INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES & SEGURIDAD

20

SERVIDORES DE ARCHIVOS E IMPRESIÓN

En este fascículo aprenderemos a configurar y administrar un servidor de archivos dentro de un sistema Windows y GNU/Linux. También revisaremos las ventajas de establecer un servidor de impresión.

- FILE SERVER EN LINUX Y WINDOWS
- SERVIDOR DE IMPRESIÓN
- POLÍTICAS DE USO
- SEGURIDAD Y AUDITORÍA

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Ventajas y uso de File Servers y Print Servers, las características y la forma en que debemos implementarlos, tanto en sistemas Windows como en distribuciones GNU/Linux.

En la clase anterior, analizamos el funcionamiento de un servidor de correo electrónico; aprendimos a instalarlo y a configurarlo en sistemas operativos Windows y GNU/Linux. Conocimos los peligros del spam y de qué forma se filtra en el servidor; aprendimos a deshabilitar el Open Relay y vimos algunos servicios para obtener cuentas de e-mail temporales. Para terminar, realizamos el análisis de los headers de e-mails.
En este fascículo, comenzaremos conociendo las funciones que desempeña un File Server; luego, aprenderemos a administrarlo en un sistema Windows y también en un sistema GNU/Linux. Veremos las opciones de seguridad y las alternativas de auditoría que es necesario tener en cuenta. Para continuar, conoceremos el funcionamiento de un servidor de impresión, la forma correcta de administrarlo y cómo podemos aumentar su nivel de seguridad, y la forma de realizar algunas tareas de auditoría.

20

Servidor de archivos

¿Qué es un servidor de archivos? ¿En qué nos beneficia? Son algunas de las preguntas que responderemos en estas páginas.

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 las limitaciones que ello implica) 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.

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.

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 le 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.

SMB/CIFS (Common Internet File System)

Es la modificación realizada por Microsoft al protocolo SMB original creado por IBM, utilizado a partir de la versión 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.

CON UN SERVIDOR DE ARCHIVOS, PODEMOS CREAR UNA LISTA DE CONTROL DE ACCESO Y RESGUARDAR INFORMACIÓN.

- **Optimización de vínculos lentos**: el protocolo CIFS se adaptó para funcionar con la más baja velocidad en conexiones dial-up.
- **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.
- **Nombres de archivo global**: los usuarios no tienen que montar sistemas de archivos remotos, pero pueden 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 archivos son compatibles, por lo que una letra de unidad no necesita ser creada antes que los archivos remotos puedan acceder.

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 sistema operativos Windows (SMB/CIFS), Linux, Mac OS o UNIX.

NFS (Network File System)

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; 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 que perdamos tiempo en realizar, a diario, backups de los equipos personales, en el servidor de archivos. ■

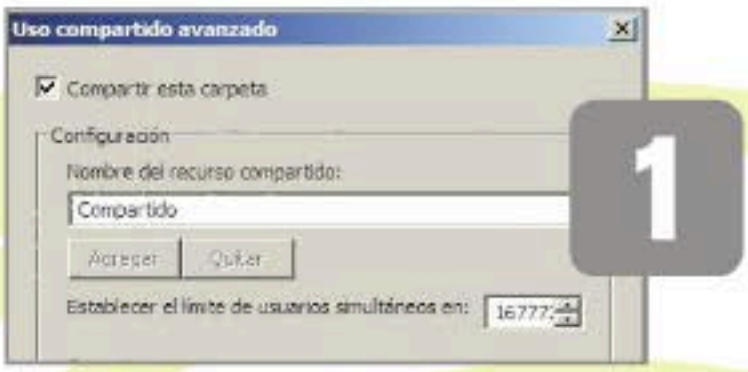
Samba, nos permite compartir archivos; estos se puedan acceder desde clientes Windows y Mac OS X.

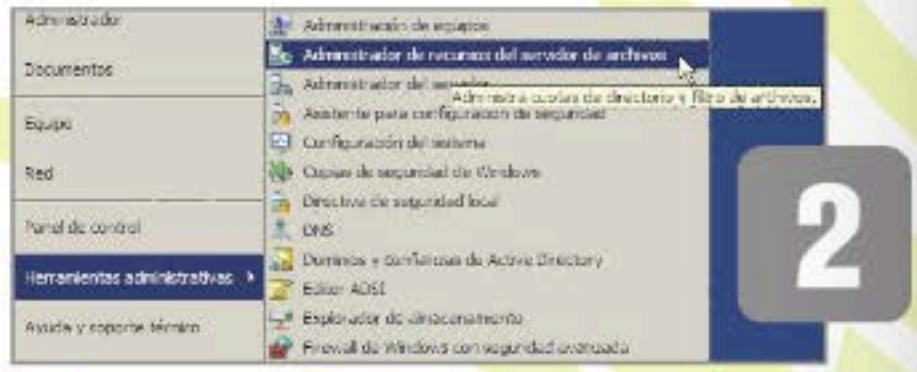
Copias de seguridad

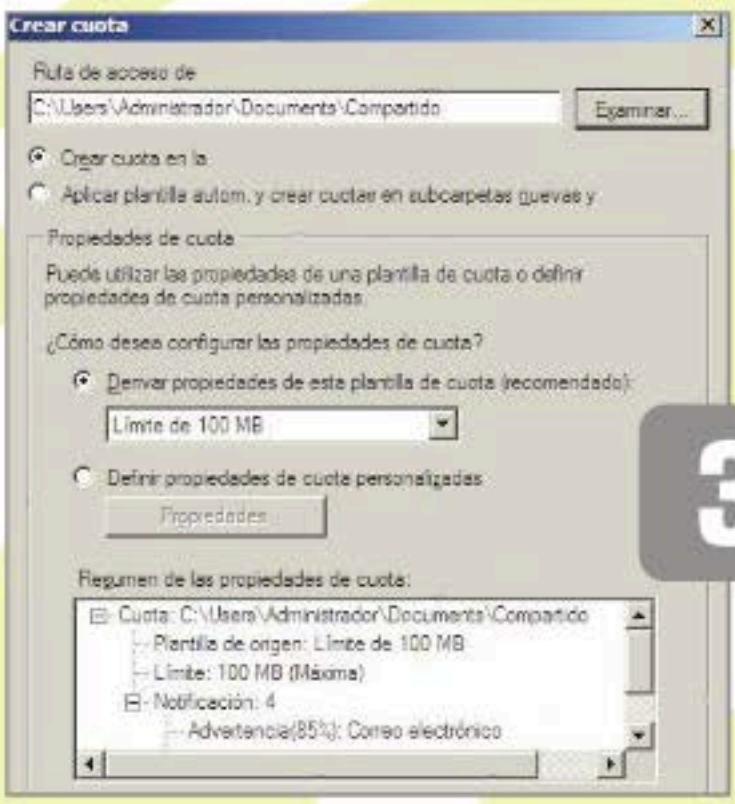
Un servidor de archivos nos brindará muchos beneficios, como los ya mencionados, pero debemos tener en cuenta que la disponibilidad de esos archivos debe encontrarse resguardada por un backup periódico (según la criticidad de la información almacenada). En caso de que el servidor dejara de funcionar ante cualquier tipo de contingencia, debemos disponer de un plan de recuperación de la información; por tal motivo los resguardos y el plan de recuperación es un detalle no menor para tener en cuenta al utilizar un servidor de archivos, ya que la continuidad de una empresa puede estar en riesgo ante la pérdida de información sensible surgida en un incidente con el servidor de archivos.

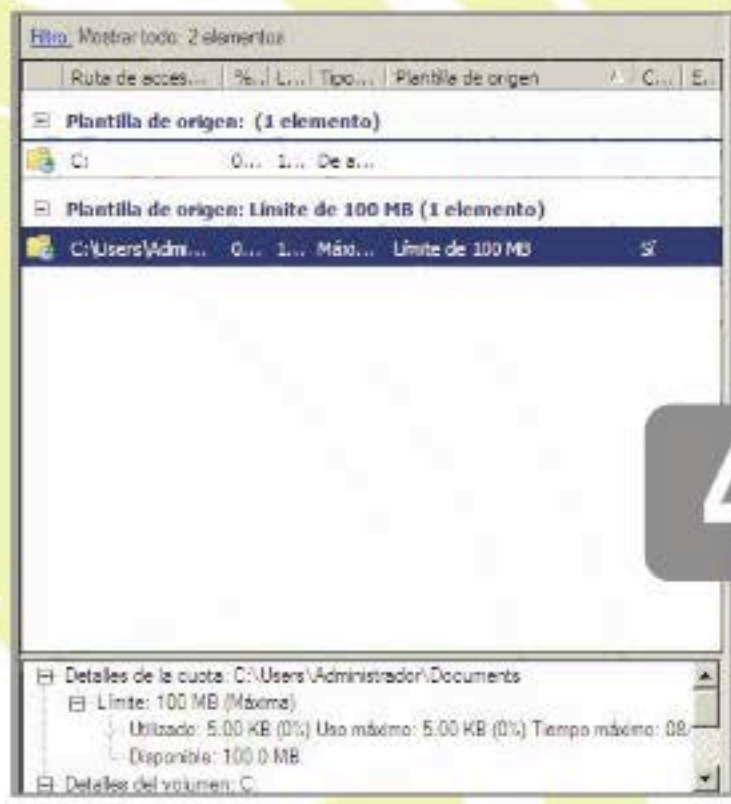
Administrar un File Server en Windows

La administración básica de un File Server en sistemas Windows requiere que tengamos en cuenta algunos consejos importantes.







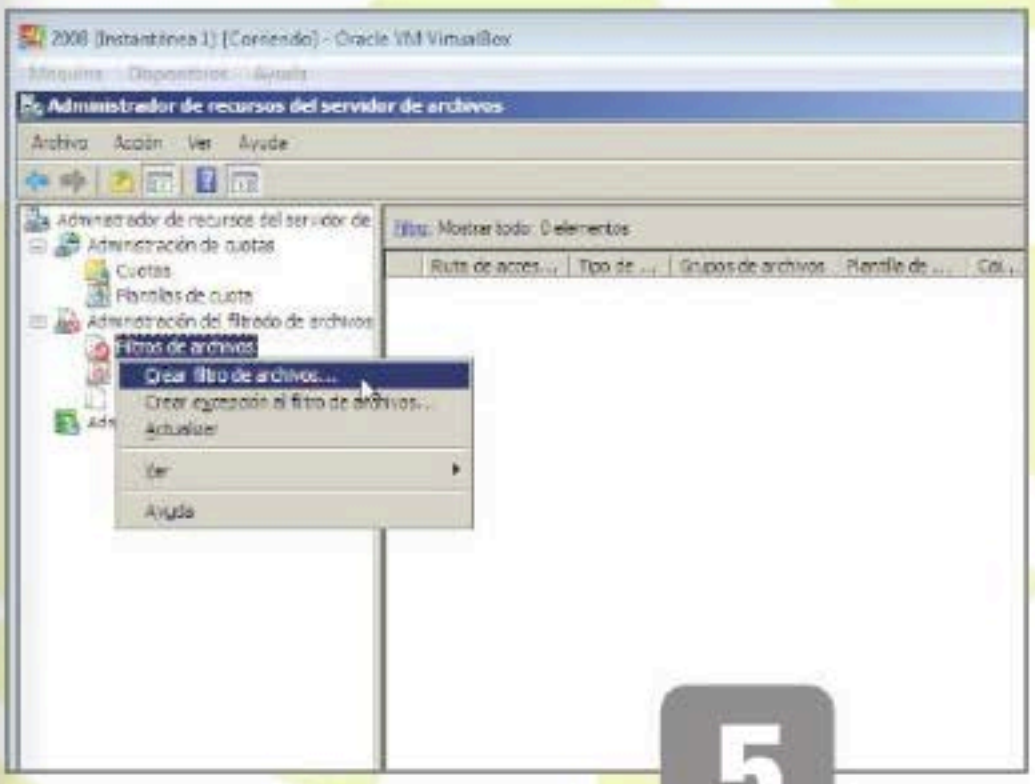


1 Inicie compartiendo un archivo desde el servidor de Windows. Para ello, es necesario crear una carpeta con el nombre **Compartido**, la cual puede estar ubicada en: **C:\Usuarios\Administrador\Documentos\Compartido**. Finalice asignando los permisos correspondientes.

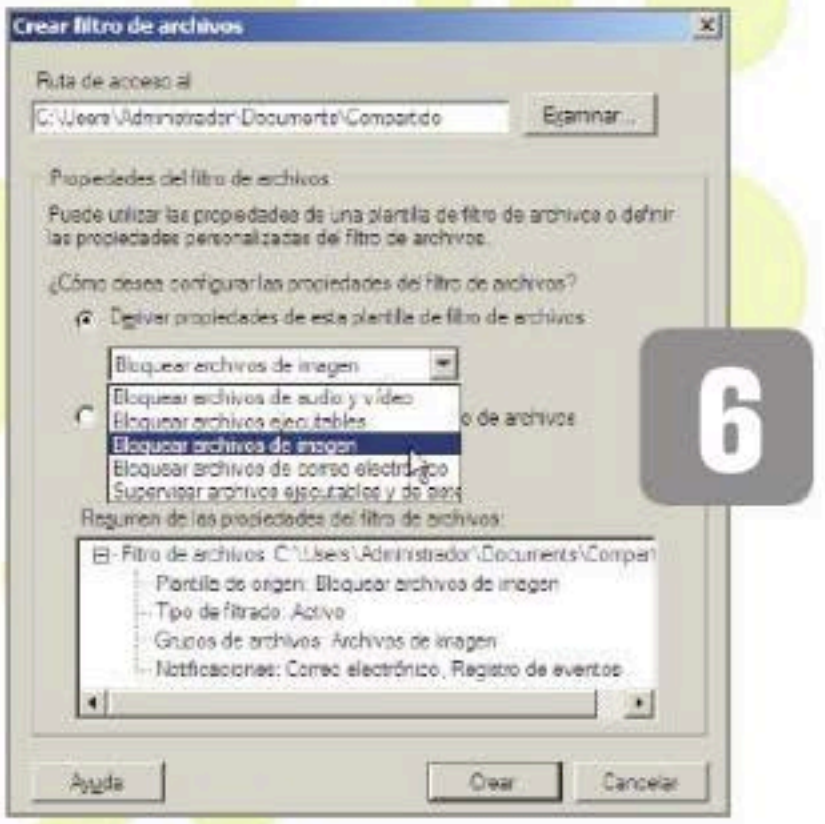
2 Desde **Inicio/Herramientas administrativas**, ingrese a **Administrador de recursos del servidor de archivos**. Desde aquí, comienza la administración básica del servidor, creando una cuota para limitar la capacidad de almacenamiento de la carpeta creada.

3 Para crear una cuota, presione clic derecho del mouse y elija la opción: **Crear cuota**. En la nueva ventana, coloque la ruta donde se halla almacenada la carpeta compartida (**Compartido**). Luego, asigne un límite de prueba (por ejemplo: 100 MB). Presione el botón **Crear**.

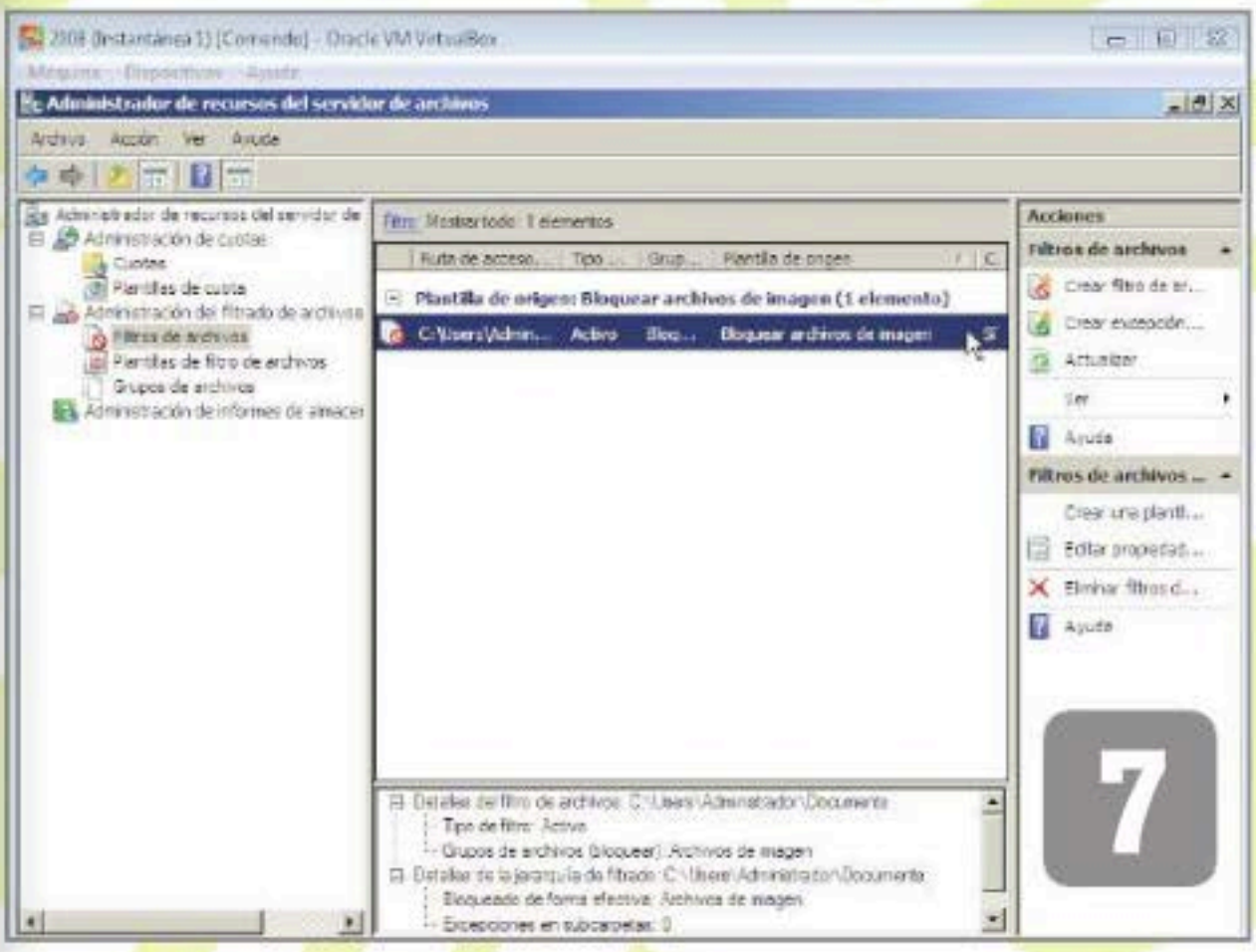
4 Para comprobar que se ha llevado a cabo la creación y configuración adecuada de la cuota, seleccione la opción **Cuota** que aparece en el panel de la izquierda de la ventana **Administrador de recursos del servidor de archivos** y verifique su configuración, desde la sección **Mostrar todo**.



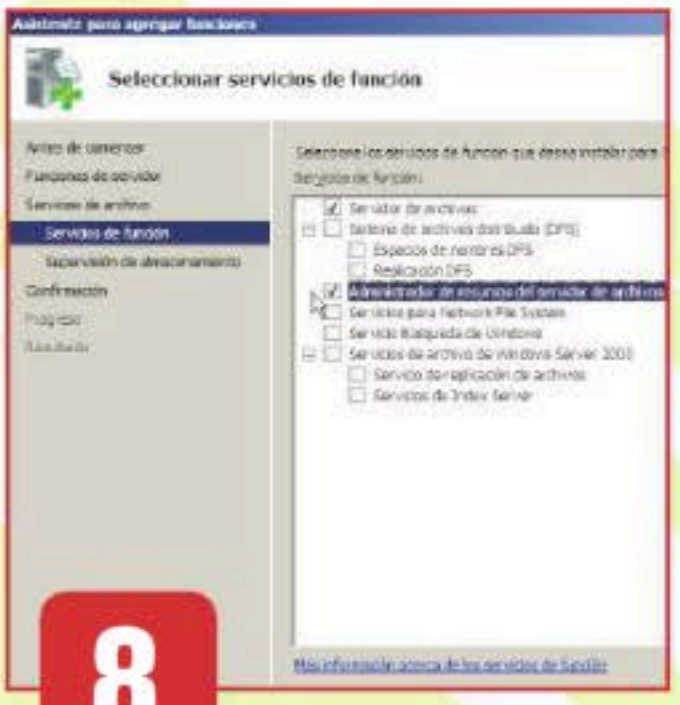
5



6



7



8

5 Para continuar con la administración de archivos desde el servidor, 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**.

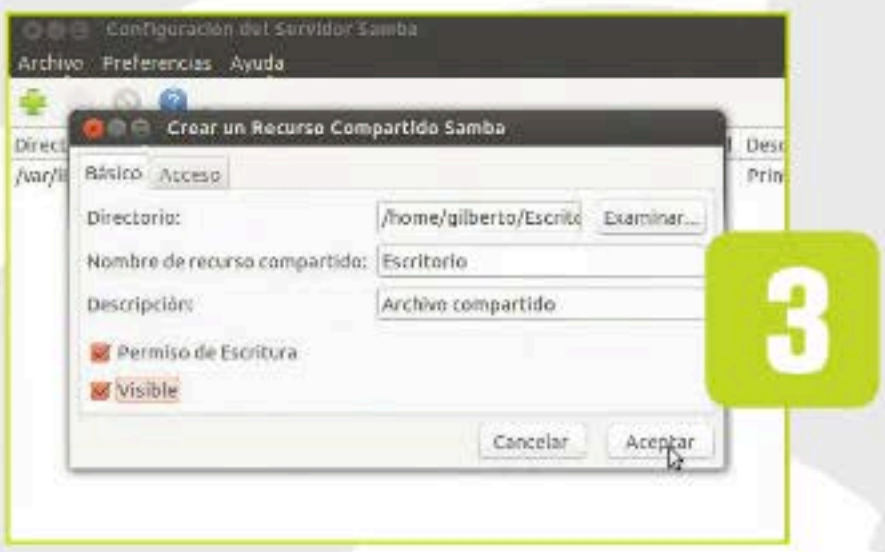
6 Coloque la ruta donde se halla almacenada la carpeta compartida (**Compartido**). Después, presione el botón **Propiedades**, para definir las características correspondientes al filtro de archivos. Una vez allí, elija del combo la opción **Bloquear archivos de imagen**. Presione **Crear**.

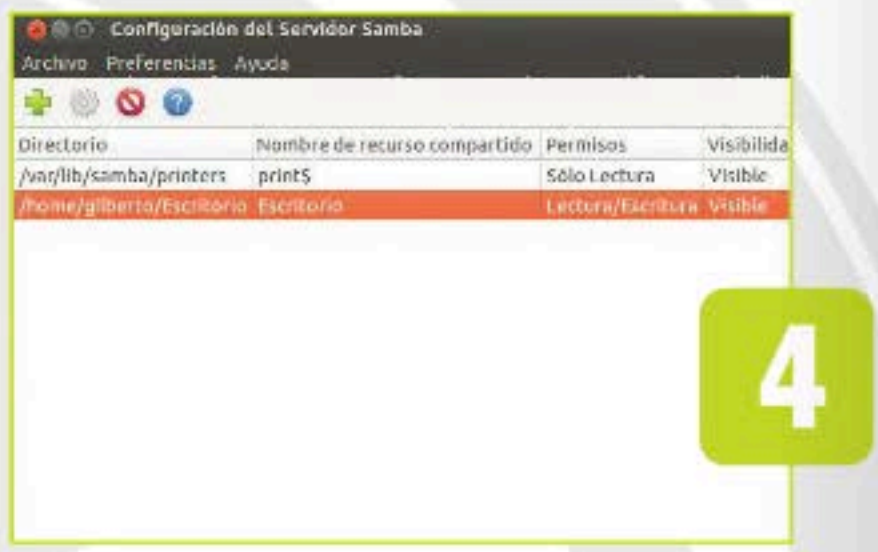
7 Verifique ahora si se ha llevado a cabo la creación del filtro deseado. Para ello, seleccione la opción **Filtros de archivos**, ubicada en el panel izquierdo de la pantalla. Los datos de alta se aprecian en la sección **Filtro**, ubicada en el centro de la ventana.

8 Para tener acceso a la opción de **Administrador de recursos del servidor de archivos**, será necesaria la instalación de la función **Servicios de archivos**. De lo contrario, no estará visible desde las herramientas administrativas del servidor.

Administrar un File Server en Linux

En estas páginas, aprenderemos a realizar la administración básica de un File Server desde un entorno GNU/Linux.



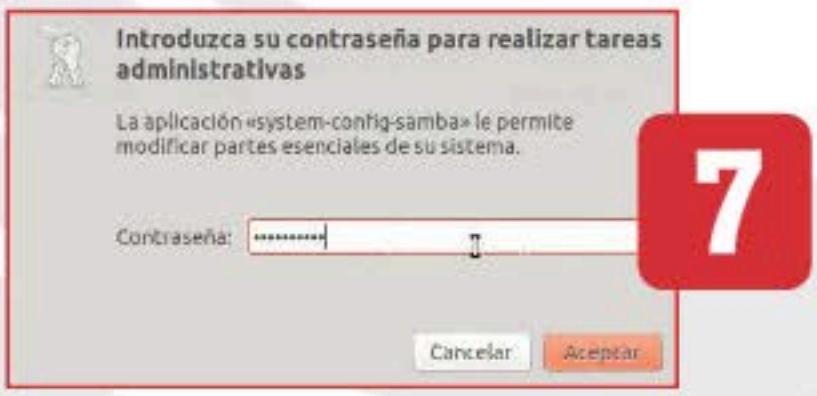


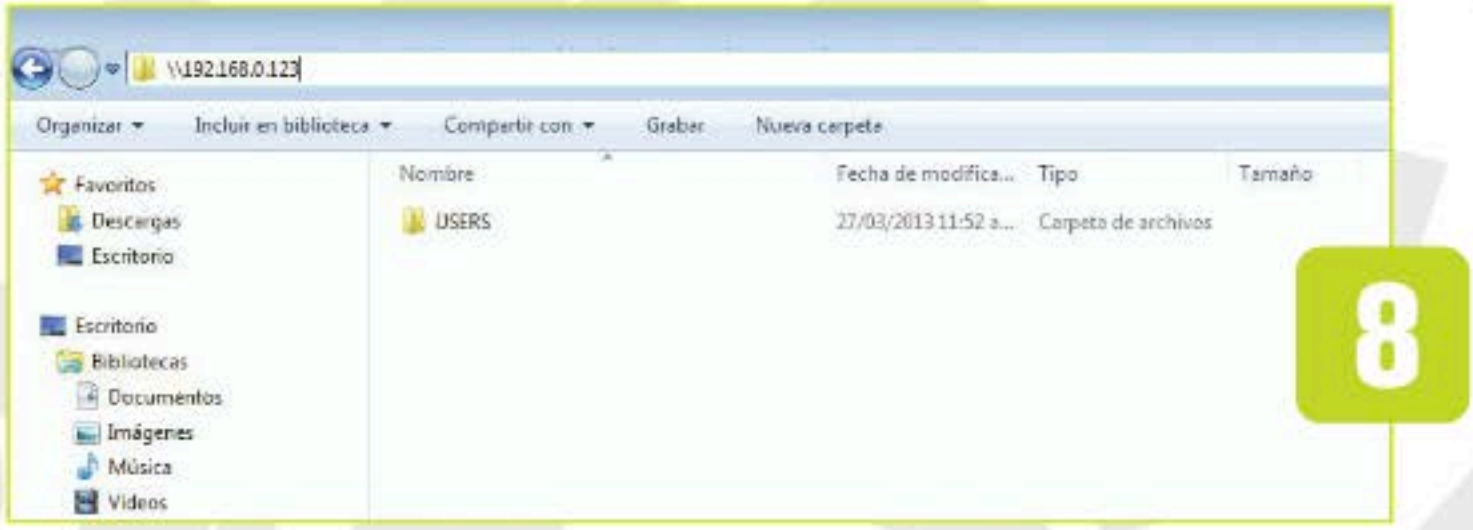
1 Encienda su PC y cargue el escritorio de Ubuntu 12.10. Abra la terminal e instale Samba. Esto se logra mediante el comando **#sudo apt-get install samba samba-common**, luego pulse **ENTER**. Instale la interfaz gráfica del sistema de configuración de Samba.

2 Desde el botón **Inicio** de Ubuntu. Escriba la palabra **Terminal** y seleccione la funcionalidad **Samba instalada**. Aparecerá la ventana **Configuración del servidor Samba**, donde debe presionar el icono en forma de cruz de la ventana para comenzar a compartir archivos.

3 Comparta un archivo seleccionando el botón **Examinar** del campo **Directorio** de la pestaña **Básico**. Después, agregue una descripción y delegue los permisos necesarios de acceso a la información compartida (haciendo clic en la pestaña **Acceso**). Pulse **Aceptar**.

4 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 poder continuar con la compartición de los ficheros en la red corporativa.





5 Ubique el archivo que se va a compartir en la red corporativa. Posteriormente, presione el botón derecho del mouse sobre la carpeta deseada y seleccione **Opciones de compartición**. Asigne un nombre al archivo compartido y delegue el acceso a los usuarios de su preferencia.

6 Proceda a abrir las propiedades del archivo compartido. Esto se realiza para asignar valores de acceso compartido, políticas de seguridad y permisos en la red. Seleccione el fichero por compartir y despliegue sus propiedades. Navegue por las fichas **Básico**, **Permisos** y **Compartir**.

7 Es posible que, en la inspección o apertura de algunas ventanas de configuración del sistema, por ejemplo para el acceso a Samba, se le haya solicitado una contraseña. Esta es la misma que utilizó en el momento de instalar su sistema Linux Server.

8 Ahora compruebe la conectividad desde otro equipo. 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. Pruebe el resultado accediendo al archivo compartido.

Seguridad en File Servers

Una vez que hayamos implementado un File Server, será necesario tener en cuenta algunos consejos sobre su seguridad; en estas páginas analizaremos los aspectos más importantes.

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).

En la página principal de Bitdefender, encontraremos una versión de prueba descargable de productos Security for File Servers.

Soluciones

Las soluciones Security for File Servers representan hoy en día una utilidad altamente demandada, que garantiza la seguridad de la información. Se trata de un servicio dedicado a servidores. 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.

Instalación

Para realizar la instalación de funcionalidades File Server sobre plataformas Microsoft Windows, tenemos que 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 también debemos contar con un espacio en el disco de 230 MB (se trata del espacio en el disco requerido después de realizar la instalación y las actualizaciones necesarias).

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

Utilidades de seguridad en File Servers

Utilidad	Descripción
Panda Security for File Servers	Ofrece una eficaz protección preventiva contra malware e intrusos, para servidores Windows. Para mayor información, se 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, ingresamos en **www.eset.es/empresas/productos/file-windows**.
AVG File Server Business Edition 2013	Brinda un control completo de sus archivos, protegiéndolos ante amenazas en línea, y mantiene un máximo rendimiento del servidor de Windows. Podemos 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. Podemos 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. Podemos consultar en **www.bitdefender.es/business/security-for-file-servers.html**.

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 tener en cuenta que 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 que circulan en nuestra red, incrementemos también la necesidad de protegerla del malware, para ello tendremos que contar con soluciones de seguridad especializadas.

MANTENER EL SOFT DE SEGURIDAD AL DÍA AYUDA A EVITAR EL MALWARE EN LA RED.

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 **ESET**, por mencionar algunas.

Los servidores de archivos basados en GNU-Linux, por lo general, cuentan con una sólida y segura plataforma de almacenamiento. Lo anterior se debe a que el kernel es mucho más estable y se halla protegido a una escala mayor en comparación con el residente en la plataforma Windows. Esto impide definitivamente el daño en cualquiera de los módulos que conforman el sistema. Los File Servers GNU/Linux incluyen, además, un conjunto de interfaces gráficas de configuración local y remota protegidas en su totalidad contra amenazas en comparación con el sistema operativo de Microsoft. Esto lo convierte en el número uno en cuanto a inmunidad. ■

Auditoría de File Servers

En estas páginas, conoceremos las opciones y ventajas que nos ofrece la habilitación de auditorías en File Servers.

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. 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 realizar la completa protección y el control de la información con el fin de evitar que esta pueda ser rastreada, modificada, robada e, incluso, eliminada.

En el portal de **Quest** de Dell, podemos encontrar una demo de la utilidad **Quest ChangeAuditor.**

Integridad de los archivos

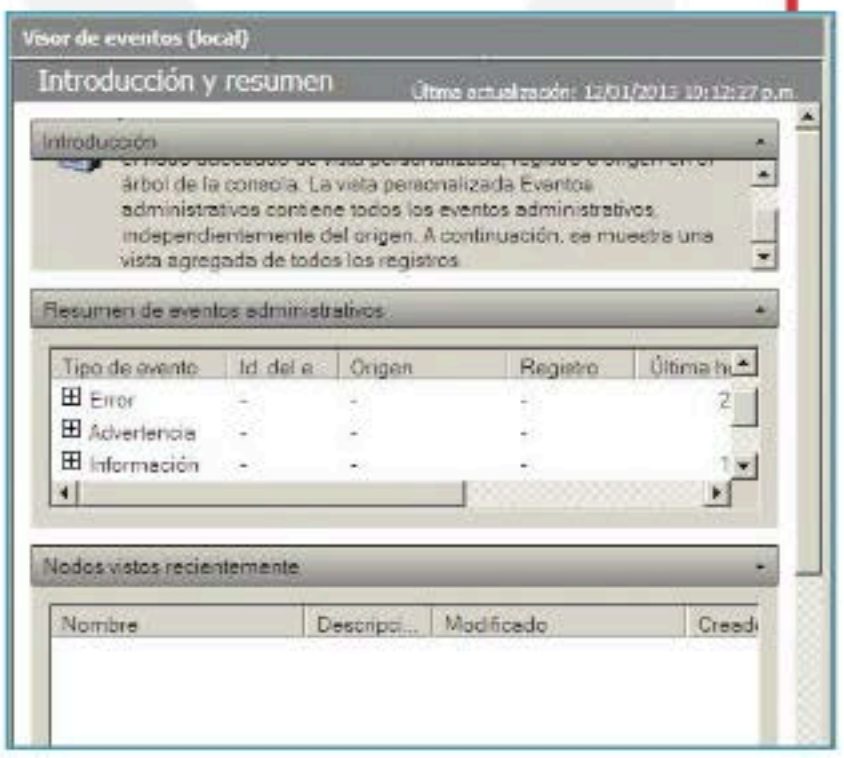
Con seguridad, muchos nos hemos preguntado alguna vez qué hacer cuando notamos que los archivos almacenados en el servidor de archivos sorpresivamente han desaparecido o han sido modificados y, derivado de ello, quién es el causante de todo esto. En estos casos, el presunto causante del intercambio o 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.

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 comenzar activando la auditoría de nuestro file server, debemos tener claros algunos conceptos:

- **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

En la imagen, se muestra la interfaz del **Event Viewer** residente en servidores Windows.



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 obtener más información sobre este apartado, es recomendable consultar la siguiente página de Microsoft: **www.microsoft.com/spain/technet/recursos/articulos/secmod50.mspx**.

▶ **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

En la actualidad, la tarea de realizar 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.

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.
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**.

SE PODRÁN AUDITAR LOS EVENTOS QUE OCURREN SOLO DESPUÉS DE HABILITAR LA AUDITORÍA.

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*). En este punto hacemos una especial mención del estándar denominado **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)**. ■

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. Una utilidad recomendada para llevar a cabo la auditoría de un File Server es NetWrix File Server Change Reporter.

Servidor de impresión

La habilitación de un servidor de impresión nos proporciona una serie de ventajas; aquí las conoceremos en detalle.

Los servidores de impresión son también conocidos como **Print Servers**. Son servidores especiales que, conectados a un dispositivo de impresión, permiten imprimir desde cualquier equipo 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). Debemos tener en cueta que un Print Server externo, por lo general, consiste en 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.

Características

Los servidores de impresión (cualquiera que sea su tipo) cumplen prácticamente con las mismas características, entre las cuales podemos mencionar las siguientes:

- **Funcionan como un servidor dedicado**: cumplen 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 determinado.
- **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 computadora**: cualquier equipo en la red, puede ser capaz de administrar un servidor de impresión. Para ello, es necesaria la instalación de un sistema operativo 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 realizar la configuración de impresoras virtuales, además del uso del servicio de manera remota.
- **Permiten la asignación de políticas de seguridad**: se delegan permisos y prioridades de impresión a los usuarios que pertenezcan a la red.

LOS SERVIDORES DE IMPRESIÓN SUELEN IMPLEMENTARSE A NIVEL SOFTWARE Y DE HARDWARE.

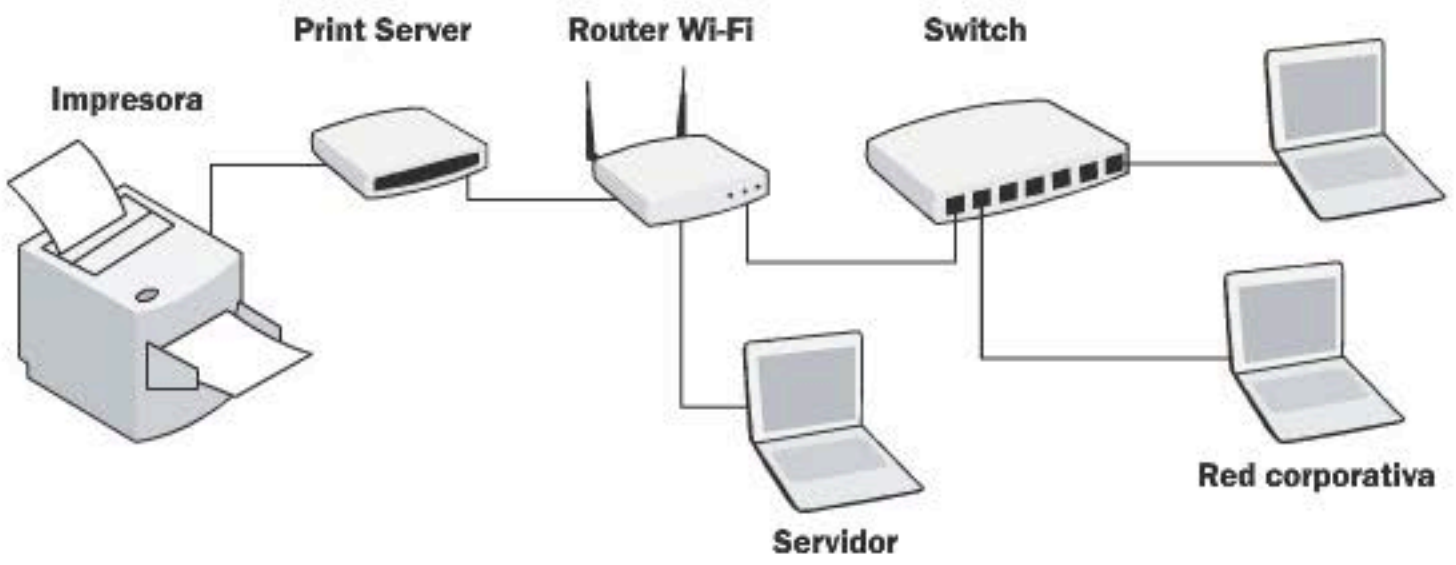
Ventajas

Los Print Servers a menudo cumplen con una serie de ventajas que los convierten en los preferidos de muchas compañías.

- **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 del Print Server, a menudo se evitan colas o retrasos en los procesos de 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.



En el esquema, se muestra la forma de conectar un servidor de impresión a la red de datos de una organización.

▶ **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 la expansión.

Servidores de impresión en Windows Server

Los Print Servers casi siempre son configurados sobre equipos que fungen como servidores en la red (servidores locales). Esto quiere decir que pueden ser gestionados desde cualquier PC 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 de la prueba de conectividad. Windows Server es un sistema operativo robusto que requiere ser ejecutado en un equipo con características especiales; recomendamos para ello un microprocesador de 2 GHz, 1 GB de memoria RAM, y un disco duro de, al menos, 40 GB de almacenamiento. Luego de completar los 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 conocimientos elementales.

Servidores de impresión para Linux

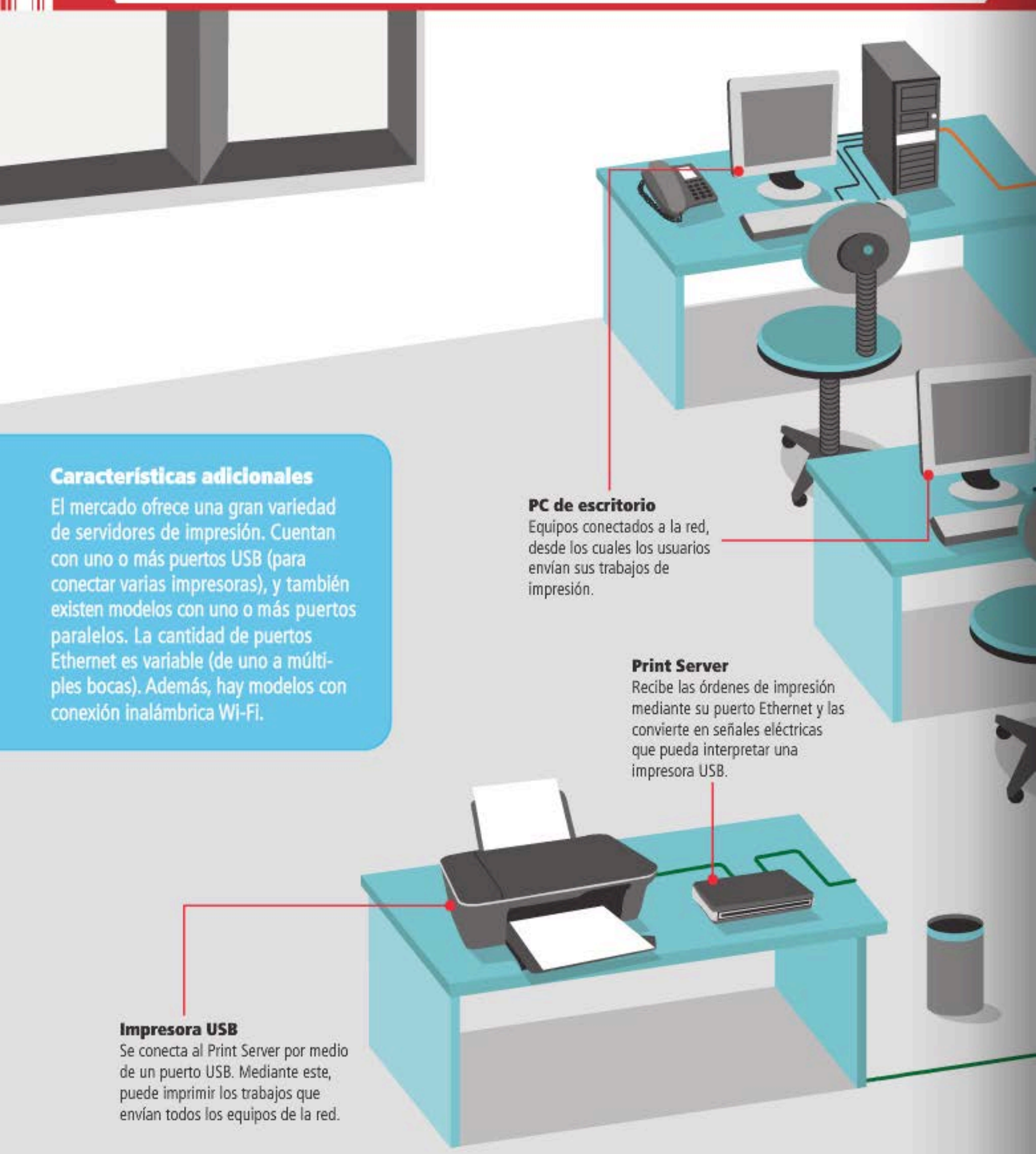
Los servidores de impresión para GNU/Linux poseen prácticamente las mismas ventajas que un Print Server para Windows, solo que son acreedores a un nivel de seguridad mayor por la plataforma en la que se ejecutan. Los servidores Linux, a menudo, hacen uso de un conjunto de herramientas, mejor conocidas como CUPS. Este sistema consiste en un nuevo estándar de impresión vigente en la mayoría de las distribuciones de GNU/Linux. CUPS utiliza IPP para la gestión de las tareas de impresión y colas de impresión a través de Internet. Se encarga de proveer las instrucciones de impresión de los sistemas Unix, además de un soporte de operaciones bajo el Bloque de Mensajes del Servidor (SMB), protocolo que permite compartir archivos e impresoras desde un servidor. ■

El rol Servicios de impresión debe darse de alta desde el Administrador del servidor de Windows 2008 para configurar un Print Server.

Print server

Características adicionales

El mercado ofrece una gran variedad de servidores de impresión. Cuentan con uno o más puertos USB (para conectar varias impresoras), y también existen modelos con uno o más puertos paralelos. La cantidad de puertos Ethernet es variable (de uno a múltiples bocas). Además, hay modelos con conexión inalámbrica Wi-Fi.

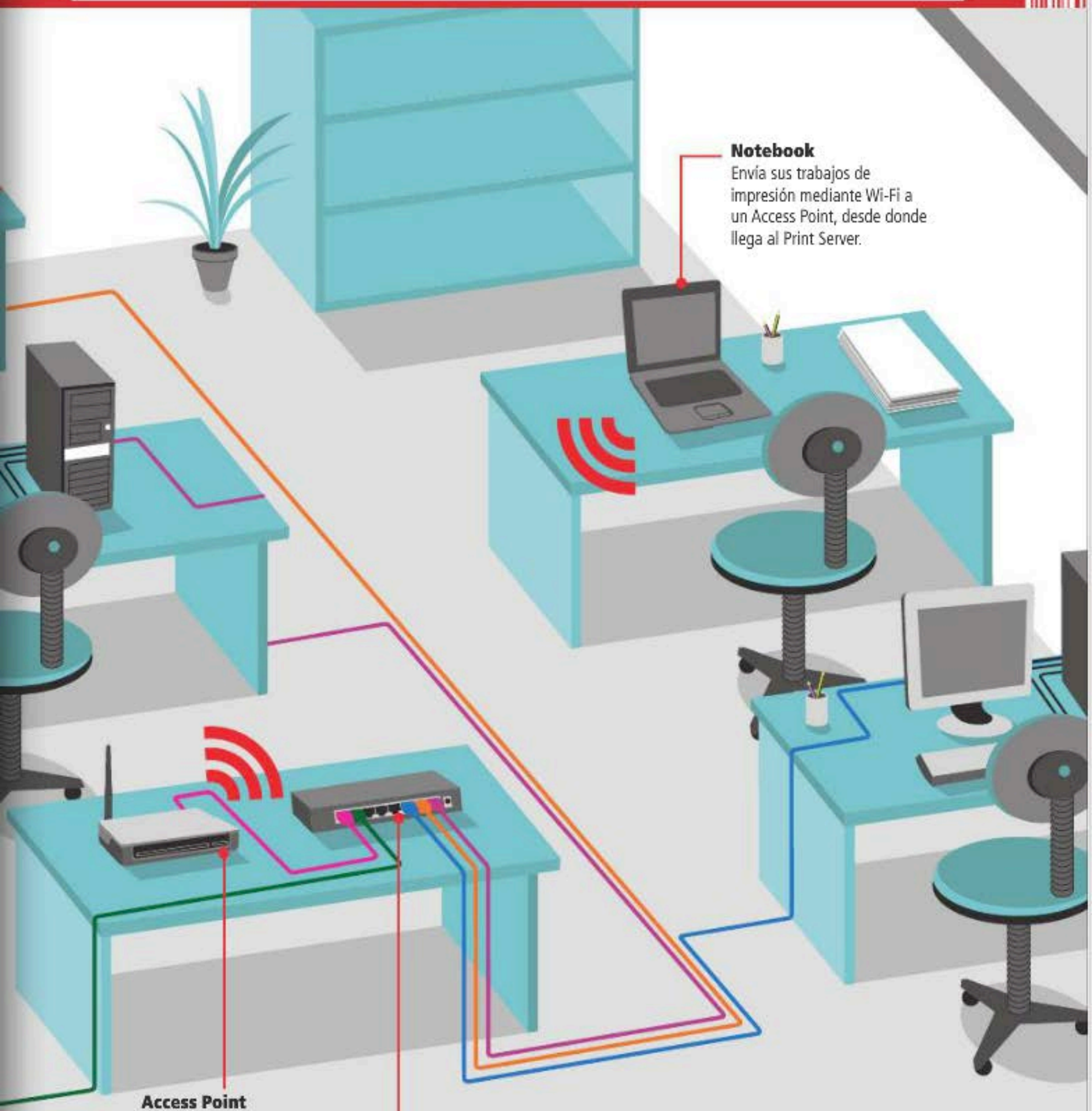


PC de escritorio
Equipos conectados a la red, desde los cuales los usuarios envían sus trabajos de impresión.

Print Server
Recibe las órdenes de impresión mediante su puerto Ethernet y las convierte en señales eléctricas que pueda interpretar una impresora USB.

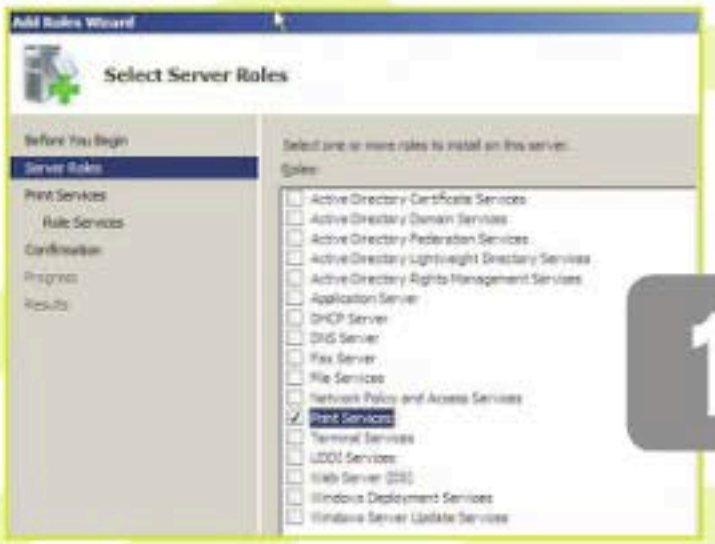
Impresora USB
Se conecta al Print Server por medio de un puerto USB. Mediante este, puede imprimir los trabajos que envían todos los equipos de la red.

LA INSTALACIÓN DE UN PRINT SERVER OFRECE OPCIONES ADICIONALES EN UNA RED DE DATOS.

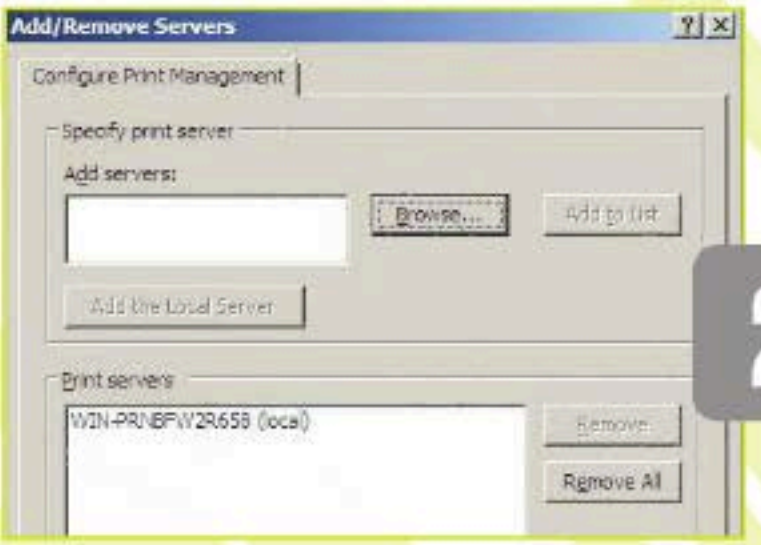


Administración de un Print Server en Windows

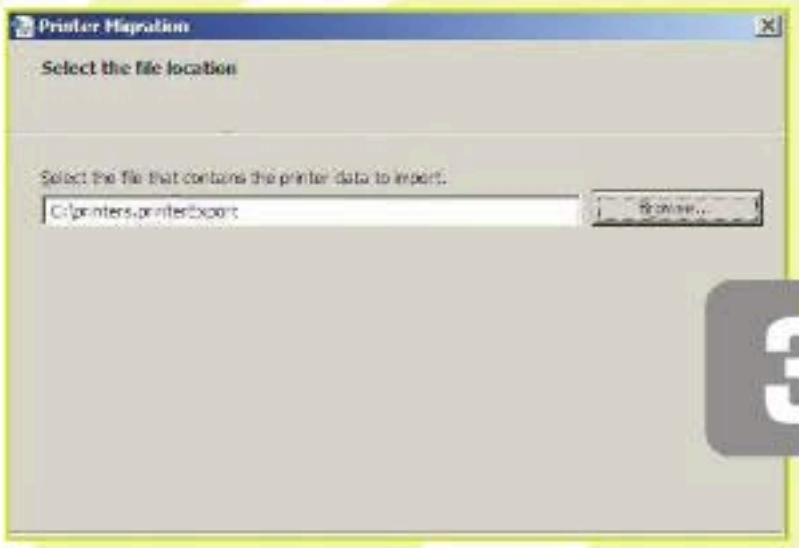
La administración de las impresoras en forma centralizada utilizando Windows Server debe ser realizada en forma cuidadosa.



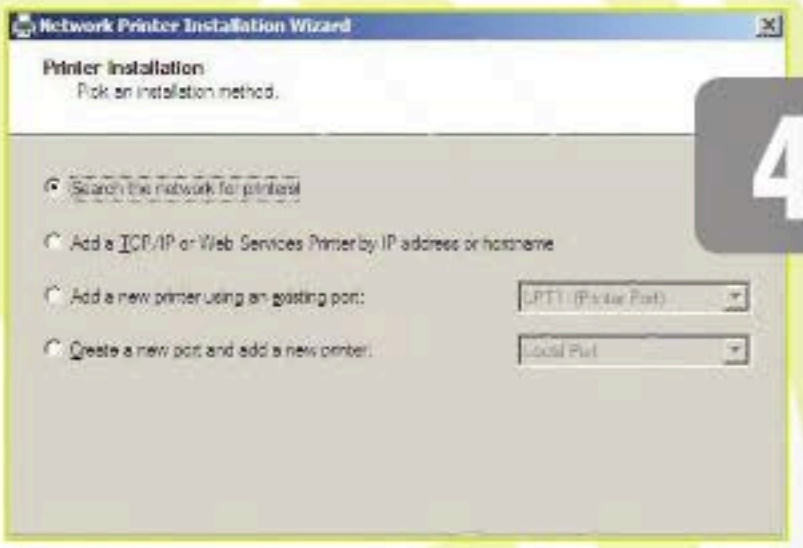
1



2



3



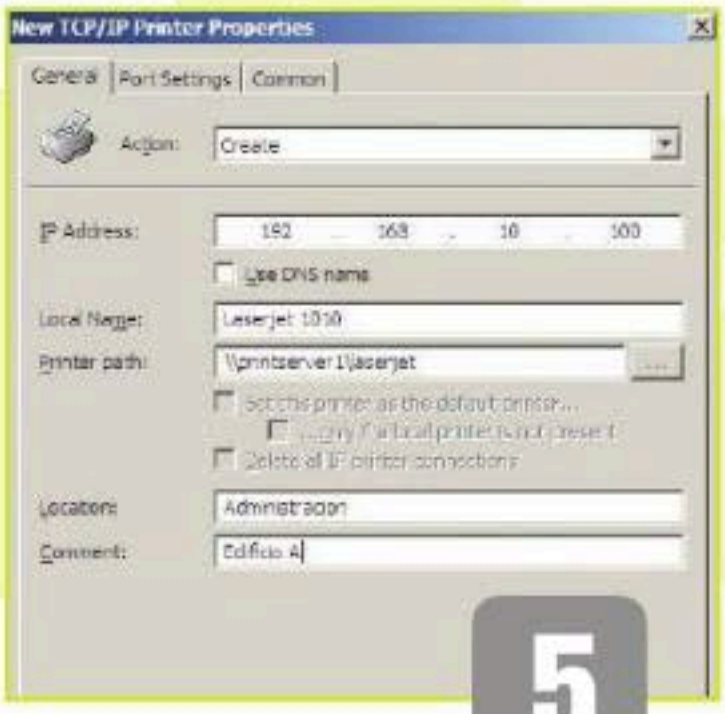
4

1 El complemento **Print Management** se instala de forma predeterminada en las versiones desktop de Windows, pero no en equipos Windows Server 2008 y superiores. Para instalarlo desde el **Administrador de servidores**, abrimos el asistente para agregar funciones y seleccionamos el rol **Print Services**.

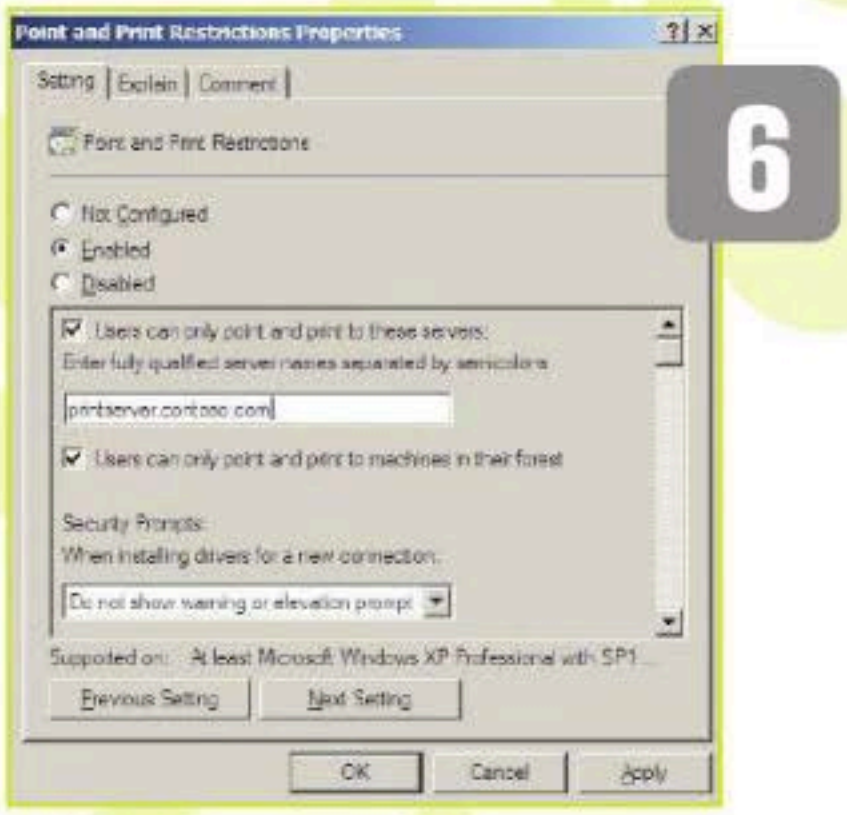
2 Para agregar **Print Servers** al **Print Management** vamos a **Administrative Tools** y, luego, a **Print Management**. Presionamos **Add/Remove Servers**, e ingresamos el nombre adecuado. Presionamos **Add to List**. Para agregar el servidor local, hacemos clic en **Add the Local Server**.

3 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**. Esta es una forma de consolidar las impresoras en un Print Server.

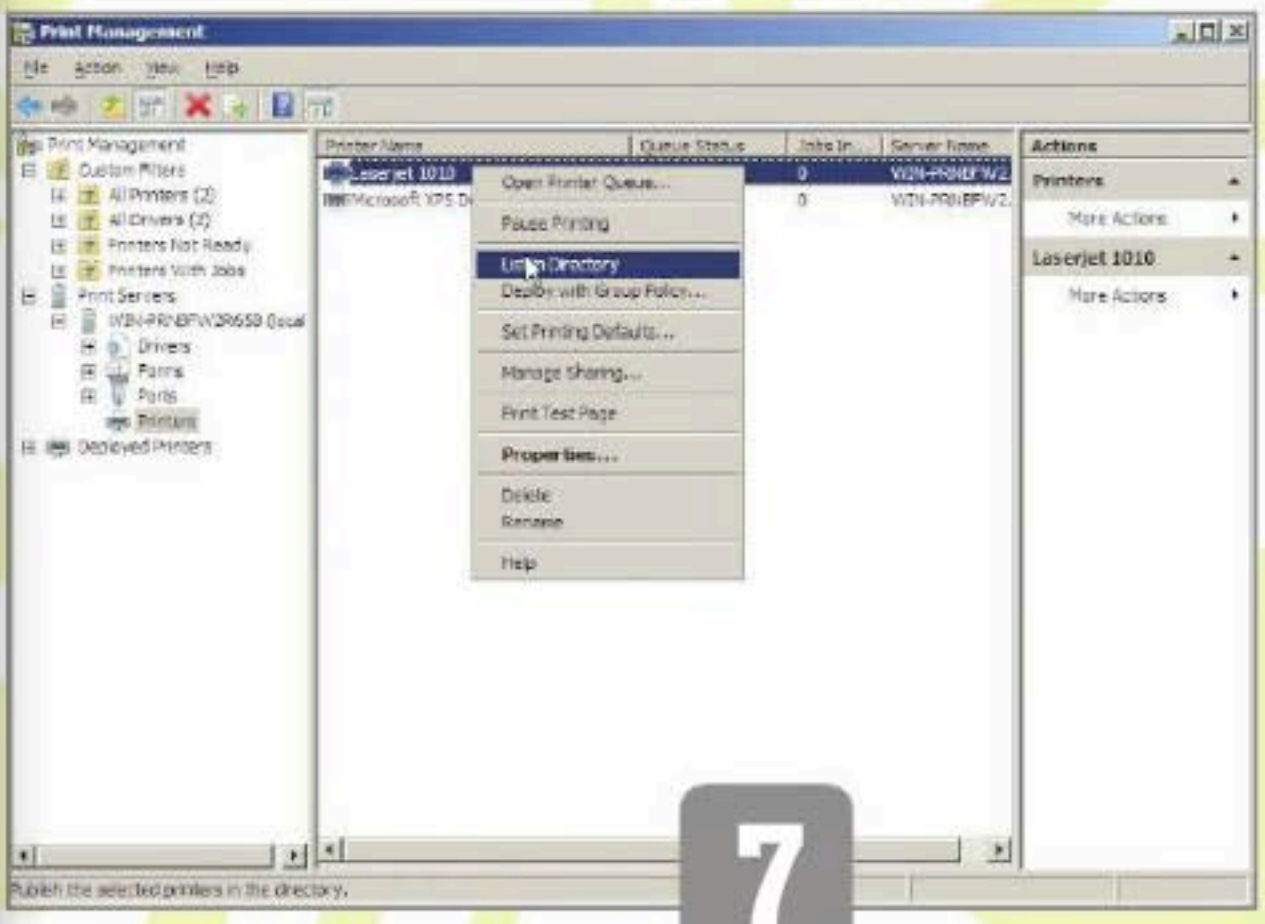
4 **Print Management** puede detectar automáticamente las impresoras que se encuentran en la misma red. Para esto, presionamos **Add Printer** y hacemos clic en **Search the Network for Printers**. Es posible que solicite los drivers si no están presentes.



5



6



7

8

5 Una vez instaladas las impresoras en el Print Server, se pueden instalar en forma centralizada en las estaciones de trabajo, utilizando **Group Policy**. Se requiere como mínimo Windows Server 2003 R2. Es posible hacerlo por grupo de usuarios o de PC según se necesite.

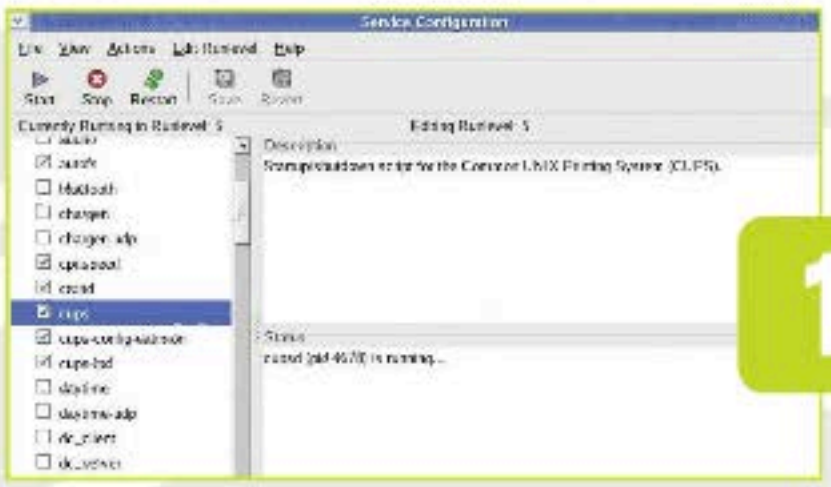
6 La configuración por defecto de Windows Vista en adelante permite a usuarios no administradores instalar solo drivers firmados digitalmente. Para que las impresoras instalen drivers no firmados, se debe configurar la opción **Point and Print Restrictions** en la GPO.

7 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**.

8 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.

Administración de un Print Server en Linux

En esta oportunidad, conoceremos algunos consejos para instalar y administrar las impresoras de forma centralizada utilizando CUPS.



1

2

3

4

1 Como primera acción, debemos verificar que poseamos el servicio CUPS instalado y habilitado en el sistema. Podemos utilizar la interfaz gráfica o el comando **/etc/init.d/cups start**.
En caso de que equipos Windows requieran utilizar las impresoras, es necesario que instalemos Samba y Kerberos.

2 Si contamos con una infraestructura Active Directory, es recomendable que Samba se convierta en un miembro, usando el modo de autenticación ADS. De esta forma, los usuarios no deberán autenticarse.
La hora debe estar sincronizada con Active Directory usando NTP.

3 Para acceder a CUPS mediante un browser, ingresamos a **http://localhost:631**. Allí podremos crear y testear las impresoras definidas. Podremos agregar impresoras locales o de red. CUPS posee gran cantidad de drivers. Desde **http://www.cups.org/ppd.php**, es posible consultar el listado.

4 Es posible visualizar los trabajos activos y suspenderlos o cancelarlos. También se puede consultar la lista de los trabajos finalizados. Todas estas tareas pueden ser realizadas tanto local como remotamente.
Desde la consola, es posible consultar los logs en el directorio **/var/log/cups**.

5

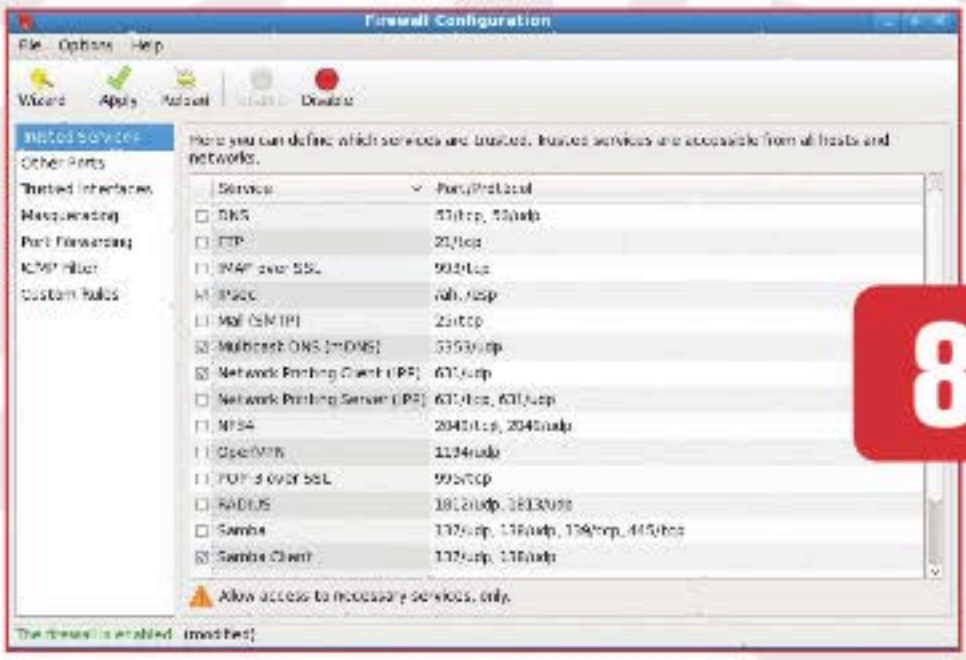
```
File  Edit  View  Terminal  Tabs  Help
[root@oradb oracle]# lp -d Epson /home/oracle/readme
request id is Epson-7 (1 file(s))
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]# lpstat -p epson
printer Epson is idle.  enabled since Jan 01 00:00
        CUPS v1.1.22rc1 is ready to print.
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]# lpstat -t
scheduler is running
system default destination: Laserjet_1010
device for Epson: parallel:/dev/lp0
device for Laserjet_1010: socket://printer01
Epson accepting requests since Jan 01 00:00
Laserjet_1010 accepting requests since Jan 01 00:00
printer Epson is idle.  enabled since Jan 01 00:00
        CUPS v1.1.22rc1 is ready to print.
printer Laserjet_1010 disabled since Jan 01 00:00 -
        Unable to locate printer 'printer01' - Host name lookup failure
[root@oradb oracle]#
```

6

```
File  Edit  View  Terminal  Tabs  Help
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]# lpoptions -d epson -l
ColorModel/Output Mode: *CMYK Gray
Resolution/Output Resolution: 180dpi *360dpi 720dpi
PageSize/Media Size: *Letter Legal A4
PageRegion/PageRegion: Letter Legal A4
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]#
[root@oradb oracle]# lprm -P epson
lprm: Unable to cancel job(s)!
[root@oradb oracle]#
```

Admin on localhost - CUPS v1.1.22rc1 - Mozilla Firefox

7



8

5 Por defecto, las impresoras agregadas en CUPS no se comparten, por lo que es necesario habilitar la posibilidad de que otras computadoras las utilicen. En RedHat, se debe ejecutar **system-config-printer** y, luego, tildar en cada impresora la opción **This queue is available to other computers**.

6 Para imprimir desde la línea de comandos, es posible utilizar el comando **lp –d Nombre Queue archivo**. Por ejemplo **lp –d Epson /home/Oracle/readme**. Para conocer el estatus de una impresora en particular, es posible ejecutar el comando **lpstat –p** impresora. Para obtener estatus detallado, ejecutar **lpstat –t**.

7 El comando **lpoptions** nos permite visualizar las características principales de cada impresora. Si direccionamos la salida a un archivo, podremos generar un inventario de ellas. Mediante el comando **lprm –P** impresora, podremos cancelar los trabajos activos que deseemos anular.

8 Para poder acceder remotamente a CUPS, es necesario habilitar el puerto 631 (TCP y UDP) en el firewall local. Para esto, en Red Hat ejecutamos **system-config-firewall**, y se abrirá la interfaz de configuración gráfica. Debemos además habilitar los puertos requeridos por Samba (Kerberos, netbios, etc.).

Print Servers y políticas de uso

Conoceremos las herramientas para controlar el uso de las impresoras y presentaremos alternativas de implementación comerciales y sin costo.

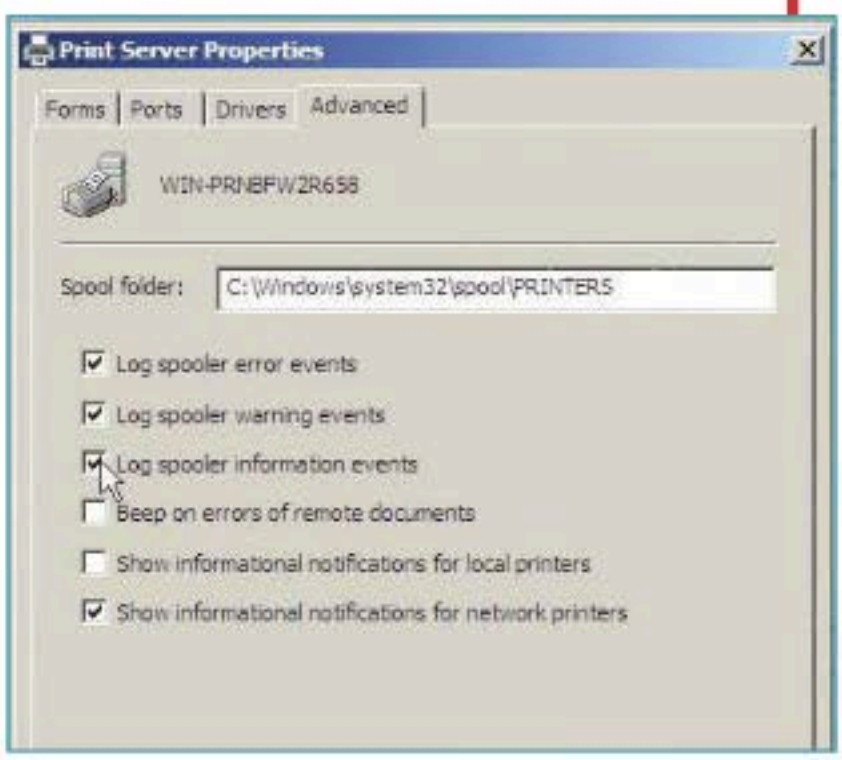
Los usuarios y las empresas cada vez más se preocupan por el consumo de papel gracias a la puesta en práctica de iniciativas de Responsabilidad Social Empresaria (RSE), pero también debido a los costos que implica el papel, el tóner y otros insumos requeridos por las impresoras. Con la popularización de las tablets y los e-readers todo tiende a digitalizarse, sin embargo, aun 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**, utilizando **Microsoft-Windows-PrintService**. Los **Group Policy Objects** (**GPO**) generados a nivel de dominio permiten deployar impresoras, definir restricciones y propiedades de las impresoras 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 tantas opciones.

Configuración de la consola Print Manager de Windows Server 2008 R2 para guardar todos los eventos del spool.



CUPS PUEDE INTEGRARSE CON SISTEMAS UNIX, LINUX, MAC OS X Y WINDOWS.

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 además soporta cuotas por usuario o impresora. Que CUPS se ejecute sobre un servidor Linux no implica que los usuarios también deban usar Linux; es posible usar CUPS como Print Server de sistemas Windows sin mayor complejidad. En este caso, es necesario configurar Samba para exportar las impresoras mediante el archivo `smb.conf`. 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, para ello deben utilizar el protocolo IPP (*Internet Printing Protocol*), por esto es importante considerar que cualquier control que hayamos implementado en Samba puede ser salteado si nos encargamos de imprimir directamente en CUPS.

Impresora **Xerox WorkCentre 7346** con soporte para **Xerox Standing Accounting** (XSA), que registra detalladamente la utilización del equipo.

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
```

Los campos que encontramos son los siguientes: 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 pueda autenticar a los usuarios que se conectan para imprimir o utilizar carpetas compartidas. De esta manera, no será necesario generar un usuario especial en el sistema Linux solo para imprimir o acceder a 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. Por su parte, Hewlett-Packard posee la solución **HP Access Control Printing Solutions**, que permite autenticar a 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, se puede 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). ■

Configuración de seguridad sobre una impresora. Desde la solapa Security, con el botón Advanced se definen los eventos por auditar.

Seguridad en Print Servers

La seguridad en los Print Servers suele ser subestimada. En estas páginas ofrecemos algunos consejos importantes para conseguir seguridad y confidencialidad en sistemas Windows y GNU/Linux.

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 se lo ha definido en cada impresora. Así, se puede auditar el uso de las impresoras y de los privilegios.

Existe gran cantidad de malware embebido en drivers de impresoras, por lo que controlarlos es crucial es 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.

Autenticación biométrica para impresoras **HP LaserJet**. Permite limitar el uso del dispositivo a usuarios habilitados.

Xerox y McAfee

Xerox y McAfee **desarrollaron una serie multifunciones que se encargan de proteger contra el malware y los virus. El software McAfee que se encuentra embebido posee un eficiente sistema de filtrado que permite que solo los programas debidamente 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. Este riesgo, muchas veces subestimado, puede afectar la confidencialidad o integridad de la información intercambiada.**

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

Existen algunos dispositivos específicos que pueden tener sus propias herramientas de seguridad. Por ejemplo, la empresa Xerox dispone de una serie de funcionalidades de seguridad como las que mencionamos a continuación:

- **Sobrescritura de datos**: en forma periódica se escribe el disco con sucesivas pasadas de forma de evitar que el contenido almacenado en él pueda ser copiado.
- **Encriptación de datos**: los datos que se encuentran 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.
- **Xerox Standard Accounting (XSA)**: permite realizar el 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.

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. Tengamos en cuenta que los Print Servers y las impresoras utilizan gran cantidad de aplicaciones y, como todo, debe encontrarse actualizado con los últimos firmware disponibles. Por ejemplo, el firmware que corresponde a los Jetdirects de HP puede ser actualizado utilizando la aplicación **Download Manager** o también mediante el software denominado **HP Web Jetadmin**. ■

LA CONFIDENCIALIDAD DE LA INFORMACIÓN QUE SE IMPRIME DEBE CONSIDERARSE ENCRIPTANDO LOS DATOS.

Aquí vemos la interfaz de administración de **CUPS**. Esta puede ser accedida en forma remota utilizando un navegador web.

Print Servers: auditoría

En esta sección, conoceremos la forma en que debemos habilitar la auditoría de Print Servers en sistemas Windows.

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

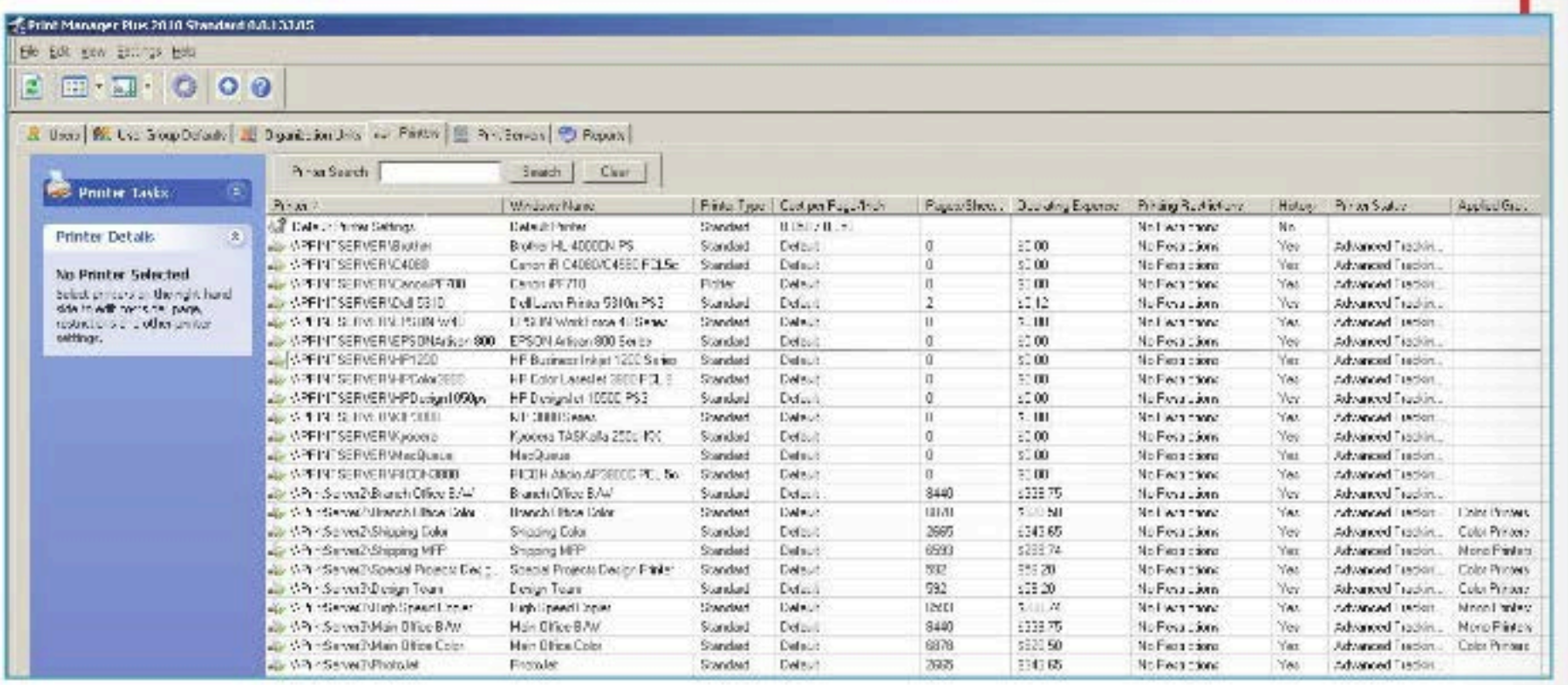
En la plataforma Windows, podemos almacenar, visualizar y publicar información en varios formatos utilizando el Event Viewer. Para definir las acciones por auditar, se deben modificar las propiedades de cada impresora. Si necesitamos agregar, remover o ver las entradas de auditoría de una impresora, es necesario acceder a sus propiedades, ir 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 muchos eventos considerados inútiles si tildamos todas las opciones. Por esta razón, 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. ■

Información de costo detallada provista por el complemento Print Manager Plus.



PRÓXIMA ENTREGA

21

SERVIDORES ADICIONALES

En esta clase conoceremos diversos servidores adicionales que nos permitirán implementar funciones específicas en nuestra red. Revisaremos su configuración y los primeros

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00020
9 789871 857784

CONTENIDO DE LA OBRA