipo de backup y el listado de la información que se deberá transferir desde cada servidor a los medios de almacenamiento.

Cuando nuestra infraestructura pasa a tener una cantidad importante de servicios, servidores y PCs, y aumentan las exigencias relacionadas con la disponibilidad de los servicios que brindamos, es imprescindible que contemos con equipos especializados para implementar nuestra estrategia de backup, la que nos permitirá recuperar los servicios en el caso de que nos ocurra algún evento no deseado.

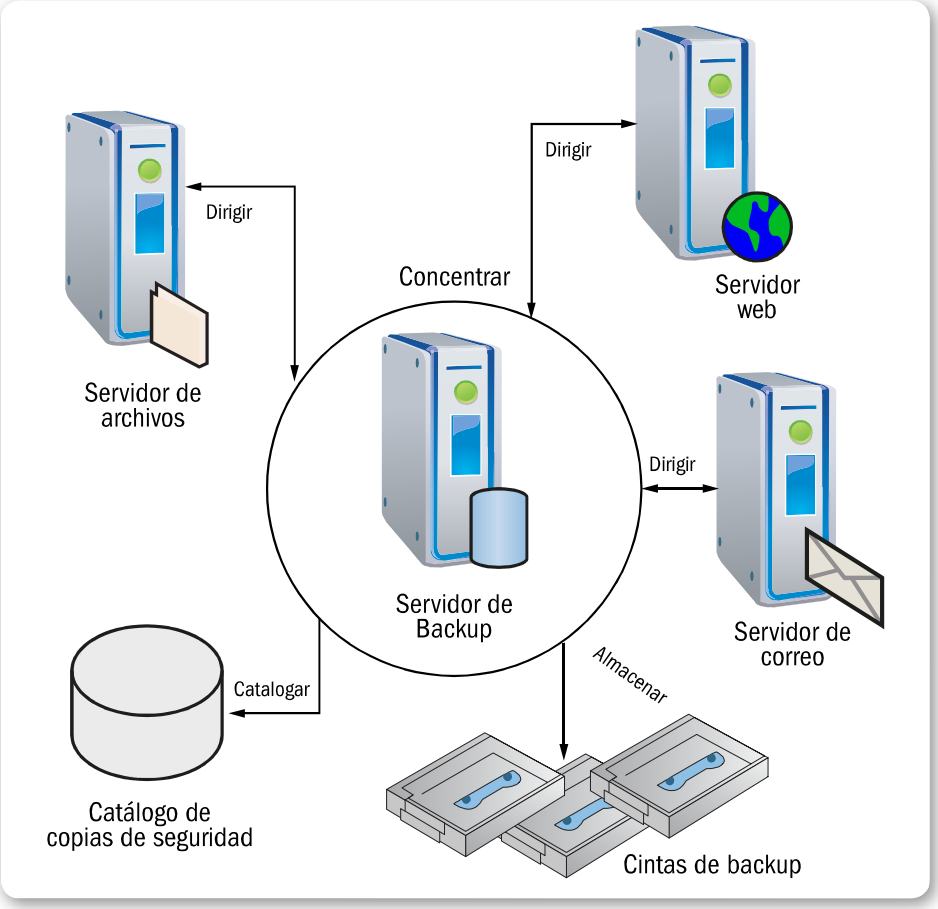


Figura 3. Esquema de las interacciones entre el servidor de backup, los orígenes de copias de seguridad, los medios y el catálogo.

Tipos de backup

Una vez que tenemos instalado el software de backup, definidos los equipos que contienen la información que tenemos que respaldar y establecidos los grupos de archivos por copiar, es necesario que definamos los parámetros que implementarán nuestra estrategia de copia de seguridad.

Una de las opciones más importantes que tenemos que definir es qué tipo de backup realizamos; a continuación, se describen las diferentes opciones con las que contamos:

Backup completo

Es el método más simple para realizar nuestras copias de seguridad. Consiste en efectuar la copia completa de un grupo de objetos especificado.

Por ejemplo, si tenemos que copiar una carpeta que contiene un conjunto de archivos, mediante el backup completo realizamos la copia de todos los archivos, independientemente de si hayan sido modificados o no.

> LOS DISTINTOS TIPOS DE BACKUPS NOS PERMITEN APROVECHAR LOS RECURSOS

Este tipo de backup es el que, por lo general, implementamos cuando realizamos las copias de respaldo de forma manual ya que solo es necesario utilizar las funcionalidades básicas que nos brinda el sistema operativo.

Las principales ventajas de este tipo de backup son la facilidad con la que se implementa, así como también la simpleza con la que se recuperan los datos, dado que siempre tenemos la copia completa en un solo medio. Como desventaja podemos mencionar que, para

COMBINAR ES LA CLAVE

En los casos en los que no sea posible efectuar las copias del tipo completo sobre todos los grupos de objetos, lo recomendable es que realicemos el análisis doble de cada grupo por separado. Esto se realiza con el fin de seleccionar la combinación más adecuada de tipos de backup para cada uno y lograr, de ese modo, la mejor utilización de los medios de almacenamiento de backup, además de una recuperación acorde con nuestras necesidades en cuanto a tiempo y complejidad.

volúmenes de datos importantes, el tiempo que se tarda en realizar la copia y el tamaño del backup que resulta hacen que el tipo de backup completo no sea la opción más adecuada.

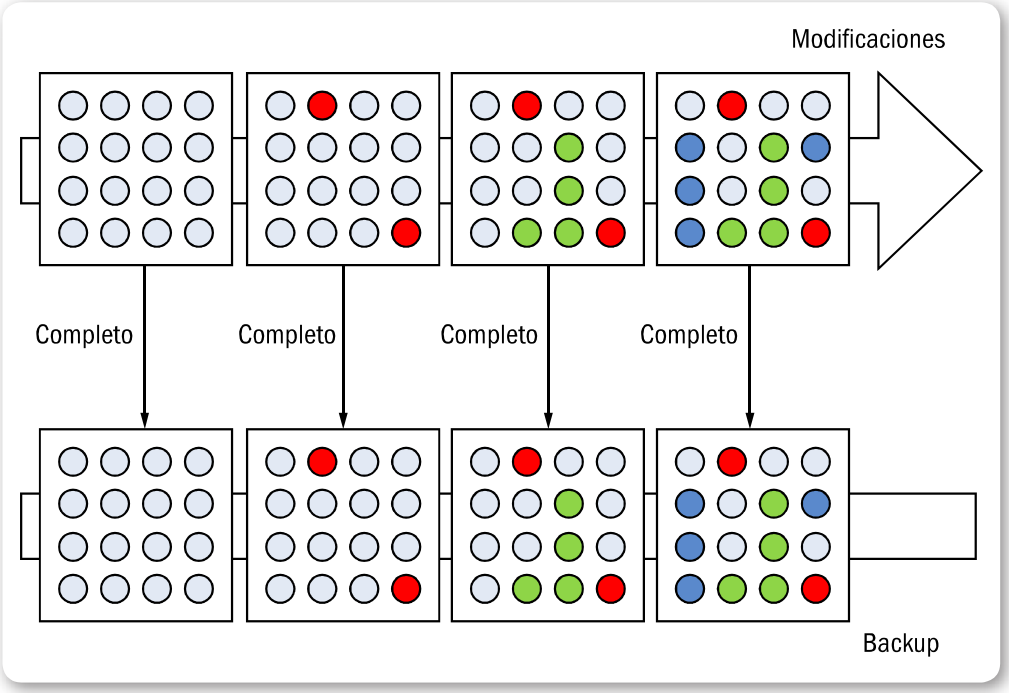


Figura 4. Esquema del tipo de backup completo, en el que se puede apreciar la copia de la totalidad de los objetos.

Backup diferencial

Cuando el volumen de información para resguardar aumenta, el modelo de backup completo puede no ser el más adecuado, sobre todo si en el grupo de objetos a los que les realizamos la copia de seguridad existe una gran proporción que no sufre modificaciones con frecuencia.

El backup diferencial realiza la copia de los objetos que sufrieron modificaciones desde el último backup completo.

Debido a que es necesario registrar los datos de los objetos que copiamos para realizar luego el cálculo de cuáles son los que sufrieron modificaciones, necesitamos software específico de backup para realizar este tipo de copias de respaldo.

Esta clase de backup, al transferir solo los objetos modificados, produce copias de seguridad que ocupan menos tamaño que las de tipo completa y, por consiguiente, se copian en menos tiempo.

La principal desventaja es la complejidad en la recuperación ya que, para realizar una recuperación del grupo completo de objetos a la versión más reciente, necesitaremos el medio que contiene el backup completo y el medio que almacena el último backup diferencial del grupo de objetos por restaurar.

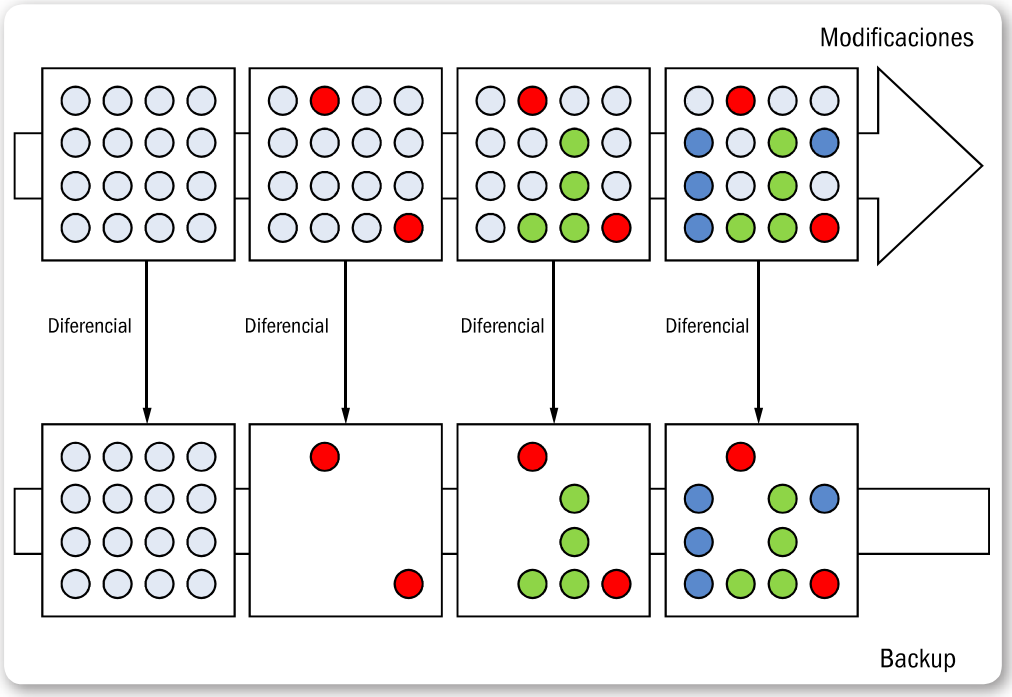


Figura 5. El tipo de backup diferencial realiza las copias de los objetos que cambiaron desde el último backup de tipo completo.

Backup incremental

El tipo de backup incremental es similar al de tipo diferencial; lo único que cambia es que, en este caso, se copian los objetos que fueron modificados teniendo en cuenta el último backup, sin importar si la última copia de respaldo fue del tipo completa, diferencial o incremental.

Al igual que en el caso del backup diferencial, el tipo de backup incremental se lleva a cabo mediante software específico de backup.

La ventaja del backup incremental es que genera las copias de seguridad más rápido y tiene como resultado backups de menor tamaño que las otras dos alternativas.

La desventaja de este tipo de backup reside en que es el que tiene la recuperación más compleja ya que, siempre que debamos restaurar

un grupo completo de objetos, necesitaremos, en el peor de los casos, el medio que contiene el último backup completo y todos los medios que contienen las copias de seguridad del tipo incremental, para poder realizar la recuperación.

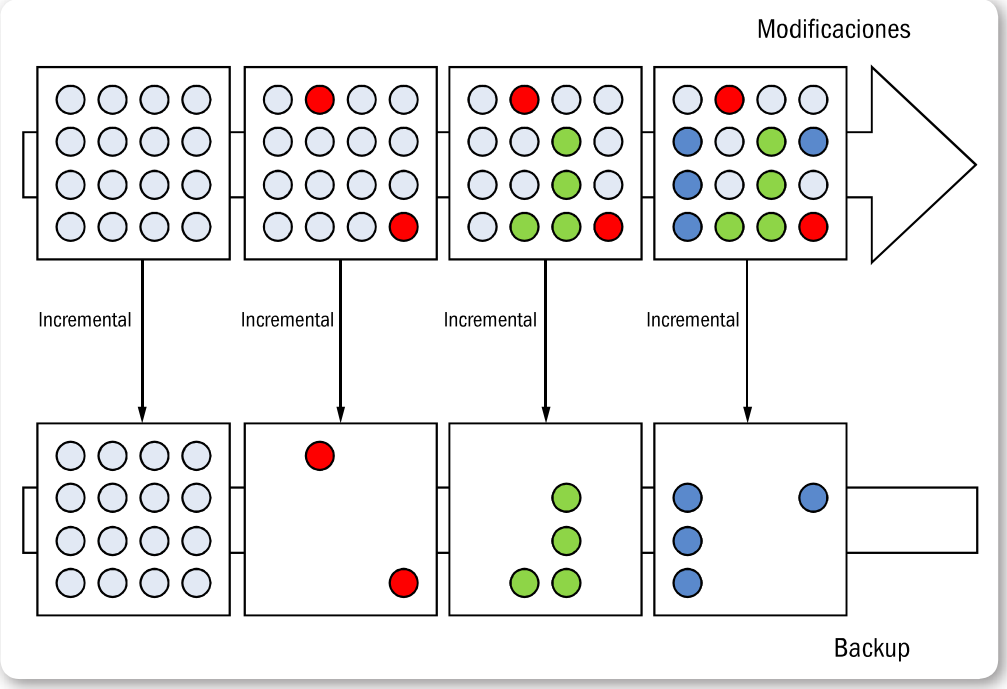


Figura 6. Demostración del tipo de backup incremental, en el que se copian solamente los objetos que sufrieron cambios desde el último backup.

Aspectos para tener en cuenta

En el momento de definir el tipo de backup que realizaremos para cada grupo de objetos por copiar, debemos tener en cuenta algunos aspectos básicos; a continuación, se detallan los más importantes.

Quizás el aspecto más relevante que tenemos que tener en cuenta a la hora de decidir el tipo de backup para un grupo de objetos sea el espacio que ocupan. Si el tamaño del grupo de objetos no es significativo, la opción más recomendada es siempre realizar backups completos; a medida que el tamaño del grupo de objetos aumenta, empezaremos a pensar en un esquema mixto entre copias de respaldo del tipo completas y copias del tipo diferenciales o incrementales.

Otro factor que condiciona la elección del tipo de copia de seguridad por realizar es la capacidad de los medios a los que vamos a transferir

el backup. Consideremos que si la capacidad del disco duro, cinta de backup, DVD o CD al que vamos a transferir nos resulta suficiente, podemos optar por realizar todas las copias en el modo completo, de lo contrario debemos plantear un esquema mixto.

La frecuencia en la que se modifican los datos nos define si es conveniente o no optar por copias del tipo diferencial o incremental si el volumen de la información y la capacidad de los medios lo justifican.

En el caso de que, en un grupo de archivos, la mayor parte de ellos sufra modificaciones en forma continua, las copias del tipo diferencial o incremental tendrán un tamaño similar a las del tipo completo, por esta razón debemos considerar que en algunos casos nos conviene realizar solo copias del tipo completo, ya que las ventajas relacionadas con el espacio ocupado por el backup son mínimas.

Soporte de los backups

Si bien sobre este tema hay mucha información y también aplicaciones disponibles, nos vamos a enfocar en el ámbito empresarial. Antes de realizar un backup de información, hay que ver realmente qué es lo importante para realizar la copia de respaldo ya que el espacio que necesitamos podría ser considerable.

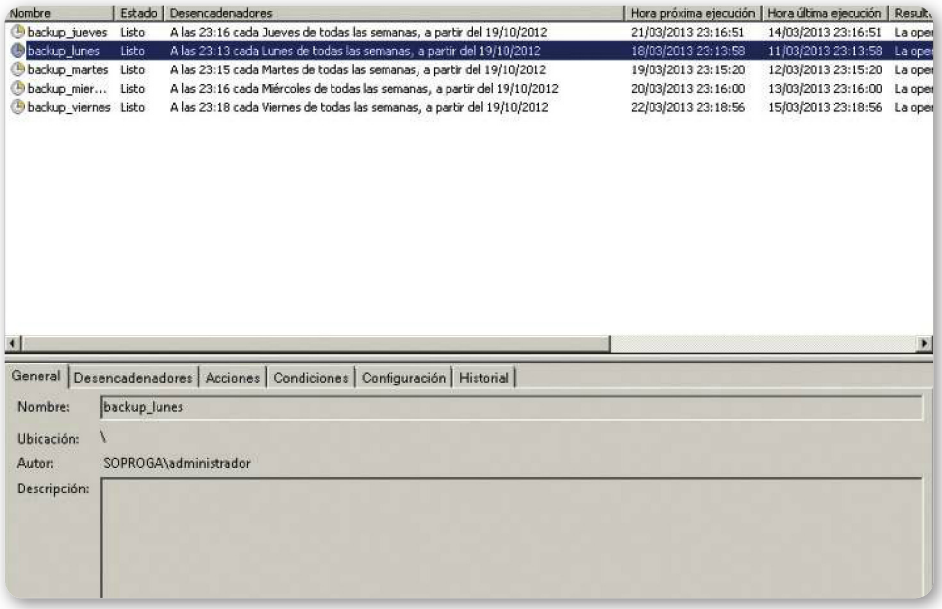


Figura 7. El script se tiene que ejecutar en el directorio en el que está situado y se configura en las opciones.

En una empresa que cuenta con tres PCs, pero no tiene servidor, quizás, el backup se realice de forma manual en un disco externo; sin embargo, cuando hablamos de un gran número de computadoras, con información confidencial, con el tiempo esto se vuelve engorroso, no productivo y puede consumir horas laborales del departamento de sistemas.

> RESGUARDAR LA INFORMACIÓN ES CLAVE PARA LA CONTINUIDAD DEL NEGOCIO

Al hablar de servidores basados en plataformas Windows (2003, 2008, 2012) y también Linux, si bien hay herramientas que realizan este trabajo, es recomendable usar un script que controle tanto la copia de archivos como su compresión (para ahorrar espacio), el envío de e-mails y su borrado cada cierto período. Para ello, vamos a necesitar dos programas: uno llamado **Robocopy**, que permite realizar solo la copia de los archivos que han sido modificados, con log incluido; y también la aplicación **Postie**, un pequeño cliente SMTP para el envío de correo.

Implementación

En primer lugar, creamos un archivo de extensión .BAT, en el cual escribiremos las líneas de código que nos permitirán controlar las tareas de respaldos. A continuación, vemos un ejemplo de este archivo; sus líneas se pueden modificar dependiendo del tipo de backup y de las necesidades específicas:

```
@echo off
setlogbakdiarios="E:\gyb\Tareas Programadas\Logs\%1_LogBackup_po12.txt"
setlogerror="E:\gyb\Tareas Programadas\Logs\ERROR.txt"
set origen="E:\backup\temp\documentos"
set destino="E:\backup\%1\documentos"
set origen2="E:\backup\gb_admin"
set destino2="E:\backup\%1\gb_admin"
```

Para establecer la fecha como nombre de archivo:

```
for /f "tokens=1-2 " %%A in ('DATE /T') do set datedia=%%A
for /f "tokens=1-3 delims=/" %%A in ('echo %DATEDIA%') do set
datedia=%%A-%%B-%%C
```

Comienzo de backup:

```
%logbakdiarios%
echo. >> %logbakdiarios%
```

Mostrar la fecha y la hora:

```
echo. >> %logbakdiarios%
echo ************************* >> %logbakdiarios%
echo * %DATE% %TIME% * >> %logbakdiarios%
echo ************************* >> %logbakdiarios%
echo. >> %logbakdiarios%
```

Backup de sistema:

```
robocopy E:\gyb\ E:\backup\temp\gyb /MIR /e /copy:D
/R:1 /W:1 /NP >> %logbakdiarios%
```

> ROBOCOPY ES UNA APLICACIÓN QUE NOS PERMITE REALIZAR COPIAS UTILIZANDO COMANDOS

Creación de los archivos comprimidos:

```
7za.exe -ssw -tzip -r a %destino2%\gb_admin.zip
%origen2%\ >> %logbakdiarios%
del /q origen2%\*.* >> %logbakdiarios%
```

Backup de documentos:

```
robocopy E:\documentos\ E:\backup\temp\documentos /MIR /e /copy:D /R:1
/W:1 /NP >> %logbakdiarios%
```

Compresión de los logs:

```
7za.exe a ..\Logs\%datedia%.zip %logbakdiarios%
::Busqueda de errores
::FIND /N "ERROR " %logbakdiarios% > %logerror%
```

Envío de mail:

```
postie.exe -esmtp -host:mail.gbconsulting.com.ar -user:backups@consultora.
com.ar -pass:xxxxxxx -to:soporteit@consultora.com.ar -from:backups@
consultora.com.ar -s:"Empresa- Backup del %date%" -msg:"Reporte de backup
del servidor Empresa" -a:"E:\ \Tareas Programadas\Logs\%datedia%.zip"
del /q %logbakdiarios%
```

Como se puede ver, primero se copian a una carpeta temporal y, luego, sobre esa carpeta, se realiza la compresión. Al finalizar esto,

el script nos envía un e-mail con el reporte del backup comprimido (reporte del copiado y la compresión).

Si bien el backup puede estar en un disco interno, con RAID 5 y más medidas de seguridad para proteger los datos, siempre es imprescindible contar con un medio físico externo de backup, para el caso de cortes de energía, robo o incendio.

Figura 8. Las cintas pueden guardar más información y en menos tiempo.

Otras soluciones

Ahora, si optamos por una solución paga que incluya desde el backup local hasta la copia en disco tanto externo como interno, y en cintas, existe una gama de herramientas muy importantes, pero la más recomendable es **Symantec Backup Exec**, que cuenta además con la integración a diferentes aplicaciones propias de entornos corporativos.

Es muy configurable en cuanto a los períodos de backups, se realizan verificaciones y no hace falta ningún script, por ejemplo, para conectarse a SQL y realizar el backup de las bases de datos.

Actualmente, los medios en los cuales se realizan copias de seguridad son bastantes. Los más difundidos por su redundancia en

seguridad en cuanto a información son los discos duros internos, con métodos de redundancia RAID ya sea por hardware o software. Luego, tenemos medios externos que nos facilitan esta tarea, y su transporte: discos duros portátiles y cintas, los cuales pueden tener una capacidad de almacenamiento igual o superior a un disco duro interno, pero que poseen un grado de durabilidad y protección más alto.

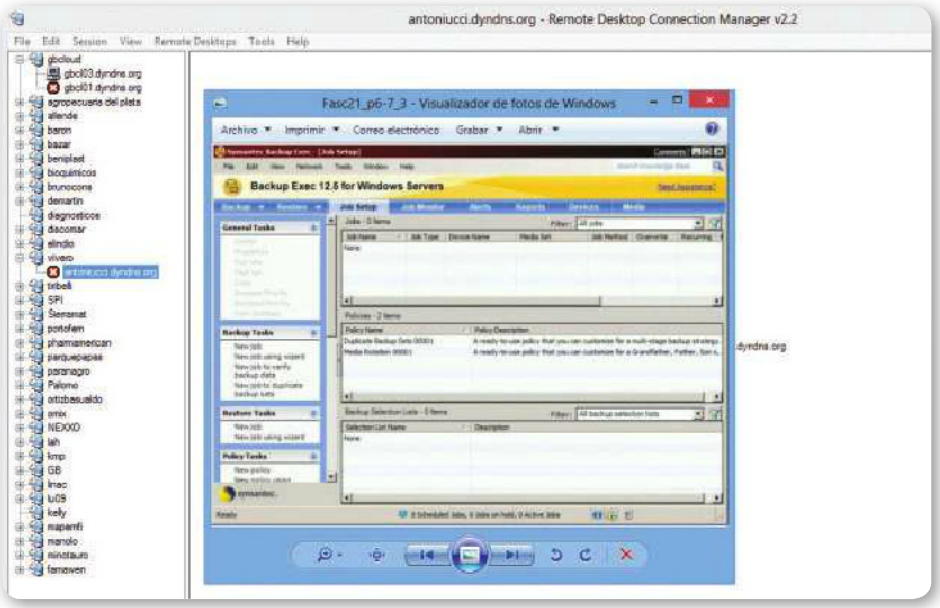


Figura 9. Se puede observar que la administración es sencilla y amigable para el usuario.

Si bien son más recomendables las cintas por su duración, además tenemos que disponer de una unidad de cinta a la hora de realizar la restauración, por esta razón también hay que fijarse en el grado de inversión que estamos dispuestos a realizar.

RESPALDO COMPLETO

Si bien el respaldo de la información es crucial, muchas veces el backup del entorno también lo es. Un ejemplo de esto son las máquinas virtuales o servidores de base de datos (SQL por ejemplo). Esto quiere decir que, en máquinas virtuales, está bien hacer un backup del disco, pero a la hora de restaurarlo también hay que crear la máquina virtual con las mismas especificaciones y actualizaciones que tenía, si no, cuando se restaura el disco, es probable que no prenda la máquina virtual.

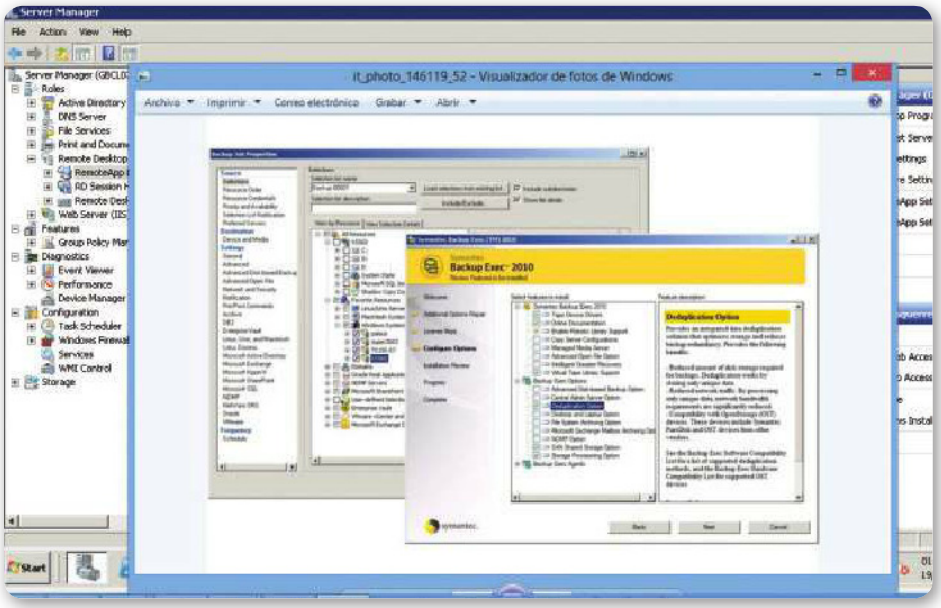


Figura 10. Symantec Backup Exec se adapta fácilmente a cualquier plataforma y sistema físico.

Servidor de actualización

Estamos ante un mundo muy cambiante en el cual, día a día, aparecen nuevas implementaciones, hardware y descubrimientos de vulnerabilidades que ponen en situación riesgosa nuestro sistema e infraestructura informática.

En este caso, vamos a revisar el concepto de servidor de actualización tanto de Windows como en sistemas GNU/Linux. De esta forma, conoceremos sus principales características y, también, las opciones que tenemos a nuestra disposición para implementar un servidor de este tipo.

Sistemas Windows

Es necesario considerar que para el caso de **Windows Server** (en sus versiones 2003 R2, 2008 R2 y 2012), uno de los roles que se deben instalar para implementar un servidor de actualizaciones es **Windows Server Update Services**, el cual permite a los administradores de red especificar las actualizaciones de Microsoft que se deben instalar,

crear grupos separados de equipos para diferentes conjuntos de actualizaciones y también obtener completos informes sobre los niveles de compatibilidad de los equipos y actualizaciones que se deben instalar. Esto permite optimizar el funcionamiento de la red y de esta forma obtener un entorno controlado.

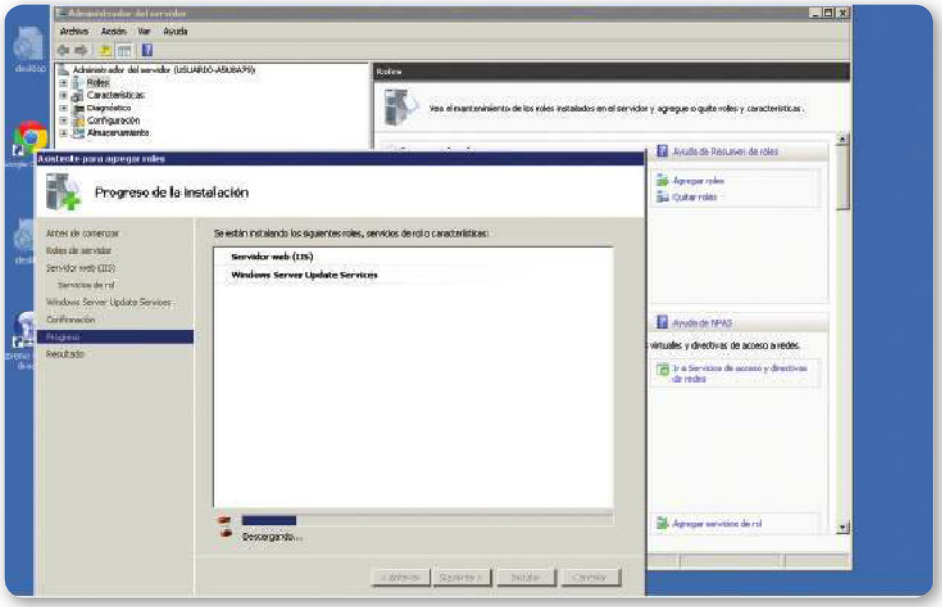


Figura 11. La instalación de Windows Server Updates Services es sencilla; requiere IIS incluido en Windows Server en todas sus versiones.

Una vez instalado el rol desde Windows Server, debemos acceder a las opciones de administración de nuestro servidor; allí especificamos qué tipos de actualizaciones se destinarán para determinados equipos. No se trata de una tarea compleja, ya que Windows Server nos entrega un completo asistente que nos orientará durante su configuración.

ACTUALIZACIONES

Si bien la actualización del sistema operativo con los últimos paquetes es algo que se recomienda en materia de seguridad y rendimiento, no siempre ocurre esto. Muchas veces, los paquetes se instalan mal o tienen problemas de versionado y ocasionan problemas, como lentitud del sistema o la no carga de la plataforma, por lo que no hay que borrarlos manualmente. Siempre hay que elegir con cuidado qué se va a instalar, y en qué sectores o áreas va a repercutir cada cambio.

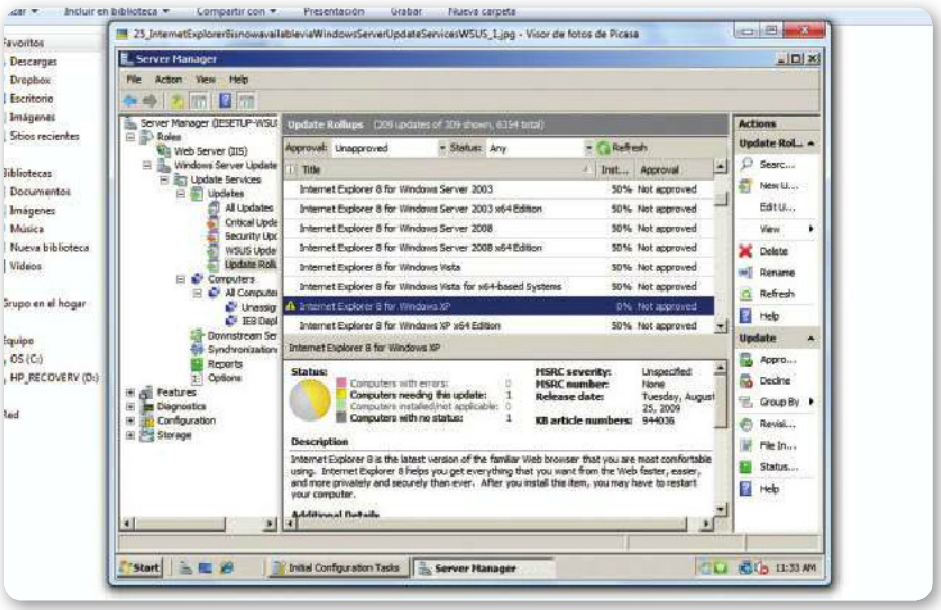


Figura 12. Se puede visualizar que es fácil la distribución e instalación en equipos del dominio, separándolos por su tipo.

Sistemas GNU/Linux

En entornos GNU/Linux, la actualización es más compleja, ya que requiere que realicemos algunos pasos previos para que las computadoras hagan uso del servidor de actualizaciones ubicado en la red LAN.

> DEBEMOS EMPLEAR ESTRATEGIAS DE INSTALACIÓN Y DISTRIBUCIÓN ACORDES CON EL USO

El objetivo es lograr que todos estos paquetes puedan ser leídos por las otras máquinas. Para ello, utilizaremos el comando **apt-move.**

Básicamente, esta herramienta toma una serie de paquetes .DEB de cualquier sitio y los inserta en una estructura con la misma jerarquía que un espejo de Debian. Lo primero que debemos hacer es instalar el paquete **apt-move**, para esto utilizamos el comando

apt-getinstallapt-move

El siguiente paso consiste en configurar **/etc/apt-move.conf**, aquí debemos cambiar una serie de valores para que funcione en forma correcta.

En la variable **APTSITES**, especificamos los sitios de **sources.list** que estarán disponibles. Un ejemplo del archivo **sources.list** es el siguiente:

ftp://ftp.us.debian.org/debian/ unstablemain non-free contribdeb
http://non-us.debian.org/debian-non-US unstable/non-US maincontrib non-free

La variable **APTSITES** podría definirse como **ftp.us.debian.org non-us.debian.org**; recordemos que los sitios especificados deben estar separados por espacios.

Figura 13. En Ubuntu, hay un gestor de actualizaciones similar a Windows, que comprueba la compatibilidad con cada paquete.

Consideremos que en la variable **ARCHS**, especificamos las arquitecturas que queremos replicar; para una arquitectura Intel escribimos lo siguiente: **ARCHS="i386".**

Por otra parte, en **LOCALDIR**, es necesario que ingresemos el directorio que va a contener el espejo que estamos creando. Por ejemplo **/mnt/disk2**. Este directorio debe ser accesible por HTTP, FTP, NFS o SMB, por cada uno de los clientes que se encuentran conectados a la red. Para ello, podemos utilizar un servidor Apache en la dirección **/var/www**; en ese directorio, creamos un enlace (**ln -s /var/www/apt /mnt/disk2**) al directorio **LOCALDIR**, de forma que una petición **http://192.168.0.1/apt** devolvería el contenido de **LOCALDIR.**

En **DIST** especificamos las distribuciones que deseamos replicar; tenemos las opciones **stable**, **unstable**, **potato**, **woody** y **sid**. Un ejemplo de configuración de este parámetro es **DIST="unstable".**

EN PKGTYPE DEBEMOS ESPECIFICAR EL TIPO DE PAQUETES QUE SE REPLICARÁN

En **PKGTYPE** especificamos qué tipo de paquetes queremos replicar: binarios, fuentes o ambos, las opciones son **binary**, **source** y **both**; solo se puede elegir una opción.

Para continuar, en **FILECACHE** y **LISTSTATE**, debemos especificar dónde se encuentran los archivos locales de los paquetes. Salvo que hubiésemos cambiado la configuración de **apt-get** los valores que se muestran en forma predeterminada funcionarán correctamente:

FILECACHE=/var/cache/apt/archives y LISTSTATE=/var/lib/apt/lists

Por último existe la opción **DELETE** que nos permite eliminar la versión más antigua de cada programa. Las opciones son **yes** o **no**. Una vez guardados los cambios en el archivo **/etc/apt-move.conf**, podemos utilizarlo.

El procedimiento es el siguiente: en el servidor actualizamos con el comando **apt-getupdate** y **apt-getdist-upgrade**; una vez finalizada tecleamos **apt-moveupdate.**

En los clientes, debemos editar el archivo **/etc/apt/sources.list** de forma que en la primera línea añadiremos la ruta que hemos creado en el servidor. Un ejemplo sería la siguiente línea:

deb http://192.168.27.1/apt/ distribuciónmain non-free contrib

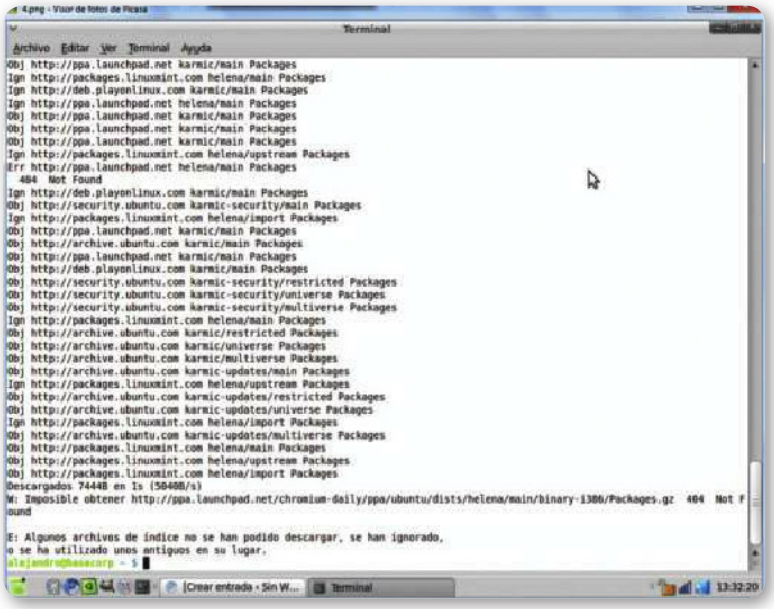


Figura 14. No siempre están los paquetes necesarios para actualizar, muchas veces hay que bajarlos en forma manual.

Servidor de antivirus

En la actualidad, sabemos que existen una infinidad de amenazas que hacen que no solo nuestros sistemas sean vulnerables, sino que nuestra información personal esté expuesta al quehacer de desconocidos. Si bien podemos tener en nuestras PCs hogareñas antivirus gratuitos, antimalware, anti-spyware o antiphishing, que por cierto son medidas altamente efectivas a la hora de combatir estos ataques, estos, aun juntos, no son capaces de brindarnos una seguridad total a nivel empresarial, y que estén centralizados para actuar en conjunto.

> LOS ANTIVIRUS GRATUITOS NO SON CAPACES DE BRINDAR SEGURIDAD A NIVEL EMPRESARIAL

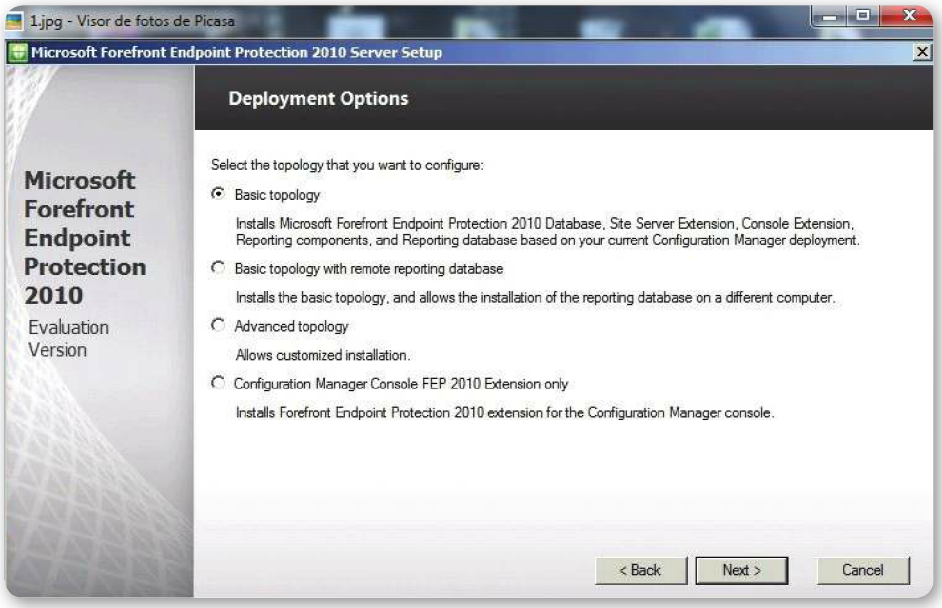


Figura 15. Aquí seleccionamos la topología básica que es la más empleada. Suele usarse la segunda opción en caso de que tengamos un servidor de Bases de Datos dedicado.

A la hora de hablar del ámbito empresarial, estamos de acuerdo que, en materia de seguridad, hace falta invertir ya sea en capital humano o en software. En este punto, los servidores de antivirus se hacen presentes, ya que la mayoría son comerciales. Nos permiten manipular la detección y el tratamiento de virus y malware, así como monitorear

los archivos del sistema para asegurar que no sean modificados. Existen varias opciones de servidores de antivirus, aunque bajo la plataforma Windows (2003 y 2008 R2; con Active Directory), los que entregan mejores resultados son **Microsoft Forefront EndPoint Protection y Bitdefender Security**.

Microsoft Forefront EndPoint Protection

Si bien contamos con **Microsoft Security Essential**, que es gratuito, este sirve solo para 10 PCs, y su administración no es centralizada. Al encontrarnos en una infraestructura más grande, la solución es **Microsoft Forefront EndPoint Protection**. Este producto no tiene más complejidad que su implementación ya que la administración es muy sencilla. Simplemente tenemos que contar con una versión de **SQL Server Express** y tener en cuenta que se va a instalar solo en nuestro servidor.

> UN SERVIDOR DE ANTIVIRUS PERMITE ADMINISTRAR Y AISLAR AMENAZAS EN FORMA EFICIENTE

Una vez concluida la instalación, tenemos dos formas de acceder: vía HTTP o por la consola de administración del servidor. El servidor va a ser el único que recibirá las actualizaciones correspondientes, que luego va a distribuir en las demás PCs, mostrándonos en cuáles se pudo instalar el agente Forefront para la detección de virus o malware.

Desde la administración, podemos configurar intervalos de escaneo, actualizaciones y qué se va a hacer en cada caso al detectarse una

PARA TENER EN CUENTA

Siempre es necesario tener una herramienta que centralice el uso y la detección de virus o malware, pero lo más importante es no perder esa información ni que sea robada más allá del servidor antivirus que se utilice. Usando los reportes se pueden prevenir muchas amenazas, al detectar qué usuarios entran a ciertas páginas o descargan software infectado, para advertirles sobre esto o bien bloquear sus accesos. Siempre hay que tener una copia de respaldo de todos los datos, ya sea local o externa.

amenaza. Es transparente para los usuarios, y ninguno de ellos puede administrarlo. En caso de detectarse una amenaza, se pueden especificar los pasos por seguir para ver de qué manera se trata sin interferir con los demás usuarios de la empresa y que tampoco noten esto, para no parar la productividad; todo se realiza de forma automatizada.

Si bien, en forma predeterminada, Windows 7 y 8 en todas sus versiones posee instalado el Microsoft Security Essentials, este se debe desinstalar ya que no es compatible.

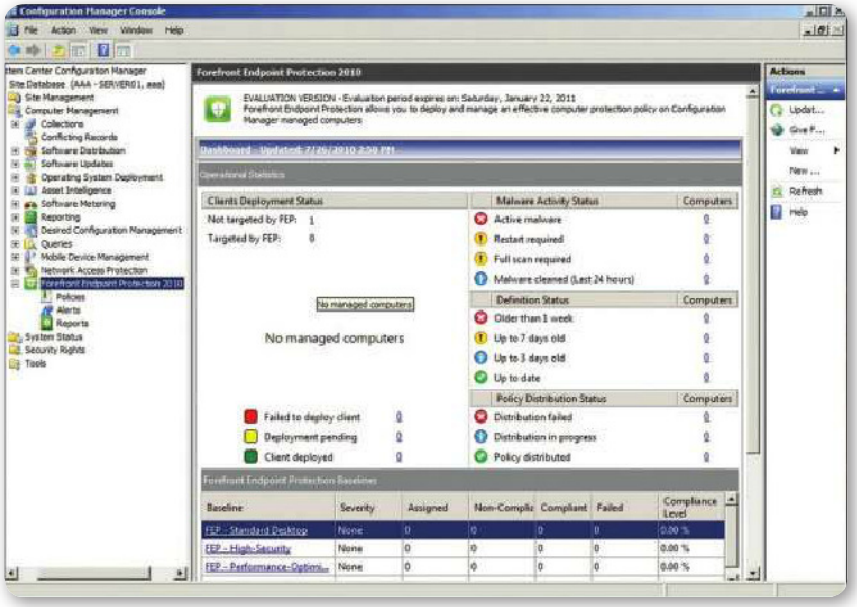


Figura 16. Se observa que, en la consola de administrador del servidor, hay una solapa de Microsoft Forefront donde vemos el estado de cada PC.

Bitdefender Security

Bitdefender, por otro lado, nos muestra una solución más personalizable pero administrable con algo de complejidad, ya que este producto también sirve, tanto para plataformas Windows como para sistemas Linux/Unix; en este último caso, la instalación y la configuración son un poco más complejas.

Si bien la instalación en el servidor es similar a Microsoft Forefront Endpoint, presenta una serie de complejidades cuando deseamos realizar la instalación en servidores GNU/Linux. Debemos considerar que el **Management Server** de Bitdefender proporciona una potente

consola de administración centralizada para todas las soluciones de protección de puesto final, servidores críticos y puertas de enlace. Combina tanto la visibilidad a la hora de implementar políticas de seguridad en la empresa mediante la configuración remota de puntos finales, como la política de refuerzo a través de una interfaz centralizada.

La instalación del agente en plataformas Linux requiere que se descargue el paquete desde el CD de instalación<, luego debe ubicarse en la carpeta **/opt**, y la instalación se realiza desde una consola:

```
# sh BitDefender-Security-Mail-3.1.2-linuxgcc3x-i586.rpm.run
```

En algún momento, se le preguntará si quiere activar la integración con **Bitdefender Management Server**. Escribimos **S** y pulsamos **ENTER.** Luego hay que especificar el host de Bitdefender Management Server:

```
# cd /opt/BitDefender/bin
# ./bdsafebdem host <host[:port]>
```

A continuación, reiniciamos el producto:

```
# cd /opt/BitDefender/bin
# ./bdrestart
```

Desde este momento, vemos las soluciones instaladas para servidores Unix en la consola de administración de Bitdefender en Windows. Esta integración se puede desactivar en cualquier momento usando los comandos siguientes:

```
# cd /opt/BitDefender/bin
# ./bdsafebdem enable N
# ./bdrestart
```

Ventajas

Sin duda, una de las ventajas más importantes de centralizar el servidor de antivirus, malware, etcétera, es no solo su administración, sino el rápido aislamiento de la amenaza, ya que la separa del resto de la red, tanto LAN como WAN, sin intervención de ningún técnico o administrador de redes. Esto hace que, siempre previniendo el problema, no se pierda información alguna o que esta sea robada, ya que es lo más valioso para una empresa. Este trabajo tiene que estar acompañado por una buena planificación y un diagrama de infraestructura de la red, para que esté completamente segura y no haya ningún agujero.

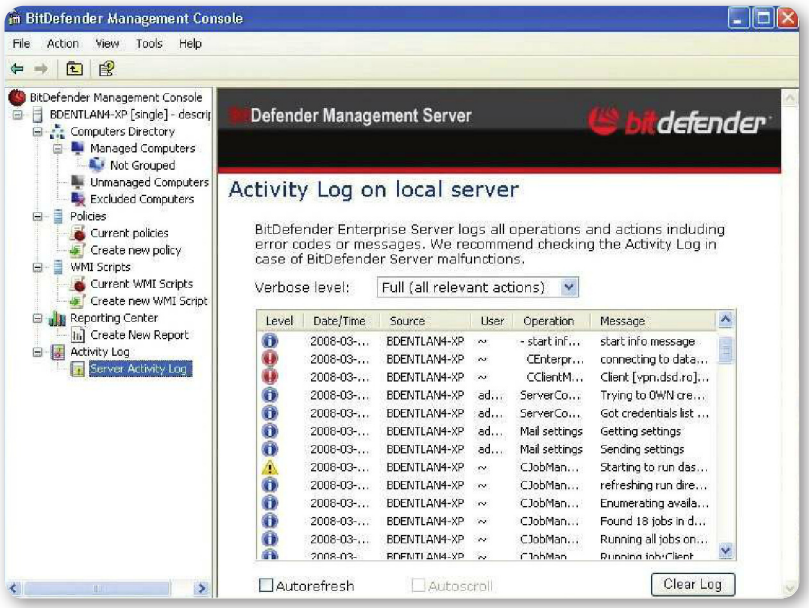


Figura 17. Como se puede observar, Bitdefender es mucho más configurable; permite incorporarse a Active Directory y distribuir políticas con facilidad.

Servidor proxy

Es interesante mencionar que cuando Internet comenzaba a ampliar sus horizontes, nuestras máquinas se conectaban a la Web con direcciones IP públicas y, más allá de eso, nadie se preocupaba por la seguridad relacionada a estas conexiones.

En la década de los 80, con la adopción por parte de ARPANET del protocolo TCP/IP, dividimos las redes en distintas clases; de cada una se separaron redes especiales de carácter privado. Estas redes privadas se crearon para evitar la exposición de los equipos de las organizaciones.

> EN LA DÉCADA DE LOS 80 SE PROCEDIÓ A DIVIDIR LAS REDES EN DISTINTAS CLASES

Las redes creadas, y que actualmente utilizamos, se clasifican en tres tipos: A, B y C. Cada una tiene lo que se denomina una **máscara de subred**, lo cual permite subdividirla en varias redes más pequeñas (para que podamos manejar mejor la administración de las máquinas y las direcciones).

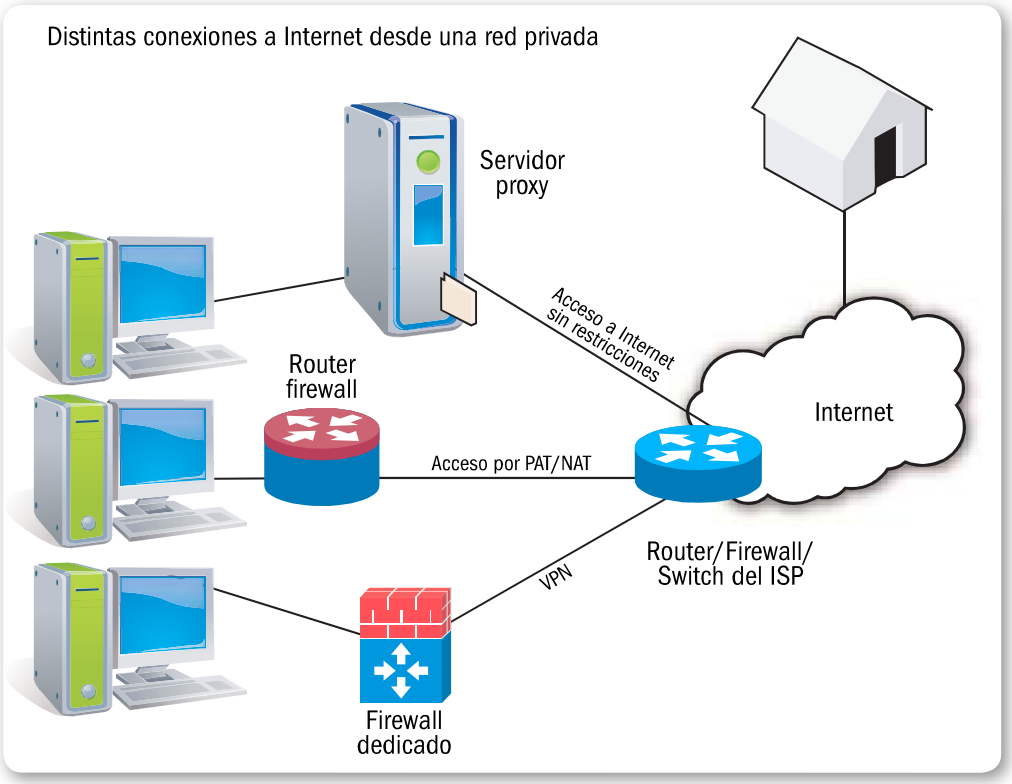


Figura 18. Esquema donde se pueden ver los tres tipos de conexión a Internet: por NAT-PAT a través de un firewall, por proxy caché y por VPN.

Conexión a Internet

Para conectarnos a Internet, utilizamos varias técnicas de networking entre las que se encuentran **NAT/PAT** (*Network/Port Address Translation*) en firewalls, **VPN** (*Virtual Private Network*) y **proxies.**

Estos últimos comenzaron a tener auge en la década de 1990 con la aparición del protocolo HTTP y de su consecuente expansión debido al éxito comercial que tuvo la WWW (*World Wide Web*).

Proxy

Debemos saber que proxy significa **intermediario**, y su acepción la utilizamos en distintos ámbitos como sinónimo de *representante*; y es que la función principal de este software o hardware es justamente esa, intermediar o ser representante de un ente, ante otras entidades. Hablamos de entes ya que los representados por el proxy pueden ser desde máquinas a partes de software.

Consideremos que podemos encontrar distintos tipos de proxy; su implementación puede ser por software o hardware.

Entre los implementados por software, se hallan los denominados **proxy caché**, **proxy database**, **proxy pattern**, **proxy socks**, **proxy local**, **proxy público** y **proxy Ajax.**

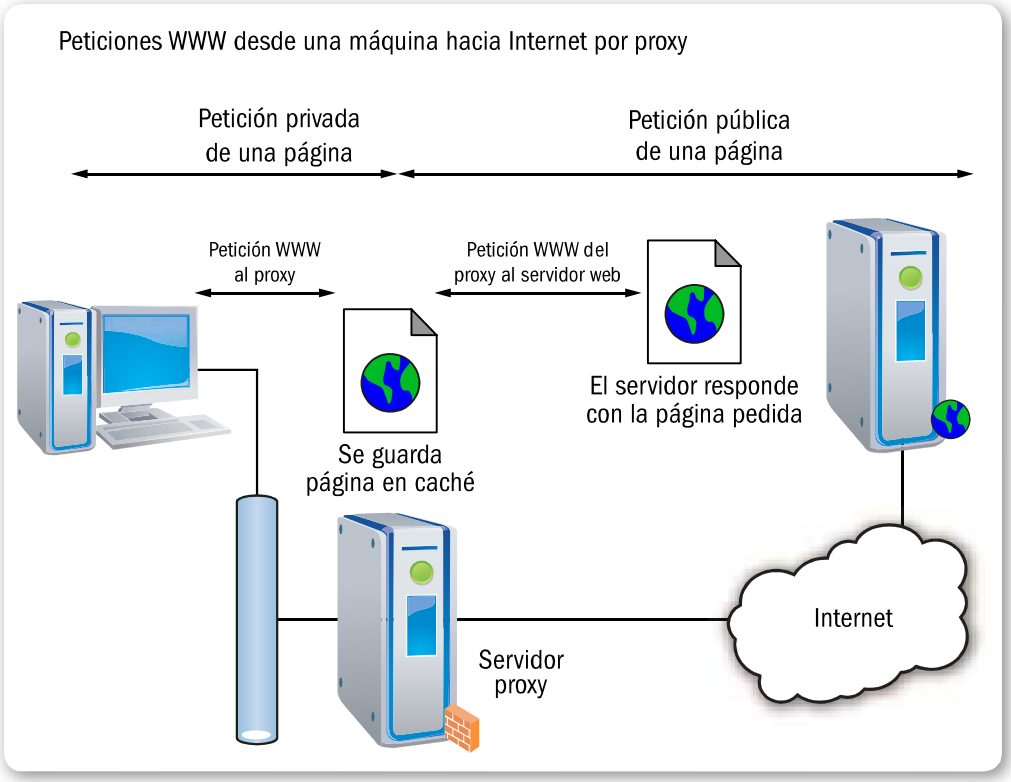


Figura 19. Esquema donde se puede visualizar cómo las peticiones de páginas son administradas por el servidor proxy.

Tengamos en cuenta que de los que lo son por hardware, tenemos los **proxy ARP** y **proxy firewall**. Podemos acercarnos a la definición declarando que proxy es una aplicación utilizada por una máquina para lograr la representación de una red de computadoras ante otras máquinas; en nuestro caso particular lo utilizaremos para representar una red ante Internet.

Nuestro enfoque aquí es sobre el proxy caché, quién nos permite, entre otras cosas, navegar con seguridad por páginas del WWW.

> EXISTEN DOS TIPOS DE PROXY POR HARDWARE: PROXY ARP Y PROXY FIREWALL

Proxy caché

El nombre de caché se adicionó ya que, para lograr acelerar la navegación en la era en que las computadoras se conectaban a un ISP mediante el uso de un módem, el proxy se encargaba de utilizar un banco de memoria o disco para almacenar temporalmente las páginas más visitadas (la caché), lo cual era un alivio para aquellas conexiones que utilizaban 56.000 bps.

> EL FUNCIONAMIENTO DEL PROXY ES SENCILLO Y SE BASA EN LA TOPOLOGÍA CLIENTE-SERVIDOR

El funcionamiento del proxy es muy simple y se basa en la topología cliente-servidor. Esta topología otorga el título de servidor a quien ofrece un servicio, en este caso el proxy, y el cliente es quien consume este servicio, en este caso las PCs que están en una red.

Sin embargo, es interesante considerar que para el caso en particular del proxy caché, el servicio se da a nivel de aplicación, por lo tanto la computadora (que funciona como cliente) debe tener una aplicación que se encargue de consumir este servicio; esta aplicación es, por lo general, un navegador web.

Figura 20. Configuración de un proxy mediante un archivo de comandos propio de la organización en IE 9.

En la actualidad, existen muy pocos navegadores que no permiten la configuración de proxy entre sus funciones; casi siempre, son versiones muy viejas o muy específicas. Entre estos, se encuentran el navegador **Lynx** de Linux y **Mosaic** o **Erwise** para Windows. En las versiones modernas de los navegadores más populares, estas opciones están disponibles en todos los casos.

Para que el circuito funcione, el navegador web deberá tener configurado los datos necesarios para realizar las peticiones al servidor proxy; entre estos datos, deberemos brindar una URL, una dirección IP, o un archivo con las políticas propias de conexión.

Una vez configurado, el navegador realiza una petición HTTP al servidor proxy, este toma la consulta y primero verifica si la URL solicitada está guardada en la caché propia, si es así, le da al cliente la copia que tiene localmente; en el caso contrario, realiza la consulta HTTP al server destino, toma la respuesta y, además de dársela al cliente, se guarda la copia en el caché. De esta forma, el servidor se encargará de presentar en internet su IP pública, esto sucede mientras el rango de direccionamiento de toda la organización quedará oculta para el resto del mundo.

> EL NAVEGADOR WEB DEBERÁ TENER CONFIGURADOS LOS DATOS PARA REALIZAR PETICIONES

Debemos tener en cuenta que en algunos casos se pedirá un usuario y una contraseña para acceder a las páginas que sean externas al servidor; en otros casos con medios de autenticación más sofisticados, esta tarea es realizada con certificados digitales, los cuales pueden ser de entidad pública o privada; incluso la conexión al servidor proxy puede llegar a encriptarse para mayor seguridad.

EVILDNS

Evilgrade se potenció con la vulnerabilidad DNS de Dan Kaminsky; esta utiliza peticiones DNS para poder colar una petición falsa (**Hijacking**) propia y redirigir, de esta forma, el tráfico de un cliente a un servidor **Web Rogue** (ladrón). Así, Evilgrade toma el control de las consultas DNS de los clientes para realizar las actualizaciones. En la actualidad, además de los parches para los DNS, se utiliza un hashing con **MAC Address** para evitar la actualización maliciosa y, aun así, Evilgrade es peligroso a nivel de red interna.

Conexiones

Algunas organizaciones pueden requerir que el proxy realice conexiones internas y externas, por lo cual se creará un archivo en el servidor con una extensión particular, para que la configuración sea automática.

> PROXY REENVÍA PETICIONES DE OTRAS MÁQUINAS, REPRESENTÁNDOLAS EN UNA RED EXTERNA

La instalación de un servidor proxy puede establecerse mediante un asistente, como en el caso de los servidores proxy en plataformas Windows; o mediante instalaciones complicadas y con administración de archivos de texto, como los que están bajo plataformas Linux.

Ambos tienen sus pros y sus contras. En el caso de Windows, si bien la instalación es muy fácil, la adaptación del software a esquemas donde las tareas son muy complicadas resulta muy difícil y, muchas veces, imposible. Todo lo contrario sucede en las plataformas Linux donde el servidor es muy flexible ante las necesidades de las redes modernas, pero su implementación lleva mucho tiempo.

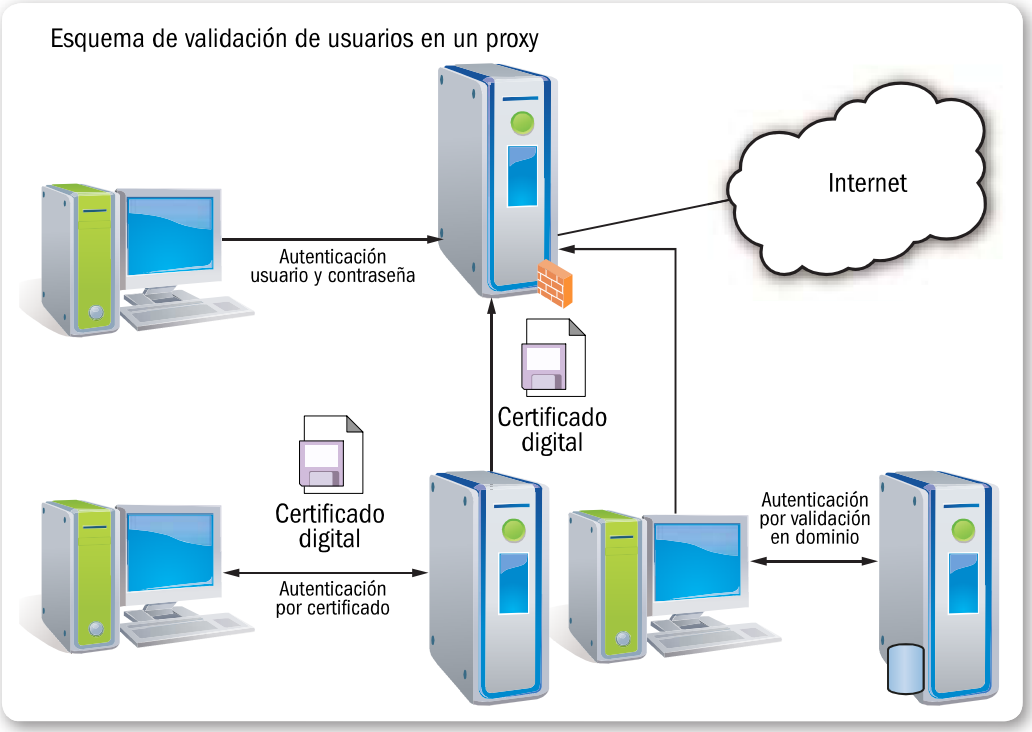


Figura 21. Distintas formas de validación de un servidor proxy: por usuario y contraseña, por certificado digital y por autenticación remota.

En ambos casos, la tarea del administrador del proxy es balancear entre el espacio asignado para la caché en disco del servidor, qué sitios web o URL son permitidos o negados a los clientes, qué cantidad de conexiones concurrentes puede haber desde un mismo cliente y hasta qué cantidad de ancho de banda o tráfico está permitido para cada uno.

Ventajas y desventajas

Las ventajas no solo se encuentran del lado de quien quiere acceder a Internet al acelerar la navegación, sino también del lado administrador, ya que nos permite disminuir el ancho de banda que se consume en la conexión a Internet, bajamos las colisiones de paquetes y, también, podemos administrar el acceso a los sitios.

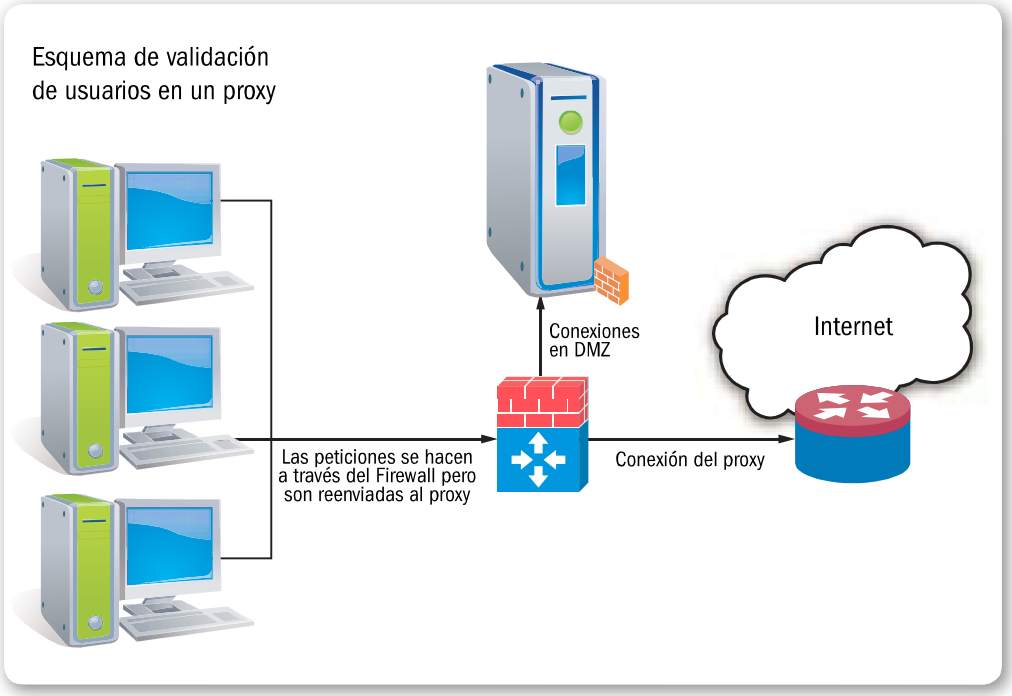


Figura 22. Esquema de protección mediante DMZ en un ambiente bajo firewall dedicado.

Es relevante mencionar que una de las desventajas más importantes que nos encontramos a la hora de utilizar un proxy caché para navegar por Internet consiste en que no sabemos si las páginas a las que accedemos se encuentran correctamente actualizadas, como sucede en el caso de los sitios de Internet que poseen un tiempo de refresco muy

bajo; otra de las desventajas es poseer un solo punto de falla, lo cual resulta en que proxy deja a la organización muy vulnerable a un ataque del tipo DoS. Por otra parte, en el caso de ciertas aplicaciones que han sido desarrolladas con tecnologías nuevas como las que utilizan JavaScript y generación de contenido en forma dinámica, podemos encontrarnos con que su funcionamiento será incorrecto al usar proxy.

> EN GRANDES ORGANIZACIONES ES COMPLEJO ADMINISTRAR A LOS USUARIOS

Además, podemos tener inconvenientes en la administración de los usuarios ya que, en grandes organizaciones, estos literalmente pueden necesitar una granja de servidores de bases de datos para administrarlos, lo cual complejiza más el sistema en vez de simplificarlo.

Ubicación

Por lo general, ubicaremos un servidor proxy caché en un área de seguridad informática denominada **DMZ** (*Demilitarized Zone*), que se encuentra aislada por medio de un firewall (que puede ser un software o hardware) corporativo tanto de Internet como de la red privada de la organización. Esta estructura de seguridad se diseña para brindar una mayor restricción a la organización, ya que impide que se pueda acceder libremente al servidor desde el interior de la red corporativa, así como también protege al servidor de las intrusiones externas (desde Internet).

Existen versiones de proxy caché, que también brindan servicios a otras aplicaciones que no son necesariamente web; en ese caso, se llaman proxy socks, ya que realizan el redireccionamiento de

PROPIEDADES DE PROXY CACHÉ

Las propiedades de un **servidor de proxy caché** son: permite navegar por internet sin necesidad de consumir direcciones públicas IPv4; permite aumentar el nivel de seguridad, pero solo en un servicio en particular; es vulnerable a ataques informáticos DOS/DDOS; aumenta las necesidades de control para evitar fraudes desde la red interna; disminuye las capacidades de los atacantes para conocer la topología de la red privada y permite manejar el ancho de banda consumido en la navegación por internet.

protocolos y puertos hacia los servidores destino. El funcionamiento es similar, aunque no pueden cachearse los datos para volver a brindarlos.

La evolución del servicio proxy continúa en la actualidad, permitiendo no solo una navegación segura, sino también una administración de recursos para optimizar su utilización.

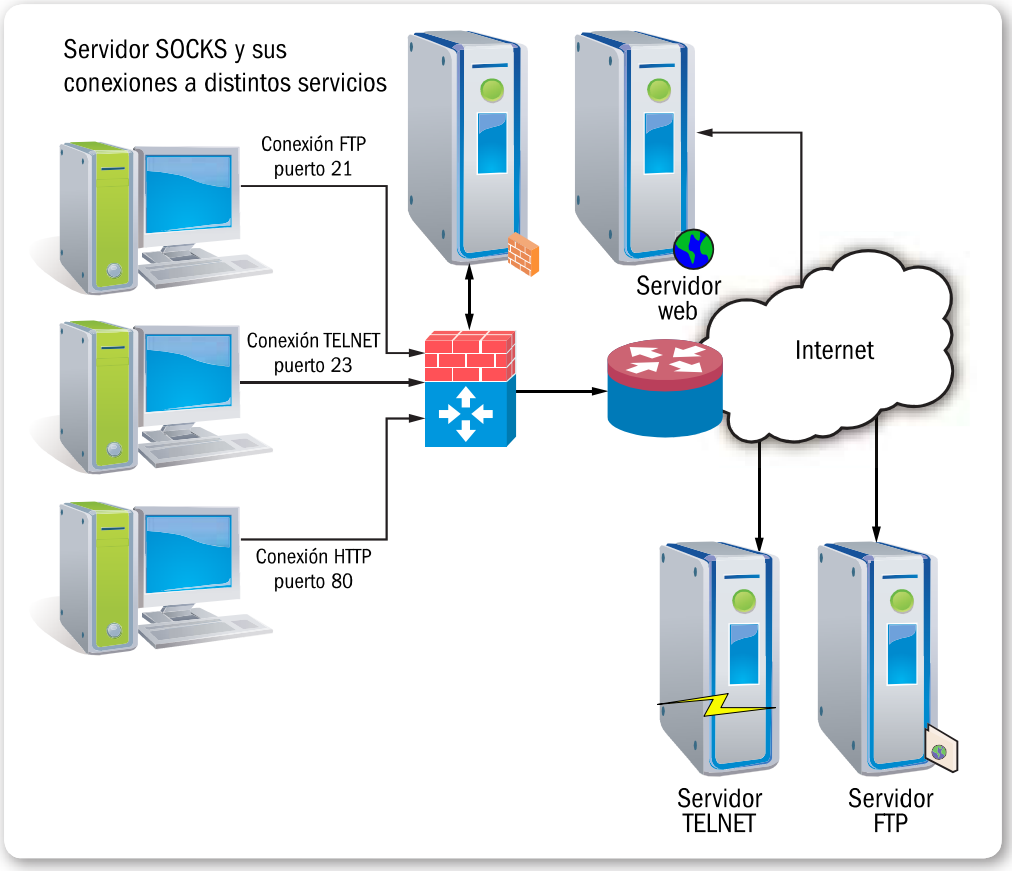


Figura 23. Esquema del proxy socks para conexiones a través de otros servicios IP.

USAR KERBEROS

Si decide usar Kerberos en su red, debe darse cuenta de que es una elección algo compleja. Si se transmite cualquier contraseña a un servicio que no usa Kerberos para realizar la autenticación, se corre el riesgo de que el paquete pueda ser interceptado. Así, la red no obtendría ningún beneficio al usar Kerberos. Para asegurar su red con Kerberos, solo debe utilizar las versiones de este protocolo que sean aceptadas por todas las aplicaciones cliente/servidor que envíen contraseñas.

Servidores y protocolos de autenticación

Un **protocolo de autenticación** es un tipo de protocolo encriptado, que tiene el propósito de autentificar entidades, usuarios, computadoras o servidores, que desean comunicarse de forma segura y de acuerdo con una serie de pasos establecidos.

> EL PROCESO DE AUTENTICACIÓN ES UN COMPONENTE CRÍTICO EN LA ACTIVIDAD DE LA PC

Consideremos que los protocolos de autenticación se negocian inmediatamente después de determinar la calidad del vínculo y antes de negociar el nivel de red. El proceso de autenticación es un componente crítico en la actividad de la computadora. Los usuarios no pueden realizar muchas funciones en una red de computadoras o en Internet sin autenticarse antes en el servidor.

La tarea de acceder a una computadora individual o a un sitio web requiere un protocolo de autenticación confiable para ejecutar un proceso de fondo y establecer la verificación del usuario. Una variedad de protocolos están en uso activo por parte de muchos servidores por el mundo, en diferentes situaciones cotidianas.

Figura 24. Un típico caso es el nombre de usuario y contraseña en Windows, mediante una autenticación RADIUS.

Protocolos

En este momento es importante realizar la separación de los protocolos de autenticación, ya que no son los mismos protocolos los que se usan para autenticarse en Windows, para la conexión remota, o para establecer un VPN o, incluso, medios físicos (métricos, eléctricos, biométricos). Algunos protocolos son los siguientes:

- **PAP**: protocolo de autentificación de contraseña.
- **CHAP**: protocolo de autentificación por desafío mutuo.
- **SPAP**: protocolo de autentificación de contraseña de Shiva.
- **MS-CHAP** y **MS-CHAP v2**: protocolo de autentificación por desafío mutuo de Microsoft (variantes de CHAP).
- **EAP**: protocolo de autentificación extensible.
- **Diameter**: protocolo para conexión por línea conmutada o RTC.
- **Kerberos**: protocolo de autenticación de usuario/contraseña.
- **NTLM**: protocolo de autenticación utilizado en redes Microsoft.
- **PEAP**: protocolo de autenticación extensible protegido.
- **RADIUS**: protocolo de autenticación, administración y autorización.
- **TACACS**: protocolo de autenticación remota.
- **TACACS+**: se trata de un protocolo de autenticación remota que no presenta compatibilidad con TACACS.

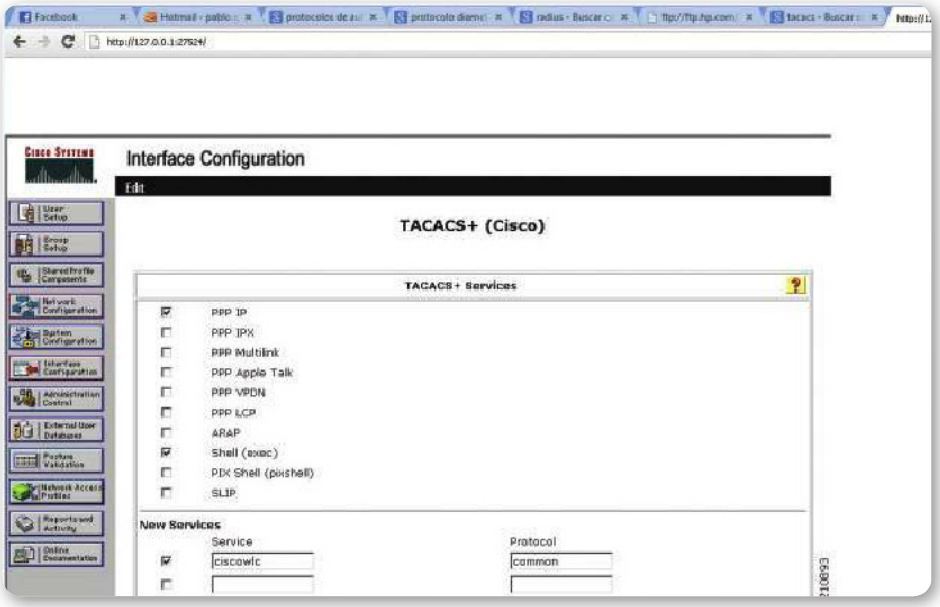


Figura 25. El protocolo TACACS es propietario de Cisco, y muy usado en redes Unix.

Protocolos más difundidos

A continuación, vamos a referirnos a los tres protocolos más difundidos: RADIUS, Diameter y TACACS.

Empezaremos por **RADIUS** (*Remote Authentication Dial In User Service*). Es un protocolo **AAA** (Autenticación, Autorización y Administración); este protocolo es usado por los ISP. Es requerido para que se ingrese y se conecten los usuarios usando un nombre y contraseña.

TACACS PROVEE UNA UBICACIÓN CENTRALIZADA AAA PARA DISPOSITIVOS CISCO

Una vez que los datos han sido escritos, la información pasa por un dispositivo **NAS** (*Network Access Server*) sobre un protocolo de capa de enlace y, luego, hacia un servidor RADIUS sobre un protocolo RADIUS.

Figura 26. En esta imagen, vemos la sección de autenticación de un router Speedy.

El servidor RADIUS chequea que esa información sea correcta usando esquemas de autentificación como **PAP**, **CHAP** o **EAP**. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP y parámetros L2TP. Además de esto, RADIUS nos provee de diferente información, como el inicio de sesión del usuario, la finalización de sesión del usuario, el total de paquetes transferidos

durante la sesión, el volumen de datos transferidos durante la sesión y la razón para la terminación de la sesión.

Por otro lado, el **Diameter** es un protocolo que se usa para las personas y los servicios que se conectan de manera remota a Internet a través de una línea conmutada o RTC. También, según el caso, provee de servicios de autorización y auditoría para aplicaciones, como por ejemplo, acceso de red o movilidad IP. El concepto básico del protocolo Diameter, cuyo desarrollo se ha basado en el protocolo RADIUS, es proporcionar un protocolo que esté diseñado tanto para trabajar de una manera local como en un estado de alerta, sondeo y captura, que le permite ofrecer servicios móviles, dinámicos, flexibles y versátiles.

Por último vamos a hablar del **TACACS**. Un servidor TACACS provee una ubicación centralizada AAA para dispositivos **Cisco**. La autenticación de los usuarios se puede realizar de dos formas: con la base de datos local del dispositivo o con el servidor TACACS. El modelo TACACS provee funcionalidades adicionales tales como la autorización de comandos específicos según el usuario además de un registro histórico detallado de los accesos a los dispositivos y los comandos ejecutados. Para este protocolo, debemos tener en cuenta aspectos como los archivos de configuración y la validación de usuarios.

Diferencias

A simple vista, no parece haber mucha diferencia entre TACACS y RADIUS, pero a grandes rasgos las diferencias son las siguientes: TACACS utiliza TCP mientras RADIUS utiliza UDP, RADIUS encripta solo las contraseñas en el paquete de respuesta al acceso mientras que TACACS+ encripta el cuerpo completo del paquete, y, por último, a diferencia de TACACS+, RADIUS no permite al usuario el control de los comandos que pueden ser ejecutados.

SELECCIÓN DEL PROTOCOLO

La elección del protocolo depende de lo que busquemos a la hora de hacer más segura la conexión y la forma en que se conectan los usuarios, además de estar acorde a la infraestructura y compatibilidad con programas y dispositivos. El más usado es RADIUS, pero no se trata del más seguro.

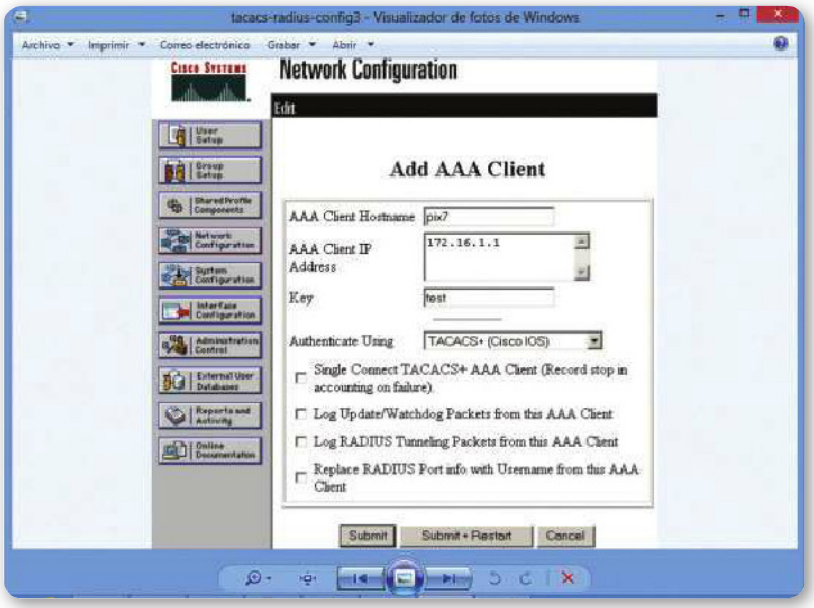


Figura 27. La configuración de TACACS es amigable al administrador y se configura por interfaz gráfica o línea de comando.

Protocolo Kerberos

Kerberos es un protocolo de validación e identificación usado en muchos sistemas para comprobar la identidad del usuario o de la máquina. Un servidor **Kerberos** se denomina **KDC** (*Kerberos Distribution Center*); provee de dos servicios fundamentales: el de autenticación (AS, *Authentication Service*) y el de tickets (TGS, *Ticket Granting Service*).

KERBEROS ES UN PROTOCOLO USADO PARA COMPROBAR LA IDENTIDAD DEL USUARIO O MÁQUINA

El primero tiene como función autenticar inicialmente a los clientes y proporcionarles un ticket para comunicarse con el segundo, el servidor de tickets, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece un servicio. Además, el servidor posee una base de datos de sus clientes (ya sean usuarios o programas) con sus respectivas claves privadas, las cuales son conocidas únicamente por dicho servidor y por el cliente al que pertenece.

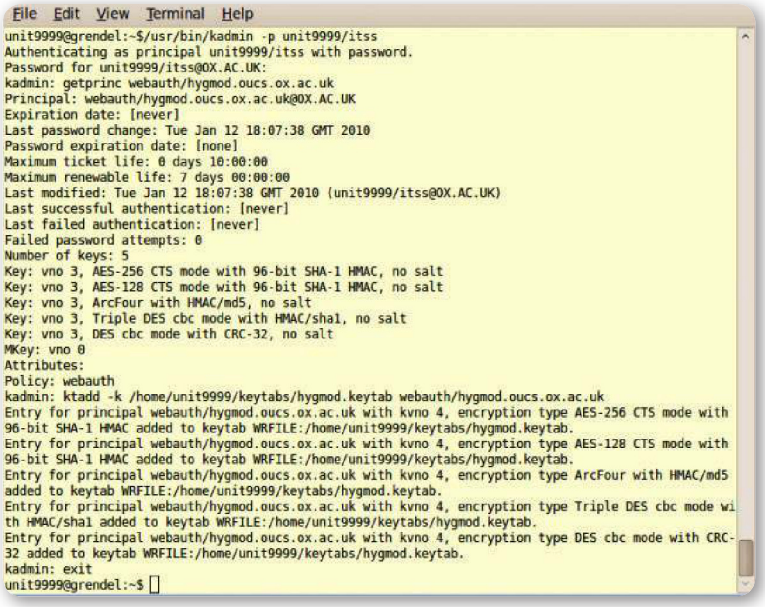


Figura 28. Necesita mucha lectura y prueba y error configurar Kerberos para su correcto funcionamiento.

Arquitectura

La arquitectura de Kerberos está basada en tres objetos de seguridad: **Clave de Sesión**, **Ticket** y **Autenticador**. La clave de sesión es una clave secreta generada por Kerberos y entregada a un cliente para su uso con un servidor durante una sesión; no es obligatorio utilizarla en toda la comunicación con el servidor, solo si el servidor lo requiere (porque los datos son confidenciales) o si el servidor es un servidor de autenticación. Se suele denominar a esta clave **KCS.**

Las claves de sesión se utilizan para minimizar el uso de las claves secretas de los diferentes agentes: estas últimas son válidas durante mucho tiempo, por lo que es conveniente, para minimizar ataques, utilizarlas lo menos posible.

Es importante mencionar que el Ticket es un testigo entregado al cliente para solicitar los servicios de un servidor; garantiza que el cliente ha sido autenticado en forma reciente.

Kerberos siempre proporciona el ticket ya cifrado con la clave secreta del servidor al que se le entrega.

El Autenticador es un testigo construido por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación; solo puede ser utilizado una vez.

Instalación

En este apartado, vamos a ver la instalación en GNU/Linux. Para configurar un servidor Kerberos básico, seguimos las indicaciones proporcionadas a continuación.

En primer lugar, nos aseguramos de que tanto el reloj como el DNS funcionen correctamente en todas las máquinas servidores y clientes antes de configurar **Kerberos 5**. Debemos poner atención a la sincronización de la hora entre el servidor Kerberos y sus clientes; si la sincronización de los relojes del servidor y de los clientes se diferencia en más de cinco minutos (la cantidad predeterminada es configurable en Kerberos 5), los clientes de Kerberos no podrán autentificarse al servidor.

> ANTES DE INSTALAR KERBEROS DEBEMOS VERIFICAR QUE EL RELOJ Y DNS SEAN CORRECTOS

La sincronización de los relojes es necesaria para evitar que un intruso use un ticket viejo de Kerberos para hacerse pasar como un usuario autorizado.

Se recomienda configurar una red cliente/servidor compatible con **Network Time Protocol** (NTP) aun si no está usando Kerberos. **Red Hat Enterprise Linux** incluye el paquete **ntp** para este propósito.

Instale los paquetes **krb5-libs**, **krb5-server**, y **krb5-workstation** en una máquina dedicada que ejecutará el KDC. Esta máquina tiene que ser muy segura; si es posible, no debería ejecutar ningún otro servicio excepto KDC. Si desea usar una utilidad de interfaz gráfica para administrar Kerberos, instale el paquete **gnome-kerberos**. Este contiene **krb5**, que es una herramienta tipo GUI para manejar tickets.

Los archivos de configuración se encuentran en **/etc/krb5.conf** y **/var/kerberos/krb5kdc/kdc.conf**; en ellos, debemos reflejar las opciones que corresponden a nuestra implementación de seguridad. Tengamos en cuenta que se puede construir un reino simple sustituyendo las

FUNCIONAMIENTO DE KERBEROS

El funcionamiento de Kerberos puede ser resumido de la sigueinte forma: en primer lugar el cliente se autentica a sí mismo contra el AS, de esta forma demuestra al TGS que está autorizado para recibir un ticket de servicio, luego puede demostrar al SS que ha sido aprobado para usar el servicio kerberizado.

instancias de **EXAMPLE.COM** y **example.com** con el nombre correcto del dominio —siempre y cuando se respete el formato correcto de los nombres escritos en mayúscula y en minúscula— y se cambie el KDC del **kerberos.example.com** con el nombre de su servidor Kerberos.

En general, los nombres de reinos se escriben en mayúscula, y los nombres DNS de host y nombres de dominio se escriben en minúscula.

Para continuar, es necesario que realicemos la creación de la base de datos usando **kdb5_util** desde el intérprete de comandos, escribiendo lo siguiente: **shell:/usr/kerberos/sbin/kdb5_util create–s.**

El comando **create** genera la base de datos que será usada para almacenar las llaves para el reino Kerberos. La opción **-s** fuerza la creación de un archivo en el cual la llave maestra del servidor es guardada. Si no se presenta un archivo desde donde leer la llave, el servidor Kerberos (**krb5kdc**) le pedirá al usuario que ingrese la contraseña maestra del servidor (la cual puede ser usada para regenerar la llave) cada vez que arranca.

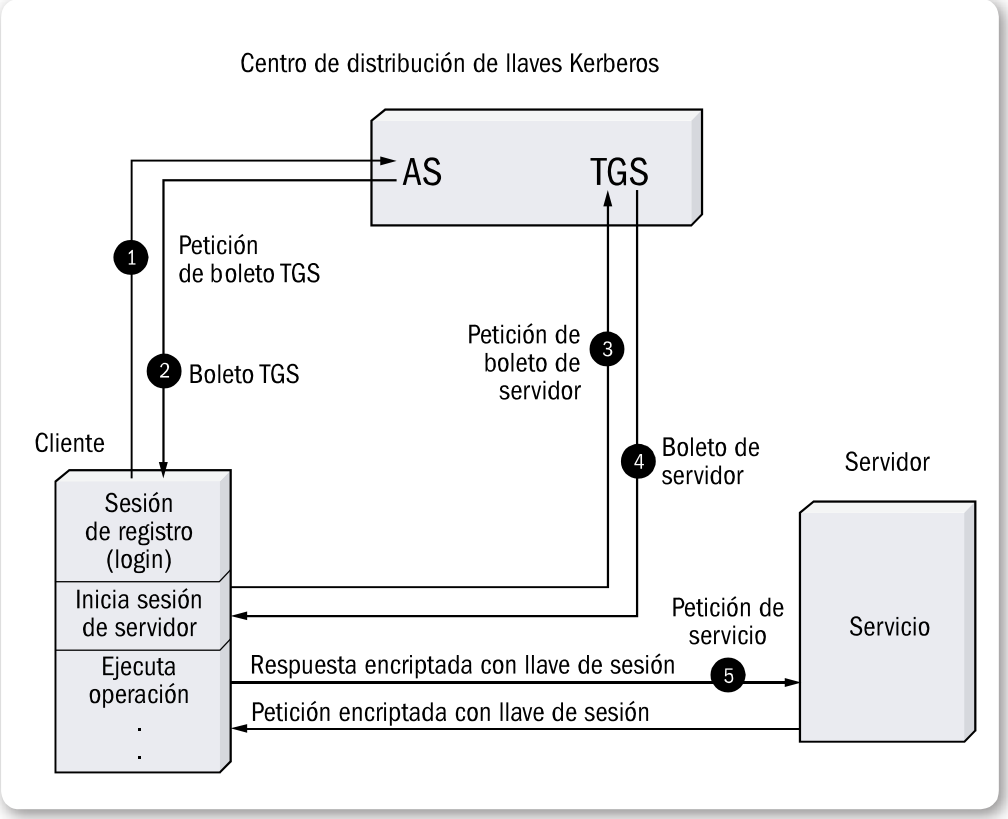


Figura 29. Este diagrama nos muestra la forma en que funciona Kerberos y cómo se comunica.

Luego, modificamos el archivo **/var/kerberos/krb5kdc/kadm5.acl**. Este archivo es usado para determinar los accesos administrativos a la base de datos Kerberos. La mayoría de las organizaciones pueden resolverse con una sola línea:***/admin@EXAMPLE.COM***. De igual forma, la mayoría de los usuarios serán presentados en la base de datos por un principal simple (con una instancia **NULL**, o vacía, tal como **joe@EXAMPLE.COM**). Con esta configuración, los usuarios con un segundo principal con una instancia de **admin** (por ejemplo, **joe/admin@EXAMPLE.COM**) podrán tener todo el acceso sobre la base de datos del reino Kerberos.

Una vez que se arranca **kadmin** en el servidor, cualquier usuario puede acceder a sus servicios ejecutando **kadmin** en uno de los clientes o servidores en el reino. Sin embargo, solamente los usuarios que aparecen en la lista del archivo **kadm5.acl** podrán modificar la base de datos, excepto por sus propias contraseñas. Escribimos el comando **kadmin.local** en una terminal KDC para crear la primera entrada como usuario principal:

```
/usr/kerberos/sbin/kadmin.local -q "addprincusername/admin"
```

Arrancamos Kerberos usando los siguientes comandos:

```
/sbin/service krb5kdc start
;/sbin/servicekadminstart;/sbin/service krb524 start
```

Agregamos principales para sus usuarios con el comando:

```
addprinc
kadmin.
```

Verificamos que el servidor KDC esté creando tickets. Primero, ejecutamos **kinit** para obtener un ticket y guardarlo en un archivo de credenciales caché. Luego, usamos **klist** para ver la lista de credenciales en su caché y **kdestroy** para eliminar la caché y las credenciales que contenga.

Para que exista compatibilidad con entornos distintos, entre Windows y Linux por ejemplo, solo hace falta activar características de Windows o roles de acuerdo a su versión, así, en Windows 2008 hay que activar e instalar **Active Directory Rights Management Services** (AD RMS) con la autenticación Kerberos. En Windows 7 y Windows 8, vamos a **Directivas del grupo local**, accedemos a **Configuración de Windows/Configuración de seguridad/Opciones de seguridad y seguridad en redes/Configurar tipos de cifrado permitidos por Kerberos.**

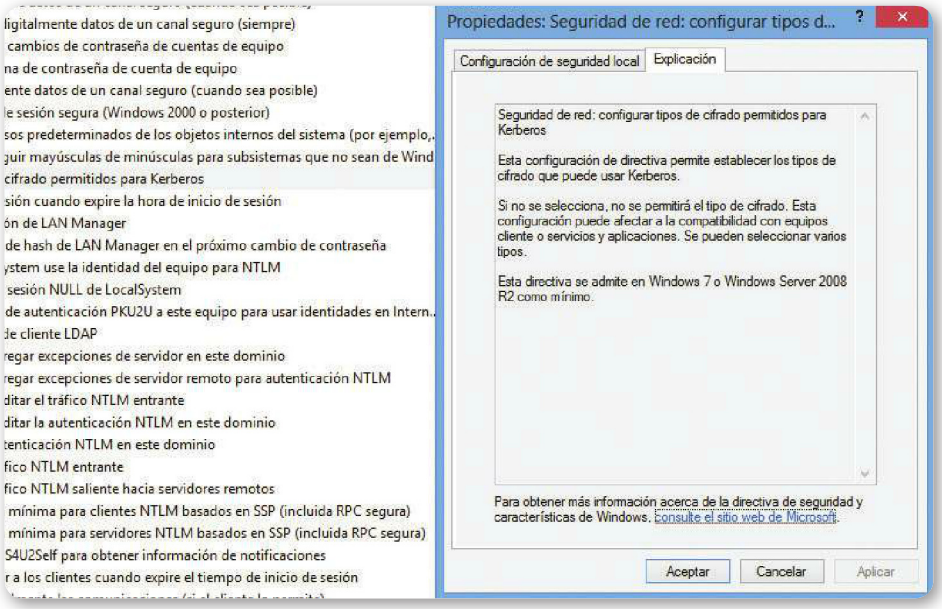


Figura 30. Desde Windows 7, 2008 y 2008 R2 se encuentra la directiva local de asignación.

Técnica Evilgrade

Evilgrade es un framework modular que permite realizar la intrusión en sistemas cuyas implementaciones son débiles en cuanto a la autenticación de fuentes. Fue creado alrededor del año 2007 por el especialista en seguridad informática Francisco Amato. Está basado en programación PERL, pero podemos portarlo a cualquier lenguaje.

Básicamente se trata de una técnica utilizada para ataques informáticos con la que podemos realizar otro tipo de irrupciones de penetración profunda tales como acceso interno a DNS, arrebatamiento de ARP, envenenamiento de DNS, sustitución TCP, entre otros.

Funcionamiento

Este framework permite trabajar en forma modular, y cada módulo del sistema actúa en forma independiente. La vulnerabilidad la encontramos en el fabricante del producto de software y, para comprobarlo, solo hay que obtener la distribución para Linux de Evilgrade, disponible actualmente en una gran cantidad de sitios en

Internet, y comenzar a realizar las pruebas de penetración desde nuestra consola; hasta es posible modificar su código fuente para realizar tareas más puntuales.

Entre el software más conocido con vulnerabilidad, está la familia de productos **Adobe**, **Microsoft**, **VMWare**, **VirtualBox**, entre otros.

El framework es de sistema operativo cruzado, razón por la cual puede ejecutarse bajo casi cualquier SO, ya que depende más del software cliente y de las medidas de autenticación del servidor.

Figura 31. Evilgrade en acción, en una distribución de Bug Track Linux, un set de herramientas de seguridad informática muy popular entre la comunidad hacker y cracker.

Problemas y soluciones

Entre las posibles soluciones, está implementar un certificador de servidores por IP-MAC address. En este caso, un servidor de actualizaciones intermedio entre el servidor público y la red privada realiza una autenticación del origen de la conexión de aviso para el upgrade. Esta técnica de firewall es muy complicada de llevar a cabo, ya que depende mucho de la información que brinde el proveedor, y requiere de muchos recursos humanos para poder administrarla.

Del lado de los proveedores de software, se está llevando a cabo una incesante búsqueda de métodos de autenticación robustos tales como

la aplicación de autenticación hash; pero no se han tenido resultados esperanzadores (el hash también puede ser simulado por Evilgrade).

Desde su aparición en 2007 (en forma oficial), Evilgrade fue y sigue siendo un problema para los analistas de seguridad informática debido a la compleja tarea que se necesita para tratar de detener esta vulnerabilidad desde afuera de las organizaciones que son propietarias.

> EVILGRADE FUE PRESENTADO EN LA EKOPARTY ARGENTINA, EN EL AÑO 2007

Sin embargo, esta vulnerabilidad se vio potenciada por otra de Dan Kaminsky a nivel de los servidores DNS, y es que, antes de esta novedad, el ataque por Evilgrade a lo sumo podía darse en forma local; con la vulnerabilidad de Kaminsky, el proceso se extendió a Internet en 2008.

Desde ese entonces y hasta ahora, han aparecido multitud de parches de seguridad para los servidores vulnerables al bug Kaminsky, lo cual disminuye en gran parte la técnica de EG (Evilgrade).

Desde la otra vereda, tenemos un set de herramientas de intrusión que utiliza Evilgrade como plataforma de lanzamiento, así como también varias *Intruders Tools* (ITS) que automatizan el proceso; incluso, se habla de virus que utilizarían un set de herramientas entre las cuales se encuentra EG, para poder infectar otras máquinas.

RESUMEN

En este capítulo revisamos alternativas de servidores adicionales que es necesario tener en cuenta para nuestra red de datos, conocimos el funcionamiento de los servidores de backup y entregamos algunas recomendaciones de aplicaciones y consejos para administrarlos. Vimos el funcionamiento de los servidores de actualización y de los servidores de antivirus. Por otra parte conocimos los servidores proxy y vimos algunos protocolos de autenticación importantes.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice a un servidor de backup.
2. Mencione las etapas de una estrategia de copias de seguridad.
3. ¿Cómo podemos catalogar las copias de seguridad?
4. ¿Qué soportes podemos utilizar para los backups?
5. ¿Qué es un servidor de actualización?
6. ¿Para qué sirve un servidor de antivirus?
7. ¿Qué es **Microsoft Forefront EndPoint Protection**?
8. ¿Qué es un servidor **proxy**?
9. ¿Qué significa **proxy caché**?
10. ¿Cuáles son las ventajas y desventajas de un servidor **proxy**?

EJERCICIOS PRÁCTICOS

1. Implemente una estrategia de copias de seguridad.
2. Configure un servidor de actualización en GNU/Linux.
3. Instale un servidor de antivirus en Windows.
4. Descargue e instale **Bitdefender**, configúrelo mediante **Management Server**.
5. Instale un servidor proxy en Windows.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*08

Aspectos legales para el administrador

En este capítulo conoceremos los aspectos legales importantes, los alcances y también las formas de atenuar la responsabilidad civil del administrador de redes.

La responsabilidad del administrador de la red

Tener **responsabilidad** significa que, en caso de que se produzca algún daño, será él quien deba repararlo. Y si se tratase de un **delito**, entonces también podría ser el administrador quien, además de la eventual reparación civil, deba cumplir la condena correspondiente.

Como veremos, la particular situación en la que se encuentra el administrador de la red determina que su responsabilidad, en algunos casos, no se limite a sus propias acciones. En efecto, podría ser responsable por acciones de la empresa titular de la red que administra o, incluso, de los usuarios de dicha red.

Debemos saber que la responsabilidad civil tiene como principal finalidad reparar un daño. El daño se repara, en primer término y si esto fuera posible, volviendo las cosas al estado anterior a que ocurriera la acción que causó el daño.

Ahora bien, si esto no fuera posible, entonces se procura resarcir a la víctima del daño, de modo de compensar de algún modo la lesión que ha sufrido en sus bienes o sentimientos.

Es decir, se trata de una **responsabilidad patrimonial**. Es por eso que en el ámbito de la responsabilidad civil no rigen las estrictas normas de interpretación, por lo que son válidas las interpretaciones analógicas o extensivas, y actualmente, el Derecho Civil tiene un enfoque más basado en la **víctima** que en el hecho en sí.

Figura 1. La responsabilidad civil es de contenido patrimonial. Su finalidad es resarcir a la víctima.

En este contexto, ante todo, debemos establecer una distinción para el caso del administrador de la red que es **empleado**, respecto del que es un **contratista independiente**.

El administrador de la red empleado

Respecto del administrador que es empleado de la empresa titular de la red, su responsabilidad civil frente a terceros se encuentra sustancialmente acotada.

En efecto, en términos generales, las legislaciones de los distintos países establecen que el empleador debe responder civilmente por las acciones de sus empleados. Por lo tanto, cuando el administrador de la red es empleado, si alguna de sus acciones (u omisiones) causara un daño a terceros, dichos terceros seguramente demandarían a la empresa para la cual trabaja el administrador, y no a este último. Más aún, en algunos casos, la normativa podría impedir que se demandara directamente al administrador cuando este sea dependiente.

Figura 2. La empresa debe responder civilmente por las acciones de sus empleados.

Sin embargo, en este escenario, la responsabilidad que se ve acrecentada es la del administrador respecto de la empresa para la que trabaja. Porque si bien dicha empresa será responsable frente

a los terceros, luego podrá reclamar civilmente al administrador para recuperar lo que hubiera pagado (además, por supuesto, del eventual despido que podría disponerse en el ámbito laboral).

El administrador de la red como contratista independiente

LA RESPONSABILIDAD CIVIL DEL CONTRATISTA ES BASTANTE AMPLIA

En el caso del administrador de la red que no es empleado sino contratista independiente, su responsabilidad civil es amplia, tanto respecto de los terceros que pudieran resultar damnificados, como de la empresa titular de la red. Además, tengamos en cuenta que si el administrador de la red tuviera, a su vez, empleados, también es responsable por los actos de estos.

A continuación, analizaremos los presupuestos de la responsabilidad civil y cómo se aplican al administrador de la red.

Presupuestos de la responsabilidad civil

Es importante saber que para que exista responsabilidad civil deben darse los siguientes presupuestos:

1. Daño.
2. Antijuridicidad.
3. Factor de atribución.
4. Nexo de causalidad.

El daño

El **daño** es la lesión en los bienes (daño material) o en los sentimientos (daño moral) de una persona. Es el primer presupuesto

de la responsabilidad civil, por esta razón, debemos tener en cuenta que si no hay daño, tampoco existe la responsabilidad civil.

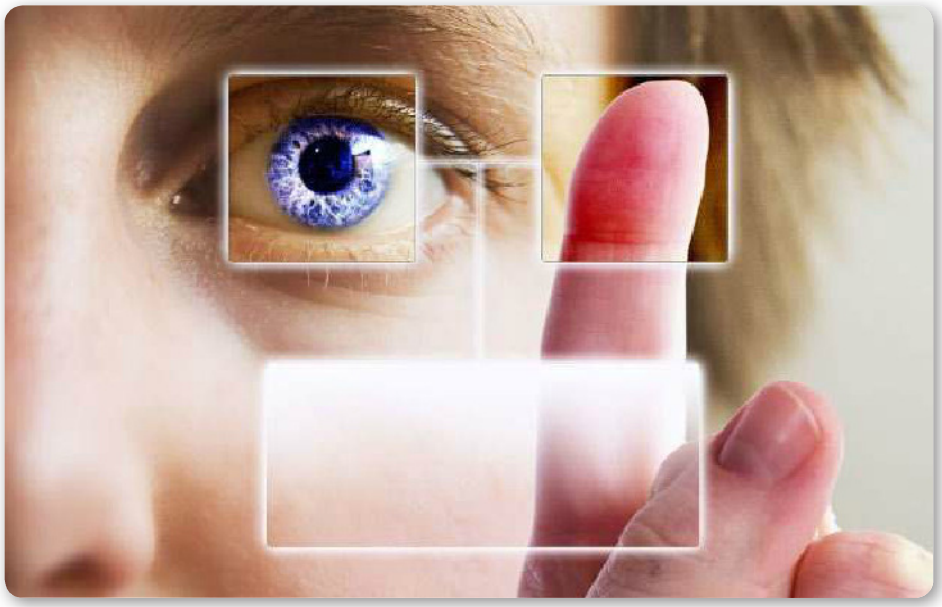


Figura 3. El daño no necesariamente debe ser físico. También puede ser emocional.

La antijuridicidad

El segundo presupuesto es la **antijuridicidad** de la acción. Esto significa que la conducta de quien causa el daño debe ser **ilegítima.**

Figura 4. La conducta dañosa debe ser ilegítima.

Ahora bien, es importante destacar que el concepto de antijuridicidad ha ido cambiando a lo largo del tiempo, y en la

actualidad no se requiere que la acción sea ilegítima en sí, sino que basta con que sea **reprochable**. A modo de ejemplo, la conducta del administrador de una red que ha omitido instalar la actualización de un programa de seguridad no es, en sí misma, una conducta ilegítima, pero sí es reprochable. Y esto alcanza para que esté cumplido el requisito de antijuridicidad.

El factor de atribución

El tercer presupuesto de la responsabilidad civil es el denominado **factor de atribución**. Se trata del fundamento por el cual se responsabiliza a quien realizó la conducta reprochable.

Este puede ser **subjetivo**, es decir, basado en la **culpa**; u **objetivo**, basado en el **riesgo** u otra circunstancia que resulta independiente de la voluntad de quien realiza la acción.

Figura 5. Hay quienes sostienen que la actividad informática es peligrosa y, por lo tanto, la responsabilidad debe ser objetiva.

BUSCADORES DE INTERNET

Hace poco tiempo, Google fue condenado civilmente en la Argentina por la existencia de contenidos agraviantes subidos por terceros, aplicando el factor objetivo de atribución. Esta condena generó mucha preocupación en las empresas de internet.

En materia de responsabilidad civil, el factor de atribución tradicional era subjetivo, basado en la culpa. Es decir, una persona tendría que responder civilmente únicamente si había existido un obrar **negligente**, **imprudente** o mediando **impericia** de su parte.

Ahora bien, con el desarrollo de la tecnología, el factor de atribución subjetivo comenzó a resultar insuficiente. En efecto, esto quedó en evidencia con la generalización del uso de los automóviles, porque existían casos en los cuales, a pesar de no existir culpa por parte del dueño del automóvil, se generaba un daño a un tercero. Y en estos casos, el sistema basado en el factor de atribución subjetivo no brindaba una solución justa para las víctimas. Fue entonces que se pensó en un factor de atribución distinto, **objetivo**, basado originalmente en el **riesgo**. El razonamiento fue el siguiente: quien introduce en la sociedad un elemento riesgoso, como lo es el automóvil, debe responder civilmente por los daños que este pueda causar.

> EL FACTOR DE ATRIBUCIÓN SUBJETIVO SE PRESENTA COMO INSUFICIENTE

El nexo de causalidad

Por último, resta mencionar el **nexo de causalidad**. Este presupuesto de la responsabilidad civil exige que exista una relación directa entre la conducta y el daño. Es decir, el daño debe haber sido causado como consecuencia de la conducta.

Siguiendo con el ejemplo que dimos respecto de la conducta reprochable, si como consecuencia de la falta de actualización del programa de seguridad por parte del administrador de la red, un hacker ingresara y generara algún daño a la información de los

CUANTIFICACIÓN DE LOS DAÑOS

Es importante señalar que los daños informáticos son muy difíciles de cuantificar. Por ejemplo en el caso de que exista una sustracción ilegítima de información, como puede ocurrir mientras administramos una red de datos, debe tenerse en cuenta cuánto dinero dejó de ganar la víctima y, por otra parte, cuánto pudo haberse enriquecido el autor del hecho.

usuarios, existiría un claro nexo de causalidad entre la conducta del administrador y el daño ocasionado. Si el administrador de la red hubiera actualizado el programa de seguridad, el hacker no habría entrado y, por lo tanto, el daño no se hubiera causado.

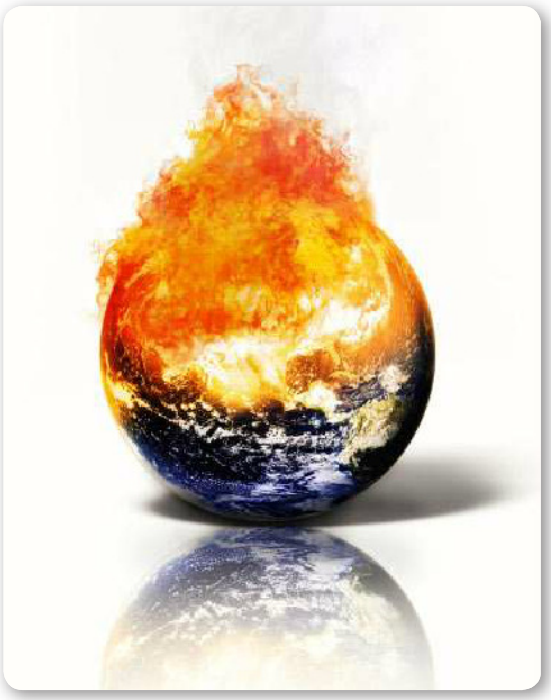


Figura 6. El daño debe ser consecuencia de la conducta antijurídica: sin esa conducta no hubiera habido daño.

Resumen sobre los presupuestos de la responsabilidad civil

A continuación, detallamos las principales características de los presupuestos de la responsabilidad civil que explicamos en este capítulo.

EL CONCEPTO DE CASO FORTUITO

Consiste en un evento que impide el cumplimiento de la obligación y que no ha podido preverse o que, previsto, no ha podido evitarse. Un ejemplo de esto podría ser un terremoto o un tsunami, que interrumpen las comunicaciones en una red.

PRESUPUESTOS DE LA RESPONSABILIDAD CIVIL

PRESUPUESTO	DESCRIPCIÓN
Daño	Para que exista responsabilidad civil debe haberse ocasionado un daño. El daño es la lesión en los bienes o sentimientos de una persona.
Antijuridicidad	La conducta que ocasionó el daño debe ser reprochable. Este criterio se ve atenuado cuando el factor de atribución es objetivo, porque en tal caso, la voluntad de quien realiza la conducta no resulta relevante.
Factor de atribución	Es el fundamento por el cual se responsabiliza a quien realizó la acción reprochable que ocasionó el daño. Puede ser subjetivo, atendiendo a la culpa de la persona que efectuó la acción; u objetivo, atendiendo al riesgo creado.
Nexo de causalidad	Es la relación directa que debe existir entre la conducta reprochable y el daño ocasionado. Este requisito es menos importante cuando estamos ante un factor de atribución objetivo.

Tabla 1. Resumen de los presupuestos de la responsabilidad civil.

Responsabilidad civil aplicable al administrador

Hasta aquí hemos descripto, en términos generales, los presupuestos de la responsabilidad civil. A continuación, nos referiremos, específicamente, al régimen que resulta aplicable al administrador de la red, dejando aclarado que en la actualidad existe una importante discusión sobre la responsabilidad civil en materia tecnológica.

Si como consecuencia de alguna actividad ocurrida en la red se produjera un **daño** (primer presupuesto de la responsabilidad civil), debería analizarse si la responsabilidad por dicho daño puede ser imputada al administrador de la red. Para esto, básicamente, deben repasarse los presupuestos de la responsabilidad civil.

Ante todo, debemos señalar que, desde el punto de vista jurídico, el administrador de la red es un **profesional**. Por lo tanto, su conducta se evaluará con estándares más estrictos que la de cualquier persona que no tenga su nivel de conocimiento.

Para saber si el administrador de la red ha incurrido en una acción **reprochable** (que es el segundo presupuesto de la responsabilidad civil) se analizará su conducta comparándola, en abstracto, con la conducta esperable para un profesional que hubiera estado en la misma situación. Ahora bien, lo más importante para poder evaluar la responsabilidad civil del administrador es determinar si resulta aplicable el factor de atribución subjetivo o, por el contrario, nos encontramos ante un régimen objetivo.

> EL RÉGIMEN DE RESPONSABILIDAD PROFESIONAL ES DE CARÁCTER SUBJETIVO

En este sentido, debemos señalar que, en principio, el régimen de responsabilidad profesional es de carácter **subjetivo**. Es decir, los profesionales en general solo responden cuando han obrado con culpa, y esto sería aplicable al administrador de la red.

Por lo tanto, para eximirse de responsabilidad, el administrador de la red deberá demostrar que actuó con plena diligencia, adoptando todas las medidas que resultaban exigibles, según el estado de la técnica y sus conocimientos específicos, para evitar el daño.

Sin embargo, debemos señalar que en el último tiempo ha surgido una importante corriente de pensamiento, que considera que la actividad informática es una **actividad riesgosa**. Si esto fuera así, entonces el factor de atribución será objetivo, y ya no se tendrá en cuenta si el administrador de la red ha actuado con culpa o no: sería responsable por el solo hecho de ser el administrador de la red de datos en la que se causó el daño.

En este caso, el administrador de la red únicamente podría eximirse de responsabilidad acreditando que:

1. No existe nexo causal entre el hecho y el daño (en nuestro ejemplo, que el daño no se debió a alguna acción ocurrida en la red).
2. Existió culpa de la víctima.
3. Concurre alguna situación de caso fortuito.

Como puede apreciarse, si los tribunales comienzan a adoptar esta idea de que la actividad informática es peligrosa, las contingencias en materia de responsabilidad civil para quienes administren las redes se verán incrementadas sustancialmente.

Por último, siguiendo con nuestro análisis, para verificar si podría existir responsabilidad del administrador de la red, debería analizarse el **nexo de causalidad** entre su conducta y el daño ocasionado.

Con relación a esta última cuestión, la actividad informática muchas veces genera inconvenientes interpretativos. Es que, en el ámbito físico, es mucho más sencillo probar la relación de causalidad que cuando estamos enfocados en el ámbito virtual.

Ejemplos prácticos del análisis de la responsabilidad civil

A continuación, veremos dos ejemplos prácticos respecto de cómo se analizaría la responsabilidad civil en un hecho ocurrido en el mundo físico y, luego, en un hecho ocurrido en el ámbito virtual.

Ámbito físico

El primer ejemplo es sobre algo muy simple y que ocurre a diario. Supongamos que una persona patea una pelota y rompe el vidrio de un vecino. El análisis de su responsabilidad civil es muy sencillo:

1. El **daño** es patrimonial, y consiste en el valor de ese vidrio, más los eventuales perjuicios que pudiera haber ocasionado con su rotura.
2. La **antijuridicidad** está dada por la conducta **reprochable** de haber pateado la pelota sin tener en cuenta las distancias o calculando mal.
3. El **factor de atribución** es **subjetivo** y, en este caso, se basa en la **imprudencia** de quien pateó la pelota.
4. El **nexo de causalidad** claro: si la persona no pateaba la pelota, la pelota no golpeaba el vidrio, y no había daño alguno.

SEGUROS

Es importante mencionar que hasta hace poco tiempo, no era posible asegurar los riesgos derivados de la actividad informática. El seguro es el método más fácil de cobertura en caso de que se decida aplicar la responsabilidad objetiva a la actividad informática.

Ámbito virtual

Ahora, realizaremos el mismo análisis pero referido a la conducta del administrador de una red. El administrador omitió aplicar un parche de seguridad en el sistema de validación de usuarios, que determinó que quienes tuvieran sus computadoras infectadas con un malware determinado vieran comprometidas sus credenciales de acceso a la red:

1. El **daño** consiste en la pérdida de información y/o de la violación de la privacidad de los usuarios que vieron comprometidas sus credenciales de acceso. Corresponderá efectuar la cuantificación de este daño en un tribunal judicial.
2. La **antijuridicidad** está dada por la conducta **reprochable** del administrador de la red, que omitió aplicar el parche de seguridad.
3. El **factor de atribución** es **subjetivo** y, en este caso, se basa en la **impericia** del administrador, que en su condición de profesional, no podía ignorar que debía aplicarse un parche de seguridad.
4. El **nexo de causalidad** no es tan claro, o al menos podría ser cuestionado, porque la realidad es que solo resultaron afectados los usuarios que ya tenían infectadas sus máquinas. Es decir, si esas máquinas no hubiesen estado infectadas con el malware, entonces no habría habido consecuencias negativas de la conducta reprochable del administrador de la red. En este caso, en la relación de causalidad confluyen dos situaciones, una de las cuales es imputable al administrador de la red, pero la otra no.

Estos dilemas con el nexo de causalidad son muy comunes en el ámbito de la tecnología, y muchas veces resultan imposibles de probar (por ejemplo, cuando una computadora falla, a veces no puede determinarse si eso se debió al hardware, al software o a ambos, con lo cual se complica el análisis de la responsabilidad civil).

CADENA DE CUSTODIA DE LOS REGISTROS

Tengamos en cuenta que también en el ámbito civil es importante que el administrador de una red de datos guarde adecuadamente los registros que puedan servir como prueba de su accionar en un pleito. A tal fin, deberá conservar la cadena de custodia de dichos registros.

Limitar la responsabilidad civil del administrador

En este punto nos referiremos a distintas acciones que el administrador de la red debería de tener en cuenta a fin de atenuar o limitar su responsabilidad civil.

Es importante dejar aclarado que enunciaremos estándares de conducta generales, que deberán ser evaluadas en cada caso de acuerdo con la legislación que resulte aplicable. Además, algunas de estas acciones se referirán al administrador de la red que, a la vez, es empleado; mientras que otras estarán dirigidas al administrador de la red que es contratista independiente.

Redactar políticas claras de uso de la red

Sin dudas, la primera acción que resulta recomendable es procurar que la red tenga **políticas claras de utilización**, que deben ser **notificadas** a todos los usuarios, y cuyo cumplimiento debe ser exigido por el administrador de la red.

> DEBEMOS PROCURAR QUE LA RED POSEA POLÍTICAS DE UTILIZACIÓN ESPECÍFICAS

Si el administrador es un empleado de la empresa titular de la red, entonces debería requerir a dicha empresa la redacción de las políticas. En caso de que fuese un contratista independiente, tal vez él mismo debería redactar las políticas. Pero en cualquier caso, la existencia de políticas de uso claras de la red beneficiará la evaluación de las conductas del administrador (de hecho, la inexistencia de políticas evidenciaría, de por sí, una conducta negligente del administrador).

Ahora bien, consideremos lo siguiente ¿qué deben contener estas políticas para que resulten útiles a los fines de demostrar la diligencia del administrador de la red? En términos generales, podemos decir que las políticas deben establecer:

1. Con qué finalidad los usuarios deben utilizar la red, y las limitaciones a su uso, si las hubiera.
2. Qué actividades no se pueden realizar en la red, con el mayor grado de detalle para evitar que pueda entenderse que alguna actividad no estaba prohibida cuando, en realidad, sí lo estaba.
3. Qué facultades de control tiene el administrador de la red, y cuál es el ámbito de privacidad de los usuarios, si lo hubiera (por ejemplo, debería aclararse si el administrador puede acceder a las claves de los usuarios o si no puede hacerlo).
4. Cuáles son las consecuencias de violar las políticas de uso.
5. Debería existir una previsión específica relacionada con los derechos de propiedad intelectual, dado que son los que más comúnmente se violan a través de las redes de computadoras.

Figura 7. Para limitar la responsabilidad del administrador es fundamental la redacción de políticas de uso.

LA FIRMA DIGITAL

La firma digital se presenta como un procedimiento matemático que otorga al documento dos presunciones: de **autoría** (que fue enviado por el firmante) y de **integridad** (que el documento enviado no fue modificado). En algunos países se la denomina **firma electrónica**.

Por otra parte, es fundamental que las políticas sean **notificadas** a los usuarios, de modo tal que quede **alguna constancia** de ello que permita probar ante terceros (por ejemplo, un tribunal) que estas fueron notificadas.

Figura 8. Las políticas de uso deben ser notificadas de un modo que permita probar tal notificación.

En aquellas jurisdicciones en las que se ha implementado la firma digital o electrónica, sería ideal que la notificación de las políticas se realizara con este procedimiento. Y para las jurisdicciones en las que aún no está implementada, deberían al menos conservarse los registros o logs que permitan acreditar la notificación.

Requerir instrucciones escritas para realizar tareas que puedan considerarse violatorias

Esta acción resultará aplicable, sobre todo, a los administradores de redes que son, a su vez, empleados de la empresa titular de la red que administran. Estos administradores muchas veces se encuentran en situaciones complejas, porque no existen normas claras en la empresa

respecto de su actuación, y reciben órdenes que deben cumplir, pero que podrían comprometer su responsabilidad personal. Un ejemplo claro sería el de una auditoría de correos electrónicos u otro tipo de comunicaciones internas.

La violación del correo electrónico es un delito penal, y las empresas no pueden cometer delitos penales. Por lo tanto, si la auditoría pudiera ser considerada un delito, el administrador de la red sería el **autor material** (por lo menos, en principio) de dicho delito. Entonces, si bien entendemos que en el caso de la auditoría no debería haber problemas porque se trataría de correos electrónicos laborales (a los cuales el empleador tiene derecho a acceder), lo cierto es que resultaría conveniente que el administrador de la red tuviera instrucciones escritas de sus superiores antes de realizar tales tareas.

Figura 9. Para resguardar su responsabilidad, es conveniente que el administrador requiera instrucciones por escrito.

CORREO ELECTRÓNICO LABORAL Y DELITO

Algunos juristas sostienen que el empleador no tiene facultades para acceder al correo electrónico laboral sin orden de un juez. Por lo tanto, aun cuando pensemos en sentido contrario, alguien podría formular una denuncia para que un juez definiera el tema.

Es importante aclarar que la instrucción escrita de un superior jerárquico en una empresa no eximirá al administrador de la red de su eventual responsabilidad penal si comete un delito, siempre que este delito se presente como evidente.

Para ejemplificar pensemos en lo siguiente: si la empresa encomienda al administrador que, aprovechando su acceso a información confidencial, monitoree el uso de las cuentas de correo electrónico personal de dichos usuarios, el administrador debería negarse, porque esa conducta constituye un delito penal.

Suscribir acuerdos de confidencialidad con empleados

En este caso, nos referiremos a una acción aplicable a los administradores que no son empleados, sino contratistas independientes. Como vimos, ellos son, a su vez, responsables por las acciones de sus propios empleados. Por lo tanto, resulta conveniente que suscriban con ellos acuerdos específicos de confidencialidad, dado que cualquier filtración de información que pudiera darse por los empleados del administrador será imputable directamente a él.

Figura 10. La suscripción de acuerdos de confidencialidad con sus propios empleados es otra buena práctica.

Cláusulas de limitación de la responsabilidad o acuerdos de indemnidad

Esta acción será útil tanto para el administrador de la red que es empleado como para el que es contratista independiente del titular de la red. Se trata de una acción fundamental porque tiene como finalidad limitar a un monto cierto y previsible la responsabilidad civil asumida por el administrador de la red.

Figura 11. Es importante negociar acuerdos de limitación de responsabilidad para el administrador.

En el caso del administrador que es empleado, es conveniente que requiera la suscripción de un acuerdo de indemnidad con la empresa. En algunos casos, dependiendo de la jerarquía del administrador dentro de la organización, y del tamaño de la organización, estos acuerdos se pueden firmar directamente con los dueños (por ejemplo, los accionistas extranjeros si se trata de una empresa multinacional que tiene una empresa chica en el país). El objeto de estos acuerdos es que la empresa o sus accionistas mantengan indemne al administrador ante cualquier reclamo que pudieran formular terceros por daños y perjuicios. Es decir, si el administrador de la red fuera demandado,

y eventualmente condenado por considerarlo responsable civilmente de algún daño, la empresa (o sus accionistas) pagarían lo que corresponda para liberarlo de toda responsabilidad patrimonial. Es importante aclarar que estos acuerdos de indemnidad solo se refieren a los aspectos patrimoniales de la responsabilidad. Esto significa que, si el administrador de la red fuera imputado por un delito, y eventualmente condenado, **nadie podría sustituirlo** en el cumplimiento de la condena. Lo que suele acordarse para estos casos es que la empresa tomará a su cargo los eventuales gastos de defensa.

En el caso del administrador de la red que es un contratista independiente, resultaría conveniente que, en su contrato con la empresa titular de la red, acordara una cláusula limitativa de la responsabilidad civil.

> NADIE PUEDE SUSTITUIR AL ADMINISTRADOR EN EL CUMPLIMIENTO DE UNA CONDENA

En este sentido, dado que la responsabilidad civil, como dijimos, es de índole patrimonial, casi todas las legislaciones admiten que las partes puedan limitarla en forma libre. Pero no ocurre así, por ejemplo, con la responsabilidad penal, que no podría limitarse.

Entonces, lo que el administrador puede pactar con la empresa titular de la red es que la responsabilidad civil del administrador, por todo concepto, no exceda de un monto determinado. Esta limitación, cabe señalar, solo tendrá efecto entre las partes, lo que significa que terceros podrían demandar al administrador y, entonces, no se aplicaría el tope previsto contractualmente. Para estos casos, podría pactarse, además del límite contractual, una obligación de indemnidad de la empresa hacia el administrador, según la cual la empresa se comprometa a mantenerlo indemne de cualquier reclamo de terceros vinculado a su condición de administrador.

DAÑOS EN MATERIA DE SOFTWARE

En algunos paises no existe un sistema de daños tarifados en propiedad intelectual. Por esta razón, el criterio judicial predominante en materia de daños por distribución ilegítima de software es que la indemnización sea similar al valor de la licencia.

Realizar denuncias ante la evidencia de un delito penal

Por último, es fundamental que el administrador de la red formule las **denuncias pertinentes** al verificar incumplimientos de las políticas de uso de la red o, en su caso, al comprobar la existencia de algún delito.

En el caso de incumplimientos de las políticas de uso de la red, el administrador (ya sea en su condición de empleado o de contratista independiente) debería dar inmediato aviso a la empresa para que esta tome los recaudos que considere. Para resguardar la responsabilidad del administrador, sería conveniente que estas comunicaciones se efectuaran por escrito, de modo tal que puedan probarse.

Figura 12. Si verifica un ilícito en la red, el administrador debe denunciarlo ante sus superiores o la Justicia.

En caso de que el administrador verificase la comisión de algún delito en la red (por ejemplo, si algún usuario está cometiendo delitos contra la propiedad intelectual), si es empleado tendría que informarlo por escrito, recomendando que se realice la correspondiente denuncia

EL CONCEPTO DEL DAÑO PUNITIVO

Debemos considerar que los daños punitivos, que típicamente se presentan en Common Law, tienen como finalidad castigar (y no reparar). Es por eso que las condenas por daños punitivos suelen ser exorbitantes, ya que no guardan relación con el daño en sí.

penal para deslindar las responsabilidades.
Si el administrador trabaja como un contratista independiente, también debería informarlo por escrito, pero si advirtiera que la empresa se muestra permisiva con tales conductas, será necesario que se proceda a evaluar la posibilidad de realizar él mismo, en forma personal, la denuncia penal correspondiente.

> PUEDE SER NECESARIO REALIZAR UNA DENUNCIA PENAL EN FORMA PERSONAL

Esto dependerá, en gran medida, del delito del que se trate, pero podría ocurrir, por ejemplo, que el administrador de la red advierta que algún usuario está distribuyendo pornografía infantil. Si la empresa no hiciera nada al respecto, luego podrían ser todos imputados por facilitar la comisión de ese delito, o bien por encubrirlo.

RESUMEN

En este capítulo hemos aprendido que el administrador de red debe extremar las precauciones a fin de evitar que, ante un evento que pueda provocar daños, se le endilgue responsabilidad por negligencia dado que se trata de la persona responsable de una red. Al mismo tiempo, debe procurar asegurarse de que su responsabilidad civil se encuentre limitada contractualmente.

Actividades

TEST DE AUTOEVALUACIÓN

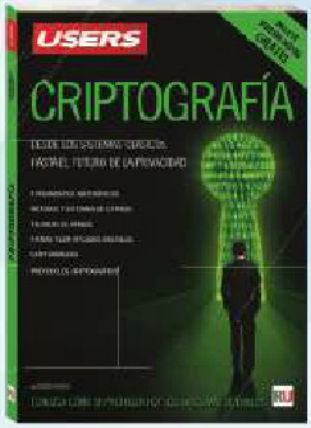
1. ¿Qué significa tener responsabilidad?
2. ¿Qué es la responsabilidad patrimonial?
3. Caracterice al administrador empleado y contratista.
4. ¿Cuáles son los presupuestos de la responsabilidad civil?
5. ¿Qué es el daño?
6. Defina la antijuridicialidad.
7. ¿Qué es el nexo de causalidad?
8. ¿Qué es el ámbito virtual?
9. ¿Cómo podemos generar políticas claras?
10. ¿Qué son los acuerdos de confidencialidad?

EJERCICIOS PRÁCTICOS

1. Defina algunos ejemplos de análisis de responsabilidad civil.
2. Realice un análisis considerando el ámbito físico.
3. Realice un análisis considerando el ámbito virtual.
4. Implemente algunas acciones para limitar la responsabilidad civil.
5. Defina una política clara de utilización.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

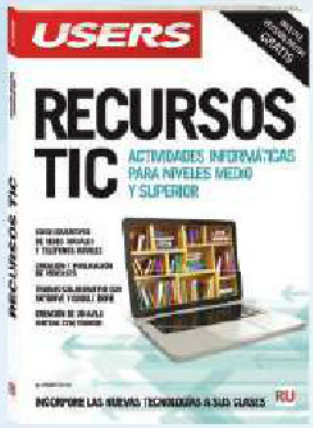


Una obra única que analiza la protección de datos y su evolución, desde la criptografía clásica a los algoritmos modernos.

→ 208 páginas / ISBN 978-987-1949-35-9

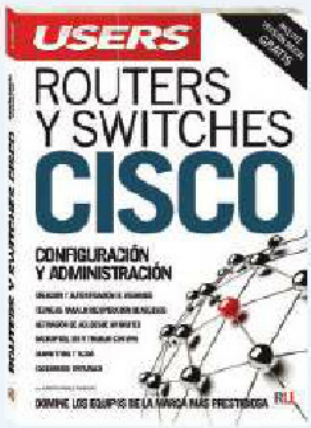
Herramientas, conceptos y consejos fundamentales para la instalación y configuración de redes cableadas e inalámbricas.

→ 320 páginas / ISBN 978-987-1949-46-5



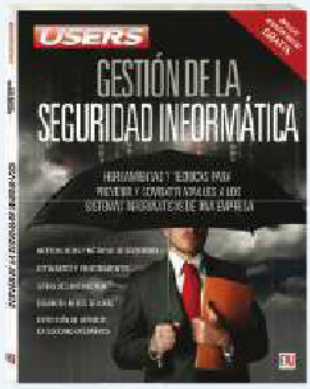
Esta obra invita a reflexionar sobre el lugar que deben ocupar las TICs en las aulas de los niveles Medio y Superior.

→ 320 páginas / ISBN 978-987-1949-33-5



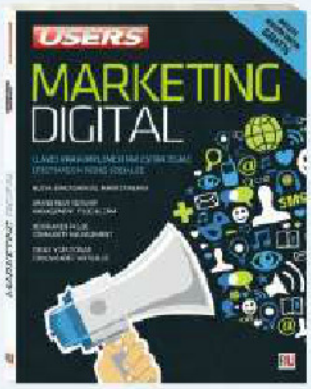
Capacítese para obtener una certificación Cisco y amplíe sus oportunidades laborales en el rubro de las telecomunicaciones.

→ 320 páginas / ISBN 978-987-1949-34-2



Conozca herramientas y técnicas necesarias para prevenir y combatir ataques a los sistemas informáticos de una empresa.

→ 192 páginas / ISBN 978-987-1949-30-4

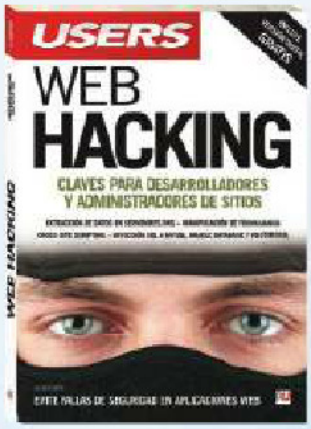


Este libro revela técnicas y herramientas indispensables a la hora de encarar una estrategia de marketing en medios sociales.

→ 192 páginas / ISBN 978-987-1949-32-8

Con los mismos datos, puede obtener resultados muy diferentes: implemente herramientas interactivas de inteligencia empresarial.

→ 192 páginas / ISBN 978-987-1949-29-8

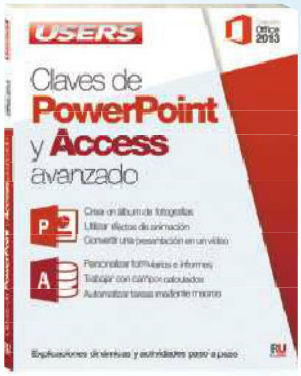


Indispensable para desarrollares y administradores de sitios, este libro explica las técnicas de ataque utilizadas por los hackers.

→ 320 páginas / ISBN 978-987-1949-31-1

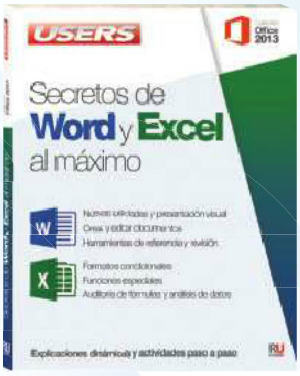
El libro indicado para quienes buscan aprender a confeccionar y administrar bases de datos en Microsoft Access desde cero.

→ 192 páginas / ISBN 978-987-1949-27-4



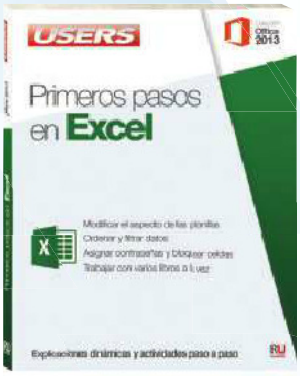
Aproveche la versatilidad de PowerPoint para crear presentaciones y especialícese en el manejo de bases de datos con Access.

→ 192 páginas / ISBN 978-987-1949-28-1



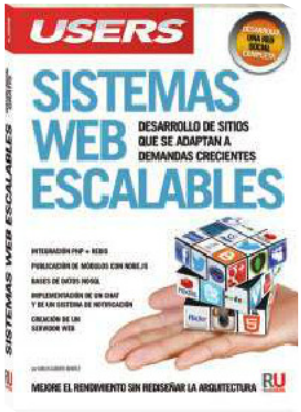
Manténgase actualizado: conozca las nuevas herramientas de Word y trabaje con las funciones avanzadas de Excel

→ 192 páginas / ISBN 978-987-1949-26-7



Aprenda a utilizar Excel 2013 y desarrolle planillas adaptadas a sus necesidades de registro y seguimiento de información.

→ 192 páginas / ISBN 978-987-1949-25-0



Cree su propia red social e implemente un sistema capaz de evolucionar en el tiempo y responder al crecimiento del tráfico.

→ 320 páginas / ISBN 978-987-1949-20-5

Conozca la integración con redes sociales y el trabajo en la nube, en aplicaciones modernas y más fáciles de utilizar.

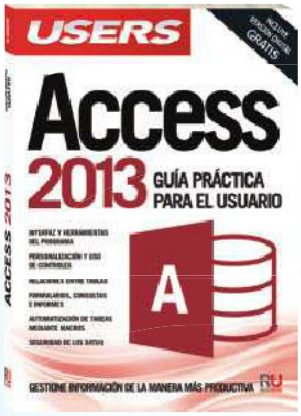
→ 320 páginas / ISBN 978-987-1949-21-2

Conozca claves y herramientas más potentes de esta nueva versión de Excel y logre el máximo de efectividad en sus planillas

→ 320 páginas / ISBN 978-987-1949-18-2

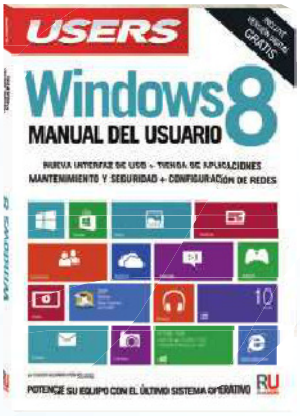
Consejos y secretos indispensables para ser un técnico profesional e implementar la solución más adecuada a cada problema

→ 320 páginas / ISBN 978-987-1949-19-9



Simplifique tareas cotidianas de la manera más productiva y obtenga información clave para la toma de decisiones.

→ 320 páginas / ISBN 978-987-1949-17-5



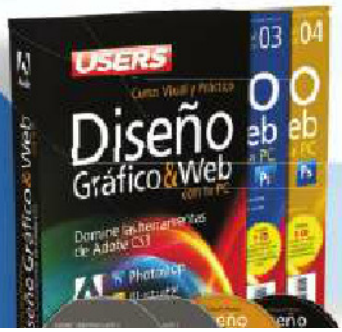
Acceda a consejos indispensables y aproveche al máximo el potencial de la última versión del sistema operativo más utilizado.

→ 320 páginas / ISBN 978-987-1949-09-0

CURSOS

CON SALIDA LABORAL

Los temas más importantes del universo de la tecnología, desarrollados con la mayor profundidad y con un despliegue visual de alto impacto: explicaciones teóricas, procedimientos paso a paso, videotutoriales, infografías y muchos recursos más.



- 25 Fascículos
- 600 Páginas
- 2 DVDs / 2 Libros

Curso para dominar las principales herramientas del paquete Adobe CS3 y conocer los mejores secretos para diseñar de manera profesional. Ideal para quienes se desempeñan en diseño, publicidad, productos gráficos o sitios web.

- 25 Fascículos
- 600 Páginas
- 4 CDs

Obra ideal para ingresar en el apasionante universo del diseño web y utilizar Internet para una profesión rentable. Elaborada por los máximos referentes en el área, con infografías y explicaciones muy didácticas.

Brinda las habilidades necesarias para planificar, instalar y administrar redes de computadoras de forma profesional. Basada principalmente en tecnologías Cisco, busca cubrir la creciente necesidad de profesionales.

- 25 Fascículos
- 600 Páginas
- 3 CDs / 1 Libros

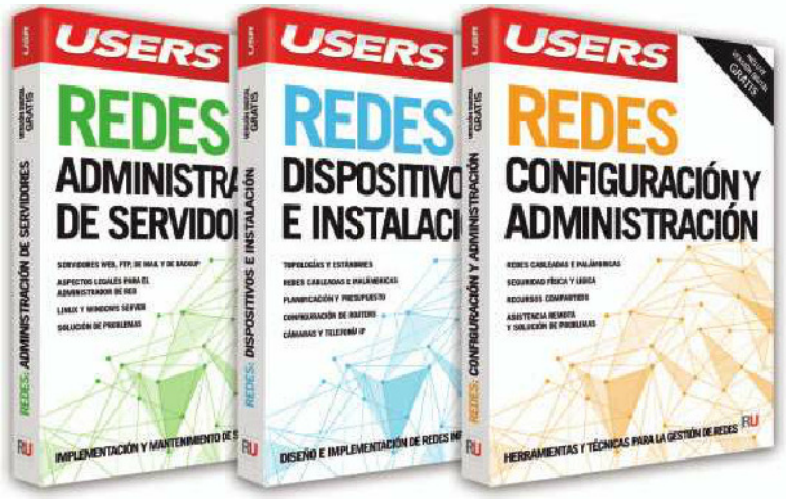
USERS

REDES
ADMINISTRACIÓN DE SERVIDORES

Último volumen de la colección *Redes*, este libro presenta los conceptos y técnicas necesarios para implementar y configurar diversos tipos de servidores en una red de datos. A lo largo de los capítulos se describen las particularidades del hardware de un servidor y se detallan las características y el funcionamiento de los servidores de backup, de actualización, de impresión y de FTP, entre otros. Además, se realiza una distinción entre sistemas Windows y GNU/Linux y se brindan consejos legales y de seguridad para quienes cumplan el rol de administrador de red.

EN ESTE LIBRO ENCONTRARÁ:

Hardware de servidores: componentes internos, tecnología RAID, BIOS Setup y seguridad. / **Windows Server:** características y Active Directory. Derechos y restricciones. / **Sistemas GNU/Linux:** servidores Linux. Comandos de consola. Diagnósticos de red y sistemas de verificación. / **Servidores web y FTP:** funcionamiento, aplicaciones y administración. / **Servidor de correo electrónico:** plataformas y consola de administración. Control de SPAM. / **Servidores de archivos e impresión:** ventajas y administración. Seguridad. Auditoría. / **Servidores adicionales:** servidor de backup, servidor de actualización, servidor de antivirus y servidor Proxy. / **Consideraciones para el administrador:** aspectos legales y ética. Consejos sobre seguridad.



COLECCIÓN REDES

El contenido de esta colección fue publicado previamente en los fascículos del curso visual y práctico *Técnico en redes y seguridad.*

ISBN 978-987-1949-48-9

RU

REDUSERS.com
En nuestro sitio podrá encontrar noticias relacionadas y también participar de la comunidad de tecnología más importante de América Latina.

PROFESOR EN LÍNEA
Ante cualquier consulta técnica relacionada con el libro, puede contactarse con nuestros expertos: profesor@redusers.com.