Red Hat Linux 7.1

Official Red Hat Linux Reference Guide

ISBN: N/A


Red Hat, Inc.

2600 Meridian Parkway
Durham , NC 27713 USA

Research Triangle Park, NC 27709 USA

rhl-rg(ES)-7.1-Print-RHI (2001-02-21T10:50-0500)

Impreso en Canadá, Irlanda y Japón

Índice

Red Hat Linux 7.1

Introducción

Bienvenido a la *Official Red Hat Linux Reference Guide*.

La *Official Red Hat Linux Reference Guide* contiene la información necesaria sobre el sistema Red Hat Linux. Desde conceptos fundamentales, tales como la estructura del sistema de ficheros de Red Hat Linux, al particionamiento de discos y el control de autentificación. Esperamos que este manual sea un recurso valioso para usted.

Esta guía le ayudará a aprender más sobre el funcionamiento de su sistema Red Hat Linux. Podrá profundizar en los siguientes temas:

- Conceptos sobre la creación de particiones — Una introducción al particionamiento de los discos y técnicas para ubicar más de un sistema operativo en un solo disco duro.
- *Arranque de Red Hat Linux* — Información sobre los niveles de ejecución, los directorios `rc.d` y el modo de iniciar sus aplicaciones preferidas al mismo tiempo que arranca.
- *Seguridad del sistema y de la red* — Averigüe los métodos más comunes usados por los agresores para comprometer su sistema y cómo prevenir los problemas de seguridad.
- *Conceptos sobre RAID* — Creación de varias unidades de disco que actúan como una única unidad lógica, consiguiendo una mayor ejecución y fiabilidad.
- *Instalación de un servidor Web seguro* — Añadiendo capacidades de encriptación a su servidor Web Apache.

Antes de leer esta guía, debería estar familiarizado con los contenidos de la *Official Red Hat Linux x86 Installation Guide* relativos a la instalación, la *Official Red Hat Linux Getting Started Guide* para conceptos básicos sobre Linux y la *Official Red Hat Linux Customization Guide* para instrucciones personalizadas. La *Official Red Hat Linux Reference Guide* contiene información sobre temas muy específicos que no afectan a todos los usuarios, dependiendo del uso que se le quiere dar al sistema Red Hat Linux.

Las versiones en HTML y en PDF de todos los manuales oficiales de Red Hat Linux están disponibles en línea en http://www.redhat.com/support/manuals.

Cómo encontrar la documentación apropiada

Necesita documentación apropiada a su nivel de experiencia con Linux. De lo contrario, se sentirá abrumado o no encontrará la información necesaria para responder a sus dudas. La *Official Red Hat Linux Reference Guide* trata de aspectos más técnicos y de opciones de su sistema Red Hat Linux. Esta sección le ayudará a decidir, dependiendo de la información que necesite, si leer este manual u otros manuales Red Hat Linux, incluidos los recursos en línea.

Podemos establecer tres categorías de personas que usan Red Hat Linux, e intentar ser más explícitos en cuanto a la documentación y fuentes de información necesarias. Podemos empezar viendo el nivel de conocimiento que tiene uno mismo. Aquí hacemos referencia a las tres categorías básicas:

Nuevo en Linux

Nunca ha usado el sistema operativo Linux o similar; o tiene muy pocos datos acerca de él. Tiene o no ha tenido experiencias usando otros sistemas operativos (como por ejemplo Windows). ¿Es ésta su situación? Si es así, por favor vuelva a la *Documentación para usuarios principiantes de Linux*.

Alguna experiencia con Linux

Ha instalado con éxito Linux y lo ha usado con anterioridad (pero no Red Hat Linux) O bien ha tenido experiencias equivalentes con otros sistemas operativos parecidos a Linux ¿Se encuentra usted entre este tipo de personas? Si es así,vuelva a leer la *Para los más experimentados*.

Usuario avanzado

Ha instalado y usado Red Hat Linux con éxito en otras ocasiones. Si es así lea la *Documentación para gurús de Linux*

Documentación para usuarios principiantes de Linux

Para alguien nuevo en Linux, la cantidad de información disponible sobre cada tema, como imprimir, arrancar el sistema o particionar su disco duro, puede ser abrumadora. Es conveniente que primero adquiera una buena base de conocimientos centrados entorno a cómo funciona Linux antes de entrar en temas más avanzados.

Su primer objetivo debería ser el de obtener documentación útil. De lo contrario se sentiría frustrado nada más empezar.

Trate de adquirir el siguiente tipo de documentación:

- *Una breve historia de Linux* — Muchos aspectos de Linux están ligados a precedentes históricos. Un poco de cultura sobre Linux puede ser útil a la hora de solventar problemas potenciales antes de que surjan.
- *Explicación acerca de cómo funciona Linux* — Aunque no es necesario profundizar en la mayoría de los aspectos del kernel Linux, es conveniente saber algo sobre cómo ha surgido Linux. Puede ser especialmente importante si está trabajando con otros sistemas operativos, ya que algunas de las suposiciones que tiene sobre cómo funcionan los ordenadores pueden no cumplirse en Linux.
- *Vista preliminar a un comando de introducción (con ejemplos)* — Probablemente esto es lo más importante a buscar en la documentación linux. La filosofía de Linux es que es mejor usar pequeños comandos conectados de diferentes modos, que utilizar pocos comandos amplios (y complejos) que hagan todo el trabajo por si mismos. Sin algunos ejemplos que ilustren el acercamiento a

Linux para hacer cosas , se puede sentir intimidado por el gran número de comandos disponibles en el sistema Red Hat Linux.

Tenga en cuenta que no tiene que memorizar todos los comandos Linux. Existen diversas técnicas para ayudarle a encontrar el comando específico que necesita para realizar un tarea determinada. Tan sólo necesita saber el modo en que Linux funciona, lo que necesita llevar a cabo y cómo acceder a la herramienta que le dará las instrucciones exactas para ejecutar el comando.

La *Official Red Hat Linux x86 Installation Guide* constituye una referencia excelente de ayuda para instalar y configurar con éxito su sistema Red Hat Linux. La *Official Red Hat Linux Getting Started Guide* cubre la historia de Linux, los comandos de sistema básicos, GNOME, KDE, RPM y otros muchos conceptos fundamentales. Debería empezar con estos dos libros y usarlos para conseguir una base de conocimiento sobre su sistema Red Hat Linux. Verá como después los conceptos más complicados empezarán a tener sentido, una vez que tenga las conceptos básicos claros.

A parte de leer los manuales Red Hat Linux, existen otras fuentes excelentes de documentación disponibles por poco dinero o gratis.

Introducción a sitios Web Linux

- http://www.redhat.com — en el sitio Web, podrá encontrar enlaces del proyecto de documentación Linux (LDP), versiones en línea de las FAQs (preguntas y respuestas más frecuentes), una base de datos que puede ayudarle en la búsqueda de grupos de usuarios Linux cercanos a usted, información técnica en la base de conocimientos de soporte de Red Hat y mucho más.
- http://www.linuxheadquarters.com — El sitio Web de la sede central de Linux le ofrece guías fáciles para una variedad de tareas Linux.

Introducción a los newsgroups Linux

Puede participar en newsgroups viendo las conversaciones de otros intentando solventar problemas, o bien puede participar activamente preguntando y contestando. Los usuarios experimentados de Linux le serán de una gran ayuda — especialmente si sus preguntas van a parar al punto de reunión justo. Si no tiene acceso a una aplicación de lector de noticias, puede acceder a esta información vía web en http://www.deja.com. Existen docenas de newsgroups relacionados con Linux entre las que se incluyen:

- linux.help — Un buen lugar donde encontrar ayuda de compañeros usuarios de Linux.
- linux.redhat — Este newsgroup cubre aspectos específicos a Red Hat Linux.
- linux.redhat.install — Para preguntas sobre instalación o para ver cómo otros han resuelto problemas similares.
- linux.redhat.misc — Preguntas o peticiones de ayuda que no encajan en ninguna de las categorías tradicionales.

- linux.redhat.rpm — Sitio donde dirigirse si tiene problemas con el uso de RPM para conseguir algún propósito en particular.

Libros sobre Linux

- *Red Hat Linux for Dummies, 2* edición* de Jon "maddog" Hall; IDG
- *Special Edition Using Red Hat Linux* de Alan Simpson, John Ray y Neal Jamison; Que
- *Running Linux* de Matt Welsh y Lar Kaufman; O'Reilly & Associates
- *Red Hat Linux 7 Unleashed* de William Ball y David Pitts; Sams

Los libros aquí sugeridos constituyen fuentes excelentes de información para un conocimiento básico del sistema Red Hat Linux. Para una información más detallada sobre los diversos temas que aparecerán a través del libro, muchos de los capítulos listan títulos de libros específicos, habitualmente en la parte de *Recursos adicionales*.

Para los más experimentados

Si ha utilizado otras distribuciones Linux, tendrá un dominio básico de los comandos usados más frecuentemente. Puede que haya instalado su propio sistema Linux e incluso haya descargado y creado software que ha encontrado en Internet. Después de instalar Linux, no obstante, los puntos sobre configuración pueden ser confusos.

La *Official Red Hat Linux Customization Guide* está diseñada para ayudar a explicar los diversos modos en que su sistema puede ser configurado. Utilice este manual para aprender las opciones de configuración y cómo ponerlas en práctica.

Cuando instale software que no aparezca en la *Official Red Hat Linux Customization Guide*, le será útil ver lo que otra gente en las mismas circunstancias ha hecho. Los documentos HOWTO del LDP (proyecto de documentación de Linux), disponibles en http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, documentan aspectos particulares de Linux, desde cambios del kernel hasta el uso de Linux en una estacisn de trabajo "radio amateur".

Documentación para gurús de Linux

Si es un usario Red Hat Linux desde hace tiempo. sabrá probablemente que uno de los mejores modos para entender un programa en particular es leyendo su código fuente y/o sus archivos de configuración. Una gran ventaja de Red Hat Linux es la disponibilidad del código fuente para cualquiera.

Obviamente, no todo el mundo es programador de C, por lo que el código fuente no le puede ser de ayuda. Sin embargo, si tiene los conocimientos y la habilidad necesarios para leerlo, el código fuente alberga todas las respuestas.

Convenciones del documento

Cuando lea este manual, verá que algunas palabras aparecen con fuentes, tamaños y grosores diferentes. Este método de evidenciado es sistemático; palabras diferentes son representadas en el mismo estilo para indicar su inclusión en una categoría específica. Los tipos de palabras representados de este modo incluyen:

`commando`

Los comandos Linux (y otros comandos del sistema operativo, cuando son usados) se representan de este modo. Este estilo debería indicarle que puede introducir la palabra o frase en la línea de comandos y pulsar [Intro] para solicitar un comando. A veces, un comando contiene palabras que verá en un estilo diferente cuando aparezcan solas (por ejemplo, nombres de archivo). En estos casos, son consideradas como parte del comando, de modo que la frase entera aparecerá como un comando. Ejemplo:

Use el comando `cat testfile` para visionar los contenidos de un archivo, llamados `testfile`, en el directorio en el que se está trabajando.

`nombre de archivo`

Los nombres de archivo, nombres de directorio, rutas y nombres de paquetes del RPM se presentan de este modo. Este estilo debería indicar que un archivo o un directorio en particular existen con ese nombre en su sistema Red Hat Linux. Por ejemplo:

El archivo `.bashrc` del directorio raíz, contiene definiciones de bash shell y aliases para su propio uso.

El archivo `/etc/fstab` contiene información sobre los diversos dispositivos de sistema y sistema de archivos.

El directorio `/usr/share/doc` contiene documentación para varios programas.

Instale el RPM de `webalizer` si quiere utilizar un programa de análisis de archivo log del servidor web.

aplicación

Este estilo le indica que el programa nombrado es una aplicación para el usuario final. Por ejemplo:

Use Netscape Navigator para navegar por la web.

[tecla]

Una tecla del teclado aparece en este estilo. Ejemplo:

Para usar la funcionalidad de completar palabras [Tab], escriba un carácter y pulse la tecla [Tab]. Su terminal visualizará la lista de archivos en el directorio que inician con esa letra.

[tecla]-[combinación]

Una combinación de teclas se representa del siguiente modo. Por ejemplo:

La combinación de teclas [Ctrl]-[Alt]-[Atrás] reiniciará el sistema X Window.

texto encontrado en una interfaz GUI

Un pequeña palabra o frase encontrada en una pantalla o ventana de interfaz GUI aparecerá en este estilo. Cuando aparezca, se usa para identificar un pantalla GUI o un elemento en una pantalla GUI (por ejemplo, un texto asociado con una casilla de verificación o un campo). Por ejemplo:

En la pantalla de GNOME **Centro de control**, usted puede personalizar su gestor de ventanas GNOME.

Seleccione la casilla de verificación **contraseña requerida** si desea que su salvapantallas le pida una contraseña antes de deterse.

nivel superior de un menú en una pantalla o ventana GUI

Cuando vea una palabra en este estilo, significa que la palabra esta en el nivel superior de un menú descendente. Si hace click en la palabra de la pantalla GUI, debería aparecer el resto del menú. Ejemplo:

En un terminal GNOME bajo **Configuración**, verá los siguientes componentes del menú: **Preferencias**, **Terminal de reinicio**, **Reiniciar y borrar** y **Selector de color**.

Si necesita seleccionar una secuencia de comandos en el menú GUI, éstos serán mostrados como en el siguiente ejemplo:

Haga click en **Programas**=>**Aplicaciones**=>**Emacs** Para iniciar el editor de texto Emacs.

botón de una pantalla o ventana GUI

Este estilo indica el texto que encontrará al hacer click en un botón de la pantalla GUI. Ejemplo:

Haga click en el botón **Atrás** para volver a la última página web que ha visto.

`salida de datos del ordenador`

Cuando vea el texto en este estilo, significa que el ordenador visualiza el texto en la línea de comandos. Verá respuestas a comandos que usted ha escrito, mensajes de error e indicadores de comandos interactivos para su entrada durante los scripts o programas visualizados de este modo. Ejemplo:

Use el comando `ls` para visualizar el contenido de un directorio:

```
$ ls
Desktop              axhome          logs          nirvana.gif
Mail                 backupfiles     mail          reports
```

La salida de respuesta al comando (en este caso, los contenidos del directorio) aparecen en este estilo.

`indicador de comandos`

Un indicador de comandos, es la forma que tiene el ordenador de decirle que está preparado para que la entrada de datos. Ejemplos:

```
$
```

```
#
```

```
[truk@bleach truk]$
```

```
leopard login:
```

`entrada de datos de usuario`

Texto que debe escribir el usuario, en la línea de comandos o en la casilla del texto en una pantalla GUI. En el siguiente ejemplo, el **`texto`** aparece en este estilo:

Para arrancar su sistema en una programa de instalación en modo texto, deberá escribir en el comando **`texto`** en el indicador de comandos `boot:`.

Otro ejemplo, con la palabra **`root`** visualizada para que el usuario deba escribir algo dentro:

Si necesita registrarse como root cuando se registre por primera vez en su sistema y va a utilizar la pantalla gráfica de login, escriba **`root`**. Teclee la contraseña de root en el indicador de comandos `Password`.

entrada de glosario

Palabra que aparece en el glosario y que aparece en el documento en este estilo. Ejemplo:

El **demonio** lpd gestiona las peticiones de impresión.

En este caso, el estilo de la palabra **demonio** debería indicarle que una definición de la palabra está disponible en el glosario.

Se usan, además, diferentes estrategias para centrar su atención en determinada información. Esta información será marcada en orden de importancia para su sistema como: nota, advertencia o atención. Por ejemplo:

Nota

Recuerde que Linux es sensible a minúsculas y mayúsculas. Es decir, no es lo mismo escribir rosa, que ROSA o rOsA.

No haga tareas rutinarias como root — use una cuenta de usuario normal a menos que necesite usar la cuenta de root para administrar su sistema.

Si escoge no hacer un particionamiento manual, una instalación de tipo servidor borrará todas las particiones existentes en todos los discos duros. No escoja este tipo de instalación a menos que esté seguro de que no tiene datos que necesite salvar.

Uso del ratón

Red Hat Linux está diseñado para usar un ratón de tres botones. Si tiene un ratón de dos botones, debería haber seleccionado la emulación de tres botones durante el proceso de instalación. Si está utilizando la emulación de tres botones, pulsar los dos botones del ratón al mimo tiempo corresponde a pulsar el tercer botón (el central).

En este documento, cuando se le indica que haga click con el ratón sobre algo, significa pulsar el botón izquierdo. De tener que usar el botón central o derecho, le será indicado explícitamente. (Naturamente, todo esto será al revés si su ratón ha sido configurado para una persona zurda.)

La frase "arrastrar y soltar" le debe ser familiar. Si se indica arrastrar y soltar un elemento de su escritorio GUI, haga click en este elemento y mantenga el botón del ratón pulsado mientras arrastra el elemento moviendo el ratón hacia la nueva ubicación. Cuando haya alcanzado la ubicación deseada, deje de apretar el botón del ratón para soltar el elemento.

Copiar y pegar un texto con X

Copiar y pegar un texto mediante el uso del ratón y del sistema X Window es fácil. Para copiar un texto, haga click y arrastre el ratón sobre el texto para resaltararlo. Para copiarlo en algún sitio, haga click en el botón central del ratón en el lugar justo donde quiere copiar el texto.

Aún hay más

La *Official Red Hat Linux Reference Guide* constituye parte del compromiso de Red Hat de proporcionar un soporte útil y oportuno a los usuarios de Red Hat Linux. Las ediciones futuras albergarán información ampliada sobre los cambios en la estructura del sistema y la organización, herramientas de seguridad potentes y otros recursos que le ayudarán a ampliar las posibilidades de su sistema Red Hat Linux y su habilidad para usarlo.

Aquí es donde le pedimos su ayuda.

¡Necesitamos saber su opinión!

Si encuentra un error en la *Official Red Hat Linux Reference Guide* o si tiene ideas para mejorar este manual, nos encantaría saberlo. Envíe un comentario a Bugzilla (http://bugzilla.redhat.com/bugzilla) mencionando la *Official Red Hat Linux Reference Guide*.

Asegúrese de mencionar el identificador del manual:

```
rhl-rg(ES)-7.1-Print-RHI (2001-02-21T10:50-0500)
```

Si menciona el identificador del manual, sabremos con exactitud qué versión de la guía tiene.

Si tiene alguna sugerencia para mejorar la documentación, intente ser lo más específico posible al describirla. Si ha encontrado un error, incluya el número de sección y una parte del texto de alrededor para que podamos encontrarlo fácilmente.

Regístrese para obtener soporte

Si tiene una edición oficial de Red Hat Linux 7.1, no olvide registrarse para obtener los beneficios que le corresponden como cliente de Red Hat.

Tiene derecho a todos estos beneficios, dependiendo del producto oficial Red Hat Linux que haya comprado:

- Soporte oficial Red Hat — Obtenga ayuda con las preguntas de instalación del equipo de soporte de Red Hat, Inc..
- Red Hat Network — Actualice sus paquetes con facilidad y reciba mensajes de seguridad personalizados para su sistema. Vaya a http://www.redhat.com/network para más detalles.
- Acceso prioritario FTP — No más visitas a sitios espejo. Los propietarios de Red Hat Linux 7.1 reciben acceso gratuito a priority.redhat.com, el servicio FTP preferido por los clientes de Red Hat, que ofrece conexiones con elevado ancho de banda noche y día.
- *E-Newsletter oficial de Red Hat* — Cada mes, obtenga las últimas noticias informaciones sobre productos directamente de Red Hat.

Para registrarse para obtener soporte técnico, vaya a http://www.redhat.com/apps/activate. Encontrará el ID de su producto en una tarjeta negra, roja y blanca en la caja oficial de Red Hat Linux.

Para leer más acerca del soporte técnico para Red Hat Linux, remítase al apéndice *Obtención de soporte técnico* en la *Official Red Hat Linux x86 Installation Guide*.

¡Buena suerte y gracias por haber escogido Red Hat Linux!!

Equipo de documentación de Red Hat

Parte I El sistema

1 Estructura del sistema de ficheros

1.1 ¿Por qué compartir una estructura común?

Una estructura de sistema de ficheros de un sistema operativo es el nivel más básico de organización. Casi siempre un sistema operativo interactúa con sus usuarios, aplicaciones y modelos de seguridad que dependen de la manera en que almacena los ficheros en un dispositivo de almacenamiento primario (normalmente una unidad de disco duro). Por varios motivos, es muy importante que los usuarios, así como los programas para la instalación y demás, sean capaces de referirse a unas pautas comunes para saber donde escribir y leer los ficheros binarios, la configuración, registro y otros ficheros.

Un sistema de ficheros se podría resumir en términos de dos categorías diferentes de ficheros:

- ficheros compartibles vs. no compartibles
- ficheros variables vs. estáticos

Los ficheros **compartibles** son aquéllos a los que se puede acceder desde varios hosts; mientras que los ficheros **no compartibles** no están disponibles a todos los hosts. Los ficheros **variables** pueden cambiar en cualquier momento sin una intervención del gestor de sistemas (activa o pasiva); los ficheros **estáticos**, tales como documentación y binarios, no cambian sin una actuación por parte del gestor de sistemas o de una agente que el gestor de sistemas haya escogido para realizar esta tarea.

El hecho de que estos ficheros sean vistos de esta manera se debe al tipo de permisos otorgados por el directorio que los sostiene. El modo en que el sistema operativo y sus usuarios necesitan utilizar los ficheros determina el directorio en el cual estos ficheros deberían estar ubicados, dependiendo de si el directorio está montado sólo en modo escritura o en modo lectura-escritura. El nivel más alto de esta organización es crucial, de la misma manera que el acceso a los directorios marcados puede ser restringido o se podrían manifestar problemas de seguridad si el nivel más alto se queda desorganizado o sin una estructura ampliamente utilizada.

No obstante, el hecho de tener simplemente una estructura no significa mucho a menos que ésta sea estándar. Las estructuras competitivas pueden causar más problemas de los que solucionan. Por esta razón, Red Hat ha escogido la estructura de sistema de ficheros y la ha extendido ligeramente para acomodar los ficheros especiales usados en Red Hat Linux.

1.2 Vista preliminar al estándar de jerarquía del sistema de ficheros (FHS)

Red Hat se ha comprometido a respetar el **Estándar de Jerarquía del Sistema Ficheros** (**FHS** del inglés Filesystem Hierarchy Standard), un documento de consenso que define los nombres y la situación

de muchos ficheros y directorios. En el futuro se seguirá el estándar para asegurar la compatibilidad de Red Hat Linux

El documento que define el FHS es la referencia autorizada para cualquier sistema compatible FHS, sin embargo el estándar da pie a la extensibilidad de unas áreas o no define otras. En esta sección se proporciona un resumen del estándar y una descripción de aquellas partes del sistema de ficheros que no cubre el estándar.

El estándar completo está disponible en:

http://www.pathname.com/fhs

El cumplimiento del estándar significa varias cosas, los dos aspectos más importantes son la compatibilidad con otros sistemas que siguen el estándar y la capacidad de poder montar la partición `/usr` en modo sólo lectura pues contiene ejecutables comunes y no está pensado para ser alterada por los usuarios. Por este motivo, `/usr` puede ser montado directamente desde el CD-ROM o desde otro ordenador vía NFS en modo sólo lectura.

1.2.1 Organización de FHS

Los directorios y ficheros aquí anotados, son sólo un subconjunto de los especificados por el FHS. Véase la última versión del FHS para una descripción detallada.

Directorio `/dev`

El directorio `/dev` contiene archivos que representan dispositivos del sistema. Estos archivos son esenciales para el correcto funcionamiento del sistema.

Directorio `/etc`

El directorio`/etc` está reservado para archivos de configuración que afectan directamente a su ordenador. No deben colocarse ejecutables en `/etc`. Los ejecutables que antiguamente se colocaban en `/etc` deberían estar en `/sbin` o posiblemente en `/bin`.

Los directorios `X11` y `skel` deben ser subdirectorios de `/etc`:

```
/etc
  |- X11
  |- skel
```

El directorio `X11` es para archivos de configuración de X11 como `XF86Config`. El directorio `skel` es para archivos "esqueleto" (del inglés "skeleton") para usuarios, archivos que se utilizan para rellenar el directorio raíz de un usuario cuando éste es creado.

Directorio /lib

El directorio /lib debería contener sólo las librerías necesarias para ejecutar los binarios en /bin y /sbin. Estas imágenes de librerías compartidas son particularmente importantes para arrancar el sistema y ejecutar comandos en el sistema de ficheros de root.

Directorio /mnt

El directorio /mnt se refiere a sistemas de ficheros montados temporalmente, tales como CD-ROMs y discos flexibles.

Directorio /opt

El directorio /opt proporciona un área para almacenar habitualmente paquetes de software de una aplicación estática y amplia.

Para paquetes en los que se evite poner ficheros a través del sistema de ficheros, proporciona un sistema de organización predecible y lógico bajo el directorio de paquetes. Esto le aporta al gestor del sistema un modo sencillo de determinar el rol de cada fichero en un paquete particular.

Por ejemplo, si sample fuese el nombre de un paquete de software particular localizado en /opt, todos sus ficheros podrían ser emplazados en directorios dentro de /opt/sample, tales como /opt/sample/bin para binarios y /opt/sample/man para páginas de manual.

Los paquetes grandes que abarcan diferentes subpaquetes, cada uno de los cuales desempeñan una tarea especifica, también funcionan con /opt, aportando a este gran paquete un modo estándar de organizarse. De este modo, el paquete sample tendrá diferentes herramientas cada una de las cuales irá a sus subdirectorios, tales como /opt/sample/tool1 y /opt/sample/tool2, cada uno de los cuales puede tener su propio bin, man y otros directorios similares.

Directorio /sbin

El directorio /sbin es para ejecutables usados sólo por el usuario root. Los ejecutables en /sbin sólo se usan para arrancar y montar /usr y ejecutar operaciones de recuperación del sistema. El FHS dice:

> "/sbin contiene típicamente archivos esenciales para arrancar el sistema además de los binarios en /bin. Cualquier archivo ejecutado tras /usr , será montado (si no surge ningún problema) y ubicado en /usr/sbin. Los binarios de administración de sistema sólo local, deberían ser ubicados en /usr/local/sbin.

Los siguientes programas deberían encontrarse, al menos, en /sbin:

```
arp, clock, getty, halt, init, fdisk,
fsck.*, ifconfig, lilo, mkfs.*, mkswap, reboot,
route, shutdown, swapoff, swapon, update
```

Directorio /usr

El directorio /usr es para archivos que puedan ser compartidos a través de todo el sitio. El directorio /usr habitualmente tiene su propia partición y debería ser montable en sólo lectura. Los siguientes directorios deberían ser subdirectorios /usr:

```
/usr
  |- bin
  |- doc
  |- etc
  |- games
  |- include
  |- kerberos
  |- lib
  |- libexec
  |- local
  |- man
  |- sbin
  |- share
  |- src
  |- X11R6
```

El directorio bin contiene ejecutables, doc contiene páginas de documentación incompatibles con FHS, etc contiene ficheros de configuración de sistema, games es para juegos, include contiene los ficheros de cabecera C, kerberos contiene binarios y muchos más ficheros de Kerberos y lib contiene ficheros objeto y librerías que no están diseñadas para ser directamente utilizadas por usuarios o scripts de shell. El directorio libexec contiene programas de pequeña ayuda llamados por otros programas, sbin es para los binarios de administración del sistema (aquéllos que no pertenecen a /sbin), share contiene ficheros que no son de una arquitectura específica, src es para el código fuente y X11R6 es para el sistema X Window (XFree86 de Red Hat Linux).

Directorio /usr/local

El FHS dice:

> "La jerarquía /usr/local es para uso del gestor del sistema al instalar localmente el software. Necesita ser seguro para ser sobreescrito cuando el software del sistema es compartible entre un grupo de hosts, pero no se encuentra en /usr."

El directorio /usr/local es similar en estructura al directorio /usr. Tiene los siguientes subdirectorios, que son similares a los del directorio /usr:

```
/usr/local
       |- bin
       |- doc
       |- etc
```

```
        |- games
        |- info
        |- lib
        |- man
        |- sbin
        |- src
```

Directorio `/var`

Ya que el FHS requiere que sea capaz de montar `/usr` en sólo lectura, cualquier programa que escriba ficheros log o que necesite los directorios `spool` o `lock` debería escribirlos en el directorio `/var`. El FHS constata que `/var` es para:

> "…ficheros de datos variables. Esto incluye ficheros spool, de administración, de registro y ficheros temporales."

Los siguientes directorios deberían ser subdirectorios de `/var`:

```
/var
  |- arpwatrch
  |- cache
  |- db
  |- ftp
  |- gdm
  |- kerberos
  |- lib
  |- local
  |- lock
  |- log
  |- named
  |- nis
  |- opt
  |- preserve
  |- run
  +- spool
       |- anacron
       |- at
       |- cron
       |- fax
       |- lpd
       |- mail
       |- mqueue
       |- news
       |- rwho
       |- samba
       |- slrnpull
```

```
        |- squid
        |- up2date
        |- uucp
        |- uucppublic
        |- vbox
        |- voice
    |- tmp
    |- www
    |- yp
```

Los ficheros log de sistema tales como `messages` y `lastlog` estan en `/var/log`. El directorio `/var/lib/rpm` también contiene el sistema de datos RPM. Los ficheros lock van en `/var/lock`, habitualmente en directorios particulares para el programa en el uso del fichero. El directorio `/var/spool` tiene subdirectorios para varios sistemas que necesitan almacenar los ficheros de datos de almacenamiento.

1.2.2 `/usr/local` en Red Hat Linux

En Red Hat Linux, el uso del directorio `/usr/local` es ligeramente diferente de lo especificado por FHS. El FHS establece que en `/usr/local` debería memorizarse el software que permanece seguro en las actualizacione de software de sistemas. Ya que las actualizaciones de sistemas de Red Hat se han realizado de forma segura con `/usr/local` y Gnome-RPM, no necesita proteger archivos poniéndolos en `/usr/local`. Le recomendamos que use `/usr/local` para el software local de su máquina.

Por ejemplo, si usted ha montado `/usr` mediante sólo lectura de NFS desde un host local llamado `jake`. Si existe un paquete o programa que le gustaría instalar, pero no le es posible escribir en `jake` debería instalarlo bajo `/usr/local`. Si ha conseguido que el gestor de sistema de `jake` instale el programa en `/usr`, puede desinstalarlo desde `/usr/local`.

1.3 `/proc` y sus" ficheros"

El directorio `/proc` contiene "ficheros" especiales que o bien extraen información del kernel o bien la envían a éste.

No obstante, el directorio `/proc` es mucho más potente de lo que inicialmente se pueda pensar. A través de los diversos ficheros en este directorio (que realmente no son ficheros sino interfaces en el kernel), un gestor de sistema puede utilizar `/proc` como un método fácil para acceder a información sobre el estado del kernel, los atributos de la máquina, los estados de los procesos individuales y mucho más. Al usar `cat` en combinación con las interfaces dentro de `/proc`, puede acceder immediatamente a una cantidad enorme de información sobre cualquier sistema. Vea el ejemplo, si desea saber cómo están asignados los registros de memoria en su ordenador:

```
[truk@tictactoe /proc]$ cat iomem
```

```
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-002553d7 : Kernel code
  002553d8-0026d91b : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140
  ea000000-ea00007f : eth0
ffff0000-ffffffff : reserved
[truk@tictactoe /proc]$
```

Si se conectara a una máquina desconocida y quisiera saber su tipo de CPU y velocidad, puede usar el siguiente comando:

```
cat /proc/cpuinfo
```

Se pueden añadir otros bits válidos de información sobre el sistema desde `cmdline`, `meminfo`, `partitions` y `version`, entre otros.

Los directorios en `/proc` simbolizan una información sobre una aplicación particular o proceso. Por ejemplo, el directorio `/proc/sys/kernel` está lleno de información sobre el kernel, como por ejemplo, el número máximo de cadenas (`threads-max`) y el número máximo de mensajes (`msg-max`).

1.4 Directorios especiales de Red Hat Linux

Además de los archivos concernientes al sistema RPM que se encuentran en `/var/lib/rpm` (véase el capítulo RPM para obtener más información sobre RPM), hay otras dos localizaciones especiales que están reservadas para la configuración y el mantenimiento de Red Hat Linux.

Las herramientas de configuración proporcionadas por Red Hat Linux instalan muchos scripts, mapas de bits y ficheros de texto en `/usr/lib/rhs`. Ya que estos ficheros son generados por software de su sistema, probablemente no deseará modificar ninguno de ellos.

Otra de las ubicaciones especiales (`/etc/sysconfig`) almacena la información de la configuración. Muchos scripts que se ejecutan al iniciar el sistema, usan los ficheros de este directorio. Estos

ficheros pueden ser modificados, pero también pueden ser configurandos usando Linuxconf, una herramienta del panel de control u otra herramienta de configuración. Consulte la *Official Red Hat Linux Customization Guide* para instrucciones sobre el uso de Linuxconf.

2 Usuarios y grupos

Existe control de **usuarios** y **grupos** en el núcleo de la administración del sistema de Red Hat Linux.

Los **usuarios** pueden ser gente real (cuentas ligadas a un usuario físico en particular) o usuarios lógicos (cuentas existentes para aplicaciones particulares). Ambos tipos de usuarios, reales o lógicos, tienen un **ID de usuario** y un **ID de grupo**. Los IDs de usuario habitualmente son únicos (pero no tienen por qué serlo).

Los **grupos** son siempre expresiones lógicas de organización. Los usuarios forman grupos y los grupos forman fundaciones de usuarios ligados a los que les dan permisos de lectura, escritura o de ejecución de un archivo determinado.

Cualquier archivo creado se asigna a un usuario y a un grupo cuando se crea, de la misma manera que se asignan la lectura, la escritura y la ejecución de permisos para el propietario del archivo, para el grupo asignado al archivo y para cualquier otro usuario en un host. El usuario y el grupo de un archivo particular, así como los permisos en ese archivo, pueden ser cambiados por un root o, en menor grado, por el creador de un archivo.

Una de las tareas más importantes de cualquier administrador del sistema, es la de asignar y revocar permisos. Afortunadamente, Red Hat Linux hace este trabajo lo más sencillo posible al mismo tiempo que preserva la seguridad de los archivos en el host.

2.1 Herramientas para usuarios y gestión de grupos

La gestión de usuarios y grupos ha sido tradicionalmente tediosa, pero Red Hat Linux posee algunas herramientas y convenciones que facilitan el manejo de usuarios y grupos.

De la misma manera que puede utilizar `useradd` para crear un nuevo usuario desde un intérprete de comandos de la shell, un manera bastante conocida de manejar usuarios y grupos es a través de Linuxconf (consulte la *Official Red Hat Linux Customization Guide* para más detalles sobre Linuxconf).

2.2 Usuarios estándar

En la Tabla 2–1, *Usuarios estándar*, puede econtrarse la lista de usuarios estándar creada por el proceso de instalación. (esencialmente el archivo `/etc/passwd`). El ID de grupo (GID) en esta tabla es el *grupo primario* para el usuario. Véase la Sección 2.4, *Grupos privados de usuarios* para más información sobre cómo se utilizan los grupos.

Tabla 2–1 Usuarios estándar

Usuario	UID	GID	Directorio raíz	Shell
root	0	0	/root	/bin/bash
bin	1	1	/bin	
daemon	2	2	/sbin	
adm	3	4	/var/adm	
lp	4	7	/var/spool/lpd	
sync	5	0	/sbin	/bin/sync
shutdown	6	0	/sbin	/sbin/shutdown
halt	7	0	/sbin	/sbin/halt
mail	8	12	/var/spool/mail	
news	9	13	/var/spool/news	
uucp	10	14	/var/spool/uucp	
operator	11	0	/root	
games	12	100	/usr/games	
gopher	13	30	/usr/lib/gopher-data	
ftp	14	50	/var/ftp	
nobody	99	99	/	

2.3 Grupos estándar

En la Tabla 2–2, *Grupos estándar*, encontrará los grupos estándar configurados en el proceso de instalación (esto es básicamente el fichero `/etc/group`).

Tabla 2–2 Grupos estándar

Grupo	GID	Miembros
root	0	root
bin	1	root, bin, daemon

Grupo	GID	Miembros
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
nobody	99	
users	100	

2.4 Grupos privados de usuarios

Red Hat Linux utiliza un esquema de **grupo privado de usuario** (**UPG**), que hace que los grupos UNIX sean más fáciles de usar. El esquema UPG no añade ni cambia nada en el modo estándar de UNIX en el manejo de grupos; simplemente ofrece una nueva convención. Siempre que cree un usuario nuevo, por defecto, éste pertenece a un único grupo. El esquema funciona de la siguiente manera:

Grupo de usuario privado

Cada usuario tiene un grupo primario; el usuario es el único miembro del grupo.

umask = 002

La máscara de permisos umask para sistemas UNIX es habitualmente de 022, lo que elimina de la posibilidad de que otros usuarios *y otros miembros del grupo primario del usuario* eliminen ficheros del usuario. Puesto que cada usuario tiene su propio grupo privado en el esquema UPG, esta "protección de grupo" no es necesaria. Una umask de 002 prohibirá a los usuarios modificar ficheros privados de otros usuarios. El valor de umask se asigna en `/etc/profile`

activar el bit setgid en un directorio

Si activa el bit setgid en un directorio (con `chmod g+s` *`directorio`*), los archivos creados en ese directorio tendrán su propio grupo en el grupo del directorio.

En la mayoría de las organizaciones de IT (del inglés Information Technologies) se crea un grupo para cada proyecto y se asigna a la gente a los grupos en los que deben estar. Gestionar los archivos ha sido tradicionalmente difícil, porque cuando alguien crea un archivo, éste pertenece al grupo primario al que pertenezca el creador. Cuando una misma persona trabaja en múltiples proyectos, es difícil asociar un grupo adecuado con los ficheros adecuados. Con el esquema UPG, la asignación de grupos a archivos creados en ese directorio es automática, lo que permite gestionar grupos de proyectos de manera simple.

Suponiendo que estemos ejecutanto un proyecto llamado *devel*, con muchos usuarios que modifican los ficheros `devel` en un directorio `devel`. Cree un grupo llamado `devel`, aqada el directorio `devel` (`chgrp`) y todos los usuarios del proyecto a `devel`.

Puede añadir un usuario a un grupo usando Linuxconf (consulte la *Official Red Hat Linux Customization Guide*). Si prefiere usar la línea de comandos, utilice `/usr/sbin/groupadd` *`groupname`* command> para crear un grupo. El comando `/usr/bin/gpasswd -a` *`loginname groupname`* añadirá un *loginname* de usuario a un grupo. (Consulte `groupadd` y la páginas de manual `gpasswd` si necesita más información sobre sus opciones.) El archivo `/etc/group` contiene la información de grupo para su sistema.

Si ha creado el grupo `devel`, ha añadido usuarios al grupo `devel`, cambiado el grupo por el directorio `devel` en el grupo `devel` y activado el bit de setgid para el directorio `devel`, todos los usuarios *devel* serán capaces de conservar su estatus de grupo `devel`, para que otros usuarios *devel* sean capaces de modificarlos.

Si se tienen múltiples proyectos como *devel* y usuarios que trabajan en múltiples proyectos, estos usuarios nunca tendrán que cambiar su umask o grupo cuando cambien de proyecto. El bit setgid en el directorio principal de cada proyecto "selecciona" el grupo adecuado.

Puesto que el directorio raíz de cada usuario pertenece al usuario y a su grupo privado, es seguro dejar activado el bit setgid en el directorio raíz del usuario. Sin embargo, por defecto, los archivos se crean con el grupo primario del usuario, así que el bit setgid resulta redundante.

2.4.1 Concepto de grupo privado de usuario

Aunque UPG ha existido en Red Hat Linux durante algún tiempo, mucha gente todavía tiene preguntas, tales como, por qué es necesario UPG. A continuación observe el esquema.

- Para que un grupo de usuarios trabaje en un conjunto de ficheros en, por ejemplo, el directorio `/usr/lib/emacs/site-lisp`. Es razonable que unas cuantas personas accedan al directorio, pero no todo el mundo.
- En primer lugar cree `emacs`:

  ```
  /usr/sbin/groupadd emacs
  ```

  A continuación, teclee:

  ```
  chown -R root.emacs /usr/lib/emacs/site-lisp
  ```

  para asociar los contenidos del directorio con el grupo `emacs` y añadir usuarios adecuados al grupo:

  ```
  /usr/bin/gpasswd -a <username> emacs
  ```

- Para permitir a los usuarios crear archivos en el directorio teclee:

  ```
  chmod 775 /usr/lib/emacs/site-lisp
  ```

- Cuando un usuario crea un nuevo archivo, se le asigna el grupo del grupo del usuario por defecto (habitualmente `users`). Para evitarlo, teclee:

  ```
  chmod 2775 /usr/lib/emacs/site-lisp
  ```

  que hace que todo lo que se cree en el directorio tenga el grupo "emacs".
- Para que un usuario del grupo emacs pueda modificar un archivo nuevo, es necesario que éste sea creado con la modalidad 664. Para tal propósito, debe utilizar unmask por defecto.
- Todo esto funciona bien, salvo que si el grupo por defecto es "usuarios", todos los archivos creados en el directorio raíz del usuario serán sobreescribibles por cualquier miembro del grupo "usuarios" (habitualmente todos los usuarios).
- Para solucionar esto, se hace que cada usuario tenga un "grupo privado" como grupo por defecto.

Llegados a este punto, al hacer la umask 002 por defecto y dar a todo el mundo un grupo privado por defecto, se pueden crear fácilmente grupos de los que los usuarios pueden sacar provecho sin realizar ningún tipo de magia. Simplemente se crea el grupo y se añaden los usuarios, se ejecuta el comando `chown` y `chmod` en los directorios del grupo.

3 Proceso de arranque, inicio y cierre del sistema

Este capítulo contiene información sobre lo que ocurre al arrancar o apagar un sistema bajo Red Hat Linux.

3.1 Introducción

Uno de los aspectos más importantes de Red Hat Linux consiste en su método para encender y apagar el sistema operativo, que cuando carga programas específicos usando sus configuraciones particulares, permite el cambio de esas configuraciones para controlar el proceso de arranque y apagar de manera ordenada. Mientras otros sistemas operativos intentan controlar la manera en que el ordenador arranca o le impiden personalizar lo que sucede en el apagado, Red Hat Linux le permite acceder completamente a cada paso del proceso.

Además del problema del control de arranque o del proceso de cierre, Red Hat Linux hace que sea mucho más fácil determinar la causa precisa de la mayoría de los problemas relacionados con el encendido y el apagado de su sistema. La comprensión de este proceso es de gran ayuda para la resolución de problemas básicos.

3.2 Entre bastidores en el proceso de arranque.

Nota

Esta sección trata del proceso de arranque x86 en particular. Según la arquitectura de su sistema, su proceso de arranque podría ser ligeramente diferente. Sin embargo, una vez que el sistema haya encontrado y cargado el núcleo, el proceso de arranque predeterminado de Red Hat Linux es idéntico para todas las arquitecturas. Para más información acerca de un proceso de arranque diferente al x86 consulte la sección Sección 3.8, *Diferencias en el proceso de arranque en otras arquitecturas*.

Cuando el ordenador está encendido, el procesador busca la **BIOS** (Entrada/Salida Básica del sistema) en la ROM del equipo y lo ejecuta. El programa de la BIOS está escrito dentro de la memoria permanente de sólo lectura (ROM) y está siempre disponible para el uso. El programa de la BIOS provee el más bajo nivel de interfaz para dispositivos periféricos y controla el primer paso del proceso de arranque.

El programa de la BIOS prueba el sistema, busca y controla los periféricos y después busca una unidad en uso para activar el sistema. Normalmente, busca en la disquetera (o en la unidad CD-ROM de los sistemas más nuevos) medios de arranque, si los hubiera, y luego se dirije a la unidad del disco duro. El orden de las unidades usadas para el arranque se controla normalmente por medio de una configuración especial de la BIOS en el sistema. Una vez que Red Hat Linux esté instalado en la unidad del disco duro de un sistema, la BIOS intentará iniciar desde el **Master Boot Record** (MBR) en el primer sector de la primera unidad del disco duro, que carga sus contenidos en la memoria, y lo controla todo.

Entonces, este código del programa del MBR busca la primera partición activa y lee el registro de arranque de la misma. El registro de arranque contiene instruciones acerca de cómo cargar el gestor de arranque, **LILO** (*LI*nux *LO*ader). El MBR carga LILO, que se hace cargo del proceso (siempre que LILO esté instalado en el MBR). En la configuración de Red Hat Linux predeterminada, LILO usa el MBR para mostrar opciones de arranque y permitirle al usuario la entrada en el sistema operativo con el que realmente iniciará.

La pregunta que surge es:¿Cómo sabe LILO, en el MBR, qué hacer cuando el MBR ha sido leído? LILO ya ha leído allí las instrucciones a través del fichero `/etc/lilo.conf`.

3.2.1 Opciones de `/etc/lilo.conf`

La mayor parte de las veces no necesitará cambiar el Master Boot Record de su unidad del disco duro a menos que necesite activar un sistema operativo recién instalado o bien esté tratando de usar un núcleo nuevo. Si necesita crear un nuevo MBR usando LILO pero usando, a su vez, una configuración diferente, deberá editar el fichero `/etc/lilo.conf` y hacer funcionar `lilo` de nuevo para que se actualicen los cambios.

ADVERTENCIA

Si quiere modidificar `/etc/lilo.conf`, asegúrese de tener una copia de seguridad antes de hacer algún cambio. Asegúrese también de tener a disposición un disquete de arranque funcionando, para poder activar el sistema y hacer cambios en el MBR si hubiera un problema. Para mas información sobre la creación de un disquete de arranque vea el manual de `mkbootdisk`.

El fichero `/etc/lilo.conf` se usa a través del comando `lilo` para determinar qué sistema operativo utilizar o qué núcleo activar, así como para saber donde auto-instalar (por ejemplo `/dev/hda` para la primera unidad del disco duro IDE). Una muestra de fichero `/etc/lilo.conf`:

```
boot=/dev/hda
map=/boot/map
```

```
install=/boot/boot.b
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
 read-only
 root=/dev/hda5

other=/dev/hda1
 label=dos
```

Este ejemplo muestra un sistema configurado para activar dos sistemas operativos: Red Hat Linux y DOS. He aquí un análisis más profundo de unas pocas líneas de este archivo (su fichero `/etc/lilo.conf` podría aparecer un poco diferente):

- `boot=/dev/hda`, dice a LILO que mire en la primera unidad del disco duro en el primer controlador IDE.
- `map=/boot/map`, localiza el mapa del archivo. En una utilización normal de LILO, este parámetro no debería de ser modificado.
- `install=/boot/boot.b`, dice a LILO que instale el archivo especificado como sector de nuevo arranque. En una utilización normal, esto no debería de ser modificado. Si la línea `install` falta, LILO supondrá, por defecto, que quiere utilizar el fichero `/boot/boot.b`.
- El parámetro `prompt` hace que LILO le muestre lo que aparece como referencia en la línea `message`. No se aconseja quitar la línea `prompt` pero, si lo hace, encontrará todavía una salida rápida manteniendo la tecla [Shift] pulsada mientras su máquina comienza el arranque.
- `timeout=50`, establece la cantidad de tiempo que LILO esperará durante el inicio antes de proceder con la activación de la línea de entrada `default`. Este valor se mide en décimas de segundo, con 50 como valor predeterminado.
- `message=/boot/message`, se refiere a la pantalla que LILO muestra para permitirle seleccionar el sistema operativo o el núcleo que quiere activar.
- `lba32`, describe a LILO la geometría de la unidad del disco duro. Otro parámetro habitual aquí es `linear`. No debería cambiar esta línea a menos que esté muy seguro de lo que está haciendo. De lo contrario, podría poner su sistema en situación de no poder arrancarse.

- `default=linux`, se refiere al sistema operativo predeterminado con el que LILO arrancará, partiendo de las opciones listadas debajo de esta línea. El nombre `linux` se refiere a la línea `label` en cada una de las opciones de activación abajo citadas.
- `image=/boot/vmlinuz-2.4.0-0.43.6`, especifica el núcleo linux que se activará con esta opción particular.
- `label=linux`, es el nombre de la opción del sistema operativo que aparecerá en la pantalla de LILO. En este caso, este es también el nombre al que se hace referencia en la línea `default`.
- `initrd=/boot/initrd-2.4.0-0.43.6.img`, se refiere a la imagen **initial ram disk** que se usará en el arranque para inicializar y ejecutar el procedimiento que hace que la activación del núcleo sea posible. El disco de RAM inicial está formado por una acumulación de las unidades específicas de la máquina necesarias para hacer funcionar la unidad del disco duro y lo necesario para cargar el núcleo. Nunca debería tratar de usar los discos RAM de inicio en diferentes máquinas a menos que estos tengan una configuración hardware idéntica (y aún así, esto es una mala idea).
- `read-only`, especifica que esta partición raíz (vea la línea abajo citada `root`) no puede ser escrita, sino sólo leída.
- `root=/dev/hda5`, informa a LILO qué partición de disco usar como partición de raíz.

A continuación, LILO mostrará la pantalla inicial de Red Hat Linux y los diferentes sistemas operativos o núcleos con los que ha sido configurado para el arranque. Si tan sólo tiene instalado Red Hat Linux y no ha cambiado nada en el fichero `/etc/lilo.conf`, sólo verá la opción linux. Si ha configurado LILO para activar también otros sistemas operativos, esta pantalla le dará la oportunidad de seleccionar el sistema operativo con el que arrancará. Utilice la tecla de la flecha para resaltar el sistema operativo y pulse la tecla [Intro]

Si desea poder obtener una línea de comando para dar órdenes a LILO, pulse la combinación de teclas [Ctrl]-[X]. LILO mostrará un mensaje de `LILO:` en la pantalla. LILO esperará el período de tiempo que se haya predefinido para la entrada del usuario. (La cantidad de tiempo que LILO espera se establece en la línea `timeout` en el fichero `/etc/lilo.conf`). Si su fichero `/etc/lilo.conf` estuviera configurado para permitir a LILO la posibilidad de elegir sistema operativo, podría escribir en la etiqueta cualquier sistema operativo que desee activar.

Si LILO está activando Linux, cargará primero el núcleo en la memoria, que es un archivo del estilo `vmlinuz` (más el número de versión, por ejemplo, `vmlinuz-2.4.0-xx`), ubicado en el directorio `/boot`. Depués, es el núcleo quien controla el proceso `init` (inicialización) del sistema.

En este momento, con el núcleo cargado en la memoria y en funcionamiento, Linux ya habrá sido iniciado, aunque a un nivel muy básico. Sin embargo, sin las aplicaciones que utilicen el núcleo y sin la capacidad del usuario para dar un significado al inicio del sistema, no se puede hacer mucho.

El programa de comando `init` resuelve este problema sacando a relucir los diferentes servicios que permiten al sistema desempeñar su papel.

3.2.2 Init

El kernel encuentra `init` en el directorio `/sbin` y lo ejecuta. `init` coordina el resto del proceso de arranque.

Cuando el comando `init` inicia, se transforma en el padre (o en el abuelo) de todos los procesos que se producen automáticamente en su sistema Red Hat Linux. Primero, pone en funcionamento el guión establecido en el fichero `/etc/rc.d/rc.sysinit`, que establece la ruta a otros programas, comienza a intercambiar datos, controla los sistemas de archivo, etc. Básicamente, el fichero `rc.sysinit` se encarga de todo lo que su sistema tiene que realizar durante la inicialización. Por ejemplo, en un sistema de red, el fichero `rc.sysinit` utiliza la información del archivo `/etc/sysconfig/network` para iniciar la red. La mayor parte de los sistemas usan un reloj, por lo tanto, en ellos, el `rc.sysinit` tendrá una referencia a `/etc/sysconfig/clock` para inicializar el reloj. Si tiene procesos especiales en el puerto serie que necesiten ser inicializados, el `rc.sysinit` podría también poner en funcionamiento el `rc.serial`.

Entonces, el `init` ejecuta el guión `/etc/inittab`, que describe cómo debería de ser configurado el sistema en cada **nivel de ejecución** y configura el nivel de ejecución predeterminado. (vea la Sección 3.4, *Niveles de ejecución Init* para obtener más información acerca de los niveles de ejecución en las diversas utilidades.) Este archivo establece, entre otras cosas, que el comando `/sbin/update` debería ser ejecutado siempre que comience un nivel de ejecución. El `programa update` se usa para reenviar al disco buffers sucios.

Siempre que el nivel de ejecución cambia, `init` utiliza los guiones de `/etc/rc.d/init.d` para iniciar e interrunpir diferentes servicios, como puedan ser su servidor de red, su servidor DNS, etc. Primero, el comando `init` establece la librería de funciones de origen para el sistema (normalmente `/etc/rc.d/init.d/functions`), que explica cómo iniciar o anular un programa y cómo encontrar el PID de un programa. Luego, el comando `init` determina el nivel de ejcución en curso y el precedente.

El comando `init` inicia todos los procesos de segundo plano necesarios para que el sistema los ejecute considerando el directorio `rc` apropiado para ese nivel de ejecución (`/etc/rc.d/rc`<*x*>`.d`, donde el <*x*> se numera de 0 a 6). El comando `init` ejecuta cada uno de los guiones anulados (el nombre de sus archivos comienza con una K), con un parámetro `stop`. El comando `init` ejecuta el inicio de todos los guiones (los nombres de sus archivos comienzan con una S) en el nivel de ejecución apropiado del directorio mediante el comando `start`, para que todos los servicios y aplicaciones se inicien correctamente. De hecho, puede ejecutar los mismos guiones manualmente después de que el sistema haya terminado de arrancar con un comando como `/etc/rc.d/init.d/httpd stop` o un comando `service httpd stop`, registrado como root. Esto interrumpirá el servidor `httpd`.

Nota

Cuando se inicien los servicios manualmente, debería estar como super-usuario. Si aparece un error cuando ejecute el comando `service httpd stop`, podría no estar en la ruta `/sbin` ni en `/root/.bashrc` (o no tener el archivo `.rc` adecuado para su shell preferida). Podría escribir el comando completo, como `/sbin/service httpd stop` o agregar el directorio mediante el comando `export PATH="$PATH:/sbin"` a su archivo de shell `.rc`. Si edita el archivo de configuración de su shell, salga del sistema y entre de nuevo como administrador para hacer que la configuración cambiada del archivo de shell sea efectiva.

Ninguno de los guiones que inician e interrunpen los servicios está realmente localizados en el fichero `/etc/rc.d/init.d`. Más bién, todos los archivos de `/etc/rc.d/rc`*x*`.d` son **enlaces simbólicos** que señalan los guiones localizados en el `/etc/rc.d/init.d`. Una conexión simbólica no es más que un archivo que señala simplemente a otro archivo, y se usa en este caso porque puede ser creada y borrada sin afectar al guión real que anula o inicia el servicio. Las conexiones simbólicas a los diferentes guiones están numeradas en un orden particular para que empiecen en ese orden. Podrá cambiar el orden en que los servicios inician o se interrumpen cambiando el nombre del enlace simbólico que se refiere al guión, y que realmente es quien inicia o interrumpe el servicio. Puede dar un mismo número a diferentes conexiones simbólicas si quiere que ese servicio empiece o termine inmediatamente después o antes de otro servicio.

Por ejemplo, para el nivel de ejecución 5, el comando `init` entra en el directorio `/etc/rc.d/rc5.d` y podría encontrar lo siguiente (la salida que verá por pantalla podría variar en función de su sistema y de su configuración):

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
```

```
K30mcserv -> ../init.d/mcserv
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
```

```
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S97rhnsd -> ../init.d/rhnsd
S99linuxconf -> ../init.d/linuxconf
S99local -> ../rc.local
```

Estos enlaces simbólicos informan a `init` de que necesita eliminar los comandos `pppoe`, `innd`, `ntpd`, `httpd`, `mysqld`, `pvmd`, `rarpd`, `bootparamd`, `nfs`, `rstatd`, `rusersd`, `rwalld`, `rwhod`, `squid`, `amd`, `mcserv`, `yppasswdd`, `dhcpd`, `smb`, `vncserver`, `arpwatch`, `named`, `snmpd`, `pxe`, `routed`, `mars-nwe`, `ldap`, `kadmin`, `kprop`, `krb524`, `krb5kdc`, `gated`, `nscd`, `ypserv`, `ups`, y `irda`. Después de que todos los procesos hayan sido eliminados, el proceso `init` mira en el mismo directorio y encuentra comienzos de guión para los comandos `kudzu`, `reconfig`, `ipchains`, `portmap`, `nfslock`, `autofs`, `random`, `netfs`, `apmd`, `identd`, `atd`, `pcmcia`, `sshd`, `rawdevices`, `xinetd`, `lpd`, `keytable`, `isdn`, `sendmail`, `gpm`, `canna`, `crond`, `FreeWnn`, `xfs`, `anacron`, `rhnsd`, y `linuxconf`. La última cosa que `init` ejecuta es `/etc/rc.d/rc.local` para hacer funcionar cualquiera de los guiones especiales configurados para el host. En este momento, se considera que el sistema está operando en el nivel de ejecución 5.

Después de que el `init` haya pasado a través de todos los niveles de ejecución, el guión de `/etc/inittab` ejecuta un proceso `getty` para cada consola virtual (login prompts) para cada nivel de ejecución (los niveles de ejecución 2-5 emplea seis consolas; el nivel de ejecución 1, que funciona en el modo de usuario único, sólo emplea una; los niveles de ejecución 0 y 6 no tienen consolas virtuales). Basicamente, el `getty` abre las líneas tty, establece sus modos, imprime el indicador de comandos de inicio de sesión, toma el nombre del usuario y luego comienza con el proceso de inicio de sesión para ese usuario. Esto permite a los usuarios autentificarse en el sistema y comenzar a usarlo.

También, el fichero `/etc/inittab` indica al `init` cómo debería manejar el que un usuario pulse [Ctrl]-[Alt]-[Suprimir] en la consola. Como Red Hat Linux debería ser cerrado e inmediatamente reiniciado, se da la orden a `init` de ejecutar el comando `/sbin/shutdown -t3 -r now` cuando un usuario ejecuta esta combinación de teclas. Además, en `/etc/inittab` se establece qué comando `init` debería funcionar en caso de fallar la energía, si su sistema tiene una unidad SAI (Sistema de Alimentación Ininterrumpida) conectado.

En el nivel de ejecución 5, el `/etc/inittab` ejecuta un guión llamado `/etc/X11/prefdm`. El guión `prefdm` hace funcionar su gestor de pantalla para X preferido (`gdm` si utiliza GNOME, `kdm` si utiliza KDE, o `xdm` si utiliza otro, basándose en los contenidos del archivo del directorio `/etc/sysconfig/desktop`

Ahora, debería estar viendo un indicador de comandos de inicio de sesión parpadeando en su pantalla. Todo esto no dura más que unos pocos segundos.

3.2.3 SysV Init

Como hemos visto, el programa `init` se pone en funcionamento a través del núcleo en el momento del arranque. Éste se encarga de iniciar todos los procesos normales que se necesita iniciar junto con el sistema. Éstos incluyen los procesos preparados que le permiten el registro de usuarios, demonios de NFS, demonios de FTP y cualquier otra cosa que necesite ejecutar cuando su máquina arranque.

SysV init es el proceso init estáandar en el mundo linux para controlar el inicio del software en el arranque del sistema, porque es más fácil de usar, más potente y flexible que el comando tradicional BSD `init`.

SysV init se diferencia también de BSD init en que los archivos de configuración están en `/etc/rc.d` en vez de encontrarse directamente en `/etc`. En `/etc/rc.d`, encontrará el fichero `rc`, el `rc.local`, el `rc.sysinit` y los siguientes directorios:

```
init.d
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
```

SysV init representa cada uno de los niveles de ejecución de init con un directorio separado, usando el `init` y enlaces simbólicos en cada uno de los directorios para interrumpir e iniciar los diferentes servicios mientras que el sistema cambia de un nivel de ejecución a otro.

Resumiendo, lo que ocurre en el arranque de un SysV init es lo siguiente:

- El núcleo entra en el `/sbin` en busca de `init`
- `init` ejecuta el guión `/etc/rc.d/rc.sysinit`
- `rc.sysinit` maneja la mayoría de los procesos de arranque del cargador y después ejecuta el `rc.serial` (si existe)
- `init` ejecuta todos los guiones para el nivel de ejecución predeterminado.
- `init` ejecuta `/etc/rc.d/rc.local`

El nivel de ejecución predeterminado se decide en el fichero `/etc/inittab`. Debería haber una línea en la parte superior como la siguiente:

```
id:3:initdefault:
```

El nivel de ejecución predeterminado es 3 en este ejemplo, el número inmediatamente después de los primeros dos puntos. Si desea cambiarlo, puede editar el fichero `/etc/inittab` manualmente.

Tenga mucho cuidado cuando esté modificando el archivo `inittab`. Si se equivoca, puede solucionarlo reiniciando el equipo, accediendo al indicador de comandos `boot:` con la combinación de teclas [Cntl]-[X] y tecleando

```
boot:  linux single
```

Esto *debería* permitirle arrancar en el modo de usuario único para que pueda volver a modificar el fichero `inittab` en su valor precedente.

A continuación hablaremos de información dentro de los archivos de `/etc/sysconfig`, que definen los parámetros usados por los servicios de diferentes sistemas cuando se inicia el sistema.

3.3 Información sobre Sysconfig

La información siguiente perfila algunos de los diferentes archivos de `/etc/sysconfig`, su función y sus contenidos. Esta información no pretende ser completa ya que muchos de estos archivos permiten una variedad de opciones que se usan sólo en circunstancias muy específicas o raras.

3.3.1 Archivos de `/etc/sysconfig`

Los siguientes archivos se encuentran normalmente en `/etc/sysconfig`:

- `y`
- `apmd`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `firewall`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`

- network
- pcmcia
- rawdevices
- sendmail
- soundcard
- ups
- vncservers

Es posible que a su sistema le falten algunos de ellos si el programa que necesita ese archivo no está instalado.

Veamos uno a uno cada uno de estos ficheros.

/etc/sysconfig/amd

El archivo /etc/sysconfig/amd contiene varios parámetros usados por el comando amd que permiten montar y desmontar automáticamente los sistemas de archivo.

/etc/sysconfig/apmd

El archivo /etc/sysconfig/apmd se usa por medio de apmd como una configuración para decidir qué iniciar/interrumpir/cambiar en el momento de suspender o reanudar el sistema. Se establece si se va a encender o apagar el ordenador mediante el comando apmd durante el inicio, dependiendo de que si su hardware se apoya o no en **Advanced Power Management** (**APM**) o de que decida usarlo o no. apm es un demonio de supervisión que trabaja con el codigo de gestión de energía dentro del núcleo Linux. Puede avisarle sobre una batería descargada si está usando Red Hat Linux sobre un portátil, entre otras cosas.

/etc/sysconfig/authconfig

El archivo /etc/sysconfig/authconfig establece el tipo de autorización que tiene que ser usada en el host. Contiene una o más de las siguientes líneas:

- USEMD5=<*value*>, donde <*value*> puede ser:
  - yes — si se usa MD5 para la autentificación.
  - no — si no se usa MD5 para la autentificación.

- USEKERBEROS=<*value*>, donde <*value*> puede ser:
  - yes — si se usa Kerberos para la autentificación.

  - `no` — si no se usa Kerberos para la autentificación.

- `USELDAPAUTH=<value>`, donde `<value>` es uno de los siguientes valores:
  - `yes` — si LDAP se usa para autentificación.
  - `no` — si LDAP no se usa para autentificación.

/etc/sysconfig/cipe

El archivo `/etc/sysconfig/cipe` configura el comando `cipe` en el inicio.

Éste podría contener los siguientes valores de muestra:

- `DEVICE=eth0`, especifica el adaptador de red que `cipe` utilizará.
- `PORT=9999`, designa el número de puerto UDP que debe ser usado por el proceso `cipe` en ambos extremos de la conexión.
- `PEER=0.0.0.0`, especifica la dirección real remota del extremo de `cipe`. Puede establecer dinámicamente esta dirección poniendo este valor a 0.0.0.0.
- `IPADDR=0.0.0.0`, especifica la dirección virtual en el extremo local del túnel `cipe`.
- `PTPADDR=0.0.0.0`, especifica la dirección virtual en el extremo remoto del túnel `cipe`.

/etc/sysconfig/reloj

El archivo `/etc/sysconfig/clock` controla la interpretación de valores leída por el sistema de reloj. Anteriores versiones de Red Hat Linux usaban los siguientes valores (que están anticuados):

- `CLOCKMODE=<value>`, donde `<value>` puede ser:
  - `GMT` — indica que el reloj está regulado con la Hora Universal (Greenwich Mean Time).
  - `ARC` — indica que el período de 42 años de la consola ABC está en funcionamiento (sólo para los sistemas basados en Alpha).

Normalmente, los valores correctos son:

- `UTC=<value>`, donde `<value>` puede ser:
  - `true` — indica que el reloj está regulado con la hora universal. Cualquier otro valor indica que está regulado con la hora local.
- `ARC=<value>`, donde `<value>` puede ser:

  – `true` — indica que el período de tiempo de 42 años de la consola ARC está en funciones. Cualquier otro valor indica que se adopta la norma UNIX epoch (sólo para los sistemas basados en Alpha).

- `ZONE=<filename>` — indica el archivo del huso horario en `/usr/share/zoneinfo` del que `/etc/localtime` es una copia, como:

```
ZONE="America/New York"
```

/etc/sysconfig/desktop

El archivo `/etc/sysconfig/desktop` especifica el gestor de escritorio que va a ser ejecutado, como:

```
DESKTOP="GNOME"
```

/etc/sysconfig/firewall

El archivo `/etc/sysconfig/firewall` contiene diferentes configuraciones de firewall. Por defecto este archivo está creado, pero vacío.

/etc/sysconfig/harddisks

El archivo `/etc/sysconfig/harddisks` le permitirá configurar su(s) unidad(es) de disco duro.

No haga cambios en este archivo. Si cambia los valores predeterminados cargados aquí, podría dañar toda la información de sus discos duros.

El archivo `/etc/sysconfig/harddisks` podría contener lo siguiente:

- `USE_DMA=1`, si este valor está a 1, se habilita el DMA. Sin embargo, con algunos grupos de chips y algunas combinaciones del disco duro, el DMA puede causar corrupción de datos. *Verifique la documentación de su disco duro o consulte su fabricante antes de habilitar esta opción.* .
- `Multiple_IO=16`, si este valor está a 16, permite la interrupción de E/S a múltiples sectores. Cuando está habilitado, se reduce la sobrecarga del sistema operativo en un 30-50% *Use esta opción con precaución.*
- `EIDE_32BIT=3`, permite el soporte de una tarjeta de E/S tipo (E)IDE 32-bit.

- LOOKAHEAD=1, permite una lectura avanzada de la unidad.
- EXTRA_PARAMS=, especifica parámetros extra.

/etc/sysconfig/hwconf

El archivo /etc/sysconfig/hwconf hace un listado de todo el hardware que kudzu detectó en su sistema, como también de los drivers que se utilizan y de la información relativa al ID del vendedor y a la de los dispositivos. El programa kudzu detecta y configura el hardware nuevo y/o cambiado de un sistema. El archivo /etc/sysconfig/hwconf no se puede modificar manualmente. Si lo modifica, los dispositivos podrían aparecer de repente como si hubieran sido cambiados o anulados.

/etc/sysconfig/i18n

El archivo /etc/sysconfig/i18n establece el idioma predeterminado, como:

```
LANG="es_ES"
```

/etc/sysconfig/init

El archivo /etc/sysconfig/init controla el modo en que el sistema aparecerá y funcionará durante el arranque.

Podrían usarse los siguientes valores:

- BOOTUP=<*value*>, donde <*value*> puede ser:
  - BOOTUP=color, significa que activaremos la pantalla estándar en color durante el arranque; donde se muestra, con diversos colores, si se cargan satisfactoriamente o no los dispositivos y los servicios durante el inicio.
  - BOOTUP=verbose, significa que activaremos un modo de inicio al modo antiguo, que proporciona mucha más información que el mero mensaje de éxito o fracaso.
  - Cualquier otro valor se traducirá como que queremos utilizar el modo de pantalla normal, sin el juego de caracteres ANSI.

- RES_COL=<*value*>, donde <*value*> es el número de la columna en la pantalla para iniciar etiquetas de status. Está predeterminado a 60.
- MOVE_TO_COL=<*value*>, donde <*value*> mueve el cursor hacia el valor de la línea RES_COL. Se predetermina el eco de salida de las secuencias ANSI con -e.
- SETCOLOR_SUCCESS=<*value*>, donde <*value*> configura el color del indicador de éxito. Se predetermina el eco de salida de las secuencias ANSI con -e, estableciendo el color a verde.

- `SETCOLOR_FAILURE=<value>`, donde `<value>` configura el color utilizado para indicar un fallo. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a rojo.
- `SETCOLOR_WARNING=<value>`, donde `<value>` configura el color utilizado para indicar atención. Se predetermina el eco de salida de las secuencias ANSI con `-e`, estableciendo el color a amarillo.
- `SETCOLOR_NORMAL=<value>`, donde `<value>` configura el color 'normal'. Se predetermina el eco de salida de las secuencias ANSI con `-e`.
- `LOGLEVEL=<value>`, donde `<value>` configura el nivel inicial de identificación de la consola para el kernel. El valor por defecto es 7; 8 significa todo (incluso el depurado); 1 significa todo expecto el kernel. `syslogd` ignorará esto una vez se ejecute.
- `PROMPT=<value>`, donde `<value>` puede tener uno de los siguientes:
  - `yes` — Activa la verificación de teclado para el modo interactivo.
  - `no` — Desactiva la verificación de teclado para el modo interactivo.

`/etc/sysconfig/irda`

El fichero `/etc/sysconfig/irda` controla cómo están configurados los dispositivos infrarrojos al arranque del sistema.

Se pueden utilizar los siguientes valores:

- `IRDA=<value>`, donde `<value>` puede tomar uno de los siguiente valores booleanos:
  - `yes` — `irattach` deberá estar en ejecución, para chequear periódicamente si hay algún dispositivo intentando conectarse al puerto infrarrojos, como podría ser el caso de un portátil realizando una conexión de red. Si va a utilizar dispositivos infrarrojos en su sistema, debería usar este valor.
  - `no` — el programa `irattach` no se ejecutará, evitando la comunicación por infrarrojos.

- `DEVICE=<value>`, donde `<value>` se refiere al dispositivo (normalmente el puerto serie) que maneja las comunicaciones infrarrojas.
- `DONGLE=<value>`, donde `<value>` el tipo de "dongle" que se utiliza para la comunicación en infrarrojos. Esta configuración existe para la gente que utilice "dongles" serie en lugar de puertos infrarrojos reales. Un "dongle" es un dispositivo que se pone en un puerto serie estanard para comunicar mediante infrarrojos. Esta línea está comentada por defecto porque los ordenadores

portátiles con puerto infrarrojos son menos comunes que los ordenadores que disponen de "dongles" para simularlo.

- DISCOVERY=<*value*>, donde <*value*> puede tomar uno de los siguientes valores booleanos:
  - yes — Inicia irattach en modo discovery, que es el modo que chequea en busca de otros dispositivos infrarrojos. Esta opción se tiene que activar para que una máquina busque activamente conexiones infrarrojas (teniendo en cuenta que el otro dispositivo no puede iniciar la conexión).
  - no — No inicia irattach en modo discovery.

/etc/sysconfig/keyboard

El fichero /etc/sysconfig/keyboard controla el comportamiento del teclado. Se pueden utilizar los siguiente valores:

- KEYBOARDTYPE=sun|pc, que se utiliza sólo en estaciones SPARC. sun quiere decir que un teclado de Sun está conectado en /dev/kbd, y pc quiere decir que un teclado del estilo PC está en el puerto PS/2.
- KEYTABLE=<*file*>, donde <*file*> es el nombre de un fichero de página de códigos de teclado. Por ejemplo: KEYTABLE="es". Los ficheros que se pueden utilizar como páginas de códigos de teclado están en /usr/lib/kbd/keymaps/i386 y se ramifican en diferentes configuraciones a partir de aquí y están nombrados como <*file*>.kmap.gz. El primer fichero que se encuentre en /usr/lib/kbd/keymaps/i386 y que corresponda al valor KEYTABLE será el que se utilice.

/etc/sysconfig/kudzu

El fichero /etc/sysconfig/kuzdu le permitirá realizar una prueba segura del hardware de su sistema con kudzu en el arranque. Una prueba segura desactiva el puerto serie y la prueba de monitor DDC.

- SAFE=<*value*>, donde <*value*> puede tomar uno de los siguientes valores:
  - yes — kuzdu realiza una prueba segura.
  - no — kuzdu realiza una prueba normal.

/etc/sysconfig/mouse

El fichero /etc/sysconfig/mouse se utiliza para especificar información sobre el ratón disponible. Se pueden usar los siguientes valores:

- `FULLNAME=<value>`, donde `<value>` se refiere al nombre completo del ratón que se está utilizando.
- `MOUSETYPE=<value>`, donde `<value>` puede tener uno de los siguientes valores:
  - `microsoft` — Un ratón Microsoft™.
  - `mouseman` — Un ratón MouseMan™.
  - `mousesystems` — Un ratón Mouse Systems™ mouse.
  - `ps/2` — Un ratón PS/2.
  - `msbm` — Un ratón tipo bus de Microsoft™.
  - `logibm` — Un ratón tipo bus de Logitech™.
  - `atibm` — Un ratón tipo bus de ATI™.
  - `logitech` — Un ratón Logitech™.
  - `mmseries` — Un viejo ratón MouseMan™ mouse.
  - `mmhittab` — Un ratón mmhittab.

- `XEMU3=<value>`, donde `<value>` puede tener uno de los siguientes valores booleanos:
  - `yes` — Si el ratón tiene tan sólo dos botones y se quieren emular tres.
  - `no` — Si el ratón ya tiene dos botones.

- `XMOUSETYPE=<value>`, donde `<value>` se refiere al tipo de ratón que se utilizará mientras se ejecute X. Estas opciones son las mismas que las de `MOUSETYPE` en este mismo fichero.

Además, existe un enlace dinámico ,`/dev/mouse`, que apunta al dispositivo de ratón que se está utilizando actualmente.

`/etc/sysconfig/network`

El fichero `/etc/sysconfig/network` se utiliza para especificar información sobre la configuración de red que deseamos tener. Se pueden tener los siguientes valores:

- `NETWORKING=<value>`, donde `<value>` puede tener los siguientes valores booleanos:
  - `yes` — Se debería configurar la red.
  - `no` — No se debería configurar la red.

- HOSTNAME=<*value*>, donde <*value*> debería ser un **Nombre de Dominio Cualificado** (**FQDN**), como pudiera ser `hostname.domain.com`, aunque pudiera ser cualquiera que usted desee.

> **Nota**
>
> Para mantener la compatibilidad con el software antiguo que se pueda tener instalado (como puediera ser `trn`), el fichero `/etc/HOSTNAME` debería tener el mismo valor que aquí.

- GATEWAY=<*value*>, donde <*value*> es la dirección IP de la puerta de enlace de la red.
- GATEWAYDEV=<*value*>, donde <*value*> es el dispositivo de la puerta de enlace, como por ejemplo `eth0`.
- NISDOMAIN=<*value*>, donde <*value*> es el nombre del dominio NIS.

/etc/sysconfig/pcmcia

El fichero `/etc/sysconfig/pcmcia` se utiliza para especificar la configuración PCMCIA. Se pueden utilizar los siguientes valores:

- PCMCIA=<*value*>, donde <*value*> se corresponde a uno de los siguientes valores:
  - `yes` — si activamos el soporte de PCMCIA.
  - `no` — si no activamos el soporte PCMCIA.

- PCIC=<*value*>, donde <*value*> se corresponde a uno de los siguientes valores:
  - `i82365` — El ordenador tiene un juego de chips PCMCIA de estilo i82365.
  - `tcic` — El ordenador tiene un juego de chips PCMCIA de estilo tcic.

- PCIC_OPTS=<*value*>, donde <*value*> corresponde a los parámetros de temporización del driver del socket (i82365 o tcic).
- CORE_OPTS=<*value*>, donde <*value*> es la lista de las opciones `pcmcia_core`.
- CARDMGR_OPTS=<*value*>, donde <*value*> en la lista de las opciones del comando PCMCIA `cardmgr` (como, por ejemplo, `-q` para el modo silencioso; `-m` para buscar módulos del kernel cargables desde un directorio, y demás). Consulte la página de manual sobre `cardmgr` para obtener más información.

/etc/sysconfig/rawdevices

El fichero /etc/sysconfig/rawdevices se utiliza para configurar el mapeo de los dispositivos "raw":

```
/dev/raw/raw1 /dev/sda1
/dev/raw/raw2 8 5
```

/etc/sysconfig/sendmail

El fichero /etc/sysconfig/sendmail permite que se puedan enviar mensajes a uno o más receptores, enrutando el mensaje sobre tantas redes como sea necesario. Este fichero configura los valores por defecto que el programa Sendmail necesita para ejecutarse. Estos valores por defecto son para ejecutarlo como un demonio en segundo plano y para verificar la cola una vez cada hora.

Se pueden utilizar los siguientes valores:

- DAEMON=<*value*>, donde <*value*> corresponde a uno de los siguientes valores booleanos:
  - yes — Sendmail debería configurarse para escuchar en el puerto 25 a la escucha de correo de entrada. La opción yes implica la utilización de la opción -bd de Sendmail.
  - no — Sendmail no deberí de ser configurado para escuchar la llegada de correo por el puerto 25.

- QUEUE=1h se envía a Sendmail como -q$QUEUE. La opción -q no se pasa a Sendmail si existe /etc/sysconfig/sendmail el parámetro QUEUE está vacío o incompleto.

/etc/sysconfig/soundcard

El fichero /etc/sysconfig/soundcard es generado por el comando sndconfig y no debería de ser modificado. El único uso de este fichero es determinar qué tarjeta aparecerá por defecto en el menú de selección de sndconfig la próxima vez que se ejecute. La configuración de la tarjeta de sonido se localiza en el fichero /etc/modules.conf.

Este fichero puede contener lo siguiente:

- CARDTYPE=<*value*>, donde <*value*> se configura, por ejemplo, como SB16 en el caso de una tarjeta de sonido Soundblaster 16.

/etc/sysconfig/ups

El fichero /etc/sysconfig/ups se utiliza para especificar información sobre cualquier **Sistema de Alimentación Ininterrumpida** (**SAI**) conectado a su sistema. Un SAI puede ser una buena opción para un sistema Red Hat Linux ya que le proporcionarát el tiempo necesario para apagar el sistema correctamente en el caso de la interrupció del servicio elétrico. Se pueden utilizar los siguientes valores:

- SERVER=<*value*>, donde <*value*> puede tomar los siguientes valores:
  - yes — Si se ha instalado un SAI en su sistema.
  - no — Si no se ha instalado ningún SAI en su sistema.

- MODEL=<*value*>, donde <*value*> debe estar seleccionado a uno de los siguientes valores o bien a NONE si no hay ningú SAI instalado en su sistema:
  - apcsmart — Para un dispositivo APC SmartUPS™ o similar.
  - fentonups — Para un dispositivo Fenton UPS™.
  - optiups — Para un dispositivo OPTI-UPS™.
  - bestups — Para un SAI Best Power™.
  - genericups — Para un SAI genérico.
  - ups-trust425+625 — Para un SAI Trust™.

- DEVICE=<*value*>, donde <*value*> especifica dónde está conectado el SAI, como pueda ser /dev/ttyS0.
- OPTIONS=<*value*>, donde <*value*> es un comando especial que hay que pasarle al SAI.

/etc/sysconfig/vncservers

El fichero /etc/sysconfig/vncservers configura cómo el servidor de **Virtual Network Computing** (**VNC**) se inicia. VNC es un sistema de visualizació remoto que permite visualizar escritorios remotos en otras máquinas diferentes de donde lo estamos ejecutando, pero a través de diferentes redes, (desde una LAN a Internet) usando una variedad de parámetros considerable.

Puede contener lo siguiente:

- VNCSERVERS=<*value*>, donde <*value*> se suele poner com algo parecido a "1:root".

3.3.2 Ficheros de `/etc/sysconfig/network-scripts/`

Los siguientes ficheros se suelen encontrar en `/etc/sysconfig/network-scripts`, donde *<if-name>* corresponde a la interfaz de red:

- `/etc/sysconfig/network-scripts/ifup`
- `/etc/sysconfig/network-scripts/ifdown`
- `/etc/sysconfig/network-scripts/network-functions`
- `/etc/sysconfig/network-scripts/ifcfg-`*<if-name>*
- `/etc/sysconfig/network-scripts/ifcfg-`*<if-name>*`-`*<clone-name>*
- `/etc/sysconfig/network-scripts/chat-`*<if-name>*
- `/etc/sysconfig/network-scripts/dip-`*<if-name>*
- `/etc/sysconfig/network-scripts/ifup-post`

Miremos cada uno de ellos.

`/etc/sysconfig/network-scripts/ifup` y `/etc/sysconfig/network-scripts/ifdown`

Se trata de enlaces simbólicos a `/sbin/ifup` y a `/sbin/ifdown`, respectivamente. Son los dos únicos scripts de este directorio que deberían poder ser llamados directamente; estos dos scripts llaman a los demás en función de si los necesitan o no. Estos enlaces simbólicos están aquí por motivos prácticos — seguramente se borrarán en próximas versiones, así que solamente se debería usar `/sbin/ifup` y `/sbin/ifdown`.

Estos scripts toman un argumento: el nombre del dispositivo (como `eth0`). Se llaman con un segundo argumento `boot` durante la secuencia de arranque, de tal forma que los dispositvos que no tienen por qué estar en funcionamiento (`ONBOOT=no`, [mire más abajo]) pueden ser ignorados durante el arranque.

`/etc/sysconfig/network-scripts/network-functions`

Realmente no se trata de un fichero público. Contiene funciones con las que los scripts pueden levantar y bajar las interfaces. Particularmente, contiene la mayoría del código de manejo de interfaces alternativas así como notificación de cambio de interfaces con `netreport`, que es el programa que dice a los scripts de administración que envien una señal proceso llamado `netreport` cuando ocurra cualquier tipo de cambios en las interfaces de red.

/etc/sysconfig/network-scripts/ifcfg-<*if-name*> y /etc/sysconfig/network-scripts/ifcfg-<*if-name*>:<*clone-name*>

El primero de los dos ficheros define la interfaz, mientras que el segundo contiene tan sólo las definiciones que son diferentes en una interfaz "alias" (o alternativa). Ambos requieren que se epecifique un <*if-name*> (nombre de la interfaz de red). Por ejemplo, los números de red pueden ser diferentes pero todo lo demás debería estar en un clon del fichero mientras que toda la configuración del dispositivo debería estar en el fichero `ifcfg`.

Los objetos que pueden ser definidos en un fichero `ifcfg` dependen del tipo de interfaz.

Los siguientes valores suelen ser habituales:

- `DEVICE=`<*name*>, donde <*name*> es el nombre del dispositivo físico (excepto en el caso de los dispositivos PPP asignados dinámicamente, dónde estaría el "nombre lógico").
- `IPADDR=`<*addr*>, donde <*addr*> es la dirección IP.
- `NETMASK=`<*mask*>, donde <*mask*> es el valor de la máscara de red.
- `NETWORK=`<*addr*>, donde <*addr*> es la dirección de red.
- `BROADCAST=`<*addr*>, donde <*addr*> es la dirección de broadcast.
- `GATEWAY=`<*addr*>, donde <*addr*> es la dirección de la puerta de enlace.
- `ONBOOT=`<*answer*>, done <*answer*> puede ser:
  - `yes` — si queremos iniciar el dispositivo en el momento del arranque.
  - `no` — si no queremos iniciar el dispositivo en el momento del arranque.
- `USERCTL=`<*answer*>, donde <*answer*> puede ser:
  - `yes` — si cualquier usuario puede controlar este dispostivo.
  - `no` — si los usuarios no-administradores no pueden cotnrolar este dispositivo.
- `BOOTPROTO=`<*proto*>, donde <*proto*> puede ser:
  - `none` — No se usará ningún protocolo en el momento del arranque.
  - `bootp` — Se usará el protocolo BOOTP.
  - `dhcp` — Se usará el protocolo DHCP.

Los siguientes valores son comunes a todos los ficheros SLIP:

- `PERSIST=`<*answer*>, donde <*answer*> puede ser:

  - `yes` — Si este dispositivo se debe mantener activo todo el tiempo, incluso después de haber sido desactivado una vez haya colgado el módem.
  - `no` — Este dispositivo no deberá mantenerse activo todo el tiempo.

- `MODEMPORT=<port>`, donde `<port>` es el nombre del dispositivo del puerto del módem (por ejemplo, "`/dev/modem`").
- `LINESPEED=<baud>`, donde `<baud>` es la velocidad del modem (por ejemplo, "`115200`").
- `DEFABORT=<answer>`, donde `<answer>` puede ser:
  - `yes` — Para insertar las cadenas por defecto al crear/modificar un script para esta interfaz.
  - `no` — Para no insertar las cadenas por defecto al crear/modificar un script para esta interfaz.

`/etc/sysconfig/network-scripts/chat-<if-name>`

Este fichero es un script de chat para conexiones SLIP y pretende ser quien establezca la conexión. Para dispositivos SLIP, se escribe un script DIP desde el script de chat.

`/etc/sysconfig/network-scripts/ifup-post`

Este fichero se llamará cuando un dispositivo de red (excepto un dispositivo SLIP) se inicie. Llama a `/etc/sysconfig/network-scripts/ifup-routes` para proporcionar rutas estáticas que dependen de ese dispositivo, proporcionar alias para ese dispositivo, y configurar un nombre de host, si todavía no ha sido configurado — y el nombre de host se puede encontrar mediante la IP de ese dispositivo. `ifup-post` envía SIGIO a cualquier programa que haya solicitado notificaciones de eventos de red.

Se puede extender este fichero para que configure el servicio de nombrado, llamadas arbitrarias a scripts y mucho más, en función de sus necesidades.

3.4 Niveles de ejecución Init

La idea que se esconde detrás del funcionamiento de diferentes servicios en diferentes niveles de ejecución radica esencialmente en el hecho de que diferentes sistemas se pueden usar de diferentes formas de inicio. Algunos servicios no se pueden utilizar hasta que el sistema se encuentre en un estado particular, o **modo**, como puede ser preparado para más de un usuario, o con la red disponible. Existen situaciones en las que puede que nos interese operar en un nivel de ejecución más bajo, como por ejemplo si queremos verificar errores de red en el nivel de ejecución 2, o queremos dejar el nivel de ejecución en 3 sin que se ejecute ninguna sesión de X. En estos casos, ejecutar servicios que requieren de un modo de sistema más alto no tiene sentido, ya que no funcionarán correctamente de ninguna

manera. Configurando cada servicio para que se inicie cuando estemos en un nivel de ejecución particular, aseguraremos que los procesos se iniciarán en orden y que podremos cambiar rápidamente el modo de la máquina sin molestarnos de qué servicios tenemos que iniciar o parar manualmente.

Normalmente, Red Hat Linux opera en el nivel de ejecución 3 — modo multiusuario completo. En Red Hat Linux se contemplan los siguientes niveles de ejecución:

- `0` — Halt (Parada)
- `1` — Single-user mode (Modo monousuario)
- `2` — Multi-user mode (Modo multiusuario), sin soporte de red
- `3` — Full multi-user mode (Modo multiusuario completo)
- `4` — No se utiliza
- `5` — Full multi-user mode (Modo multiusuario completo) (con login gráfico basado en X)
- `6` — Reboot (Reiniciar)

El nivel de ejecución para el inicio y parada de un sistema se configura en `/etc/inittab`. Para más información sobre `/etc/inittab`, consulte la Sección 3.2.3, *SysV Init*.

Si su máquina se queda en un estado en el que no arranca, debido a una mala configuración de `/etc/inittab` o no le deja hacer login en su sistema por tener corrupto el fichero `/etc/passwd` (o simplemente ha olvidado su contraseña), arranque el sistema en modo monousuario tecleando **`linux single`** en la línea `boot:` de LILO. Se iniciará el sistema en modo básico y tendrá una shell para poder arreglar los problemas que tenga.

3.5 Utilidades Initscript

La utilidad `chkconfig` que se encuentra en `/sbin` proporciona un comando de mantenimiento para la jerarquía de ficheros `/etc/rc.d/init.d`. Alivia un poco a los administradores de sistemas de tener que manipular directamente la mayoría de los enlaces simbólicos en los directorios de `/etc/rc.d`.

Además, existe la utilidad `ntsysv` en `/usr/sbin` que proporciona una interfaz de pantalla, que puede resultar mucho más fácil de utilizar que `chkconfig`. Ambas utilidades deben ejecutarse como root.

Mire las páginas de man de `chkconfig` y `ntsysv` para obtener más información.

3.6 Ejecutar programas en el inicio

El script `/etc/rc.d/rc.local` es ejecutado en el inicio del sistema por el comando `init`, una vez que el resto de la inicialización se ha completado, y siempre que cambiemos de nivel de ejecución. Podrá añadir comandos adicionales de inicialización aquí. Por ejemplo, si desea iniciar demonios adicionales o inicializar una impresora determinada.

Además, si requiere configurar los puertos serie, puede crear y editar el fichero `/etc/rc.serial`, que será ejecutado automáticamente en el inicio. Este script puede ejecutar un número de comandos `setserial` para configurar los puertos serie del sistema. Mire la página de manual de `setserial` para obtener más información.

El `/etc/rc.d/rc.local` por defecto crea un banner de login con el nombre de la máquina y la versión del kernel que tenga instalada.

3.7 Apagar

Para apagar Red Hat Linux, ejecute el comando `shutdown`. Puede leer la página de manual de `shutdown` para obtener más detalles, pero los parámetros más usuales son:

```
/sbin/shutdown -h now
/sbin/shutdown -r now
```

Deberá ejecutar `shutdown` como root. Una vez que haya apagado todo, la opción `-h` parará la máquina y la opción `-r` la reiniciará.

Aunque el comando `reboot` y el comando `halt` puedan invocar `shutdown`, mientras el sistema se ejecute en los niveles de ejecución 1-5, es una mala costumbre, ya que no todos los sistemas Linux soportan esta opción.

ADVERTENCIA

Si su ordenador no se apaga por sí solo, no deberá apagarlo hasta que no vea un mensaje en la pantalla indicándole que puede hacerlo.

Si se produce un fallo mientras que espera este mensaje, esto quiere decir que lo mismo está intentando apagar su máquina antes de que las particiones de disco hayan sido desmontadas. Esto puede provocar errores en el sistema de ficheros, incluso hasta el punto de no permitirle arrancar el sistema la próxima vez que intente iniciarlo. Tenga paciencia a la hora de apagar su sistema.

3.8 Diferencias en el proceso de arranque en otras arquitecturas

Cada una de las arquitecturas soprtadas por Red Hat Linux arranca el sistema operativo de una forma. Sin embargo, una vez que el kernel de Red Hat Linux se empieza a iniciar y transfiere el proceso de inicio a `init`, aparecen los mismos eventos en cada arquitectura de la misma manera. La única diferencia es la forma en la que Red Hat Linux encuentra el kernel y lo carga para poder iniciar `init`.

Consulte la información de instalación para cada tipo de arquitectura para obtener información detallada sobre los diferentes métodos de inicio.

4 Lightweight Directory Access Protocol (LDAP)

4.1 ¿Qué es LDAP?

LDAP (**Lightweight Directory Access Protocol**) es un estándar abierto para los servicios globales o locales en una red y/o en Internet. Un directorio, gestionado desde el LDAP se parece a una guía telefónica. LDAP puede gestionar mucha otra información, pero en la actualidad se utiliza principalmente para asociar nombres a números de teléfono y a direcciones e-mail. Los directorios soportan un gran volumen de tráfico, pero los datos en los directorios después no cambian tan a menudo.

LDAP es mucho más útil que una guía telefónica de papel, dado que el diseño de LDAP ha sido pensado para soportar la difusión a través de los servidores LDAP en Internet, un poco como para el **Domain Name Service** (**DNS**). El DNS funciona como una agenda teniendo rastro de la copia nombre_dominio/IP. El servidor DNS informa a las máquinas de la red de donde enviar los paquetes. En el futuro, LDAP proporcionará el mismo tipo de acceso global para muchos tipos de información a los directorios: en la actualidad, LDAP se usa habitualmente en el interior de determinadas empresas grandes, como universidades o sociedades, para gestionar los servicios a los directorios.

LDAP es un sistema cliente-servidor. Un cliente LDAP se conecta a un servidor LDAP y requiere de información o proporciona los datos necesarios para acceder a un directorio. El servidor responde a la solicitud, envía la consulta a otro servidor o acepta la información para incorporarla al directorio.

LDAP se conoce a veces como **X.500 Lite**. X.500 tiene un estándar internacional para los directorios. X.500 incluye muchas características interesantes pero es mucho más complejo y requiere de grandes recursos y una estructura OSI totalmente compatible. LDAP, por el contrario, funciona de manera correcta en cualquier PC y es compatible con el protocolo TCP/IP. LDAP puede acceder a los directorios X.500 pero no soporta todas las funciones de X.500.

En este capítulo haremos referencia a la configuración y uso de OpenLDAP, una implementación open-source de LDAP. OpenLDAP incluye `slapd`, que es un servidor independiente LDAP; `slurpd`, un servidor independiente con propagación de LDAP; librerías que implementan el protocolo LDAP utilidades; instrumentos y clientes de muestra.

4.2 Ventajas y desventajas de LDAP

La ventaja principal de usar LDAP es la consolidación de cierto tipo de información en el interior de su empresa. Por ejemplo, todas las diferentes listas de usuarios en el interior de su empresa pueden ser fusionadas en un solo directorio LDAP. Este directorio, a continuación, podrá ser consultado desde cualquier aplicación habilitada para LDAP a la que le sirva la información. El directorio también podrá ser utilizado por los usuarios que necesiten información sobre éste.

Otras ventajas de LDAP son que incluye entre otras cosas gran facilidad de implementar (si lo comparamos con X.500) y la coherencia de sus API. Lo cual significa que el número de aplicaciones y de puertas de enlace de que distruta LDAP puede crecer en el futuro.

El lado negativo es que si desea utilizar LDAP, debe usar un cliente habilitado para LDAP o bien pasar a través de una puerta de enlace LDAP. Como ya hemos mencionado anteriormente, la presencia de LDAP crecerá en el futuro, pero por ahora, no hay muchas aplicaciones de las que disfrutar. Además, si bien LDAP soporta algunos controles en el acceso, no soporta todos los aspectos de la seguridad incluidos en X.500.

4.3 Uso de LDAP

Muchas aplicaciones de Netscape, incluido Netscape Roaming Access están habilitadas para LDAP. Sendmail puede usar LDAP para buscar una dirección. Su empresa puede utilizar LDAP como un directorio compartido por toda la empresa y/o un servidor de nombres (en el lugar del NIS o ficheros planos). También puede usar un servidor LDAP personal para llevar su agenda privada (consulte la Sección 4.11, *Recursos adicionales*)

Ya que LDAP es un protocolo configurable, se puede utilizar para guardar casi cualquier tipo de información relativa a una estructura de organización particular.

4.3.1 Aplicaciones LDAP

Muchas aplicaciones cliente disponibles visionan y cambian la información LDAP:

- Navegador/Editor LDAP — Herramienta escrita al 100% Java para el desarrollo a través de diferentes plataformas, disponibles en http://www.iit.edu/~gawojar/ldap
- GQ — Cliente LADP que soporta GTK, disponible con la distribución de Red Hat Linux 7.1 o en http://biot.com/gq
- kldap — Cliente para el proyecto KDE, disponible en http://www.mountpoint.ch/oliver/kldap

4.3.2 LDAP y PAM

LDAP puede ser usado como un servicio de autenticación a través del módulo `pam_ldap`. LDAP se usa habitualmente como servidor centralizado de manera tal que los usuarios tengan un login unificado que cubra los terminales, los servidores POP, los servidores IMAP, máquinas conectadas a la red que utilizan SAMBA y también las máquinas Windows NT/2000. Todas estas situaciones pueden ser gestionadas a través del mismo ID del usuario y su contraseña, usando LDAP. El módulo `pam_ldap` está incluido en el paquete `nss_ldap`.

4.4 Terminología LDAP

Una **entrada** es una unidad en un directorio LDAP. Una entrada es identificada desde **Distinguished Name** (DN).

Cada entrada tiene atributos; los atributos son fragmentos de información directamente asociados con la entrada. Por ejemplo, una empresa podría ser una entrada LDAP. Los atributos asociados a una empresa podrían ser el número de fax, la dirección, etc. Las personas podrían ser otra entrada del directorio LDAP. Atributos comunes a las personas son el número de teléfono y sus direcciones de e-mail.

Ciertos atributos son necesarios, mientras que otros son opcionales. Un **objectclass** discrimina los atributos necesarios de los que no lo son. La definición de objectclass la encuentra en el directorio `etc/openldap/schema`.

El **LDAP Data Interchange Format** (LDIF) es un fichero con formato texto ASCII para las entradas LDAP. Los ficheros que exportan e importan datos de un servidor LDAP deben estar en formato LDIF. Una entrada LDIF se parece a:

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

Una entrada puede contener tantas líneas emparejadas `<attrtype>: <attrvalue>` como sean necesarias. Una línea vacía indica que la entrada ha terminado y que otra entrada está a punto de comenzar.

Las parejas `<attrtype>` y `<attrvalue>` *deben* ser definidas en un esquema antes de que puedan ser usadas. No puede definirlas simplemente en un fichero LDIF y esperar un servidor LDAP sin datos correspondientes en el esquema para ser capaces de usar esta información.

Cualquier cosa comprendida entre < > es variable y puede ser configurada por usded cuando añada una entrada LDAP, a excepción de <id>. El <id> es un número normalmente configurado por las herramientas LDAP cuando añade una nueva entrada y probablemente no necesitará nunca configurarla manualmente.

4.5 Mejoras de OpenLDAP 2.0

OpenLDAP 2.0 representa una mayor actualización para la aplicación, incluyendo:

- *Soporte LDAPv3* — Actulamente funciona con SASL, TLS, and SSL, entre otros, con soporte completo para RFC 2251-2256; muchos de los cambios desde LDAPv2 tienen como objetivo ayudar a hacer un protocolo más seguro de LDAP.
- *Soporte IPv6* — Actualmente soporta la siguiente generación de protocolos de Internet.
- *IPC sobre LDAP* — OpenLDAP puede comunicarse dentro de un sistema particular sin tener que pasar a través de una red, de manera que sea más seguro.
- *API de C actualizada* — Mejora el modo en que los programadores se pueden conectar y usar la aplicación.
- *Soporte LDIFv1* — Compatible completamente con la versión 1 del formato de intercambio de datos (LDIF)de LADP.
- *Sevidor LDAP independiente mejorado* — Incluye el sistema de control de acceso actualizado, herramientas mejoradas y mucho más.

4.6 Ficheros OpenLDAP

Los archivos de configuración OpenLDAP están instalados en el directorio `/etc/openldap`. Si hace un `ls` en `/etc/openldap`, verá algo parecido a:

```
ldap.conf         ldapsearchprefs.conf  schema
ldapfilter.conf   ldaptemplates.conf    slapd.conf
```

4.6.1 Modificar `/etc/openldap/slapd.conf`

El archivo `slapd.conf`, localizado en `/etc/openldap`, contiene la información de la configuración necesaria para su servidor `slapd` LDAP. Necesitará modificar este archivo para hacerlo específico a su dominio y su servidor.

La línea suffix asigna el dominio para el que el servidor LDAP proporcionará información. La línea suffix debería ser cambiada:

```
suffix          "dc=your-domain, dc=com"
```

para que refleje el nombre de dominio. Por ejemplo:

```
suffix          "dc=acmewidgets, dc=com"
```

o

```
suffix          "dc=acmeuniversity, dc=edu"
```

La entrada rootdn es el DN para un usuario que no está limitado por el control de acceso o por los parámetros administrativos limitados para las operaciones en el directorio LDAP. El usuario rootdn puede ser visto como el usuario root para el directorio LDAP. La línea rootdn debe ser cambiada desde:

```
rootdn          "cn=root, dc=your-domain, dc=com"
```

a algo como:

```
rootdn          "cn=root, dc=redhat, dc=com"
```

o

```
rootdn          "cn=ldapmanager, dc=my_organization, dc=org"
```

Cambie la línea rootpw:

```
rootpw          secret
```

a algo como:

```
rootpw          {crypt}s4L9sOIJo4kBM
```

En este ejemplo, se usa una contraseña de root encriptada, mejor solución que usar contraseñas de root en texto plano en el fichero `slapd.conf`. Para hacer esta cadena encriptada, deberá o copiarlo desde un fichero `passwd`, o usar Perl:

```
perl -e "print crypt('passwd','a_salt_string');"
```

En la línea Perl precedente, se ha utilizado un criterio de dos caracteres, y `passwd` es la versión texto de la contraseña.

También puede copiar una entrada `passwd` desde `/etc/passwd`, pero esto no funciona si la entrada `passwd` es una contraseña MD5 (por defecto en Red Hat Linux 7.1).

4.6.2 El directorio schema

Nuevo en la versión 2 de OpenLDAP, el directorio `schema` sostiene varias definiciones de LDAP, previamente localizadas en los ficheros `slapd.at.conf` y `slapd.oc.conf`. Todas las **definiciones de sintaxis de atributos** y **definiciones objectclass** están localizadas en archivos de un esquema diferente. Los archivos con esquemas diferentes en `/etc/openldap/slapd.conf` usan líneas `include`, como se muestran en el ejemplo:

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

No debería modificar ningún artículo del esquema definido en los archivos de esquema instalados por OpenLDAP.

Puede extender el esquema utilizado por OpenLDAP para soportar tipos de atributos adicionales y clases de objetos usando los ficheros de esquema como guía. Para hacerlo, cree un archivo `local.schema` en el directorio `/etc/openldap/schema`. Refíerase a este nuevo esquema en `slapd.conf` añandiendo la siguiente línea en las líneas predeterminadas del esquema de `include`:

```
include  /etc/openldap/schema/local.schema
```

Defina los tipos de atributos y las clases de objetos en el archivo `local.schema`. Muchas organizaciones utilizan tipos de atributos y clases de objetos de los ficheros de esquema instalados por defecto y modificados para su uso en el archivo `local.schema`. Esto representa una ayuda para la sintaxis del esquema al mismo tiempo que se encuentra las necesidades immediatas de su organización.

El objetivo de este capítulo es el de ampliar esquemas para unir ciertos requisitos específicos. Vea http://www.openldap.org/doc/admin/schema.html para informarse sobre cómo escribir nuevos ficheros de esquema.

4.7 Demonios y utilidades OpenLDAP

El paquete OpenLDAP incluye dos demonios: `slapd` y `slurpd`.

El demonio `slapd` es el demonio estándar de LDAP, que necesitará para ejecutar LDAP.

El demonio `slurpd` controla la réplica de los directorios LDAP en una red. `Slurpd` envia los cambios del directorio maestro LDAP al directorio esclavo LDAP. No necesitará usar `slurpd` a no ser que tenga más de un servidor LDAP en su red. Si tiene más de un servidor LDAP, tendrá que usar `slurpd` para tener el directorio LDAP sincronizado.

OpenLDAP también incluye algunas utilidades para añadir, modificar y borrar las entradas en un directorio LDAP:

- El dispositivo `ldapmodify` se usa para modificar las entradas en una base de datos LDAP, aceptando la entrada mediante un fichero o entrada estándar.
- La utilidad `ldapadd` se usa para añadir entradas al directorio (`ldapadd` es un enlace fijo para `ldapmodify -a`).
- `Ldapsearch` se usa para buscar entradas en el directorio LDAP usando el indicador de comandos de la shell.

- `ldapdelete` — borra las entradas del directorio LDAP, aceptando entradas a través de un archivo o del indicador de comandos de la shell.

A excepción de `ldapsearch`, cada una de estas utilidades es mucho más fácil de usar refiriéndose a un fichero con los cambios por realizar que a escribir los comandos uno tras otro. Cada una de las páginas de manual respectivas cubre la sintaxis de estos ficheros.

Para importar o exportar bloques de información con un directorio `slapd` o para ejecutar tareas administrativas similares se requieren diferentes utilidades, localizadas en `/usr/sbin`:

- `slapadd` — añade entradas desde un fichero LDIF a un directorio LDAP. Por ejemplo, ejecute *ldif* donde *`ldif`* es el nombre del fichero LDIF que contiene nuevas entradas.
- `slapcat` — deja fuera del directorio LAPD entradas y las guarda en el fichero LDIF. Por ejemplo, ejecute `/usr/sbin/slapcat -l` *`ldif`* donde *`ldif`* es el nombre de un archivo LDIF que contiene la entrada de un directorio LDAP.
- `slapindex` — vuelve a poner en un índice la base de datos `slapd` basada en el contenido de la base de datos actual. Ejecute `/usr/sbin/slapindex` para empezar con el índice.
- `slappasswd` — genera un valor de contraseña de usuario para usar con el valor `ldapmodify` o `rootpw` en `/etc/openldap/slapd.conf`. Ejecute `/usr/sbin/slappasswd` para crear una contraseña.

ADVERTENCIA

Asegúrese de detener `slapd` antes de usar `slapadd`, `slapcat` o `slapindex`. De lo contrario, la consistencia de su base de datos LDAP correrá riesgo.

Lea las páginas de manual (man pages) para obtener más información sobre estas utilidades.

4.8 Módulos para añadir funcionalidad a LDAP

Red Hat Linux incluye varios paquetes que añaden funcionalidad a LDAP.

El módulo `nss_ldap` es un módulo LDAP para el **Solaris Nameservice Switch** (NSS). NSS es un conjunto para las librerías C, necesarias para acceder a la información del directorio LDAP, junto al **Network Information Service** (NIS). El módulo `nss_ldap` es necesario para usar LDAP como un servicio de nombres nativo.

El módulo `pam_ldap` es necesario para integrar la autenticación de LDAP en los módulos de autentificación conectables (PAM) API. Si usa `pam_ldap`, los usuarios pueden verificar y cambiar sus

contraseñas usando el directorio LDAP. Los módulos `nss_ldap` y `pam_ldap` forman parte del paquete `nss_ldap`.

Red Hat Linux también incluye los módulos LDAP para el servidor web Apache. El módulo `auth_ldap` sirve para autentificar los clientes HTTP para las entradas del usuario en el directorio LDAP. El módulo `php-ldap` añade soporte LDAP al lenguaje escrito PHP4 HTML-embedded. Los módulos `auth_ldap` y `php-ldap` deberán ser compilados en Apache como **Dynamic Shared Objects**(**DSO**s)

4.9 LDAP How To: Resumen breve

Este apartado permite dar un repaso a los pasos necesarios para hacer funcionar un directorio LDAP.

1. Asegúrese de que RPM `openldap` y cualquier otro RPM relativo a LDAP que necesite estén instalados.
2. Lea la Guía Quick Start en el sitio OpenLDAP (http://www.openldap.org/faq/data/cache/172.html; comience por "Modificar la configuración de los ficheros para slapd", visto que los ficheros LDAP están ya instalados), o el Linux-LDAP HOWTO (http://www.linuxdoc.org/HOWTO/LDAP-HOWTO.html) para las instrucciones de como usar LDAP en su sistema. Ambos explican el resto de los pasos a seguir.
3. Modifique el fichero `/etc/openldap/slapd.conf` para adaptarlo a su sistema. (Consulte la Sección 4.6.1, *Modificar `/etc/openldap/slapd.conf`* para más información sobre como modificar `slapd.conf`.)
4. Comience `slapd` tecleando `/etc/rc.d/init.d/ldap start`. Tras haber configurado LDAP correctamente, debería usar Linuxconf o `ntsysv` para configurar LDAP e iniciar el sistema.
5. Cree su directorio LDAP (ejemplos de entradas LDAP, las encontrará en el sitio PADL Software en http://www.padl.com/ldap_examples.html).
6. Añada las entradas a su directorio LDAP con `ldapadd` o con un script.
7. Use `ldapsearch` para verificar que `slapd` funcione.
8. Llegados a este punto su directorio LDAP debe haber sido ya creado. EL siguiente paso es configurar las aplicaciones habilitadas para LDAP de manera que puedan usar el directorio LDAP.

4.10 Configurar su sistema para la autentificación mediante OpenLDAP

Este apartado ofrece una supervisión de cómo configurar su sistema Red Hat Linux para autentificarse con el uso de OpenLDAP OpenLDAP. A menos que usted sea un experto de OpenLDAP, necesitará

más documentación que la proporcionada. Para obtenerla remítase a la Sección 4.11, *Recursos adicionales*

4.10.1 Instalación de los paquetes LDAP necesarios

En primer lugar asegúrese de que los paquetes apropiados son instalados tanto en el servidor LDAP como en las máquinas cliente LDAP. El servidor LDAP necesita del paquete `openldap`.

Las máquinas cliente LDAP necesitan de la instalación de los siguientes paquetes: `openldap`, `auth_ldap` y `nss_ldap`.

4.10.2 Modificar los ficheros de configuración

Modificar `/etc/openldap/slapd.conf`

A continuación, modifique el fichero `slapd.conf` para asegurarse de que se adapta a las necesidades de su organización.

Remítase a la Sección 4.6.1, *Modificar `/etc/openldap/slapd.conf`* para ulterior información sobre modificar `slapd.conf`.

Modificar `ldap.conf`

Modifique los ficheros `ldap.conf` en `/etc` y en `/etc/openldap` sobre el servidor LDAP y sobre los clientes.

Modifique `/etc/ldap.conf`, el fichero de configuración para `nss_ldap` y `pam_ldap`, para reflejar su base de organización y búsqueda. El fichero `/etc/openldap/ldap.conf` es el fichero de configuración para las herramientas en línea de comandos como `ldapsearch`, `ldapadd`, etc y deberá ser modificado para la configuración de su LDAP. Las máquinas cliente necesitarán que ambos ficheros estén modificados para su sistema.

Modificar `/etc/nsswitch.conf`

Para usar `nss_ldap`, debe añadir `ldap` en los campos apropiados en `/etc/nsswitch.conf`. (Ponga mucha atención cuando cambie este fichero; asegurese de lo que está haciendo). Por ejemplo:

```
passwd: files ldap
shadow: files ldap
group: files ldap
```

PAM y LDAP

Para tener las aplicaciones estándar PAM, ejecute `authconfig` y seleccione **Usar LDAP**. (PAM va más allá de realizar esta supervisión de LDAP, por lo que si necesita ayuda consulte la Capítulo 8, *Módulos de autentificación conectables (PAM)* y/o las páginas de manual de PAM.

4.10.3 Migrar su viejo método de autentificación al formato LDAP

El directorio `/usr/share/openldap/migration` contiene un conjunto de scripts de shell y Perl para cambiar sus métodos antiguos de autentificación al formato LDAP. Deberá haber instalado Perl en su sistema para usar estos scripts.

En primer lugar deberá modificar el fichero `migrate_common.ph` de manera que refleje su dominio. El dominio DNS por defecto debería cambiarse de:

```
$DEFAULT_MAIL_DOMAIN = "padl.com";
```

a algo parecido a:

```
$DEFAULT_MAIL_DOMAIN = "your_company.com";
```

También la base por defecto debería ser cambiada, de:

```
$DEFAULT_BASE = "dc=padl,dc=com";
```

a algo parecido a:

```
$DEFAULT_BASE = "dc=your_company,dc=com";
```

Después, debe decidir qué script utilizar. La siguiente tabla debería servirle de ayuda:

Tabla 4–1 Scripts de migración a LDAP

Nombre actual del servicio	¿LDAP está activado?	Utilice este script:
`/etc` flat files	sí	`migrate_all_online.sh`
`/etc` flat files	no	`migrate_all_offline.sh`
NetInfo	sí	`migrate_all_netinfo_online.sh`
NetInfo	no	`migrate_all_netinfo_offline.sh`
NIS (YP)	sí	`migrate_all_nis_online.sh`
NIS (YP)	no	`migrate_all_nis_offline.sh`

Ejecute el script adecuado basándose en su nombre de servicio actual.

Los ficheros `README` y `migration-tools.txt` en `/usr/share/openldap/migration` proporcionan más detalles.

4.11 Recursos adicionales

En la web puede encontrar más información útil referente a LDAP. Use estos recursos, en especial visite el sitio web OpenLDAP y el LDAP HOWTO, antes de iniciar e introducir LDAP en su sistema.

4.11.1 Documentación instalada

- La página de manual `ldap` es un buen lugar donde empezar a documentarse sobre LDAP. Existen también páginas de manual para los demonios y las utilidades LDAP. Revise las páginas de manual si necesita más información sobre `ldapmodify`, `ldapsearch`, etc.
- `/usr/share/docs/openldap-`*`versionnumber`* — contiene un documento general `README` e información variada.

4.11.2 Sitios Web útiles

- http://www.openldap.org — Sitio del proyecto OpenLDAP, intento de desarrollar un paquete open source LDAP de herramientas de desarrollo y aplicaciones.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Documento LDAP Linux HOWTO, que cubre la instalación a través de la autentificación y el registro.
- http://www.padl.com — Desarrolladores de `nss_ldap` and `pam_ldap`, entre otras herramientas útiles de LDAP.
- http://www.innosoft.com/ldapworld — Contiene información referente a las versiones LDAP RFCs y LDAP.
- http://www.kingsmountain.com/ldapRoadmap.shtml — El Road Map de LDAP de Jeff Hodges contiene enlaces a diversas FAQs útiles y emite noticias referentes a LDAP.
- http://www.rudedog.org/auth_ldap — Sitio del módulo de autentificación `auth_ldap` para Apache.
- http://www.stanford.edu/~bbense/Inst.html — Habla del uso de LDAP con Sendmail.
- http://www.webtechniques.com/archives/2000/05/wilcox — Vista preliminar útil para gestionara grupos en LDAP.
- http://www.ldapman.org/articles — Artículos que ofrecen una buena introducción a LDAP, incluyendo métodos para diseñar un árbol de directorio y estructuras de directorio personalizadas.

4.11.3 Libros relacionados

- *Implementing LDAP* de Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* de Tim Howes et al.; Macmillan Technical Publishing

5 Sistema de verificación de tarjeta de crédito (CCVS)

El sistema de verificación de tarjetas de crédito (CCVS) usa su ordenador y módem para simular una tarjeta de crédito (también conocido como **Punto de venta** (**POS**). CCVS incluye varias interfaces de programación de aplicaciones (APIs) que facilitan la personalización e integración con aplicaciones software o productos de la base de datos.

CCVS es seguro y fácil de usar. Escrito en ANSI C y ajustado a estándares POSIX, CCVS es portable y de fácil integración en los sitemas operativos modernos, lenguajes de programación e Internet. CCVS puede ser usado para automatizar procesos de lotes o mejorar cualquier aplicación que requiera procesar tarjetas de crédito.

CCVS puede ser usado en otros países si su banco puede soportar una de los protocolos soportados por CCVS. Si está en Canadá, CCVS soporta el protocolo NDC, que puede ser usado por cualquier banco en Canadá para configurar su cuenta mercantil. Si está en un país que no sea Estados Unidos o Canadá, necesitar verificarlo con su banco. El protocolo soportado por CCVS que tiene más oportunidades de ser soportado por una institución financiera fuera de Estados Unidos es el protocolo Visa 2nd generation “K Format” (VITAL).

Una versión de muestra de CCVS está incluida con Red Hat Linux. La versión demo es completamente funcional y puede ser usada para CCVS y su sistema. La versión demo hará todo excepto contactar con su institución financiera. Si elige comprar CCVS necesitará contactar con Red Hat para comprar una licencia. Vaya a http://www.redhat.com/products/ccvs/, para más información de como activar CCVS.

5.1 Usos de CCVS

CCVS destaca en la creación de conexiones entre una aplicación e-commerce y una puerta de enlace de pago con tarjeta de crédito. Mientras que los modos en que puede utilizar CCVS dependen del protocolo que utiliza su puerta de enlace de pago, en muchos casos, CCVS puede ser utilizada con muy pocos cambios en un sistema ya existente. Vaya a http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html, para información específica sobre los diferentes protocolos soportados por CCVS.

Observe los siguientes ejemplos de cómo se puede usar CCVS:

- CCVS puede soportar un sistema para operadores de teléfono que toma órdenes de catálogo por teléfono. Las extensiones Tcl de CCVS pueden ser usadas para crear un GUI (interfaz gráfica de usuario) Tcl/Tk que presenta una interfaz sencilla para los operadores de teléfono. Los operadores pueden entonces usar los terminales simples X y todo el software se ejecutará en el servidor central.

CCVS solamente necesita ser instalado en un ordenador y los operadores no tienen que esperar a tener una línea disponible — todas esas transacciones irán sobre la misma llamada de teléfono.

- CCVS puede ser usado para ayudar a automatizar la facturación. Por ejemplo, el servidor de servicios de internet (ISP) puede tener una base de datos de clientes en una base de datos del servidor. El administrador de base de datos ISP puede escribir un script Perl, combinando el módulo Perl de CCVS con un módulo para el sistema de la base de datos ISP. El script leería los datos del cliente, procesará la facturación mensualmente y actualizaría el registro de la base de datos para indicar que el pago ha sido realizado.
- CCVS puede utilizarse para agilizar los procesos de pago de un escaparate de también utiliza una centralita para gestionar los pedidos por teléfono. De este modo, los pedidos procesados a través de la web, mediante el uso de una aplicación estándar CGI o mediante un agente de ventas que usa el programa de personalización Java y ejecutándolo a través de la LAN, pueden hacerse a través de la misma conexión. Además, el sistema de verificación de direcciones (AVS) de CCVS puede utilizarse para prevenir el fraude en los dos métodos de pedido sin tener que preocuparse sobre la implementación de esta característica por separado en cada una de las aplicaciones, por lo tanto, ahorro de tiempo de desarrollo.

Aquí encontrará algunos ejemplos de lo que es capaz de hacer CCVS. Se puede utilizar para mejorar cualquier aspecto de sus operaciones que requiera el tratamiento de la tarjeta de crédito. Entre las muchas características de CCVS se incluyen:

- Una librería C con un API documentado autoriza a los usuarios a integrar CCVS con las aplicaciones existentes.
- Una extensión Tcl habilita el uso de CCVS con un lado del servidor Tcl como NeoWebScript.
- Un módulo Perl 5.0 permite a CCVS trabajar con el lenguaje de programación CGI más popular usado hoy en día.
- La capacidad de construir rápidamente GUIs personalizados usando — Tcl/Tk — tiempo estimado de desarrollo, menos de un día.
- Los módulos Python, PHP3 y Java permiten a CCVS funcionar con otros lenguajes de programación comunes.
- Los programas Command Line Interface (CLI) de uso interactivo — llaman a programas desde cualquier shell UNIX y programa en el lenguaje UNIX que prefiera.
- La protección contra el fraude AVS , permite a los comerciantes comprobar las tarjetas de crédito robadas. Muchos bancos de compensación ofrecen un mejor cambio(rate) a los comerciantes que usan AVS, incluso en pedidos hechos por teléfono.
- Soporta múltiples cuentas mercantiles, permitiendo a los usuarios abrir sus propias tiendas virtuales con escaparates ilimitados. Una **cuenta mercatil** es un tipo especial de cuenta bancaria que

permite a los compradores aceptar pagos con tarjetas de crédito de los clientes. La cuenta mercantil mantiene los procedimientos desde las transacciones de las tarjetas de crédito.

- La habilidad de dirigir mútiples transacciones en una única sesión, (dos segundos por transacción) sin coste extra o complejidad.
- La seguridad de ser capaz de comprobar y crear programas de desarrollo del producto sin cargar tarjetas de crédito reales.

5.2 Proceso de verificación de la tarjeta de crédito

¿Cómo se le dice a la gente corriente que con un pequeño trozo de plástico puede permitirse el lujo de comprar una TV de pantalla grande?

En primer lugar, un consumidor da la información de su tarjeta de crédito al comerciante. El comerciante transmite esos datos, con el código ID del comerciante, a un banco de compensación. Ista puede ser el banco que ha emitido al comerciante su cuenta de la tarjeta de crédito, pero es más parecido a una empresa que ha pactado con el banco del comerciante compensar cobros a cambio de una cuota fija y un porcentaje de cada cobro procesado.

Los datos se transmiten leyendo la tarjeta y los números del comerciante a través del teléfono, usando un terminal POS, o usando CCVS u otro tipo de sotfware para transmitir información desde un ordenador

El banco de compensación se pone en contacto con el banco que emite la tarjeta de crédito del cliente y verifica que éste acepta el cobro. Si es aceptado, el banco de compensación manda un mensaje de confirmación al comerciante. Al mismo tiempo, el crédito disponible de la tarjeta de crédito del cliente se le descuenta la cantidad de la transacción.

Al final de un día de compras, el comerciante (de hecho, el ordenador del comerciante o terminal de las tarjetas de crédito) llamará al banco de compensación y verificará todas las transaccionte del día para garantizar que el sistema del comerciante y al banco de compensación están de acuerdo con las transacciones que se han producido a lo largo del día. A continuación el banco de compensación inicia el proceso de transferir el dinero desde el banco de tarjeta de crédito a la cuenta bancaria del comerciante.

5.3 Todo lo que necesita para ejecutar CCVS

Para ejecutar CCVS, necesitará un módem y una cuenta mercantil. También necesitará seguir unas pautas para ejecutar correctamente CCVS.

5.3.1 Módems

Necesitará como mínimo un módem dedicado al uso de CCVS. Los protocolos de las tarjetas de crédito no soportan compresión o corrección de errores durante la conexión del módem. Podemos proporcionarle información acerca de las características de los siguiente módems:

- Hayes Optima
- US Robotics Courier
- US Robotics Sportster
- Chase Research PCI-RAS

Nota

Por favor use un módem o los módems de la lista anterior.

Si usa un módem que no se soporte, puede ser muy difícil hacer que éste funcione con CCVS. También debe comprobar la lista de compatibilidad del hardware de Red Hat Linux en http://www.redhat.com/support/hardware/ para estar seguro que su módem funcionará con Red Hat Linux

Si el módem que usa no aparece en la lista, consulte el manual del módem para encontrar el string que desactiva *todas* las compresiones y correcciones de errores y el string que reinicia su módem para uso normal. Necesitará proporcionar estos dos strings cuando configure CCVS.

5.3.2 Cuentas mercantiles

Si está configurando una cuenta mercantil o está modificando una cuenta mercantil existente para usar CCVS, el proveedor de la cuenta mercantil querrá comprobar que CCVS puede funcionar con el protocolo que usa. Las cartas de certificación para protocolos específicos están disponibles en http://www.redhat.com/certifications.html. Imprima todas las páginas de la carta correspondientes al protocolo que usará y muéstrelas a su proveedor de cuenta mercantil.

El proveedor debe usar uno de los protocolos soportados por CCVS:

- Protocolo First Data Corporation’s ETC PLUS (conocido también como FDR7, ETC+, ETC7, Omaha)
- Protocolo First Data Corporation’s South Platform (conocido también como Nabanco)
- Protocolo Global Payment Systems’ MAPP (conocido también como St. Louis)
- Protocolo Global Payment Systems’ NDC (conocido también como Atlanta)

- Protocolo Visa International's VITAL (conocido también como VisaNet, Visa 2nd generation, K format)
- Protocolo Paymentech's UTF (conocido también como GENSAR)
- Protocolo NOVA Information Systems protocol

Si su proveedor de cuenta mercantil posee uno de estos protocolos, podrá usar CCVS.

Una vez haya identificado qué protocolo usará, revise la información aplicable a ese protocolo en http://www.redhat.com/CCVS3.3docs/protocol-specific.html antes de iniciar el proceso de configuración de CCVS. La *Guía del protocolo CCVS* describe la funcionalidades soportadas por los diferentes protocolos.

5.3.3 Pautas para usar CCVS en su sistema

Los siguientes requisitos permiten ejecutar CCVS fácilmente y eficazmente. Por favor asegúrese de seguir todas las pautas antes de intentar ejecutar CCVS.

Uso exclusivo del módem mientras que se ejecuta CCVS

No ejecute otras aplicaciones de software que necesiten acceso al módem mientras esté ejecutando CCVS. Istas pueden interferir en las operación correcta de CCVS haciendo que el módem sea inaccesible y evitando que los nuacute;meros de tarjeta de crédito sean procesados.

Permisos, privilegios y accesos al módem

La mayoría de los permisos necesarios para CCVS son configurados durante el proceso de instalación, a través de la creación de un grupo especial llamado "ccvs". Sin embargo, deberá estar al tanto de ciertas cuestiones referentes a los permisos de sistema y a CCVS. Dichas cuestiones vienen detalladas en esta sección.

Todas las operaciones para un configuración particular de CCVS deben realizarse desde una cuenta de usuario simple. Una cuenta es requerida para que todos los ficheros propios y permisos sean correctamente fijados y protegidos (por usted o por su administrador del sistema). Esta cuenta de usuario debe ser añadida al grupo ccvs antes de ejecutar el programa de configuración.

Después de que el usuario haya sido añadido al grupo ccvs, ejecuta el programa de configuración CCVS (`ccvs_configure`) como ese usuario. Tras haber ejecutado el programa de configuración, el mismo usuario ejecuta los comandos de CCVS para esa configuración.

Si quiere ejecutar CCVS con un módem, los usuarios en el grupo ccvs deben ser añadidos también al grupo uucp. Los permisos del grupo uucp pueden no ser suficientes para ejecutar los módems. Si éste es el caso de su sistema, asegúrese de que los miembros del grupo ccvs también tienen acceso al puerto serie para los módems que CCVS necesita usar.

Si está usando PHP con CCVS, habilite el servidor Web para ejecutar los comandos de CCVS. Para lograr esto, tiene que hacer del usuario del servidor Web un miembro del grupo ccvs. Normalmente, el usuario también necesita ser miembro del grupo uucp.

Si no está usando PHP, pero quiere hacer que el servidor Web sea capaz de ejecutar CCVS, tiene otra opción (por ejemplo, `suexec`, `setuid`) haciendo al usuario del servidor Web un miembro del grupo ccvs. Puede configurarlo como quiera, menos si está usando PHP.

Versiones de software

CCVS requiere la versión Tcl 7.6 o superior para ejecutar el GUI incluido o para usar las APIs Tcl/Tk incluidas para desarrollar su propio escaparate gráfico. La versión Tcl 8.3 está incluida en Red Hat Linux 7.1.

CCVS requiere la versión Perl 5.0 o superior para usar las APIs de Perl incluidas. La versión de Perl 5.6 está incluida en Red Hat Linux7.1.

5.4 Instalación de CCVS

Los RPMs de CCVS están disponibles en el CD Linux Applications Library Workstation.

Puede usar RPM, Gnome-RPM o Kpackage para instalar los paquetes de CCVS:

- `CCVS` — El núcleo de los programas CCVS
- `CCVS-devel` — El kit de desarrollo en C
- `CCVS-perl` — La interfaz Perl interface para CCVS
- `CCVS-python` — La interfaz Python para CCVS
- `CCVS-php3` — La interfaz PHP3 para CCVS
- `CCVS-tcl` — La interfaz Tcl CCVS
- `CCVS-java` — La interfaz Java para CCVS (incluida como código fuente)
- `CCVS-examples` — Ejemplo de código fuente, necesario para el desarrollo

5.5 Antes de configurar CCVS

Antes de configurar CCVS, es necesario que responda ciertas preguntas sobre su sistema y sobre como quiere configurar CCVS. Para preparar el proceso de configuración, asegúrese de seguir estos pasos:

1. Lea atentamente toda la documentación y errata que viene con el programa. Consulte la Sección 5.11, *Recursos adicionales* para la localización de la documentación instalada o en línea de CCVS.
2. Compile `setup.txt`. El fichero `setup.txt` explica las diferentes informaciones necesarias cuando se configura CCVS para usar protocolos particulares. Si compila `setup.txt`,

tendrán toda la información necesaria para el proceso de configuración, evitando, de este modo, cualquier sorpresa al ejecutar el programa de instalación Puede encontralo en el directorio `/usr/share/doc/CCVS-<version>`. `setup.txt` esta también disponible en http://www.redhat.com/products/ccvs/support/CCVS3.3docs/setup.txt.

Nota

En la configuración de la hoja de trabajo, se le pedirá información específica sobre un protocolo. Sólo necesitará proporcionar informació sobre el protocolo que va a usar, no es necesario que lo haga para otros protocolos.

---

3. El programa de instalación de CCVS le preguntará varias cosas acerca del módem, tenga a mano la información necesaria. Los siguientes init strings pueden ser usados con los módems que son soportados:

Hayes Optima or ACCURA

```
\r~~~\rAT &D3 X4 E0 &K0 &Q0
```

U.S. Robotics Sportster or Courier

```
\r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
```

Chase Research PCI-RAS

```
\r~~~\rAT E0 %C0 \\N0
```

Si usa uno de los módems soportados, el programa de configuración tan sólo le preguntará que confirme el string init. Si su módem no aparece en la lista, consulte el manual del módem para encontrar el string que anula la compresión y correción de errores, así como, el string que reinicia el módem para uso normal. Necesitará fijar esos dos strings durante el proceso de configuración.

5.6 Configuración de CCVS

Debe configurar CCVS para su sistema, si está ejecutando CCVS en modo de prueba o para procesar los datos reales.

Use `su` para cambiar la cuenta de usuario que creó (un miembro del grupo ccvs) para esta configuración.

Ejecute el programa de configuración de CCVS con el siguiente comando:

```
/usr/sbin/ccvs_configure
```

El resto de esta sección hablará del programa de configuración CCVS. Debería leer la pantalla inicial "splash". Pulse [Intro] para leer la licencia de software de CCVS. Puede usar los comandos estándar de barras de desplazamieto y paginación de `more` (o el programa de paginación configurado por su variable de entorno $PAGER) para leer la licencia.

Cuando haya leído la licencia y salido de la página, verá

```
Type "accept" to accept this license, or anything else to exit.
```

Teclee la palabra **`accept`** para aceptar las condiciones de la licencia y continuar configurando CCVS. Cualquier otra entrada le hará salir del programa.

Le aparecerá esta pantalla:

```
This program creates the configuration file for CCVS functions.
To do this, you will require the following information:
 1: The clearing protocol you will be using. This may be MAPP,
ETC+, or any of the other protocols which CCVS supports. There
is also a demo protocol; if you have downloaded the free demo of
CCVS, you will be using the demo protocol.
 2: The unique number which identifies you to the clearing
house. This may be your merchant account number or a terminal id
number, depending on what protocol you will be using. This number
will be supplied when you set up your merchant account.
 3: Your modem type, and the serial port your modem is attached
to. You will also need modem configuration strings. (We can
supply modem configuration strings for many popular modems.)
 4: The location of your data directory. This is where the
configuration file and data directories will be placed.
 5: Other information as needed for particular protocols. This
information will generally be supplied when you set up your
merchant account.

We supply a worksheet which you can use to organize all this
information, including the details for each protocol. See the
file "setup.txt" in /usr/share/doc/CCVS-<version>.

The configuration program is running as user "<username>".
It is important that this be the same user which the actual CCVS
software will run as. (We recommend creating a special user
account for just this purpose.)

Do you wish to continue configuring CCVS as user "<username>"?

[Enter Y to continue, or N to stop here:]
```

Presione [Y] para continuar. Si ejecuta `su` como root, le aparecerá el siguiente error. Si esto ocurre debería ejecutar `su` para el usuario de CCVS y volver a ejecutar `ccvs_configure`.)

```
The configuration program may not be run as root. You must run
this as the same user which the actual CCVS software will run as.
(We recommend creating a special user account for just this
purpose.)
```

Cuando continúe, el programa le solicitará infomación. En cualquier momento, puede volver atrás tecleando **.** y presionando [Intro].

```
Do you want to configure CCVS for the free demo, or a working
merchant account? (If you have not purchased a license for CCVS,
only the demo configuration is available.)

[Enter Y to use the demo configuration, N for a real configuration,
or . to exit:]
```

A menos que haya comprado una clave de software y una licencia para CCVS, teclee [Y]. Esto instala una configuración demo, que no marca el número de módem ni usa una cuenta mercantil real. Si ha comprado una licencia y está preparado para instalar una configuración que ya funciona, teclee [N].

```
Where do you want to place the CCVS configuration files and
transaction queues? This should be a directory name which is
writable by the current user.
The default is "/var/ccvs".
Enter directory, or Return for default value, or . by itself to
back up.
>
```

A menos que tenga razones específicas para trasladar los ficheros de configuración de CCVS y las colas de transacciones, déjelos en su localización por defecto. Si necesita trasladarlos, recuerde que también necesita fijar una variable de entorno.

```
What do you want to name this configuration? This should be a
short filename.
The default is "ccvs".
Enter name, or Return for default value, or . by itself to back
up.
>
```

Por ejemplo, puede tener una configuración llamada **`camiseta`** para un comerciante que vende camisetas y otra llamada **`música`** para un vendedor al por menor de partituras. El nombre introducido servirá para distinguir entre las dos configuraciones.

La versión demo de CCVS no requiere otra información. A continuación verá:

```
Writing "/var/ccvs/ccvs.conf"...
```

```
The CCVS system is now configured.
```

Puede empezar comprobando el software demo. El software demo es igual al software completo de CCVS, con la excepción de que no marca el nuacute;mero de módem o habla con un procesador mercantil real.

Si tiene una licencia de la versión completa de CCVS y elige instalar un configuración real, verá algo como esto:

```
Which protocol and merchant processor will you be using?

Credit card clearing protocols:
  1: ETC PLUS (FDR7/ETC7/FDR "Omaha"): First Data Corporation
  2: South Platform (FDR "Nabanco"): First Data Corporation
  3: MAPP: Global Payment Systems "St. Louis"
  4: NDC: Global Payment Systems "Atlanta" / NDC
  5: VITAL (Visa 2nd generation, K format): Visa/Total System Services
  6: UTF: Paymentech Inc.
  7: NOVA: NOVA Information Systems

[Enter a number, or . by itself to back up:]
```

Seleccione del protocolo para que tenga una licencia de CCVS y una cuenta mercantil válida.

```
What is the number of your merchant account?
Enter number, or . by itself to back up.
>
```

Este número debería haber sido proporcionado con su cuenta mercantil.

```
What is your CCVS software customer number?
Enter number, or . by itself to back up.
>
```

Este número habrá sido proporcionado con su licencia CCVS.

```
What is your CCVS software license key?
Enter number, or . by itself to back up.
>
```

Este número también habrá sido proporcionado con su licencia CCVS.

```
What is the phone number of your merchant processor?
Enter number, or . by itself to back up.
>
```

Pueden aparecer preguntas adicionales, ya que algunos protocolos en particular requieren información diferente. Si ha compilado la hoja de trabajo de `setup.txt` para su protocolo, deberá estar preparado para estas preguntas. Por ejemplo, VITAL continua con varias como el nombre del comprador, dirección, banco,etc. Debería tener localizada toda esta información cuando establezca una cuenta mercantil VITAL. Éste es el objetivo del archivo de la hoja de trabajo `setup.txt`, que debería haber completado antes de ejecutar el programa de configuración CCVS. Consulte la Sección 5.5, *Antes de configurar CCVS* para más información referente al uso de `setup.txt`.

A continuación introduzca la información acerca de cómo comunicarse con su módem. La información de configuración del módem es muy importante. Asegúrese de que introduce la información correcta para la configuración de su sistema; CCVS no funcionará si el módem está configurado incorrectamente.

```
Do you want to configure a pool of several modems? (If you answer
yes, all the modems must be exactly the same make and model. If
you want to use just one modem, answer no.)

[Enter Y or N, or . to back up:]
```

Si tiene varios módems idénticos, puede configurar CCVS para usarlos todos, como pool. Cada proceso de CCVS que necesite usar un módem dibujará uno del pool, asumiendo que hay alguno disponible. Varias configuraciones CCVS pueden compartir un conjunto de módems de esta manera. Puede configurar también una configuración simple con dos módems, para que las autorizaciones y settlement batch pueda ocurrir al mismo tiempo.

```
What serial port is your modem connected to? (Do not include the
"/dev/" prefix.) The default is ttyS0. The modem should be
connected and ready now, so that the serial port can be tested.

Enter port name, or Return for default value, or . by itself to
back up.
>
```

El programa comprobará el puerto serie que utilizará. Si configura más de uno, comprobará cada uno de ellos. No incluya `/dev/`. Este paso puede llegar hasta los treinta segundos si el módem no responde.

```
What type of modem do you have? This information makes it
possible to suggest modem configuration strings. If your modem
is not listed, you can choose "none of the above"; but you will
then have to create your own configuration strings, which is a
difficult process.

 1: USR Sportster/Courier
 2: Hayes Optima
 3: Chase Research PCI-RAS
```

```
 4: None of the above

[Enter a number, or . by itself to back up:]
```

Será introducido a la inicialización del módem, a la acción de marcar y a los strings de la acción de colgar. (Si configura un pool de módems, todos deberían ser idénticos, de manera que utilicen los mimsos strings.) Si CCVS conoce strings apropiados para el módem, serán sugeridos y usted tendrá simplemente que pulsar [Intro].

```
The modem initialization string should set the modem to do no
protocol
negotiation. What string do you want to use?
A string which works for your modem is:
 \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Enter string, or Return for suggested value.
>

The modem dial string should dial the modem. (Do not include a
phone number.)
What string do you want to use?
A string which works for your modem is:
 ATDT
Enter string, or Return for suggested value.
>

The modem hang-up string should hang the modem up if it's
connected. What string do you want to use?
A string which works for your modem is:
 ~~~+++~~~~~~~~~\rATH0\r~~~
Enter string, or Return for suggested value.
>

Initialize: \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Dial: ATDT
Hang up: ~~~+++~~~~~~~~~\rATH0\r~~~
Are these the values you want?

[Enter Y to accept, N to change, . to back up.]
```

Puede que no vea exactamente la misma pantalla porque los valores por defecto varían dependiendo del módem selecionado.

La siguiente pregunta hace referencia a la frecuencia en baudios que utilice el módem:.

```
What baud rate do you want to use? You should use the
default unless you have explicit information that another
```

```
value is appropriate.
The default baud rate is 1200.

Enter rate, or Return for default value, or . by itself to
back up.
>
```

Cuando haya finalizado de introducir la información de la configuración verá:

```
Writing "/var/ccvs/ccvs.conf"...

The CCVS system is now configured.
```

5.7 Cuentas mercantiles múltiples

Si necesita soportar más cuentas mercantiles, simplemente siga el proceso de configuración de nuevo. Use un nombre de configuración diferente para cada cuenta mercantil.

Diferentes configuraciones pueden compartir el mismo puerto serie o el mismo pool de puertos serie. Los módems serán usados de menera que el primero en llegar, será el primero en salir.

5.8 Inicio de CCVS

Para ejecutar CCVS para una aplicación en particular, deberá haberse registrado como la cuenta de usuario que ha creado esa configuración. Si está usando una cuenta de usuario ccvs con este propósito y ya se ha registrado en el sistema como un usuario diferente, escriba `su ccvs` para cambiar al usuario adecuado.

Cuando se haya registrado como la configuracíón de usuario para ejecutar los programas CCVS, necesitará iniciar el demonio `ccvsd` para cada cuenta mercantil y necesitará ejecutar el programa `cvupload` en una base regular. Usar `cron` para ejecutar `cvupload` todo los días es buena idea (consulte las páginas de manual para las instrucciones referentes a procesos automáticos).

5.8.1 Demonio ccvsd

Para ejecutar CCVS, debe ejecutar el demonio `ccvsd`. El demonio `ccvsd`, de hecho, hace las llamadas de teléfono y dirige las transacciones. Al comando `ccvsd` le debe seguir el nombre de la cuenta especificado cuando configuró la cuenta.

Por ejemplo, si quiere empezar procesando las transacciones del ejemplo del vendedor al por menor de partituras mencionado durante el programa de configuración e instala el software en la localización por defecto de `/usr/sbin`, deberá teclear el siguiente comando para iniciar `ccvsd`:

```
/usr/sbin/ccvsd music
```

Cada vez que añada una cuenta mercantil, necesita empezar `ccvsd` por esa cuenta, si quiere procesar las transacciones para esa cuenta.

Para más información de `ccvsd`, consulte la página de manual de `ccvsd`.

5.8.2 Comando `cvupload`

Algunas transacciones (como autorizaciones) ocurren al mismo tiempo que se presenta la tarjeta de crédito. Otras transacciones (como compras o devoluciones) son grabadas y no son procesadas inmediatamente. Esas transacciones son agrupadas procesadas como grupo.

CCVS usa el programa `cvupload` para realizar el proceso batch. Le recomendamos que ejecute `cvupload` como una tarea diaria `cron`, para que `cvupload` se ejecute automáticamente todos los días, sin ninguna intervención por su parte.

Por ejemplo, el comando utilizado para el proceso periódico del vendedor de partituras será el siguiente:

```
/usr/sbin/cvupload music
```

Para más información acerca de `cvupload`, consulte la página de manual `cvupload`.

5.9 Consideraciones especiales sobre el lenguaje

- C — La librería C CCVS está incluida en el paquete `CCVS-devel`. Al compilar un programa C que usa CCVS, añada el indicador `-lccvs` en la línea de montaje.
- Vaya a http://www.redhat.com/CCVS3.3docs/AdminJava.html, para más información sobre la construción de la interfaz Java de CCVS. El código fuente de la interfaz Java está incluido en el paquete `CCVS-java`.
- Perl — La interfaz Perl incluida en el paquete `CCVS-perl`.
- Python — La interfaz Python interface incluida en el paquete `CCVS-python`.
- PHP — La interfaz PHP3 incluida en el paquete `CCVS-php3`.
- Tcl — La interfaz Tcl incluida en el paquete `CCVS-tcl`.

5.10 Soporte para CCVS

El soporte para CCVS puede comprarse a Red Hat. Cuando compre la clave para activar CCVS, asegúrese de repasar las opciones de soporte disponibles. Vaya a http://www.redhat.com/products/ccvs/ para más información sobre la compra de una clave y la obtención de soporte para CCVS.

Si necesita soporte, asegúrese de tener la siguiente información a mano, antes de contactar con el soporte:

- Nombre de su empresa.
- La versión de CCVS que está usando.
- Su número mercantil.
- Su número de cliente CCVS.
- Su sistema operativo y la versión.

La asistencia técnica Red Hat intentará resolver cualquier problema relativo a CCVS. No soportamos productos de terceros, a excepción de problemas referentes a la integración con CCVS.

5.11 Recursos adicionales

Información adicional relativa a CCVS.

5.11.1 Documentación instalada

- `/usr/share/doc/CCVS–<version-number>` — contiene los ficheros `CHANGES`, `LICENSE` y `README`, más la hoja de trabajo para ayudar a recopilar la información necesaria antes de ejecutar el programa de instalación.
- Teclee `man ccvs` para obtener una descripción de los diferentes estados de la transacción, códigos de errores CCVS y más. Las páginas de manual para `ccvsd`, `cvreport` se pueden utilizar con estos comandos.

5.11.2 Sitios Web útiles

- http://www.redhat.com/products/software/ecommerce/ccvs — desde esta localización, puede conectar con recursos muy diversos CCVS, incluyedo las FAQs, especificaciones técnicas e información general sobre CCVS.
- http://www.redhat.com/products/software/ecommerce/ccvs/support/documentation.html — contiene enlaces a diversas guías, escritas específicamente para explicar todas las posibilidades de uso de CCVS. Estos manuales en línea cubren todo, desde la instalación y la configuración de CCVS a la descripción de los APIs para los diversos idiomas que se pueden usar.

6 Sendmail

6.1 Introducción a Sendmail

Sendmail es un conocido **agente de transferencia de correo** (**MTA**) usado en Internet, que maneja un amplio porcentaje de todos los correos ruteados en Internet a la vez que se traslada de un host a otro. Existen otros agentes de transferencia de correo (que pueden ser utilizados con Red Hat Linux), pero la mayoría de administradores eligen utilizar Sendmail como MTA debido a su potencia, escalabilidad y compatibilidad con los estándares de Internet.

El deber principal de Sendmail, como otros MTAs, es el de trasladar con seguridad emails entre hosts, habitualmente usando el **Simple Mail Transfer Protocol** (**SMTP**). No obstante, Sendmail es altamente configurable, permitiendo controlar cada aspecto de cómo se gestiona un correo.

Los inicios de Sendmail pueden ser trazados desde el nacimiento del email que ocurrió en el década antes del nacimiento de ARPANET, el precursor de Internet. En aquel tiempo, cada buzón de correo de usuario era un archivo que sólo tenían derecho a leer el usuario y las aplicaciones de correo añadían simplemente texto a aquel archivo. Cada usuario tenía que franquear sus archivos de correo para poder encontrar un correo antiguo y ser capaz de leer correo nuevo era todo un trabajo. La primera transmisión de un mensaje de correo desde un host a otro, no tuvo lugar hasta el 1972, cuando el correo electrónico (email) se empezó a transferir mediante FTP sobre el protocolo de red NCP. Este sencillo método de comunicación se hizo popular rápidamente, hasta llegar al punto de realizar la mayoría de tráfico de ARPANET en menos de un año. No obstante, la falta de estandarización entre protocolos hizo que el correo electrónico fuera difícil de enviar desde algunos sistemas, problema que se prolongó hasta la llegada en 1982 de de ARPANET estandarizado. Se hizo posible con SMTP, un nuevo protocolo para el transporte de mensajes. Estos avances, combinados con archivos de HOSTS siendo reemplazados con DNS, permitieron realizar un MTA sólido. Sendmail, surgió de un sistema anterior de entrega de correo electrónico llamado Delivermail y se convirtió rápidamente en estándar cuando Internet empezó a ser ampliamente utilizada.

Es importante ser consciente de lo que Sendmail representa y de lo que le puede ayudar, así como de lo que no es capaz. Actualmente, con las aplicaciones monolíticas que cumplen diferentes roles, podría pensar inicialmente en la necesidad de ejecutar un servidor de correo dentro de su organización. Tecnicamente, Sendmail puede poner en espera el correo a los directorios de sus usuarios y acepta nuevos correos electrónicos a través de la línea de comandos. Pero, los usuarios de hoy en día necesitan bastante más que una sencilla entrega de correo electrónico. Casi siempre desean interactuar con su correo electrónico mediante el uso del **agente de usuario de correo** (**MUA**) que utiliza el **Protocolo Post Office** (**POP**), el **Protocolo de acceso a mensajes de Internet** (**IMAP**)o incluso la Web. Estos otros protocolos pueden trabajar conjuntamente a Sendmail y SMTP, pero de hecho existen por razones diversas y pueden operar por separado.

El objetivo de este capítulo es el de mostrarle todo lo que es capaz de hacer Sendmail. Consulte las fuentes de información en línea y fuera de ésta en Sendmail para poderse hacer una idea de sus necesidades. No obstante, debería saber qué archivos han sido instalados en su sistema por Sendmail por defecto, saber como realizar cambios básicos de configuración, ser capaz de detener correo electrónico no deseado (spam) enviado a través de Sendmail y saber como ampliar Sendmail con el **Lightweight Directory Access Protocol** (**LDAP**).

6.2 La instalación Sendmail por defecto

Mientras que descarga el código fuente para Sendmail y construir su propia copia, muchos usuarios prefieren instalar Sendmail mediante RPM desde el CD-ROM (durante la instalación de Red Hat Linux o posteriormente).

La aplicación Sendmail está ubicada en `/usr/sbin`.

La longitud de Sendmail y el archivo de configuración detallada `sendmail.cf` son instalados en `/etc`. No debería modificar el archivo `sendmail.cf` sin usar el macro procesador `m4` para crear un nuevo `/etc/sendmail.cf` (obviamente tras haber hecho un copia de seguridad del antiguo `/etc/sendmail.cf`). Para más información sobre la configuración de Sendmail, remítase a la Sección 6.3, *Cambios comunes de configuración*.

Varios archivos de configuración Sendmail están instalados en `/etc/mail` incluyendo:

- `access` — especifica qué sistemas pueden usar Sendmail para transferir un email.
- `domaintable` — le permite proporcionar un mapeo del nombre de dominio.
- `local-host-names` — el lugar donde se incluyen todos los aliases para su máquina.
- `mailertable` — especifica las instrucciones que sobreescriben el ruteo de dominios particulares.para sobreescribir.
- `virtusertable` — le permite realizar una forma de dominio específico de alias, permitiéndole dominios virtuales múltiples para ser host en una máquina.

Algunos de los ficheros de configuración en `/etc/mail`, tales como `access`, `domaintable`, `mailertable` y `virtusertable`, deben almacenar su información en archivos de base de datos antes de que Sendmail pueda cambiar de configuración. Para incluir cualquier cambio que haga en esa configuración en sus archivos de base de datos, debe ejecutar un comando con la sintaxis `make-maphash /etc/mail/`*`name`* `< /etc/mail/`*`name`* donde *name* es el nombre del archivo de configuración a convertir.

Por ejemplo, si desea que todos los emails dirigidos a cualquier cuenta `domain.com` sean entregados a `bob@otherdomain.com`, necesitará añadir una línea al archivo `virtusertable`:

```
@domain.com       bob@otherdomain.com
```

Para añadir esta nueva información al archivo `virtusertable.db`, ejecute `makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable` como root. Esto creará un nuevo `virtusertable.db` que contiene la nueva configuración.

6.3 Cambios comunes de configuración

Un archivo predeterminado `sendmail.cf` será instalado en `/etc`. La configuración por defecto debería funcionar en la mayoría de los sitios SMTP. *No* funcionará en sitios UUCP (copia de UNIX a UNIX); necesitará generar un nuevo `sendmail.cf` si debe transferir correo con UUCP.

Nota

Aunque los servidores SMTP están soportados automáticamente, no es el caso de los servidores **IMAP** (Internet Message Access Protocol). Si su ISP prefiere un servidor IMAP a un servidor SMTP, debe instalar el paquete IMAP o recuperar su correo.

Si necesita generar un archivo nuevo `/etc/sendmail.cf` para configurar Sendmail, debería utilizar el macro procesador `m4`. Si alguna vez modifica `/etc/mail/sendmail.mc` para añadir funcionalmente Sendmail, haga una copia de segurid de su archivo actual `/etc/sendmail.cf`, genere uno nuevo ejecutando el comando `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf` y añadiendo cualquier cambio previo desde el archivo `/etc/sendmail.cf` del que hizo la copia de seguridad al nuevo. Tras la creación de un nuevo `/etc/sendmail.cf`, debería reiniciar Sendmail para llegar a su propósito. El modo más sencillo de hacerlo es tecleando el comando `/sbin/service sendmail restart` como root.

Por defecto, el macro procesador `m4` está instalado con Sendmail. El macro procesador `m4` viene incluido con el paquete `sendmail-cf`, que está instalado en `/usr/lib/sendmail-cf`.

Debería consultar el archivo `/usr/lib/sendmail-cf/README` antes de modificar cualquier archivo en los directorios bajo el directorio `/usr/lib/sendmail-cf`, ya que pueden afectar a la configuración de archivos `/etc/sendmail.cf` futuros.

¡No utilice Linuxconf para configurar Sendmail! El módulo `mailconf`, diseñado para modificar `/etc/sendmail.cf` más fácilmente, no funciona y contiene información antigua sobre los grupos de reglas usadas en la configuración de Sendmail.

Una configuración común Sendmail es la de tener una sola máquina que actue como una puerta de enlace de correo para todos las máquinas de su red. Por ejemplo, una compañía puede querer tener una máquina llamada `mail.bigcorp.com` que realice todo su correo. En esta máquina, simplemente se necesita añadir los nombres de máquinas para las cuales `mail.bigcorp.com` realizará el correo para `/etc/mail/local-host-names`. Aquí tiene un ejemplo:

```
# sendmail.cw - incluye todos los aliases para su máquina
# here.
torgo.bigcorp.com
poodle.bigcorp.com
devel.bigcorp.com
```

En las otras máquinas, `torgo`, `poodle` y `devel`, es necesario modificar `/etc/sendmail.cf` para enmascarar como `mail.bigcorp.com` al enviar un email y al adelantar cualquier correo local procesándose en `bigcorp.com`. Encuentre las líneas `DH` y `DM` en `/etc/sendmail.cf` y modifíquelas como:

```
# who I send unqualified names to
# (null means deliver locally)
DRmail.bigcorp.com

# who gets all local email traffic
DHmail.bigcorp.com

# who I masquerade as (null for no masquerading)
DMbigcorp.com
```

Con este tipo de configuración, todos los mails enviados apareceran como si fueran enviados desde `bigcorp.com` y cualquier correor enviado a`torgo.bigcorp.com` o a los otros hosts será enviado a `mail.bigcorp.com`.

Si configura su sistema para enmascararlo como otro, cualquier email enviado de su sistema a su sistema será enviado a la máquina de la que está enmascarando. Por ejemplo, en la ilustración superior, se registran los archivos que periódicamente se envían a `root@poodle.bigcorp.com`.

6.4 Detener Spam

El **spam** de correo electrónico se puede definir como el correo innecesario y no deseado que se recibe un usuario que probablemte no conoce al remitente ni ha pedido esa información. Es costoso, perjudicial y abusa de los estándares de comunicación de Internet.

Afortunadamente, para Sendmail es relativamente fácil bloquear las nuevas técnicas de publicidad no deseada que se emplean para enviar correo basura. Bloquea incluso muchos de los métodos más comunes de spam por defecto, de manera que necesitaría activarlos conscientemente cambiando su archivo `/etc/mail/sendmail.cf` de una manera particular para que su sistema sea susceptible.

Por ejemplo, el envío de mensajes SMTP, también conocido como **transferencia de SMTP**, ha sido deshabilitado por defecto desde esta versión de Sendmail. Antes de que esto ocurra, Sendmail le indicará a su host de correo (`x.org`) que acepte mensajes desde partícipe (`y.com`) y que los envíe a un partícipe diferente (`z.net`). Sin embargo, tiene que especificar Sendmail para permitir a un dominio transmitir correo a través de su dominio. Modifique `/etc/mail/relay-domains` y reinicie Sendmail tecleando el comando `/sbin/service sendmail restart` como root para activar los cambios.

Muchas veces, sus usuarios pueden ser bombardeados de spam desde otros servidores a través de Internet bajo su control. En estos casos, puede ver las características de control de Sendmail disponibles a través del archivo `/etc/mail/access`. Como root, añada simplemente los dominios que le gustaría bloquear o permitir el acceso, tales como:

```
badspammer.com       550 Go away and don't spam us anymore
tux.badspammer.com   OK
10.0                 RELAY
```

Ya que `/etc/mail/access` es una base de datos, necesita usar makemap para activar sus cambios recreando el mapa de la base de datos. Esto se soluciona fácilmente al ejecutar el comando `makemap hash /etc/mail/access < /etc/mail/access` como root.

Este ejemplo muestra que cualquier email enviado desde `badspammer.com` a usted se bloquearía con el código de error 550 RFC 821 y el mensaje se reenvía al remitente, excepto los emails enviados desde el sub-dominio `tux.badspammer.com`, que serían aceptados. La úlitma línea muestra que cualquier email enviado desde la red 10.0.*.* puede transmitirse a través de su servidor de correo.

Como es de esperar, este ejemplo es sólo una muestra de lo que Sendmail puede hacer a la hora de permitir o bloquear el acceso. Consulte `/usr/share/doc/sendmail/README.cf` para más información y ejemplos.

6.5 Uso de Sendmail con LDAP

Como ya se ha visto en el Capítulo 4, *Lightweight Directory Access Protocol (LDAP)*, el (LDAP) es un método rápido y potente de encontrar información específica sobre un usuario particular desde un grupo mucho más amplio. Por ejemplo, podría usar un servidor LDAP para buscar una dirección de email particular desde un directorio común por el apellido de un usuario. En esta clase de implementación, LDAP difiere bastante de Sendmail, con LDAP se almacena la información jerárquica del usuario y a Sendmail sólo le viene dado el resultado de las consultas LDAP en los mensajes de email con dirección previa.

No obstante, Sendmail soporta una integración mayor con LDAP, ya que lo usa para sustituir archivos mantenidos por separado, tales como `aliases` y `virtusertables`, en diferentes servidores de correo que trabajan juntos para soportar una organización a nivel de empresa media. Es decir, puede

utilizar LDAP para abstraer el nivel del ruteado del correo desde Sendmail y los archivos de configuración a un grupo LDAP potente que influye en Sendmail por otras muchas aplicaciones.

La versión actual de Sendmail contiene el soporte para LDAP. Para extender su servidor Sendmail mediante el uso de LDAP, obtenga un servidor LDAP, como OpenLDAP, debidamente configurado. Necesitará modificar su `/etc/mail/sendmail.mc` para incluir:

```
LDAPROUTE_DOMAIN('yourdomain.com')dnl
FEATURE('ldap_routing')dnl
```

Nota

Esto sirve sólo para una configuración básica de Sendmail con LDAP. Su configuración debería diferir de ésta dependiendo de la implementación de LDAP, especialmente si desea configurar varias máquinas Sendmail para usar un servidor común LDAP.

Consulte `/usr/share/doc/sendmail/README.cf` para más información y ejemplos sobre el ruteado de LDAP.

A continuación, vuelva a crear su archivo `/etc/sendmail.cf` ejecutando `m4` y reiniciando Sendmail. Consulte la Sección 6.3, *Cambios comunes de configuración* para más información.

Para información ulterior sobre LDAP, consulte Capítulo 4, *Lightweight Directory Access Protocol (LDAP)*.

6.6 Recursos adicionales

Muchos usuarios encuentran inicialmente Sendmail difícil de configurar, en primer lugar debido al amplio número de opciones disponibles. El acceso a la documentación adicional de Sendmail puede serle muy útil, especialmente las opciones de configuración.

6.6.1 Documentación instalada

Las mejores fuentes de información sorbre cómo configurar Sendmail están incluidas en los paquetes `sendmail` y `sendmail-cf`.

- `/usr/share/doc/sendmail/README.cf` — contiene información sobre `m4`, localizaciones de archivos para Sendmail, mailers soportados, el modo de acceder a características avanzadas y mucho más
- `/usr/share/doc/sendmail/README` — contiene información sobre la estructura del directorio Sendmail, el soporte del protocolo IDENT, detalles en los permisos del directorio y los problemas más comunes que estos permisos pueden causar si se desconfiguran.

6.6.2 Sitios Web útiles

- http://www.sendmail.net — noticias, entrevistas y artículos referentes a Sendmail, que ofrecen una visión amplia de muchas opciones disponibles.
- http://www.sendmail.org — ofrece una completa interrupción técnica de las características y ejemplos de configuración de Sendmail.

6.6.3 Libros relacionados

- *Sendmail* de Bryan Costales con Eric Allman et al; O'Reilly & Associates — una buena referencia de Sendmail escrita con la ayuda del creador original de Delivermail y Sendmail.

Parte II La seguridad

7 Elementos básicos de seguridad de Red Hat

Además de la instalación y configuración apropiadas de su sistema Red Hat Linux, es de extrema importancia que asegure el sistema a un nivel aceptable de riesgo según su papel, importancia, y uso previsto. La seguridad es un tema increíblemente complejo que tiene que enfrentarse constantemente tanto a problemas emergentes como a problemas potenciales.

Dada su naturaleza amorfa e complicada, muchos administradores de sistemas y usuarios cometen el error de ocuparse de problemas pequeños y aislados mientras permiten que cuestiones mucho más grandes y peligrosas queden sin resolver. La verdadera seguridad de un sistema va más allá de la instalación de la actualización más reciente, la configuración de un cierto fichero, o la cuidadosa administración del acceso de los usuarios a los recursos de sistema. Es una manera de ver las diferentes amenazas que acechan su sistema y lo que está dispuesto a hacer para evitarlas.

Ningún sistema es totalmente seguro a menos que esté apagado (y aún así, es posible que se lo roben). Cada vez que el sistema esté encendido puede ser atacado, desde una broma inocua a un virus capaz de destruir el hardware, a la posibilidad que los datos sean borrados. Pero no todo está perdido. Con una actitud apropiada además de algunas buenas herramientas, podrá gozar de un sistema sano sin problema alguno de seguridad. Las siguientes secciones fueron ideadas para perfilar una manera para tratar el tema de la seguridad de sistema y amenazas potenciales un contexto bajo el cual hay que tomar en consideración varias herramientas de seguridad, costos y beneficios cuando ejecuta Red Hat Linux.

7.1 El dilema de seguridad inevitable

Todo usuario de cualquier sistema operativo se enfrenta a un dilema en común al construir un paradigma de seguridad para su sistema. Por un lado, intenta evitar hacer el sistema tan seguro que nada en él funcionará correctamente. Pero por otro lado, también trata de evitar dejar el sistema tan inseguro que cualquiera podría (y lo haría seguramente) hacerle lo que se le antoje, incluido borrar el trabajo de otros o cosas mucho peores.

No existe una manera exacta para resolver este dilema. Algunos sistemas, ya sea por la naturaleza de su utilidad o la importancia de los datos que protegen, caen por un lado del dilema mientras que otros sistemas, ya sea por la amplia variedad de usuarios que los utilizan o el hecho de ser máquinas de prueba, caen por el otro lado.

La cosa más importante que puede hacer al configurar la seguridad de su sistema es determinar dónde en la gama del dilema de seguridad se encuentra su sistema. Esto puede llevarse a cabo por su política de compañía. O es un investigador con un sistema que nunca conecta a redes públicas, y nadie aparte de usted tiene acceso físico a la máquina, o usted es un usuario que se conecta desde su casa a una

conexión de banda ancha y (con toda razón) esté preocupado por las maneras en que algunos usuarios mal intencionados muy lejos de donde está usted podrían arreglárselas para dañar sus datos.

Prescindiendo de las innumerables posibles situaciones que lo definan, usted tiene la responsabilidad de establecer su exposición adecuada al riesgo contra las metas que su sistema debe alcanzar. Luego, una vez que lo defina, use este conocimiento como guía a seguir para configurar y mantener las pautas de seguridad en su sistema.

7.2 Enfoque activo contra pasivo

Los enfoques relativos a la seguridad se pueden siempre separar en dos tipos diferentes: **activo** o **pasivo**. Un enfoque **activo** hacia la seguridad cubre todas las actividades ideadas para prevenir que se abra una brecha en el modelo de seguridad de su sistema. Un enfoque **pasivo** hacia la seguridad se refiere a las actividades desempeñadas para supervisar la seguridad de su sistema basándose en ese modelo de seguridad.

Todos los usuarios deberían emplear enfoques ya sea activos como pasivos hacia la seguridad. Cada uno de estos enfoques refuerza el otro. El hecho que sepa por medio de los registros de servidor que un determinado usuario está intentando violar su seguridad (enfoque pasivo hacia la seguridad) podría impulsarle a instalar una aplicación que los bloquee hasta para que obtengan un indicador de inicio de sesión (enfoque activo hacia la seguridad). De la misma manera, el hecho de usted no esté utilizando contraseñas shadow para proteger su sistema (activo) podría impulsarle a fijarse detenidamente por si hay cambios en los ficheros más importantes en su sistema utilizando una herramienta como Tripwire (pasivo). (Para obtener más información sobre Tripwire, consulte el Capítulo 10, *Instalación y configuración de Tripwire*.)

Red Hat Linux contiene una variedad de herramientas que le ayudará a emplear ambos enfoques hacia la seguridad. Sin embargo, el uso apropiado de los métodos con cada enfoque es esencial para prevenir un exceso de dependencia de herramientas que protejan su sistema.

7.2.1 Herramientas y métodos para un enfoque activo hacia la seguridad

La gran mayoría de las herramientas de seguridad para Red Hat Linux trabajan para proteger activamente su sistema. Estas son algunas de las más comunes y útiles herramientas de open source:

- *Utilidades Shadow* — Una colección de herramientas a norma industrial para administrar usuarios locales y grupos en un sistema que utiliza contraseñas encriptadas.
- *Kerberos 5* — Un sistema seguro que proporciona servicios de autentificación de redes. No permite que contraseñas de texto común pasen sobre una red para obtener acceso a los servicios. (Vea el Capítulo 9, *Uso de Kerberos 5 en Red Hat Linux* para obtener más información sobre Kerberos 5.)

- *OpenSSL* — Le ayuda a proteger una amplia gama de servicios que soportan operaciones sobre una capa de encriptación. (Vea la *Official Red Hat Linux Customization Guide* para obtener más información sobre OpenSSL.)
- *OpenSSH* — Un conjunto de utilidades que puede fácilmente sustituir herramientas omnipresentes pero inseguras como `telnet` y `ftp` con las potentes y seguras `ssh` y `scp`. (Vea la *Official Red Hat Linux Customization Guide* para obtener más información sobre OpenSSH.)

Los siguientes son métodos que soportan el enfoque activo hacia la seguridad:

- *Limitar el número de usuarios que pueden ejecutar comandos como root* — Ya sea intencionalmente que accidentalmente, un gran porcentaje de los problemas de seguridad surge al menos indirectamente de alguien que conoce la contraseña de root o a quien ha sido dado permiso por medio de `sudo` para ejecutar un comando en el ámbito de root.
- *Saber qué paquetes de software se han instalado en su sistema y permanecer alerta para detectar brechas de seguridad recientemente descubiertas* — No sabrá qué paquetes hay que supervisar si no es consciente de cuáles están instalados en su sistema y no sabrá que hay que actualizarlos a menos que supervise las fuentes de información, como Red Hat Network.
- *Limitar los servicios que se ejecutan en el sistema sólo a aquellos que en realidad necesita* — Fundamentalmente, mientras más programas se ejecuten, más posibilidades hay que se quebranten o proporcionen el acceso no autorizado. Conserve los recursos del sistema (y de este modo ahórrese la molestia de mantener cosas que no utiliza) y desinstale paquetes que no usa. Como mínimo ejecute una herramienta como `ntsysv` para evitar que servicios innecesarios inicien con el sistema a la hora del arranque. (Consulte el *Control de acceso a los servicios* en la *Official Red Hat Linux Customization Guide*.)
- *Requerir que los usuarios creen contraseñas seguras y cambiarlas a menudo* — La mayoría de los problemas de seguridad empiezan con el acceso no autorizado al sistema. Este riesgo puede minimizarse imponiendo a sus usuarios que también ellos practiquen métodos de seguridad activos protegiendo las claves que abren su puerta.
- *Asegurarse que los permisos de fichero no estén abiertos sin que esto sea necesario* — la mayoría de los ficheros no deberían ser escribibles.

7.2.2 Herramientas y métodos para un enfoque pasivo hacia la seguridad

Mientras la mayoría de las herramientas de seguridad para Red Hat Linux fueron ideadas para un enfoque activo hacia la seguridad, hay algunas herramientas que ayudan a que la seguridad pasiva sea una carga administrativa mucho menos pesada:

- *Tripwire* — una aplicación ideada para dar la alerta si directorios y ficheros de sistema específicos son modificados. De esta manera por lo menos sabrá si hay usuarios no autorizados que están teniendo acceso a su sistema o si usuarios autorizados están haciendo cambios indeseados a ficheros importantes. (Consulte el Capítulo 10, *Instalación y configuración de Tripwire* para obtener más información sobre Tripwire.)
- *COPS* — una colección de herramientas de seguridad ideadas para desempeñar una cantidad de cosas diferentes, desde el control de puertos abiertos en un determinado host a estar atento a contraseñas de usuario incorrectas.

Otros métodos que soportan el enfoque pasivo hacia la seguridad son:

- *Convertir en una rutina la actividad de supervisión de los registros de sistema* — Por omisión, Red Hat Linux atrapa una cantidad enorme de datos útiles en los registros de sistema situados en el directorio `/var/log`, especialmente en el fichero `messages`. Una tarea sencilla ejecutada como root, como el comando `grep "session opened for user root" /var/log/messages | less`, le permite desempeñar una potente revisión parcial de su sistema y supervisar quién está en el sistema a la root. Esto le permitiría, por ejemplo, reducir rápidamente el número de posibles usuarios que podrían haber cambiado un determinado fichero que se puede sólo escribir como root, simplemente comparando la hora en que el fichero en cuestión fue cambiado con la hora de los inicios de sesión en el fichero `/var/log/messages`. Sin embargo, considere que este no es un método a prueba de fallos, porque alguien con el poder de escritura sobre un fichero de sistema importante también podría tener el derecho de modificar el fichero `/var/log/messages` para borrar su rastro.

7.3 El desarrollo de políticas de seguridad

Todo sistema, desde una máquina usada sólo por una persona a un servidor en el ámbito empresarial utilizado por miles de usuarios, debería tener políticas de seguridad. Las políticas de seguridad son un conjunto de pautas utilizadas para medir si una determinada actividad o aplicación debiese o no ser desempeñada o utilizada en un sistema, basándose en los particulares objetivos para ese sistema.

Las políticas de seguridad entre sistemas diferentes pueden variar mucho, pero la cosa más importante es que exista una para su sistema no importa si está escrita en el manual de políticas de la empresa o simplemente se recuerda.

Cualquier política de seguridad debería estar construida con estas características como pautas:

- *Que sea sencilla en vez de compleja* — mientras más sencilla y clara la política de seguridad, más fácil será que las pautas sean respetadas y el sistema permanezca seguro.
- *Que sea fácil de mantener en vez de difícil* — como todo, los métodos y herramientas de seguridad pueden cambiar dependiendo de necesidades y retos nuevos. Su política de seguridad debería

construirse con un enfoque hacia la minimización del impacto que los cambios tendrán en su sistema y en sus usuarios.

- *La promoción de la libertad a través de la confianza en la integridad del sistema en vez de una sofocante utilización de sistema* — evite métodos y herramientas de seguridad que limiten innecesariamente la utilidad de su sistema cuando esté haciendo más seguro el sistema. Los métodos y herramientas de seguridad de calidad son casi siempre una ventaja segura y ofrecen más elecciones a los usuarios cada vez que sea posible.
- *El reconocimiento de la falibilidad en vez de una falsa sensación de seguridad* — una de las maneras más exitosas de atraer un problema de seguridad es a través de la creencia que su sistema no podría tener un problema como ese. En vez de dormirse en los laureles, hay que estar siempre alerta.
- *El enfoque debería estar en los problemas reales en vez de en problemas teóricos* — Emplee su tiempo y esfuerzo ocupándose de los problemas reales más grandes y luego prosiga con los menores. Dé la prioridad de sus esfuerzos a los problemas mayores y resuélvalos cuanto antes. Para ayudarle a determinar contra qué debería estar alerta principalmente, considere consultar http://www.sans.org/topten.htm o sitios web parecidos que dan descripciones detalladas de problemas de seguridad que constituyen una verdadera amenaza y exactamente qué hay que hacer para eliminarlos.
- *La inmediatez en vez de la desidia* — resuelva los problemas como vayan surgiendo y determine que equivalen a un riesgo. No piense que es posible ocuparse del problema más tarde. En realidad no hay mejor momento que ahora mismo, especialmente cuando se trata de una amenaza a la incolumidad de su sistema.

Si considera que su política de seguridad es tan restrictiva que no permite que el sistema sea usado en el modo en que fue destinada, entonces podría pensar en modificar la política lo suficiente como para aflojar el acceso al sistema. De la misma manera, si considera que la seguridad de su sistema está continuamente bajo amenaza, debería cambiar algunos aspectos de su política de seguridad para limitar el acceso. Lo más importante es que recuerde que una política de seguridad no es una idea o un documento estático. Debe ser modificado según cambien las necesidades de los objetivos de su sistema y de sus usuarios. Revise continuamente su política de seguridad actual para que refleje los requisitos reales.

7.4 Más allá de la protección del root

Muchos usuarios ponen la mayoría de sus esfuerzos de seguridad en limitar el número de usuarios que puedan obtener acceso de root a su sistema. Esto es obviamente una cosa muy buena y un primer paso importante, pero se debe hacer mucho más para mantener seguro un sistema. Hay que recalcar que la seguridad es sólo una parte de la cuestión de estabilidad de sistema. Las cuestiones de seguridad a menudo se entrelazan con las cuestiones más grandes que tienen que ver con la estabilidad y un

sistema exitoso equilibra las herramientas y métodos usados para la protección de seguridad con un conocimiento de maneras alternativas en que tal daño puede ser infligido.

Antes que nada, si su sistema es usado por muchos usuarios y esos usuarios cambian, asegúrese de borrar las cuentas de los usuarios antiguos inmediatamente después de que esas cuentas dejen de usarse. Mejor aún, desarrolle una lista clara y concisa de lo que se debe hacer cuando ya no se utiliza una cuenta de usuario o de grupo.

Limite el acceso físico a su sistema. Si tiene ficheros valiosos en su sistema seguro, alguien que esté tratando de tener acceso a ellos podría encontrar su tarea facilitada si pueden robar la unidad de disco duro para luego intentar entrar con calma. Las cosas se podrían complicar para un agresor si no se le permite estar al tanto de los aspectos físicos de la máquina que desean manipular.

Ante todo piense más allá de las maneras más elementales de sobrepasar sus métodos de seguridad. Considere que no hay que proteger un posible modo de acceso al sistema sólo para dejar libre otro camino mucho más frágil. Por supuesto que la manera en que se ocupa de esto depende de usted o de las necesidades de sus usuarios. Sólo asegúrese de no poner demasiado énfasis en una sola manera en que su sistema puede ser atacado.

7.5 La importancia de las contraseñas seguras

Las contraseñas son las llaves de su sistema. Está de más decir que deberían ser lo más seguras posibles para evitar inicios de sesión no autorizados, que es el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para amortizar un ataque es un paso decisivo y a la vez sencillo que le ahorrará muchos problemas en el futuro.

Muchas contraseñas utilizadas por usuarios son bastante fáciles de adivinar. Red Hat Linux proporciona una cantidad de maneras diferentes de proveer autentificación al sistema, incluyendo contraseñas encriptadas con el comando `crypt`, las contraseñas shadow (tratadas detalladamente en la Sección 12.1, *Utilidades Shadow*), Kerberos 5 y más. En cualquier situación en la cual se elija una contraseña como parte de un esquema de autentificación, la seguridad de ese esquema estará por lo menos parcialmente a la merced de la complejidad de la contraseña elegida.

¿Porqué elegir siempre contraseñas seguras difíciles de adivinar? En fin, los precios del hardware de informática siguen disminuyendo mientras que la cantidad de herramientas y métodos de calidad y a libre disposición para descifrar contraseñas continúa a aumentar. Por la manera en que las contraseñas se guardan en muchos de los esquemas de autentificación, si un atacante obtiene acceso al fichero que contiene las contraseñas de los usuarios de su sistema, normalmente logra adivinar uno de ellos en un lapso de tiempo relativamente corto probando las contraseñas encriptadas frente una lista de palabras de diccionario. Mientras los esquemas de autenticación están conscientes de este tipo de ataque e intentan varios métodos para que sean menos plausibles, ninguno de estos métodos es a prueba de fallas. Así es que debería ponerle atención al tipo de contraseña que elige y qué tan a menudo la cambia, especialmente cuando se trata de cuentas de root.

Una buena contraseña debe tener las siguientes cualidades:

- *Tener por lo menos ocho caracteres* — mientras más breve sea una contraseña, generalmente es más fácil descifrarla.
- *Estar hecha de caracteres, números y símbolos* — los números y los símbolos escondidos entre las letras (o viceversa) alargan el posible número de opciones para un dado carácter, cosa que refuerza la contraseña en sí.
- *Ser única* — elija contraseñas diferentes de otras contraseñas que tal vez esté usando. Si todas sus contraseñas son iguales o muy parecidas, la magnitud de un fallo de seguridad puede ser mayor.

Debería evitar contraseñas que

- *sean palabras que se encuentran en el diccionario* — si usa palabras de diccionario como contraseñas, está contribuyendo a que su sistema de seguridad falle. No lo haga, y no ignore los esquemas de autentificación que no le permiten el uso de palabras de diccionario para permitir que sus usuarios lo hagan.
- *tengan que ver con sus datos personales* — si usa contraseñas como la fecha de su cumpleaños, el nombre de su esposo/a, o la marca de su coche, está sólo buscando problemas. Piense en todas las contraseñas que usa y determine si alguien que usted conoce podría adivinarlas. Si hay aunque sea una mínima posibilidad de que puedan hacerlo, no use esa contraseña.
- *no pueda ser escrita rápidamente* — si su contraseña es tan complicada que deber buscar los caracteres cada vez que tiene que teclearla, ojos indiscretos podrían fácilmente observar sus dedos y adivinar la contraseña. Practique por lo menos teclear su contraseña cuando esté solo para aumentar la velocidad en que la teclea.

7.6 Seguridad de redes

Si usa su sistema Red Hat Linux en una red (como una red de área local, red de área amplia o Internet), deberá ser consciente de que su sistema estará a un nivel más alto de riesgo que si no estuviese conectado a una red. Además de atentados brutales a los ficheros de contraseñas y usuarios sin acceso apropiado, la presencia de su sistema en una red más grande aumenta la oportunidad de que ocurra un problema de seguridad y la forma posible en que pueda ocurrir.

Se ha creado en Red Hat Linux una cierta cantidad de medidas de seguridad de red, y muchas herramientas de seguridad open source también están incluidas con la distribución básica. Sin embargo, a pesar de su estado de preparación, pueden ocurrir problemas de seguridad de red, debidos parcialmente a su topología de red o a una docena de otros factores. Para ayudarle a determinar la fuente y método de un problema de seguridad de red, tome en cuenta las maneras más verosímiles en que podría ocurrir:

- *Búsqueda entre los datos de autenticación* — muchos métodos de autenticación por defecto en Linux y en otros sistemas operativos dependen de enviarle su información de autentificación "en

abierto" donde su nombre de usuario y contraseña se le envían por medio de la red en texto común o sin encriptar. Existen herramientas a disposición para quienes tengan accesos a su red(o Internet, si obtiene acceso a su sistema mientras la usa) para "husmear" o detectar su contraseña grabando todos los datos transferidos por medio de la red y examinarlos para encontrar declaraciones de inicios de sesión comunes. Este método se puede usar para encontrar *cualquier* información enviada sin encriptar, hasta su contraseña de root. Es esencial que utilice herramientas como Kerberos 5 y OpenSSH para evitar que contraseñas y otros datos delicados se envíen sin encriptación. Si por cualquier motivo no es posible utilizar estas herramientas con su sistema, entonces asegúrese de no iniciar nunca sesiones como root a menos que no esté presente delante de la consola.

- *Ataque frontal* — ataques de denegación de servicio (DoS) y su tipo pueden dañar hasta un sistema seguro inundándolo con peticiones inapropiadas o mal formuladas que aplastarían su sistema o crearían procesos que pondrían en peligro su sistema o sus datos, además de otros sistemas que comuniquen con él. Existe una cantidad de protecciones diferentes a disposición para ayudar a detener el ataque y minimizar el daño, como los firewalls que filtran los paquetes. Sin embargo, los ataques frontales se encaran con una mirada exhaustiva a las maneras en que los sistemas no fiables se comunican con sus sistemas fiables, erigiendo barreras protectoras entre los dos y desarrollando una manera de reaccionar velozmente ante cualquier evento para que la irrupción y los posibles daños sean limitados.
- *Aprovechándose de un bug de seguridad o de un loophole (rendija)* — de vez en cuando se encuentran errores en el software que, si son explotados, podrían causar graves daños a un sistema no protegido. Por este motivo trate de ejecutar procedimientos desde el root lo menos posible. Use todas las herramientas que estén a su disposición, como Red Hat Network, para actualizaciones de paquete y alertas de seguridad, para resolver problemas de seguridad tan pronto como sean descubiertos. Por último, asegúrese que su sistema no tenga programas innecesarios que inicien a la hora del arranque. Mientras menos programas se ejecuten, menos probabilidades hay que un bug o error de seguridad le afecte.

7.7 Recursos suplementarios

La información sobre la seguridad está constantemente cambiando, y algunos sitios web proveen una manera conveniente de obtener las noticias más recientes. Para estar siempre al día con los más recientes avisos de seguridad o para saber más sobre varias cuestiones de seguridad relacionadas con Red Hat Linux, visite a menudo los sitios web de Linux y los de seguridad en general. Además, si necesita ayuda para construir una política de seguridad sólida para las necesidades específicas de su sistema, use un buen libro sobre la seguridad para que le dé ideas.

7.7.1 Sitios web útiles

- http://www.redhat.com/support/errata — Vaya a la sección de soporte del sitio web de Red Hat para obtener las asesorías de seguridad emitidas y las actualizaciones publicadas para cada versión de Red Hat Linux por Red Hat.
- http://www.cert.org — El sitio web de CERT ofrece una lista actualizada de incidentes y vulneralibilidades de seguridad de gran impacto, además de información detallada sobre cada aviso de seguridad y sobre cómo restablecer un sistema después de que haya sido comprometido.
- http://www.sans.org — El sitio web del Instituto de Seguridad, Redes y Administración de Sistemas (SANS) proporciona alertas de seguridad en forma de resumen, e incluye enlaces convenientes hacia RPMs actualizados (cuando están disponibles).
- http://www.linuxsecurity.com — El sitio web de Linux-Specific Security (Seguridad específica) tiene una colección de enlaces Linux relacionados con la seguridad, la documentación y mucho más.
- http://www.securityportal.com — El sitio web de Security Portal contiene una mezcla de noticias de seguridad recientes, reparaciones específicas para Linux, y documentos que explican cómo construir mejores modelos y políticas de seguridad.

7.7.2 Libros sobre el tema

- *Securing and Optimizing Linux: Red Hat Edition* (Asegurando y optimizando Linux: Edición Red Hat) de Gerhard Mourani; OpenNA — Este libro también se encuentra a su disposición a través del sitio http://www.openna.com como fichero PDF que se puede cargar gratuitamente.
- *Secrets & Lies* (Secretos y mentiras) de Bruce Schneier; John Wiley & Sons, Inc. — Un examen completo y pragmático de las más recientes cuestiones de seguridad informática.

8 Módulos de autentificación conectables (PAM)

Los programas que ofrecen privilegios a los usuarios deben autentificar (verificar la identidad de) adecuadamente cada usuario. Al iniciar una sesión en un sistema, el usuario proporciona su nombre de usuario y contraseña y el procedimiento de inicio de sesión usa el nombre de usuario y la contraseña para autentificar el inicio de sesión — para verificar que el usuario es quien dice ser. Son posibles otras formas de autentificación además de las contraseñas y las contraseñas se pueden almacenar en modos diferentes.

Los Pluggable Authentication Modules (PAM) son una manera de permitir que el administrador de sistema establezca una política de autentificación sin tener que recompilar programas de autentificación. Con PAM, se controla cómo determinados módulos de autentificación se conectan a un programa editando el fichero de configuración PAM de ese programa en `/etc/pam.d`.

La mayoría de los usuarios de Red Hat Linux nunca necesitarán modificar los ficheros de configuración de PAM para ninguno de sus programas. Cuando usa RPM para instalar programas que requieren autentificación, hacen automáticamente los cambios necesarios para llevar a cabo autentificaciones de contraseñas normales por medio de PAM. Sin embargo, si desea personalizar su configuración, deberá conocer la estructura de un fichero de configuración PAM. Hay más información a su disposición sobre el tema en la Sección 8.2.2, *Los módulos de PAM*.

8.1 Las ventajas de PAM

Cuando se usa correctamente, PAM provee muchas ventajas para un administrador de sistema, como las siguientes:

- Un esquema de autentificación común que se puede usar con una gran variedad de aplicaciones.
- PAM puede ser ejecutado con varias aplicaciones sin tener que recompilar las aplicaciones para soportar PAM específicamente.
- Gran flexibilidad y control sobre la autentificación para el administrador y para el desarrollador de aplicaciones.
- Los desarrolladores de aplicaciones no necesitan desarrollar su programa para usar un determinado esquema de autentificación. En su lugar, pueden concentrarse puramente en los detalles de su programa.

8.2 Ficheros de configuración PAM

El directorio `/etc/pam.d` contiene los ficheros de configuración de PAM. En versiones antiguas de PAM se utilizaba `/etc/pam.conf`. El fichero `pam.conf` todavía se lee si no se encuentran entradas `/etc/pam.d/`, pero se desaprueba su uso.

Cada aplicación (o *servicio*, como se conocen comúnmente las aplicaciones proyectadas para ser usadas por muchos usuarios) tiene su propio fichero. Cada fichero tiene cinco elementos diferentes: el **nombre de servicio** , el **tipo de módulo**, el **indicador de control** , la **ruta de módulo** y los **argumentos**.

8.2.1 Nombres de servicio de PAM

El nombre de servicio de todas las aplicaciones habilitadas para PAM es el nombre de su fichero de configuración en `/etc/pam.d`. Cada programa que usa PAM define su propio nombre de servicio.

Por ejemplo, el programa `login` define el nombre de servicio `login`, `ftpd` define el nombre de servicio `ftp`, etc.

Generalmente, el nombre de servicio es el nombre del programa usado para obtener *acceso* al servicio, no del programa usado para *proporcionar* el servicio.

8.2.2 Los módulos de PAM

PAM contiene cuatro tipos diferentes de módulos para controlar el acceso a determinados servicios:

- Los módulos `auth` proporcionan la autentificación en sí (tal vez pidiendo y controlando una contraseña) y establecen las credenciales, como la afiliación de grupo o los billetes de Kerberos.
- Los módulos `account` controlan que la autentificación sea permitida (que la cuenta no haya caducado, que el usuario tenga permiso de iniciar sesiones a esa hora del día, etc.).
- Los módulos `password` se usan para establecer contraseñas.
- Los módulos `session` se usan después de que un usuario ha sido autentificado. Los módulos `session` permiten que alguien use su cuenta (para armar el directorio de inicio del usuario o poner a disposición su buzón electrónico, por ejemplo).

Estos módulos se pueden *apilar*, o colocar uno sobre otro para que se puedan usar los módulos múltiples. El orden de una pila de módulos es muy importante en el procedimiento de autentificación, porque facilita mucho al trabajo del un administrador el requerir que existan varias condiciones antes de permitir que se lleve a cabo la autentificación del usuario.

Por ejemplo, `rlogin` normalmente usa por lo menos cuatro métodos de autentificación apilados, como se puede ver en su fichero de configuración PAM:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Antes de que a alguien se le permita llevar a cabo el `rlogin`, PAM verifica que el fichero `/etc/nologin` no exista, que no esté intentando iniciar una sesión en modo remoto como root y que se pueda cargar cualquier variable de entorno. Entonces se lleva a cabo una autentificación `rhosts` exitosa antes que se permita la conexión. Si falla la autentificación `rhosts`, entonces se lleva a cabo una autentificación de contraseña estándar.

Se pueden añadir módulos PAM nuevos en cualquier momento y después se pueden crear aplicaciones que se puedan usar con los módulos de PAM. Si por ejemplo usted crea un método de creación de contraseñas para usarse una sola vez y escribe un módulo PAM que lo soporte, los programas conscientes de PAM pueden usar el módulo nuevo y el método para contraseñas inmediatamente sin tener que ser recompilados o modificados. Como podrá imaginar, esto es muy positivo, porque le permite combinar y emparejar, además de probar, los métodos de autentificación muy rápidamente con programas diferentes sin tener que recompilar los programas.

La documentación sobre la escritura de módulos contenida en el sistema se encuentra en `/usr/share/doc/pam–<`*`version-number`*`>`.

8.2.3 Los indicadores de control PAM

Todos los módulos PAM generan un resultado de éxito o fracaso cuando se les hace un control. Los indicadores de control le dicen a PAM qué hacer con el resultado. Como los módulos pueden apilarse en un determinado orden, los indicadores de control le dan la posibilidad de fijar la importancia de un módulo con respecto a los módulos que lo siguen.

Una vez más, considere el fichero de configuración PAM `rlogin`:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Antes de que se especifique el tipo de módulo, los indicadores de control deciden la importancia con la que debería ser considerado ese determinado tipo de módulo en cuanto al propósito general de permitirle a ese usuario el acceso a ese programa.

El estándar PAM define cuatro tipos de indicadores de control:

- Los módulos `required` indicados deben ser controlados con éxito para que se permita la autentificación. Si fracasa el control de un módulo `required`, el usuario no recibirá un aviso hasta que no hayan sido controlados los demás módulos del mismo tipo.
- Los módulos `requisite` indicados también deben ser controlados con éxito para que la autentificación sea exitosa. Sin embargo, si fracasa un control de módulo `requisite`, el usuario recibe un aviso inmediatamente con un mensaje que refleja el primer módulo `required` *o* `requisite` fracasado.
- Si fracasan los controles a módulos `sufficient` indicados, se ignoran. Pero si un módulo `sufficient` indicado pasa el control con éxito y ningún módulo `required` indicado antes de ese ha fracasado, entonces ningún otro módulo de este tipo se controlará y este tipo de módulo será considerado como controlado exitosamente por entero.
- los módulos `optional` indicados no son esenciales para el éxito o fracaso general de la autentificación para ese tipo de módulo. Desempeñan un papel sólo cuando ningún otro módulo de ese tipo ha tenido éxito o ha fallado. En este caso el éxito o fracaso de un módulo `optional` indicado determina la autentificación PAM general para ese tipo de módulo.

Ya está a disposición para PAM una sintaxis de indicador de control más nueva que permite más control. Consulte la documentación de PAM ubicada en `/usr/share/doc/pam—<`*`version-number`*`>` para obtener más información sobre esta sintaxis nueva.

8.2.4 Rutas de módulos PAM

Las rutas de los módulos le indican a PAM dónde encontrar el módulo conectable que hay que usar con el tipo de módulo especificado. Generalmente, se proporciona como una ruta entera de módulo, como `/lib/security/pam_stack.so`. Sin embargo, si no se proporciona la ruta entera (o sea que la ruta no inicia con `/`), entonces se supone que el módulo indicado está en `/lib/security`, la ubicación por defecto para los módulos PAM.

8.2.5 Argumentos PAM

PAM utiliza argumentos para transmitir información a un módulo conectable durante la autentificación para ese determinado tipo de módulo. Estos argumentos permiten que los ficheros de configuración PAM para determinados programas utilicen un módulo PAM común pero en maneras diferentes.

Por ejemplo, el módulo `pam_userdb.so` utiliza los secretos almacenados en un fichero Berkeley DB para autentificar al usuario. (Berkeley DB es un sistema de base de datos de open source proyectado para ser incrustado en muchas aplicaciones para rastrear determinados tipos de información.) El módulo toma un argumento `db`, especificando el nombre de fichero Berkeley DB que hay que usar, el cual puede variar según el servicio.

La línea `pam_userdb.so` en un fichero de configuración PAM sería más o menos así:

```
auth      required  /lib/security/pam_userdb.so db=path/to/file
```

Los argumentos inválidos se ignoran y no afectan en ningún modo el éxito o fracaso del módulo PAM. Cuando pasa un argumento inválido, el error normalmente se escribe en `/var/log/messages`. Sin embargo, como el método de informe está controlado por el módulo PAM, depende del módulo registrar el error correctamente.

8.2.6 Muestras de ficheros de configuración PAM

Un fichero de muestra de configuración de la aplicación PAM tiene este aspecto:

```
#%PAM-1.0
auth      required  /lib/security/pam_securetty.so
auth      required  /lib/security/pam_unix.so shadow nullok
auth      required  /lib/security/pam_nologin.so
account   required  /lib/security/pam_unix.so
password  required  /lib/security/pam_cracklib.so
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
session   required  /lib/security/pam_unix.so
```

La primera línea es un comentario (cualquier línea que inicie con el carácter # es un comentario). Las líneas dos, tres y cuatro apilan tres módulos a usar para autentificaciones de inicio de sesión.

```
auth      required  /lib/security/pam_securetty.so
```

La segunda línea se asegura de *si* el usuario está intentando el registro como root, el tty en el que se están registrando está listado en el fichero `/etc/securetty`, *si* éste existe.

```
auth      required  /lib/security/pam_unix.so shadow nullok
```

La línea tres causa que se le pida la contraseña al usuario y que la contraseña sea controlada.

```
auth      required  /lib/security/pam_nologin.so
```

La línea cuatro controla si existe el fichero `/etc/nologin`. Si `/etc/nologin` existe y el usuario no es de root, la autentificación falla.

Note que se controlan los tres módulos `auth`, *no importa si falla el primer módulo* `auth`. Esta estrategia no permite que el usuario se dé cuenta de por qué no se ha permitido su autentificación. Si se sabe por qué falla una autentificación tal vez al próximo intento será más fácil pase la autentificación.

Este comportamiento se puede modificar cambiando `required` a `requisite`. Si fracasa cualquier módulo `requisite` PAM falla inmediatamente sin llamar ningún otro módulo.

```
account   required  /lib/security/pam_unix.so
```

La quinta línea hace que se efectúe cualquier verificación de cuenta que fuese necesaria. Si por ejemplo se han habilitado contraseñas shadow, el módulo `pam_unix.so` controlará si la cuenta ha caducado o si el usuario no ha cambiado su contraseña dentro del plazo permitido.

```
password  required  /lib/security/pam_cracklib.so
```

La quinta línea prueba la contraseña recién cambiada controlando si la contraseña puede ser fácilmente descubierta por un programa de descubrimiento de contraseñas basado en diccionarios.

```
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
```

La séptima línea especifica que si el programa `login` cambia la contraseña del usuario, debería utilizar el módulo `pam_unix.so` para hacerlo. (Esto sucederá sólo si un módulo `auth` ha determinado que debe cambiarse la contraseña — en el caso que haya caducado una contraseña shadow, por ejemplo.)

```
session   required  /lib/security/pam_unix.so
```

La octava y final línea especifica que el módulo `pam_unix.so` debería usarse para administrar la sesión. Actualmente ese módulo no hace nada; podría ser reemplazado por cualquier módulo necesario o suplementado por medio de una pila.

Note que el orden en que están las líneas dentro de cada fichero tiene importancia. Mientras el orden en que los módulos `required` van llamados no tiene mucha importancia, hay otros indicadores de control a disposición. Mientras `optional` se utiliza raramente, `sufficient` y `requisite` hacen que el orden tenga importancia.

Como siguiente ejemplo repasaremos la configuración `auth` para el `rlogin`:

```
#%PAM-1.0
auth      required    /lib/security/pam_nologin.so
auth      required    /lib/security/pam_securetty.so
auth      required    /lib/security/pam_env.so
auth      sufficient  /lib/security/pam_rhosts_auth.so
auth      required    /lib/security/pam_stack.so service=system-auth
```

Primero, `pam_nologin.so` controla para ver si `/etc/nologin` existe. Si existe, nadie puede iniciar una sesión excepto a nivel de root.

```
auth      required    /lib/security/pam_securetty.so
```

Segundo, `pam_securetty.so` no permite que los inicios de sesión a nivel de root ocurran en terminales inseguras. Esto rechaza eficazmente cualquier intento de `rlogin` a nivel de root. Si desea

permitirles (en tal caso debería encontrarse detrás de un buen cortafuego o no estar conectado a Internet) hacer esto, consulte la Sección 8.4, *El uso de `rlogin`, `rsh`, y `rexec` con PAM*.

```
auth       required     /lib/security/pam_env.so
```

Tercero, el módulo `pam_env.so` carga las variables de entorno especificadas en `/etc/security/pam_env.conf`.

```
auth       sufficient   /lib/security/pam_rhosts_auth.so
```

Cuarto, se `pam_rhosts_auth.so` autentifica al usuario por medio de `.rhosts` en el directorio de inicio del usuario, PAM inmediatamente autentifica el `rlogin` sin proseguir con una autentificación de contraseña normal con `pam_stack.so`. Si `pam_rhosts_auth.so` no logra autenticar al usuario, se ignora esa autentificación fracasada.

```
auth       required     /lib/security/pam_stack.so service=system-auth
```

Quinto, si `pam_rhosts_auth.so` no ha logrado autentificar al usuario, el módulo `pam_stack.so` ejecuta una autentificación de contraseña normal y se pasa al `service=system-auth` argumento.

Nota

Si no desea que se pida la contraseña cuando el control `securetty` fracasa y determina que el usuario está intentando iniciar una sesión a nivel de root en modo remoto, puede cambiar el módulo `pam_securetty.so` de `required` a `requisite`. Como alternativa, si desea permitir inicios de sesión a nivel de root remotos (que no es muy buena idea), puede convertir esta línea en comentario.

8.3 Contraseñas shadow

Si está empleando contraseñas shadow, `pam_unix.so` automáticamente detectará que se están usando y las usará para autenticar usuarios.

Consulte Sección 12.1, *Utilidades Shadow* para obtener más información sobre contraseñas shadow.

8.4 El uso de `rlogin`, `rsh`, y `rexec` con PAM

Por motivos de seguridad `rexec`, `rsh`, y `rlogin` no están habilitados por defecto en Red Hat Linux 7.1. Debería utilizar el grupo de programas de herramientas OpenSSH en su lugar. Información sobre las herramientas OpenSSH se encuentra en el Capítulo 11, *Protocolo SSH* y en la *Official Red Hat Linux Customization Guide*.

Si debe utilizar `rexec`, `rsh`, y `rlogin` y si necesita usarlos a nivel de root, necesitará efectuar algunas modificaciones al fichero `/etc/securetty`. Las tres herramientas tienen ficheros de configuración PAM que requieren el módulo PAM `pam_securetty.so`, así que debe modificar `/etc/securetty` para permitir el acceso a nivel de root por via remota.

Antes de iniciar una sesión a nivel de root utilizando estas herramientas, primero debe configurarlas adecuadamente. Primero instale RPM `rsh-server` incluido con Red Hat Linux 7.1. Consulte *Official Red Hat Linux Customization Guide* si necesita ayuda para el uso de RPM.

Luego ejecute `ntsysv` y habilite `rexec`, `rsh` y `rlogin`. Consulte la página de manual `ntsysv` si necesita ayuda para usar esta herramienta.

Por último, reinicie `xinetd` con `/sbin/service xinetd restart` para activar los cambios en `ntsysv`. Ahora todos los usuarios excepto root podrán usar `rexec`, `rsh` y `rlogin`.

Para permitir que root utilice estas herramientas, añada los nombres de las herramientas que desea permitir a `/etc/securetty`. Si deseaba habilitar el inicio de sesión a nivel de root con `rexec`, `rsh` y `rlogin`, añada las siguientes líneas a `/etc/securetty`:

```
rexec
rsh
rlogin
```

Para permitir que root inicie una sesión usando estas herramientas por `telnet` (una idea todavía peor pero necesaria en algunos entornos), añada algunas líneas más:

```
pts/0
pts/1
```

8.5 Otros recursos

Hay mucha más información sobre PAM a disposición de la que cubre este capítulo. Existen varias fuentes de información de gran valor para ayudarle a configurar y utilizar PAM en su sistema.

8.5.1 Documentación instalada

- páginas de manual `pam` — buena información introductoria sobre PAM, incluyendo la estructura y propósito de los ficheros de configuración PAM.
- `/usr/share/doc/pam–<version-number>` — contiene excelente documentación en HTML sobre PAM, además de la *Guía para administradores de sistema*, un *Manual para escritores de módulos* y un *Manual para desarrolladores de aplicaciones* . También contiene una copia del estándar PAM, DCE-RFC 86.0.

8.5.2 Sitios web útiles

- http://www.kernel.org/pub/linux/libs/pam — el sitio web principal de distribución para el proyecto Linux-PAM, contiene información sobre varios módulos y aplicaciones PAM actualmente en uso o en fase de desarrollo, un FAQ, y documentación PAM suplemental.

Además de estos recursos recomendamos que lea la mayor cantidad de ejemplos de fichero de configuración posible cuando empiece a trabajar con PAM. Muchos sitios web ofrecen ejemplos de código, ya sea para administradores que desean cambiar los ficheros de configuración predeterminados que para desarrolladores de aplicaciones que desean utilizar PAM con sus programas.

9 Uso de Kerberos 5 en Red Hat Linux

Kerberos es un sistema de seguridad para realizar servicios de autentificación en la red. La autentificación significa:

- La verificación de la identidad de las entidades en la red.
- El tráfico en la red es de la fuente que lo ha enviado.

Kerberos usa contraseñas para verificar la identificación de los usuarios, pero estas contraseñas siempre se envían encriptadas a través de la red.

9.1 ¿Por qué usar Kerberos?

La mayoría de las redes usan esquemas de autentificación basados en contraseñas. Cuando un usuario necesita una autentificación de un servicio ejecutado en un servidor de red, su contraseña es escrita para cada servicio que requiere autentificación. Su contraseña es enviada a través de la red y el servidor verifica su identidad mediante el uso de la contraseña.

La transmisión de contraseñas en texto sin retocar mediante el uso de este método, aunque hecho a menudo, representa un riesgo de seguridad tremendo. Cualquier chiflado del sistema con acceso a la red y un analizador de paquetes que puede interceptar cualquier contraseña enviada de este modo.

El primer objetivo de Kerberos es el de asegurar que las contraseñas *nunca* sean enviadas desencriptadas a través de la red. Un uso correcto Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en su red.

9.2 ¿Por qué no usar Kerberos?

Kerberos elimina una amenaza de seguridad común. ¿Por qué no se usa en todas las redes? Por varias razones, kerberos puede ser difícil de implementar:

- No existe ninguna solución rápida para migrar contraseñas de usuarios desde una base de datos de contraseñas UNIX (tales como `/etc/passwd` o `/etc/shadow`) a una base de datos de contrseñas Kerberos. La migración es técnicamente posible, pero es un tema que se escapa del dominio de este capítulo. Para decidir si una migración de contraseñas tiene sentido en su intalación Kerberos, vea las FAQ de Kerberos >Question 2.23 o la información relativa en la Sección 9.8, *Recursos adicionales* para una información más detallada.
- Kerberos es sólo compatible prácticamente con los Pluggable Authentication Modules (PAM) usados por la mayoría de los servidores en Red Hat Linux. Para más información vea la Sección 9.7, *Kerberos y Pluggable Authentication Modules (PAM)*.

- Para una aplicación use Kerberos, el código debe ser modificado para hacer las llamadas apropiadas a las librerías de Kerberos. Para algunas aplicaciones, esto puede suponer un esfuerzo excesivo de programación. Para otras aplicaciones, los cambios se deben realizar en el protocolo usado entre el servidor de red y sus clientes; de nuevo, esto puede suponer una programación excesiva. Además, resultará imposible hacer que ciertas aplicaciones closed-source funcionen con Kerberos.
- Kerberos presupone que usted está utilizando hosts fiables en una red no fiable. Su primer objetivo es el de prevenir que las contraseñas de texto sin retocar sean enviadas a través de la red. Sin embargo, si cualquier otro a parte del usuario adecuado tiene acceso físico a cualquiera de los hosts, especialmente el que emite tickets usados para la autentificación, todo sistema de autentificación de Kerberos corre el riesgo de transigir.
- Finalmente, si decide usar Kerberos en su red, debe darse cuenta de que es una elección de todo o nada. Si *alguno* de los servicios que transmite las contraseñas de texto sin retocar permanece en uso, las contraseñas pueden todavía estar comprometidas y su red no se beneficiará del uso de Kerberos. Para asegurar su red con Kerberos, debe **kerberizar** (hacer trabajar con Kerberos) *todas* las aplicaciones que mandan las contraseñas en texto sin retocar o parar el uso de esta aplicaciones en la red.

9.3 Terminología Kerberos

Como algunos otros sistemas, Kerberos tiene su propia terminología. Aquí hay una lista de términos que necesitará para estar familiarizado:

caché credencial o archivo de tickets

Un fichero que contiene las claves para encriptar las comunicaciones entre el usurario y varios servicios de red. Kerberos 5 proporciona un framework para usar otros tipos de caché (como la memoria compartida), pero los archivos están mejor soportados.

Centro de distribución de claves (KDC)

Un servicio que emite tickets Kerberos, que habitualmente se ejecutan en el mismo host como un Ticket Granting Server.

clave

Datos usados para encriptar o desencriptar otros datos. Los datos encriptados no pueden ser desencriptados sin una clave correcta.

cliente

Una entidad en la red (un usuario, un host o una aplicación) que puede obtener un ticket desde Kerberos

dominio

Red que usa Kerberos, compuesto de uno o varios servidores (también conocidos como KDCs) y un número potencial de clientes.

keytab

Un fichero que incluye una lista desencriptada de "principals" y sus claves. Los servidores recuperan las claves que necesitan del fichero keytab en lugar de usar `kinit`. `/etc/krb5.keytab` es el fichero keytab por defecto. El comando `kadmind` es el único servicio que usa cualquier otro archivo (`/var/kerberos/krb5kdc/kadm5.keytab`)

principal

Usuario o servicio que puede autentificar mediante el uso de Kerberos. Un nombre de principal está en el formato "*root*[/*instance*]*@REALM*". Para un usuario típico, el *root* es igual a su ID de login. El *instance* es opcional. Si el principal tiene un instance, se separa del root con ("/"). Una cadena vacia ("") es un instance válido (que difiere del instance por defecto *NULL*), pero usarlo puede ser confuso. Todos los principals de un dominio tienen su propia clave, que se deriva de su contraseña (para usuarios) o aleatoriamente (para servicios)

servicio

Programa u ordenador al que se accede en la red.

texto cifrado

datos encriptados

texto sin retocar

Datos no encriptados.

ticket

Grupo temporal de credenciales electrónicas que verifica la identidad de un cliente para un servicio particular.

Ticket Granting Service (TGS)

Emite tickets para un servicio deseado que usa el usuario para ganar acceso al servicio. El TGS se ejecuta en el mismo host que KDC.

Ticket Granting Ticket (TGT)

Ticket especial que permite al cliente obtener tickets adicionales sin aplicarlos desde KDC.

9.4 Modo en que funciona Kerberos

Ahora que ya conoce algunos de los términos que utiliza Kerberos, aquí tiene una explicación del funcionamiento del sistema de autentificación Kerberos:

En una red "normal" que usa contraseñas para autentificar usuarios, cuando un usuario demanda un servicio de la red que requiere autentificación, el usuario tiene que teclear su contraseña. Su contraseña es trasmitida en texto sin retocar y se concede el acceso a un servicio de la red.

El principal problema para Kerberos consiste en cómo usar contraseñas para autentificarlas sin enviarlas a la red. En una red kerberizada, la base de datos de Kerberos contiene su claves (para los usuarios, sus claves derivan de sus contraseñas). La base de datos Kerberos también contiene claves para todos los servicios de la red.

Cuando un usuario en una red kerberizada se registra en su estación de trabajo, su principal se envía al Key Distribution Center (KDC) como una demanda para un Ticket Granting Ticket (TGT). Esta demanda puede ser enviada por el programa login (para que sea transparente al usuario) o puede ser enviada por el programa `kinit` después de que el usuario se registre.

El KDC verifica el principal en su base de datos. Si lo encuentra, el KDC crea un TGT, lo encripta usando las claves del usuario y lo devuelve al usuario.

El programa login o `kinit` desencripta el TGP usando las claves del usuario. El TGT, que caduca después de un cierto período de tiempo, es almacenado en su caché de credenciales. Sólo se puede usar un cierto períiodo de tiempo que suele ser de ocho horas (a diferencia de una contraseña comprometida, que puede ser usada hasta que se cambie). El usuario no tiene que introducir su contraseña otra vez hasta que el TGT caduca o se desconecta y vuelve a conectarse.

Cuando el usuario necesita acceder a un servicio de red, el cliente usa el TGT para pedir un ticket para el servicio de Ticket Granting Service (TGS), que se ejecuta en el KDC. El TGS emite un ticket por el servicio deseado, que se usa para autentificar el usuario.

Como es de suponer la explicación es demasiado simplificada. Si necesita una explicación más detallada sobre el funcionamiento de kerberos, vea la Sección 9.8, *Recursos adicionales*.

Nota

Kerberos depende de ciertos servicios de la red para trabajar correctamente. Primero, Kerberos necesita una sicronización de reloj entre los ordenadores y su red. Si no ha configurado un programa de sincronización de reloj para su red, deberá hacerlo. Ya que ciertos aspectos de kerberos se apoyan en el Domain Name System (DNS), debe de asegurarse de que las entradas DNS y los hosts en su red están configuradas correctamente. Vea la *Guía del administrador kerberos V5*, proporcionada en formatos PostScript y HTML, en `/usr/share/doc/krb5-server-`*`versionnumber`*`/`, si necesita más información sobre estos temas.

9.5 Configuración de un servidor Kerberos 5 en Red Hat Linux 7.1

Cuando configure Kerberos, instale primero el servidor(es) en primer lugar . Si necesita servidores esclavos, encontrará los detalles de la configuración entre el servidor maestro y el esclavo en la *Guía de instalación de Kerberos 5* (en el directorio `/usr/share/doc/krb5-server-`*`versionnumber/`*).

Para instalar un servidor Kerberos:

1. Asegúrese de que tiene una sincronización de reloj y DNS funcionando en su servidor antes de instalar Kerberos 5. Ponga especial atención a la sincronización del tiempo entre el servidor Kerberos y sus diversos clientes. Si los relojes de servidor y cliente difieren más de 5 minutos (esta cantidad por defecto puede ser configurada en Kerberos 5), a los clientes Kerberos no les será posible autentificarse en el servidor. Esta sincronización de reloj es necesaria para evitar que un agresor use un atentificador antiguo para hacerse pasar por un usuario válido.

   Debería configurar un Network Time Protocol (NTP) compatible con una red cliente/servidor usando Red Hat Linux, aunque no utilice Kerberos. Red Hat Linux 7.1 incluye el paquete `ntp` para una instalación fácil. Vaya a http://www.eecis.udel.edu/~ntp para información adicional sobre NTP.

2. Instale los paquetes `krb5-libs`, `krb5-server` y `krb5-workstation` en el ordenador que ejecutará su KDC. Este ordenador debe ser seguro — si es posible, no debería ejecutar ningún servicio aparte de KDC.

   Si quiere usar la utilidad Graphical User Interface (GUI) para administrar Kerberos, debería instalar también el paquete `gnome-kerberos`. `gnome-kerberos` contiene `krb5`, una herramienta GUI para administrar tickets y `gkadmin`, una herramienta GUI para administrar dominios Kerberos.

3. Modifique los ficheros de configuración `/etc/krb5.conf` y `/var/kerberos/krb5kdc/kdc.conf` para reflejar su nombre de entorno y sus mapas de entorno a dominio. Un entorno sencillo puede ser construido para reemplazar instances de *EXAMPLE.COM* y *example.com* con su nombre del dominio (asegúrese de mantener los nombres en mayúsculas y minúsculas en el formato correcto) y cambiando el KDC desde *kerberos.example.com* por el nombre de su servidor Kerberos. Por convenio, todos los nombres de entornos son en mayúsculas y todos los nombres de host DNS y nombres de dominios son en minúsculas. Para más detalles sobre el formato de estos ficheros, lea las páginas de manual correspondientes.

4. Cree la base de datos usando la utilidad `kdb5_util` desde el intérprete de comandos de la shell:

   ```
   /usr/kerberos/sbin/kdb5_util create -s
   ```

El comando `create` crea la base de datos que será usada para guardar las claves de su entornos Kerberos. La opción `-s` fuerza la creación de un fichero **stash** en el que se guarda la clave del servidor maestro. Si no existe ningún fichero stash del que leer la clave, el servidor Kerberos (`krb5kdc`) pedirá al usuario la contraseña del servidor maestro (que puede ser usada para regenerar la clave) cada vez que inicie.

5. Modifique el fichero `/var/kerberos/krb5kdc/kadm5.acl`. `kadmind` usa este fichero para determinar qué principals tienen acceso a la base de datos Kerberos y su nivel de acceso. La mayoría de las organizaciones podrán estar en una sola línea:

```
*/admin@EXAMPLE.COM  *
```

La mayoría de usuarios están representados en la base de datos por un sólo principal (con un *NULL*, o vacío, instance, como *joe@EXAMPLE.COM*). Con esta configuración, los usuarios con un segundo principal con un instance de *admin* (por ejemplo, *joe/admin@EXAMPLE.COM*) podrán ejercer un dominio completo sobre la base de datos del entorno Kerberos.

Una vez que `kadmind` esté iniciado en un servidor, algunos usuarios podrán acceder a sus servicios ejecutando `kadmin` o `gkadmin` en cualquiera de los clientes o servidores en el entorno. Sin embargo, sólo los usuarios listados en el fichero `kadm5.acl` podrán modificar la base de datos de cualquier modo,excepto para cambiar sus propias contraseñas.

Nota

La utilidades `kadmin` y `gkadmin` comunican con el servidor `kadmind` sobre la red. Naturalmente, necesita crear el primer principal antes de que pueda conectarse al servidor sobre la red para administarlo. Cree el primer principal con el comando `kadmin.local`, que está especialmente diseñado en el mismo host que el KDC y no usa Kerberos para la autentificación.

Teclee el siguiente comando `kadmin.local` en el terminal KDC para crear el primer principal:

```
/usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
```

6. Inicie Kerberos utilizando los siguientes comandos:

```
/sbin/service krb5kdc start
/sbin/service kadmin start
/sbin/service krb524 start
```

7. Añada principals para sus usuarios utilizando el comando `addprinc` con `kadmin` o usando la opción del menú **Principal** => **Añadir** en `gkadmin`. `kadmin` (y `kadmin.local` en el maestro KCD) es una interfaz de línea de comandos para el sistema de administración de Kerberos. Como

tales, muchos comandos están disponibles tras la puesta en marcha del programa `kadmin`. Vea la página de manual `kadmin` para más información.

8. Verifique que su servidor emite los tickets. En primer lugar, ejecute `kinit` para obtener un ticket y guardarlo en un fichero de caché credencial. A continuación use `klist` para ver la lista de credenciales en su caché y use `kdestroy` para destruir el caché y los credenciales que contiene.

Nota

Por defecto, `kinit` intenta autentificarle usando el nombre de login de usuario de la cuenta que ha usado cuando se registró en su sistema por primera vez (no en el servidor Kerberos) . Si el nombre de usuario del sistema no corresponde con una base de datos principal de Kerberos, obtendrá un mensaje de error. Si esto sucede, dé a `kinit` el nombre de su principal como un argumento en la línea de comandos (`kinit` *`principal`*).

Una vez que se hayan completado los pasos anteriores, su servidor Kerberos debería estar funcionando. A continuación, necesitará configurar sus clientes Kerberos.

9.6 Configuración de un cliente Kerberos 5 en Red Hat Linux 7.1

Configurar un cliente Kerberos 5 es menos complicado que configurar un servidor. Necesitará instalar los paquetes de clientes y proveer a sus clientes con un fichero de configuración válido `krb5.conf`. Las versiones Kerberizadas de `rsh` y `rlogin` también requieren algunos cambios en la configuración.

1. Asegúrese de que la sincronización del tiempo se encuentra entre el cliente de Kerberos y KDC. Consulte la Sección 9.5, *Configuración de un servidor Kerberos 5 en Red Hat Linux 7.1* para más información. DNS debería funcionar correctamente en el cliente Kerberos antes de instalar los porgramas de cliente Kerberos.

2. Instale los paquetes `krb5-libs` y `krb5-workstation` en todos los clientes de su entorno. Deberá proporcionar su versión de `/etc/krb5.conf` para sus estaciones de trabajo de clientes; normalmente esto puede ser el mismo `krb5.conf` usado por el KDC.

3. Antes de que una estación de trabajo de su entorno en particular pueda permitir a los usuarios conectar `rsh` y `rlogin`, la estación de trabajo necesitará tener instalado el paquete `xinetd` y tener su propio host principal en la base de datos Kerberos. Los programas de servidor `kshd` y `klogind` también necesitan las claves para el principal de sus servicios.

El uso de `kadmin`, añade un host principal para la estación de trabajo. El instance en este caso será el nombre del host de la estación de trabajo. Para no tener que teclear nunca más la contraseña para este principal, puede usar la opción `-randkey` para el comando `addprinc` de kadmin, creando el principal y asignándole una clave aleatoria.

```
addprinc -randkey host/blah.example.com
```

Ahora que ha creado el principal, puede extraer las claves para la estación de trabajo mediante la ejecución de `kadmin` *en la propia estación de trabajo* y el uso del comando `ktadd` en `kadmin`:

```
ktadd -k /etc/krb5.keytab host/blah.example.com
```

Para usar las versiones kerberizadas de `rsh` y `rlogin`, deberá habilitar `klogin`, `eklogin` y `kshell`, realizado habitualmente mediante el uso de `ntsysv` o `chkconfig`.

4. Es necesario iniciar otros servicios de red kerberizados. Para usar `telnet` kerberizado, debe habilitar `krb5-telnet`. Use los programas `ntsysv` o `chkconfig` para configurar el servicio `krb5-telnet` para iniciar su sistema.

   Para proporcionar acceso FTP, cree y extraiga una clave para un principal con un root de ftp y el instance fijado para el nombre del host del servidor FTP. Use `ntsysv` o `chkconfig` para habilitar `gssftp`.

   El servidor IMAP incluido en el paquete `imap` usará la autentificación GSS-API usando Kerberos 5 si encuentra la clave correcta en `/etc/krb5.keytab`. El root para el principal será imap. El gserver CVS usa un principal con un root de `cvs` y es por otra parte idéntico a un `pserver`. pserver.

Con esto debería bastar para hacer que se configure un entorno Kerberos sencillo.

9.7 Kerberos y Pluggable Authentication Modules (PAM)

Actualmente, los servicios Kerberizados no hacen uso de PAM — un servidor kerberizado omite PAM completamente. Las aplicaciones que usan PAM pueden hacer uso de Kerberos para comprobar las contraseñas si el módulo `pam_krb5`pam_krb5 module (proporcionado en el `pam_krb5`) es instalado. El paquete `pam_krb5` contiene un ejemplo de ficheros de configuración que permiten servicios como `login` y `gdm` para autentificar usuarios y obtener credenciales iniciales usando sus contraseñas. Si el acceso a servicios de red siempre se realiza mediante servicios kerberizados (o servicios que usan GSS-API, como IMAP), la red puede ser considerada razonablemente segura.

Los administradores de sistemas cuidadosos no añaden verificación de contraseñas Kerberos a los servicios de la red, porque la mayoría de los protocolos usados por estos servicios no encriptan la contraseña antes de enviarla a través de la red — obviamente esto es algo a evitar.

9.8 Recursos adicionales

Kerberos representa un desafío para los nuevos usuarios a la hora de entenderlo, implementarlo y configurarlo. Remítase a las siguientes fuentes de información, si desea tener más ejemplos e instrucciones sobre el uso de Kerberos:

9.8.1 Documentación instalada

- `/usr/share/doc/krb5-server-<version-number>` — La *Guía de instalación de Kerberos V5* y la *Guía del administrador del sistema Kerberos V5*, en formato PostScript y HTML formats, instalados por el RPM `krb5-server`.
- `/usr/share/doc/krb5-workstation-<version-number>` — La *Guía del usuario UNIX de Kerberos V5*, en formato PostScript y HTML, instalada por el RPM `krb5-workstation`.

9.8.2 Sitios Web útiles

- http://web.mit.edu/kerberos/www — Página inicial de Kerberos en el sito Web MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — Preguntas más frecuentes sobre Kerberos (FAQ).
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Enlace a una versión PostScript de *Kerberos: An Authentication Service for Open Network Systems* de Jennifer G. Steiner, Clifford Neuman y Jeffrey I. Schiller. Documento original que describe Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* originariamente de Bill Bryant en 1988, modificado por Theodore Ts'o en 1997. Este documento es una conversación entre dos diseñadores que están pensando la creación de un sistema de autentificación Kerberos. El estilo desenfadado de esta conversación lo convierte en un buen material para aquéllos que no tienen ningún tipo de familiaridad con Kerberos.
- http://www.ornl.gov/~jar/HowToKerb.html — Consejo práctico para kerberizar su red.

10 Instalación y configuración de Tripwire

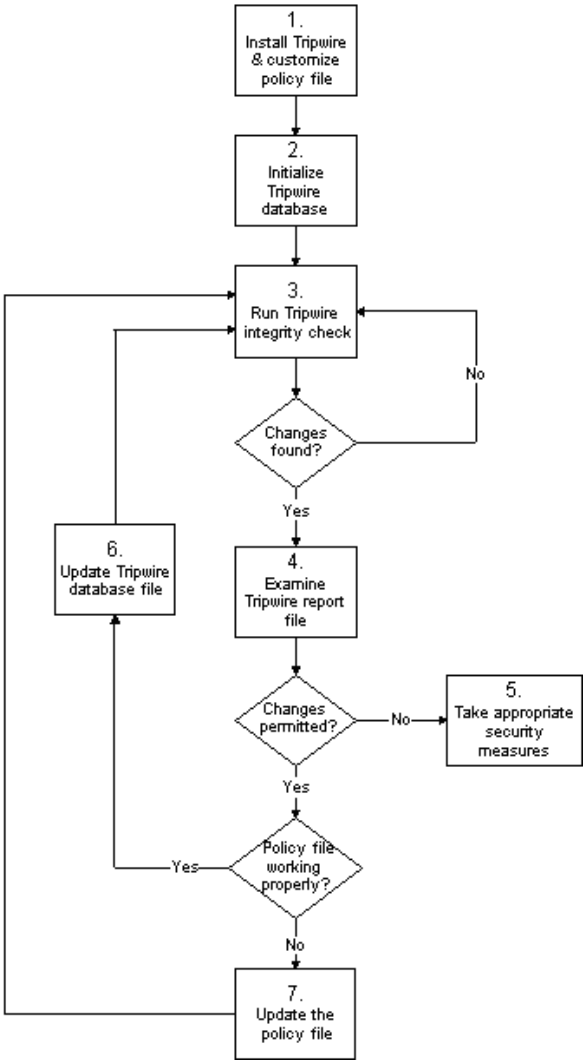
El software Tripwire puede ayudarle a asegurar la integridad de ficheros y directorios de sistema esenciales identificando todos los cambios hechos a ellos. Las opciones de configuración de Tripwire incluyen la capacidad de recibir alertas por medio de correo electrónico si hay ficheros específicos que han sido modificados y el control de integridad automatizado a través de un trabajo `cron`. El uso de Tripwire para detectar intrusiones y fijar daños le ayuda a mantenerlo al tanto de los cambios del sistema y puede agilizar el restablecimiento de una entrada forzada reduciendo el número de ficheros que hay que restablecer para reparar el sistema.

Tripwire compara los ficheros y directorios con una base de datos de la ubicación de los ficheros, las fechas en que han sido modificados y otros datos. Tripwire genera la base tomando una instantánea de ficheros y directorios específicos en estado conocido como seguro. (Para máxima seguridad, Tripwire debería ser instalado y la base debería ser creada antes que el sistema sea expuesto al riesgo de intrusión.) Después de haber creado la base de datos de base, Tripwire compara el sistema actual con la base y proporciona información sobre cualquier modificación, añadidura, o supresión.

10.1 Cómo usar Tripwire

El siguiente diagrama de flujo ilustra cómo debería usarse Tripwire:

Gráfico 10–1 Cómo usar Tripwire



Los pasos a tomar para instalar, usar y mantener Tripwire adecuadamente son los siguientes:

1. *Instale Tripwire y personalice el fichero de política* — si no lo ha hecho ya, instale el RPM de `tripwire` (vea la Sección 10.2.1, *Instrucciones para la instalación de RPM*). Luego personalice la configuración de muestra (`/etc/tripwire/twcfg.txt`) y los ficheros de política (`/etc/tripwire/twpol.txt`) y ejecute la secuencia de comandos (`/etc/tripwire/twinstall.sh`). Consulte la Sección 10.2.2, *Instrucciones de post-instalación* para obtener más información.

2. *Inicialice la base de datos de Tripwire* — construya una base de datos de los ficheros de sistema esenciales para supervisarlos basándose en el contenido del fichero de política Tripwire nuevo y firmado (`/etc/tripwire/tw.pol`). Consulte la Sección 10.7, *Inicialización de la base de datos* para obtener más información.

3. *Ejecute un control de integridad Tripwire* — compare la base de datos Tripwire recién creada con los ficheros de sistema reales en busca de ficheros modificados o desaparecidos. Consulte la Sección 10.8, *Ejecución de un control de integridad* para obtener más información.

4. *Examine el fichero de informes Tripwire* — Examine el fichero de informes Tripwire con `twprint` para distinguir las violaciones a la integridad. Consulte la Sección 10.9, *Impresión de informes* para obtener más información.

5. *Tome las medidas de seguridad adecuadas* — si los ficheros bajo supervisión han sido modificados en modo inadecuado, los puede reemplazar con los originales salvados en copias de seguridad o reinstalar el programa.

6. *Actualice el fichero de la base de datos de Tripwire* — si las violaciones a la integridad son intencionales y válidas, como si usted hubiese intencionalmente modificado un fichero o reemplazado un determinado programa, debería avisarle al fichero de base de datos de Tripwire que no lo indique como violación en informes futuros. Consulte la Sección 10.10, *Actualización de la base de datos después de un control de integridad* para obtener más información.

7. *Actualice el fichero de política Tripwire* — si necesita cambiar la lista de ficheros que Tripwire supervisa, o la manera en que trata las violaciones a la integridad, debería actualizar su fichero de muestra de política (`/etc/tripwire/twpol.txt`), regenerar una copia firmada (`/etc/tripwire/tw.pol`), y actualizar su base de datos de Tripwire. Consulte Sección 10.11, *Actualización del fichero de política* para obtener más información.

Consulte las secciones adecuadas en este capítulo para obtener instrucciones detalladas sobre estos pasos.

10.2 Instrucciones de instalación

Una vez instalado, Tripwire debe además ser correctamente inicializado para poder mantener una supervisión cuidadosa de sus ficheros. Estas secciones proporcionan detalles sobre cómo instalar el

programa, si no está ya presente en su sistema y luego cómo inicializar posteriormente la base de datos de Tripwire.

10.2.1 Instrucciones para la instalación de RPM

La forma más fácil de instalar Tripwire es instalando el RPM de `tripwire` durante el procedimiento de instalación de Red Hat Linux 7.1. Sin embargo, si ya había instalado Red Hat Linux 7.1, puede usar RPM, Gnome-RPM, o Kpackage para instalar el RPM de Tripwire con los CD-ROMs de Red Hat Linux 7.1. Los siguientes pasos perfilan este procedimiento con el uso de RPM:

1. Localice el directorio `RedHat/RPMS` en el CD-ROM de Red Hat Linux 7.1.
2. Localice el RPM binario de `tripwire` tecleando `ls -l tripwire*` en el directorio `RedHat/RPMS`.
3. Teclee `rpm -Uvh <name>` (donde `<name>` es el nombre del RPM de Tripwire que se encuentra en el paso 2)
4. Después de haber instalado el RPM de `tripwire`, siga las instrucciones de post-instalación abajo.

Nota

Las notas de versión y el fichero `LIAME` se encuentran en `/usr/share/doc/tripwire-<version-number>`. Estos documentos contienen información importante sobre el fichero de política predeterminado y otras cuestiones.

10.2.2 Instrucciones de post-instalación

El RPM de `tripwire` instala los ficheros de programa necesarios para ejecutar el software. Después de haber instalado Tripwire, debe configurarlo para su sistema tal y como se describe en los siguientes pasos:

1. Si ya sabe de varios cambios que deberían efectuarse al fichero de configuración (`/etc/tripwire/twcfg.txt`) o al fichero de política (`/etc/tripwire/twpol.txt`), modifique ahora esos ficheros.

Nota

Como se tienen que modificar los ficheros de configuración y de política para personalizar Tripwire a su situación específica, para ello no es necesario usar Tripwire. Si tiene intenciones de modificar el fichero de configuración o el de política, deberá efectuar esos cambios antes de ejecutar la secuencia de comandos de configuración (`/etc/tripwire/twinstall.sh`). Si modifica el fichero de configuración o el de política después de haber ejecutado la secuencia de comandos de configuración, deberá volver a ejecutar la secuencia de comandos de configuración antes de inicializar el fichero de la base de datos. Recuerde que *puede* modificar los ficheros de configuración y de política *después* de inicializar el fichero de la base de datos y de haber ejecutado un control de integridad.

---

2. Teclee `/etc/tripwire/twinstall.sh` en la línea de comandos como root y pulse [Intro] para ejecutar la secuencia de comandos de configuración. La secuencia de comandos `twinstall.sh` le acompaña a través de los procedimientos para fijar frases de contraseña, generar las claves criptográficas que protegen los ficheros de configuración y de política de Tripwire, y firmar estos ficheros. Consulte laSección 10.6, *La selección de las frases de contraseña* para obtener más información sobre cómo fijar frases de contraseña.

Nota

Una vez cifrados y firmados, el fichero de configuración (`/etc/tripwire/tw.cfg`) y el de política (`/etc/tripwire/tw.pol`) generados al ejecutar la secuencia de comandos `/etc/tripwire/twinstall.sh` no deberían ser movidos ni se les debe cambiar de nombre.

---

3. Inicialice el fichero de la base de datos de Tripwire lanzando el comando `/usr/sbin/tripwire --init` desde la línea de comandos.

4. Ejecute el primer control de integridad comparando su base de datos de Tripwire nuevo con sus ficheros de sistema lanzando el comando `/usr/sbin/tripwire --check` desde la línea de comandos y buscando errores en el informe generado.

Una vez que termine estos pasos exitosamente, Tripwire tiene la instantánea de línea de base de su sistema de ficheros que necesita para revisar si hay cambios hechos a los ficheros esenciales.

Además, el RPM de `tripwire` añade un fichero llamado `tripwire-check` en el directorio `/etc/cron.daily` que ejecutará un control de integridad automáticamente una vez al día.

10.3 La ubicación de los ficheros

Antes de trabajar con Tripwire debería saber dónde se encuentran los ficheros que son importantes para la aplicación. Tripwire almacena sus ficheros en varios sitios según el papel que desempeñan:

- El directorio `/usr/sbin` almacena los programas `tripwire`, `twadmin` y `twprint`.
- El directorio `/etc/tripwire` contiene las claves locales y de sitio (`*.key` files) y la secuencia de comandos de inicialización (`twinstall.sh`), además de los ficheros de configuración y de política de muestra y reales.
- El directorio `/var/lib/tripwire` contiene la base de datos de Tripwire de los ficheros de su sistema (`*.twd`) y un directorio `report` donde se almacenan los informes de Tripwire. Los informes de Tripwire, llamados *`host_name-date_of_report-time_of_report`*`.twr`, proporcionan detalles de las diferencias entre la base de datos de Tripwire y sus ficheros de sistema reales.

10.4 Los componentes de Tripwire

El fichero de política de Tripwire es un fichero de texto que contiene comentarios, reglas, directivas y variables. Este fichero dicta la manera en que Tripwire controla su sistema. Cada regla en el fichero de política especifica un objeto de sistema que hay que supervisar. Las reglas también describen sobre qué cambios hay que informar y cuáles ignorar.

Los objetos de sistema son los ficheros y directorios que desea supervisar. Cada objeto se identifica con un nombre de objeto. Una propiedad se refiere a una sola característica de un objeto que el software Tripwire puede supervisar. Las directivas controlan el procesamiento condicional de conjuntos de reglas en un fichero de política. Durante la instalación, el fichero de política de texto (`/etc/tripwire/twpol.txt`) se cifra y se le da otro nombre, convirtiéndose así en un fichero de política activo (`/etc/tripwire/tw.pol`).

Cuando se acaba de inicializar, Tripwire usa las reglas del fichero de política firmado para crear el fichero de base de datos (`/var/lib/tripwire/`*`host_name`*`.twd`). El fichero de base de datos es una instantánea de línea de base del sistema en estado seguro conocido. Tripwire compara esta línea de base con el sistema actual para determinar los cambios que han ocurrido. A esta comparación se le llama **control de integridad**.

Tripwire produce ficheros de informe en el directorio `/var/lib/tripwire/report` cuando se ejecuta un control de integridad. Los ficheros de informe resumen cualquier cambio a los ficheros que haya violado las reglas del fichero de política durante el control de integridad.

El fichero de configuración de Tripwire (`/etc/tripwire/tw.cfg`) almacena información específica al sistema, como la ubicación de los ficheros de datos de Tripwire. Tripwire genera la información del fichero de configuración necesaria durante la instalación, pero el administrador del sistema puede cambiar los parámetros en el fichero de configuración en cualquier momento después de eso. Note que el fichero de configuración modificado debe de estar firmado de la misma manera que el fichero de política para que se pueda usar por defecto.

Las variables del fichero de configuración **POLFILE**, **DBFILE**, **REPORTFILE**, **SITEKEYFILE** y **LOCALKEYFILE** especifican la ubicación del fichero de política, el de base de datos, los de informe y los de clave local y de sitio. Estas variables se definen por defecto a la hora de la instalación. Si modifica el fichero de configuración y deja las variables sin definir, Tripwire considerará el fichero de configuración inválido. Esto causará un error en la ejecución de `tripwire`, haciendo que el programa salga del sistema.

Note que el fichero de configuración modificado debe ser firmado de la misma manera que el fichero de política para que Tripwire lo pueda usar. Consulte la Sección 10.11.1, *La firma del fichero de configuración* para obtener instrucciones sobre cómo firmar el fichero de configuración.

10.5 Modificación del fichero de política

Usted puede especificar cómo Tripwire debe controlar su sistema modificando el fichero de política de Tripwire (`twpol.txt`). La modificación del fichero de política adaptándolo a su determinado configuración de sistema aumenta la utilidad de los informes de Tripwire minimizando los alertas falsos por ficheros o programas que usted no está usando pero sobre los cuales Tripwire todavía está dando informes como modificados o desaparecidos.

Localice el fichero de política predeterminado en `/etc/tripwire/twpol.txt`. Hay un fichero de política de ejemplo (ubicado en `/usr/share/doc/tripwire-<version-number>/policyguide.txt`) incluido para ayudarle a aprender el lenguaje de política. Lea el fichero de política de ejemplo para obtener las instrucciones sobre cómo modificar el fichero de política predeterminado.

Si modifica el fichero de política inmediatamente después de haber instalado el paquete `tripwire`, no olvide teclear `/etc/tripwire/twinstall.sh` para ejecutar la secuencia de comandos de configuración. Esta secuencia de comandos firma el fichero de política modificado y le da otro nombre a `tw.pol`. Este es el fichero de política activo usado por el programa `tripwire` cuando se ejecuta.

Si modifica el fichero de política de muestra después de haber ejecutado la secuencia de comandos de configuración, consulte la Sección 10.11, *Actualización del fichero de política* para obtener las instrucciones sobre cómo firmarlo para que se convierta en el fichero `tw.pol` requerido.

Nota

Si modifica el fichero de política de muestra, Tripwire no lo utilizará hasta que sea firmado, cifrado y convertido en el fichero `/etc/tripwire/tw.pol` nuevo (vea Sección 10.11, *Actualización del fichero de política*).

10.6 La selección de las frases de contraseña

Los ficheros de Tripwire se firman o se cifran usando claves locales o de sitio que protegen los ficheros de configuración, de política, de la base de datos, y de los informes evitando que sean vistos o modificados por usuarios que no poseen las frases de contraseña de sitio o locales. Esto significa que aunque un intruso lograse obtener acceso cormo root a su sistema, no sería capaz de alterar los ficheros de Tripwire para borrar su propia pista a menos que también conozca las frases de contraseña. A la hora de seleccionar las frases de contraseña, debe usar por lo menos ocho caracteres alfanuméricos y simbólicos por cada frase de contraseña. El tamaño máximo de una frase de contraseña es de 1023 caracteres. No deberían usarse citas como caracteres de frases de contraseña. Además, asegúrese que sus frases de contraseña sean completamente diferentes de la contraseña de root para el sistema.

Debería asignar frases de contraseña únicas ya sea para la clave de sitio como para la clave local. La frase de contraseña de la clave de sitio protege la clave de sitio, la cual se usa para firmar los ficheros de configuración y de política de Tripwire. La clave local firma los ficheros de la base de datos y de los informes de Tripwire.

Almacene las frases de contraseña en una ubicación segura. *No hay manera de descifrar un fichero firmado si olvida su frase de contraseña.* Si olvida las frases de contraseña, los ficheros no se podrán utilizar y deberá ejecutar de nuevo la secuencia de comandos de configuración, que también reinicializa la base de datos de Tripwire.

10.7 Inicialización de la base de datos

Cuando Tripwire inicializa su base de datos, crea una colección de objetos de sistema de ficheros basada en las reglas en el fichero de política. Esta base de datos funciona como la línea base para controles de integridad.

Utilice el siguiente comando para inicializar la base de datos de Tripwire:

```
/usr/sbin/tripwire --init
```

Este comando puede tardar varios minutos en ejecutarse.

10.8 Ejecución de un control de integridad

Cuando ejecuta un control de integridad, Tripwire compara los objetos de sistema de ficheros actuales y reales con sus propiedades como han sido indicadas en su base de datos. Las violaciones se imprimen a una salida estándar y se guardan en un fichero de informe al cual se pueda tener acceso más tarde mediante `twprint`. Para obtener más información sobre la lectura de informes Tripwire, vea la Sección 10.9, *Impresión de informes*.

Una opción de configuración de correo electrónico en el fichero de política permite además que determinadas direcciones de correo electrónico reciban avisos cuando ocurren ciertas violaciones a la integridad. Consulte Sección 10.12, *Tripwire y el correo electrónico* para obtener instrucciones sobre cómo configurar esta opción.

Utilice el siguiente comando para ejecutar un control de integridad:

```
/usr/sbin/tripwire --check
```

Este comando requiere algo de tiempo para ejecutar en la mayoría de las situaciones, según el número de ficheros que hay que controlar.

10.9 Impresión de informes

El comando `twprint -m r` muestra el contenido de un informe Tripwire en texto sin cifrar. Usted debe decirle a `twprint` cuál informe poner en pantalla.

Un comando `twprint` para imprimir informes Tripwire sería semejante a lo siguiente (todo en una línea):

```
/usr/sbin/twprint -m r --twrfile
          /var/lib/tripwire/report/<name>.twr
```

La opción `-m r` en el comando le ordena a `twprint` que descifre el informe Tripwire. La opción `--twrfile` le ordena a `twprint` que use un fichero de informe Tripwire específico.

El nombre del informe Tripwire que desea ver contiene el nombre del host que Tripwire ha controlado para generar el informe, además de la fecha y hora de la creación. Usted puede consultar informes guardados previamente en cualquier momento. Simplemente teclee `ls /var/lib/tripwire/report` para ver una lista de informes Tripwire.

Los informes Tripwire pueden ser algo largos, según la cantidad de violaciones encontrada o los errores generados. Un informe de muestra empieza así:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================================
Report Summary:
===============================================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

10.9.1 El uso de `twprint` para ver la base de datos de Tripwire

También puede usar `twprint` para ver la base de datos entera o información sobre determinados ficheros en la base de datos Tripwire. Esto es útil para ver qué tanta información Tripwire está supervisando en su sistema.

Teclee este comando para ver la base de datos Tripwire entera:

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Este comando genera una gran cantidad de salida, con las primeras línea parecidas a esto:

```
Tripwire(R) 2.3.0 Database
```

```
Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
     Mode        UID          Size       Modify Time
     ------      ----------   ---------- ----------
 /
     drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXXX
 /bin
     drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
 /bin/arch
     -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
 /bin/ash
     -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
 /bin/ash.static
     -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Para ver información sobre un determinado fichero que Tripwire está supervisando, como `/etc/hosts`, teclee otro comando `twprint`:

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

El resultado será algo parecido a esto:

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
```

```
Object Type             Regular File
Device Number           773
Inode Number            216991
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

Consulte la página de manual de `twprint` para conocer otras opciones.

10.10 Actualización de la base de datos después de un control de integridad

Si ejecuta un control de integridad y Tripwire encuentra violaciones, primero habrá que determinar si las violaciones detectadas son realmente brechas en la seguridad o el producto de modificaciones autorizadas. Si ha instalado recientemente una aplicación o ha modificado ficheros de sistema esenciales, Tripwire le informará (debidamente) de violaciones a la integridad. En este caso debería actualizar su base de datos Tripwire para que esos cambios no vuelvan a aparecer en los informes como violaciones. Sin embargo, si se efectúan cambios no autorizados a ficheros de sistema, generando violaciones al control de integridad, entonces debería restablecer el fichero original de una copia de seguridad o reinstalar el programa.

Para actualizar su base de datos de Tripwire de modo que acepte las violaciones encontradas en un informe, debe especificar el informe que desea usar para actualizar su base de datos. Cuando inicie un comando para integrar esas violaciones válidas en su base de datos, asegúrese de usar el informe más reciente. Teclee el siguiente comando (todo en una línea), donde *name* es el nombre del informe que deber usarse:

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<name>.twr
```

Tripwire le mostrará el informe específico por medio del editor de textos predeterminado (especificado en el fichero de configuración Tripwire en la línea **EDITOR**). Esta es su oportunidad para quitar de la selección ficheros que no desea que se actualicen en la base de datos de Tripwire. Es importante que permita que sólo se cambien las violaciones autorizadas a la integridad en la base de datos.

Todas las actualizaciones propuestas a la base de datos de Tripwire inician con una `[x]` antes del nombre del fichero. Si desea excluir específicamente que una violación válida sea añadida a la base de datos de Tripwire, quite la `x` de la casilla. Para aceptar como cambio cualquier fichero con la `x` al lado, escriba el fichero en el editor y salga del editor de textos. Esto da la señal a Tripwire de modificar su base de datos y no incluir estos ficheros como violaciones en el informe.

Por ejemplo, el editor de texto predeterminado para Tripwire es `vi`. Para escribir un fichero con `vi` y efectuar los cambios a la base de datos de Tripwire cuando actualice con un informe específico, teclee

`:wq` en el modo de comando de `vi` y pulse [Intro]. Se le pedirá que teclee su frase de contraseña local. Posteriormente se escribirá un fichero nuevo de base de datos que incluya las violaciones válidas.

Después de que se haya escrita una nueva base de datos de Tripwire, las violaciones a la integridad recién integradas no volverán a aparecer como advertencias cuando se ejecute el siguiente control de integridad.

10.11 Actualización del fichero de política

Si en realidad desea modificar los ficheros que Tripwire escribe en su base de datos o modificar la severidad con la cual se informan las violaciones, necesita modificar su fichero de política Tripwire.

Primero haga todos los cambios necesarios en el fichero de política de muestra (`/etc/tripwire/twpol.txt`). Un cambio común a este fichero de política es convertir en comentario cualquier fichero que no existe en su sistema para que no genere un mensaje de error de `file not found` en los informes de Tripwire. Si por ejemplo su sistema no contiene un fichero `/etc/smb.conf`, puede decirle a Tripwire que no intente buscarlo a través de la conversión de su línea en comentario en `twpol.txt`:

```
#     /etc/smb.conf                       -> $(SEC_CONFIG) ;
```

Luego debe decirle a Tripwire que genere un fichero nuevo `/etc/tripwire/tw.pol` firmado y después que genere un fichero de base de datos actualizado basado en esta información de política. Suponiendo que `/etc/tripwire/twpol.txt` es el fichero de política modificado, use este comando:

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Se le pedirá la frase de contraseña de sitio. Luego el fichero `twpol.txt` se analizará sintácticamente y se firmará.

Es importante actualizar la base de datos de Tripwire después de haber creado un fichero `/etc/tripwire/tw.pol` nuevo. La forma más confiable para llevarlo a cabo es borrando su base de datos de Tripwire actual y creando una base de datos nueva con el fichero de política nuevo.

Si su fichero de base de datos de Tripwire se llama `wilbur.domain.com.twd`, teclee este comando:

```
rm /var/lib/tripwire/wilbur.domain.com.twd
```

Luego teclee el comando para crear una base de datos nueva:

```
/usr/sbin/tripwire --init
```

Se creará una base de datos nueva según las instrucciones en el fichero de política nuevo. Para asegurarse que la base de datos haya sido modificada correctamente, ejecute manualmente el primer control de integridad y vea el contenido del informe consiguiente. Consulte la Sección 10.8, *Ejecución de un*

control de integridad y la Sección 10.9, *Impresión de informes* para obtener instrucciones específicas sobre estas cuestiones.

10.11.1 La firma del fichero de configuración

El fichero de texto con los cambios al fichero de configuración (comúnmente `/etc/tripwire/twcfg.txt`) debe firmarse para que reemplace `/etc/tripwire/tw.cfg` y para que Tripwire lo utilice al ejecutar su control de integridad. Tripwire no reconocerá los cambios en la configuración hasta que el fichero de texto de la configuración esté correctamente firmado y sea usado para reemplazar el fichero `/etc/tripwire/tw.pol`.

Si su fichero de texto de configuración modificado es `/etc/tripwire/twcfg.txt`, teclee este comando para firmarlo, reemplazando el actual fichero `/etc/tripwire/tw.pol`:

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Como el fichero de configuración no altera ninguna de las políticas de Tripwire ni ninguno de los ficheros supervisados por la aplicación, no es necesario regenerar la base de datos de los ficheros de sistema supervisados.

10.12 Tripwire y el correo electrónico

Tripwire puede enviar un mensaje de correo electrónico a alguien si se ha violado un tipo específico de regla en el fichero de política. Para configurar Tripwire de manera que haga esto, primero hay que saber la dirección de correo electrónico de la persona que recibirá el mensaje si ocurre un determinado tipo de violación a la integridad, además del nombre de la regla que desea supervisar. Nótese que en sistemas grandes con administradores múltiples, puede avisar diferentes conjuntos de personas para determinadas violaciones y no avisarle a nadie si ocurren sólo violaciones menores.

Una vez que se sabe a quién avisar y sobre qué avisar, añada la línea **emailto=** a la sección de directivas de reglas de cada regla. Hágalo añadiendo una coma después de la línea **severity=** y poniendo **emailto=** en la línea siguiente, seguida por las direcciones de correo electrónico a las cuales enviar los informes de violaciones a esa regla. Se enviarán mensajes de correo electrónico múltiples si más de una dirección de correo electrónico ha sido especificada y si están separadas por un punto y coma.

Si por ejemplo usted quisiera que a dos administradores, Sam y Bob, se les avise que se ha modificado el programa de red, cambie la directiva de la regla de Programas de Red en el fichero de política de esta manera:

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = bob@domain.com;sam@domain.com
)
```

Cuando se haya generado un fichero de política firmado nuevo desde el fichero `/etc/tripwire/twpol.txt`, las direcciones de correo electrónico especificadas recibirán un aviso cuando ocurran violaciones a esa determinada regla. Para obtener las instrucciones sobre cómo firmar su fichero de política, consulte la Sección 10.11, *Actualización del fichero de política*.

10.12.1 Envío de mensajes de correo electrónico de prueba

Para asegurarse que la configuración para los avisos de correo electrónico por parte de Tripwire realmente sea capaz de enviar mensajes de correo electrónico correctamente, use el siguiente comando:

```
/usr/sbin/tripwire --test --email your@email.address
```

Se enviará inmediatamente un mensaje de correo electrónico de prueba a la dirección de correo electrónico por medio del programa `tripwire`.

10.13 Otros recursos

Tripwire es capaz de hacer más de lo que se cubre en este capítulo. Consulte estas fuentes de información adicionales para saber más sobre Tripwire.

10.13.1 Documentación instalada

- `/usr/share/doc/tripwire-<version-number>` — un excelente punto de inicio para aprender sobre cómo personalizar los ficheros de configuración y de política en el directorio `/etc/tripwire`.
- Consulte además las páginas de manual para `tripwire`, `twadmin` y `twprint` donde encontrará ayuda para el uso de estas utilidades.

10.13.2 Sitios web útiles

- http://www.tripwire.org — La sede del Tripwire Open Source Project (proyecto de open source de Tripwire), donde podrá encontrar las más recientes noticias sobre el programa, incluyendo una lista de FAQ.

11 Protocolo SSH

Este capítulo cubre los beneficios del protocolo SSH™, la secuencia de eventos que ocurre cuando se efectúa una conexión segura a un sistema remoto, las diferentes capas de SSH, y los métodos para asegurarse que los usuarios que se conectan a su sistema usen SSH.

Los métodos comunes para iniciar sesiones en otro sistema en modo remoto a través de una shell (`telnet`, `rlogin`, o `rsh`) o copiar ficheros entre hosts (`ftp` o `rcp`) resultan inseguros y deberían ser evitados. En su lugar, debería sólo conectarse a un host remoto por medio de una shell segura o una red privada virtual cifrada. Si usa métodos seguros para iniciar sesiones en otros sistemas remotamente, disminuirá los riesgos de seguridad ya sea para su sistema como para el sistema remoto.

11.1 Introducción

SSH (o *S*ecure *SH*ell) es un protocolo para crear conexiones seguras entre dos sistemas. Usando SSH, la máquina del cliente inicia una conexión con una máquina de servidor. SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor durante sesiones ulteriores.
- El cliente puede transmitir su información de autentificación al servidor, como el nombre de usuario y la contraseña, en formato cifrado.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación fuerte, lo cual los hacen extremamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de usar X11[1]aplicaciones lanzadas desde el indicador de comandos de la shell. Esta técnica proporciona una interfaz gráfica segura (llamada **reenvío por X11**).

El servidor también obtiene beneficios por parte de SSH, especialmente si desempeña una cierta cantidad de servicios. Si usa el **reenvío por puerto**, los protocolos que en otros casos serían considerados inseguros (POP, por ejemplo) se pueden cifrar para garantizar comunicación segura con máquinas remotas. SSH hace relativamente sencilla la tarea de cifrar tipos diferentes de comunicación que normalmente se envía en modo inseguro a través de redes públicas.

Red Hat Linux 7.1 contiene los paquetes de servidor (`openssh-server`) y cliente (`openssh-clients`) OpenSSH, al igual que el paquete OpenSSH general (`openssh`) que debe ser instalado para que cualquiera de los dos funcione. Consulte *Official Red Hat Linux Customization Guide* para obtener las instrucciones para instalar y desplegar OpenSSH en su sistema Red Hat Linux.

[1] X11 se refiere al sistema de visión por ventanas X11R6, tradicionalmente llamado X. Red Hat Linux contiene XFree86, un sistema X Window open-source muy conocido, que se basa en X11R6.

Los paquetes OpenSSH requieren del paquete OpenSSL (`openssl`). OpenSSL instala varias bibliotecas criptográficas importantes que sirven para que OpenSSH proporcione comunicaciones cifradas. Debe instalar el paquete `openssl` antes de instalar cualquiera de los paquetes OpenSSH.

Una gran cantidad de programas de cliente y servidor puede usar el protocolo SSH, incluyendo muchas aplicaciones open source a disposición gratuita. Hay varias versiones de cliente diferentes de SSH a disposición para casi todos los sistemas operativos más importantes en uso actualmente. Aún si los usuarios que se conectan a su sistema no ejecutan Red Hat Linux, de cualquier manera pueden encontrar y usar un cliente de SSH nativo para su sistema operativo.

11.1.1 ¿Porqué usar SSH?

Entre las amenazas al tráfico de red están incluidos el husmeo de paquete y la falsificación de DNS e IP[2]y la promulgación de información de ruteo falso. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

- *Interceptación de la comunicación entre dos sistemas* — bajo esta hipótesis, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información, o puede modificar la información y luego enviarla al recipiente al cual estaba destinada.
- *Personificación de un determinado host* — con esta estrategia, un sistema interceptor finge ser el recipiente a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa a comunicar con el interceptor como si su mensaje hubiese llegado a su destinación exitosamente.

Ambas técnicas causan que se intercepte información, posiblemente con propósitos hostiles. El resultado puede ser catastrófico, ya sea que ese propósito se alcance por medio de escuchar todos los paquetes en un LAN o por un servidor DNS sometido a un hack que apunta hacia un host duplicado intencionalmente.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar ficheros, estas amenazas a la seguridad se pueden disminuir notablemente. La firma digital de un servidor proporciona la verificación para su identidad. No es posible utilizar la comunicación entera entre los sistemas si ha sido interceptada, porque cada uno de los paquetes está cifrado. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

11.2 Secuencia de eventos de una conexión SSH

Una cierta serie de eventos ayuda a proteger la integridad de una comunicación SSH entre dos hosts.

2 La falsificación comúnmente significa aparecer ante los demás como un determinado sistema cuando en realidad no se es ese sistema

Primero, se crea una **capa de transporte** segura para que el cliente sepa que está efectivamente comunicando con el servidor correcto. Luego se cifra la comunicación entre el cliente y el servidor por medio de un código simétrico.

Después, con la conexión segura al servidor en su lugar, el cliente se autentifica ante el servidor sin preocuparse de que la información de autentificación pudiese exponerse a peligro. OpenSSH en Red Hat Linux usa claves DSA o RSA y la versión 2.0 del protocolo SSH para autentificaciones predeterminadas.

Por último, con el cliente autentificado ante el servidor, se pueden usar varios servicios diferentes con seguridad a través de la conexión, como una sesión shell interactiva, aplicaciones X11 y túneles TCP/IP.

El procedimiento de conexión en total se lleva a cabo sin grandes esfuerzos suplementales por parte del sistema local. De hecho, bajo muchos aspectos, SSH trabaja bien porque les es familiar a usuarios acostumbrados a métodos de conexión menos seguros.

En el siguiente ejemplo user1 en el sistema del cliente está iniciando una conexión SSH con un servidor. La dirección IP del servidor es 10.0.0.2, pero se podría usar su nombre de dominio en su lugar. El nombre de inicio de sesión de user1 en el servidor es user2. El comando `ssh` se escribe así:

```
[user1@machine1 user1]$ ssh user2@10.0.0.2
```

El cliente OpenSSH pedirá la frase de contraseña de la clave privada del usuario para descifrar la clave privada, que se utiliza para llevar a cabo la autentificación. Sin embargo, la frase de contraseña de la clave privada no se envía a través de la ya segura conexión entre el cliente y el servidor. En vez de eso, se usa la frase de contraseña para abrir el fichero `id_dsa` y generar una firma, que luego envía al servidor. El usuario será autentificado si el servidor tiene una copia de la clave pública del usuario que se pueda usar para verificar la firma.

En este ejemplo el usuario usa una clave DSA (también se pueden usar las claves RSA, entre muchas otras) y ve el siguiente indicador de comandos:

```
Enter passphrase for DSA key '/home/user1/.ssh/id_dsa':
```

Si por cualquier motivo llegase a fallar la autentificación de la clave pública (tal vez la frase de contraseña ha sido tecleada erróneamente o la información de autentificación no existe todavía en el servidor), por lo general se intenta otro tipo de autentificación. En nuestro ejemplo el servidor OpenSSH permite que user1 se autentifique a sí mismo con el uso de la contraseña de user2 porque la firma enviada no correspondía con la clave pública almacenada por user2:

```
user2@machine2's password:
```

Al usuario se le ofrece un indicador de comandos de shell cuando teclea la contraseña correcta. User2 debería ya tener una cuenta en la máquina 10.0.0.2 para que funcione la autentificación de la contraseña, por supuesto.

```
Last login: Mon Apr 15 13:27:43 2001 from machine1
[user2@machine2 user2]$
```

Llegado a este punto, el usuario puede interaccionar con la shell del mismo modo en que podría hacerlo con `telnet` o `rsh`, excepto que la comunicación está cifrada.

Otras herramientas SSH como `scp` y `sftp` trabajan de manera parecida a las herramientas inseguras `rcp` y `ftp`, respectivamente. Consulte *Official Red Hat Linux Customization Guide* para obtener las instrucciones y los ejemplos para usar estos y otros comandos SSH.

11.3 Capas de seguridad SSH

El protocolo SSH permite que cualquier programa de cliente y servidor construido según los planes detallados del protocolo comuniquen con seguridad y se usen de manera intercambiable.

Actualmente existen dos variedades diferentes de SSH. La versión 1 de SSH contiene varios algoritmos de encriptación patentados (sin embargo varios de estas patentes han caducado) y un agujero de seguridad que potencialmente permitiría que datos se inserten en el flujo de datos. Se recomienda el uso de servidores y clientes compatibles con la versión 2 de SSH, si es posible.

OpenSSH incluye el soporte para la versión 2 (y claves de encriptación DSA a disposición gratis). Combinado con las bibliotecas de encriptación OpenSSL, OpenSSH proporciona una gama completa de servicios de seguridad.

Ambas versiones del protocolo SSH (1 y 2) usan capas de seguridad parecidas para reforzar la integridad de la comunicación desde varios puntos de vista. Cada capa proporciona su propio tipo de protección que cuando se usa en conjunto con las otras refuerza la seguridad total de la comunicación y la hace más fácil de usar.

11.3.1 Capa de transporte

El papel principal de la capa de transporte es el de facilitar una comunicación segura entre dos hosts a la hora de y después de la autentificación. Normalmente ejecutado a través de TCP/IP, la capa de transporte logra hacer esto ocupándose de la encriptación y descifrado de datos, verificando que el servidor sea la máquina correcta para la autentificación, y proporcionando protección a la integridad de los paquetes de datos al momento de ser enviados y recibidos. Además, la capa de transporte también puede proveer la compresión de los datos, acelerando así la transmisión de la información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente:

- Intercambio de claves
- El algoritmo de la clave pública que hay que usar
- El algoritmo de la encriptación simétrica que hay que usar

- El algoritmo de la autentificación de mensajes que hay que usar
- El algoritmo de hash que hay que usar

El servidor se identifica ante el cliente con una **clave de host** durante el intercambio de claves. Obviamente si este cliente nunca había comunicado antes con este determinado servidor, la clave del servidor le resultará desconocida al cliente. OpenSSH evita este problema permitiendo que el cliente acepte la clave de host del servidor la primera vez que se lleva a cabo una conexión SSH. Luego la clave de host del servidor se puede verificar con la versión guardada en el cliente en las siguientes conexiones, proporcionando la confianza que el cliente está realmente comunicando con el servidor deseado.

El método de verificación de la clave de host utilizado por OpenSSH no es perfecto. Un agresor podría fingir ser el servidor durante el contacto inicial, porque el sistema local no necesariamente reconocería la diferencia entre el servidor deseado y el agresor a ese punto. Pero hasta que no se encuentre a disposición un método mejor de distribución de claves de host, este método inicialmente inseguro es mejor que nada.

SSH fue ideado para funcionar con casi cualquier tipo de algoritmo de clave pública o formato de codificación. Después de que el intercambio de claves inicial crea dos valores (un valor de hash usado para intercambios y un valor de secreto compartido), los dos sistemas empiezan inmediatamente a calcular claves y algoritmos nuevos para proteger la autentificación y los datos que se enviarán a través de la conexión en el futuro.

11.3.2 Autentificación

Cuando la capa de transporte haya construido un túnel seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autentificación soportados, como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autentificarse ante el servidor mediante el uso de cualquiera de los métodos soportados.

Ya que los servidores se pueden configurar para que concedan varios tipos de autentificación, este método proporciona a cada parte un control óptimo. Luego el servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad, y el cliente puede elegir el orden en que intentará utilizar los métodos de autentificación entre las opciones a disposición. Gracias a la naturaleza segura de la capa de transporte de SSH, hasta métodos de autentificación que parecen inseguros, como la autentificación basada en el host, son en realidad seguros.

La mayoría de los usuarios que requieren de una shell segura se autentificarán por medio de una contraseña. En contraste con otros esquemas de seguridad por medio de autentificación, la contraseña se transmite al servidor en texto sin cifrar. Sin embargo, ya que la contraseña entera va cifrada al pasar por la capa de transporte, puede ser enviada a través de cualquier red sin problemas de seguridad.

11.3.3 Conexión

Después de una autentificación exitosa sobre una capa de transporte SSH, se abren **canales** múltiples por medio de la multiplexión[3]la conexión individual entre dos sistemas. Cada canal se ocupa de la comunicación para sesiones entre terminales diferentes, el reenvío de información por X11 o cualquier servicio aparte que intente usar la conexión SSH.

Ya sea los clientes como los servidores pueden crear un canal nuevo, con cada canal asignado un número diferente en cada orilla. Cuando una parte intenta abrir un canal nuevo, el número para el canal de esa parte se envía junto con la petición. Esta información se almacena por la otra parte y se usa para dirigir un determinado tipo de comunicación de servicio a ese canal. Esto se lleva a cabo para que diferentes tipos de sesiones no se afecten los unos por los otros y que los canales puedan cerrarse sin interrumpir la conexión SSH principal entre los dos sistemas.

Los canales también soportan el control de flujo, el cual les permite enviar y recibir datos ordenadamente. De esta manera, los datos no se envían a través del canal sino hasta que el host haya recibido un mensaje avisando que el canal puede recibirlos.

Los canales son especialmente útiles con el reenvío por X11 y el reenvío por puerto TCP/IP con SSH. Se pueden configurar canales aparte en modo diferente, tal vez para usar un tamaño de paquete máximo diferente o para transferir un determinado tipo de datos. Esto permite que SSH sea flexible en su modo de encargarse de los diferentes tipos de conexiones remotas, como el acceso telefónico en redes públicas o enlaces LAN de alta velocidad, sin tener que cambiar la infraestructura básica del protocolo. El cliente y el servidor se ponen de acuerdo automáticamente sobre la configuración de cada canal dentro de la conexión SSH para el usuario.

11.4 Ficheros de configuración OpenSSH

OpenSSH tiene dos conjuntos diferentes de ficheros de configuración, uno para los programas del cliente (`ssh`, `scp`, y `sftp`) y el otro para los servicios del servidor (`sshd`), ubicados en dos sitios diferentes.

La información de configuración SSH para todo el sistema está almacenada en el directorio `/etc/ssh`:

[3] Una conexión multiplexada consiste en varias señales enviadas simultáneamente por un medio compartido. Con SSH, se envían varios canales en una conexión en común segura.

- `primes` — contiene grupos Diffie-Hellman que sirven para el intercambio de claves Diffie-Hellman. Fundamentalmente, este intercambio de claves crea un valor de secreto compartido que ninguna de las partes puede determinar sola y se usa para proporcionar la autentificación del host. Este fichero es esencial para la construcción de una capa de transporte segura.
- `ssh_config` — el fichero de configuración de cliente SSH para todo el sistema se usa para dirigir al cliente SSH. Si un usuario tiene su propio fichero de configuración a disposición en su directorio de inicio (`~/.ssh/config`), sus valores predominarán sobre los valores almacenados en `/etc/ssh/ssh_config`.
- `sshd_config` — el fichero de configuración para `sshd`.
- `ssh_host_dsa_key` — la clave privada DSA usada por `sshd`.
- `ssh_host_dsa_key.pub` — la clave pública DSA usada por `sshd`.
- `ssh_host_key` — la clave privada RSA usada por `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_key.pub` — la clave pública RSA usada por `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_rsa_key` — la clave privada RSA usada por `sshd` para la versión 2 del protocolo SSH.
- `ssh_host_rsa_key.pub` — la clave pública RSA usada por `sshd` para la versión 2 del protocolo SSH.

La información para la configuración SSH específica para el usuario está almacenada en el directorio de inicio del usuario dentro del subdirectorio `.ssh`:

- `authorized_keys2` — el fichero que contiene una lista de claves públicas "autorizadas". Si un usuario que se conecta puede comprobar que conoce la clave privada que corresponde a cualquiera de las claves públicas, entonces será autentificada. Note que esto es sólo un método de autentificación opcional.
- `id_dsa` — contiene la identidad de autentificación DSA del usuario.
- `id_dsa.pub` — la clave pública DSA del usuario.
- `known_hosts2` — almacena las claves de host DSA de los servidores a los cuales los usuarios dan inicio a una sesión por medio de SSH cuando el usuario decide guardarlas. Si a un servidor se le modifican las claves de host en modo legítimo, tal vez a la hora de reinstalar Red Hat Linux el usuario recibirá un aviso que la clave de host almacenada en el fichero `known_hosts2` que debería corresponder con este host no corresponde. Entonces el usuario debe borrar esa clave de host en `known_hosts` para poder almacenar la clave de host nueva para ese sistema. El fichero `known_hosts2` es muy importante para asegurar que el cliente se esté conectando con el servidor correcto. Si ha cambiado una clave de host, y usted no está perfectamente seguro el

motivo por el que ha sido cambiada, entonces debería contactar el administrador de sistema del host para asegurarse que el host no haya sido expuesto a peligro.

Consulte las páginas de manual `ssh` y `sshd` para obtener información acerca de las directivas disponibles en los ficheros de configuración SSH.

11.5 Más que una shell segura

Una interfaz de línea de comandos segura es sólo el inicio de las muchas maneras de usar SSH. Dada una cantidad apropiada de ancho de banda, las sesiones X11 se pueden dirigir por un canal SSH. O se pueden asignar conexiones de puerto entre sistemas que previamente eran inseguras a canales SSH específicos usando el reenvío por TCP/IP.

11.5.1 Reenvío por X11

Abrir una sesión X11 a través de una conexión SSH establecida es tan fácil como ejecutar un programa X mientras se está ya ejecutando un cliente X en su host. Cuando un programa X se ejecuta desde un indicador de comandos de shell segura, el cliente y el servidor SSH crean un nuevo canal seguro dentro de la conexión SSH actual, y los datos del programa X se envían a través de ese canal a la máquina de cliente como si usted estuviese conectado al servidor X por medio de una terminal local.

Como podrá imaginar, el reenvío por X11 puede ser muy útil. Por ejemplo, se puede usar el reenvío por X11 para crear una sesión segura e interactiva con el GUI `up2date` en el servidor para actualizar paquetes en modo selectivo (si posee los paquetes Red Hat Network necesarios instalados en el servidor). Para hacer esto simplemente hay que conectarse al servidor mediante `ssh` y teclear:

```
up2date
```

Se le pedirá proporcionar la contraseña de root para el servidor. Luego aparecerá el Red Hat Update Agent y usted podrá actualizar sus paquetes en el servidor como si estuviese sentado delante de la máquina.

Sin embargo, los gastos generales de procesamiento requeridos para cifrar y descifrar la información segura que se envía a través del canal, además del ancho de banda extra necesario para enviar datos de aplicaciones X encriptados pueden ser cuantiosos. Es necesario llevar a cabo pruebas adecuadas para asegurarse que el programa X todavía es utilizable, dadas sus condiciones de hardware y ancho de banda particulares.

11.5.2 Reevío por TCP/IP

El reenvío por TCP/IP trabaja con el cliente SSH y pide que un determinado puerto en el lado del cliente o del servidor sea asignado a la conexión SSH existente.

Para asignar un puerto local del cliente a un puerto remoto del servidor, primero hay que saber los números de puerto de ambas máquinas. Hasta es posible asignar dos puertos no estándar, diferentes el uno del otro.

Use el siguiente comando (todo en la misma línea) para crear un canal de reenvío por TCP/IP que escuche las conexiones en el host local:

```
ssh -L <local-port>:<remote-hostname>:<remote-port>
          <username>@<hostname>
```

Nota

Configurar un reenvío por TCP/IP para que escuche en puertos inferiores a 1024 requiere acceso a la raíz del mismo modo que iniciar servicios que escuchan en puertos bajo 1024.

Si por ejemplo desea controlar su correo electrónico en un servidor llamado mail.domain.com usando POP y SSH está a disposición en ese servidor, puede usar este comando para configurar el reenvío por TCP/IP:

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Después de que el reenvío por TCP/IP esté situado entre las dos máquinas puede indicarle a su cliente de correo POP que use localhost como servidor POP y 1100 como puerto para controlar si hay correspondencia nueva. Cualquier petición enviada al puerto 1100 en su sistema será reenviada en modo seguro al servidor mail.domain.com.

Si mail.domain.com no está ejecutando un demonio de servidor SSH pero es posible iniciar una sesión por medio de SSH a una máquina cercana, quizás a través de un cortafuego, puede de todos modos usar SSH para asegurar la parte de la conexión POP que ocurre a través de redes públicas. Para esto es necesario un comando ligeramente diferente:

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

En este ejemplo, usted está reenviando su petición POP desde el puerto 1100 en su máquina a través de la conexión SSH en el puerto 22 hacia other.domain.com. Luego other.domain.com se conecta al puerto 110 en mail.domain.com para permitirle controlar su correspondencia. Sólo la conexión entre su sistema y other.domain.com es seguro, pero en muchas situaciones esto basta para tener acceso a su información con seguridad a través de redes públicas proporcionando más seguridad de la que tenía anteriormente.

Por supuesto que en este ejemplo y en el precedente hay que ser capaces de autentificarse ante el servidor SSH para desempeñar el reenvío por TCP/IP. Asegúrese de poder ejecutar comandos SSH normales antes de intentar configurar el reenvío por TCP/IP.

El reenvío por TCP/IP puede ser especialmente útil para obtener información en modo seguro a través de cortafuegos de red. Si el cortafuego está configurado para permitir el tráfico SSH a través de su puerto estándar (22) pero bloquea el acceso a través de otros puertos, sigue siendo posible una conexión entre dos hosts usando los puertos bloqueados desviando su comunicación a través de una conexión SSH establecida entre ellos.

Nota

Sin embargo, esto puede ser muy peligroso. El uso del reenvío por TCP/IP para reenviar conexiones de esta manera permite que cualquier usuario en el sistema del cliente se conecte al servicio al cual usted está reenviando conexiones, que podría ser peligroso si su sistema de cliente se convierte en un sistema expuesto.

Controle con el administrador de sistema que administra su cortafuego antes de usar el reenvío por TCP/IP para superarlo. Los administradores de sistemas a quienes les preocupa el reenvío por TCP/IP pueden inhabilitar esta función en el servidor especificando un parámetro `No` para la línea **AllowTcpForwarding** en `/etc/ssh/sshd_config` y luego reiniciando el servicio `sshd`.

11.6 Requisitos de SSH para conexiones remotas

Para que SSH sea realmente eficaz para proteger sus conexiones de red, deberá dejar de usar protocolos de conexión inseguros, como por ejemplo `telnet` y `rsh`. De otra manera, la contraseña de un usuario podría ser protegida un día si se usa `ssh` y luego ser capturada al día siguiente cuando inicia una sesión por medio de `telnet`.

Para inhabilitar métodos de conexión inseguros a su sistema use `ntsysv` o `chkconfig` para asegurarse que estos servicios no inicien junto con el sistema. Escriba el siguiente comando para hacer que `ntsysv` configure los servicios que inician a niveles de ejecución 2, 3, y 5:

```
/usr/sbin/ntsysv 235
```

Dentro de `ntsysv` se pueden inhabilitar el inicio de servicios anulando la selección. La tecla de [espacio] cambia los servicios de activos a inactivos. Como mínimo debería desactivar `telnet`, `rsh`, `ftp` y `rlogin`. Cuando termine, seleccione el botón **OK** para conservar sus cambios `ntsysv`. Consulte la página de manual que corresponde a `ntsysv` para obtener más ayuda en el uso de esta utilidad.

Los cambios hechos con `ntsysv` no surtirán efecto sino hasta que se reinicie el sistema o cambia los niveles de ejecución. Si ha desactivado servicios que se usan con `xinetd`, deberá reiniciar `xinetd`. Por defecto, `rlogin`, `rsh` y `telnet` son controlados por `xinetd`. Para reiniciar `xinetd` teclee:

```
/sbin/service xinetd restart
```

Deberá inhabilitar manualmente los servicios que no se usan con `xinetd` a menos que desee reiniciar su sistema después de haber usado `ntsysv`. Para inhabilitar un servicio probablemente usará un comando como:

```
/sbin/service <service-name> stop
```

Después de haber reiniciado `xinetd` e inhabilitado cualquier servicio que haya configurado para que no inicie automáticamente, los métodos de conexión inhabilitados ya no serán aceptados por su sistema. Si inhabilita todos los métodos de conexión remotos aparte del demonio de servicio `sshd`, los usuarios deberán usar una aplicación de cliente SSH para conectarse al servidor.

12 Control de acceso y privilegios

El sistema de seguridad se confía a usuarios o grupos que no son capaces de hacer más de lo que deberían, de acuerdo con una política de seguridad. La mayoría de los cambios del día a día relacionados con el control de acceso y privilegios se refieren al uso adecuado de usuarios y grupos. (Consulte el Capítulo 2, *Usuarios y grupos* para más información sobre la creación y configuración de usuarios y grupos.)

No obstante, muchas organizaciones que usan Red Hat Linux tienen pautas o entornos de trabajo particulares que requieren una seguridad más estricta o configuraciones especiales para accesos estrictos a aplicaciones o dispositivos de sistema. Esta sección le muestra diferentes maneras de abordar su sistema para que proporcione un nivel apropiado de acceso y privilegios para los usuarios en su situación.

12.1 Utilidades Shadow

Si está en un entorno multiusuario y no utiliza ni PAM ni Kerberos, debería considerar el uso de utilidades Shadow (también conocidas como **contraseñas shadow**) para la protección incrementada ofrecida por los ficheros de autentificación de su sistema. Durante la instalación de Red Hat Linux la protección de la contraseña shadow para su sistema se habilita por defecto, así como **contraseñas MD5** (método alternativo para encriptar contraseñas para el almacenamiento en su sistema).

Las contraseñas shadow ofrecen ventajas respecto a los almacenamientos de contraseñas estándar anteriores de UNIX y LINUX que incluyen:

- Seguridad del sistema mejorada al trasladar las contraseñas encriptadas (que se encuentran normalmente en `/etc/passwd`) a `/etc/shadow` que tan sólo puede ser leído por root.
- Información referente a la antigüedad de la contraseña (tiempo transcurrido desde la última vez que se cambió la contraseña)
- Control sobre el tiempo que puede permanecer una contraseña antes de que al usuario se le pida que la cambie.
- Habilidad para usar el fichero `/etc/login.defs` para reforzar la política de seguridad, especialmente en lo referente a la antig|edad de la contraseña.

El paquete `shadow-utils` contiene un número de utilidades que soportan:

- Conversión de contraseñas normales a shadow y viceversa (`pwconv`, `pwunconv`)
- Verificación de la contraseña, grupo y ficheros shadow asociados (`pwck`, `grpck`)
- Métodos estándar de industria para añadir, borrar y modificar las cuentas de usuario (`useradd`, `usermod`, y `userdel`)

- Métodos estándar de industria para añadir, borrar y modificar los grupos de usuario (`groupadd`, `groupmod`, y `groupdel`)
- Método estándar de industria para adminstrar el fichero `/etc/group` utilizando `gpasswd`

Nota

Puntos adicionales que hacen referencia a estas utilidades:

- Las utilidades funcionarán dependiendo de si se permite o no el shadowing.
- Las utilidades se han modificado ligeramente para soportar el esquema de grupo del usuario privado de Red Hat. Para ver una descripción de las modificaciones, lea la página de manual `useradd` Para ulterior información sobre los grupos privados de usuario remítase a la Sección 2.4, *Grupos privados de usuarios*.
- El script `adduser` ha sido sustituido por un enlace simbólico en `/usr/sbin/useradd`.
- Las herramientas en el paquete `shadow-utils` no están habilitadas ni por Kerberos ni por LDAP. Los usuarios nuevos serán sólo locales. Para más información consulte el Capítulo 9, *Uso de Kerberos 5 en Red Hat Linux* y el Capítulo 4, *Lightweight Directory Access Protocol (LDAP)*.

12.2 Configuración del acceso de consola

Cuando los usuarios normales (que no son root) se conectan a un ordenador localmente, se les dan dos tipos de permisos:

1. Pueden ejecutar ciertos programas que de otra manera no serían capaces de ejecutar.
2. Pueden acceder a ciertos ficheros (generalmente ficheros de dispositivos especiales usados para acceder a diskettes, CD-ROMS, etc) a los que, de lo contrario, no les sería posible acceder.

Ya que existen múltiples consolas en un solo ordenador y múltiples usuarios pueden conectarse al ordenador localmente al mismo tiempo, uno de los usuarios tiene que "ganar" la carrera para acceder a los ficheros. El primer usuario que se conecte a la consola posee esos ficheros. Una vez que el primer usuario se desconecta, el siguiente usuario que se conecte tendrá esos archivos.

Por el contrario, a *cada* usuario que se conecte a la consola se le permitirá ejecutar programas que realicen tareas restringidas normalmente al usuario root. Si se está ejecutando X, estas acciones pueden

incluirse como menú de items en la interfaz gráfica de usuario. Los programas accesibles a consolas incluyen `halt` y `reboot`.

12.2.1 Deshabilitar el apagado a través de Ctrl-Alt-Supr

Por defecto, `/etc/inittab` especifica que su sistema está configurado para apagarse y rearrancar el sistema como respuesta a la combinación de teclas usadas en la consola [Ctrl]-[Alt]-[Supr]. Si quiere deshabilitar esta habilidad, necesitará añadir la siguiente línea en `/etc/inittab`:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Otra alternativa, es la de conceder a ciertos usuarios no que no son root, el derecho a shutdown el sistema desde la consola mediante [Ctrl]-[Alt]-[Supr]. Puede restringir este privilegio a ciertos usuarios, siguiendo los siguientes pasos:

1. Añada una opción `-a` a la línea `/etc/inittab` mostrada anteriormente, de manera que quede así:

   ```
   ca::ctrlaltdel:/sbin/shutdown         -a -t3 -r now
   ```

   El indicador `-a` le pide a `shutdown` que busque el fichero `/etc/shutdown.allow`, que creará en el siguiente paso.

2. Cree un fichero llamado `shutdown.allow` en `/etc`. El fichero `shutdown.allow` debería listar los nombres de usuario de cualquier usuario al que se le permita apagar el sistema usando [Ctrl]-[Alt]-[Supr]. El formato del fichero `/etc/shutdown.allow` es una lista de nombres de usuarios, uno por línea, como sigue a continuación:

   ```
   stephen
   jack
   sophie
   ```

De acuerdo con este ejemplo de fichero `shutdown.allow`, stephen, jack y sophie están autorizados a apagar el sistema desde la consola usando [Ctrl]-[Alt]-[Supr]. Cuando se usa esa combinación de claves, el `shutdown -a` comprueba que cualquiera de los usuarios en `/etc/shutdown.allow` (o root) están conectados a una consola virtual. Si es uno de ellos, el apagado del sistema continuará; de lo contrario, aparecerá un mensaje de error escrito en la consola del sistema.

Para información ulterior sobre `shutdown.allow` consulte la página de manual `shutdown`.

12.2.2 Deshabilitar el acceso desde la consola a programas

Para deshabilitar el acceso de usuario a programas de consola, debería ejecutar el siguiente comando como root:

```
rm -f /etc/security/console.apps/*
```

En entornos donde la consola se encuentra asegurada (BIOS y LILO tienen contraseña, [Ctrl]-[Alt]-[Suprimir] está deshabilitado, los interruptores de encendido y reinicio están desactivados, etc.), puede que no desee permitir a ningún usuario que ejecute en la consola `poweroff`, `halt`, y `reboot`, que son accesibles desde la consola por defecto.

Para desactivar estas habilidades, hay que ejecutar los siguientes comandos como root:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

12.2.3 Deshabilitar el acceso a la consola totalmente

El módulo PAM `pam_console.so` gestiona los permisos y la autentificación de los archivos de consola. (Consulte el Capítulo 8, *Módulos de autentificación conectables (PAM)* para ulterior información sobre la configuración de PAM.) Si quiere deshabilitar el acceso a la consola totalmente, incluido el acceso a programas y ficheros, añada todas las líneas que hacen referencia `pam_console.so` en el directorio `/etc/pam.d`. El siguiente script lo hará todo:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

12.2.4 Definición de la consola

El módulo `pam_console.so` utiliza el fichero `/etc/security/console.perms` para determinar los permisos de los usuarios para la consola del sistema. La sintaxis del fichero es muy flexible; puede modificar el fichero de manera que las instrucciones no se apliquen nunca más. No obstante, el fichero predeterminado tiene una línea que se parece a la siguiente:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Cuando los usuarios se conectan, están conectados a algún tipo de terminal con nombre, ya sea un servidor de X con un nombre como `:0` o `mymachine.example.com:1.0`; o a un dispositivo como `/dev/ttyS0` o `/dev/pts/2`. Por defecto se define que las consolas locales virtuales y los servidores locales de X se consideran locales, pero si se quiere se puede considerar local un puerto serie como `/dev/ttyS1`, cambiando esa línea a:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

12.2.5 Creación de archivos accesibles desde la consola

En `/etc/security/console.perms`, hay una sección con líneas como:

```
<floppy>=/dev/fd[0-1]* \
```

```
    /dev/floppy/*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
    /dev/mixer* /dev/sequencer \
    /dev/sound/*
<cdrom>=/dev/cdrom* /dev/cdwriter*
```

Puede añadir sus propias líneas a esta sección , si lo considera necesario. Asegúrese de que las líneas que añada se refieren a un dispositivo apropiado. Por ejemplo, puede añadir la siguiente línea:

```
<scanner>=/dev/sga
```

(Naturalmente, asegúrese de que `/dev/sga` es realmente su escáner y no su disco duro.)

Éste es el primer paso. El segundo es definir lo que se ha hecho con estos archivos. Mire en la sección anterior de `/etc/security/console.perms` para ver líneas similares a:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

y añada una línea como:

```
<console> 0600 <scanner> 0600 root
```

Cuando se conecte a la consola, se le dará un dispositivo de pertenencia y los permisos serán 0600 (que sólo podrá leer usted). Cuando se desconecte, el dispositivo pertenecerá a root y todavía tendrá permisos 0600 (que en este caso sólo podrá leer y escribir root).

12.2.6 Habilitar el acceso de consola para otras aplicaciones

Si desea que otras aplicacioness sean accesibles a los usuarios de consolas, tendrá que hacer un último esfuerzo.

Lo primero de todo, el acceso de consola *sólo* funciona para aplicaciones que estén en los directorios `/sbin` o `/usr/sbin`, así que la aplicación a ejecutar debe estar ahí. Una vez verificado, siga los siguientes pasos:

1. Cree un enlace partiendo del nombre de la aplicación, como en nuestro programa de ejemplo *`foo`*, para la aplicación `/usr/bin/consolehelper`:

   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```

2. Cree el archivo `/etc/security/console.apps/`*`foo`*:

   ```
   touch /etc/security/console.apps/foo
   ```

3. Cree un archivo de configuración de PAM para el servicio *foo* en `/etc/pam.d/`. Una forma fácil de realizarlo es empezar con una copia del archivo de configuración PAM del servicio parada y modificar el archivo si quiere cambiar el entorno:

```
cp /etc/pam.d/halt /etc/pam.d/foo
```

A partir de ahora, cuando ejecute `/usr/bin/`*foo*, se pondrá en contacto con `consolehelper`, que autentificará al usuario con la ayuda de `/usr/sbin/userhelper`. Para autentificar el usuario, `consolehelper` le pedirá la contraseña de usuario si `/etc/pam.d/`*foo* es una copia de `/etc/pam.d/halt` (de lo contrario, hará lo que está especificado en `/etc/pam.d/`*foo*) y, por consiguiente, ejecutará `/usr/sbin/`*foo* con permisos de root.

12.3 El grupo `floppy`

Si, por cualquier razón, el acceso desde consola no es apropiado, y se necesita dar acceso a usuarios normales a la disquetera del sistema, se puede hacer usando el grupo `floppy`. Simplemente hay que añadir a los usuarios al grupo `floppy` utilizando cualquier herramienta apropiada. Aquí hay un ejemplo que muestra como `gpasswd` puede usarse para añadir el usuario fred al grupo `floppy`:

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

En este momento, el usuario fred puede acceder a la disquetera del sistema.

Parte III Apache

13 Uso de Apache como servidor Web seguro

13.1 Introducción

Este capítulo proporciona información básica sobre cómo instalar el servidor Apache World Wide Web (WWW or Web) con el módulo de seguridad mod_ssl y con las librerías y el kit de herramientas OpenSSL. La combinación de estos tres componentes, proporcionados por Red Hat Linux, aparecerá en este manual como secure Web server o simplemente como servidor seguro.

Los Servidores Web suministran páginas web a los navegadores (como por ejemplo, Netscape Navigator, Internet Explorer de Microsoft) que lo solicitan. En términos más técnicos, los servidores Web soportan el Protocolo de Transferencia de Hypertexto conocido como HTTP (HyperText Transfer Protocol), el estándar de Internet para comunicaciones web. Usando HTTP, un servidor web envía páginas web en HTML y CGI, así como otros tipos de scripts a los navegadores o browsers cuando éstos lo requieren. Cuando un usuario hace click sobre un enlace (link) a una página web, se envía una solicitud al servidor Web para localizar los datos nombrados por ese enlace. El servidor Web recibe esta solicitud y suministra los datos que le han sido solicitados (una página HTML, un script interactivo, una página web generada dinámicamente desde un base de datos,...), o bien devuelve un mensaje de error. Apache, el servidor Web suministrado con este producto, es el más usado en Internet actualmente (vayaa http://www.netcraft.net/survey/).

El servidor Web Apache está diseñado de forma modular; consiste en muchas porciones de código que hacen referencia a diferentes aspectos o funcionalidades del servidor Web. Esta modularidad es intencionada, con lo cual, cada desarrollador puede escribir su propia porción de código para cubrir una necesidad en particular. Su código, llamado módulo, puede ser integrado en el servidor Web Apache con relativa facilidad.

El módulo mod_ssl es un módulo de seguridad para el Servidor Web Apache. El módulo mod_ssl usa las herramientas suministradas por el OpenSSL Project para añadir una característica muy importante al Apache —, la posibilidad de encriptar las comunicaciones. A diferencia de las comunicaciones entre un navegador y un servidor web usando HTTP "normal", en la que se envía el texto íntegro, pudiendo ser interceptado y leído a lo largo del camino entre servidor y navegador.

El OpenSSL Project incluye un kit de herramientas que implementa los protocolos SSL (Secure Sockets Layer) y TLS (Transport Layer Security), así como una librería de codificación de propósito general. El protocolo SSL se usa actualmente para la transmisión de datos segura sobre Internet; El protocolo TLS es un estándar de Internet para comunicaciones privadas (seguras) y fiables a través de Internet. Las herramientas OpenSSL son usadas por el módulo mod_ssl para aportar seguridad en las comunicaciones Web.

Este capítulo no es una documentación completa ni exclusiva de cada uno de estos programas. Cuando sea posible, esta guía le citará los lugares apropiados donde podrá encontrar información que trate sobre temas particulares con más detalle.

Este capítulo le mostrará cómo instalar los programas incluidos, así como los pasos necesarios para generar una clave privada y una petición certificada. También se le enseñarán los pasos adecuados para generar su propio certificado firmado y como instalar un certificado para usarlo con el servidor Web seguro.

13.2 Reconocimientos

el secure Web server incluye lo siguiente:

- Software desarrollado por el grupo Apache para usar en proyecto del servidor Apache HTTP (http://httpd.apache.org)
- El módulo de seguridad mod_ssl, desarrollado por Ralf S. Engelschall (http://www.modssl.org/)
- El kit de herramientas OpenSSL, desarollado por Mark J. Cox, Ralf S. Engelschall, Dr. Stephen Henson y Ben Laurie (http://www.openssl.org/)
- Software basado en el proyecto de servidor HTTP Apache-SSL desarrollado por Ben Laurie (http://www.apache-ssl.org/)
- Software basado en el software de encriptación SSLeay escrito por Eric Young y Tim Hudson.

Red Hat agradece estas contribuciones para la consecución de este producto.

13.3 Introducción a los paquetes relacionados con la seguridad

Para instalar un servidor seguro, necesitará instalar como mínimo tres paquetes:

`apache`

El paquete `apache`contiene el demonio `httpd` y utilidades relacionadas, ficheros de configuración, iconos, módulos Apache, páginas de manual y otros ficheros usados por el servidor Web Apache.

`mod_ssl`

El paquete `mod_ssl` incluye el módulo mod_ssl, que proporciona una potente criptografía para el servidor Web Apache a través de los protocolos SSL (Secure Sockets Layer) y TLS (Transport Layer Security).

`openssl`

El paquete `openssl` contiene el kit de herramientas OpenSSL. Este kit de herramientas implementa los protocolos SSL y TLS, del mismo modo que incluye una librería de criptografía de propósito general.

Además, otros paquetes software incluidos con Red Hat Linux pueden añadir funciones de seguridad (sin ser imprescindibles para el correcto funcionamiento del servidor):

`apache-devel`

El paquete `apache-devel` contiene los ficheros incluidos en Apache, ficheros de cabecera y la utilidad APXS. Los necesitará si intenta cargar módulos extra, distintos de los suministrados con este producto. Consulte la Sección 14.3, *Añadir módulos a su servidor* para más información sobre carga de módulos en su secure Web server usando la función DSO de Apache.

Si no tiene la intención de cargar otros módulos en su secure Web server, no necesitará instalar este paquete.

`apache-manual`

El paquete `apache-manual` contiene la *Guía de usuario Apache 1.3* del Proyecto Apache en formato HTML. Este manual también está disponible en el Web http://www.apache.org/docs/.

Paquetes OpenSSH

Los paquetes OpenSSH proporcionan un set de herramientas de conectividad de redes para registrarse y ejecutar comandos en una máquina remota. Las herramientas OpenSSH encriptan todo el tráfico (incluyendo las contraseñas), para evitar el espionaje, secuestro de conexiones y otros ataques en las comunicaciones entre su ordenador y una máquina remota.

El paquete `openssh` incluye los achivos de núcleo necesarios para ambos, tanto el programa cliente, como el servidor OpenSSH. El paquete `openssh` también contiene lientes OpenSSH: `scp`, un sustituto seguro para `rcp` (para la copia de ficheros entre máquinas) y `ftp` (para la transferencia de ficheros entre máquinas).

El paquete `openssh-askpass` soporta la visualización de la ventana de diálogo en la que se le invita a introducir una clave durante el uso del agente OpenSSH con autentificación RSA.

El paquete `openssh-askpass-gnome` contiene una ventana de diálogo para el entorno de escritorio GNOME GUI que se presenta cuando el OpenSSH le indica la introducción de una contraseña. Si está ejecutando GNOME y está usando utilidades OpenSSH, debería instalar este paquete.

El paquete `openssh-server` contiene el demonio de la shell de seguridad `sshd` y archivos relacionados. El demonio de la shell de seguridad es el lugar donde se acomoda el OpenSSH y debe ser instalado en su host si quiere permitir a los clientes SSH conectarse a su host.

El paquete `openssh-clients` contiene los programas cliente necesarios para hacer conexiones encriptadas a los servidores SSH, un sustituto seguro para `rsh`;y `slogin`, así como

para `rlogin` (para un login remoto) y `telnet` (para comunicar con otro host a través del protocolo TELNET).

Para obtener más información sobre OpenSSH, vea el Capítulo 11, *Protocolo SSH* y el sitio web OpenSSH en http://www.openssh.com.

`openssl-devel`

El paquete `openssl-devel` contiene las librerías estáticas y los ficheros necesarios para compilar aplicaciones con soporte para varios algoritmos codificadores y protocolos. Tendrá que instalar este paquete sólo si está utilizando aplicaciones que incluyen soporte SSL — no necesitará este paquete para usar SSL.

`stunnel`

El paquete `stunnel` suministra la wrapper SSL Stunnel. Stunnel soporta la codificación SSL de conexiones TCP, así podrá dar la capacidad de codificar a demonios que no son SSL y protocolos (como POP, IMAP, LDAP) sin tener que cambiar el código de los demonios.

La Tabla 13–1, *Paquetes seguros* visualiza la localización de los paquetes de servidor seguro y los paquetes adicionales relacionados con la seguridad dentro de los grupos de paquetes proporcionados por Red Hat Linux. Esta tabla también le dice si cada paquete es opcional o no para la instalación de un servidor Web seguro.

Tabla 13–1 Paquetes seguros

Nombre del paquete	Localizada en grupo	¿Opcional?
`apache`	Entorno del sistema/Demonios	no
`mod_ssl`	Entorno del sistema/Demonios	no
`openssl`	Entorno del sistema/Librerías	no
`apache-devel`	Desarrollo/Librerías	sí
`apache-manual`	Documentación	sí
`openssh`	Aplicaciones/Internet	sí
`openssh-askpass`	Aplicaciones/Internet	sí
`openssh-askpass-gnome`	Aplicaciones/Internet	sí
`openssh-clients`	Aplicaciones/Internet	sí
`openssh-server`	Entorno del sistema/Demonios	sí

Nombre del paquete	Localizada en grupo	¿Opcional?
`openssl-devel`	Desarrollo/Librerías	sí
`stunnel`	Aplicaciones/Internet	sí

13.4 ¿Cómo instalar el servidor seguro?

Puede instalar el secure Web server de los siguientes modos:

- *Durante una instalación nueva de Red Hat Linux* — Ya que el secure Web server viene incluido con el sistema operativo Red Hat Linux, el método más fácil durante la instalación de Red Hat Linux. Si está a punto de completar la instalación de Red Hat Linux, debería instalar el servidor seguro de esta manera. Vea la Sección 13.5, *Instalación de un servidor seguro con Red Hat Linux* para ulterior información sobre este método.
- *Al actualizar Red Hat Linux mediante el uso del programa de instalación* — si ya tiene una versión previa de Red Hat Linux en su sistema lo está actualizando a Red Hat Linux 7.1, puede instalar los paquetes de servidor seguro durante el proceso de actualización. Vea la Sección 13.6, *Actualización desde una versión previa de Red Hat Linux* para ulterior información sobre este método.
- *Instalar el servidor seguro después de la instalación de Red Hat Linux* 7.1 — Si ha instalado previamente Red Hat Linux 7.1 y un tiempo después decide que quiere proveerse de las funciones del servidor seguro, podrá usar el RPM, Gnome-RPM o Kpackage para instalar los paquetes del servidor seguro desde un CD de Red Hat Linux. Consulte la Sección 13.7, *Instalación del servidor seguro después de la instalación de Red Hat Linux* para instrucciones sobre como instalar el servidor seguro después de haber instalado Red Hat Linux.

Actualización de Apache

Cuando instale el secure Web server, si usted está actualizando desde una versión de Apache (incluyendo cualquier versión previa de secure Web server), necesitará conocer ciertos procedimientos relativos al proceso de actualización. Vea la Sección 13.8, *Actualización desde una versión previa de Apache* antes de comenzar el proceso de instalación, si está actualizando Apache.

13.5 Instalación de un servidor seguro con Red Hat Linux

Si está instalando Red Hat Linux y secure Web server al mismo tiempo siga las instrucciones proporcionaddas por el manual de instalación de su arquitectura. Si quiere utilizar su sistema Red Hat Linux

como servidor seguro, deberá realizar una instalación de tipo servidor o personalizado. Los diferentes tipos de instalación entre los que puede escoger son los que siguen a continuación:

- Si elige una instalación de tipo servidor, los paquetes de servidor seguro (`apache`, `mod_ssl` y `openssl`) serán seleccionados automáticamente. Los paquetes `stunnel` y `openssh`, que otorgan funciones de seguridad, también serán seleccionados.
- Si elige una instalación de tipo estación de trabajo, los paquetes de servidor seguro y paquetes relativos a seguridad no serán seleccionados para la instalación automáticamente, pero podrá elegir instalarlos durante el proceso de personalización de la selección de paquetes.
- Si elige una instalación de clase personalizada, una vez que haya revisado qué paquetes serán instalados, tendrá que seleccionar los paquetes de servidor seguro y los paquetes de seguridad que desea.

Una vez que haya elegido un tipo ed instalación, siga las instrucciones de instalación para configurar y particionar su sistema. Cuando llegue a la sección de selección de grupos de paquetes, o componentes, seleccione el grupo de paquetes **Servidor Web**. El **Servidor Web** incluye los paquetes `apache` y `mod_ssl` que debe instalar para iniciar el servidor seguro. Ya que `mod_ssl` es dependiente del paquete `openssl`, `openssl` deberá elegirse para la instalación.

Si desea instalar cualquier paquete adicional relativo a seguridad descrito en la Sección 13.3, *Introducción a los paquetes relacionados con la seguridad*, deberá identificar esos paquetes con programa de instalación. Para hacerlo, elija **Selección individual de paquetes** en la misma pantalla que **Selección de paquetes en grupo**.

Seleccione los paquetes relativos a seguridad que quiera instalar según las instrucciones dadas en el manual de instalación. Para ayudarle a encontrarlos se suministra una tabla con sus localizaciones en la Tabla 13–1, *Paquetes seguros*.

Después de asegurarse de que los paquetes que necesita son seleccionados, continúe con el proceso de instalación. Cuando haya acabado de instalar Red Hat Linux y el servidor seguro, vea la Sección 13.9, *Introducción a certificados y seguridad*.

13.6 Actualización desde una versión previa de Red Hat Linux

Si ya está ejecutando una versión previa de Red Hat Linux en su sistema, puede escoger actualizar Red Hat Linux 7.1(en lugar de realizar una instalación completa). Si decide actualizarlo, debe escoger **Actualización** en vez de escoger un tipo de instalación. Siga las instrucciones sobre como actualizar su sistema proporcionadas por el manual apropiado para su arquitectura. Durante la instalación, necesitará asegurarse de que los paquetes de servidor seguro son seleccionados por el programa de instalación.

Cuando ejecute una actualización de su sistema Red Hat Linux, el programa de instalación comprueba los paquetes que ya están instalados. Éstos, vendrán actualizados automáticamente en las versiones incluídas en Red Hat Linux 7.1 durante el proceso de actualización. No obstante, si no tiene un paquete en particular instalado, el programa de instalación no instalará la nueva versión del paquete — a menos que personalice su actualización.

Si está actualizando desde Red Hat Linux 7.0 o posterior y tiene los paquetes de secure Web server instalados, el proceso de actualización actualizará los paquetes de servidor seguro. Si está actualizando desde Red Hat Linux 7.0 o posterior, pero no tiene instalados los paquetes secure Web server, necesitará seleccionar los paquetes `apache`, `mod_ssl` y `openssl` durante el proceso de personalización de paquetes. Para indicaciones sobre la localización de los paquetes que necesitará escoger, consulte la Sección 13.6.1, *Personalizar su actualización para instalar el servidor seguro*.

Si está actualizando desde la versión US/Canada de Red Hat Linux Professional, necesitará personalizar su actualización y elegir los paquetes de seguridad para el servidor a instalar. Puede que ya tenga instalado `apache`, pero `mod_ssl` y `openssl` no serán instalados (ya que no están incluidos en versiones de Red Hat Linux anteriores a Red Hat Linux 7.1). Necesitará personalizar la actualización para elegir al menos `mod_ssl` y `openssl`. Vea la Sección 13.6.1, *Personalizar su actualización para instalar el servidor seguro* para consultar instrucciones sobre la localización de paquetes que necesita elegir.

Si está actualizando desde una versión internacional de Red Hat Linux Professional y tenía los paquetes `apache`, `mod_ssl` y `openssl` instalados, el programa de instalación seleccionará y actualizará estos programas automáticamente.

Si se encuentra actualizando desde una versión de Red Hat Linux Professional, pero no tenía instalados los paquetes `apache`, `mod_ssl` o `openssl`, necesitará personalizar su actualización y elegir instalar estos paquetes. Vea la Sección 13.6.1, *Personalizar su actualización para instalar el servidor seguro* para consultar instrucciones sobre la localización de paquetes que necesita elegir.

13.6.1 Personalizar su actualización para instalar el servidor seguro

Si necesita personalizar el proceso de actualización, siga las instrucciones de actualización contenidas en la *Official Red Hat Linux Installation Guide*;, básicamente, elija **Actualización** como **Tipo de Instalación** y seleccione después **Personalización de paquetes para que sean actualizados**. Necesitará seleccionar los paquetes a actualizar, como se describe en Official Red Hat Linux x86 Installation Guide. Para recibir ayuda en su selección, la Tabla 13–1, *Paquetes seguros* le aporta la localización de cada paquete en relación con el servidor seguro y si este paquete es opcional.

Cuando haya acabado, si también está actualizando cualquier versión de Apache, vea la Sección 13.8, *Actualización desde una versión previa de Apache*. Si no está actualizando Apache, continúe en la Sección 13.9, *Introducción a certificados y seguridad*.

13.7 Instalación del servidor seguro después de la instalación de Red Hat Linux

Si ha instalado Red Hat Linux 7.1 sin los paquetes relacionados con la seguridad del servidor y un tiempo después decide que quiere instalar un servidor seguro, lo podrá hacer. La forma más fácil de llevarlo a cabo es usar RPM, Gnome-RPM, o Kpackage para instalar los paquetes RPM incluidos en el CD de Red Hat Linux.

13.7.1 Detener procesos del servidor Web

Antes de iniciar este proceso, si está funcionando algún servidor Web sobre su sistema, deberá detener el proceso el servidor antes de instalar secure Web server. Si es un servidor Web Apache el que se está ejecutando, detenga el proceso del servidor procediendo con uno o ambos de los siguientes comandos:

```
/etc/rc.d/init.d/httpsd stop
/etc/rc.d/init.d/httpd stop
```

13.7.2 Uso de Gnome-RPM o Kpackage

Si está ejecutando GNOME o KDE, podrá usar un programa gráfico GUI como Gnome-RPM o Kpackage para instalar los paquetes de servidor seguro.

Encontrará más información sobre el uso de Gnome-RPM en el Gnome-RPM y en la *Official Red Hat Linux Getting Started Guide*. Las instrucciones para el uso de Kpackage se incluyen en la página web del *Kpackage Handbook* que encontrará en http://www.general.uwa.edu.au/u/toivo/kpackage/.

Una vez que haya instalado los paquetes necesarios, el siguiente paso es el de crear una clave y obtener un certificado. ContinÚE leyendo la Sección 13.9, *Introducción a certificados y seguridad*.

13.7.3 Uso de RPM

Los paquetes secure Web server vienen proporcionados en formato RPM format, de manera que puede instalar los paquetes mediante el uso de RPM. Vea la *Official Red Hat Linux Customization Guide* para más información sobre la aplicación RPM. Consulte la Tabla 13–1, *Paquetes seguros* si no está seguro de qué paquetes desea instalar.

Después de haber instalado los paquetes de servidor seguro, si está acutualizando cualquier versión de Apache, consulte la Sección 13.8, *Actualización desde una versión previa de Apache*. Si no está actualizando Apache, continúe con la Sección 13.9, *Introducción a certificados y seguridad*.

13.8 Actualización desde una versión previa de Apache

Durante la instalación de paquetes de servidor seguro, si está actualizando Apache, necesitará tener en cuenta dos cosas:

- En la versión de Apache incluida en Red Hat Linux 7.1, el comando `DocumentRoot` es `/var/www/html`.
- Si ha personalizado el archivo de configuración de Apache (`httpd.conf`), querrá saber qué sucederá con sus personalizaciones durante el proceso de actualización.

13.8.1 ¿Dónde está el DocumentRoot?

Básicamente, el `DocumentRoot` es el directorio de su sistema que mantiene la mayoría de las páginas web atendidas por su servidor Web Apache. El `DocumentRoot` es convertido por una directiva de configuración en fichero de configuración de Apache, `httpd.conf`. Si no está familiarizado con la directiva de configuración de `DocumentRoot`, consulte la Sección 14.2.28, *`DocumentRoot`* , para una explicación más detallada.

En versiones previas a Red Hat Linux 7.0, el servidor de Apache proporcionado por Red Hat Linux, usaba `/home/httpd/html`como `DocumentRoot`. En la versión por defecto (sin-seguridad) del fichero de configuración de Apache, el `DocumentRoot` es `/usr/local/apache/htdocs`. También es posible que usted (o alguien, previamente) usara un `DocumentRoot` completamente diferente. El punto importante es — en Red Hat Linux 7.1 el `DocumentRoot` será ahora `/var/www/html`.

¿Esto es de su incumbencia? Por supuesto, si usó una versión previa de Apache para atender páginas web. Cualesquiera páginas web que sean servidas previamente desde un `DocumentRoot` diferente, no serán encontradas (o servidas) por Apache lanzado con Red Hat Linux 7.1 en su configuración por defecto. Necesitará seguir uno de los siguientes pasos:

Mueva todos los archivos del antiguo `DocumentRoot` (`/home/httpd/html`, `/usr/local/apache/htdocs`, o donde se encuentre) hacia el nuevo (`/var/www/html`).

o

modifique el fichero de configuración de Apache y cambie todas las referencias al `DocumentRoot` que llevan a la ruta del directorio anterior.

La solución que elija dependerá de la configuración de su sistema. Generalmente, si usted ha montado `/home` en su sistema, no querrá tener el `DocumentRoot` en `/home`. Por otra parte, si no dispone de mucho espacio en `/var`, probablemente tampoco querrá el `DocumentRoot` en `/var`. Usted, o el administrador de sistema, tendrá que decidir cual será la mejor solución basándose en la configuración de su sistema y las necesidades de su servidor Web. La configuración por defecto de secure Web server

intentará direccionar a la mayoría de los Webmasters; desafortunadamente, no podremos configurarlo para cada situación.

13.8.2 ¿Qué le ocurrirá a mi antiguo fichero?

Si usted tiene otra versión de Apache instalada con sus ficheros de configuración personalizados por usted mismo, los ficheros de configuración serán salvados en sus directorios con la extensión de `.rpmsave` durante la instalación de Apache. Si dispone de otra versión de Apache instalada pero usted nunca alteró los ficheros de configuración, estos serán sobreescritos durante la instalación de este producto.

Después de instalar Apache, podrá cortar y pegar sus configuraciones personalizadas desde su antiguo fichero de configuración de Apache (`httpd.conf.rpmsave`) en su nuevo fichero de configuración `httpd.conf` para la seguridad de su servidor. Observe que si va a utilizar la herramienta de configuración de Apache, no debería modificar `httpd.conf` a mano. Consulte la *Official Red Hat Linux Customization Guide* para más información sobre la herramienta de configuración Apache.

13.9 Introducción a certificados y seguridad

Su secure Web server le proporciona seguridad mediante el uso de una combinación del protocolo SSL (Secure Sockets Layer) y (en la mayoría de casos) un certificado digital de una CA (Certificate Authority). SSl gestiona las comunicaciones encriptadas y la autentificación mutua entre navegadores y su secure Web server. El certificado digital aprovado por la CA proporciona autentificación para su secure Web server (la CA pospone la reputación a la certificación de la identidad de su organización). Cuando su navegador se esté comunicando mediante el uso de la encriptación SSL, verá el prefijo https:// al inicio del Uniform Resource Locator (URL) en la barra de navegación.

La encriptación depende del uso de las claves (piense en ellas como anillos de codificador/descodificador secreto en formato data). En la criptografía convencional o simétrica, ambos finales de la transacción tienen la misma clave, que usan para descodificar cada una de las otras transmisiones. En la criptografía pública o asimétrica, coexisten dos claves: una clave pública y una clave privada. Una persona o una organización mantiene su clave privada en secreto y publica su clave pública. Los datos codificados con la clave pública sólo pueden ser descodificados con una clave privada; mientras que los datos codificados con la clave privada pueden sólo ser descodificados con la clave pública.

Para configurar su servidor seguro, utilizará criptografía pública para crear una clave para pública y privada. En la mayoría de los casos, enviará su petición de certificado (incluyendo su clave pública), la prueba de la identidad de la compañía y el pago a CA. La CA verificará la petición de certificado y su identidad y le devolverá un certificado a su secure Web server.

Un servidor seguro usa un certificado para identificarse con los navegadores de Web. Puede generar su propio certificado (conocido como certificado "auto-firmado") o puede obtener un certificado de

una Autoridad de Certificado o CA. Un certificado de una CA con buena reputación le garantiza que un sitio web está asociado con una compañía en particular o una organización.

Alternativamente, puede crear su propio certificado "auto-firmado". Observe que los certificados auto-firmados no se deberían usar en la mayoría de entornos de producción. Los certificados auto-firmados no serán automáticamente aceptados por el navegador del usuario — el navegador preguntará al usuario si quiere aceptar el certificado y crear una conexión segura. Consulte la Sección 13.11, *Tipos de certificados* para más información sobre las diferencias entre certificados auto-firmados y firmados por CA.

Una vez que tenga un certificado auto-firmado o un certificado firmado por la CA que haya elegido, necesitará instalarlo en su secure Web server.

13.10 Uso de claves pre-existentes y certificados

Si ya tiene una clave y un certificado existente (por ejemplo, si está instalando el secure Web server para reemplazar un producto del servidor de Web seguro de otra compañía), podrá utilizar su clave existente y certificarla con el secure Web server. En las dos situaciones siguientes, no podrá usar su clave y el certificado existente:

- *Si está cambiando su dirección IP o nombre de dominio* — No puede usar su clave y certificado antiguos. Los certificados son para una dirección IP y nombre de dominio par en particular. Necesitará obtener un certificado nuevo si está cambiando su dirección IP o nombre de dominio.
- *Si tiene un certificado de VeriSign y está cambiando el software del servidor* — VeriSign es una CA ampliamente usada. Si ya tiene un certificado VeriSign que utiliza para otro propósito, estará considerando la posibilidad de utilizar su certificado VeriSign existente con su nuevo secure Web server. No obstante, no se le permitirá, porque VeriSign emite certificados para un software de servidor particular y una combinación de dirección IP/nombre de dominio.

  Si cambia alguno de eso parámetros (por ejemplo, si usa previamente otro producto de servidor Web seguro y en este momento desea utilizar el secure Web server), el certificado VeriSign que obtuvo para usarlo con la configuración anterior no funcionará con la nueva configuración. Necesitará obtener un certificado nuevo.

Si tiene una clave y un certificado ya existente, no tendrá que generar una clave nueva y obtener un certificado nuevo. Sin embargo, necesitará cambiar y renombrar los archivos que contienen su clave y certificado.

Traslade el archivo de clave existente a:

```
/etc/httpd/conf/ssl.key/server.key
```

Traslade el archivo de certificado a:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Tras haber trasladado su clave y certificado, consulte la Sección 13.15, *Prueba de su certificado*.

Si está actualizando desde las versiones 1.0 y 2.0 del servidor Web seguro de Red Hat, Su clave (`httpsd.key`) y certificado (`httpsd.crt`) antiguos estarán ubicados en `/etc/httpd/conf/`. Necesitará trasladar y renombrar su clave y su certificado, para que el secure Web server pueda utilizarlos. Utilice los dos comandos siguientes para trasladar y renombrar sus archivos de clave y de certificado:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

Inicie su secure Web server como se describe en la Sección 14.1, *Arranque y apagado del* `httpd`. No debería necesitar obtener un nuevo certificado, si está actualizando desde una versión anterior al secure Web server.

13.11 Tipos de certificados

Si ha instalado su secure Web server mediante el uso del programa de instalación de Red Hat Linux, una clave de acceso y un certificado de prueba son generados y ubicados den directorios apropiados. Sin embargo, antes de que empiece a usar su servidor seguro, necesitará generar su propia clave y obtener un certificado que identifique su servidor correctamente.

Necesita una clave y un certificado para ejecutar su secure Web server — lo que significa que puede generar un certificado auto-firmado o comprar un certificado firmado por CA desde una CA. ¿Qué diferencias existen entre ambos?

Un certificado firmado por CA le proporciona a su servidor dos capacidades importantes:

- Los navegadores reconoceran (habitualmente) de forma automática el certificado y permitirán que se realice una conexión segura, sin avisar al usuario.
- Cuando una CA emite un certificado firmado, se garantiza la identidad de la organización que le proporciona las páginas Web al navegador.

Si el público en masa puede acceder a su servidor seguro, su secure Web server necesita un certificado firmado por una CA, para que la gente que visita su sitio web, pueda confiar en que el sitio pertenece a la organización que dice poseerlo. Antes de firmar un certificado, una CA verifica que la organización que pide el certificado es, de hecho, la que dicen ser.

La mayoría de navegadores Web que soportan SSL tienen una lista de CAs cuyos certificados aceptarán automáticamente. Si un navegador encuentra un certificado cuya CA de autorización no está en la lista, el navegador le pedirá al usuario que escoja si acepta o no la conexión.

Puede generar un certificado auto-firmado para su secure Web server, pero sepa que un certificado auto-firmado no le proporcionará la misma funcionalidad que un certificado firmado por una CA. Un certificado auto-firmado no será reconocido automáticamente reconocido por los navegadores de los

usuarios y no proporciona ninguna garantía referente a la identidad de la organización que proporciona el sitio. Un certificado firmado por una CA provee a un servidor seguro de ambas capacidades. Si utiliza su servidor seguro en un entorno de producción, probablemente necesitará un certificado firmado por una CA.

El proceso de obtención de un certificado desde una CA es bastante fácil. A continuación sigue una vista preliminar:

1. Creación de un par de claves públicas y privadas encriptadas.
2. Creación de una petición de certifificado basado en una clave pública. La petición de certificado contiene información sobre su servidor y la compañía que lo albergue.
3. Envío de una petición de certificado a una CA, junto a los documentos que demuestran su identidad. No le podemos decir qué autoridad de certificado escoger. Su elección se basará en sus experiencias pasadas, o en las experiencias de sus amigos y colegas, o simplemente en factores económicos.

   Para ver una lista de CAs, pulse el botón **Seguridad** en su barra de herramientas Navigator o en el icono de candado en la parte izquierda de abajo de la pantalla. A continuación haga click en **Señaladores** para ver una lista de señaladores de certificado desde los cuales su navegador aceptará certificados. También puede buscar el Web para las CAs. Una vez que se haya decidido por un CA, necesitará seguir con las instrucciones proporcionadas sobre cómo obtener un certificado.
4. Cuando la CA comprueba que usted es quien dice ser, se le enviará un certificado digital.
5. Instale este certificaddo en su servidor Web y empiece a realizar transacciones seguras.

Si obtiene un certificado de una CA o genera su propio certificado auto-firmado, el primer paso es generar una clave. Consulte la Sección 13.12, *Generar una clave* para más instrucciones sobre cómo generar una clave.

13.12 Generar una clave

En primer lugar, teclee `cd` en el directorio `/etc/httpd/conf`. Sustituya la clave y el certificado falsos que se han generado durante la instalación con los siguientes comandos:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

A continuación, necesita crear su propia clave de acceso. Teclee el siguiente comando:

```
make genkey
```

Su sistema visualizará un mensaje similar al siguiente:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
```

```
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Introduzca una contraseña. Para más seguridad, su contraseña debería contener al menos ocho caracteres, incluya números y/o puntuación, no puede ser una palabra de diccionario. Recuerde que su contraseña es sensible a mayúsculas y minúsculas.

Nota

Necesitará recordar e introducir esta contraseña cada vez que inicie se secure Web server, de manera que no la olvide.

Se le pedirá re-escribir la contraseña, para verificar que es correcta. Una vez que haya la haya escrito correctamente, se creará un archivo llamado `server.key` que contiene su clave.

Si no desea introducir la contraseña cada vez que inicie su secure Web server, necesitará usar los siguientes dos comandos en lugar de `crear genkey`. Ambos deberían escribirse en la misma línea.

Utilice el siguiente comando:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

para crear su clave. Utilice ahora este otro comando:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

para asegurarase que los permisos están configurados correctamente en su clave.

Después de haber usado los comandos precedentes para crear su clave, no necesitará usar una contraseña para iniciar su secure Web server.

Deshabilitar la característica de la contraseña de su servidor Web seguro es un resgo para la seguridad. NO le recomendamos que lo haga.

Los problemas relacionados con el hecho de no usar una contraseña se deben al mantenimiento de la seguridad de la máquina host. Por ejemplo, si alguien compromete la seguridad habitual de UNIX en la máquina host, esa persona podría obtener su clave privada (el contenido de su archivo `server.key`). La clave podría ser usada para servir páginas Web que parecerán ser de su servidor Web.

Si las prácticas de seguridad UNIX se mantienen rigurosamente en el ordenador host (todos los parches y actualizaciones del sistema operativo son instalados tan pronto como están disponibles, no se ejecutan servicios innecesarios o de riesgo, etc), la contraseña de su the secure Web server le parecerá innecesaria. No obstante, ya que su secure Web server no debería necesitar ser re-arrancado muy a menudo, la seguridad extra proporcionada por el hecho de tener que introducir la contraseña es un esfuerzo que vale la pena en la mayoría de los casos.

El archivo `server.key` debería ser poseído por el usuario root en su sistema y no debería ser accesible a ningún otro usuario. Haga una copia de seguridad de este archivo y guarde dicha copia en un lugar seguro. Necesita una copia de seguridad por si pierde alguna vez el archivo `server.key` tras usarlo para crear su petición de certificado, su certificado no funcionará más y la CA no podrá ayudarle. Su única opción será pedir (y pagar) un nuevo certificado.

Si va a comprar a una CA, vaya a la Sección 13.13, *Generar una petición de certificado para enviar a una CA*. Si ha generado su propio certificado auto-firmado, vaya a la Sección 13.14, *Creación de un certificado auto-firmado*.

13.13 Generar una petición de certificado para enviar a una CA

Una vez que haya creado una clave, el siguiente paso es el de generar una petición de certificado que necesitará enviar a la CA que haya escogido. Introduzca el siguiente comando:

```
make certreq
```

Su sistema visualizará la siguiente salida y le pedirá su contraseña (a menos que haya deshabilitado la opción de contraseña)

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Introduzca la contraseña que ha escogido al generar la clave. Su sistema visualizará algunas instrucciones y le pedirá una serie de respuestas. Sus entradas se incorporarán a la petición de certificado. La visualización, con repuestas de ejemplo, se parecerán a esto:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.mydomain.com
Email Address []:admin@mydomain.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Las respuestas predeterminadas aparecen entre paréntesis `[]` inmediatamente después de cada petición de entrada. Por ejemplo, la primera información requerida es el nombre del país donde se utilizará el certificado, que aparecerá de la siguiente manera:

```
Country Name (2 letter code) [AU]:
```

La entrada por defecto, entre paréntesis, es **AU**. Para aceptarla, pulse [Intro], o compile el código de su país con dos letras.

Deberá teclear en el resto de entradas el (`Estado o provincia`, el `Nombre de la localidad`, el `Nombre de la organización`, el `Nombre del la unidad de orgnización`, el `Nombre común`, y la `dirección de email`). Con esto bastaría, pero necesita seguir unas pautas:

- No abrevie la localidad o el estado. Escríbalos enteros (por ejemplo, St. Louis debería ser escrito como Saint Louis).
- Si envia este CRS a la CA, asegúrese de proporcionar la información correcta para todos los campos, pero especialmente en el `Nombre de organización` y el `Nombre común`. Las CAs prueban la información proporcionada en el CSR para determinar si su organización se hace responsable de lo que usted ha escrito como `Nombre común`. CAs rechaza los CSRs que incluyen información que perciben como incorrecta.
- Para el `Nombre común`, asegúrese de que escribe el nombre *real* de su secure Web server (un nombre DNS válido) y ningún alias que pueda tener el servidor.
- La `dirección de email` debería ser la dirección de email de la webmaster o del administrador del sistema.
- Evite caracteres especiales como @, #, &, !, etc. Algunas CAs rechazarán una petición de certificado que contenga un carácter especial. Si el nombre de su compañía incluye una e comercial, deletréela como "y", en lugar de "&".

- No utilice ninguno de los datos extra (`Una contraseña por desafío` y `Un nombre de compañía opcional`). Para continuar sin introducir estos campos, pulse [Intro] para aceptar ambos campos en blanco por defecto.

Cuando haya finalizado de introducir su información, se creará un archivo llamado `server.csr`. Este archivo es su petición de certificado, preparada para ser enviada a su CA.

Cuando se haya decidido por una CA, siga las instrucciones proporcionadas en el sitio web. Éstas le dicen cómo enviar su petición de certificado y cualquier otra documentación que requieran , así como el pago.

Después de haber cumplido con todos los requisitos, le enviarán un certificado (habitualmente vía email). Guarde (o haga copiar y pegar) el certificado que le han enviado como `/etc/httpd/conf/ssl.crt/server.crt`.

13.14 Creación de un certificado auto-firmado

Puede crear su propio certificado auto-firmado. Observe que un certificado auto-firmado no le proporcionará las garantías de seguridad que le proporciona un certificado firmado por una CA. Consulte la Sección 13.11, *Tipos de certificados* para más información sobre certificados.

Si desea crear su propio certificado auto-firmado, necesitará crear una clave de acceso usando las instrucciones proporcionadas en la Sección 13.12, *Generar una clave*. Una vez que tenga una clave, utilice el siguiente comando:

```
make testcert
```

Verá lo siguiente y se le pedirá su contraseña (a menos que genere una clave sin una contraseña):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Uso de la configuración desde /usr/share/ssl/openssl.cnf
Introduzca la frase del pase PEM:
```

Después de introducir su contraseña, se le pedirá más información. La información será del tipo de la que encontrará a continuación (deberá proporcionar la información correcta de su organización y de su host):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.mydomain.com
Email Address []:admin@mydomain.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Después de haber proporcionado la información correcta, será creado y ubicado en `/etc/httpd/conf/ssl.crt/server.crt` un certificado auto-firmado. Necesitará reiniciar su servidor seguro después de generar el certificado. Consulte la Sección 14.1, *Arranque y apagado del* `httpd` para más instrucciones sobre el reinicio de su servidor Web seguro.

13.15 Prueba de su certificado

Cuando el programa de instalación Red Hat Linux instala el servidor seguro, crea también una clave de acceso y un certificado genérico de prueba. Para cualquier otro propósito, necesitará obtener un certificado desde una CA o generar un certificado auto-firmado. Consulte la Sección 13.11, *Tipos de certificados* si necesita más información sobre los tipos diferentes de certificados disponibles.

Si ha comprado un certificado desde una CA o generado un certificado auto-firmado, debería tener un archivo llamado `/etc/httpd/conf/ssl.key/server.key` que contenga su clave y un archivo `/etc/httpd/conf/ssl.crt/server.crt` que contenga su certificado. Si su clave y certificado están en otro en algún otro sitio, trasládelas a estos directorios. Si ha cambiado cualquiera de las localizaciones por defecto, debería introducir estos dos archivos en el directorio adecuado, basándose en sus modificaciones.

Detenga y reinicie su servidor como se describe en la Sección 14.1, *Arranque y apagado del* `httpd`. Si su archivo clave está encriptado, se le pedirá la contraseña. Introduzca su contraseña y su servidor debería empezar.

Indique su navegador Web a la página inicial. El URL para acceder a su secure Web server será parecido a lo que sigue a continuación:

```
https://your_domain
```

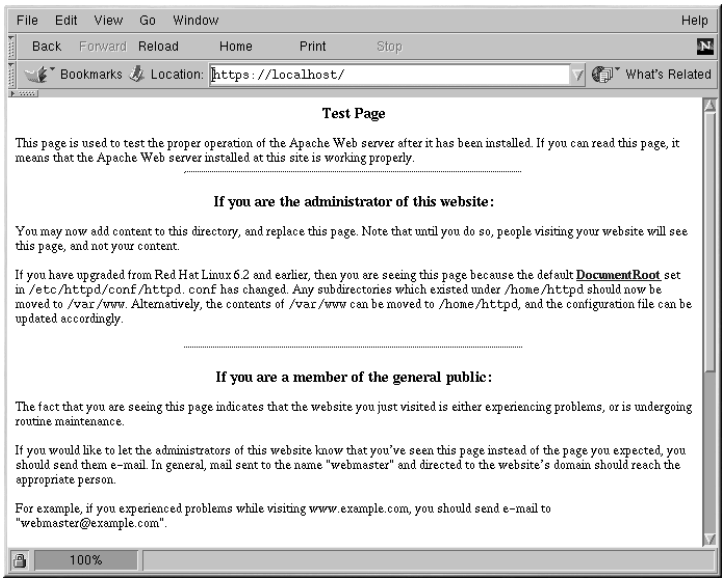
Nota

Observe la "s" después de "http." Los https: el prefijo se usa para asegurar las transacciones seguras HTTP.

Si está utilizando un certificado firmado por CA de una CA conocida, su navegador aceptará probablemente de forma automática el certificado (sin indicar su entrada) y crear una conexión segura. Su navegador no reconocerá una prueba o un certificado auto-firmado, porque el certificado no está firmado por una CA, siga las instrucciones proporcionadas por su navegador para aceptar el certificado. Si pulsa **Siguiente** hasta que finalicen los diálogos, aceptará por defecto.

Una vez que su navegador acepte el certificado, su secure Web server le mostrará una página inicial por defecto como se muestra en el Gráfico 13–1, *Página inicial predeterminada*.

Gráfico 13–1 Página inicial predeterminada



13.16 Acceso a su servidor seguro

Para acceder a su servidor seguro, utilice una URL como el siguiente:

```
https://your_domain
```

Observe que las URLs que están pensados para conectarse a su secure Web server, deberían empezar con el indicador de protocolo https: en lugar de un indicador de protocolo http:.

Se puede acceder a un servidor no seguro usando una URL del género:

```
http://your_domain
```

El puerto estándar para un transmisor Web seguro es el puerto 443. El puerto estándar para comunicaciones Web inseguras es el puerto 80. La configuración por defecto de secure Web server escucha los dos puertos estándar. Por lo tanto, no necesitará especificar el número de puerto en una URL (se asume el nombre del puerto).

No obstante, si configura su servidor para escuchar un puerto no estándar (p.e., cualquier cosa alrededor de 80 o 443), necesitará especificar el número de puerto en cada URL que esté pensada para conectarse al servidor en un puerto no-estándar.

Por ejemplo, si ha configurado su servidor de manera que tenga un host virtual inseguro ejecutándose en un puerto 12331. Cualquier URLs pensada para conectarse a un host virtual debe especificar el número de puerto in la URL. El siguiente ejemplo de URL intentará conectarse con un servidor Web inseguro escuchando un puerto 12331:

```
http://your_domain:12331
```

Algunos de los ejemplos de URLs usados en este manual pueden necesitar un cambio, dependiendo de si usted accede a su secure Web server explícitas que funcionarán en cualquier circunstancia.

13.17 Recursos adicionales

Si ha seguido los pasos indicados en el Capítulo 13, *Uso de Apache como servidor Web seguro* pero ha surgido algún problema, lo primero que debería hacer es consultar la la sección de Erratas de Red Hat en el sito web de Red Hat en http://www.redhat.com/support/errata.

Si ha comprado un producto oficial Red Hat con soporte, dispone de soporte técnico. Asegúrese de visitar el sitio web de soporte de Red Hat en http://www.redhat.com/support para registrarse y, de esta manera, obtener soporte técnico.

Si quiere suscribirse a la lista de correo de servidor-seguro-redhat, vaya a http://www.redhat.com/mailing-lists.

También se puede suscribir a dicha lista enviando un email a `redhat-secure-server-request@redhat.com` e incluyendo la palabra "suscripción" (sin las comillas) en la línea de Objeto.

13.17.1 Documentación instalada

Si instaló el paquete `apache-manual`, podrá acceder a la documentación Apache en formato HTML en su máquina desde la siguiente URL: http://localhost/manual/.

La documentación mod_ssl la encontrará en el siguiente URL: http://localhost/manual/mod/mod_ssl/.

13.17.2 Sitios Web útiles

Las advertencias, las FAQs y los documentos HOWTO los encontrará en el sitio Web de Red Hat en http://www.redhat.com/support/docs/howto.

La base centralizada de conocimiento Apache de Red Hat Linux está disponible en http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html.

El sitio Web Apache proporciona una documentación completa para el servidor Web Apache en http://httpd.apache.org/docs.

El sitio Web mod_ssl website (http://www.modssl.org) es la fuente definitiva de información sobre mod_ssl. Incluye documentación abundante y un *Manual del usuario* en http://www.modssl.org/docs.

13.17.3 Libros relacionados

Apache: The Definitive Guide, secunda edición, de Ben Laurie y Peter Laurie, O'Reilly & Associates, Inc.

14 Módulos y directivas de Apache

Podemos decir que la configuración predeterminada de Apache se adapta a los sistemas de todos los tipos de usuarios. Por ello no es necesario que cambie las directivas de la configuración de Apache. Si desea cambiar algunas de las opciones predeterminadas de la configuración necesita concerlas y saber dónde se encuentran. Para ello lea atentamente este capítulo.

ADVERTENCIA

Si desea utilizar la Herramienta de configuración Apache, utilidad GUI que se encuentra en el paquete de Red Hat Linux no cambie el fichero `httpd.conf` fichero de configuración del servidor web Apache. Por el contrario, si desea cambiar el `httpd.conf` a mano, no use la Herramienta de configuración Apache.

Si desea más información sobre la Herramienta de configuración Apache, consulte la versión española de la *Official Red Hat Linux Customization Guide*.

Tras haber instalado el paquete `apache` podrá encontrar la documentación sobre el servidor de web Apache en el sitio http://your_domain/manual/ o via web en el sitio http://httpd.apache.org/docs/. La documentación del servidor de web Apache contiene descripciones completas y detalladas de todas las opciones de configuración. Para facilitarle la tarea, este capítulo contiene pequeñas descripciones de las directivas de configuración utilizadas en la versión Apache que se encuentra en el paquete de Red Hat Linux.

Cuando lea el fichero de configuración del servidor de Web, tenga en cuenta que la configuración predeterminada incluye tanto el servidor de web seguro como el no seguro. El servidor seguro se ejecuta como una máquina virtual, que aparece configurada en el fichero `httpd.conf`. Para más información sobre máquinas virtuales, vea la Sección 14.4, *Utilización de máquinas virtuales*.

Nota

No se incluyen extensiones FrontPage porque la licencia Microsoft (TM) prohibe la inclusión de extensiones en productos de otras compañías.

14.1 Arranque y apagado del `httpd`

Durante el proceso de instalación, en el `/etc/rc.d/init.d` se ha salvado un script de la shell "bourne" con el nombre `httpd`. Para arrancar y apagar su servidor manualmente, ejecute `httpd` tanto con el argumento `apagar` como con `arrancar`.

Para arrancar su servidor, teclee el comando:

```
/etc/rc.d/init.d/httpd start
```

Si está ejecutando Apache como servidor seguro, se le pedirá que introduzca la contraseña. Después, su servidor arrancará.

Para apagar su servidor, teclee el comando:

```
/etc/rc.d/init.d/httpd stop
```

El comando `reanudar` es una manera más corta para apagar y luego reanudar su servidor. El comando `reanudar` apaga y reanuda su servidor de manera que se le pedirá su contraseña si su servidor Apache es un servidor seguro. El comando `reanudar` tiene el siguiente aspecto:

```
/etc/rc.d/init.d/httpd restart
```

Si ha terminado de modificar alguna cosa en el fichero `httpd.conf`, no necesita apagar y reanudar su servidor.Simplemente, utilice el comando `recargar`. Cuando use el comando `recargar`, no tendrá que teclear su contraseña la cual se necesita en el caso esté usando el servidor Apache como un servidor seguro.Durante las recargas se mantendrá su contraseña pero no ocurrirá cuando apague y arranque el servidor. El comando `recargar` tiene el siguiente aspecto:

```
/etc/rc.d/init.d/httpd reload
```

El proceso de ejecución del comando `httpd` comienza automáticamente cuando se arranca el ordenador ya que está predeterminado. Si está usando el servidor Apache como un servidor seguro se le pedirá la contraseña despué de que arranque el ordenador a no ser que haya generado una clave para su servidor seguro sin crear la contraseña de protección.

14.2 Directivas de configuración en el fichero `httpd.conf`

El archivo de configuración del servidor Web Apache es `/etc/httpd/conf/httpd.conf`. El archivo `httpd.conf` está bien comentado y es bastante autoexplicativo. La configuración predeterminada de secure Web server funciona para los ordenadores de la mayoría de los usuarios, así que probablemente no necesitará cambiar ninguna de las directivas en el fichero `httpd.conf`. Sin embargo, quizás quiera conocer el resto de las opciones de configuración más importantes.

Los ficheros vacíos `srm.conf` y `access.conf` se encuentran en el directorio `/etc/httpd/conf`. Precisamente estos ficheros junto con el fichero `httpd.conf` se utilizaron anteriormente como ficheros de configuración de Apache.

Si necesita configurar Apache sólo tiene que modificar el fichero `httpd.conf` y después recargar o bien apagar y arrancar el proceso del comando `httpd`. Para mayor información consulte la Sección 14.1, *Arranque y apagado del `httpd`*.

Antes de modificar el fichero `httpd.conf` debe de copiar el fichero original dándole por ejemplo, el nombre `httpd.confold` u otro cualquiera. Si comete un error mientras está modificando el fichero de configuración, no se preocupe porque siempre dispone de una copia de seguridad.

Si comete un error y su servidor de web no funciona correctamente, el primer sitio donde acudir es lo que acaba de modificar en `httpd.conf`. Asegúrese de no haber cometido ningún gazapo. Después consulte el fichero de conexión de error (`/var/log/httpd/error_log`). Este puede ser difícil de interpretar, todo depende del nivel de experiencia. Si acaba de tener problemas, de todas formas, las últimas entradas deberían de ayudarle a saber lo que ha pasado.

Las siguientes secciones dan breves descripciones de las directivas incluídas en el fichero `httpd.conf`, ordenadas según se encuentran en él. Las descripciones no son exhaustivas. Si necesita más información, consulte la documentación de Apache en formato HTML en http://*your_domain*/manual/ o en la documentación del grupo Apache en http://www.apache.org/docs/. Para más información sobre las directivas mod_ssl, consulte la documentación incluída en formato HTML en http://*your_domain*/manual/mod/mod_ssl/, o vea el mod_ssl en el *Manual del usuario* en http://www.modssl.org/docs/2.7/.

14.2.1 `ServerType`

El comando `ServerType` puede ser tanto `inetd` como `standalone`. El servidor de web tiene como comando predeterminado el `ServerType standalone`.

Dicho comando, el `ServerType standalone` significa que el servidor arranca cuando se han llevado a cabo todas las conexiones. Por otro lado,el comando `ServerType inetd` quiere decir que arranca una nueva instancia cada vez que se produzca una conexión HTTP. Cada una de las instancias del servidor contiene la conexión y aunque acabe conexión sigue existiendo. Como puede imaginarse, la utilización del comando `inetd` no sirve para mucho. Otro problema que se presenta con este comando es que puede no funcionar correctamente según el grupo Apache. Por último, debido a que tanto Red Hat Linux y 7.1 utilizan dicho comando se necesitaría añadir otra configuración para que el comando `xinetd` arrancase el servidor. Por ello, para evitar estos problemas le aconsejamos que el comando `ServerType` sea `standalone`.

14.2.2 ServerRoot

El comando `ServerRoot` es el directorio principal donde se encuentran todos los ficheros del servidor. Tanto el servidor seguro como el no seguro utilizan un comando `ServerRoot` del `/etc/httpd`.

14.2.3 LockFile

El comando `LockFile` configura el path al fichero de bloqueo utilizado por el servidor Apache cuando se compila con `USE_FCNTL_SERIALIZED_ACCEPT` o `USE_FLOCK_SERIALIZED_ACCEPT`. No se debería de cambiar el valor predeterminado del comando `LockFile`.

14.2.4 PidFile

El comando `PidFile` nombra el archivo en el que el servidor graba su ID de proceso (pid). secure Web server está configurado para grabar su pid en `/var/run/httpd.pid`.

14.2.5 ScoreBoardFile

El comando `ScoreBoardFile` almacena información interna sobre el proceso del servidor que se utiliza para comunicar el proceso padre con los procesos hijos. secure Web server's El comando `ScoreBoardFile` se encuentra en `/var/run/httpd.scoreboard`..

14.2.6 ResourceConfig

La directiva `ResourceConfig` instruye al servidor a que lea el fichero `ResourceConfig` para buscar más directivas de configuración. La directiva `ResourceConfig` está comentada porque el servidor sólo usa `httpd.conf` para directivas de configuración.

14.2.7 AccessConfig

La directiva `AccessConfig` instruye al servidor a leer el fichero `AccessConfig` para buscar más directivas de configuración, tras haber leído el fichero `ResourceConfig`. Dicha directiva está comentada porque el servidor sólo usa `httpd.conf` para directivas de configuración.

14.2.8 Timeout

El comando `Timeout` define, en segundos, el tiempo que el servidor esperará para recibir y enviar peticiones durante la comunicación. Específicamente, el comando `Timeout` define cuánto esperará el servidor para recibir peticiones GET, cuánto esperará para recibir paquetes TCP en una petición POST o PUT y cuánto esperará entre una ACK y otra respondiendo a paquetes TCP. El comando `Timeout` está ajustado a 300 segundos, que es el tiempo apropiado para la mayoría de las situaciones.

14.2.9 `KeepAlive`

El comando `KeepAlive` determina si el servidor permitirá varias conexiones a la vez (p.e., más de una petición por conexión). `KeepAlive` puede usarse para impedir que un cliente consuma muchos recursos del servidor. El comando `KeepAlive` aparece ya en `on` por defecto, lo que significa que se permiten varias conexiones a la vez. Puede ponerse en `off` para desactivarlas. Consulte Sección 14.2.10, *`MaxKeepAliveRequests`* para conocer un método alternativo para limitar las peticiones.

14.2.10 `MaxKeepAliveRequests`

Esta directiva establece el número máximo de peticiones permitidas por cada conexión que se produzca a la vez. El Grupo Apache recomienda un valor alto, lo que mejoraría el rendimiento. El valor predeterminado del comando `MaxKeepAliveRequests` es de `100` que debería bastar en la mayoría de los casos.

14.2.11 `KeepAliveTimeout`

La directiva `KeepAliveTimeout` establece el número de segundos que el servidor esperará a la siguiente petición, tras haber dado servicio a una petición, antes de cerrar la conexión. Una vez recibida la petición, aplica la directiva `Timeout` en su lugar.

14.2.12 `MinSpareServers` y `MaxSpareServers`

El servidor Web Apache se adapta dinámicamente a la carga percibida manteniendo un número apropiado de servidores libres basado en el tráfico. El servidor comprueba el número de servidores que esperan peticiones y elimina algunos si el número es más alto que `MaxSpareServers` o crea algunos si el número de servidores es menor que `MinSpareServers`.

El valor predeterminado de `MinSpareServers` es `5` y el de `MaxSpareServers` es `20`. Estos valores predeterminados son suficientes en la mayoría de los casos. El número de `MinSpareServers` no debería de ser elevado ya que creará una gran carga incluso cuando el tráfico fuese bajo.

14.2.13 `StartServers`

`StartServers` establece cuántos procesos serán creados al arrancar. Ya que el servidor Web crea y elimina dinámicamente servidores según el tráfico, no se necesitará cambiar este parámetro. El servidor está configurado para arrancar ocho procesos al arrancar.

14.2.14 `MaxClients`

El comando `MaxClients` establece un límite al total de los procesos del servidor (es decir, clientes conectados simultáneamente) que se ejecutan a la vez. Debe mantener el comando `MaxClients` a un valor alto (el valor por defecto es 150), porque no se permitirán nuevas conexiones una vez que

se alcance el número máximo de clientes simultáneamente conectados. El valor del comando `MaxClients` no puede superar el 256 sin que se haya recompilado Apache. La principal razón de tener el parámetro `MaxClients` es evitar que un servidor errático vuelva inestable al sistema operativo.

14.2.15 MaxRequestsPerChild

El comando `MaxRequestsPerChild` establece el número máximo de peticiones que cada proceso hijo procesa antes de morir. La principal razón para tener el comando `MaxRequestsPerChild` es evitar que procesos de larga vida pierdan memoria. El valor predeterminado de `MaxRequestsPerChild` para el servidor es de `100`.

14.2.16 Listen

El comando `Listen` establece los puertos en los que secure Web server acepta las peticiones entrantes. secure Web server está configurado para escuchar en el puerto 80 para comunicaciones no seguras y (en máquinas virtuales que define el servidor seguro) en el puerto 443 para comunicaciones seguras.

Para puertos por debajo de 1024, el comando `httpd` deberá ser ejecutado como root. Para el puerto 1024 y superiores, el comando `httpd` puede ser ejecutado como si se fuera un usuario cualquiera.

El comando `Listen` también se puede usar para especificar direcciones IP específicas en las cuales aceptará conexiones el servidor.

14.2.17 BindAddress

`BindAddress` es un modo de especificar en qué direcciones IP el servidor escuchará. Debería usarse la directiva `Listen` en su lugar si se necesita esta funcionalidad. El servidor no usa el comando `BindAddress` el cual ya aparece comentado en `httpd.conf`.

14.2.18 LoadModule

El comando `LoadModule` se usa para cargar módulos Dynamic Shared Object(DSO). Para más información sobre el soprte de los DSOs de Apache y cómo usar la directiva `LoadModule`, lea Sección 14.3, *Añadir módulos a su servidor*. Nótese que el orden de los módulos es importante, así que mejor no tocarlo.

14.2.19 IfDefine

Las etiquetas `<IfDefine>` y `</IfDefine>` rodean a directivas de configuración que son aplicadas si el test aplicado a la etiqueta `<IfDefine>` resulta verdadero; las directivas no se tienen en cuenta si el test es falso.

Dicho test aplicado a la etiqueta `<IfDefine>` es un nombre de un parámetro (p.ej., `HAVE_PERL`). Si el parámetro está definido,es decir, si se da como argumento al comando de arranque del servidor,

entonces el test es verdadero. En este caso, cuando se arranca el secure Web server el test es verdadero y se aplican las directivas contenidas en las etiquetas `IfDefine`.

Por defecto, las etiquetas `<IfDefine HAVE_SSL>` rodean las etiquetas de la máquina virtual del servidor seguro. Las etiquetas `<IfDefine HAVE_SSL>` también rodean a las directivas `LoadModule` y a las `AddModule` para `ssl_module`.

14.2.20 `ClearModuleList`

El comando `ClearModuleList` se encuentra justo antes de la larga lista de directivas `AddModule`. `ClearModuleList` borra la lista interna de módulos del servidor. La lista de directivas `AddModule` recrea la lista, justo después de `ClearModuleList`.

14.2.21 `AddModule`

`AddModule` es la directiva usada para crear una lista completa de módulos disponibles. Se usa la directiva `AddModule` para añadir módulos como DSO. Para más información sobre cómo usar el comando `AddModule` para el soporte DSO, vea Sección 14.3, *Añadir módulos a su servidor*.

14.2.22 `ExtendedStatus`

La directiva `ExtendedStatus` controla si Apache genera información de estado básico (`off`) o detallada (`on`), cuando se llama al gestor `server-status`. Se llama al gestor `Server-status` utilizando la etiqueta `Location`; Para mayor información sobre cómo llamar al `server-status` consulte la Sección 14.2.71, *`Location`*

14.2.23 `Port`

Normalmente, el comando `Port` define el puerto en el que escucha el servidor. secure Web server, sin embargo, escucha en más de un puerto por defecto, ya que la directiva `Listen` también se usa. Cuando la directiva `Listen` está en uso, el servidor escucha en todos esos puertos. Consulte la descripción de `Listen` para más información sobre el comando `Listen`.

El comando `Port` también se usa para especificar el número de puerto usado para crear el nombre canónico para el servidor. Consulte la Sección 14.2.39, *`UseCanonicalName`* para más información sobre el nombre canónico del servidor.

14.2.24 `User`

La directiva `User` establece el userid usado por el servidor para responder a peticiones. El valor de `User` determina el acceso al servidor. Cualquier fichero al que no pueda acceder este usuario será también inaccesible al visitante de la web. El comando predeterminado para `User` es `apache`.

`User` debería sólo tener privilegios de tal manera que sólo puediera acceder a ficheros que se supone que todo el mundo puede ver. El comando `User` también es dueño del cualquier proceso CGI que

arranque el servidor.Al comando `User` no se le debería permitir ejecutar ningún código que no esté pensado para responder peticiones HTTP.

Nota

A menos que sepa exactamente lo que está haciendo, no utilice el comando `User` como si fuese root. Usar root para `User` creará grandes problemas de seguridad en secure Web server.

El proceso `httpd` padre se ejecuta como root durante operaciones normales, pero pasa al usuario apache inmediatamente. El servidor debe arrancar como root porque necesita un puerto por debajo de 1024 (El puerto predeterminado para comunicaciones seguras es 443; el puerto por defecto para comunicaciones no seguras es el puerto 80). Los puertos por debajo de 1024 están reservados para el sistema, así que sólo se pueden usar si se es root. Una vez que el servidor se ha conectado al puerto, pasa el proceso a `User` antes de aceptar peticiones.

14.2.25 Group

El comando `Group` es similar a `User`. `Group` establece el grupo en el que el servidor responde a las peticiones. El valor predeterminado del comando `Group` también es `apache`.

14.2.26 ServerAdmin

`ServerAdmin` debería ser la dirección de correo del administrador del secure Web server. Esta dirección de correo aparecerá en los mensajes de error generados por el servidor para páginas web,de tal manera que los usuarios pueden comunicar errores enviando correo al administrador. El comando `ServerAdmin` ya se encuentra en la dirección `root@localhost`.

Una forma buena y típica de configurar `ServerAdmin` es situarlo en la dirección `webmaster@your_domain.com`. Después cree un alias del `webmaster` para la persona responsable del servidor en `/etc/aliases`. Finalmente, ejecute `/usr/bin/newaliases` para añadir el nuevo alias.

14.2.27 ServerName

El comando `ServerName` puede usarse para establecer el nombre de la máquina del servidor diferente al nombre real de máquina como por ejemplo, usar www.your_domain.com aunque el nombre real del servidor sea foo.your_domain.com. Nótese que `ServerName` debe ser un nombre "Domain Name Service" (DNS) válido que se tenga derecho a usar (no basta con inventar uno).

Si se especifica `ServerName`, hay que asegurarse de incluir la pareja nombre-dirección IP en el fichero `/etc/hosts`.

14.2.28 `DocumentRoot`

`DocumentRoot`es el directorio que contiene la mayoría de los archivos HTML que se entregarán en respuesta a peticiones. El directorio predeterminado `DocumentRoot` para servidores seguros y no seguros es `/var/www/html`. Por ejemplo, el servidor puede recibir una petición para el siguiente documento:

```
http://your_domain/foo.html
```

El servidor buscará el fichero en el siguiente directorio por defecto:

```
/var/www/html/foo.html
```

Si se quiere cambiar `DocumentRoot` para que no lo compartan los servidores seguros y no seguros, vea Sección 14.4, *Utilización de máquinas virtuales*.

14.2.29 `Directory`

Las etiquetas `<Directory /path/to/directory>` y `</Directory>` se usan para agrupar directivas de configuración que sólo se aplican a ese directorio y sus subdirectorios. Cualquier directiva aplicable a un directorio puede usarse en las etiquetas `<Directory>`. Las etiquetas `<File>` pueden aplicarse de la misma forma a un fichero específico.

Por defecto,se aplican parámetros muy restrictivos al directorio raíz, utilizando `Options` (vea la Sección 14.2.30, *`Options`*) y `AllowOverride` (vea la Sección 14.2.31, *`AllowOverride`*). Con esta configuración, cualquier directorio del sistema que necesite valores más permisivos ha de ser configurado explícitamente.

La utilización de las etiquetas `Location`, permite al comando `DocumentRoot` (referido a `"/"`) tener parámetros menos rígidos para que el servidor sirva las peticiones HTTP.

El directorio `cgi-bin` está configurado para permitir la ejecución de scripts CGI, con la opción `ExecCGI`. Si se necesita ejecutar un script CGI en cualquier otro directorio, habrá que configurar `ExecCGI` para ese directorio. Por ejemplo, si `cgi-bin` es `/var/www/cgi-bin`, pero se quiere ejecutar scripts CGI desde `/home/my_cgi_directory`, añadirá una directiva `ExecCGI` a un par de directivas `Directory` como las siguientes al fichero `httpd.conf`:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Para permitir la ejecución de scripts CGI en `/home/my_cgi_directory`, habrá que llevar a cabo pasos extra aparte de configurar `ExecCGI`. También necesitará anular el comentario de la directiva `AddHandler` para identificar ficheros con extensión `.cgi` como scripts CGI. Vea la Sección 14.2.65, *`AddHandler`* para saber cómo configurar el comando `AddHandler`. El valor de los permisos para

scripts CGI y el recorrido entero a los scripts, debe ser de 0755. Además, el dueño del script y del directorio deben ser el mismo.

14.2.30 Options

La directiva `Options` controla características del servidor que están disponibles en un directorio en particular. Por ejemplo, en los parámetros restrictivos especificados para el directorio raíz, el comando `Options` sólo permite `FollowSymLinks`. No hay características permitidas, salvo que el servidor pueda seguir enlaces simbólicos en el directorio raíz.

Por defecto, en el directorio `DocumentRoot`, `Options` está configurado para incluir los comandos `Indexes`, `Includes` y `FollowSymLinks`. `Indexes` permite al servidor generar un listado de un directorio si no se especifica el `DirectoryIndex` (`index.html, etc.`). `Includes` implica que se permiten inclusiones en el servidor y el comando `FollowSymLinks` permite al servidor seguir enlaces simbólicos en ese directorio.

También se tienen que incluir declaraciones del comando `Options` para los directorios que estén dentro de directivas de máquinas virtuales, si se quiere que éstas reconozcan esas `Options`.

Por ejemplo, la inclusión en el servidor está activada en el directorio `/var/www/html` en la línea `Options Includes` dentro de la sección `Location "/"`. Sin embargo, si se quiere que una máquina virtual reconozca que se permite realizar la inclusión desde el servidor en `/var/www/html`, habrá que incluir una sección como la siguiente desde dentro de las etiquetas de las máqinas virtuales:

```
<Directory /var/www/html>
Options Includes
</Directory>
```

14.2.31 AllowOverride

`AllowOverride` establece qué directivas `Options` puede obviar un archivo `.htaccess`. Por defecto, tanto el directorio raíz como `DocumentRoot` están configurados para no permitir la prevalencia de `.htaccess`.

14.2.32 Order

`Order` simplemente controla el orden en que `allow` y `deny` se evaluan. El servidor está configurado para evaluar `Allow` antes que `deny` para el directorio `DocumentRoot`.

14.2.33 Allow

`Allow` especifica qué peticionario puede acceder un directorio dado. El peticionario puede ser `all`, un nombre de dominio, una dirección IP, una dirección IP parcial, un par red/máscara de red, etc. El directorio `DocumentRoot` está configurado para permitir peticiones de `all` (cualquiera).

14.2.34 `Deny`

`Deny` funciona como `allow`, pero especifica a quién se niega el acceso. `DocumentRoot` no está configurado para `rechazar` peticiones de nadie.

14.2.35 `UserDir`

`UserDir` es el nombre del subdirectorio dentro del directorio de cada usuario dónde estarán los archivos HTML que serán servidos. Por defecto, el subdirectorio es `public_html`. Por ejemplo, el servidor podría recibir la siguiente petición:

```
http://your_domain/~username/foo.html
```

El servidor buscaría el fichero:

```
/home/username/public_html/foo.html
```

En el ejemplo, `/home/username` es el directorio del usuario (nótese que la ruta predeterminada a los directorios de los usuarios puede variar entre sistemas).

Hay que asegurarse que los permisos de los directorios de usuario sean correctos. El valor de los permisos deben ser de 0755. Los bits de lectura (r) y ejecución (x) deben estar activados en el directorio del usuario `public_html` (0755 valdrá). El valor de los permisos con que se servirán los ficheros desde `public_html` debe ser 0644 por lo menos.

14.2.36 `DirectoryIndex`

`DirectoryIndex` es la página por defecto que entrega el servidor cuando hay una petición de índice de un directorio especificado con una barra (/) al final del nombre del directorio.

Por ejemplo, cuando un usuario pide la página http://*your_domain*/*this_directory*/, recibe la página `DirectoryIndex` si existe, o un listado generado por el servidor. El valor por defecto para `DirectoryIndex` es `index.html`, `index.htm` `index.shtml` e `index.cgi`. El servidor intentará encontrar cualquiera de estos cuatro, y entregará el primero que encuentre. Si no encuentra ninguno y si `Options Indexes` se encuentra en el directorio, el servidor generará un listado, en formato HTML, de los subdirectorios y archivos del directorio.

14.2.37 `AccessFileName`

`AccessFileName` denomina el archivo que el servidor utilizará para controlar el acceso en cada directorio. Por defecto, el servidor utilizará `.htaccess`, si existe, para controlar el acceso en cada directorio.

Justo tras AccessFileName,el comando Files controla el acceso a cualquier archivo que empiece con .ht. Estas directivas niegan acceso a todo tipo de archivo .htaccess (u otros archivos que empiecen .ht) por razones de seguridad.

14.2.38 CacheNegotiatedDocs

Por defecto, secure Web server requiere a los "proxies" que no hagan caché de los documentos que se negocian en base al contenido (pueden cambiar en el tiempo o según los datos del peticionario). Si se anula el comentario del comando CacheNegotiatedDocs, se desactiva la función y los "proxies" podrán hacer caché de los documentos.

14.2.39 UseCanonicalName

UseCanonicalName ya aparece en on. El comando UseCanonicalName permite que los URLs contengan sus propias referencias utilizando los comandos ServerName y Port. Cuando el servidor se refiere a si mismo en respuesta a peticiones de clientes, usa este URL. Si el UseCanonical-Name está en off, el servidor utilizará el valor que vino en la petición del cliente para referirse a si mismo.

14.2.40 TypesConfig

TypesConfig denomina el fichero que establece la lista predeterminada de mapeado de tipos MIME (extensiones de ficheros a tipos de contenido). El fichero predeterminado TypesConfig es /etc/mime.types. En vez de modificar el /etc/mime.types, se recomienda añadir mapeados de tipos MIMEs con AddType.

14.2.41 DefaultType

DefaultType establece el contenido por defecto que el servidor utilizará para documentos cuyos tipos MIME no puedan ser determinados. El servidor predispone el texto para cualquier fichero con un tipo de contenido indeterminado.

14.2.42 IfModule

<IfModule> y </IfModule> envuelven a directivas que son condicionales. Las directivas contenidas dentro de IfModule son procesadas si se cumple una de las dos condiciones. Las directivas son procesadas si el módulo contenido en la etiqueta <IfModule> está compilado en el servidor Apache. O, si una "!" (exclamación) aparece antes del nombre; las directivas son procesadas sólo si el módulo en la etiqueta <IfModule> *no* está compilado.

El fichero mod_mime_magic.c está incluído en IfModule. El módulo mod_mime_magic puede compararse al comando UNIX file, que examina los primeros bytes de un fichero, y usa "números mágicos" y otros trucos para decidir el tipo MIME del fichero.

Si el módulo mod_mime_magic está compilado en Apache, estas etiquetas `IfModule` le dicen al módulo mod_mime_magic module donde está el fichero de los trucos: `share/magic` en este caso.

El módulo mod_mime_magic module no está compilado por defecto. Si se quier usar, vea la Sección 14.3, *Añadir módulos a su servidor*, para saber cómo añadir módulos al servidor.

14.2.43 `HostnameLookups`

`HostnameLookups` puede aparecer en `on` o en `off`. Si el servidor permite la directiva `HostnameLookups` (poniéndolo en `on`), el servidor resolverá automáticamente la dirección IP de cada conexión que pida un documento del servidor. Resolver la dirección IP implica que el servidor hará una o más conexiones al DNS para averiguar qué nombre de máquina se corresponde con una dirección IP.

Generalmente, debería dejarse `HostnameLookups` en `off` porque las peticiones de DNS añanden carga al servidor y pueden ralentizarlo. Si el servidor tiene carga, los efectos de `HostnameLookups` pueden ser considerables.

`HostnameLookups` influye también en Internet en general. Cada conexión individual provoca una sobrecarga en el servidor. Por ello, por beneficio del servidor y de Internet en general, debería dejarse `HostnameLookups` en `off`.

14.2.44 `ErrorLog`

`ErrorLog` nombra el fichero donde se guardan los errores del servidor.Como viene indicado, el fichero de error del servidor es `/var/log/httpd/error_log`.

El log de errores es un buen sitio para ver si el servidor genera errores y no se sabe muy bien qué pasó.

14.2.45 `LogLevel`

`LogLevel` establece cómo serán de abundantes los logs de error. Los niveles de error del `LogLevel` (de menor a mayor) son `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` or `debug`. El `LogLevel` de secure Web server está en `warn` (nivel medio).

14.2.46 `LogFormat`

`LogFormat` pone el formato para los mensajes en el log de acceso; afortunadamente, el formato hará que el log de acceso sea más legible.

14.2.47 CustomLog

`CustomLog` identifica el log y el formato de log. La configuración por defecto de `CustomLog` de secure Web server, define el log en el que se guardan los accesos al servidor `/var/log/httpd/access_log`. Habrá que saber la localización de este archivo si se quieren generar estadísticas de rendimiento del servidor.

`CustomLog` pone el formato común para el archivo. El formato común de log es de la siguiente forma:

```
remotehost rfc931 authuser [date] "request" status bytes
```

remotehost

El nombre de la máquina: Si el nombre no está disponible en el DNS, o sí `HostnameLookups` está en `Off`, entonces *`remotehost`* será la dirección IP de la máquina remota.

rfc931

No utilizado: Se verá un `-` en el log en su lugar.

authuser

Si se requirió la autenticación, este es el usuario con el que el usuario se identificó. Generalmente, no se usa, así que se verá un `-` en su lugar.

[date]

Fecha y hora de la petición.

"request"

Cadena de texto de la petición según vino del cliente.

status

Código de estado HTTP que se devolvió al cliente.

bytes

Tamaño del documento.

El comando `CustomLog` puede utilizarse para configurar logs específicos para registrar referencias(el URL que hizo el enlace al servidor) y/o agentes (navegadores utilizados para pedir páginas al servidor). Las líneas relevantes del `CustomLog` están comentadas, como se muestra, pero se debería de anular el comentario si se quieren los dos archivos de log:

```
#CustomLog /var/log/httpd/referer_log referer
#CustomLog /var/log/httpd/agent_log agent
```

Alternativamente, se puede poner la directiva `CommonLog` para que use un log `combinado` sin el comentario en la siguiente línea:

```
#CustomLog /var/log/httpd/access_log combined
```

Un fichero de log `combined` añadirá los campos agente y referer al final de cada línea. Si desea utilizar un fichero de log `combined` elimine el comentario que aparece en `CustomLog`.

14.2.48 `ServerSignature`

El comando `ServerSignature` añade una línea que contiene la versión del servidor Apache y el `ServerName` de la máquina a los documentos generados por el servidor (p.ej, mensajes de error devueltos a clientes). `ServerSignature` ya aparece en `on`. Se puede cambiar a `off` para no añadir nada, o se puede cambiar a `EMail`. `EMail` añadirá una etiqueta HTML `mailto:ServerAdmin` a la línea de firma.

14.2.49 `Alias`

El comando `Alias` permite que haya directorios fuera del `DocumentRoot` a los que puede acceder el servidor. Cualquier URL que termine en un alias será automáticamente traducido por el recorrido del alias. Por defecto, ya existe un alias configurado. El servidor puede acceder al directorio `icons` pero el directorio no está en `DocumentRoot`. `icons` , un alias, está en `/var/www/icons/`, y no en `/var/www/html/icons/`.

14.2.50 `ScriptAlias`

El comando `ScriptAlias` define dónde pueden encontrarse los scripts CGI (u otros scripts). Normalmente, no se ponen los scripts CGI dentro de `DocumentRoot`. Si los scripts CGI se encontrasen en `DocumentRoot`, podrían , potencialmente, ser considerados como documentos de texto. Incluso si no preocupa que la gente vea (y use) los scripts CGI, mostrar cómo funcionan crea oportunidades a la gente sin escrúpulos que quiera explotar dichos agujeros en el script, y puede crear un agujero de seguridad en el servidor. Por defecto, el directorio `cgi-bin` es un `ScriptAlias` de `/cgi-bin/`, y se encuentra situado `/var/www/cgi-bin/`.

El directorio `/var/www/cgi-bin` tiene activada la directiva `Options ExecCGI`, lo que implica que se permite la ejecución de scripts CGI en el directorio.

Vea la Sección 14.2.65, *`AddHandler`* y la Sección 14.2.29, *`Directory`* para saber cómo ejecutar scripts CGI en otros directorios aparte de `cgi-bin`.

14.2.51 `Redirect`

Cuando se cambia una página de sitio, el comando `Redirect` se puede usar para pasar del viejo URL al nuevo URL. El formato es como sigue:

```
Redirect /path/foo.html http://new_domain/path/foo.html
```

Así que si se recibe una petición HTTP para un página que solía estar en http://*your_domain*/*path*/foo.html, el servidor devolverá el nuevo URL (http://*new_domain*/*path*/foo.html) al cliente, que tratará de coger el documento desde el nuevo URL.

14.2.52 IndexOptions

El comando `IndexOptions` controla la apariencia de los listados generados por el servidor, al añadir iconos y texto descriptivo, etc. Si `Options Indexes` aparece como en (véase Sección 14.2.30, *`Options`*),el servidor podrá generar el listado de un directorio al recibir una petición HTTP como la que sigue:

http://*your_domain*/*this_directory*/

Primero el servidor busca en el directorio un fichero de los de la lista de `DirectoryIndex` (p.ej., `index.html`). Si el servidor no encuentra ninguno de los ficheros, genera un listado del directorio en HTML. Se puede modificar la apariencia del listado utilizando ciertas directivas en `httpd.conf`, entre las que se encuentra `IndexOptions`.

La configuración predeterminada activa es `FancyIndexing`. Si se activa `FancyIndexing`, al hacer click en la cabecera de las columnas del listado, el listado se ordena según esa columna. Otro click en la misma cabecera cambiará el orden de ascendente a descendente y viceversa. `FancyIndexing` también muestra distintos iconos para distintos ficheros, según la extensión. Si se usa la directiva `AddDescription` y se activa `FancyIndexing`, se añade una pequeña descripción para el fichero en el listado generado.

`IndexOptions` tiene otros parámetros que pueden activarse para controlar la apariencia de los listados. Los parámetros incluyen `IconHeight` e `IconWidth`, para hacer que el servidor incluya etiquetas `HEIGHT` y `WIDTH` para los iconos; el comando `IconsAreLinks`, hace que los iconos formen parte del enlace HTML junto con el nombre del fichero, y otros.

14.2.53 AddIconByEncoding

Esta directiva denomina qué iconos se mostrarán con los archivos según su codificación MIME, en los listados de directorio. Por ejemplo, por defecto, el servidor muestra el icono `compressed.gif` junto a archivos con codificación MIME x-compress y x-gzip en los listados de directorio.

14.2.54 AddIconByType

Esta directiva denomina qué iconos se mostrarán con los archivos según su codificación MIME, en los listados del directorio. Por ejemplo, por defecto, el servidor muestra el icono `text.gif` junto a archivos con tipo MIME "text" en los listados del directorio.

14.2.55 AddIcon

AddIcon dice al servidor qué icono mostrar en los listados del directorio para ciertos tipos de archivos según la extensión. Por ejemplo, el servidor muestra el icono binary.gif para archivos con extensiones .bin o .exe.

14.2.56 DefaultIcon

El comando DefaultIcon nombra el icono de los listados del directorio que recibirán los ficheros sin un icono específico. El fichero de imagen predeterminado para esos ficheros unknown.gif es DefaultIcon.

14.2.57 AddDescription

Se puede usar AddDescription para mostrar descripciones específicas de ficheross en los listados de los directorios (habrá que activar también el FancyIndexing como una IndexOptions). Puede aplicarse a ficheros individuales, expresiones de nombre o extensiones para especificar los ficheros a los que aplicar esta directiva. Por ejemplo, podría usarse lo siguiente:

```
AddDescription "A file that ends in .ni" .ni
```

En los listados del directorio, todos los ficheros con extensión .ni tendrán la descripción Un archivo que termina en .ni tras el nombre. Nótese que necesita activarse el FancyIndexing.

14.2.58 ReadmeName

La directiva ReadmeName determina el fichero (si existe dentro del directorio) que se adjuntará a los listados de los directorios. El servidor intentará primero incluirlo como documento HTML y luego como texto. El valor predeterminado de ReadmeName es README.

14.2.59 HeaderName

La directiva HeaderName dicta el fichero (si existe dentro del directorio) que se antepondrá al comienzo de los listados de los directorios. Al igual que con ReadmeName, el servidor intentará incluirlo como documento HTML si es posible, o como texto.

14.2.60 IndexIgnore

El comando IndexIgnore lista las extensiones, los nombres de los ficheros parciales, las expresiones regulares o los nombres completos. El servidor no incluirá los ficheros que encajen en estos patrones en los listados de directorios.

14.2.61 AddEncoding

El comando `AddEncoding` dice qué extensiones especifican un tipo particular de codificación. `AddEncoding` se puede usar para decirle a los navegadores (no a todos) que descompriman ciertos ficheros mientras los descargan.

14.2.62 AddLanguage

La directiva `AddLanguage` asocia extensiones a contenidos específicos de idiomas. Esta directiva es útil para la negociación de contenidos, cuando el servidor devuelve uno de entre varios documentos según las preferencias de idiomas del cliente.

14.2.63 LanguagePriority

La directiva `LanguagePriority` permite dar la prioridad a ciertos ficheros en distintos idiomas, que entrarán en vigor si el cliente no especifica la preferencia de idioma.

14.2.64 AddType

Use la directiva `AddType` para definir parejas de tipos MIME y sus extensiones. Por ejemplo, si usa el PHP4, el servidor está usando `AddType` para que se reconozcan ficheros con extensiones PHP (`.php4`, `.php3`, `.phtml .php`) como tipos MIME PHP.

La siguiente línea `AddType` permite al servidor reconocer las extensiones `.shtml` (para la inclusión en el servidor):

```
AddType text/html .shtml
```

Se necesitará la línea de arriba dentro de las etiquetas de máquina virtual para cuando se permita la inclusión desde el servidor.

14.2.65 AddHandler

La directiva `AddHandler` mapea y amplia gestores específicos. Por ejemplo, el gestor `cgi-script` puede usarse para hacer que la extensión `.cgi` automáticamente sea manejada como un script CGI. Esto funciona, incluso para ficheros fuera de `ScriptAlias`, si se siguen las instrucciones dadas.

Hay una línea `AddHandler` CGI en `httpd.conf` como la siguiente:

```
AddHandler cgi-script .cgi
```

Habrá que anular el comentario de la línea. Así Apache ejecutará como scripts CGI los ficheros que terminen en `.cgi`, incluso si están fuera de `ScriptAlias`, que por defecto se encuentra en el directorio `/cgi-bin/` en `/var/www/cgi-bin/`.

También habrá que activar `ExecCGI` como `Options` para cualquier directorio que contenga scripts CGI. Vea Sección 14.2.29, *`Directory`* para más información sobre cómo configurar `ExecCGI` para un directorio. Además, habrá que asegurarse que los permisos sean los adecuados para los scripts CGI y los subdirectorios que contengan scripts. Los scripts CGI y todo el recorrido que conduce a ellos deben tener un valor de 0755. Finalmente, el dueño del directorio y el del script deben ser el mismo.

Habrá que añadir la misma línea `AddHandler` a la configuración de `VirtualHost`, si se usan máquinas virtuales y se quiere que se reconozcan los scripts CGI fuera de `ScriptAlias`.

El servidor también usa `AddHandler` para procesar mapas de imágenes en HTML.

14.2.66 `Action`

La directiva `Action` permite especificar un par de tipos de contenido MIME y un script CGI, de tal forma que cuando se pida un fichero de este tipo, se ejecute un script en particular.

14.2.67 `MetaDir`

`MetaDir` especifica el nombre del directorio donde el servidor debería buscar los ficheros que contengan información meta (cabeceras extra de HTTP) que se deba incluir al entregar los documentos.

14.2.68 `MetaSuffix`

`MetaSuffix` especifica el sufijo para los ficheros que contienen información meta (cabeceras extra de HTTP), que estarán en el directorio `MetaDir`.

14.2.69 `ErrorDocument`

Por defecto, en caso de error, el servidor muestra un mensaje de error (generalmente críptico) para el cliente. En vez de usar esta opción ya predeterminada, puede usarse `ErrorDocument` para devolver un mensaje de error personalizado o redireccionar al cliente a un URL local o remoto. `ErrorDocument` simplemente asocia un código de respuesta HTTP con un mensaje o un URL que se devolverá al cliente.

14.2.70 `BrowserMatch`

La directiva `BrowserMatch` permite al servidor definir variables de entorno y/o tomar acciones según sea el campo de cabecera User-Agent, que identifica al cliente. Por defecto, el servidor usa `BrowserMatch` para denegar la conexión a navegadores con problemas conocidos y para desactivar "keepalives" y vaciados de cabecera de HTTP para navegadores con problemas de esas características.

14.2.71 `Location`

Las etiquetas `<Location>` y `</Location>` permiten controlar el acceso específico a cada URL.

El primer uso de `Location` es configurar `Options` y proporcionar guías extra de configuración para `DocumentRoot`. Estas directivas de configuración, que se encuentran dentro de las etiquetas `<Location "/">` y `</Location>`, son necesarias para permitir el acceso a documentos en `DocumentRoot`.

El siguiente uso de `Location` es en las etiquetas `IfModule mod_perl.c`. Estas directivas de configuración funcionan si el DSO `mod_perl.so` está cargado. Consulte la Sección 14.3, *Añadir módulos a su servidor* para más información sobre cómo añadir módulos a Apache.

La etiqueta `Location` nombra el directorio `/var/www/perl` (un `Alias` para `/perl`) como el directorio desde el cual se sirven scripts de Perl. Si se pide un documento con un URL que contenga `/perl` en el recorrido, el servidor buscará en `/var/www/perl/` el script de Perl apropiado.

Los comentarios de otras opciones de `<Location>` están en `httpd.conf`. Si se quiere activar su funcionalidad, se necesitará anular el comentario de la sección apropiada de las directivas.

Justo tras las directivas de Perl discutidas anteriormente, `httpd.conf` incluye una sección de directivas para activar HTTP PUT (p.ej., publicación de Netscape Gold, que permite poner páginas web en un servidor). Si se quiere permitir HTTP PUT, habrá que anular el comentario de la sección entera:

```
#LoadModule put_module          modules/mod_put.so
#AddModule mod_put.c
#
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/httpd/conf/passwd
#    EnableDelete Off
#    umask 007
#    <Limit PUT>
#       require valid-user
#    </Limit>
#</Location>
```

Si se quiere que las conexiones desde dentro del mismo dominio tengan acceso a los informes de estado, se debe anular el comentario de la siguiente sección de directivas:

```
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Hay que poner el segundo nivel del nombre de dominio en vez de `.your_domain.com`.

Si se quiere dar informes de configuración del servidor (incluyendo módulos instalados y directivas de configuración) o peticiones desde dentro del dominio, habrá que anular el comentario de las siguientes líneas:

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Hay, por supuesto, que rellenar `.your_domain.com`.

La siguiente sección de directivas usa las etiquetas `Location` para permitir el acceso a la documentación en `/usr/share/doc` (p.ej, con un URL como http://*your_domain*/doc/whatever.html). Estas directivas sólo permiten el acceso a peticiones desde la misma máquina.

Otro uso de las etiquetas `Location` es una sección comentada, pensada para rastrear ataques al servidor explotando un viejo fallo de los días de pre-Apache 1.1. Si se quieren rastrear estas peticiones, anule el comentario de las siguientes líneas:

```
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>
```

Si estas líneas no están comentadas, el servidor mandará cualquier petición que termine en `/cgi-bin/phf*` a un CGI que hace log del Grupo Apache.

14.2.72 `ProxyRequests`

Si se anula el comentario de la directiva `IfModule` alrededor del `ProxyRequests`, el servidor Apache también funcionará como proxy. También habrá que cargar el módulo `mod_proxy`. Para más información sobre cómo cargar módulos, vea la Sección 14.3, *Añadir módulos a su servidor*.

14.2.73 `ProxyVia`

La directiva `ProxyVia` controla si se envía HTTP Via: junto con peticiones o respuestas que vayan vía el servidor proxy Apache. Via: header mostrará el nombre de la máquina si `ProxyVia` aparece en `On`, el nombre de máquina y la versión de Apache para `Full`, y cualquier línea Via: se enviará sin cambiar si está ProxyVia está en `Off`, y las líneas Via: serán eliminadas si está en `Block`.

14.2.74 Directivas de caché

Hay varias directivas de caché en las etiquetas de proxy `IfModule` mencionadas antes. Si se usa la funcionalidad proxy y se quiere habilitar el caché proxy, habrá que anular el comentario de las directivas según se describe. Los valores predeterminado de las directivas de caché deberían bastar para la mayoría de las configuraciones.

`CacheRoot` pone el nombre del directorio que contiene ficheros de caché. El valor predeterminado de `CacheRoot` es `/var/cache/httpd`.

`CacheSize` establece cuánto espacio puede usar el caché, en KB. El valor predeterminado de `CacheSize` es `5` KB.

`CacheGcInterval` establece el número de horas. Tras ese número se borrarán los ficheros de caché si ocupan más de lo permitido por `CacheSize`. El valor por defecto de `CacheGcInterval` es cuatro horas.

Los documentos HTML en caché se guardarán (sin una recarga desde el servidor de origen) durante el número máximo de horas establecido por `CacheMaxExpire`. El valor predeterminado es `24` horas.

`CacheLastModifiedFactor` afecta a la fecha de caducidad para documentos que no venían con caducidad desde el servidor de origen. El valor predeterminado de `CacheLastModifiedFactor` es `0.1`, lo que significa que la caducidad del documento será un décimo del tiempo total desde que se modificó el documento por última vez.

`CacheDefaultExpire` es la caducidad en horas para documentos recibidos vía protocolos que no soportan la caducidad. El valor predeterminado es de una hora.

Todo documento que provenga de una máquina y/o de un dominio que encaje en `NoCache` no se pondrá en caché. Si conoce máquinas o dominios en los que no se quiera hacer caché de sus documentos, anule el comentario de la directiva `NoCache` e introduzca dominios y nombres aquí.

14.2.75 `NameVirtualHost`

Necesitará usar la directiva `NameVirtualHost` para la dirección IP (y número de puerto si es necesario) de algún nombre de máquinas virtuales que esté estableciendo. La configuración basada en máquinas virtuales se usa para establecer máquinas virtuales para diferentes dominios, pero no tiene (o no usa) diferentes direcciones IP para todos los dominios a los cuales su Web Server sirve documentos

Nota

No puede usar nombres basados en máquinas virtuales con su servidor seguro. Algunos nombres basados en máquinas virtuales que establezca trabajarán sólo con conexiones HTTP no seguras y no con conexiones SSL.

No puede usar nombres basados en máquinas virtuales con su servidor seguro porque el acuerdo SSL (cuando el navegador acepta el certificado de autenticación de Web seguro) viene antes de la peticion HTTP con la cual identifica el nombre correcto de las máquinas virtuales. En otras palabras, la autenticación viene antes de la identificación de las máquinas virtuales. Si quiere usar máquinas virtuales con su servidor seguro necesitará usar direcciones IP basadas en máquinas virtuales.

Si está usando nombres basados en máquinas virtuales, comente la directiva `NameVirtualHost` y añada la dirección IP correcta para su servidor después del `NameVirtualHost`. Entonces añada más información sobre los diferentes dominios usando el comando `VirtualMachine` el cual envuelve el `ServerName` para cada máquina virtual, más algunas otras directivas de configuración que son sólo aplicables a la máquina virtual.

14.2.76 `VirtualHost`

`<VirtualHost>` y `</VirtualHost>` envuelven directivas de configuración que se aplican a máquinas virtuales. La mayoría de las directivas de configuración pueden usarse en etiquetas de máquina virtual, y sólo se aplicarán a esa máquina virtual.

Existen varias etiquetas `VirtualHost` que rodean a algunos modelos de directivas de configuración así como de espacios en blanco que tendrá que rellenar con información para configurar la máquina virtual. Consulte la Sección 14.4, *Utilización de máquinas virtuales*, para saber más sobre máquinas virtuales.

14.2.77 `SetEnvIf`

La directiva de configuración de Apache `SetEnvIf` se usa para desactivar HTTP keepalive y permitir a SSL cerrar las conexiones sin avisar desde el cliente. Este parámetro es necesario para clientes que no cierran bien la conexión SSL.

14.2.78 Directivas de configuración SSL

Se han incluído las directivas SSL en su fichero de servidores `httpd.conf` para permitir comunicaciones seguras Web usando las directivas SSL y TLS.

Para más información sobre directivas SSl consulte: http://*your_domain*/manual/mod/mod_ssl/ o también: http://www.modssl.org/docs/2.6/ssl_reference.html/,un capítulo en un documento Web sobre mod_ssl por Ralf Engelschall. El mismo documento, el mod_ssl *User Manual*, comienza en http://www.modssl.org/docs/2.7/ y es una estupenda referencia para mod_ssl (of course) y para criptografía web en general. Este manual da información general sobre su servidor seguro se encuentra en Capítulo 13, *Uso de Apache como servidor Web seguro*.

Nota

No modifique sus directivas SSl a menos que esté completamente seguro de lo que está haciendo. Para la mayoría de los secure Web server, las directivas SSL están configuradas e instaladas apropiadamente.

14.3 Añadir módulos a su servidor

Debido a que Apache 1.3 soporta DSOs, puede fácilmente cargar módulos Apache o compilar sus propios módulos para su secure Web server. DSO significa que se pueden cargar los módulos en tiempo de ejecución. Debido a que los módulos se cargan sólo cuando es necesario no usan la memoria hasta que la necesitan.

El grupo Apache da información completa en http://www.apache.org/docs/dso.html. Después de la instalación consulte también http://*your_domain*/manual/mod/ donde encontrará la documentación en formato HTML (si ha instalado el paquete `apache-manual`). Se da una rápida descripción de cómo cargar los módulos, pero si necesita más detalles, consulte los URLs dados.

Para que su secure Web server use un módulo dinámicamente compartido, este módulo debe tener una línea `LoadModule` y otra `AddModule` en `httpd.conf`. Muchos módulos tienen ya estas dos líneas que están incluídas en `httpd.conf`, pero algunos de los menos comunmente usados están comentados fuera. Los módulos comentados fuera, se incluyeron durante la compilación, pero no se cargaron.

Si necesita usar uno de estos módulos no cargados, mire en el fichero `httpd.conf` para ver todos los módulos posibles. Cada uno de estos módulos tiene una línea `LoadModule`. Para ver un ejemplo, la sección `LoadModule` comienza con estas siete líneas:

```
#LoadModule mmap_static_module modules/mod_mmap_static.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule env_module         modules/mod_env.so
LoadModule config_log_module  modules/mod_log_config.so
LoadModule agent_log_module   modules/mod_log_agent.so
LoadModule referer_log_module modules/mod_log_referer.so
#LoadModule mime_magic_module  modules/mod_mime_magic.so
```

Muchas de estas líneas no están comentadas lo que quiere decir que cada módulo asociado está compilado dentro y cargado por defecto. La primera línea está comentada, lo cual significa que se compiló pero no se cargó el correspondiente módulo (`mmap_static_module`).

Para que su secure Web server cargue un módulo no cargado, primero escriba no-comentada en la correspondiente línea `LoadModule`. Por ejemplo, si quiere que su secure Web server cargue el `mime_magic_module`, cambie la línea `LoadModule` del original:

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
```

No comente la línea previa para que se pueda leer:

```
LoadModule mime_magic_module modules/mod_mime_magic.so
```

Después, elimine el comentario de la correspondiente línea desde la sección `AddModule` en el `httpd.conf`. Para continuar con nuestro ejemplo, quite el comentario de la línea `mod_mime_magic`. La línea original se parecerá a la siguiente:

```
#AddModule mod_mime_magic.c
```

La línea sin comentario será así:

```
AddModule mod_mime_magic.c
```

Una vez que ha anulado el comentario de las líneas `LoadModule` y `AddModule` para el módulo que quiere cargar, pare y reinicialice su Web Server, consulte la Sección 14.1, *Arranque y apagado del `httpd`*. Después de arrancar, el módulo se cargará en su secure Web server.

Si tiene su propio módulo, puede añadirlo al fichero `httpd.conf` y así se compila y se carga como un DSO. Si quiere llevar a cabo esta operación, necesita instalar el paquete `apache-devel`, consulte el Capítulo 13, *Uso de Apache como servidor Web seguro*. Necesita este paquete `apache-devel` porque instala el fichero include, los ficheros cabeceras y el soporte de herramientas APache eXtenSion (APXS). APXS usa los ficheros include y los ficheros cabecera para compilar su módulo y así poder trabajar con Apache.

ADVERTENCIA

Si desea usar la Herramienta de configuración de Apache, una utildad GUI que se incluye en el paquete Red Hat Linux, no debe compilar sus propios módulos con su servidor Apache o modificar el fichero de configuración del servidor `httpd.conf`. Si desea añadir módulos o modificar el fichero `httpd.conf` a mano, no use la Herramienta de configuración de Apache. Si necesita más información sobre dicha herramienta consulte la versión española de la *Official Red Hat Linux Customization Guide*.

Si ha escrito su propio módulo o ha revisado algunos más, podrá usar APXS para compilar sus módulos fuentes fuera del árbol fuente Apache, sin necesitar ningún indicador del compilador y/o del creador de enlaces. Si necesita más información sobre APXS consulte la documentación en http://www.apache.org/docs/dso.html.

Una vez compilados sus móduloss usando APXS, situélos dentro de `/usr/lib/apache`. Entonces su módulo necesita ambas líneas `LoadModule`, `AddModule` en el fichero `httpd.conf`, como se describe para los módulos de Apache. Después en la lista `LoadModule` en el `httpd.conf`, añada una línea para el fichero objeto compartido para el módulo como la siguiente:

```
LoadModule foo_module  modules/mod_foo.so
```

Observe que necesitará cambiar el nombre del módulo y el nombre de su fichero objeto compartido apropiadamente.

Al final de la lista, la directiva `AddModule` en `httpd.conf`, añade una línea al fichero del código fuente para su módulo como la siguiente:

```
AddModule mod_foo.c
```

Observe que necesitará cambiar el nombre del fichero del código fuente apropiadamente.

Una vez que haya completado los pasos previos, pare y reinicialice su servidor Web como se indica en la Sección 14.1, *Arranque y apagado del `httpd`*. Si ha hecho todo correctamente, y su módulo está correctamente codificado, su servidor Web encontrará su módulo y lo cargará.

14.3.1 El módulo de segurdidad mod_ssl

La porción de seguridad mod_ssl del secure Web server se considera un Dynamic Shared Object (DSO). Esto quiere decir que los usuarios opueden recompilar el servidor Web Apache si la extensión EAPI corregida desde el módulo de seguridad mod_ssl se aplica a Apache. Sigua las instrucciones para construir el mod_ssl en el servidor Apache que se encuentran en la documentación sobre el mod_ssl pero debe añadir el siguiente indicador:

```
--with-eapi-only
```

La línea de comandos completa debe parecerse a esto:

```
./configure [userflags] --with-eapi-only
```

Entonces construya e instale Apache.

Nota

Red Hat no soporta las versiones recompiladas del servidor Web Apache. Se soporta la instalación de las versiones enviadas, pero si decide recompilar usted mismo el servidor Apache, lo tendrá que hacer solo, sin el soporte técnico. Se recomienda que no recompile Apache a menos que sepa exactamente lo que está haciendo.

14.4 Utilización de máquinas virtuales

ADVERTENCIA

Si desea usar la Herramienta de configuración Apache, una utilidad GUI que incluye el paquete de Red Hat Linux, no cambie el fichero de configuración `httpd.conf` de su servidor Apache. Por el contrario, si lo desea hacer a mano, no utilice dicha herramienta.

Si desea más información sobre la Herramienta de configuración Apache, consulte la versión española de la *Official Red Hat Linux Customization Guide*.

Se puede utilizar la capacidad de las máquinas virtuales de Apache para ejecutar servidores en distintas direcciones IP, diferentes nombres o diferentes puertos en la misma máquina. Si está interesado en utilizar máquinas virtuales,puede encontrar toda la información en la documentación de Apache en el sitio http://www.apache.org/docs/vhosts/.

Nota

El secure Web server no admite usar máquinas virtuales que estén basadas en el nombre porque el acuerdo SSL (cuando el cliente acepta el certificado SSL del servidor) ocurre antes de la petición HTTP que identifica por el nombre a la máquina virtual apropiada. Si se quieren utilizar este tipo de máquinas virtuales, lo podrá hacer sólo con servidores no seguros.

Las máquinas virtuales se configuran en `httpd.conf`, según se describe en Sección 14.2, *Directivas de configuración en el fichero `httpd.conf`*. Por favor, lea esta sección antes de empezar a cambiar la configuración de las máquinas virtuales del servidor.

14.4.1 Máquina virtual de secure Web server

La configuración predeterminada de secure Web server se ejecuta en servidores seguros y no seguros. Ambos servidores usan la misma dirección IP y nombre, pero diferentes puertos, y el servidor seguro es una máquina virtual. Esta configuración permite entregar documentos seguros y no seguros de la manera más eficiente posible. Como ya sabrá las transferencias seguras HTTP llevan más tiempo que las no seguras, ya que se pasa mucha información extra durante las transacciones seguras. Así que utilizar el servidor seguro para tráfico no seguro no es una buena idea.

Las directivas de configuración del servidor seguro están en las etiquetas de la máquina virtual en `httpd.conf`. Si se necesita cambiar la configuración del servidor seguro, habrá que cambiar las directivas que se encuentran en las etiquetas de la máquina virtual en `httpd.conf`. Si se quiere activar ciertas características (por ejemplo, inclusión en el servidor) para el servidor seguro, habrá que activarlas en las etiquetas de la máquina virtual que definen el servidor seguro.

El servidor no seguro está configurado como la máquina "no virtual" en `httpd.conf`. En otras palabras, las opciones de configuración del servidor no seguro están fuera de las etiquetas de la máquina virtual. Si se quiere cambiar la configuración del servidor no seguro, habrá que cambiar las directivas de configuración en `httpd.conf`.

Por defecto, los servidores seguros y no seguros comparten el mismo `DocumentRoot`, directiva de configuración especificada en `httpd.conf`. En otras palabras, los servidores buscan en el mismo sitio los ficheros que proporcionan como respuesta a las peticiones. El valor predeterminado de `DocumentRoot` es `/var/www/html`.

Para cambiar `DocumentRoot`, de tal forma que no lo compartan el servidor seguro y el no seguro, cambie una de las directivas `DocumentRoot` en `httpd.conf`. La directiva `DocumentRoot` fuera de las etiquetas de la máquina virtual define la directiva `DocumentRoot` para el servidor no seguro. Así mismo la directiva `DocumentRoot` dentro de las etiquetas de la máquina virtual la define para el servidor seguro.

Si por alguna razón se quiere desactivar el servidor no seguro, puede hacerlo. El servidor seguro usa el puerto 443, puerto por defecto para comunicaciones web seguras, mientras que el servidor no seguro usa el puerto 80, el puerto predeterminado para las comunicaciones web. Para evitar que el servidor no seguro acepte conexiones, busque la línea siguiente en `httpd.conf`:

```
Port 80
```

Cambie la línea:

```
Port 443
```

Anule el comentario de la línea `Listen 80`, para que en vez de:

```
Listen 80
```

diga:

```
#Listen 80
```

Tras estos dos pasos, secure Web server aceptará las conexiones en el puerto 443, el puerto predeterminado para las comunicaciones seguras y no en el puerto 80, que es para comunicaciones no seguras, de tal forma que el servidor no seguro estará desactivado.

14.4.2 Configuración de las máquinas virtuales

La mayoría de los usuarios utilizará secure Web server tal y como viene configurado. Por ello, usarán la capacidad intrínseca de las máquinas virtuales, pero no tocarán las directivas de las máquinas virtuales que se encuentran en el fichero de configuración `httpd.conf`. Sin embargo, si quiere usar la capacidad de las máquinas virtuales por alguna otra razón, lo puede hacer.

Para crear una máquina virtual, habrá que alterar las líneas de la máquina virtual dadas como ejemplo en `httpd.conf`, o crear una sección de máquinas virtuales. (Recuérdese que las máquinas virtuales basadas en el nombre no funcionan con el servidor seguro — habrá que utilizar máquinas virtuales basadas en la dirección IP si se quieren obtener máquinas virtuales con SSL activo. El servidor no seguro, sin embargo, soporta máquinas virtuales basadas en el nombre y en la dirección IP.)

Las líneas wue sirven de ejemplo de una máquina virtual son las siguientes:

```
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
```

```
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#</VirtualHost>
```

Anule el comentario de las líneas (elimínese # al comienzo de cada línea). Añada entonces la información correcta para la máquina y/o máquina virtual a cada línea.

En la primera línea, cambie `ip.address.of.host.some_domain.com` por la dirección IP del servidor. Cambie `ServerName` por un nombre DNS *válido* para la máquina virtual. (En otras palabras, no basta con inventar algo. Pregunte al administrador de red si no sabe cómo conseguir un nombre de dominio válido.)

También habrá que anular el comentario de las líneas `NameVirtualHost` en `httpd.conf`:

```
#NameVirtualHost 12.34.56.78:80
#NameVirtualHost 12.34.56.78
```

Anule el comentario de una de las líneas y cambie la dirección IP por la dirección (y puerto si es necesario) para esa máquina virtual.

Se pueden poner en las etiquetas otras directivas de configuración para la máquina virtual, según cómo se configure ésta.

Si se configura una máquina virtual para escuchar en un puerto no habitual (80 es el valor predeterminado para comunicaciones no seguras y 443 es el defecto para comunicaciones seguras), habrá que configurar una máquina virtual para el puerto y añadir la directiva `Listen` `httpd.conf`, correspondiente a ese puerto.

Para tener una máquina virtual específica para ese puerto, añada el puerto a la primera línea de la configuración de la máquina virtual. La primera línea debería parecerse a lo siguiente:

```
<VirtualHost ip_address_of_your_server:12331>
```

Esta línea crearía una máquina virtual en el puerto 12331. Sustituya `12331` por el puerto que desea usar en el ejemplo anterior.

En las líneas `Listen` de `httpd.conf`, añada lo siguiente para que el servidor escuche en el puerto 12331:

```
Listen 12331
```

Hay que rearrancar el servidor para iniciar una nueva máquina virtual.

Podrá encontrar información mucho más completa sobre cómo crear y configurar máquinas virtuales según el nombre y la dirección IP en la página web en http://www.apache.org/docs/vhosts/index.html. Vea la página del Grupo Apache sobre máquinas virtuales para más detalles sobre el uso de máquinas virtuales.

Parte IV Apéndices

A Parámetros generales y módulos

Este apéndice ilustra *algunos* de los posibles parámetros que podrían ser necesarios para configurar algunos controladores[1]para determinados dispositivos hardware. En la mayoría de casos, estos parámetros adicionales son innecesarios, si el kernel es capaz de usar el dispositivo por su cuenta. Utilice las configuraciones proporcionadas en este apéndice si tiene problemas para hacer que Red Hat Linux utilice un dispositivo determinado o si necesita sobreescribir los parámetros predeterminados del sistema para el dispositivo.

Durante la instalación de Red Hat Linux, se establecen determinados límites al sistema de ficheros y a otros controladores soportados por el kernel. Sin embargo, después de la instalación se proporciona el soporte a todos los sistemas de ficheros accesibles desde Linux. Durante la instalación el kernel modular proporciona soporte a los dispositivos (E)IDE (incluidos los CDROMs ATAPI), los adaptadores SCSI y tarjetas de red.

Nota

Dado que Red Hat Linux soporta la instalación en diversas plataformas hardware, algunos controladores (incluyendo aquéllos para los adaptadores SCSI, tarjetas de red y algunos CDROMs) no son compilados en el interior del kernel de Linux utilizado durante la fase de instalación, pero están disponibles como módulos y son descargados cuando hacen falta. Si fuese necesario, tiene la posibilidad de especificar las opciones para estos módulos en el momento en que se carguen.

Para especificar los parámetros de módulos cuando se carga un controlador, teclee **`linux expert`** en el indicador de comandos `boot:` e inserte el disco de controladores cuando se le indique en el programa de instalación. Tras haber leído el disco de controladores, el programa de instalación le pedirá que seleccione el tipo de dispositivo que está configurando. A continuación, el programa de instalación visualizará una pantalla donde puede escribir los parámetros correctos basados en el tipo determinado de dispositivo que está configurando.

Una vez completada la instalación podría querer volver a compilar el kernel para incluir el soporte a su configuración hardware específica. Observe que en la mayoría de los casos, no es necesario un kernel personalizado. Consulte la *Official Red Hat Linux Customization Guide* para obtener información sobre cómo construir un kernel personalizado.

[1] Un **controlador/driver** es un tipo de software que ayuda a su sistema usar un determinado dispositivo hardware. Sin el controlador, el kernel no sabría cómo utilizar este dispositivo correctamente.

A.1 Especificación de los parámetros del módulo

Si ha proporcionado parámetros la descarga de un módulo, podrá especificarlos usando uno o dos métodos diferentes:

- Especifique un set completo de parámetros en una frase. Por ejemplo, el parámetro `cdu31=0x340,0` podría ser utilizado con un CDU 31 de Sony en el puerto 340 sin IRQ.
- Especifique los parámetros individualmente. Este método se usa cuando no son necesarios uno o más parámetros en el primer grupo. Por ejemplo, `cdu31_port=0x340 cdu31a_irq=0` puede ser usado como el parámetro para el mismo CD-ROM usado como un ejemplo para el primer método. El *OK* se usa en las tablas de CD-ROM, SCSI y Ethernet en este apéndice para mostrar el punto en el que el primer método de parámetros se detiene y el segundo método empieza.

Nota

Utilice sólo un método y no ambos, cuando cargue un módulo con parámetros en particular.

Cuando un parámetro tiene comas, asegúrese de que *no* deja un espacio tras una coma.

A.2 Parámetros del módulo para el CD-ROM

Nota

No todas las unidades de CD-ROM listadas son soportadas. Controle para más seguridad la lista de las compatibilidades en el sitio Web de Red Hat en la dirección http://hardware.redhat.com para asegurarse de que la unidad de CD-ROM es soportada.

Aunque los parámetros son especificados tras cargar el disco de controladores y especificar el dispositivo, uno de los parámetros más comunmente usados (`hdX=cdrom`) *puede* ser introducido en el indicador de comandos de arranque (`boot:`) durante la instalación. Esta excepción a la regla es permitida porque trata con el soporte para los CD-ROMs IDE/ATAPI, que forman parte del kernel.

En las tablas que se detallan más abajo, muchos módulos son enumerados sin parámetros porque, o son capaces de efectuar automáticamente un control o bien le piden que modifique manualmente los parámetros en el código fuente del módulo y que después recompile.

Tabla A–1 Parámetros Hardware

Hardware	Módulo	Parámetros
Unidades de CD-ROM ATAPI/IDE		hd*X*=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (non-IDE)	`aztcd.o`	aztcd=*io_port*
Sony CDU-31A CD-ROM	`cdu31a.o`	cdu31a=*io_port,IRQ OR* cdu31a_port=*base_addr* cdu31a_irq=*irq*
Unidad de CDROM Philips/LMS CDROM 206 con tarjeta de adaptador host cm260	`cm206.o`	cm206=*io_port,IRQ*
Goldstar R420 CD-ROM	`gscd.o`	gscd=*io_port*
Interfaz CD-ROM de tarjeta de sonido ISP16, MAD16, o Mozart (OPTi 82C928 y OPTi 82C929) con lector Sanyo/Panasonic, Sony o Mitsumi	`isp16.o`	isp16=*io_port,IRQ,dma, drive_type OR* isp16_cdrom_base=*io_port* isp16_cdrom_irq=*IRQ* isp16_cdrom_dma=*dma* isp16_cdrom_type=*drive_type*
CD-ROM Mitsumi, estándar	`mcd.o`	mcd=*io_port,IRQ*
CD-ROM Mitsumi, experimental	`mcdx.o`	mcdx=*io_port_1,IRQ_1, io_port_n,IRQ_n*
Lector de CD-ROM de memorización óptica 8000 AT "Dolphin", Lasermate CR328A	`optcd.o`	

Hardware	Módulo	Parámetros
CD-ROM IDE de puerta paralela	`pcd.o`	
Tarjeta audio compatible 16 Compatible	`sbpcd.o`	sbpcd=*io_port*
CDR-H94A Sanyo	`sjcd.o`	sjcd=*io_port OR* sjcd_base=*io_port*
Sony CDU-535 & 531 (unidades Procomm)	`sonycd535.o`	sonycd535=*io_port*

A continuación le mostramos algunos ejemplos:

Tabla A–2 Ejemplo de configuración para los parámetros hardware

Configuración	Ejemplo
CD-ROM de ATAPI, puenteado como maestro en el segundo canal IDE	hdc=cdrom
CD-ROM Mitsumi no IDE en el puerto 340, IRQ 11	mcd=0x340,11
Tres lectores de CD-ROM Mitsumi no IDE que utilizan el controlador experimental, en los puertos 300, 304 y 320 con IRQs 5, 10 y 11	mcdx=0x300,5,0x304,10,0x320,11
CDU Sony 31 o 33 en el puerto 340, no IRQ	cdu31=0x340,0 *OR* cdu31_port=0x340 cdu31a_irq=0
CD-ROM Aztech en el puerto 220	aztcd=0x220
CD-ROM de tipo Panasonic en una interfaz SoundBlaster en el puerto 230	sbpcd=0x230,1
Phillips/LMS cm206 and cm260 at IO 340 and IRQ 11	cm206=0x340,11
Goldstar R420 at IO 300	gscd=0x300
Lector Mitsumi en una tarjeta de sonido MAD16 enIO Addr 330 y IRQ 1, probing DMA	isp16=0x330,11,0,Mitsumi
Sony CDU 531 en la dirección IO 320	sonycd535=0x320

Nota

La mayoría de tarjetas Sound Blaster tienen una interfaz IDE. Para estas tarjetas, no es necesario utilizar los parámetros `sbpcd`, utilice sólo los parámetros `hdx`.

A.3 Parámetros SCSI

Tabla A–3 Parámetros SCSI

Hardware	Módulo	Parámetros
Controlador de almacenamiento de 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Driver AM53/79C974 (PC-SCSI) Driver	`AM53C974.o`	
Casi todas las tarjetas Buslogic (actualmente Mylex) con número "BT"	`BusLogic.o`	BusLogic_Options=*option,option,…*
Controlador RAID Mylex DAC960	`DAC960.o`	
SCSI basado en MCR53c406a	`NCR53c406a.o`	
Initio INI-9100UW	`a100u2w.o`	a100u2w=*io,IRQ,scsi_id*
Adaptec AACRAID	`aacraid.o`	
Tarjetas SCSI	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*io,IRQ,scsi_id*
Adaptec AHA 154x amd 631x-based	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Hardware	Módulo	Parámetros
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x, AIC-789x, AIC-3860	`aic7xxx.o`	aic7xxx=*string*
Controlador SCSI ACARD ATP870U PCI	`atp870u.o`	
Controlador Compaq Smart Array 5300	`cciss.o`	
Controlador RAID Compaq Smart/2	`cpqarray.o`	
Controlador Compaq FibreChannel	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	

Hardware	Módulo	Parámetros
DTP SCSI host adapters (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	eata=*port0*,*port1*,*port2*,… *options OR* eata io_port=*port0*,*port1*,*port2*,… option=*value*
DTP SCSI Adapters PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
DTP EATA-PIO boards	`eata_pio.o`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (generic driver)	`g_NCR5380.o`	
Controlador RAID ICP	`gdth.o`	
Controlador de bloque I2O	`i2o_block.o`	
Adaptador SCSI en puerto paralelo IOMEGA MatchMaker	`imm.o`	
Tarjeta SCSI ISA Always IN2000	`in2000.o`	in2000=*setup_string*:*value O* in2000 *setup_string=value*
Adaptadores de host SCSI Initio INI-9X00U/UW	`initio.o`	
ServeRAID IBM	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	

Hardware	Módulo	Parámetros
Controladores SCSI INCR con chipsets 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*option1*:*value1*,*option2*:*value2*,… *OR* ncr53c8xx="*option1*:*value1 option2*:*value2*…"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
RAID PCI-2220I EIDE	`pci2220i.o`	
Array SparcSTORAGE	`pluto.o`	
Adaptador de host SCSI en puerto paralelo IOMEGA PPA3	`ppa.o`	
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
Tarjetas SCSI QLogic ISP1020 Intelligent IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
Qlogic ISP1020 SCSI SBUS	`qlogicpti.o`	
Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	
Future Domain TMC-885, TMC-950	`seagate.o`	controller_type=2 base_address=*base_addr* irq=*IRQ*
Tarjetas con el chipset sym53c416	`sym53c416.o`	sym53c416=*PORTBASE*,*[IRQ]* *OR* sym53c416 io=*PORTBASE* irq=*IRQ*

Hardware	Módulo	Parámetros
Adaptador de host SCSI Trantor T128/T128F/T228	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (not 24F)	`u14-34f.o`	
UltraStor 14F, 24F y 34F	`ultrastor.o`	
Series WD7000	`wd7000.o`	

Le mostramos algunos ejemplos sobre la utilización de estos parámetros:

Tabla A–4 Ejemplos de configuración de parámetros SCSI

Configuración	Ejemplo
Adaptec AHA1522 at port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 en el puerto 330	bases=0x330
Future Domain TMC-800 at CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

A.4 Parámetros Ethernet

Tabla A–5 Parámetros del módulo EthernetEthernet

Hardware	Módulo	Parámetros
3Com 3c501	`3c501.o`	3c501=*io_port,IRQ*
3Com 3c503 and 3c503/16	`3c503.o`	3c503=*io_port,IRQ OR* 3c503 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_n*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*io_port,IRQ OR* 3c505 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_2*
3Com EtherLink 16	`3c507.o`	3c507=*io_port,IRQ OR* 3c507 io=*io_port* irq=*IRQ*
3Com EtherLink III	`3c509.o`	3c509=*IRQ*

Hardware	Módulo	Parámetros
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Model 3200	`ac3200.o`	ac3200=*io_port,IRQ O* ac3200 io=*io_port_1*,*io_port_n* irq=*IRQ_1*,*IRQ_n*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Aironet 4500 PCI-ASI-i365 inalámbrico	`aironet4500_card.o`	
Allied Telesis AT1700	`at1700.o`	at1700=*io_port,IRQ O* at1700 io=*io_port* irq=*IRQ*
Tangent ATB-II, Novel NL-10000, Daystar Digital LT-200, Dayna DL2000, DaynaTalk PC (HL), COPS LT-95, Farallon PhoneNET PC II, III	`cops.o`	cops=*io_port,IRQ OR* cops io=*io_port* irq=*IRQ*
Controlador modular para la tarjeta serie sincrónica COSA o SRP	`cosa.o`	cosa=*io_port,IRQ,dma*
Crystal Semiconductor CS89[02]0	`cs89x0.o`	

Hardware	Módulo	Parámetros
EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, tarjetas Znyx31[45], and Znyx346 10/100 con chipsets DC21040 (no SROM), DC21041[A], DC21140[A], DC21142, DC21143	`de4x5.o`	de4x5=*io_port OR* de4x5 io=*io_port* de4x5 args='eth*X[fdx]* autosense=*MEDIA_STRING*'
Adaptador de bolsillo Ethernet D-Link DE-600	`de600.o`	
Adaptador de bolsillo Ethernet D-Link DE-620	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=*io_port,IRQ OR* depca io=*io_port* irq=*IRQ*
Digi Intl. RightSwitch SE-X EISA y PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*io_port,IRQ,mem OR* e2100 io=*io_port* irq=*IRQ* mem=*mem*

Hardware	Módulo	Parámetros
Intel EtherExpress Pro10	`eepro.o`	eepro=*io_port*,*IRQ OR* eepro io=*io_port* irq=*IRQ*
Intel i82557/i82558 PCI EtherExpressPro driver	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*io_port*,*IRQ O* eexpress io=*io_port* irq=*IRQ*
SMC EtherPower II 9432 PCI (83c170/175 EPIC series)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*io_port*,*IRQ OR* eth16i ioaddr=*io_port* IRQ=*IRQ*
EtherWORKS 3 (DE203, DE204 and DE205)	`ewrk3.o`	ewrk=*io_port*,*IRQ O* ewrk io=*io_port* irq=*IRQ*
Fujitsu FMV-181/182/183/184	`fmv18x.o`	fmv18x=*io_port*,*IRQ O* fmv18x io=*io_port* irq=*IRQ*
Paquete Engines GNIC-II Gigabit	`hamachi.o`	
Driver modular para el Comtrol Hostess SV11	`hostess_sv11.o`	hostess_sv11=*io_port*,*IRQ*, *DMABIT OR* hostess_sv11 io=*io_port* irq=*IRQ* dma=*DMABIT*
HP PCLAN/plus	`hp-plus.o`	hp-plus=*io_port*,*IRQ OR* hp-plus io=*io_port* irq=*IRQ*
HP LAN Ethernet	`hp.o`	hp=*io_port*,*IRQ OR* hp io=*io_port* irq=*IRQ*

Hardware	Módulo	Parámetros
Adaptador de red 100VG-AnyLan HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*io_port,name O* hp100 hp100_port=*io_port* hp100_name=*name*
IBM Token Ring 16/4	`ibmtr.o`	ibmtr=*io_port,IRQ,mem OR* ibmtr io=*io_port* irq=*IRQ* mem=*mem*
AT1500, HP J2405A, la mayoría de NE2100/clone	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
	`ltpc.o`	ltpc=*io_port,IRQ OR* ltpc io=*io_port* irq=*IRQ*
MyriCOM MyriNET SBUS	`myri_sbus.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (non-pci)	`ne.o`	ne=*io_port,IRQ O* ne io=*io_port* irq=*IRQ*
PCI NE2000 cards RealTEk RTL-8029, Winbond 89C940, Compex RL2000, KTI ET32P2, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
Tarjeta NI5210 (chip i82586 Ethernet)	`ni52.o`	ni52=*io_port,IRQ OR* ni52 io=*io_port* irq=*IRQ*
NI6510 Ethernet	`ni65.o`	

Hardware	Módulo	Parámetros
Older DEC 21040, most 21*40 Ethernet	`old_tulip.o`	old_tulip=*io_port OR* old_tulip io=*io_port*
AMD PCnet32 y AMD PCnetPCI	`pcnet32.o`	
Comunicaciones PCI RedCreek	`rcpci.o`	
Tarjetas RealTek que usan RTL8129 o RTL8139 chipsets Ethernet rápidos	`rtl8139.o`	
Sangoma S502/S508 multi-protocol FR	`sdla.o`	
Sangoma S502A, ES502A, S502E, S503, S507, S508, S509	`sdladrv.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.o`	
Adaptador ISA/PCISysKonnect Token Ring, TR4/16(+) ISA o PCI, TR4/16 PCI y antiguas tarjetas SK NET TR4/16 ISA	`sktr.o`	sktr=*io_port*,*IRQ*,*mem O* sktr io=*io_port* irq=*IRQ* mem=*mem*
Tarjetas ether SMC Ultra y SMC EtherEZ ISA (8K, 83c790)	`smc-ultra.o`	smc-ultra=*io_port*,*IRQ O* smc-ultra io=*io_port* irq=*IRQ*
Tarjeta Ethernet SMC Ultra32 EISA (32K)	`smc-ultra32.o`	
Series de tarjetas Ethernet SMC 9000	`smc9194.o`	smc9194=*io_port*,*IRQ O* smc9194 io=*io_port* irq=*IRQ* ifport=*[0,1,2]*
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	

Hardware	Módulo	Parámetros
Sun Happy Meal Ethernet	`sunhme.o`	
Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
Digital 21x4x Tulip PCI Ethernet cards SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	
Tarjetas Ethernet rápidas PCI VIA Rhine con VIA VT86c100A Rhine-II PCI o 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	
Tarjeta ISA AT&T GIS (nee NCR) WaveLan	`wavelan.o`	wavelan=*[IRQ,0],io_port,NWID*
Tarjetas Ethernet compatibles con WD8003 and WD8013	`wd.o`	wd=*io_port,IRQ,mem, mem_end OR* wd io=*io_port* irq=*IRQ* mem=*mem* mem_end=*end*
Compex RL100ATX-PCI	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
Tarjetas HDLCZ basadas en 8530 para AX.25	`z85230.o`	

A continuación le ponemos algunos ejemplos de estos módulos.

Tabla A–6 Ejemplos de configuración de parámetros Ethernet

Configuración	Ejemplo
Tarjeta ISA NE2000 en dirección IO 300 yIRQ 11	ne=0x300,11 ether=0x300,11,eth0
Tarjeta Wavelan en IO 390, autoprueba para IRQ y uso del NWID para 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

A.4.1 Utilización de múltiples tarjetas Ethernet

Puede usar más de una tarjeta Ethernet en una máquina. Si cada tarjeta utiliza un controlador diferente (por ejemplo, un 3c509 y un DE425), deberá sencillamente añadir `alias` (y posiblemente `opciones`) a cada una de las tarjetas en `/etc/conf.modules`. Consulte la *Official Red Hat Linux Customization Guide* para más información al respecto.

Si dos tarjetas Ethernet utilizan el mismo controlador (por ejemplo, dos 3c509 o una 3c595 y una 3c905), necesitará especificar en la línea de las opciones del controlador las direcciones de ambas tarjetas (en el caso de las tarjetas ISA) o (en el caso de las tarjetas PCI) deberá añadir una línea de `alias` para cada una de las tarjetas.

Para ulterior información sobre el uso de más de una tarjeta Ethernet, consulte la *Linux Ethernet-HOWTO* en http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

B Introducción a la creación de particiones

Las particiones en el disco son partes estándar de los entornos de un ordenador y lo han sido durante bastante tiempo. De todas formas, con tantas personas que compran un ordenador con un sistema operativo preinstalado, pocas entienden el funcionamiento de las particiones. Este capítulo trata de explicar cómo funcionan las particiones de manera que pueda encontrar la instalación de Red Hat Linux lo más sencilla posible.

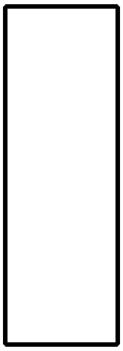
Si ya conoce cómo funcionan las particiones de los discos, debería seguir más adelante con la Sección B.1.4, *Crear espacio para Red Hat Linux* para obtener más información relativa al proceso de liberar espacio en el disco para efectuar una instalación de Red Hat Linux. Esta sección, además, le muestra el esquema utilizado en Linux para asignar los nombres a las particiones, para compartir el espacio del disco con otros sistemas operativos y otros temas relacionados con ello.

B.1 Conceptos básicos sobre el disco duro

Los discos duros cumplen una función muy sencilla -- pueden contener datos y recuperarlos de manera segura si se lo pedimos.

Para crear particiones en el disco, es importante saber algo del hardware; desafortunadamente, es fácil confundirse. Por lo que utilizaremos un gráfico sencillo del ordenador de un disco duro para que nos ayude en la explicación que lo que hay "detrás de la caja" del ordenador. El Gráfico B–1, *Unidad no utilizada* muestra una unidad disco que no está utilizada.

Gráfico B–1 Unidad no utilizada

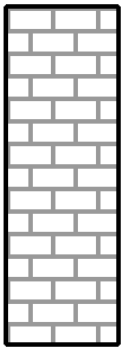


… No hay mucho que añadir. Sin embargo si hablamos de discos duros a nivel básico, el asunto cambia. Supongamos que queremos guardar unos datos en un disco. Según están las cosas, no funcionará. Tenemos que hacer algo antes ….

B.1.1 No se trata de lo que escribe, sino de cómo lo escribe

Aquéllos que ya han utilizado Red Hat Linux, probablemente ya han ejecutado estas operaciones. Tendrá que **formatear** el disco. El formateo (es "la creación de un **sistema de archivos**") que escribe informaciones en el disco, ordenando el espacio vacío en un disco no formateado.

Gráfico B–2 Unidad de disco con un sistema de archivos



Como en el Gráfico B–2, *Unidad de disco con un sistema de archivos*, el orden seguido en un sistema de archivos presupone unas concesiones.

- Un pequeño porcentaje del espacio disponible en el disco es utilizado para grabar los datos relativos al sistema de archivos y puede ser considerado como sobrecarga.
- Un sistema de archivos parte el espacio que queda en pequeños segmentos de tamaño consistente. En el mundo de Linux, estos segmentos son conocidos como **bloques**. [1]

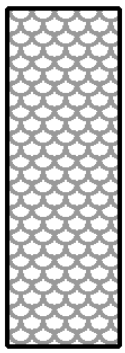
Puesto que los sistemas de ficheros hacen posibles cosas como la creación de ficheros y directorios, estas concesiones son aceptadas como pequeños precios que hay que pagar.

También es verdad que no hay un único y universal sistema de archivos; como muestra el Gráfico B–3, *Unidad de disco duro con un sistema de archivos diferente*, un disco puede tener uno o más sistemas de archivos distintos. Como puede imaginar, distintos sistemas de archivos tienden a no ser compatibles entre ellos; esto quiere decir que un sistema operativo que soporta un tipo de sistema de archivos (o más) no tendrá necesariamente que soportar otro sistema de archivos diferente. Esto que acabamos

[1] Los bloques *son* de un tamaño consistente, distinto de las imágenes. Ponga atención en el hecho de que un disco duro contiene miles de bloques. Sin embargo, visto el objetivo de nuestra explicación, ignore estas pequeñas diferencias.

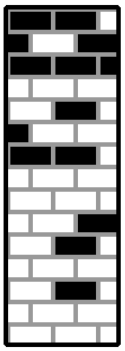
de decir no es una ley exacta. Por ejemplo, Red Hat Linux soporta una gran variedad de sistemas de archivos (incluidos los más comunes soportados por otros sistemas operativos) haciendo más sencillo el intercambio de datos.

Gráfico B–3 Unidad de disco duro con un sistema de archivos diferente



Escribir un sistema de archivos es sólo el principio. El objetivo de este proceso es realmente el de *almacenar* y *recuperar* datos. Observe como queda su unidad tras la escritura de algunos archivos.

Gráfico B–4 Unidad de disco duro con datos escritos



Como muestra el Gráfico B–4, *Unidad de disco duro con datos escritos*, 14 de los bloques que antes estaban vacíos, ahora contienen datos. No podemos establecer cuántos ficheros se encuentran en este disco; podría ser uno o 14 puesto que todos los ficheros utilizan por lo menos un bloque. Otro aspecto importante a observar es que los bloques utilizados no tienen necesariamente una región continua; los bloques utilizados pueden encontrarse en posiciones separadas. Este concepto se conoce como **fragmentación**. La fragmentación puede realizar un papel muy importante cuando se trata de reducir una partición existente.

Con el paso del tiempo y el avance de las tecnologías relacionadas con el ordenador, también las unidades de disco han cambiado. En concreto, han cambiado de una forma específica -- los discos son más grandes. No grandes por tamaño, sino por capacidad. Y ha sido esta capacidad la que ha llevado a un cambio en la manera en que se utilizan los discos.

B.1.2 Particiones: Covertir un disco en muchos otros

Como las unidades de disco aumentan su capacidad, algunas personas llegadas a este punto se preguntan si es conveniente tener todo ese espacio formateado junto. Esta forma de pensar ha sido debatida por diversas tesis, algunas filosóficas, otras técnicas. Bajo el punto de vista filosófico, parece que el espacio añadido en un disco de tamaño más grande, crea sólo confusión. Bajo el punto de vista técnico se defiende que algunos sistemas de archivos nunca han sido proyectados para soportar discos de este

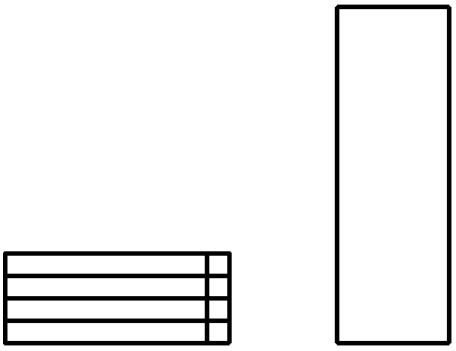
tamaño. O bien, que los sistemas de archivos *podían* soportar discos más grandes, pero el tamaño que ocuparía el sistema de ficheros es excesivo.

La solución a este problema ha sido la de partir los discos creando más **particiones**. Se puede acceder a cada partición como si fuese un disco a parte. Esto se hace por medio de una **tabla de particiones**.

Nota

Cuando los diagramas de este capítulo muestran la tabla de las particiones separada de la restante parte del disco, esto no es exacto. En realidad la tabla de particiones se guarda al comienzo del disco, antes de cualquier dato o sistema de archivos. Sin embargo, para ser más claros la mantendremos separada.

Gráfico B–5 Disco duro con la tabla de particiones



Como se muestra en el Gráfico B–5, *Disco duro con la tabla de particiones*, la tabla de las particiones está repartida en cuatro secciones. Cada sección puede contener la información necesaria para definir una partición, esto quiere decir que la tabla de las particiones puede definir no más de cuatro particiones.

Cada elemento de la tabla de las particiones contiene importantes características relativas a la partición:

- Puntos en el disco donde la partición empieza y termina.
- Si la partición está "activa".
- Tipo de partición.

Observe detenidamente cada característica. Los puntos de comienzo y de fin realmente definen el tamaño de las particiones y su posición en el disco. La opción "activa" es utilizada en el arranque de algunos sistemas operativos. De todas formas, el sistema operativo que se encuentra con la partición definida como "activa" es donde arrancará el ordenador.

El tipo de partición puede crear confusión. El tipo es un número que define previamente el uso que se hará de la partición. Si esto le parece un poco extraño es porque incluso el significado del tipo de partición es un poco vago. Algunos sistemas operativos utilizan un tipo de partición para detectar un tipo específico de sistema de archivos, para asociar la partición a un sistema operativo, para indicar que la partición contiene un sistema operativo que puede ser arrancado o para una combinación de los tres.

La Tabla B–1, *Tipos de particiones* contiene una lista de algunos tipos de particiones de las más conocidas (y oscuras), junto a sus valores numéricos.

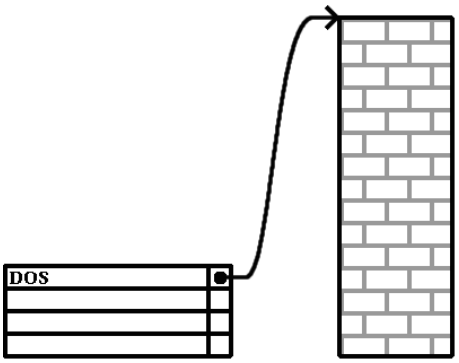
Tabla B–1 Tipos de particiones

Tipos de particiones	Valor	Tipo de partición	Valor
Vacío	00	Novell Netware 386	65
DOS 12-bit FAT	01	PIC/IX	75
XENIX root	02	Old MINIX	80
XENIX usr	03	Linux/MINUX	81
DOS 16-bit <=32M	04	Linux swap	82
Extended	05	Linux native	83
DOS 16-bit >=32	06	Linux extendido	85
OS/2 HPFS	07	Amoeba	93
AIX	08	Amoeba BBT	94
AIX de arranque	09	BSD/386	a5
Gestor de arranque OS/2	0a	OpenBSD	a6

Tipos de particiones	Valor	Tipo de partición	Valor
Win95 FAT32	0b	NEXTSTEP	a7
Win95 FAT32 (LBA)	0c	BSDI fs	b7
Win95 FAT16 (LBA)	0e	BSDI swap	b8
Win95 extendido (LBA)	0f	Syrinx	c7
Venix 80286	40	CP/M	db
Novell	51	DOS access	e1
Microport	52	DOS R/O	e3
GNU HURD	63	DOS secundario	f2
Novell Netware 286	64	BBT	ff

Ahora estará preguntándose como se utiliza esta complejidad añadida. Véase el Gráfico B–6, *Disco duro con una sola partición* para tener un ejemplo.

Gráfico B–6 Disco duro con una sola partición



En muchos casos hay una única partición que ocupa todo el disco. La tabla de las particiones en este caso muestra sólo un elemento y se encuentra al comienzo de la partición.

Hemos llamado a esta partición como si fuera de tipo "DOS", también, como puede ver en la Tabla B–1, *Tipos de particiones*, esto es un poco simplista, pero útil para nuestra explicación. Esta es una configuración típica de las particiones en la mayor parte de los ordenadores en que hay una versión pre-instalada de Windows.

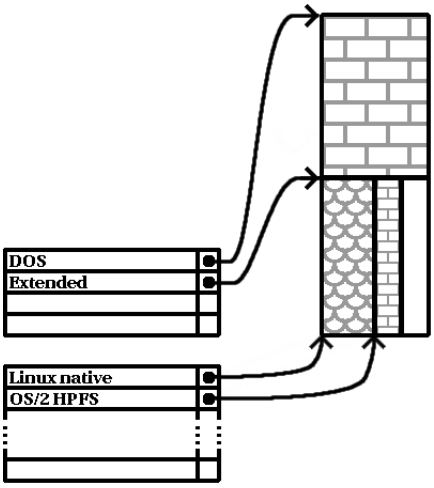
B.1.3 Particiones en el interior de particiones – Una introducción a las particiones extendidas.

El paso del tiempo ha evidenciado el hecho de que cuatro particiones no bastan. Al crecer las dimensiones de los discos duros, se ha vuelto siempre más común la utilización de particiones de tamaño considerable y a pesar de ello es normal que quede espacio libre en el disco. Era necesario buscar soluciones nuevas para crear más particiones.

De este modo nacen las particiones extendidas. Como habrá visto en la Tabla B–1, *Tipos de particiones*, hay una partición de tipo "extendida". Es un tipo de partición que representa el núcleo de las particiones extendidas.

Cuando se crea una partición y es seleccionada como tipo "extendida", se crea una tabla de las particiones extendidas. De hecho, una partición extendida es una unidad disco con todas sus características -- Tiene incluso una tabla de las particiones que señala una o más particiones (ahora llamadas **Particiones Lógicas**, en vez de las primeras cuatro **Particiones Primarias**) contenidas por entero en el interior de la misma partición extendida. El Gráfico B–7, *Unidad disco con partición extendida* muestra una unidad disco con una partición primaria que contiene dos particiones lógicas (junto con el espacio libre no utilizado).

Gráfico B–7 Unidad disco con partición extendida



Como puede verse en esta figura, hay diferencia entre particiones lógicas y primarias -- sólo se pueden crear cuatro particiones primarias, sin embargo no hay ningún límite para el número de particiones lógicas.)(De todas formas, no es una buena idea intentar crear más de 12 particiones en la misma unidad).

Ahora que hemos tratado de forma general el asunto sobre las particiones, podemos aplicar estos conocimientos en la instalación de Red Hat Linux.

B.1.4 Crear espacio para Red Hat Linux

Hay tres posibles casos que se puede encontrar durante la creación de particiones en el disco:

- Hay espacio libre disponible sin particiones
- Partición inusual disponible
- Hay espacio libre disponible en una partición utilizada

Veamos estos casos por orden.

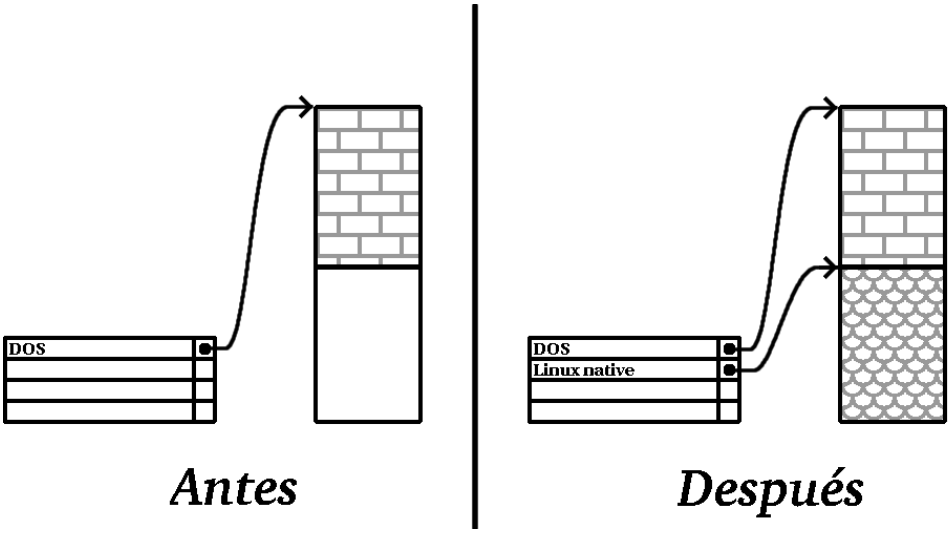
Nota

Tiene que considerar que las imágenes que se muestran a continuación han sido simplificadas para que queden más claras y no muestran la estructura general de las particiones que encontrará durante la instalación de Red Hat Linux.

Uso del espacio libre no particionado

En este caso, las particiones ya definidas no ocupan el disco por entero, dejando espacio no ocupado que no forma parte de ninguna partición definida. El Gráfico B–8, *Unidad de disco con espacio libre no utilizado para particiones* muestra un ejemplo de esta situación.

Gráfico B–8 Unidad de disco con espacio libre no utilizado para particiones



Si se fija, un disco que no ha sido utilizado puede también incluirse en esta categoría; la única diferencia es que *todo* el espacio está libre y no pertenece a ninguna partición definida.

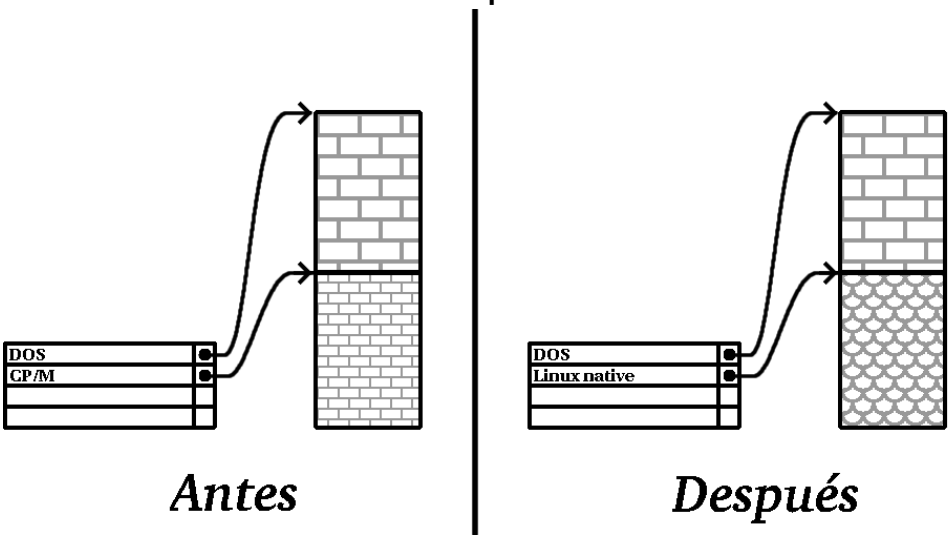
De todas formas, podrá simplemente crear las particiones necesarias del espacio no utilizado. Desafortunadamente, esta situación, tan sencilla, no es común (a menos que haya comprado un disco nuevo sólo para Red Hat Linux). La mayoría de los sistemas operativos pre-instalados están configurados para ocupar todo el espacio disponible de la unidad de disco (vea el *Uso del espacio libre de una partición activa* en la sección B.1.4).

Veamos una situación un poco más habitual.

Uso del espacio de una partición no utilizada

En este caso, puede ser que tenga una o más particiones que no utiliza; quizás había utilizado otro sistema operativo y las particiones (o la partición) que le había dedicado no se utilizarán más. El Gráfico B–9, *Disco duro con una partición no utilizada* muestra una situación parecida.

Gráfico B–9 Disco duro con una partición no utilizada



Si se encuentra en esta situación, puede utilizar el espacio usado por la partición no utilizada. Tendrá en primer lugar que borrar la partición y luego crear las particiones necesarias para Linux. Podrá borrar la partición utilizando el comando `fdisk` de DOS, tendrá la posibilidad de hacerlo también durante la instalación de clase personalizada.

Uso del espacio libre de una partición activa

Ésta es la situación más común. Desafortunadamente es también la más difícil de gestionar. De hecho, el problema es que, aunque tenga bastante espacio libre, éste es ocupado por una partición que ya ha sido utilizada. Si ha comprado un ordenador con unos programas (incluido el sistema operativo) preinstalados, el disco duro probablemente tiene una gran partición que contiene todos los datos y el sistema operativo.

Aparte de añadir un nuevo disco duro a su sistema, tendrá dos soluciones posibles:

Creación destructiva de particiones

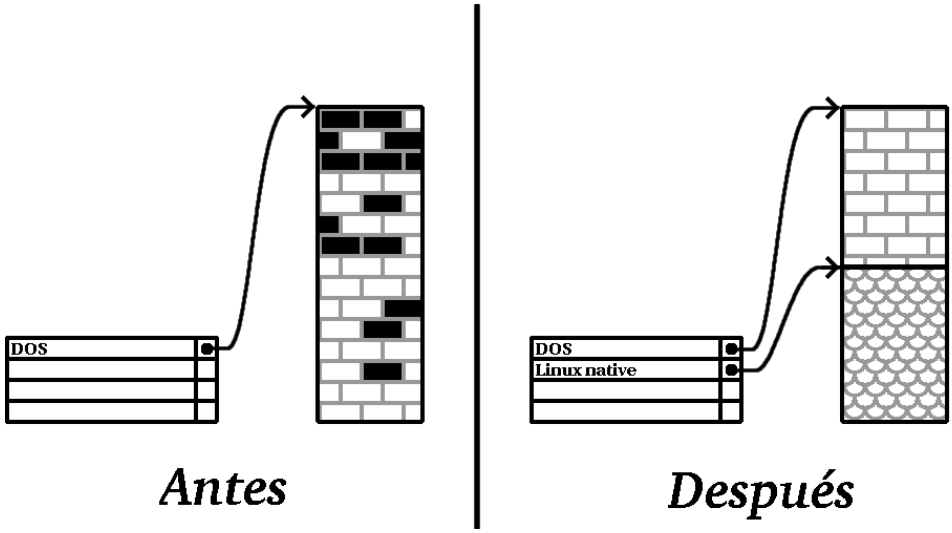
Haga lo siguiente: borre la partición única y cree particiones más pequeñas. Como puede imaginar, todos los datos que tenía en la partición original serán destruidos. Esto quiere decir que es preciso hacer una copia de seguridad antes de comenzar. Por su seguridad haga dos copias, utilice la verificación (si lo permite su programa de hacer copias de seguridad) e intente leer los datos de esas copias *antes* de empezar el proceso de creación de particiones.

ATENCION

Si había un sistema operativo instalado en la partición, deberá volver a instalarlo. Sepa que algunos ordenadores vendidos con sistemas operativos preinstalados, no incluyen CD-ROM(s) para reinstalar el sitema operativo inicial. Es conveniente que compruebe si es éste el caso de su sistema *antes* de destruir su partición original y la instalación de su sistema operativo.

Después de haber creado una partición más pequeña para el software existente, podrá reinstalar cualquier software, recuperar sus datos y seguir con la instalación de Red Hat Linux. El Gráfico B–10, *Disco duro particionado de forma no destructiva* muestra esta operación.

Gráfico B–10 Disco duro particionado de forma no destructiva



Como se muestra en la figura del Gráfico B–10, *Disco duro particionado de forma no destructiva*, ¡todos los datos presentes en la partición original se perderán sin la posibilidad de recuperarlos!

Reparticionamiento no destructivo

Podrá ejecutar un programa que hace lo que parece imposible: crea una partición más pequeña sin perder ninguno de los ficheros contenidos en la partición primaria. Muchos usuarios han encontrado este método seguro sin que plantee demasiados problemas. ¿Qué software debería usar para cumplir con esta tarea? Hay varios programas de gestión del disco duro disponibles en el mercado; tendrá que buscar lo que mejor se adapte a su situación.

Aunque el proceso de re-particionamiento no destructivo es bastante fácil, hay siempre algunos pasos que seguir:

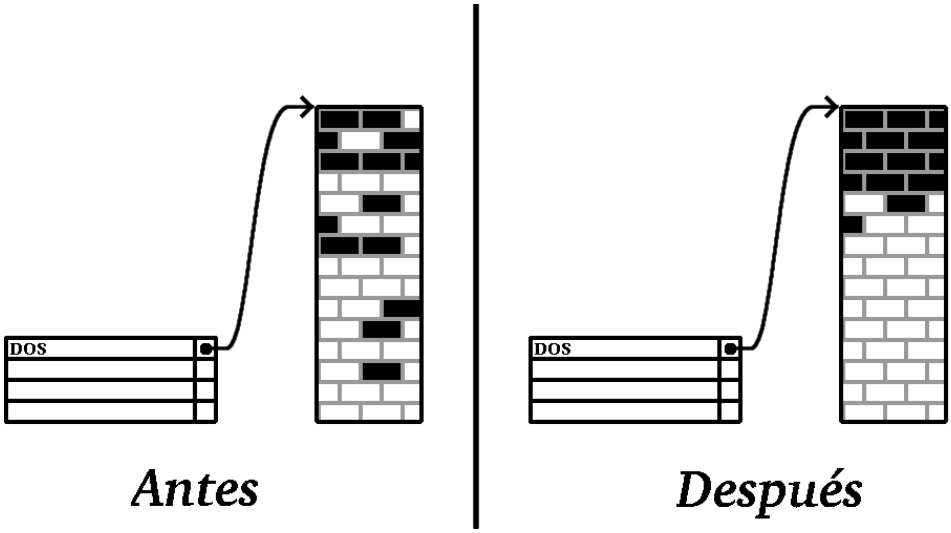
- Comprimir los datos existentes
- Reducir la partición
- Crear nuevas particiones

Veamos cada paso con más detalle.

Comprimir los datos existentes

Como se muestra en el Gráfico B–11, *Disco duro durante la compresión*, el primer paso es el de comprimir los datos de la partición existente. La razón de esta operación es la de reorganizar los datos para maximizar el espacio libre disponible al final de la partición.

Gráfico B–11 Disco duro durante la compresión

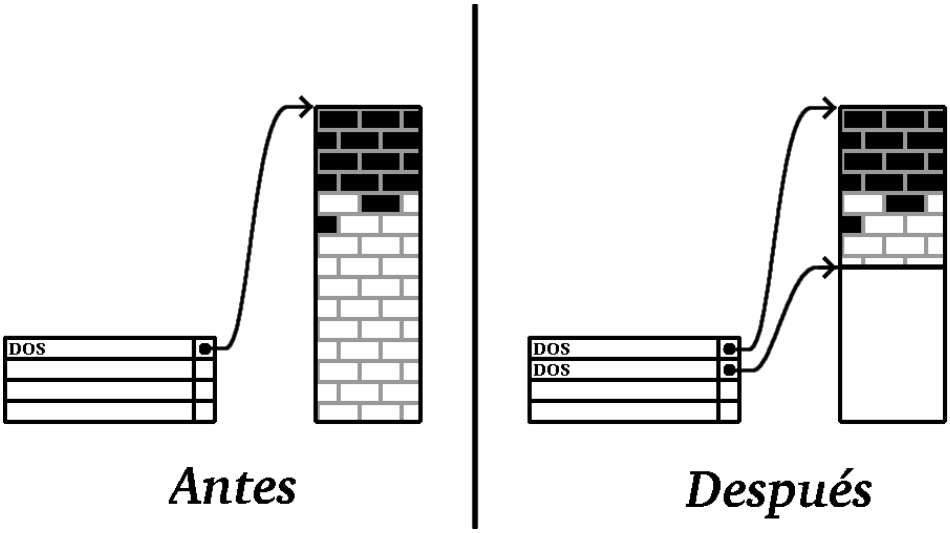


Este paso es crucial; sin ello, es posible que la posición de sus datos impida que la partición sea reducida de forma deseada. Ponga también atención en que, por una u otra razón, podrían no ser desplazados. Si éste es su caso (y es imposible la creación de su nueva partición), se verá forzado a realizar un particionamiento destructivo.

Cambiar el tamaño de una partición

El Gráfico B–12, *Disco duro con la partición de tamaño cambiada* muestra el proceso del cambio de tamaño. El resultado final de la operación de cambio puede variar según el software utilizado, pero en muchos casos el espacio que ha quedado libre es utilizado para crear una partición no formateada del mismo estilo de la partición original.

Gráfico B–12 Disco duro con la partición de tamaño cambiada

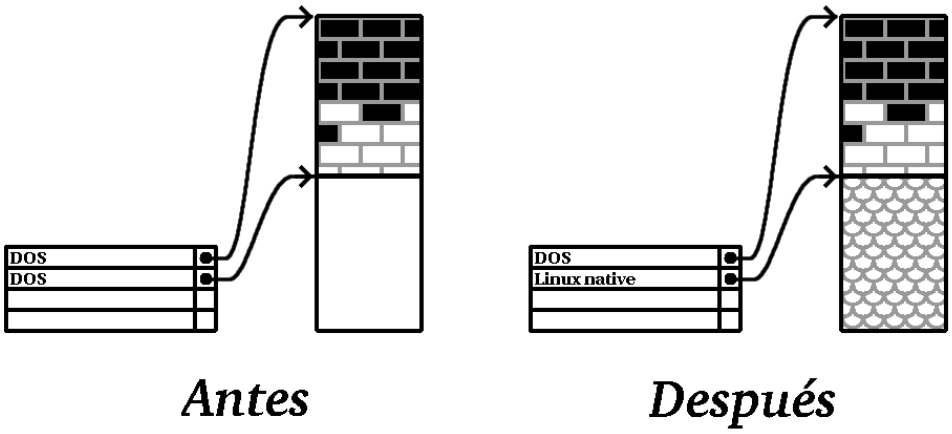


Es importante comprender cómo trabaja el software para cambiar el tamaño de las particiones que ha utilizado y dejar espacio libre en el disco, así que hay que seguir los pasos adecuados. En el caso que le hemos mostrado, sería mejor borrar la nueva partición DOS y crear las particiones para Linux.

Creación de nuevas particiones

Como indica el paso anterior, puede resultar necesario o no crear nuevas particiones. Sin embargo a menos que su software tenga en cuenta la existencia de Linux, ese será el proceso que se deberá seguir. Veáse el Gráfico B–13, *Disco duro con una configuración de particiones finales*.

Gráfico B–13 Disco duro con una configuración de particiones finales



Nota

La siguiente información es específica sólo para ordenadores basados en la tecnología Intel.

Éste es un programa distribuido libremente que puede cambiar el tamaño de particiones FAT (File Allocation Table).

ADVERTENCIA

Muchas personas han utilizado con éxito `fips` para crear particiones en sus discos duros. Sin embargo, a causa de la clase de operaciones que `fips` debe hacer y las diferencias entre las distintas configuraciones hardware en las que debería ejecutarse, Red Hat no puede garantizar que `fips` funcione correctamente en su sistema. No hay disponible ningún soporte para la instalación de `fips`; *utilícelo teniendo en cuenta que lo hace bajo su responsabilidad*.

Si elige crear particiones en el disco duro con `fips`, es *muy importante* que haga dos cosas:

- *Efectúe una copia de seguridad* — Haga dos copias de todos los datos importantes presentes en su ordenador. Estas copias tendrá que hacerlas en dispositivos extraibles (como cintas magnéticas o disquetes) y antes de empezar tendrá que averiguar si pueden ser legibles.
- *Lectura de la Documentación* — -- Lea completamente la documentación de `fips`, que se encuentra en el subdirectorio `/dosutils/fipsdocs` en el primer CD de Red Hat Linux/x86.

Si elige utilizar `fips`, tenga cuidado ya que después de haber lanzado `fips` obtendrá *dos* particiones: la que ha cambiado de tamaño y la que `fips` ha creado en el espacio que la primera ha dejado libre. Si su objetivo es el de utilizar este espacio para instalar Red Hat Linux, tendrá que borrar la partición que acaba de crear, utilizando `fdisk` bajo el sistema operativo actual y configurando las particiones durante la instalación de clase personalizada.

B.1.5 Ficha de los nombres para las particiones

Linux hace referencia a las particiones del disco duro utilizando un conjunto de números y letras que le puede confundir, especialmente si está acostumbrado al método de referencia "unidad C" para los discos y las particiones. En el mundo DOS/Windows, las particiones son llamadas así

- Cada tipo de partición es controlada para determinar si puede ser leída por DOS/Windows.
- Si el tipo de partición es compatible, se le asigna una letra. Las letras de los discos empiezan por la C" y van pasando a letras sucesivas dependiendo de el número de particiones a etiquetar.
- La letra del disco puede, entonces, ser utilizada para referirse tanto a esta partición como al sistema de ficheros contenido en esta partición.

Red Hat Linux utiliza un esquema de nombres que es mucho más flexible y contiene mucha más información que el que usan otros sistemas operativos. Este esquema tiene nombres de ficheros de la siguiente manera:

`/dev/`*`xxyN`*

Aquí tiene el método para entender el esquema del nombre de la partición:

`/dev/`

Esta cadena es el nombre de un directorio en la que están todos los ficheros de los dispositivos. Puesto que las particiones residen en el disco y los discos duros son dispositivos, los ficheros que representan todas las posibles particiones están contenidos en `/dev/`.

`xx`

Las dos primeras letras del nombre de la partición se refieren al tipo de periférico en el que se encuentra la misma partición. En general, encontrará o `hd` (para discos IDE), o `sd` (para discos SCSI).

y

Esta letra indica en qué periférico se encuentra la partición. Por ejemplo, `/dev/hda` (El primer disco duro IDE) o `/dev/sdb` (el segundo disco duro SCSI).

N

El número que aparece al final indica la partición. Las cuatro primeras (primarias o extendidas) se enumeran a partir de `1` hasta `4`. Las particiones lógicas empiezan en `5`. Por ejemplo, `/dev/hda3` es la tercera partición primaria o extendida en el primer disco IDE; `/dev/sdb6` es la segunda partición lógica en el segundo disco SCSI.

Nota

No hay ninguna parte de esta convención que se base en un tipo de partición; a diferencia de DOS/Windows, *todas* las particiones pueden identificarse bajo Red Hat Linux. Por supuesto, esto no quiere decir que Red Hat Linux puede acceder a los datos en cualquier tipo de partición, pero en muchos casos es posible acceder a los datos de particiones dedicadas a otros sistemas operativos.

Considerar esta información le hará más sencillas las cosas a la hora de configurar las particiones requeridas por Red Hat Linux.

B.1.6 Particiones y otros sistemas operativos

Aunque las particiones de Red Hat Linux dividirán el disco duro en particiones utilizadas por otros sistemas operativos, en general no tendrá ningún problema. De todas formas, hay algunas combinaciones entre Linux y otros sistemas operativos que le pedirán más precauciones. Más información sobre la creación de particiones del disco compatibles con otros sistemas operativos están disponibles en muchos HOWTO y Mini-HOWTO que podrá encontrar en el CD de Red Hat Linux en los directorios `doc/HOWTO` y `doc/HOWTO/mini`. Resultan muy útiles los Mini-HOWTO cuyos nombres empiezan por `Linux+`.

Nota

Para que Red Hat Linux/x86 pueda coexistir en su máquina con OS/2, deberá crear las particiones con el software para la gestión de las particiones de OS/2 -- sino OS/2 podría no reconocer las particiones en el disco. Durante la instalación no intente crear ninguna nueva partición, cree las justas particiones de Linux utilizando el comando `fdisk` de Linux.

B.1.7 Particiones en el disco y punto de montaje

Una parte donde muchos nuevos usuarios de Linux encuentran problemas es la forma en que se utilizan las particiones bajo Linux. En DOS/Windows el asunto es bastante sencillo: si tiene más de una partición, cada partición utiliza una "letra de unidad". Entonces podrá utilizar esta letra para referirse únicamente a esta partición.

El método con el que Red Hat Linux gestiona las particiones y, por tanto, las unidades de disco en general, es totalmente diferente. La diferencia en general está en el hecho que cada partición es utilizada como parte integrante del arbol del sistema de ficheros de Linux. Esto se hace asociando a cada partición un directorio distinto por medio de un proceso llamado **montaje**. Montar una partición quiere decir hacer su contenido disponible a partir del directorio especificado (al cual nos referimos con el nombre de **punto de montaje**).

Por ejemplo, si se monta la partición `/dev/hda5` en `/usr`, esto quiere decir que todos los ficheros y los directorios bajo `/usr` estarían físicamente en `/dev/hda5`. Por eso, el fichero `/usr/share/doc/FAQ/txt/Linux-FAQ` estaría en `/dev/hda5` , pero no el fichero `/etc/X11/gdm/Sessions/Gnome` .

Siguiendo con este ejemplo, sería posible que uno o más directorios de `/usr` fueran los puntos de montaje para otras particiones. Por ejemplo, una partición como `/dev/hda7` podría ser montada en `/usr/local`, que quiere decir que, por ejemplo, `/usr/local/man/whatis` estaría en `/dev/hda7` y no en `/dev/hda5`.

B.1.8 ¿Cuántas particiones?

Llegados a este punto en el proceso de preparación de la instalación de Red Hat Linux, tendrá que considerar el número y el tamaño de las particiones que serán utilizadas por el nuevo sistema operativo. La pregunta "¿Cuántas particiones?" sigue dividiendo en dos el mundo de Linux y, sin querer por ello acabar esta discusión, es posible que haya muchas posibilidades de crear tantas particiones como personas hablan de ello.

Teniendo esto en cuenta, le aconsejamos crear, a menos que no tenga una razón para hacerlo de forma distinta, las particiones siguientes:

- *Partición swap* — Las particiones swap son utilizadas para soportar la memoria virtual. Con otras palabras, los datos son escritos en la swap cuando no hay bastante memoria disponible para contener los datos que su ordenador está procesando. Si su ordenador tiene 16 Megas de RAM o incluso menos, *tiene* que crear una partición swap. También si tiene más memoria, se recomienda la utilización de una partición swap. El tamaño mínimo para una partición de swap tendría que ser igual a la cantidad de memoria RAM presente en su ordenador, o por lo menos 16MB (entre las dos se aconseja eligir la cantidad mayor).

- *Una `/boot` partición* — La partición que se crea bajo `/boot` contiene el kernel del sistema operativo (que permite el arranque de su sistema con Red Hat Linux), junto con algunos ficheros utilizados durante el proceso de arranque.

  Asegúrese de leer la Sección B.1.9, *Uso de LILO* -- la información que aquí encontrará está relacionada con la partición `/boot`.

  Debido a las limitaciones de la mayoría de BIOSes de PCs, es una buena idea crear una partición pequeña para estos ficheros. Esta partición no debería superar los 32 MG.

- *Partición root (`/`)* — La partición root es donde se encuentra `/` (el directorio de root). En esta configuración de las particiones, todos los ficheros (excepto los que residen en `/boot`) están en la partición de root. Por ello sería una buena elección hacer lo más grande posible el tamaño de su partición de root. Una partición root de 1.2 GB es equivalente a la que es instalada por una instalación de clase estación de trabajo (con *poquísimo* espacio libre), mientras que una partición root de 2.4 GB le permitirá instalar todos los paquetes. Es obvio que cuanto más espacio pueda darle a la partición root mejor.

Puede encontrar recomendaciones específicas sobre el tamaño adecuado de algunas particiones Red Hat Linux en la *Official Red Hat Linux x86 Installation Guide*.

B.1.9 Uso de LILO

LILO (el LInux LOader) es el método más normal de arrancar Red Hat Linux en sistemas basados en tecnología Intel. Como cargador del sistema operativo, el LILO opera externamente a cualquier sistema operativo, utilizando sólo el el sistema básico de entrada/salida (o BIOS) incluido en el hardware del mismo sistema. Esta sección describe la interacción entre LILO y la BIOS de los ordenadores y es especifíca para ordenadores Intel.

Limitaciones relativas a la BIOS y al LILO

LILO está afectado por algunas limitaciones puestas por el BIOS en muchos ordenadores basados en Intel. De forma específica, la mayor parte de las BIOS no pueden acceder a más de dos discos duros y no pueden acceder a los datos localizados más allá del cilidro 1023 de cualquier unidad. Algunos BIOS nuevos no tienen estas limitaciones, sin embargo, esto no quiere decir que el problema sea normal.

Todos los datos que LILO necesita al arranque de la máquina (incluido el kernel de Linux) están contenidos en el directorio `/boot`. Si sigue la configuración para las particiones que acabamos de explicar o si está efectuando una instalación de clase estación de trabajo o servidor, el directorio `/boot` será creado en una pequeña partición separada. De otro modo, residirá en la partición de root. En cualquier

caso la partición en la que reside `/boot` debe seguir las reglas que se exponen a continuación para que LILO funcione correctamente en su sistema Red Hat Linux:

En los dos primeros discos IDE

Si tiene dos discos IDE (o EIDE), `/boot` debe estar en uno de estos. Observe que este límite de dos unidades también incluye cualquier CD-ROM IDE en su controladora primaria IDE. Por tanto, si tiene un disco duro IDE, y un CD-ROM IDE en su controladora primaria, `/boot` debe estar debe estar localizado sólo en el primer disco duro, incluso si tiene discos duros en su controladora IDE secundaria.

En el primer disco IDE o SCSI

Si tiene una unidad IDE (o EIDE) y una o más unidades SCSI, `/boot` tiene que estar o en el disco IDE o en la SCSI en el ID 0. Otros ID SCSI no funcionarán.

En los dos primeros discos SCSI

Si tiene sólo discos SCSI, `/boot` debe encontrarse en un disco en el ID 0 o ID 1. Otros ID SCSI no funcionarán.

Partición *completamente* dentro del Cilindro 1023

No importa qué configuración descrita utilice, la partición que contendrá `/boot` debe ser creada antes del cilidro 1023. Si la partición que contiene `/boot` supera el cilindro 1023, podría encontrarse en situaciones en que LILO funcionará inicialmente (porque todas las informaciones necesarias se encuentran antes del cilidro 1023), sin embargo, no funcionará si tiene que cargar un kernel nuevo y éste se encuentra más allá de este cilindro

Como ya se dijo, es posible que algunas BIOS nuevas permitan a LILO funcionar con configuraciones que no corresponden a las que acabamos de describir. De la misma manera, se pueden utilizar algunas formas más "esotéricas" de LILO para arrancar el sistema también con configuraciones distintas de las que hemos visto. De todas formas, ante el número de variables posibles existentes, Red Hat Linux no puede soportar otros métodos extraordinarios relacionados con este asunto.

Nota

Disk Druid, así como las instalaciones de clase estación de trabajo y servidor tienen en cuenta estas limitaciones debidas a la BIOS.

C Discos de driver

C.1 ¿Por qué necesito un disco que contenga un driver?

Mientras se carga el programa de instalación Red Hat Linux podría aparecer una pantalla que le pide que introduzca un disco que contenga un driver. Se le pedirá el disco de drivers en los tres casos siguientes:

- Si está ejecutando una instalación en modo `expert mode`
- Si ejecuta el programa de instalación tecleando `linux dd` en el prompt `boot`:
- Si ejecuta el programa de instalación en un ordenador sin dispositivos PCI

C.1.1 ¿Qué es un disco de drivers?

Un disquete de drivers añade el soporte para la gestión de determinados periféricos hardware que de otro modo no serían soportados por el programa de instalación. El disquete de drivers podría ser creado por Red Hat, podría crearlo usted o podría ser un disquete que le ha sido proporcionado junto al hardware por su vendedor.

No debería necesitar un disquete de drivers a menos que tenga necesidad del soporte de un dispositivo en concreto para instalar Red Hat Linux. El disquete de drivers es utilizado normalmente por unidades de CD-ROM muy nuevas o que no son estándar, adaptadores SCSI o NICs. Éstos son los únicos dispositivos usados durante la instalación que requieren drivers no incluidos en los CD-ROMs Red Hat Linux (o disco, si es que ha creado un disco de arranque para iniciar el sistema de instalación).

Nota

Si un dispositivo no es requerido para la instalación de Red Hat Linux, continúe con la instalación estándar y añada la gestión del nuevo hardware cuando haya completado la instalación.

C.1.2 ¿Cómo obtener un disquete de drivers?

El CD-ROM 1 de Red Hat Linux incluye una imagen de disco de driver (`images/drivers.img`) que contiene drivers utilizados raramente. Si cree que su sistema necesitará uno de estos drivers, sería

una buena idea proseguir con la creación de un disco de driver antes de empezar la instalación de Red Hat Linux.

Otra opción para encontrar información sobre un disco de driver especializado es visitando el sitio web de Red Hat en http://www.redhat.com/support/errata en una sección llamada **Bug Fixes**. En ocasiones, tras una "release" de Red Hat Linux, tendrá a su disposición hardware muy conocido, que no funcionará con los drivers que ya tiene en el programa de instalación o con aquéllos incluidos en la imagen del disco de driver en el CD-ROM 1 de Red Hat Linux. En estos casos, el sitio web de Red Hat suele contener un enlace a una imagen de disco de driver que puede utilizar al instalar Red Hat Linux con ese hardware.

Creación de un disco de driver desde una imagen de fichero

Si tiene una imagen de disco de driver que necesita para escribir el disco, puede hacerlo desde dentro de DOS o Red Hat Linux.

Para crear un disco de driver desde una imagen de disco de driver mediante el uso de Red Hat Linux:

1. Inserte un disquete vacío formateado en la primera disquetera.
2. Escriba `cat`*`dd.img`* `> /dev/fd0` como root, desde el directorio que contiene la imagen del disco de driver *`dd.img`*. root.

Para crear un disco de driver desde una imagen de disco de driver:

1. Inserte un disquete vacío formateado en la unidad a:.
2. Escriba `rawrite`*`dd.img`* `a:` en la línea de comandos, desde el mismo directorio que contiene la imagen de disco de driver.

C.1.3 Uso de un disco de driver durante la instalación

No es suficiente tener un disco de driver. Debe especificarle al programa de instalación de Red Hat Linux que cargue el disco de driver y que lo utilice para el proceso de instalación.

Note

Un disco de driver difiere de un disco de arranque. Si necesita un disco de arranque para iniciar la instalación de Red Hat Linux en su sistema, deberá crearlo y arrancar desde éste antes de utilizar el disco de driver.

Si no posee un disco de instalación y su sistema no puede arrancar desde el CD-ROM, cree un disco de instalación mediante el uso de el fichero adecuado *`filename`*`.img` (como `boot.img`)en el CD-ROM 1 de Red Hat Linux en el directorio `images`. Para las instrucciones de cómo crear un disco de arranque, consulte la *Official Red Hat Linux x86 Installation Guide* en la sección llamada *Creación de discos de instalación*.

Cuando haya creado el disquete de drivers, efectúe el arranque desde el CD-ROM 1 (o desde el disco de instalación que ha creado si no puede arrancar desde el CD-ROM por cualquier motivo). Teclee **`linux expert`** o **`linux dd`** en el indicador de comandos `boot:`.

El programa de instalación de Red Hat Linux le pedirá que introduzca el disco de driver. Una vez que el disco de driver ha sido leído por el instalador, estos drivers son aplicables al hardware que se encuentre en su sistema tras el proceso de instalación.

D RAID (Redundant Array of Independent Disks)

D.1 ¿Qué es el RAID?

La idea básica del RAID es la de combinar discos de modestas dimensiones y de coste reducido en una serie de discos que superen en prestaciones las de un único disco grande y costoso. Este conjunto de discos es considerado por el ordenador como un solo disco.

RAID es un método en el que la información se divide en varios discos, usando técnicas como **disk striping** (RAID Level 0) y **doble escritura en disco** (RAID level 1) y **disk striping con paridad** (RAID nivel 5) para añadir redundancia, baja latencia y/o alta velocidad de lectura y/o escritura, maximizando también la recuperabilidad de los datos en caso de fallo del sistema.

El concepto básico del RAID es que los datos pueden ser distribuidos entre los discos del grupo de manera consistente. Para hacer esto, los datos deben ser primero divididos en "chunks" (a menudo de 32k o 64k, aunque también se pueden usar otros tamaños). Cada chunk es escrito en los discos por turno. Cuando los datos son leidos, el proceso sucede al contrario, dando la impresión de que muchos discos son combinados en uno solo.

D.1.1 ¿Quién debería usar RAID?

Aquéllos que necesiten controlar grandes cantidades de datos (como los administradores de sistemas), se benificiarían del uso de la tecnología RAID. Los motivos para utilizar RAID son:

- Aumento de la velocidad
- Aumento de la capacidad de archivo mediante el uso de un disco virtual
- Gran eficacia en recuperarse de un fallo del sistema

D.1.2 RAID: Hardware vs. Software

Existen dos posibilidades de realizar un sistema basado en la tecnología RAID: RAID Hardware o Software.

Hardware RAID

Las soluciones hardware gestionan el subsistema RAID independientemente del host, presentándole a este un solo disco.

Un ejemplo de hardware RAID podría ser el conectado al controlador SCSI que presenta al sistema un único disco SCSI. Un sistema RAID externo se encarga de la gestión del RAID con el controlador

localizado en el subsistema externo de los discos. Todo el subsistema está conectado a un host a través de un controlador SCSI normal y se le presenta al host como un solo disco.

Existen también controladores RAID en forma de tarjetas que se *comportan* como un controlador SCSI con el sistema operativo, pero gestionan todas las comunicaciones reales entre los discos de manera autónoma. En estos casos, basta con conectar los discos a un controlador RAID como lo haría con un controlador SCSI, pero después podrá configurarlo como un controlador RAID sin que el sistema operativo aprecie la diferencia.

Software RAID

El Software RAID Software implementa los diferentes niveles de RAID en el código del kernel que tienen que ver con la gestión del disco (block device). Ofrece además la solución menos costosa, ya que las tarjetas caras de controladores de disco o chasis hot swap [1]no son requeridas. El software RAID funciona con discos IDE menos costosos así como con discos SCSI. Con las rápidas CPU de hoy en día, las prestaciones del software RAID software pueden competir con las del hardware RAID.

El controlador MD del kernel de Linux es un ejemplo de que la solución RAID es completamente independiente del hardware. Las prestaciones de un RAID basado en el software dependen de las prestaciones y de la carga del CPU.

Remítase a la *Official Red Hat Linux Customization Guide*, para ulterior información sobre la configuración del software RAID en el programa de instalación de Red Hat Linux.

Para aquéllos que estén interesados en saber lo que el software RAID ofrece, aquí tiene una breve lista de algunas de sus características más importantes.

- Proceso de reconstrucción entrelazado.
- Configuración basada completamente en el kernel.
- La portabilidad de RAID entre ordenadores Linux sin reconstruir.
- Reconstrucción del array en segundo plano usando recursos no utilizados del sistema.
- Soporte para discos hot-swappable.
- Reconocimiento automático de la CPU para disfrutar de algunas de sus ventajas.

D.1.3 Niveles de RAID Levels y soporte lineal

RAID soporta varias configuraciones, incluyendo los niveles 0, 1, 4, 5 y el soporte lineal. Estos tipos de RAID se definen de la siguiente manera:

- *Nivel 0* — El RAID nivel 0, a menudo llamado "striping," es una técnica orientada a las prestaciones de conversión de datos "striped". Esto quiere decir que los datos que son escritos en el array,

[1] Un chasis hot-swap le permite eliminar un disco rígido sin tener que apagar el ordenador.

son divididos en líneas y escritos en discos miembros del array. Esto permite altas prestaciones de I/O con un bajo coste pero no proporciona redundancia. La capacidad de memorizar del array es igual a la capacidad total de los discos miembros en un hardware RAID o a la capacidad total de las particiones miembros en un software RAID.

- *Nivel 1* — El RAID nivel 1, o "mirroring," se viene utilizando desde hace mucho más tiempo con cualquier otra forma de RAID. El nivel 1 proporciona redundancia escribiendo datos idénticos en cada disco miembros del array, dejando una copia "idéntica" en cada uno de los discos. El mirroring es muy popular a causa de su simplicidad y el alto nivel de disponibilidad de datos que tiene. El nivel 1 opera con dos o más discos que pueden utilizar una modalidad de acceso paralelo para transferir de manera rápida datos de lectura, pero más comunmente opera de manera independiente para ocuparse de valores altos de transacciones I/O. El nivel 1 proporciona una alta fiabilidad y mejora las prestaciones de las aplicaciones de lectura de datos pero con un coste relativamente elevado. [2]. La capacidad de archivo del nivel l del array es igual a la capacidad de un disco duro espejo en una hardware RAID o la de las particiones espepo en un software RAID.

- *Nivel 4* — El RAID nivel 4 utiliza la paridad [3]concentrado en un solo disco para la protección de los datos. Está más orientado a la transacción de I/O que para la transferencia de grandes ficheros. Ya que el disco dedicado a la paridad representa un inherente cuello de botella, el nivel 4 se utiliza raramente sin usar la tecnología write-back caching. A pesar de que el RAID de nivel 4 es una opción en algunos esquemas de reparticionamiento RAID, no es una opción permitida en la instalación RAID Red Hat Linux[4]. La capacidad de archivo del hardware RAID nivel 4 equivale a la de los discos miembros menos la capacidad de un disco miembros. La capacidad de archivo del software RAID nivel 4 equivale a la capacidad de las particiones miembros, menos el tamaño de una de las particiones si éstas son del mismo tamaño.

- *Nivel 5* — Es el tipo más común de RAID. Distribuyendo la paridad entre algunos o todos los discos miembros, el RAID nivel 5 elimina el cuello de botella inherente al nivel 4. El único cuello de botella es el proceso del cálculo de la paridad. Con las modernas CPU y el software RAID, esto no representa un gran cuello de botella. Como con el nivel 4, los resultados son prestaciones muy elevadas, con las lecturas que sustancialmente son más rápidas que las escrituras. El nivel 5

[2] El RAID nivel 1 tiene un alto coste ya que escribe la misma información en todos los discos del array, malgastando de este modo el espacio del disco. Por ejemplo: Ha configurado el RAID nivel 1 de manera que su partición "/" (root) se expanda a traves de dos discos de 40G. Tiene un total de 80G pero sólo puede acceder a 40 de los 80G. Los otros 40G se comportan como un espejo de los primeros 40G.

[3] La información sobre la paridad es calculada en base al contenido del resto de los discos miembros del array. Esta información puede ser utilizada para la reconstrucción de datos cuando uno de los discos del array se daña. Los datos reconstruidos pueden, por tanto, ser utilizados para satisfacer las peticiones de I/O del disco corregido y para volver a escribir ese disco después de haber sido reparado o sustituido.

[4] El RAID nivel 4 requiere el mismo espacio que requiere el nivel 5, pero el nivel 5 tiene muchas ventajas con respecto al nivel 4. Por este motivo, el nivel 4 no está soportado.

se utiliza a menudo con el write-back caching para reducir la asimetría. La capacidad de archivo del hardware RAID nivel 4 equivale a la de los discos miembros menos la capacidad de un disco miembro. La capacidad de archivo del software RAID nivel 4 equivale a la capacidad de las particiones miembro, menos el tamaño de una de las particiones si éstas son del mismo tamaño.

- *RAID lineal* — El RAID lineal es una simple agrupación de discos de manera que se crea un disco virtual más grande. En el RAID lineal, los chunk están dispuestos secuencialmente y se pasa de un disco miembro al disco siguiente, tan solo una vez que el primer disco ha sido completado en su totalidad. Este agrupamiento no tiene ninguna ventaja en cuanto a prestaciones, pues es improbable que alguna operación de I/O sea divida entre los discos miembros. El RAID lineal no ofrece redundancia y de hecho la fiabilidad disminuye -- si uno de los discos se daña, el RAID en su totalidad no puede ser utilizado. La capacidad es el total de todos los discos miembros.

E PowerTools

E.1 ¿Qué son las PowerTools?

Powertools de Red Hat son una colección de paquetes software creados para el sistema operativo Red Hat Linux 7.1. PowerTools incluye las últimas versiones (desde la fecha de entrega del producto) de centenares de programas. Por ello le resultará sencillo encontrar algunos tipos de aplicaciones.

Este grupo de software contiene aplicaciones audio, información en línea, herramienta para el desarrollo, editor, administrador de ficheros , simuladores, juegos, programas para gráficos, productividad, paquetes matemático/estadísticos, administración de sistema y herramientas para la gestión de la red y administrador de ventanas.

¿Es usted administrador de sistema? PowerTools comprende un array de herramientas que pueden facilitar su archivo y reemplazar varias utilidades con una aplicación común. Eche un vistazo a aplicaciones como Ethereal para analizar los portocolos de red, PortSentry para detener los escáners de puerto o Postfix como una alternativa a Sendmail.

¿Le gusta jugar? PowerTools contiene un número de juegos básicos, divertidos, tales como SpeedX, XFrisk, y Amphetamine.

Como la instalación y la desinstalación de paquetes de software en Red Hat Linux es fácil usando RPM o Gnome-RPM, puede intentar aplicaciones diferentes que hagan lo mismo antes de decidir cuál le conviene más.

E.2 Paquetes de PowerTools

Si ya conoce el paquete de PowerTools que le gustaría instalar, consulte la Sección E.3, *Instalación de los paquetes PowerTools* para más información sobre la instalación.

No obstante, debido a un gran número de paquetes de PowerTools, resulta útil buscar a través de las descripciones del paquete para encontrar aquéllas que cumplen nuestros requisitos.

E.2.1 Lectura del contenido del CD-ROM

Puede acceder al contenido de los CD-ROM PowerTools desde el el indicador de comandos de la shell (en una ventana terminal o en modo consola). Previamente debe montar la unidad de CD-ROM.

Montaje del CD-ROM de PowerTools

Si su sistema no está configurado para automontar la unidad de CD-ROM cuando se inserte un CD-ROM, meta el CD de PowerTools en su unidad de CD-ROM. Teclee lo siguiente, como root:

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

Nota

Usted o el administrador del sistema podrían permitir a los demás usuarios efectuar la operación del montaje de la unidad de CD-ROM. Los usuarios pueden beneficiarse de esta ventaja sólo si la opción `user` está incluida en la línea `/dev/cdrom` en el archivo `/etc/fstab`. Solamente el usuario root puede instalar los paquetes RPM PowerTools.

Navegar por el fichero `CONTENTS`

Después de montar la unidad, `cd` en el directorio del CD-ROM montado con el siguiente comando:

```
cd /mnt/cdrom
```

Finalmente, teclee `less CONTENTS` para visionar las aplicaciones disponibles. El fichero `CONTENTS` contiene cada programa en el CD-ROM PowerTools, listadas en orden alfabético.

Leer el archivo `CONTENTS` en el CD-ROM de PowerTools puede ser una tarea desalentadora, considerando el complejo de aplicaciones disponibles. Aquí tiene algunos trucos para encontrar un tipo particular de programa sin tener que leer a través de todas las descripciones:

- *Use el nombre del grupo* — A cada aplicación le viene asignado un grupo. Por ejemplo, la utilidad para enviar faxes FaxMail se encuentra en el grupo Aplicaciones/Comunicaciones y el sistema broadcasting de Internet MP3, está en el grupo Aplicaciones/Multimedia. Si ve los nombres de los grupos, se ahorrará tener que leer las descripciones de cada paquete.
- *Búsqueda mediante el uso de claves* — El comando `ls` soporta la búsqueda fácil. Si sabe que está buscando un cliente IRC, escriba c`less CONTENTS` para ver `CONTENTS`; escriba entonces **`/IRC`** y pulse [Intro]. Dará con el primer cliente IRC en la lista. Si esto no le interesa, pulse la tecla [n] repetidamente hasta que vaya a parar al archivo `CONTENTS`, en busca de los paquetes relacionados con IRC.

Si tiene problema en el uso del comando `less`, teclee `man less` en el indicador de comandos de ayuda.

Desmontar el CDD-ROM de PowerTools

Cuando acabe de usar el CD-ROM de PowerTools para instalar los paquetes, puede eliminarlos de su unidad de CD-ROM. Si tiene un CD-ROM montado en el directorio `/mnt/cdrom`, proceda de la siguiente manera:

1. Cambie los directorios usando `cd /mnt` para estar en un nivel superior al directorio `/mnt/cdrom`.
2. Teclee `umount /mnt/cdrom` para desmontar el CD-ROM.

3. Teclee `eject /dev/cdrom` y la unidad de CD-ROM se abrirá para que pueda sacar el CD.

E.3 Instalación de los paquetes PowerTools

E.3.1 Instalación de PowerTools en un entorno GUI

Si está utilizando la interfaz gráfica GNOME o KDE, introduzca el CD en su lector CD-ROM. Se le pedirá la contraseña de root a fin de que pueda instalar los nuevos paquetes. Después de haber tecleado la contraseña de root, será ejecutado automáticamente el programa Gnome-RPM o Kpackage según el entorno gráfico que utilice.

Consulte la *Official Red Hat Linux Getting Started Guide* para más información sobre como utilizar Gnome-RPM. Vaya a http://www.general.uwa.edu.au/u/toivo/kpackage para más información sobre cómo utilizar Kpackage.

Si no está utilizando GNOME o KDE, debería utilizar la el indicador de comandos de la shell para instalar PowerTools.

E.3.2 Instalación de PowerTools desde el indicador de comandos de la shell

En primer lugar, monte el CD-ROM de PowerTools en su lector de CD-ROM y utilice `ls` para ver sus contenidos. Si necesita saber como montar un CD-ROM, consulte el *Montaje del CD-ROM de PowerTools* en la sección E.2.1.

Verá los siguientes directorios: SRPMS y `RedHat`. El directorio SRPMS contiene la fuente RPMs de PowerTools. El directorio `RedHat/RPMS` contiene los RPMs para las arquitecturas de tres sistemas operativos específicos.

La ruta `RedHat/RPMS` se usa como un ejemplo general. Debería sustituir el directorio correcto para `RedHat/RPMS`, dependiendo de su arquitectura y del paquete que está instalando.

`cd` al directorio `RedHat/RPMS`:

```
cd RedHat/RPMS
```

Liste los ficheros RPM en el directorio con `ls` para ver la lista completa de paquetes RPM por los sistemas Intel-compatibles.

Probablemente desee tener más información sobre un paquete específico antes de que decida si quiere instalarlo. Puede utilizar la capacidad de consulta de RPM para encontrar más información sobre los paquetes, tales como funciones de paquetes y origen. Vea la *Official Red Hat Linux Customization Guide* para una información más detallada sobre como consultar paquetes usando RPM.

Alternativamente, puede buscar a través del fichero `CONTENTS`para encontrar paquetes que le interesen. Lea *Navegar por el fichero `CONTENTS`* en la sección E.2.1 para más información.

Puede instalar los paquetes seleccionados con RPM. RPM es un sistema de gestión del programa de un comando que se puede gestionar desde la línea de comandos. Lea la *Official Red Hat Linux Customization Guide* para más información sobre como usar RPM para instalar y gestionar los paquetes PowerTools.

Una vez que haya acabado de instalar sus paquetes, debería desmontar su CD-ROM. Si no sabe todavía como desmontar el lector CD-ROM, consulte *Desmontar el CDD-ROM de PowerTools* en la sección E.2.1.

E.4 Desinstalar PowerTools

Para desinstalar los paquetes PowerTools de su sistema, simplemente debe eliminarlos de la misma manera en que eliminaría cualquier otro paquete RPM instalado.

En primer lugar, debe saber el nombre del paquete que le gustaría desinstalar. Por ejemplo, si sabe que quiere eliminar `thrust-0.83c-11` de su sistema, teclee como root:

```
rpm -e thrust
```

En general, `rpm -e <packagename>` eliminará el paquete y los archivos relacionados con su sistema. El CD-ROM PowerTools no es necesario para esta operación.

Para más información referente al uso de RPM, consulte la *Official Red Hat Linux Customization Guide*.

Índice temático

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W