Red Hat Linux 9

Manual de personalización de Red Hat Linux

Red Hat Linux 9: Manual de personalización de Red Hat Linux


Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072
USA
Teléfono: +1 919 754 3700
Teléfono: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC
27709 USA

rhl-cg(ES)-9-Print-RHI (2003-02-13T16:45)

Tabla de contenidos

Introducción

Bienvenido a la versión en español del *Manual de personalización de Red Hat Linux*.

El *Manual de personalización de Red Hat Linux* contiene información sobre cómo personalizar su sistema Red Hat Linux para satisfacer sus necesidades. Si esta buscando una guía paso a paso, orientada a tareas para la configuración y personalización de su sistema, este es el manual para usted. Este manual discute muchos tópicos para usuarios de nivel intermedio tales como:

- Configurar la interfaz de la tarjeta de red (NIC)
- Instalación de kickstart
- Configurar el sistema con Samba para compartir ficheros e impresoras
- Gestionar su software con RPM
- Determinar información sobre el sistema
- Actualización del kernel

Este manual está dividido fundamentalmente en las siguientes categorías:

- Referencias sobre la instalación
- Referencias sobre la red
- Configuración del sistema
- Administración de paquetes

Se supone que cuando lea este manual ya posee conocimientos sobre el sistema Red Hat Linux. Si necesita más información sobre aspectos básicos como la configuración del escritorio o cómo reproducir CD-ROMs de sonido, consulte el *Manual del principiante de Red Hat Linux*. Para temas de mayor envergadura consulte el *Manual de referencia de Red Hat Linux*.

Las versiones en HTML y PDF de todos los manuales Red Hat Linux están disponibles en el CD de documentación y en línea en http://www.redhat.com/docs/.

Nota

Aunque este manual recoge información de lo más actual posible, le recomendamos que lea las *Notas de última hora de Red Hat Linux* por si desea información que no se encuentra a su disposición en este manual o que todavía no se había completado para el momento de la publicación de este manual. Se encuentran en el CD 1 de Red Hat Linux y en:

`http://www.redhat.com/docs/manuals/linux`

1. Cambios a este manual

Este manual ha sido ampliado para incluir nuevas características en Red Hat Linux 9 así como temas solicitados por nuestros lectores. Algunos cambios significativos del manual incluyen:

Implementación de cuotas de discos

Este nuevo capítulo explica cómo configurar y administrar cuotas de discos.

Configuración de la autenticación

Este nuevo capítulo explica cómo usar la **Herramienta de configuración de autenticación**.

Configuración de usuarios

Este capítulo ha sido expandido para incluir las utilidades de línea de comandos para administración de usuarios así como también una explicación de lo que ocurre cuando un nuevo usuario es añadido al sistema.

Samba

Este capítulo ha sido expandido para incluir la nueva **Herramienta de configuración del servidor Samba**.

Configuración de la impresora

Este capítulo ha sido reescrito para la nueva interfaz de la **Herramienta de configuración de impresoras**, el nuevo **Administrador de impresión de GNOME**, y el nuevo icono de arrastre y suelte del panel.

Kickstart

Las opciones kickstart han sido actualizadas para incluir las nuevas opciones en Red Hat Linux 9, y el capítulo **Configurador de Kickstart** ha sido actualizado para poder incluir muchas nuevas características.

Configuración de la red

Este capítulo ha sido actualizado para los últimos cambios de la interfaz de la **Herramienta de administración de redes**.

Configuración de la fecha y hora

Se ha movido este capítulo al *Manual del principiante de Red Hat Linux*.

2. Convenciones del documento

Cuando lea este manual, verá que algunas palabras están representadas en fuentes, tipos de letra, tamaño y peso diferentes. Esta forma de evidenciar es sistemática; se representan diferentes palabras con el mismo estilo para indicar su pertenencia a una categoría específica. A continuación tiene una lista de los tipos de palabras representados de una manera determinada:

`comando`

Los comandos en Linux (y otros sistemas operativos) se representan de esta manera. Este estilo le indica que puede escribir la palabra o frase en la línea de comandos y pulsar [Intro] para aplicar el comando. A veces un comando contiene palabras que aparecerían con un estilo diferente si fueran solas (p.e, nombres de archivos). En estos casos, se las considera como parte del comando, de manera que toda la frase aparece como un comando. Por ejemplo:

Utilice el comando `cat testfile` para ver el contenido de un archivo, llamado `testfile`, en el directorio actual.

`nombre del archivo`

Los nombres de archivos, nombres de directorios, rutas y nombres de rutas y paquetes RPM aparecen siempre en este modo. Este estilo indica que un archivo o directorio en particular existe con ese nombre en su sistema Red Hat Linux. Ejemplos:

El archivo `.bashrc` en su directorio principal contiene definiciones de la shell de bash y alias para su propio uso.

El archivo `/etc/fstab` contiene información sobre diferentes dispositivos del sistema y sistemas de archivos.

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

aplicación

Este estilo indica que el programa es una aplicación de usuario final (lo contrario a software del sistema). Por ejemplo:

Use **Mozilla** para navegar por la Web.

[tecla]

Una tecla del teclado aparece en el siguiente estilo. Por ejemplo:

Para utilizar [Tab], introduzca un carácter y pulse la tecla [Tab]. Aparecerá una lista de archivos en el directorio que empiezan con esa letra. Su terminal visualizará la lista de archivos en el directorio que empieza con esa letra.

[tecla]-[combinación]

Una combinación de teclas aparece de la siguiente manera. Por ejemplo:

La combinación de teclas [Ctrl]-[Alt]-[Backspace] le hará salir de la sesión gráfica y volver a la pantalla gráfica de login o a la consola.

texto de una interfaz gráfica (GUI)

Un título, palabra o frase dentro de una pantalla o ventana de interfaz gráfica GUI aparecerá de la siguiente manera. La finalidad del texto escrito en este estilo es la de identificar una pantalla GUI o un elemento e una pantalla GUI en particular (p.e, un texto relacionado con una casilla de verificación o un campo). Ejemplos:

Seleccione la casilla de verificación **Pedir contraseña** si quiere que su salvapantallas pida una contraseña antes de terminar.

nivel superior de un menú en una pantalla o ventana GUI

Cuando vea una palabra con este estilo, significa que la palabra está en el nivel superior de un menú desplegable. Si hace click sobre la palabra en la pantalla GUI, aparecerá el resto del menú. Por ejemplo:

Bajo **archivo** en una terminal de GNOME verá los siguientes elementos en el menú: opción **Nueva pestaña** que le permite abrir múltiples intérpretes de comandos de la shell en la misma ventana.

Si tiene que escribir una secuencia de comandos desde un menú GUI, aparecerán como en el siguiente ejemplo:

Vaya a **Botón del menú principal** (en el Panel) => **Programación** => **Emacs** para iniciar el editor de textos **Emacs**.

botón en una pantalla o ventana GUI

Este estilo indica que el texto se encuentra en un botón que se pulse en una pantalla GUI. Por ejemplo:

Pulse el botón **Anterior** para volver a la última página Web que haya visitado.

`salida de pantalla`

Cuando vea el texto en este estilo, significa que verá una salida de texto en la línea de comandos. Verá respuestas a comados que haya escrito, mensajes de error e intérpretes de comandos para la entrada de datos durante los scripts o programas mostrados de esta manera. Por ejemplo:

Utilice `ls` para visualizar los contenidos de un directorio:

```
$ ls
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

La salida de pantalla que le devuelvan como respuesta al comando (en este caso, el contenido del directorio) se mostrará en este estilo.

`intérprete de comandos`

El intérprete de comandos es el modo en el que el ordenador le indica que está preparado para que usted introduzca datos, aparecerá con el siguiente estilo. Ejemplos:

```
$
#
[stephen@maturin stephen]$
leopard login:
```

`entrada del usuario`

El texto que el usuario tiene que escribir, ya sea en la línea de comandos o en una casilla de texto de una pantalla GUI, se visualizará en este estilo. En el siguiente ejemplo, **`text`** se visualiza en este estilo:

Para arrancar su sistema en modo texto de su programa de instalación, necesitará escribir en el comando **`text`** en el intérprete de comandos `boot:`.

Adicionalmente, usamos diferentes tipos de estrategias para llamar su atención para determinados tipos de información. Dependiendo de lo importante que esta información sea para su sistema, estos elementos serán marcados como nota, atención o aviso. Por ejemplo:

Nota

Recuerde que Linux es sensible a mayúsculas y minúsculas. En otras palabras, rosa no es lo mismo que ROSA o rOsA.

Sugerencia

El directorio `/usr/share/doc` contiene documentación adicional para paquetes instalados en su sistema.

Importante

Si modifica el archivo de configuración DHCP, los cambios no surtirán efecto hasta que el demonio DHCP se reinicie.

Atención

No lleve a cabo tareas rutinarias como root — utilice una cuenta de usuario normal a menos que necesite usar una cuenta de usuario para administrar su sistema.

Aviso

Si escoge no particionar de forma manual, una instalación de tipo servidor borrará todas las particiones ya existentes en los discos duros instalados. No escoja este tipo de instalación a menos que esté seguro de que no desea guardar los datos.

3. Y además...

El *Manual de personalización de Red Hat Linux* forma parte del creciente compromiso de Red Hat consistente en proveer soporte útil y actualizado a todos los usarios del sistema Linux. Es decir, a medida que van saliendo versiones nuevas de herramientas y de aplicaciones se irá ampliando este manual.

3.1. Envíenos su opinión

Si encuentra un error en el *Manual de personalización de Red Hat Linux* o si tiene nuevas ideas o sugerencias que crea lo pueda mejorar, escríbanos a Bugzilla (http://bugzilla.redhat.com/bugzilla/) indicando el tema en el `rhl-cg`.

No se olvide de mencionar el número de identificación del manual:

```
rhl-cg(ES)-9-Print-RHI (2003-02-13T16:45)
```

Así sabremos la versión del manual al que se refiere.

Si tiene alguna sugerencia para mejorar la documentación, sea lo más específico posible. Si ha encontrado algún error, incluya el número de la sección y parte del texto de manera que podamos encontrarlo fácilmente.

4. Regístrese para el soporte

Si tiene una edición de Red Hat Linux 9, recuerde que para beneficiarse de las ventajas que le corresponden como cliente de Red Hat, deberá registrarse.

Tiene derecho a disfrutar las siguientes ventajas, dependiendo del producto Red Hat Linux que haya comprado:

- Soporte Red Hat — Obtenga ayuda con las preguntas de instalación del equipo de soporte de Red Hat, Inc..
- Red Hat Network — Actualice de forma sencilla los paquetes y reciba avisos de seguridad personalizados para su sistema. Vaya a http://rhn.redhat.com para más detalles.
- *Under the Brim: Boletín de Red Hat* — Obtenga mensualmente las últimas noticias e información sobre el producto directamente desde Red Hat.

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

Para leer más acerca del soporte técnico para Red Hat Linux remítase al apéndice *Obtener soporte técnico* en el *Manual de instalación de Red Hat Linux*.

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

El equipo de documentación de Red Hat

I. Sistemas de archivos

Un *Sistema de archivos* se refiere a los archivos y directorios almacenados en un computador. Un sistema de archivos puede tener formatos diferentes llamados *tipos de sistemas de archivos*. Estos formatos determinan cómo se almacenará la información como archivos y directorios. Algunos tipos de sistemas de archivos almacenan copias redundantes de datos, mientras que otros tipos de sistemas de archivos hacen el acceso al disco duro más rápido. Esta parte discute los tipos de sistemas de archivos ext3, swap, RAID, y LVM. También se discute `parted`, una utilidad para el manejo de particiones.

Tabla de contenidos

redhat.

Capítulo 1.

Sistema de archivos ext3

Con la versión Red Hat Linux 7.2, el sistema de archivos por defecto cambia del formato ext2 al sistema de archivos journaling *ext3*.

1.1. Características de ext3

Básicamente, el sistema de archivos ext3 es una versión mejorada de ext2. Las mejoras introducidas proporcionan las siguientes ventajas:

Disponibilidad

Tras un corte eléctrico o una caída inesperada del sistema (también se denomina *cierre no limpio del sistema*), se debe comprobar con el programa `e2fsck` cada sistema de archivos ext2 montado en la máquina para ver si es consistente. El proceso de comprobación lleva mucho tiempo y puede prolongar el tiempo de arranque del sistema de un modo significativo, especialmente si hay grandes volúmenes que contienen un elevado número de archivos. Durante este proceso, no se puede acceder a los datos de los volúmenes.

Con la característica journaling del sistema de archivos ext3 ya no es necesario realizar este tipo de comprobación en el sistema de archivos después de un cierre no limpio del sistema. En el sistema ext3, únicamente se realiza una comprobación de consistencia en los casos puntuales en los que se producen determinados errores de hardware, como, por ejemplo, fallos en el disco duro. El tiempo empleado para recuperar un sistema de archivos ext3 tras un cierre no limpio del sistema no depende del tamaño del sistema de archivos ni del número de archivos, sino del tamaño del *journal* (diario), utilizado para mantener la consistencia en el sistema. Por defecto, la recuperación del tamaño del "journal" tarda alrededor de un segundo, según la velocidad del hardware.

Integridad de los datos

El sistema de archivos ext3 proporciona una integridad superior de los datos si se produce un cierre no limpio del sistema. El sistema de archivos ext3 le permite seleccionar el tipo y el nivel de protección de los datos. Por defecto, Red Hat Linux 9 configura los volúmenes ext3 para que el nivel de consistencia de los datos sea elevado en relación con el estado del sistema de archivos.

Velocidad

El sistema de archivos ext3, aparte de permitir escribir datos más de una vez, en la mayoría de los casos tiene un rendimiento superior al que proporciona ext2 porque los "journals" de ext3 optimizan el movimiento de los cabezales de los discos duros. Se pueden seleccionar tres modos de journaling para optimizar la velocidad, pero, como contrapartida, la integridad de los datos se verá afectada.

Fácil transición

La migración de ext2 a ext3 es muy sencilla y se pueden aprovechar las ventajas de un sólido sistema de archivos con journaling sin tener que volver a dar formato al sistema. Consulte la Sección 1.3 para más información sobre como realizar esta tarea.

Si realiza una instalación nueva de Red Hat Linux 9, el sistema de archivos por defecto que se asigna a las particiones Linux del sistema es ext3. Si realiza una actualización a partir de una versión de Red Hat Linux con particiones ext2, el programa de instalación le permitirá convertir estas particiones a ext3 sin perder los datos. Consulte el apéndice titulado *Actualización del sistema actual* en el *Manual de instalación de Red Hat Linux* para obtener más detalles.

En las siguientes secciones se describirán los pasos para crear y configurar las particiones ext3. Si tiene particiones ext2 y está ejecutando Red Hat Linux 9, puede omitir las secciones en las que se explican los pasos para particionar y dar formato al disco, y, en su lugar, puede ir directamente a la Sección 1.3.

1.2. Creación de un sistema de archivos ext3

A menudo es necesario, después de la instalación, crear un nuevo sistema de archivos ext3. Por ejemplo, si añade un nuevo disco duro al sistema Red Hat Linux puede desear particionar el disco duro y usar el sistema de archivos ext3.

Los pasos para crear un sistema de archivos ext3 son los siguientes:

1. Cree la partición utilizando `parted` o `fdisk`.
2. Dé formato a la partición con el sistema de archivos ext3 usando `mkfs`.
3. Etiquete la partición usando `e2label`.
4. Cree el punto de montaje.
5. Añada la partición a `/etc/fstab`.

Para obtener más información sobre la ejecución de estos pasos recurra al Capítulo 5.

1.3. Conversión a un sistema de archivos ext3

El programa `tune2fs` permite añadir un journal a un sistema de archivos ext2 existente sin modificar los datos en la partición. Si el sistema de archivos ya está montado mientras se realiza la migración, el journal estará visible como `.journal` en el directorio raíz del sistema de archivos. Si el sistema de archivos no está montado, el journal se ocultará y no aparecerá en el sistema de archivos.

Para convertir un sistema de archivos ext2 a ext3, conéctese como root y escriba:

```
/sbin/tune2fs -j /dev/hdbX
```

En el comando anterior, reemplace /dev/*hdb* con el nombre del dispositivo y *X* con el número de partición.

Una vez realizado esto, asegúrese de cambiar el tipo de partición de ext2 a ext3 en `/etc/fstab`.

Si está migrando el sistema de archivos raíz, tendrá que usar una imagen `initrd` (o disco RAM) para arrancar. Para crear una, ejecute el programa `mkinitrd`. Para obtener más información sobre el uso del comando `mkinitrd`, escriba `man mkinitrd`. Asegúrese también de que la configuración LILO o GRUB carga el archivo `initrd`.

Aunque no consiga realizar este cambio, el sistema se arrancará, pero el sistema de archivos se montará como ext2 en vez de como ext3.

1.4. Volver al sistema de archivos ext2

Puesto que ext3 es relativamente nuevo, algunas utilidades de disco todavía no son compatibles con este sistema. Por ejemplo, tal vez deba reducir el tamaño de una partición con `resize2fs`, que todavía no es compatible con ext3. En estos casos, deberá volver temporalmente al sistema de archivos ext2.

Para revertir una partición, primero deberá desmontar la partición conectándose como root y escribiendo:

```
umount /dev/hdbX
```

En el comando anterior, sustituya /dev/*hdb* por el nombre del dispositivo y *X* con el número de la partición. En el resto de esta sección, los comandos de ejemplo utilizarán *hdb1* para estos valores.

A continuación, cambie el tipo del sistema de archivos a ext2. Para ello, escriba el comando siguiente como root:

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

Compruebe si la partición tiene errores. Para ello, escriba el comando siguiente como root:

```
/sbin/e2fsck -y /dev/hdb1
```

A continuación, vuelva a montar la partición como sistema de archivos ext2. Para ello, escriba:

```
mount -t ext2 /dev/hdb1 /mount/point
```

En el comando anterior, sustituya */mount/point* por el punto de montaje de la partición.

Luego, quite el archivo `.journal` del nivel root de la partición cambiando el directorio donde está montado y escribiendo:

```
rm -f .journal
```

Ahora tendrá una partición ext2.

Si cambia definitivamente la partición a ext2, recuerde que debe actualizar el archivo `/etc/fstab`.

redhat.

Capítulo 2.

Espacio Swap

2.1. ¿Qué es el espacio Swap?

El *Espacio swap* en Linux es usado cuando la cantidad de memoria física (RAM) está llena. Si el sistema necesita más recursos de memoria y la memoria física está llena, las páginas inactivas de la memoria se mueven al espacio swap. Mientras que el espacio swap puede ser de ayuda para las máquinas con poca memoria RAM, no debería considerarse como algo que pueda sustituir a más RAM. El espacio Swap se encuentra en discos duros, que tienen un tiempo de acceso más lento que la memoria física.

El espacio Swap puede ser una partición swap dedicada (recomendable), un archivo swap o una combinación de particiones y archivos swap.

El tamaño de su espacio swap debería ser igual o dos veces mayor que la memoria RAM de su ordenador, o 32 MB, la cantidad que sea más grande de estas dos, pero no más de 2048 MB (o 2 GB).

2.2. Añadir el espacio Swap

A veces es necesario añadir más espacio swap después de la instalación. Por ejemplo, puede actualizar la cantidad de RAM en su sistema de 64 MB a 128 MB, pero hay tan sólo 128 MB de espacio swap. Sería conveniente aumentar la cantidad de espacio swap hasta 256 MB sobre todo si lleva a cabo operaciones de uso intensivo de memoria o si ejecuta aplicaciones que requieran gran cantidad de memoria.

Tiene dos opciones: añadir una partición swap o un archivo swap. Se recomienda que añada una partición swap, pero a veces no resulta fácil si no cuenta con espacio libre disponible.

Para añadir una partición swap (asumiendo que `/dev/hdb2` es la partición que quiere agregar):

1. El disco duro no puede estar en uso (no puede tener particiones montadas, y no se puede tener activado el espacio swap). El modo más fácil para lograr esto es iniciar su sistema de nuevo en modo de rescate. Consulte el Capítulo 9 para obtener instrucciones sobre cómo iniciar en modo de rescate. Cuando le pida montar el sistema de archivos, seleccione **Skip**.

   Por otro lado, si la unidad no contiene ninguna partición en uso, puede desmontarlas y eliminar todo el espacio swap del disco duro con el comando `swapoff`.

2. Cree la partición swap usando `parted` o `fdisk`. Usar `parted` es más fácil que `fdisk`; por esto es que sólo se explica el uso de `parted`. Para crear una partición swap con `parted`:

   - En el intérprete de comandos del shell, como usuario root, escriba el comando `parted /dev/`*`hdb`*, donde /dev/*hdb* es el nombre del dispositivo para el disco duro con espacio libre.
   - En el prompt de `(parted)`, escriba **`print`** para ver las particiones existentes y la cantidad de espacio disponible. Los valores de comienzo y fin están en megabytes. Determine cuánto espacio libre hay en el disco duro y cuánto quiere dedicar a la nueva partición swap.
   - En el indicador `(parted)`, escriba **`mkpartfs`** ***`tipo-particion`*** **`linux-swap`** ***`inicio fin`***, donde *`tipo-particion`* es primaria, extendida, o lógica, *`inicio`* es el punto de comienzo de la partición, y *`fin`* es el punto donde termina la partición.


Aviso

Los cambios tomarán efecto de inmediato. Tenga cuidado con lo que escribe.

- Salga de `parted` escribiendo **`quit`**.

3. Ahora que tiene la partición swap, use el comando `mkswap` para configurar la partición swap. En el indicador de comandos shell como root, escriba lo siguiente:
   ```
   mkswap /dev/hdb2
   ```
4. Para activar la partición swap inmediatamente, escriba el comando siguiente:
   ```
   swapon /dev/hdb2
   ```
5. Para activarlo cuando se arranca, edite `/etc/fstab` para incluir:
   ```
   /dev/hdb2               swap                    swap    defaults        0 0
   ```
   La próxima vez que se arranque el sistema, activará la nueva partición swap.
6. Después de añadir la nueva partición swap y de haberla activado, asegúrese de que está activa visualizando el resultado del comando `cat /proc/swaps` o `free`.

Para añadir un archivo swap:

1. Determine el tamaño del nuevo archivo swap y multiplique por 1024 para determinar el tamaño de bloque. Por ejemplo, el tamaño de bloque de un archivo swap de 64 MB es 65536.
2. En un indicador de comandos shell como root, escriba el siguiente comando con `count` lo que equivale al tamaño de bloque deseado:
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. Configure el archivo swap con el comando:
   ```
   mkswap /swapfile
   ```
4. Para activar el archivo swap inmediatamente pero no automáticamente cuando se arranca:
   ```
   swapon /swapfile
   ```
5. Para activarlo cuando se arranca, edite `/etc/fstab` para incluir:
   ```
   /swapfile               swap                    swap    defaults        0 0
   ```
   La próxima vez que se arranque el sistema, se activará el nuevo archivo swap.
6. Después de haber añadido el nuevo archivo swap y de haberlo activado, asegúrese de que está activado visualizando el resultado del comando `cat /proc/swaps` o `free`.

2.3. Eliminar el espacio Swap

Para eliminar una partición swap:

1. El disco duro no puede estar en uso (no puede haber particiones montadas, y el espacio swap no puede estar activado). El modo más fácil para lograr esto es arrancar el sistema en modo de rescate. Consulte el Capítulo 9 para obtener instrucciones sobre cómo arrancar en modo rescate. Cuando se le pida que monte el sistema de archivos, seleccione **Skip**.

   Por otro lado, si la unidad no contiene ninguna partición en uso, puede desmontarlas y eliminar todo el espacio swap del disco duro con el comando `swapoff`.
2. En un indicador de comandos shell como root, ejecute el comando siguiente para asegurarse de que la partición swap está desactivada (donde `/dev/hdb2` es la partición swap):
   ```
   swapoff /dev/hdb2
   ```
3. Elimine su entrada desde `/etc/fstab`.

4. Elimine la partición usando `parted` o `fdisk`. Aquí sólo se va a discutir `parted`. Para eliminar la partición usando `parted`, haga lo siguiente:
   - En un indicador de comandos shell como root, escriba el comando `parted /dev/`*`hdb`*, donde /dev/*`hdb`* es el nombre del dispositivo para el disco duro con la partición swap a ser eliminada.
   - En el indicador `(parted)`, escriba **`print`** para visualizar las particiones existentes y determine el número minor de la partición swap que desea borrar.
   - En el indicador `(parted)`, escriba **`rm`** ***`MINOR`***, donde *`MINOR`* es el número minor de la partición a eliminar.

     
     Aviso

     Los cambios se efectúan inmediatamente; debe escribir el número minor correcto.
   - Escriba **`quit`** para salir de `parted`.

Para eliminar un archivo swap:

1. En un indicador de comandos shell como usuario root, ejecute el comando siguiente para desactivar el archivo swap (donde `/swapfile` es el archivo swap):
   ```
   swapoff /swapfile
   ```
2. Elimine su entrada de `/etc/fstab`.
3. Elimine el archivo actual:
   ```
   rm /swapfile
   ```

2.4. Mover el espacio Swap

Para mover el espacio swap de un emplazamiento a otro, siga los pasos para eliminar el espacio swap y a continuación los pasos para añadir el espacio swap.

redhat.

Capítulo 3.

Arreglo redundante de discos independientes (RAID)

3.1. ¿En qué consiste RAID?

RAID se basa en la combinación de múltiples unidades de disco pequeñas y baratas que se agrupan en un conjunto de discos para llevar a cabo acciones que no se pueden realizar con unidades grandes y costosas. El ordenador las considerará como si fueran una única unidad de disco lógica.

RAID es el método que se usa para expandir información en diversos discos utilizando técnicas como el *vaciado del disco* (RAID Nivel 0), la *creación de réplicas del disco* (RAID nivel 1) y el *vaciado del disco con paridad* (RAID Nivel 5) para obtener redundancia, menos latencia y/o aumentar el ancho de banda para leer o escribir en discos y maximizar así la posibilidad de recuperar información cuando el disco duro no funciona.

RAID está basado en el concepto de que los datos tienen que ditribuirse en cada conjunto de discos de manera consistente. Para ello, los datos se rompen en *pedazos* o grupos de datos con un tamaño que varía normalmente entre 32K y 64K aunque se pueden usar otros tamaños. Cada grupo de datos se escribe en el disco duro según el nivel de RAID. Cuando se leen los datos, se invierte el proceso de manera que parece que existan muchas unidades de disco en una sola.

3.2. Quién debe usar RAID

Cualquier persona que necesite tener a mano grandes cantidades de datos, como por ejemplo un administrador de sistemas, obtendrá grandes beneficios de la tecnología RAID. Entre otros beneficios, se incluyen los siguientes:

- Mayor velocidad
- Mayor capacidad de almacenamiento usando un solo disco virtual.
- Disminución del impacto del fallo de un disco.

3.3. Hardware y Software RAID

Existen dos posibilidades de usar RAID: hardware RAID o software RAID.

3.3.1. Hardware RAID

El sistema basado en el hardware gestiona el subsistema independientemente de la máquina y presenta a la máquina un único disco por conjunto de discos RAID.

Un ejemplo del hardware RAID sería el que se conecta a un controlador SCSI y presenta el conjunto de discos RAID en una sola unidad de disco. Un sistema externo RAID se encarga de mover la "inteligencia" RAID a un controlador que se encuentra en un subsistema de discos externo. Todo el subsistema está conectado a la máquina con un controlador SCSI normal y para la máquina es como si se tratara de una sola unidad de disco.

Los controladores RAID también tienen la forma de tarjetas que *actúan* como un controlador SCSI del sistema operativo pero se encargan de todas las comunicaciones del disco actual. En estos casos, tiene que conectar las unidades de disco al controlador RAID como si se tratara de un controlador

SCSI pero tiene que añadirlas a la configuración del controlador RAID; de todas maneras el sistema operativo nunca nota la diferencia.

3.3.2. Software RAID

El software RAID implementa los diversos niveles de RAID en el código del kernel (dispositivo de bloque). Ofrece la solución más barata ya que las tarjetas de controladores de disco o los chassis "hot-swap" son bastante caros. [1] no son requeridos. El software RAID también funciona con discos IDE más baratos así como también con discos SCSI. Con los CPUs rápidos de hoy en día, el rendimiento del software RAID aumenta considerablemente con respecto al hardware RAID.

El controlador MD en el kernel de Linux es un ejemplo de la solución RAID que es completamente independiente del hardware. El rendimiento del conjunto de discos del software RAID depende del rendimiento y de la carga del servidor CPU.

Para obtener más información sobre la configuración del Software RAID en el programa de instalación de Red Hat Linux vea la Sección 3.3.2.

Para los que estén interesados en conocer más cosas sobre el software RAID, le mostramos a continuación una lista de las principales funciones:

- Proceso de reconstrucción de subprocesos
- Configuración basada en el kernel
- Portabilidad de los conjuntos de discos entre máquinas Linux sin reconstrucción.
- Reconstrucción de los conjuntos de discos con el uso de los recursos que no se usan del sistema.
- Soporte para las unidades de disco en las que se pueden hacer cambios "en caliente" (hot-swappable)
- Detección automática de CPU con el objetivo de obtener beneficios de las mejoras de CPU.

3.4. Niveles RAID y soporte lineal

RAID soporta varias configuraciones, entre las que se incluyen los niveles 0, 1, 4, 5 y lineal. Estos tipos RAID se definen de la manera siguiente:

- *Nivel 0* — Nivel RAID 0, también llamado "striping," es una técnica de vaciado de datos. Esto significa que los datos que se escriben en la unidad de disco se rompen en grupos y se escriben en los discos que forman parte del conjunto, lo que permite un rendimiento alto de E/S a un coste inherente pero no proporciona redundancia. La capacidad de almacenamiento del nivel o es igual a la capacidad de los discos pertenecientes al hardware RAID o igual a la capacidad total de las particiones miembro del software RAID.
- *Nivel 1* — RAID level 1, o "réplicas" ha sido la técnica más usada de RAID. El nivel 1 proporciona redundancia al escribir datos idénticos en cada uno de los discos miembros dejando una copia en cada disco. Esta técnica es muy conocida debido a su simplicidad y al alto nivel de transferencia de datos cuando se leen éstos pero normalmente actúan independientemente y dan altos niveles de transferencia de datos I/O. El nivel 1 ofrece una gran fiabilidad de los datos y mejora el rendimiento

1. Un chasis de "hot-swap" le permite quitar un disco duro sin tener que apagar el ordenador.

de las aplicaciones de lectura intensa sólo que a un precio bastante alto. [2] La capacidad de almacenamiento del nivel 1 es igual a la capacidad de las réplicas de los discos duros en el hardware RAID o en una de las réplicas de las particiones del software RAID.

- *Nivel 4* — El nivel 4 usa paridad [3] concentrada en una sola unidad de disco para proteger los datos. Es mejor la transferencia de E/S que la de un fichero grande. Debido a que el disco con la paridad representa un cuello de botella inherente, el nivel 4 se usa raramente sin tecnologías como el caché de retroceso en la escritura o "write-back caching". Aunque el nivel 4 es la opción en algunos esquemas de particionamiento RAID, no se permite en las instalaciones RAID del sistema operativo Red Hat Linux. [4] La capacidad de almacenamiento del nivel 4 del hardware RAID es igual a la capacidad de los disco miembro menos la capacidad de cada disco. La capacidad de almacenamiento del software RAID en el nivel 4 es igual a la capacidad de las particiones miembro menos las dimensiones de una de las particiones si tienen el mismo tamaño.
- *Nivel 5* — Este es el tipo de RAID más común. Al distribuir la paridad entre los discos miembro, el nivel 5 elimina el cuello de botella de la escritura del nivel 4. El único cuello de botella sería el proceso para calcular la paridad. Con los software RAID y las CPUs modernas no hay problemas. Como con el nivel 4, el resultado es un rendimiento asimétrico haciendo que el de la lectura sea menor del de la escritura. El nivel 5 normalmente se usa para el caché de la escritura en retroceso para reducir la asimetría. La capacidad de almacenamiento del nivel 5 del hardware RAID es igual a la capacidad de los discos miembro menos la capacidad de cada disco miembro. La capacidad del nivel 5 del software RAID es igual a la capacidad de las particiones miembro menos el tamaño de cada una de las particiones si tienen el mismo tamaño.
- *Lineal RAID* — El nivel lineal de RAID consiste en un simple reagrupamiento de las unidades de disco para crear una unidad de disco virtual más grande. Los grupos de datos o "chunks" están situados en los discos miembro siguiendo una secuencia de manera que pasan al siguiente cuando el anterior se ha llenado. Esto no da ningún rendimiento ya que las operaciones de E/S no se rompen entre cada uno de los discos miembro. El nivel lineal de RAID no da redundancia y de hecho reduce la fiabilidad —— si uno de los discos falla, no se puede usar el conjunto de discos. La capacidad es la capacidad total de todos los discos miembro.

2. El nivel RAID 1 cuesta bastante debido a que escribe la misma información en todos los discos lo que representa una pérdida de espacio. Por ejemplo, si tiene configurado el nivel RAID 1 de manera tal que exista la partición de root en dos discos de 40G, tiene en total 80G pero solo tienen acceso 40. Los otros 40 son la réplica de los primeros 40.
3. La paridad se calcula en base a los contenidos del resto de los discos miembro. Esta información se puede usar para reconstruir los datos cuando uno de los discos falla. Los datos reconstruidos se usan para satisfacer las peticiones de E/S del disco que antes había fallado y para rellenarlo antes de que se le reemplace.
4. El nivel 4 ocupa la misma cantidad de espacio que el nivel 5 pero el nivel 5 tiene más ventajas. Por ello no se soporta el nivel 4.

Capítulo 4.

Gestor de volúmenes lógicos (LVM)

Iniciando con Red Hat Linux 9, el gestor de volúmenes lógicos (LVM) está disponible para la localización del disco duro.

LVM es un método de localización del espacio disco duro en voúmenes lógicos que pueden ser fácilmente redimensionados en vez de particiones.

Con LVM, el disco duro o grupo de discos duros está localizado para uno o más *volúmenes físicos*. Un volumen físico no abarca más de una unidad.

Los volúmenes físicos están combinados en *grupos de volúmenes lógicos*, a excepción de la partición `/boot`. La partición `/boot` no puede estar en un grupo de volúmenes lógicos porque el gestor de arranque no puede leerlo. Si desea tener la partición root `/` en un volumen lógico, necesitará crear una partición `/boot` separada que no es una parte de un grupo de volumen.

Ya que un volumen físico no puede abarcar más de una unidad, si desea que el grupo de volumen abarque más de una unidad, deberá crear uno o más volúmenes físicos por unidad.

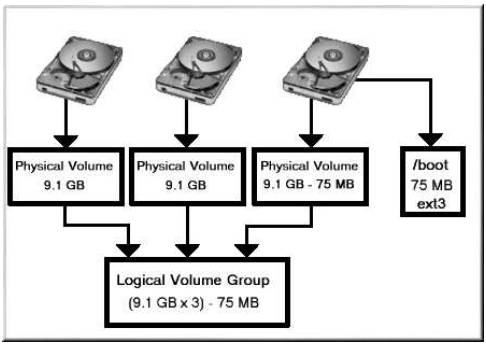

Figura 4-1. Grupo de volúmen lógico

El grupo de volumen lógico está dividido en *volúmen lógicos* , que son puntos de montaje asignados tales como `/home` y `/` y tipos de sistemas de archivos tales como ext3. Cuando las "particiones" alcanzan toda su capacidad, se puede añadir espacio libre desde el grupo de volúmenes lógicos al volumen lógico para incrementar el tamaño de la partición. Cuando se añade un nuevo disco duro a un sistema, se puede añadir al grupo de volumen lógico y los volúmenes lógicos que son particiones pueden expandirse.

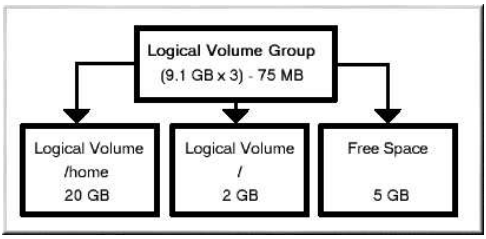

Figura 4-2. Volúmenes lógicos

Por otra parte, si un sistema está particionado con un sistema de archivos ext3, el disco duro se divide en particiones de tamaños definidos. Si una partición está completa, no es sencillo expandir el tamaño de la partición. Incluso si la partición se mueve a otro disco duro, el espacio del disco duro original deberá ser recolocado como una partición diferente o sin usar.

El soporte LVM deberá ser compilado en el kernel. El kernel por defecto para Red Hat Linux 9 está compilado con soporte LVM.

Para aprender cómo configurar LVM durante el proceso de instalación Red Hat Linux, remítase al Capítulo 11.

redhat.

Capítulo 5.

Gestión del almacenamiento en disco

Después de haber instalado su sistema Red Hat Linux, puede que desee visualizar la tabla de particiones existente, cambiar el tamaño de las particiones, eliminar particiones o añadir particiones desde espacio libre o discos duros adicionales. La utilidad `parted` le permite llevar a cabo estas tareas. Este capítulo trata de cómo usar `parted` para llevar a cabo tareas de sistemas de archivo. Por otra parte, puede usar `fdisk` para realizar la mayoría de estas tareas, excepto redimensionar las particiones. Para más información sobre `fdisk`, refiérase a la página del manual o de información de `fdisk`.

Si quiere visualizar el uso del espacio del disco de sistema o controlar el uso del espacio de disco, consulte Sección 26.3.

Debe tener instalado el paquete `parted` para usar la utilidad `parted`. Para iniciar `parted`, en un indicador de comandos shell como root, escriba el comando `parted /dev/hdb`, donde */dev/hdb* es el nombre del dispositivo para el disco que desea configurar. Verá un indicador `(parted)`. Escriba `help` para visualizar una lista de comandos disponibles.

Si desea crear, eliminar o cambiar el tamaño a una partición, el dispositivo no puede estar en uso (no puede haber particiones montadas y el espacio swap no puede estar activado). El modo más fácil de lograr esto es arrancando el sistema en modo de rescate. Consulte el Capítulo 9 para instrucciones sobre cómo arrancar en modo de rescate. Cuando aparezca el indicador para montar el sistema de archivos, seleccione **Saltar**.

Por otra parte, si la unidad no contiene ninguna partición en uso, puede desmontarlas con el comando `umount` y eliminar todo el espacio swap en el disco duro con el comando `swapoff`.

La Tabla 5-1 contiene una lista de los comandos `parted` más usados. Las secciones siguientes explican algunos de ellos con más detalles.

Comando	Descripción
`check` *`minor-num`*	Ejecuta un chequeo sencillo del sistema de archivos
`cp` *`desde a`*	Copiar un sistema de archivos desde una partición a otra; *`desde`* y *`hasta`* son los números 'minor' de las particiones
`help`	Muestra una lista de los comandos disponibles
`mklabel` *`etiqueta`*	Crea una etiqueta de disco para la tabla de particiones
`mkfs` *`numero-minor tipo-de-sistema-de-archivos`*	Crea un sistema de archivos del tipo *`tipo-de-sistema-de-archivos`*
`mkpart` *`tipo-particion tipo-sa start-mb end-mb`*	Crea una partición sin crear un nuevo sistema de archivos
`mkpartfs` *`tipo-particion tipo-sa start-mb end-mb`*	Crea una partición y crea un nuevo sistema de archivos
`move` *`numero-minor start-mb end-mb`*	Mueve la partición
`print`	Visualiza la tabla de particiones
`quit`	Sale de `parted`

Comando	Descripción
`resize numero-minor start-mb end-mb`	Redimensiona la partición desde *start-mb* a *end-mb*
`rm numero-minor`	Elimina la partición
`select dispositivo`	Selecciona un dispositivo diferente a configurar
`set numero-minor bandera estado`	Coloca una bandera a la partición; *estado* es 'on' o 'off'

Tabla 5-1. Comandos `parted`

5.1. Visualizar la tabla de particiones

Después de iniciar `parted`, escriba el comando siguiente para visualizar la tabla de particiones:

```
print
```

Aparecerá una tabla similar a lo siguiente:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor    Start       End     Type      Filesystem  Flags
1          0.031    101.975  primary   ext3        boot
2        101.975    611.850  primary   linux-swap
3        611.851    760.891  primary   ext3
4        760.891   9758.232  extended              lba
5        760.922   9758.232  logical   ext3
```

La primera línea muestra el tamaño del disco, la segunda muestra el tipo de etiqueta del disco y el resto de la salida muestra la tabla de partición. En la tabla en particular, el número **Minor** es el número de la partición. Por ejemplo, la partición con número minor 1 corresponde a `/dev/hda1`. Los valores de **Inicio** y **Final** están en megabytes. El **Tipo** es primario, extendido o lógico. El **Sistema de archivos** es el tipo de sistema de archivos, que puede ser uno de los siguientes: ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs, o xfs. La columna **Etiquetas** enumera todas la etiquetas colocadas para la partición. Las etiquetas disponibles son boot, root, swap, hidden, raid, lvm, o lba.

Sugerencia

Para seleccionar un dispositivo diferente sin tener que reiniciar `parted`, use el comando `select` seguido del nombre del dispositivo, como por ejemplo `/dev/hdb`. A continuación, puede visualizar o configurar la tabla de particiones.

5.2. Creación de una partición

Aviso

No intente crear una partición en un dispositivo que se encuentre en uso.

Antes de crear una partición, arranque en modo de rescate (o desmonte cualquier partición en el dispositivo y elimine cualquier espacio swap).

Inicie `parted`, donde /dev/*hda* es el dispositivo en el que se crea la partición:

```
parted /dev/hda
```

Visualice la tabla de particiones actual para determinar si hay suficiente espacio libre:

```
print
```

Si no hay suficiente espacio libre, puede cambiar el tamaño de partición ya existente. Consulte Sección 5.4 para obtener más detalles.

5.2.1. Crear la partición

Desde la tabla de particiones, determine los puntos de comienzo y fin de la nueva partición y qué tipo de partición debe ser. Puede tener solamente cuatro particiones primarias (sin partición extendida) en un dispositivo. Si necesita más de cuatro particiones, puede tener tres particiones primarias, una partición extendida y varias particiones lógicas dentro de la extendida. Para obtener una visión general de las particiones de disco, consulte el apéndice *Introducción a la creación de particiones* en el *Manual de instalación de Red Hat Linux*.

Por ejemplo, para crear una partición primaria con un sistema de archivos ext3 desde 1024 megabytes hasta 2048 megabytes en un disco duro, escriba el siguiente comando:

```
mkpart primary ext3 1024 2048
```

Sugerencia

Si en cambio usa el comando `mkpartfs`, el sistema de archivos se creará después de que se haya creado la partición. Sin embargo, `parted` no soporta crear un sistema de archivos ext3. Por ello, si desea crear un sistema de archivos ext3, use `mkpart` y cree el sistema de archivos con el comando `mkfs` como se describe a continuación. `mkpartfs` funciona para el tipo de sistema de archivos linux-swap.

Los cambios se harán efectivos tan pronto como presione [Intro], por tanto revise bien el comando antes de ejecutarlo.

Después de crear la partición, use el comando `print` para confirmar que está en la tabla de particiones con el tipo de partición, tipo de sistema de archivos y tamaño correctos. Recuerde también el número minor de la nueva partición, de modo que pueda etiquetarla. También debería visualizar la salida de

```
cat /proc/partitions
```

para asegurarse de que el kernel reconoce la nueva partición.

5.2.2. Formatear la partición

La partición no tiene todavía un sistema de archivos. Cree el sistema de archivos:

```
 /sbin/mkfs -t ext3 /dev/hdb3
```


Aviso

Al formatear la partición se destruirán permanentemente los datos que existan en la partición.

5.2.3. Etiquetar la partición

A continuación, dé una etiqueta a la partición. Por ejemplo, si la nueva partición es `/dev/hda3` y quiere etiquetarla `/work`:

```
e2label /dev/hda3 /work
```

Por defecto, el programa de instalación de Red Hat Linux utiliza el punto de montaje de la partición como la etiqueta para asegurarse de que la etiqueta es única. Puede utilizar cualquier etiqueta que desee.

5.2.4. Crear un punto de montaje

Como usuario root, cree un punto de montaje:

```
mkdir /work
```

5.2.5. Añadir `/etc/fstab`

Como root, edite el archivo `/etc/fstab` para incluir la nueva partición. La nueva línea debe ser parecida a la siguiente:

```
LABEL=/work           /work                ext3    defaults        1 2
```

La primera columna debe contener `LABEL=` seguida de la etiqueta que usted dió a la partición. La segunda columna debe contener el punto de montaje para la nueva partición y la columna siguiente debería ser el tipo de sistema de archivo (por ejemplo, ext3 o swap). Si necesita más información sobre el formato, lea la página man con el comando `man fstab`.

Si la cuarta columna es la palabra `defaults`, la partición se montará en el momento de arranque. Para montar la partición sin arrancar de nuevo, como root, escriba el comando:

```
mount /work
```

5.3. Eliminar una partición


Aviso

No intente eliminar una partición en un dispositivo que se encuentre en uso.

Antes de eliminar una partición, arranque en modo de rescate (o desmonte cualquier partición en el dispositivo y elimine cualquier espacio swap).

Inicie `parted`, donde /dev/*hda* es el dispositivo en el que se va a eliminar la partición:

```
parted /dev/hda
```

Visualice la tabla de particiones actual para determinar el número minor de la partición que se quiere eliminar:

```
print
```

Elimine la partición con el comando `rm`. Por ejemplo, para eliminar la partición con un número minor 3:

```
rm 3
```

Los cambios comienzan a efectuarse en el momento en que usted presiona [Intro], así que revise el comando antes de ejecutarlo.

Luego de eliminar la partición, use el comando `print` para confirmar que se ha eliminado de la tabla de particiones. Debería también visualizar la salida de datos de

```
cat /proc/partitions
```

para asegurarse de que el kernel sabe que la partición se ha eliminado.

El último paso es eliminarla del archivo `/etc/fstab`. Encuentre la línea que dice que la partición ha sido borrada y bórrela del archivo.

5.4. Redimensionar una partición

Aviso

No intente cambiar el tamaño de una partición en un dispositivo que se encuentra en uso.

Antes de cambiar el tamaño a una partición, arranque en modo de rescate (o desmonte cualquier partición en el dispositivo y elimine cualquier espacio swap en el dispositivo).

Arranque `parted`, donde /dev/*hda* es el dispositivo en el cual se redimensionará la partición:

```
parted /dev/hda
```

Visualice la tabla de particiones actual para determinar el número minor de la partición que se quiere redimensionar, así como los puntos de comienzo y fin para la partición:

```
print
```

Aviso

El espacio usado de la partición que se quiere redimensionar no puede ser mayor que el nuevo tamaño.

Para redimensionar la partición, use el comando `resize` seguido del número minor de la partición, el lugar comienzo y fin en megabytes. Por ejemplo:

```
resize 3 1024 2048
```

Después de cambiar el tamaño a la partición, use el comando `print` para confirmar que se ha cambiado el tamaño de la partición correctamente, que es el tipo de partición y de sistema de archivos correcto.

Después de reiniciar el sistema el modo normal, use el comando `df` para asegurarse que la partición fué montada y que es reconocida con el nuevo tamaño.

redhat.

Capítulo 6.

Implementación de cuotas de disco

Además de controlar el espacio en disco usado por el sistema (consulte la Sección 26.3.1), el almacenamiento en disco se puede restringir mediante la implementación de cuotas de disco y de esta manera el administrador es notificado antes de que un usuario consuma mucho espacio en disco o que una partición se llene.

Las cuotas se pueden configurar para usuarios individuales o para grupos. Este tipo de flexibilidad hace posible darle a cada usuario una pequeña porción del disco para que maneje sus archivos personales (tales como correo o informes), mientras que se le permite tener más espacio para manejar los proyectos en los que estén trabajando o cuotas más grandes (asumiendo que a los proyectos se les dá sus propios grupos).

Además, se puede configurar las cuotas no sólo para que controlen el número de bloques de disco pero también el número de inodes. Debido a que los inodes son usados para contener información relacionada a los archivos, esto permite controlar el número de archivos que pueden ser creados.

El RPM `quota` debe estar instalado para implementar las cuotas de disco. Para más información sobre la instalación de paquetes RPM, consulte Parte V.

6.1. Configuración de cuotas de disco

Para implementar cuotas de disco, siga los pasos siguientes:

1. Active cuotas por sistema de archivo modificando `/etc/fstab`
2. Vuelva a montar el sistema de archivos
3. Cree los archivos cuota y genere la tabla de uso de espacio en disco
4. Asigne las cuotas

A continuación se describen cada uno de estos pasos en detalle.

6.1.1. Activar cuotas

Como usuario root, use el editor de texto de su preferencia, añada las opciones `usrquota` y/o `grpquota` al sistema de archivos que requiere cuotas:

```
LABEL=/           /              ext3    defaults         1 1
LABEL=/boot       /boot          ext3    defaults         1 2
none              /dev/pts       devpts  gid=5,mode=620   0 0
LABEL=/home       /home          ext3    defaults,usrquota,grpquota 1 2
none              /proc          proc    defaults         0 0
none              /dev/shm       tmpfs   defaults         0 0
/dev/hda2         swap           swap    defaults         0 0
/dev/cdrom        /mnt/cdrom     udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0          /mnt/floppy    auto    noauto,owner,kudzu 0 0
```

En este ejemplo, el sistema de archivos `/home` tiene cuotas de usuario y grupo ambas activadas.

6.1.2. Volver a montar un sistema de archivos

Después de agregar las opciones `userquota` y `grpquota`, vuelva a montar cada sistema de archivos cuyas entradas `fstab` hayan sido modificadas. Si el sistema de archivo no está siendo usado por ningún proceso, use el comando `umount` seguido de `mount` para volver a montar el sistema de archivos. Si el sistema de archivos está siendo usado actualmente, el método más fácil para volver a montar el sistema de archivos es reiniciando el sistema.

6.1.3. Creación de archivos de cuotas

Después de volver a montar cada sistema de archivos con cuotas, el sistema puede funcionar con cuotas de disco. Sin embargo, el sistema de archivos mismo no está listo para soportar cuotas. El próximo paso es ejecutar el comando `quotacheck`.

El comando `quotacheck` examina los sistemas de archivos con cuotas activadas y construye una tabla del uso del disco por sistema de archivo. La tabla es luego usada para actualizar la copia del uso del disco del sistema operativo. Además, los archivos de cuotas de disco del sistema de archivos, son actualizados.

Para crear los archivos de cuotas (`aquota.user` y `aquota.group`) en el sistema de archivos, use la opción `-c` del comando `quotacheck`. Por ejemplo, si las cuotas del usuario y grupos están activadas para la partición `/home`, cree los archivos en el directorio `/home`:

```
quotacheck -acug /home
```

La opción `-a` significa que todos los sistemas de archivos no NFS montados en `/etc/mtab` son chequeados para ver si las cuotas están activadas. La opción `-c` especifica que los archivos de cuota deberían ser creados para cada sistema de archivos con cuotas activadas, la opción `-u` especifica que se debe verificar por cuotas de usuario, y la opción `-g` indica verificar por cuotas de grupo.

Si no se especifican ninguna de las opciones `-u` ni `-g`, sólo se creará el archivo de cuota de usuario. Si únicamente se especifica la opción `-g`, sólo se creará el archivo de cuota de grupo.

Después de creados los archivos, ejecute el comando siguiente para generar la tabla del uso actual del disco duro por el sistema de archivos con cuotas activadas:

```
quotacheck -avug
```

Las opciones usadas son como se muestra a continuación:

- `a` — Verifica todos los sistemas de archivos montados localmente con cuotas activadas
- `v` — Muestra detalles informativos a medida que la verificación de cuotas se ejecuta
- `u` — Verifica la información de cuota de disco
- `g` — Verifica la información de cuota de disco del grupo

Después que `quotacheck` ha finalizado, los archivos de cuotas correspondiente a las cuotas activas (usuario y/o grupos) son poblados con datos para cada sistema de archivos con cuotas activadas, tal como `/home`.

6.1.4. Asignación de cuotas por usuario

El último paso es asignar las cuotas de disco con el comando `edquota`.

Para configurar la cuota por usuario, como usuario root en el intérprete shell, ejecute el comando:

```
edquota username
```

Ejecute este paso para cada usuario para el cual desea implementar una cuota. Por ejemplo, si una cuota es activada en `/etc/fstab` para la partición `/home` (`/dev/hda3`) y se ejecuta el comando `edquota testuser`, se mostrará lo siguiente en el editor configurado como predeterminado en su sistema:

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436          0          0      37418        0        0
```

Nota

El editor de texto definido por la variable de ambiente EDITOR es usado por `edquota`. Para cambiar el editor, configure la variable de ambiente EDITOR a la ruta completa del editor de su preferencia.

La primera columna es el nombre del sistema de archivos que tiene una cuota activada. La segunda columna muestra cuántos bloques está usando el usuario actualmente. Las próximas dos columnas son usadas para colocar límites de bloques duros y suaves para el usuario del sistema de archivos. La columna `inodes` muestra cuántos inodes está usando el usuario actualmente. Las últimas dos columnas son usadas para colocar los límites duros y suaves para los inodes del usuario en el sistema de archivos.

Un límite duro es la cantidad máxima absoluta de espacio en disco que un usuario o grupo puede usar. Una vez que se alcance el límite, no se puede usar más espacio.

El límite suave define la cantidad máxima de espacio en disco que puede ser usado. Sin embargo, a diferencia del límite duro, el límite suave puede ser excedido durante cierto tiempo. Este tiempo es conocido como *período de gracia*. El período de gracia puede ser expresado en segundos, minutos, horas, días, semanas o meses.

Si cualquiera de los valores está especificado a 0, ese límite no está configurado. En el editor de texto, cambie los límites deseados. Por ejemplo:

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436     500000     550000      37418        0        0
```

Para verificar que la cuota para el usuario ha sido configurada, use el comando:

```
quota testuser
```

6.1.5. Asignación de cuotas por grupo

Las cuotas también pueden ser asignadas por grupos. Por ejemplo, para configurar una cuota de grupo para el grupo `devel`, use el comando (el grupo debe existir antes de configurar la cuota):

```
edquota -g devel
```

Este comando muestra la cuota existente para el grupo en el editor de texto:

```
Disk quotas for group devel (gid 505):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440400          0          0      37418        0        0
```

Modifique los límites y guarde el archivo, luego configure la cuota.

Para verificar que la cuota del grupo ha sido definida, use el comando:

```
quota -g devel
```

6.1.6. Asignación de cuotas por sistema de archivos

Para asignar cuotas basándose en cada sistema de archivos activado para cuotas, use el comando:

```
edquota -t
```

Como los otros comandos `edquota`, abre una de las cuotas actuales para el sistema de archivos en el editor de texto:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem             Block grace period     Inode grace period
  /dev/hda3                     7days                  7days
```

Cambie el período de gracia del bloque o inode, guarde los cambios del archivo y salga del editor.

6.2. Administración de cuotas de disco

Si se implementan cuotas, se requiere también mantenerlas — esto es, ver que las cuotas no excedan su espacio y que sean correctas. Por supuesto, si los usuarios repetidamente superan sus cuotas o regularmente alcanzan el límite suave, el administrador tiene algunas decisiones que tomar dependiendo del tipo de usuario y de cuánto espacio en disco impacta su trabajo. El administrador puede bien sea ayudar al usuario a que administre mejor su espacio o incrementar la cuota de disco, si se requiere.

6.2.1. Informes de cuotas de disco

Para crear un informe del uso del disco debe usar la utilidad `repquota`. Por ejemplo, el comando `repquota /home` produce la siguiente salida:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --      36       0       0              4     0     0
tfox      --     540       0       0            125     0     0
testuser  --  440400  500000  550000          37418     0     0
```

Para ver el informe sobre el uso del disco por parte de todos los sistemas de archivos con cuotas, use el comando siguiente:

```
repquota -a
```

Aún cuando el informe es fácil de leer, es importante resaltar algunos puntos. La marca `--` mostrada luego de cada usuario es una forma rápida de determinar si los límites del bloque o inode han sido excedidos. Si el límite suave es excedido aparecerá un símbolo `+` en lugar del correspondiente `-`; el primer `-` representa el límite del bloque, y el segundo el límite del inode.

La columna `grace` está normalmente en blanco. Si se ha excedido el límite suave, la columna contiene una especificación de tiempo igual al tiempo restante en el período de gracia. Si el período de gracia ha expirado, aparecerá `none` en su lugar.

6.2.2. Mantenimiento de la precisión de las cuotas

Cada vez que el sistema de archivos se desmonta de forma inadecuada (debido a una falla del sistema, por ejemplo), es necesario ejecutar `quotacheck`. Sin embargo, `quotacheck` puede ser ejecutado de forma regular, aún cuando el sistema no haya fallado. Mediante la ejecución regular de este comando se ayuda a mantener la exactitud de las cuotas (las opciones usadas son descritas en la Sección 6.1.1):

```
quotacheck -avug
```

La forma más fácil de ejecutar esto periódicamente es usando `cron`. Como root, puede bien sea usar el comando `crontab -e` para planificar un `quotacheck` periódicamente, o colocar un script que ejecute `quotacheck` en alguno de los directorios siguientes (usando el intervalo que más le convenga):

- `/etc/cron.hourly`
- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/etc/cron.monthly`

Las estadísticas de cuotas más exactas pueden se obtenidas cuando el sistema de archivos analizado no está en uso activo. Por tanto, la tarea cron debería ser planificada cuando se esté usando lo menos posible el sistema de archivos. Si esta hora varía para diferentes sistemas de archivos con cuotas, ejecute `quotacheck` para cada sistema de archivos en las diferentes horas mediante múltiples tareas cron.

Consulte el Capítulo 28 para más información sobre la configuración de `cron`.

6.2.3. Activación y desactivación de cuotas

Es posible desactivar cuotas sin tener que colocarlas a 0. Para desactivar todos los usuarios y grupos, use el comando siguiente:

```
quotaoff -vaug
```

Si ninguna de las opciones `-u` o `-g` son especificadas, solamente se desactivarán las cuotas de usuarios. Si únicamente se especifica `-g`, sólo se desactivarán las cuotas de grupo.

Para activar las cuotas nuevamente, use el comando `quotaon` con las mismas opciones.

Por ejemplo, para activar las cuotas de usuarios y grupos para todos los sistemas de archivos:

```
quotaon -vaug
```

Para activar cuotas para un sistema de archivos específico, tal como `/home`:

```
quotaon -vug /home
```

Si no se especifican ninguna de las opciones `-u` ni tampoco `-g`, sólo se activarán las cuotas de usuarios. Si sólo se escribe la opción `-g`, únicamente las cuotas de grupo serán activadas.

6.3. Recursos adicionales

Para más información sobre cuotas de disco, consulte los siguientes recursos.

6.3.1. Documentación instalada

- Las páginas de manual de `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon`, y `quotaoff`

6.3.2. Libros relacionados

- *Manual de administración del sistema de Red Hat Linux* — Disponible desde http://www.redhat.com/docs y en el CD de Documentación, este manual contiene información de fondo sobre la administración del almacenamiento (incluyendo cuotas) para nuevos administradores de sistemas Red Hat Linux.

II. Información relacionada a la instalación

El *Manual de instalación de Red Hat Linux* discute la instalación de Red Hat Linux y algunas alternativas para la solución de problemas después de la instalación. Sin embargo, en este manual se discuten las opciones de instalación avanzadas. Esta parte proporciona instrucciones para *kickstart* (una técnica de instalación automática), modos de recuperación del sistema (como arrancar su sistema si este es incapaz de arrancar al nivel normal), como configurar RAID durante la instalación y como configurar LVM. Use esta parte en conjunto con el *Manual de instalación de Red Hat Linux* para llevar a cabo cualquiera de estas tareas avanzadas de instalación.

Tabla de contenidos

redhat.

Capítulo 7.

Instalaciones Kickstart

7.1. ¿Qué son las instalaciones Kickstart?

Muchos administradores de sistemas preferieren usar un método de instalación automatizado para instalar Red Hat Linux en sus máquinas. Para cubrir esta necesidad, Red Hat creó el método de instalación kickstart. Usando kickstart, un administrador de sistemas puede crear un archivo conteniendo las respuestas a todas las preguntas que normalmente se le preguntarán durante una instalación típica de Red Hat Linux.

Los archivos kickstart se pueden mantener en un servidor de sistema único y ser leídos por computadores individuales durante la instalación. Este método de instalación puede soportar el uso de un sólo archivo kickstart para instalar Red Hat Linux en múltiples máquinas, haciéndolo ideal para administradores de sistemas y de red.

Kickstart le permite automatizar la instalación de Red Hat Linux.

7.2. ¿Cómo realizar una instalación de Kickstart?

Las instalaciones de Kickstart pueden realizarse usando un CD-ROM, un disco duro local, o a través de NFS, FTP, o HTTP.

Para usar kickstart, debe:

1. Crear un archivo kickstart.
2. Crear un disquete de arranque con el archivo o hacer el kickstart disponible en la red.
3. Hacer el árbol de instalación disponible.
4. Iniciar la instalación de kickstart.

Este capítulo explica estos pasos en detalle.

7.3. Crear un archivo Kickstart

El archivo kickstart es un archivo de texto simple, conteniendo una lista de items, cada uno identificado por una clave. Puede crearlo editando una copia del archivo `sample.ks` encontrado en el directorio `RH-DOCS` del CD de documentación de Red Hat Linux, usando la aplicación **Configurador de Kickstart**, o escribiéndolo desde el principio. El programa de instalación de Red Hat Linux también crea un archivo kickstart de muestra basado en las opciones que seleccionó durante la instalación. Se escribe al archivo `/root/anaconda-ks.cfg`. Debería ser capaz de modificarlo en cualquier editor de texto o procesador de texto que pueda guardar archivos como texto ASCII.

Primero, debe estar consciente de los siguientes problemas cuando está creando su archivo kickstart:

- Las secciones deben ser especificadas *en orden*. Los items dentro de las secciones no tienen que estar en un orden en particular a menos que se especifique lo contrario. El orden de la sección es:
  - Sección de comandos — Refiérase a la Sección 7.4 para una lista de las opciones de kickstart. Debe incluir las opciones requeridas.

- La sección `%packages` — Refiérase a la Sección 7.5 para más detalles.
- Las secciones `%pre` y `%post` — Estas dos secciones pueden estar en cualquier orden y no son requeridas. Refiérase a la Sección 7.6 y a la Sección 7.7 para más detalles.

- Los items que no son requeridos se pueden omitir.
- Al omitir cualquier item requerido puede resultar en que el programa de instalación solicite al usuario alguna respuesta relacionada al item, de la misma forma que se le preguntaría al usuario durante una instalación típica. Una vez que se da la respuesta, la instalación continuará (a menos que encuentre otro item faltante).
- Las líneas que comienzan con un símbolo numeral o almohadilla (#) son tratadas como comentarios y por tanto ignoradas.
- Para *actualizaciones* de kickstart, se requieren los siguientes items:
  - Idioma
  - Soporte de idioma
  - Método de instalación
  - Especificación de dispositivos (si se necesita un dispositivo para realizar la instalación)
  - Configuración del teclado
  - La palabra `upgrade`
  - Configuración del gestor de arranque

  Si otros items son especificados para una actualización, esos items serán ignorados (observe que esto incluye la selección de paquetes).

7.4. Opciones de Kickstart

Las opciones siguientes se pueden colocar en un archivo kickstart. Si prefiere usar una interfaz gráfica para la creación de su archivo kickstart, puede usar la aplicación **Configurador Kickstart**. Consulte el Capítulo 8 para más detalles.

Nota

Si la sección es seguida por símbolo igual (=), se debe especificar un valor después de él. En los comandos de ejemplo, las opciones en corchetes ([]) son argumentos opcionales para el comando.

`autostep` (opcional)

Similar a `interactive` excepto que se va a la pantalla siguiente por usted. Es usado la mayoría de las veces para depuración.

`auth` o `authconfig` (requerido)

Configura las opciones de autenticación para el sistema. Es similar al comando `authconfig`, el cual puede ser ejecutado después de la instalación. Por defecto, las contraseñas son encriptadas y no shadow.

`--enablemd5`

Use md5 encryption para contraseñas de usuario.

`--enablenis`

Activa el soporte NIS. Por defecto, `--enablenis` usa el dominio que encuentre en la red. Un dominio casi siempre se debería configurar a mano con la opción `--nisdomain=`.

`--nisdomain=`

Nombre de dominio NIS para usar con los servicios NIS.

`--nisserver=`

Servidor para usar con los servicios NIS (difusión por defecto).

`--useshadow` o `--enableshadow`

Usar contraseñas shadow.

`--enableldap`

Activa el soporte LDAP en `/etc/nsswitch.conf`, permitiéndole a su sistema recuperar información sobre usuarios (UIDs, directorios principales, shells, etc.) de un directorio LDAP. Para usar esta opción, debe instalar el paquete `nss_ldap`. Debe también especificar un servidor y una base DN con `--ldapserver=` y `--ldapbasedn=`.

`--enableldapauth`

Usar LDAP como un método de autenticación. Esto activa el módulo `pam_ldap` para autenticación y cambio de contraseñas, usando un directorio LDAP. Para usar esta opción, debe tener el paquete `nss_ldap` instalado. Debe también especificar un servidor y una base DN con `--ldapserver=` y `--ldapbasedn=`.

`--ldapserver=`

Si especificó `--enableldap` o `--enableldapauth`, use esta opción para especificar el nombre del servidor LDAP a utilizar. Esta opción se configura en el archivo `/etc/ldap.conf`.

`--ldapbasedn=`

Si especificó `--enableldap` o `--enableldapauth`, el DN (distinguished name) en su árbol de directorio LDAP bajo el cual la información de usuario es almacenada. Esta opción es configurada en el archivo `/etc/ldap.conf`.

`--enableldaptls`

Use bloqueos TLS (Transport Layer Security). Esta opción permite a LDAP enviar nombres de usuario encriptados y contraseñas a un servidor LDAP antes de la autenticación.

`--enablekrb5`

Usa Kerberos 5 para autenticación de usuarios. Kerberos mismo no conoce sobre directorios principales, UIDs, o shells. Por lo tanto si activa Kerberos necesitará hacer las cuentas de usuarios conocidas a esta estación de trabajo mediante la activación de LDAP, NIS, o Hesiod o mediante el uso del comando `/usr/sbin/useradd`. Si usa esta opción, debería tener el paquete `pam_krb5` instalado.

`--krb5realm=`

El entorno Kerberos 5 al cual su estación pertenece.

`--krb5kdc=`

El KDC (o KDCs) que sirve peticiones para el entorno. Si tiene múltiples KDCs en su entorno, separe sus nombres con comas (,).

`--krb5adminserver=`

El KDC en su entorno que también está ejecutanso kadmind. Este servidor maneja el cambio de contraseñas y otras peticiones administrativas. Este servidor debe ser ejecutado en el KDC principal si tiene más de un KDC.

`--enablehesiod`

Activa el soporte Hesiod para buscar directorios principales, UIDs y shells. Se encuentra más información sobre la configuracion y uso de Hesiod en `/usr/share/doc/glibc-2.x.x/README.hesiod`, el cual está incluido en el paquete `glibc`. Hesiod es una extensión de DNS que usa los registros DNS para almacenar información sobre usuarios, grupos y otros varios items.

`--hesiodlhs`

La opción Hesiod LHS ("left-hand side"), configurada en `/etc/hesiod.conf`. Esta opción es usada por la libreria Hesiod para determinar el nombre a buscar en DNS cuando se esté buscando información, similar al uso de LDAP de una base DN.

`--hesiodrhs`

La opción Hesiod RHS ("right-hand side"), configurada en `/etc/hesiod.conf`. Esta opción es usada por la librería Hesiod para determinar el nombre a buscar en el DNS cuando se esté buscando información, similar al uso de LDAP de una base DN.

Sugerencia

Para buscar información para "jim", la libreria Hesiod busca por *jim.passwd<LHS><RHS>*, lo cual debería resolver a un registro TXT que se parece a una entrada de contraseña (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Para grupos, la situación es idéntica, excepto que se usaría *jim.group<LHS><RHS>*.

Buscar usuarios y grupos por nombre es manejado haciendo "501.uid" un CNAME para "jim.passwd", y "501.gid" un CNAME para "jim.group". Observe que LHS y RHS no tienen puntos [.] colocados al frente de ellos cuando la libreria determina el nombre para el cual buscar, así LHS y RHS usualmente comienzan con puntos.

`--enablesmbauth`

Activa la autenticación de usuarios con un servidor SMB (típicamente un servidor Samba o Windows). La autenticación SMB no conoce sobre directorios principales, UIDs, o shells. Por lo tanto si lo activa necesita hacer las cuentas de los usuarios conocidas a la estación de trabajo activando LDAP, NIS, o Hesiod o usando el comando `/usr/sbin/useradd`. Para usar esta opción, debe tener el paquete `pam_smb` instalado.

`--smbservers=`

El nombre del o los servidores a usar para la autenticación SMB. Para especificar más de un servidor, separe los nombres con comas (,).

`--smbworkgroup=`

El nombre del grupo de trabajo para los servidores SMB.

`--enablecache`

Activa el servicio `nscd`. El servicio `nscd` captura la información sobre usuarios, grupos y otros tipos de información. El uso de caché es especialmente útil si selecciona distribuir información sobre grupos y usuarios sobre la red usando NIS, LDAP, o hesiod.

`bootloader` (requerido)

Especifica cómo el gestor de arranque debería ser instalado y si el gestor de arranque debería ser LILO o GRUB. Esta opción es requerida tanto para instalaciones como para actualizaciones. Para actualizaciones, si no se especifica `--useLilo` y LILO es el gestor de arranque actual, el gestor de arranque se cambiará a GRUB. Para mantener LILO sobre las actualizaciones, use `bootloader --upgrade`.

`--append=`

Especifica los parámetros del kernel. Para especificar múltiples parámetros, sepárelos con espacios. Por ejemplo:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

`--location=`

Especifica dónde se escribirá el registro de arranque. Los valores válidos son los siguientes: `mbr` (valor por defecto), `partition` (instala el gestor de arranque en el primer sector de la partición que contiene el kernel), o `none` (no instala el gestor de arranque).

`--password=`

Si se está usando GRUB, configura la contraseña de GRUB especificada con esta opción. Esto debería ser usado para restringir el acceso al shell de GRUB, donde se pueden pasar opciones arbitrarias del kernel.

`--md5pass=`

Si se está usando GRUB, similar a `--password=` excepto que la contraseña debería estar ya encriptada.

`--useLilo`

Use LILO en vez de GRUB como el gestor de arranque.

`--linear`

Si se está usando LILO, use la opción `linear` LILO; esto es sólo para compatibilidad hacia atrás (y linear es ahora usada por defecto).

`--nolinear`

Si se está usando LILO, use la opción `nolinear` LILO; linear es el defecto.

`--lba32`

Si se está usando LILO, forzar el uso del modo lba32 en vez de auto-detección.

`--upgrade`

Actualizar la configuración del gestor de arranque existente, preservando las viejas entradas. Esta opción está solamente disponible para actualizaciones.

`clearpart` (opcional)

Remueve las particiones del sistema, antes de la creación de nuevas particiones. Por defecto, no se remueve ninguna partición.

Nota

Si el comando `clearpart` es usado, entonces el comando `--onpart` no puede ser usado en una partición lógica.

`--linux`

Elimina todas las particiones Linux.

`--all`

Elimina todas las particiones del sistema.

`--drives=`

Especifica desde cuáles unidades limpiar las particiones. Por ejemplo, lo siguiente limpia las particiones de las primeras dos unidades en el controlador IDE primario:

```
clearpart --drives hda,hdb
```

`--initlabel`

Inicializa la etiqueta del disco al valor para la arquitectura por defecto (por ejemplo `msdos` para x86 y `gpt` para Itanium). Es útil que el programa de instalación no le pregunte si debería inicializar la etiqueta del disco si se está instalando a un nuevo disco duro.

`device` (opcional)

En la mayoría de los sistemas PCI, el programa de instalación verificará automáticamente las tarjetas Ethernet y SCSI adecuadamente. En los sistemas más viejos y en algunos sistemas PCI, sin embargo, kickstart necesita una pista para encontrar los dispositivos adecuadamente. El comando `device`, que le dice al programa de instalación que instale módulo extra, está en este formato:

`device <type> <moduleName> --opts=<options>`

<type>

Reemplace con `scsi` o `eth`

<moduleName>

Reemplace con el nombre del módulo kernel que debería ser instalado.

`--opts=`

Opciones a pasar al módulo kernel. Note que múltiples opciones pueden ser pasadas si son colocadas entre comillas. Por ejemplo:

```
--opts="aic152x=0x340 io=11"
```

`deviceprobe` (opcional)

Fuerza la verificación del bus PCI y carga módulos para todos los dispositivos encontrados si un módulo está disponible.

`driverdisk` (opcional)

Los discos de controladores se pueden usar durante instalaciones kickstart. Necesitará copiar los contenidos del disco de controladores al directorio raíz de una partición en el disco duro del sistema. Luego necesitará usar el comando `driverdisk` para indicarle al programa de instalación donde buscar por el disco de controladores.

`driverdisk <partition> [--type=<fstype>]`

<partition>

La partición que contiene el disco de controladores.

`--type=`

Tipo de sistema de archivo (por ejemplo, vfat o ext2).

`firewall` (opcional)

Esta opción corresponde a la pantalla **Configuración del Firewall** en el programa de instalación:

`firewall <securitylevel> [--trust=] <incoming> [--port=]`

<securitylevel>

Reemplace con alguno de los siguientes niveles de seguridad:

- `--high`
- `--medium`
- `--disabled`

`--trust=`

Al listar un dispositivo aquí, tal como eth0, permite que todo el tráfico proveniente de ese dispositivo pase a través del firewall. Para listar más de un dispositivo, use `--trust eth0 --trust eth1`. No use el formato de separación por comas tal como `--trust eth0, eth1`.

<incoming>

Reemplace con una o más de lo siguiente para permitir que servicios específicos pasen a través del cortafuegos.

- `--dhcp`
- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port=`

Puede especificar que los puertos sean permitidos a a través del cortafuegos usando el formato port:protocol. Por ejemplo, para permitir el acceso IMAP a través del firewall, especifique `imap:tcp`. También se puede especificar puertos numéricos explícitamente; por ejemplo, para permitir paquetes UDP en el puerto 1234, especifique `1234:udp`. Para especificar múltiples puertos, sepárelos por comas.

`install` (opcional)

Le dice al sistema que instale un sistema nuevo en vez de una actualización. Este es el modo por defecto. Para la instalación, debe especificar el tipo de instalación de una de `cdrom`, `harddrive`, `nfs`, o `url` (para instalaciones ftp o http). El comando `install` y el comando del método de instalación deben estar en líneas separadas.

`cdrom`

Instale desde la primera unidad de CD-ROM en el sistema.

`harddrive`

Instale desde un árbol de instalación de Red Hat en un disco local, el cual puede ser bien sea vfat o ext2.

- `--partition=`

  Partición a partir de la cual instalar (tal como, sdb2).

- `--dir=`

  Directorio conteniendo el directorio `RedHat` del árbol de instalación.

Por ejemplo:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

Instalar desde el servidor NFS especificado.

- `--server=`

  Servidor desde el cual instalar (hostname o IP).

- `--dir=`

  Directorio conteniendo el directorio `RedHat` del árbol de instalación.

Por ejemplo:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

Instalar desde un árbol de instalación en un servidor remoto a través de FTP o HTTP.

Por ejemplo:

```
url --url http://<server>/<dir>
```

o:

```
url --url ftp://<username>:<password>@<server>/<dir>
```

`interactive` (opcional)

Usa la información proporcionada en el archivo kickstart durante la instalación, pero permite la inspección y modificación de los valores dados. Se le presentará con cada pantalla del programa de instalación con los valores del archivo kickstart. Puede aceptar los valores haciendo click en **Siguiente** o cambiar los valores y hacer click en **Siguiente** para continuar. Vea también `autostep`.

`keyboard` (requerido)

configura el tipo de teclado del sistema. Aquí está la lista de teclados disponibles en máquinas i386, Itanium, y Alpha:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

El archivo `/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` también contiene esta lista y es parte del paquete `rhpl`.

`lang` (requerido)

Configura el idioma a utilizar durante la instalación. Por ejemplo, para configurar el idioma a English, el archivo kickstart debería contener la línea siguiente:

```
lang en_US
```

El archivo `/usr/share/redhat-config-language/locale-list` proporciona una lista de los códigos de idiomas válidos en la primera columna de cada línea y es parte del paquete `redhat-config-languages`.

`langsupport` (requerido)

Configura el o los idioma(s) a instalar en el sistema. Se pueden usar los mismos código usados con `lang` para `langsupport`.

Para instalar un idioma, especifíquelo. Por ejemplo, para instalar y usar el idioma French `fr_FR`:

```
langsupport fr_FR
```

`--default=`

Si se especifica el soporte del idioma para más de un idioma, debe especificar alguno por defecto.

Por ejemplo, para instalar English y French y usar English como el idioma por defecto:

```
langsupport --default=en_US fr_FR
```

Si usa `--default` con sólo un idioma, todos los idiomas serán instalados con el conjunto de idioma especificado al valor por defecto.

`lilo` (reemplazado por `bootloader`)

Aviso

Esta opción ha sido reemplazada por `bootloader` y sólo está disponible para compatibilidad hacia atrás. Consulte `bootloader`.

Especifique cómo el gestor de arranque debería ser instalado en el sistema. Por defecto, LILO se instala en el MBR del primer disco e instala un sistema de arranque dual si se encuentra una

partición DOS (el sistema DOS/Windows arrancará si el usuario escribe `dos` en el indicador de `LILO:`).

`--append` *<params>*

Especifica parámetros del kernel.

`--linear`

Use la opción `linear` de LILO; esto es sólo para compatibilidad hacia atrás (y linear es usada ahora por defecto).

`--nolinear`

Use la opción `nolinear` de LILO; linear es ahora usada por defecto.

`--location=`

Especifica dónde se escribe el registro de arranque de LILO. Valores válidos son: `mbr` (por defecto) o `partition` (instala el gestor de arranque en el primer sector de la partición conteniendo el kernel). Si no se especifica ninguna dirección, no se instalará LILO.

`--lba32`

Fuerza el uso del modo lba32 en vez de detección automática.

`lilocheck` (opcional)

Si está presente `lilocheck`, el programa de instalación chequea por LILO en el MBR del primer disco duro y reinicia el sistema si se encuentra — en este caso la instalación es llevada a cabo. Esto puede prevenir a kickstart de reinstalar un sistema ya instalado.

`logvol` (opcional)

Crea un volúmen lógico para Logical Volume Management (LVM) con la sintaxis:

`logvol` *mountpoint* `--vgname=`*name* `--size=`*size* `--name=`*name*

Crea la partición primero, crea el grupo de volumen lógico y luego crea el volumen lógico. Por ejemplo:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse` (requerido)

Configura el ratón para el sistema, en modos GUI y texto. Las opciones son:

`--device=`

Dispositivo de ratón está activo (tal como `--device=ttyS0`).

`--emulthree`

Si está presente, los clicks simultáneos del botón izquierdo y derecho se reconocen como el botón medio en el sistema X Window. Esta opción debería ser usada si tiene un ratón de dos botones.

Después de las opciones, el tipo de ratón puede ser especificado como uno de los siguientes:

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,
thinking, thinkingps/2, logitech, logitechcc, logibm, logimman,
```

```
logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew,
msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries,
mmhittab, sun, none
```

Esta lista también se puede encontrar en el archivo `/usr/lib/python2.2/site-packages/rhpl/mouse.py`, el cual es parte del paquete `rhpl`.

Si el comando del ratón es dado sin argumentos o es omitido, el programa de instalación intentará auto detectar el ratón. Este procedimiento funciona para la mayoría de los ratones.

`network` (opcional)

Configura la información de la red para el sistema. Si la instalación kickstart no requiere redes (en otras palabras, no es instalado sobre NFS, HTTP, o FTP), no se configurará la red para el sistema. Si la instalación no requiere redes y la información de redes no se proporciona en el archivo kickstart, el programa de instalación de Red Hat Linux asume que la instalación debería ser realizada sobre eth0 a través de dirección IP dinámica (BOOTP/DHCP) y configura el sistema instalado final a que determine su dirección IP dinámicamente. La opción `network` configura la información de red para instalaciones kickstart a través de la red así como también para el sistema instalado.

`--bootproto=`

Uno de `dhcp`, `bootp`, o `static`.

Por defecto `dhcp`. `bootp` y `dhcp` se tratán de la misma forma.

El método DHCP usa un sistema servidor DHCP para obtener su configuración de red. Como puede adivinar, el método BOOTP es similar, requiriendo un servidor BOOTP para suministrar la configuración de red. Para dirigir un sistema a que use DHCP:

```
network --bootproto=dhcp
```

Para dirigir una máquina a que use BOOTP para obtener la configuración de red, use la línea siguiente en el archivo kickstart:

```
network --bootproto=bootp
```

El método estático requiere que ingrese toda la información de red requerida en el archivo kickstart. Como su nombre implica, esta información es estática y se usará durante y después de la instalación. La línea para red estática es más compleja, pues debe incluir toda la información de la red en una línea. Debe especificar la dirección IP, máscara de red, gateway y nombre del servidor. Por ejemplo: (el \ indica que todo va en una sola línea):

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

Si usa el método estático, tenga en cuenta las siguientes dos restricciones:

- Toda la información de red estática debe ser especificada en *una* línea; no puede separar líneas usando la barra oblícua por ejemplo.
- Sólo puede especificar un nombre de servidor. Sin embargo, puede usar la sección del archivo kickstart `%post` (descrita en la Sección 7.7) para añadir más servidores si lo necesita.

`--device=`

Usado para seleccionar un dispositivo Ethernet específico para la instalación. Observe que usando `--device=` no será efectivo a menos que el archivo kickstart sea un archivo local (tal como `ks=floppy`), puesto que el programa de instalación configurará la red para encontrar el archivo kickstart. Por ejemplo:

```
network --bootproto=dhcp --device=eth0
```

`--ip=`

Dirección IP para la máquina a instalar.

`--gateway=`

Gateway por defecto como una dirección IP.

`--nameserver=`

Nombre de servidor primario, como una dirección IP.

`--nodns`

No configura un servidor DNS.

`--netmask=`

Máscara de red para el sistema instalado.

`--hostname=`

Nombre del host para el sistema instalado.

`part` o `partition` (requerido para instalaciones, ignorado para actualizaciones)

Crea una partición en el sistema.

Si hay más de una instalación de Red Hat Linux en el sistema en particiones diferentes, el programa de instalación le preguntará al usuario cúal instalación actualizar.

Aviso

Todas las particiones creadas serán formateadas como parte del proceso de instalación a menos que `--noformat` y `--onpart` sean usados.

<mntpoint>

El *<mntpoint>* es donde se montará la partición y debe ser una de las siguientes formas:

- `/`*<path>*

  Por ejemplo, `/`, `/usr`, `/home`

- `swap`

  La partición será usada como espacio swap.

  Para determinar el tamaño de la partición swap automáticamente, use la opción `--recommended`:

  ```
  swap --recommended
  ```

  El tamaño mínimo de la partición swap generada automáticamente no puede ser más pequeña que la cantidad de RAM en el sistema y no más grande que el doble de la cantidad de RAM.

- `raid.`*<id>*

  La partición será usada para RAID de software (refiérase a `raid`).

- `pv.`*<id>*

  La partición será usada por LVM (refiérase a `logvol`).

`--size=`

El tamaño mínimo de la partición en megabytes. Especifique un valor entero aquí tal como 500. No le agregue MB al número!.

`--grow`

Le indica a la partición que crezca para llenar el espacio disponible (si existe) o hasta el máximo tamaño.

`--maxsize=`

El tamaño máximo de la partición en megabytes cuando la partición es configurada a crecer. Especifique un valor entero aquí y no agregue MB al número.

`--noformat`

Le dice al programa de instalación que no formatee la partición, para usar con el comando `--onpart`.

`--onpart=` o `--usepart=`

Coloca la partición en el dispositivo *existente*. Por ejemplo:

```
partition /home --onpart=hda1
```

colocará `/home` en `/dev/hda1`, el cual debe existir.

`--ondisk=` o `--ondrive=`

Fuerza a la partición a que se cree en un disco particular. Por ejemplo, `--ondisk=sdb` colocará la partición en el segundo disco SCSI del sistema.

`--asprimary`

Fuerza la asignación automática de la partición como una partición primaria o el particionamiento fallará.

`--bytes-per-inode=`

El número especificado representa el número de bytes por inode en el sistema de archivos cuando es creado. Debe ser dado en formato decimal. Esta opción es útil para aplicaciones donde se quiere incrementar el número de inodes del sistema de archivos.

`--type=` (replaced by `fstype`)

Esta opción ya no está disponible. Use `fstype`.

`--fstype=`

Coloca el tipo de sistema de archivos para la partición. Los valores válidos son `ext2`, `ext3`, `swap`, y `vfat`.

`--start=`

Especifica el cilindro donde comienza la partición. Requiere que se especifique una unidad con `--ondisk=` o `ondrive=`. También requiere que se especifique el cilindro final con `--end=` o que el tamaño de la partición se especifique con `--size=`.

`--end=`

Especifica el cilindro final para la partición. Requiere que el cilindro de comienzo se especifique con `--start=`.

`--badblocks`

Especifica que la partición debería ser revisada por sectores dañados.

Nota

Si el particionamiento falla por alguna razón, aparecerán mensajes de diagnóstico en la consola virtual 3.

`raid` (opcional)

Ensambla un dispositivo de software RAID. Este comando es de la forma:

`raid <mntpoint> --level=<level> --device=<mddevice> <partitions*>`

`<mntpoint>`

Dirección donde el sistema de archivos RAID es montado. Si es `/`, el nivel RAID debe ser 1 a menos que esté presente una partición boot (`/boot`). Si está presente una partición boot, la partición `/boot` debe ser nivel 1 y la partición root (`/`) puede ser cualquiera de los tipos disponibles. La `<partitions*>` (lo que denota que se puede listar múltiples particiones) lista los identificadores RAID para añadir al arreglo RAID.

`--level=`

Nivel RAID a utilizar (0, 1, o 5).

`--device=`

Nombre del dispositivo RAID a utilizar (tal como md0 o md1). El rango de los dispositivos RAID va de md0 a md7 y cada uno puede que sólo se use una vez.

`--spares=`

Especifica el número de unidades extra para el arreglo RAID. Las unidades extra son usadas para reconstruir el arreglo en caso de una falla de la unidad.

`--fstype=`

Configura el tipo de sistema de archivos para el arreglo RAID. Los valores válidos son ext2, ext3, swap, y vfat.

`--noformat`

No formatear el arreglo RAID.

El ejemplo siguiente muestra cómo crear una partición RAID de nivel 1 para `/` y un RAID de nivel 5 para `/usr`, asumiendo que hay tres discos SCSI en el sistema. También crea tres particiones swap, una en cada unidad.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`reboot` (opcional)

Reinicia después que se termina la instalación (sin argumentos). Normalmente, kickstart despliega un mensaje y espera que el usuario presione una tecla antes de reiniciar.

`rootpw` (requerido)

Configura la contraseña de root al argumento *<password>*.

```
rootpw [--iscrypted] <password>
```

`--iscrypted`

Si esta presente, el argumento de la contraseña se asume que ya está encriptado.

`skipx` (opcional)

Si está presente, X no está configurado en el sistema instalado.

`text` (opcional)

Realiza la instalación kickstart en modo texto. Las instalaciones Kickstart son realizadas en modo gráfico por defecto.

`timezone` (requerido)

Configura la zona horaria del sistema a *<timezone>* lo cual puede ser cualquiera de las zonas horarias listadas por `timeconfig`.

```
timezone [--utc] <timezone>
```

`--utc`

Si está presente, el sistema asume que el reloj del hardware está configurado a UTC (Greenwich Mean).

`upgrade` (opcional)

Le dice al sistema que actualice un sistema existente en lugar de hacer una instalación fresca. Debe especificar cdrom, harddrive, nfs, o url (para ftp y http) como las ubicaciones del árbol de instalación. Consulte a `install` para más detalles.

`xconfig` (opcional)

Configura el sistema X Window. Si no se indica esta opción, el usuario necesitará configurar X manualmente durante la instalación, si X fue instalado; esta opción no se debería usar si X no está instalado en el sistema final.

`--noprobe`

No prueba el monitor.

`--card=`

Usar la tarjeta especificada; el nombre de esta tarjeta debería ser de la lista de tarjetas en `/usr/share/hwdata/Cards` del paquete `hwdata`. La lista de tarjetas también se puede encontrar en la pantalla **Configuración de X** de **Configurador de Kickstart**. Si este argumento no se proporciona, el programa de instalación probará el bus PCI para la tarjeta. Puesto que AGP es parte del bus PCI, las tarjetas AGP serán detectadas si son soportadas. El orden de verificación está determinado por el orden de escaneo de PCI de la tarjeta madre.

`--videoram=`

Especifica la cantidad de RAM de vídeo que tiene la tarjeta de vídeo.

`--monitor=`

Usar el monitor especificado: el nombre del monitor debería de provenir de la lista de monitores en `/usr/share/hwdata/MonitorsDB` del paquete `hwdata`. La lista de monitores también se puede encontrar en la pantalla **Configuración de X** del **Configurador de Kickstart**. Esto es ignorado si se proporciona `--hsync` o `--vsync`. Si no se proporciona información del monitor, el programa de instalación tratará de probarlo automáticamente.

`--hsync=`

Especifica la frecuencia de sincronización horizontal del monitor.

`--vsync=`

Especifica la frecuencia de sincronización vertical del monitor.

`--defaultdesktop=`

Especifica GNOME o KDE para el escritorio por defecto (asume que los ambientes de escritorio GNOME y/o KDE han sido instalados a través de `%packages`).

`--startxonboot`

Usar una ventana de conexión gráfica en el sistema instalado.

`--resolution=`

Especifica la resolución por defecto para el sistema X Window en el sistema instalado. Los valores válidos son 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050, 1600x1200. Asegúrese de especificar una resolución que sea compatible con la tarjeta de vídeo y monitor.

`--depth=`

Especifica la profundidad del color por defecto para el sistema X Window en el sistema instalado. Los valores válidos son 8, 16, 24 y 32. Asegúrese de especificar una profundidad de color que sea compatible con la tarjeta de vídeo y con el monitor.

`volgroup` (opcional)

Usado para crear un grupo Logical Volume Management (LVM) con la sintaxis:

```
volgroup name partition
```

Crea primero la partición, el grupo de volumen lógico y luego crea el volumen logico. Por ejemplo:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`zerombr` (opcional)

Si se especifica `zerombr` y el único argumento es `yes`, cualquier tabla de partición válida encontrada en los discos son inicializadas. Esto destruirá todos los contenidos de discos con tablas de partición inválidas. Este comando debería ser en el formato:

```
zerombr yes
```

Ningún otro formato es efectivo.

`%include`

Use el comando `%include` *`/path/to/file`* para incluir los contenidos de otro archivo en el archivo kickstart como que si los contenidos estuviesen en la ubicación del comando `%include` en el archivo kickstart.

7.5. Selección de paquetes

Use el comando `%packages` para comenzar una sección de archivo kickstart que lista los paquetes que le gustaría instalar (esto es para instalaciones únicamente, pues la selección de paquetes durante una actualización no es soportada).

Los paquetes se pueden especificar por grupo o por nombres de paquetes individuales. El programa de instalación define muchos grupos que contienen paquetes relacionados. Vea el archivo `RedHat/base/comps.xml` en el primer CD-ROM de Red Hat Linux para una lista de los grupos. Cada grupo tiene un id, valor de visibilidad de usuario, nombre, descripción y lista de paquete. En la lista de paquetes, los paquetes marcados como obligatorios son siempre instalados si el grupo es seleccionado, los paquetes marcados como predeterminados son seleccionados por defecto si el grupo es seleccionado y los paquetes marcados como opcional deben ser seleccionados específicamente aún si el grupo es seleccionado para ser instalado.

En la mayoría de los casos, sólo es necesario listar los grupos deseados y no los paquetes individuales. Note que los grupos `Core` y `Base` son siempre seleccionados por defecto, por lo tanto no es necesario especificarlos en la sección `%packages`.

Aquí hay un ejemplo de una selección de `%packages`:

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
galeon
```

Como puede ver, los grupos son especificados, uno en cada línea, comenzando con un símbolo `@`, un espacio y luego el nombre completo del grupo como en el archivo `comps.xml`. Especifique paquetes individuales sin caracteres adicionales (la línea `galeon` en el ejemplo de arriba es un paquete individual).

También puede especificar cuáles paquetes no desea instalar de la lista de paquetes predeterminados:

```
@ Games and Entertainment
-kdegames
```

Hay dos opciones disponibles para `%packages`.

`--resolvedeps`

Instala los paquetes listados y automáticamente resuelve las dependencias. Si esta opción no es especificada y hay dependencias de paquetes, la instalación automática se detendrá y le preguntará al usuario. Por ejemplo:

```
%packages --resolvedeps
```

`--ignoredeps`

Ignora las dependencias e instala los paquetes listados sin las dependencias. Por ejemplo:

```
%packages --ignoredeps
```

`--ignoremissing`[1]

Ignora los paquetes y grupos faltantes en vez de detener la instalación para preguntar si la instalación debería abortarse o continuar. Por ejemplo:

```
%packages --ignoremissing
```

7.6. Script de pre-instalación

Puede añadir comandos para ejecutar en el sistema automáticamente después de que `ks.cfg` haya sido analizado. Esta sección debe estar al final del archivo kickstart (después de los comandos) y debe comenzar con el comando `%pre`. Puede accesar la red en la sección `%pre`; sin embargo, *name service* no ha sido configurado en este punto, así que sólo funcionarán las direcciones IP.

Nota

Observe que el script de pre instalación no es ejecutado en el ambiente chroot.

`--interpreter /usr/bin/python`

Le permite especificar un lenguage de script diferente, tal como Python. Reemplace `/usr/bin/python` con el lenguage de scripting de su preferencia.

7.6.1. Ejemplo

He aquí un ejemplo de una sección `%pre`:

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
  mymedia=`cat $file/media`
  if [ $mymedia == "disk" ] ; then
      hds="$hds `basename $file`"
  fi
done

set $hds
numhd=`echo $#`

drive1=`echo $hds | cut -d' ' -f1`
drive2=`echo $hds | cut -d' ' -f2`

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
  #2 drives
  echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
```

1. Esta es una nueva opción en Red Hat Linux 9.

```
  echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
  echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
  echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
  #1 drive
  echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
  echo "part swap --recommended" >> /tmp/part-include
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

Este script determina el número de discos duros en el sistema y escribe un archivo de texto con un esquema de particionamiento diferente dependiendo de si tiene uno o dos discos. En vez de tener un conjunto de comandos en el archivo kickstart, incluye la línea:

```
%include /tmp/part-include
```

Serán usados los comandos de particionamiento seleccionados en el script.

7.7. Script de post-instalación

Tiene la opción de añadir comandos para que se ejecuten en el sistema una vez que la instalación se haya terminado. Esta sección debe estar al final del archivo kickstart y debe comenzar con el comando `%post`. Esta sección es útil para funciones tales como la instalación de software adicional y la configuración de un nombre de servidor adicional.

Nota

Si configuró la red con información IP estática, incluyendo un nombre de servidor, puede acceder a la red y resolver direcciones IP en la sección `%post`. Si configuró la red para DHCP, el archivo `/etc/resolv.conf` no ha sido completado cuando la instalación ejecute la sección `%post`. Puede acceder a la red, pero no puede resolver direcciones IP. Por lo tanto si está usando DHCP, debe especificar direcciones IP en la sección `%post`.

Nota

El script de post-instalación es ejecutado en ambiente chroot; por lo tanto, al realizar tareas tales como la copia de scripts o RPMs desde la media de instalación no funcionará.

`--nochroot`

Le permite especificar comandos que le gustaría ejecutar fuera del ambiente chroot.

El ejemplo siguiente copia el archivo `/etc/resolv.conf` al sistema de archivos que acaba de instalar.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter /usr/bin/python`

Le permite especificar un lenguage de scripting diferente, tal como Python. Reemplace `/usr/bin/python` con el lenguage de scripting de su selección.

7.7.1. Ejemplos

Activar y desactivar servicios:

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

Corra un script llamado `runme` desde una compartición NFS:

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

Añadir un usuario al sistema:

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/ ' bob
```

7.8. Colocar el archivo Kickstart disponible

Un archivo kickstart debe ser colocado en alguna de las siguientes ubicaciones:

- En un disquete de arranque
- En un CD-ROM de arranque
- En la red

Normalmente un archivo kickstart es copiado a un disquete de arranque, o se coloca disponible en la red. La solución basada en la red es la usada más comúnmente, pues la mayoría de las instalaciones kickstart tienden a ser realizadas en computadoras de red.

Demos una mirada más profunda a dónde se puede colocar el archivo kickstart.

7.8.1. Creación de un disquete de arranque Kickstart

Para realizar una instalación kickstart basada en disquete, el archivo kickstart debe ser llamado `ks.cfg` y colocarse en el directorio de nivel más alto del disquete de arranque. Consulte la sección *Creación de un disquete de arranque* en el *Manual de instalación de Red Hat Linux* para instrucciones sobre cómo crear un disco de arranque. Debido a que los discos de arranque de Red Hat Linux están en formato MS-DOS, es fácil copiar el archivo kickstart bajo Linux usando el comando `mcopy`:

```
mcopy ks.cfg a:
```

Alternativamente, puede usar Windows para copiar el archivo. También puede montar el disco de arranque MS-DOS en Red Hat Linux con el sistema de archivos vfat y usar el comando `cp` para copiar el archivo en el disquete.

7.8.2. Creación de un CD-ROM de arranque Kickstart

Para realizar una instalación basada en CD-ROM, el archivo kickstart se debe llamar `ks.cfg` y se debe ubicar en el directorio de nivel más alto en el CD-ROM de arranque. Puesto que un CD-ROM es de sólo lectura el archivo debe ser añadido al directorio usado para crear la imagen escrita al CD-ROM. Refiérase a la sección *Creación de un CD-ROM de arranque de instalación* en el *Manual de instalación de Red Hat Linux* para instrucciones sobre la creación de un CD-ROM de arranque; sin embargo, antes de hacer el archivo de imagen `file.iso`, copie el archivo kickstart `ks.cfg` al directorio `isolinux/`.

7.8.3. Colocar el archivo Kickstart disponible en la red

Las instalaciones basadas en la red usando kickstart son muy comunes porque los administradores de sistemas pueden fácilmente automatizar el proceso de instalación en muchas computadoras conectadas rápidamente y sin complicaciones. En general, la solución usada más comúnmente es para que el administrador tenga un servidor BOOTP/DHCP y un servidor NFS en la red local. El servidor BOOTP/DHCP es usado para darle al cliente su información de red, mientras que los archivos verdaderos usados durante la instalación son servidos desde el servidor NFS. A menudo, estos dos servidores se ejecutan en la misma máquina, pero no se requiere que sea así.

Para realizar una instalación kickstart basada en la red, debe tener un servidor BOOTP/DHCP en su red y este debe incluir información de configuración para la máquina en la cual está intentando instalar Red Hat Linux. El servidor BOOTP/DHCP proporcionará el cliente con su información de red así como también la ubicación del archivo kickstart.

Si un archivo kickstart es especificado por el servidor BOOTP/DHCP, el sistema cliente intentará un montaje NFS de la ruta del archivo y copiará el archivo especificado al cliente, usándolo como el archivo kickstart. Las configuraciones exactas varían dependiendo del servidor BOOTP/DHCP que utilice.

He aquí un ejemplo de una línea desde el archivo `dhcpd.conf` para el servidor DHCP distribuído con Red Hat Linux:

```
filename "/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

Observe que debería reemplazar el valor luego de `filename` con el nombre del archivo kickstart (o el directorio en el cual se encuentra el archivo kickstart) y el valor luego de `next-server` con el nombre del servidor NFS.

Si el nombre del archivo devuelto por el servidor BOOTP/DHCP termina con una barra oblicua ("/"), entonces es interpretado como una ruta. En este caso, el sistema cliente monta esa ruta usando NFS y busca por un archivo particular. El nombre del archivo que el cliente busca es:

```
<ip-addr>-kickstart
```

La sección <*ip-addr*> del nombre de archivo debería ser reemplazado con la dirección IP del cliente y anotada con puntuación decimal. Por ejemplo, el nombre de archivo para una computadora con una dirección IP 10.10.0.1 sería `10.10.0.1-kickstart`.

Note que si no especifica el nombre del servidor, el sistema cliente intentará usar el servidor que contestó la petición BOOTP/DHCP como su servidor NFS. Si no especifica una ruta o un nombre de archivo, el cliente intentará montar `/kickstart` desde el servidor BOOTP/DHCP e intentará encontrar el archivo kickstart usando el mismo nombre de archivo <*ip-addr*>`-kickstart` como se describe arriba.

7.9. Colocar el árbol de instalación disponible

La instalación kickstart necesita accesar un *árbol de instalación*. Un árbol de instalacion es una copia de los CD-ROMs binarios de Red Hat Linux con la misma estructura de directorios.

Si está llevando a cabo una instalación basada en CD, inserte el CD-ROM #1 de Red Hat Linux en el computador antes de arrancar la instalación kickstart.

Si está llevando a cabo una instalación basada en disco duro, asegúrese de que las imágenes ISO de los binarios de los CD-ROMs de Red Hat Linux están en el disco duro en el computador.

Si está realizando una instalación basada en la red (NFS, FTP, o HTTP), debe colocar el árbol de instalación disponible sobre la red. Consulte la sección *Preparación para una instalación de red* del *Manual de instalación de Red Hat Linux* para más detalles.

7.10. Inicio de una instalación Kickstart

Para comenzar una instalación kickstart, debe arrancar el sistema desde un disquete de arranque de Red Hat Linux, o un CD-ROM Red Hat Linux de arranque o desde el CD-ROM #1 de Red Hat Linux e introducir un comando de arranque especial en la línea de comandos. El programa de instalación busca un archivo kickstart si se pasa el argumento `ks` al kernel.

Disquete de arranque

Si el archivo kickstart está ubicado en un disquete de arranque como se describió en la Sección 7.8.1, arranque el sistema con el disco en la unidad e introduzca el comando siguiente en el indicador de comandos `boot:`:

```
linux ks=floppy
```

CD-ROM #1 y disquete

El comando **`linux ks=floppy`** también funciona si el archivo `ks.cfg` está localizado en un sistema de archivos vfat o ext2 en un disquete y usted arranca desde el CD-ROM #1 de Red Hat Linux.

Un método alternativo para arrancar el CD-ROM #1 de Red Hat Linux y tener el archivo kickstart en un sistema de archivos vfat o ext2 en un disquete. Para hacer esto, introduzca el comando siguiente en la línea de comandos `boot:`:

```
linux ks=hd:fd0:/ks.cfg
```

Con un disco de controladores

Si necesita usar un disco de controladores con kickstart, especifique la opción **`dd`** también. Por ejemplo, para arrancar un disquete y usar un disco de controladores, introduzca el comando siguiente en el indicador `boot:`:

```
linux ks=floppy dd
```

arranque CD-ROM

Si el archivo kickstart está en un CD-ROM de arranque como se describió en la Sección 7.8.2, inserte el CD-ROM en la máquina, arranque el sistema e introduzca el comando en `boot:` (donde `ks.cfg` es el nombre del archivo kickstart):

```
linux ks=cdrom:/ks.cfg
```

Otras opciones para arrancar una instalación kickstart son:

`ks=nfs:<server>:/<path>`

El programa de instalación buscará el archivo kickstart en el servidor NFS <*server*>, como archivo <*path*>. El programa de instalación usará DHCP para configurar la tarjeta Ethernet. Por ejemplo, si su servidor NFS es server.example.com y el archivo kickstart está en la compartición NFS `/mydir/ks.cfg`, el comando de arranque correcto será `ks=nfs:server.example.com:/mydir/ks.cfg`.

`ks=http://<server>/<path>`

El programa de instalación buscará por el archivo kickstart en el servidor HTTP <*server*>, como archivo <*path*>. El programa de instalación usará DHCP para configurar la tarjeta Ethernet. Por ejemplo, si su servidor HTTP es server.example.com y el archivo kickstart está en el directorio HTTP `/mydir/ks.cfg`, el comando correcto para arrancar será `ks=http://server.example.com/mydir/ks.cfg`.

`ks=floppy`

El programa de instalación busca por el archivo `ks.cfg` en un sistema de ficheros vfat o ext2 en el disquete en `/dev/fd0`.

`ks=floppy:/<path>`

El programa de instalación buscará por el archivo kickstart en el disquete en `/dev/fd0`, como archivo <*path*>.

`ks=hd:<device>:/<file>`

El programa de instalación montará el sistema de archivos en <*device*> (el cual debe ser vfat o ext2), y buscará por el archivo de configuración kickstart como <*file*> en ese sistema de archivos (por ejemplo, `ks=hd:sda3:/mydir/ks.cfg`).

Nota

Los dos puntos que están en segundo lugar son un cambio de sintaxis para Red Hat Linux 9.

`ks=file:/<file>`

El programa de instalación tratará de leer el archivo <*file*> desde el sistema de archivos; no se montará nada. Esto es normalmente usado si el archivo kickstart ya está en la imagen `initrd`.

`ks=cdrom:/<path>`

El programa de instalación buscará el archivo kickstart en el CD-ROM, como archivo <*path*>.

`ks`

Si se usa `ks` solo, el programa de instalación configura la tarjeta Ethernet en el sistema usando DHCP. El sistema usará "bootServer" desde la respuesta DHCP como un servidor NFS para leer el archivo kickstart (por defecto, es el mismo que el servidor DHCP). El nombre del fichero kickstart podría ser uno de los que siguen:

- Si se especifica DHCP y el archivo bootfile comienza con un `/`, el bootfile proporcionado por DHCP es buscado en el servidor NFS.
- Si se especifica DHCP y el bootfile comienza con cualquier otra cosa y luego un `/`, el bootfile proporcionado por DHCP se busca en el directorio `/kickstart` en el servidor NFS.
- Si DHCP no especifica un bootfile, entonces el programa de instalación intenta leer el archivo `/kickstart/1.2.3.4-kickstart`, donde *1.2.3.4* es la dirección IP numérica de la máquina que está siendo instalada.

`ksdevice=<device>`

El programa de instalación utiliza este dispositivo de red para conectarse a la red. Por ejemplo, para arrancar una instalación kickstart con el archivo de kickstart en un servidor NFS que está conectado al sistema a través de eth1, use el comando `ks=nfs:<server>:/<path> ksdevice=eth1` en el indicador de comandos `boot:`.

Capítulo 8.

Configurador de Kickstart

El **Configurador de Kickstart** le permite crear un archivo kickstart usando una interfaz gráfica de usuario, para que no tenga que recordar la sintaxis correcta del archivo.

Para usar el **Configurador de Kickstart**, debe estar ejecutando el sistema X Window. Para iniciar el **Configurador de Kickstart**, seleccione el **Botón de menú principal** (en el Panel) **=> Herramientas del sistema => Configurador de Kickstart**, o escriba el comando `/usr/sbin/redhat-config-kickstart`.

Mientras esté creando un archivo kickstart, puede seleccionar **Fichero => Vista Preliminar** en cualquier momento para revisar sus selecciones actuales.

8.1. Configuración básica

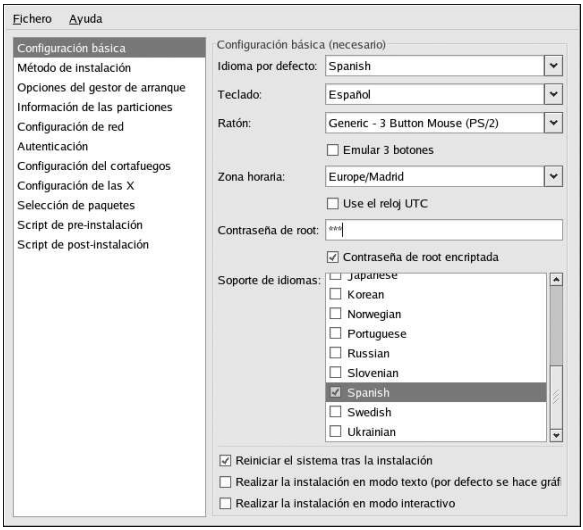

Figura 8-1. Configuración básica

Escoja el idioma que desea usar durante la instalación desde el menú **Idioma**.

Seleccione el teclado desde el menú **Teclado**.

Seleccione el ratón para el sistema desde el menú **Ratón**. Si se selecciona **No Mouse**, no se configurará ningún ratón. Si selecciona **Probe for Mouse**, el programa de instalación tratará de autodetectar el ratón. La verificación de ratón funciona para la mayoría de los ratones.

Si posee un ratón de dos botones, puede emular un ratón de tres al seleccionar **Emular 3 botones**. Si se selecciona esta opción, al hacer click de forma simultánea en los botones izquierdo y derecho, conseguirá el mismo resultado que haciendo clik en el botón de en medio.

Desde el menú **Zona horaria**, seleccione la zona horaria a usar por el sistema. Para configurar el sistema a usar UTC, seleccione **Usar el reloj UTC**.

Introduzca la contraseña root deseada para el sistema en la casilla de entrada de texto **Contraseña de root**. Si desea guardar la contraseña como una contraseña encriptada en el archivo, seleccione **Encriptar contraseña de root**. Si se selecciona esta opción, cuando se guarde el archivo, la contraseña en texto sin retocar que ha escrito será encriptada y escrita en el archivo kickstart. No teclee una contraseña que ya ha sido encriptada para encriptarla nuevamente.

Para añadir idiomas al que se ha seleccionado, verifíquelos en la lista **Soporte del idioma**. El idioma seleccionado del menú desplegable **Idioma** se usa por defecto después de la instalación; sin embargo, el idioma predeterminado se puede cambiar con la **Herramienta de configuración del idioma** (`redhat-config-language`) después de la instalación.

Si elije **Reanudar** el sistema después de la instalación, reanudará el sistema automáticamente después de que haya acabado la instalación.

Las instalaciones Kickstart se ejecutan en modo gráfico por defecto. Para sobreescribir esta predeterminación y utilizar, en su lugar, el modo texto, active la opción **Realizar instalación en modo texto**.

Puede ejecutar una instalación kickstart de un modo interactivo. Esto significa que el programa de instalación utilizará todas las opciones preconfiguradas en el archivo kickstart, pero le permitirá tener una vista preliminar de las opciones en cada pantalla antes de que pase a la siguiente. Para pasar a la siguiente pantalla, haga click en el botón **Siguiente** después de haber dado el visto bueno a la configuración. Si no le satisfacen las opciones preconfiguradas, puede cambiarlas antes de continuar con la instalación. Si prefiere este tipo de instalación, active **Realizar la instalación en modo interactivo**.

8.2. Método de instalación

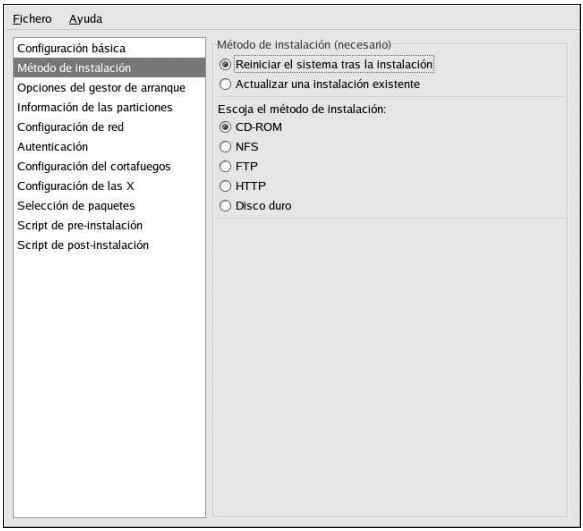

Figura 8-2. Método de instalación

La pantalla de **Método de instalación** le permite seleccionar si se realizará una nueva instalación o una actualización. Si selecciona una actualización, las opciones **Información de la partición** y **Selección de paquetes** se mostrarán. Estas no son soportadas para actualizaciones kickstart.

Escoja también el tipo de instalación kickstart a ejecutar desde esta página. Escoja entre las siguientes opciones:

- **CD-ROM** — Seleccione esta opción para instalar Red Hat Linux desde los CD-ROMs de Red Hat Linux.
- **NFS** — Escoja esta opción si desea instalar Red Hat Linux desde un directorio compartido NFS. Aparecerán dos casillas de entrada de texto para el servidor NFS y el directorio NFS. Introduzca el nombre de dominio calificado o la dirección IP del servidor NFS. Introduzca el nombre del directorio NFS que contiene el directorio `RedHat` en el árbol de instalación. Por ejemplo, si su servidor NFS contiene el directorio `/mirrors/redhat/i386/RedHat/`, introduzca `/mirrors/redhat/i386/` para el directorio NFS.
- **FTP** — Escoja esta opción si desea instalar Red Hat Linux desde un servidor FTP. Aparecerán dos casillas de entrada de texto para el servidor FTP y el directorio FTP. Para el directorio FTP, introduzca el nombre del directorio FTP que contiene el directorio `RedHat`. Por ejemplo, si su servidor FTP contiene el directorio `/mirrors/redhat/i386/RedHat/`, introduzca `/mirrors/redhat/i386/` para el directorio FTP. Si el servidor FTP requiere un nombre de usuario y contraseña, especifíquelos también.
- **HTTP** — Escoja esta opción si desea instalar Red Hat Linux desde un servidor HTTP. Aparecerán dos casillas de entrada de texto para el servidor HTTP y el directorio HTTP. Introduzca el nombre de dominio completamente calificado o la dirección IP del servidor HTTP. Para el directorio HTTP, introduzca el nombre del directorio HTTP que contiene el directorio `RedHat`. Por ejemplo, si su servidor HTTP contiene el directorio `/mirrors/redhat/i386/RedHat/`, introduzca `/mirrors/redhat/i386/` para el directorio HTTP.
- **Disco duro** — Escoja esta opción si desea instalar Red Hat Linux desde un disco duro. Aparecerán dos casillas de entrada de texto para la partición del disco duro y el directorio del disco duro. Las instalaciones del disco duro requieren el uso de imágenes ISO (o CD-ROM). Asegúrese de verificar que las imágenes ISO están intactas antes de que inicie la instalación. Para verificarlas, utilice un programa `md5sum` así como también la opción de arranque `linux mediacheck` como se discutió en el *Manual de instalación de Red Hat Linux*. Introduzca la partición del disco duro que contiene las imágenes ISO (por ejemplo, `/dev/hda1`) en la casilla de texto **Partición de disco duro**. Introduzca el directorio que contiene las imágenes ISO en la casilla de texto **Directorio de disco duro**.

8.3. Opciones del gestor de arranque

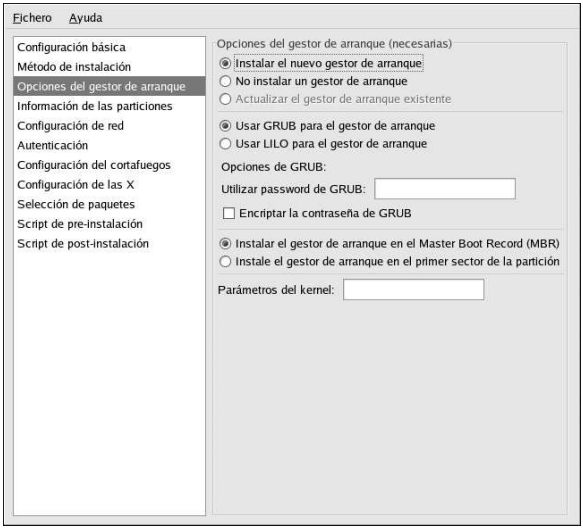

Figura 8-3. Opciones del gestor de arranque

Tiene la opción de instalar GRUB o LILO como un gestor de arranque. Si no desea instalar un gestor de arranque, active el botón **No instalar un gestor de arranque**. Si escoge no instalar un gestor de arranque, asegúrese de que crea un disco de arranque o de que tiene otro modo de arrancar (como por ejemplo un gestor de arranque proporcionado por terceros) su sistema Red Hat Linux.

Si escoge instalar un gestor de arranque, debe escoger qué gestor de arranque instalar (GRUB o LILO) y donde instalarlo (en el Master Boot Record o en el primer sector de la partición `/boot`. Instale el gestor de arranque en el MBR si desea utilizarlo como un gestor de arranque. Si está utilizando un gestor de arranque diferente, instale LILO o GRUB en el primer sector de la partición `/boot` y configure el otro gestor de arranque para arrancar Red Hat Linux.

Si necesita pasar cualquier parámetro especial al kernel que se tenga que utilizar cuando el sistema arranque, introdúzcalos en el campo del texto **Parámetros del Kernel**. Por ejemplo, si tiene una unidad de CD-ROM IDE de escritura, puede indicarle al kernel que use el controlador de emulación SCSI que deberá cargar antes de usar `cdrecord` escribiendo **`hdd=ide-scsi`** como el parámetro kernel (donde **`hdd`** es el dispositivo CD-ROM).

Si escoge GRUB como el gestor de arranque, puede protegerlo con una contraseña al configurar la contraseña GRUB. Introduzca una contraseña en el área de entrada del texto **Utilizar contraseña de GRUB**. Si desea salvar la contraseña como contraseña encriptada, seleccione el botón **Encriptar contraseña de GRUB**. Cuando se salva el archivo, la contraseña en texto plano se encriptará y se escribirá en el archivo kickstart. No escriba contraseñas que ya han sido encriptadas ni las seleccione para ello.

Si escoge LILO como el gestor de arranque, escoja si desea utilizar el modo linear y si desea forzar el uso del modo lba32.

Si seleccionó **Actualizar una instalación existente** en la página de **Método de instalación**, seleccione **Actualizar el gestor de arranque existente** para actualizar la configuración del gestor de arranque, mientras se mantienen las entradas viejas.

8.4. Información de las particiones

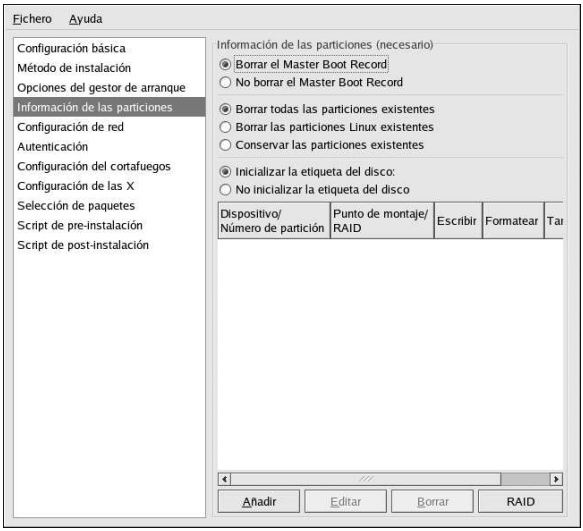

Figura 8-4. Información de las particiones

Seleccione si desea o no limpiar el Master Boot Record (MBR). Puede también decidir si eliminar todas las particiones existentes, si eliminar todas las particiones Linux o si conservar las particiones existentes.

Puede inicializar la etiqueta del disco con la arquitectura predeterminada del sistema (por ejemplo, `msdos` para x86 y `gpt` para Itanium). Seleccione **Inicializar la etiqueta del disco** si está realizando la instalación en un disco duro nuevo.

8.4.1. Creación de particiones

Para crear una partición, haga click en el botón **Añadir**. Aparecerá la ventana **Opciones de la partición** como se muestra en la Figura 8-5. Seleccione el punto de montaje, tipo de sistema de archivos y tamaño de la partición para la nueva partición. Opcionalmente, puede seleccionar desde lo siguiente:

- Opciones de tamaño adicional — Escoger hacer la partición de un tamaño fijo, hasta el tamaño que usted elija o rellenar el espacio restante en el disco duro. Si seleccionó swap como tipo de sistema de archivos, puede seleccionar que el programa de instalación cree una partición swap con el tamaño recomendado en vez de especificar el tamaño.
- Hacer que la partición se cree como partición primaria.
- Crear la partición en un disco duro determinado. Por ejemplo, para hacer una partición en el primer disco duro IDE (`/dev/hda1`), especifique **`hda1`** como controlador. No incluya `/dev` en el nombre del controlador.
- Usar una partición ya existente. Por ejemplo, para crear una partición en el primer disco duro IDE (`/dev/hda1`), especifique **`hda1`** como nombre de la partición. No incluya `/dev` en el nombre de la partición.

- Formatear la partición como el tipo de sistema de archivos escogido.

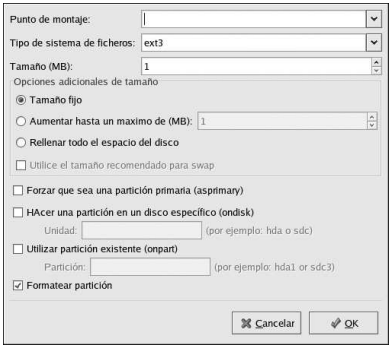

Figura 8-5. Creación de particiones

Para modificar una partición ya existente, seleccione la partición desde la lista y haga click en el botón **Editar**. Aparecerá la misma ventana **Opciones de la partición** que se muestra cuando se añade como se muestra en la Figura 8-5, excepto que refleja los valores para la partición seleccionada. Modifique las opciones de la partición y haga click en **OK**.

Para borrar una partición ya existente, seleccione la partición de la lista y haga click en el botón **Borrar**.

8.4.1.1. Creación de las particiones RAID

Consulte el Capítulo 3 para conocer mejor RAID y los distintos niveles. RAID 0, 1 y 5 se pueden configurar.

Para crear una partición RAID, siga los pasos siguientes:

1. Haga click en **RAID**.
2. Seleccione **Crear una partición RAID**.
3. Configure las particiones descritas anteriormente, excepto que seleccione **Software RAID** como el tipo de sistema de archivo. También debe especificar un disco duro en el cual hacer la partición o especificar una partición existente a utilizar.

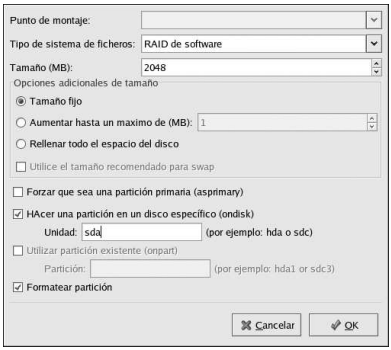

Figura 8-6. Creación de una partición RAID

Repita estos pasos hasta crear tantas particiones RAID como necesite. Todas las particiones no tienen porqué ser RAID.

Después de haber creado las particiones necesarias para el dispositivo RAID, siga los siguientes pasos:

1. Haga click en **RAID**.
2. Seleccione **Crear un dispositivo RAID**.
3. Seleccione un punto de montaje, tipo de sistema de archivos, nombre de dispositivo RAID, nivel RAID, miembros RAID, número de repuestos para el dispositivo RAID de software y si se debe formatear el dispositivo RAID.

Figura 8-7. Creación del dispositivo RAID

4. Haga click en **OK** para añadir el dispositivo a la red.

8.5. Configuración de red

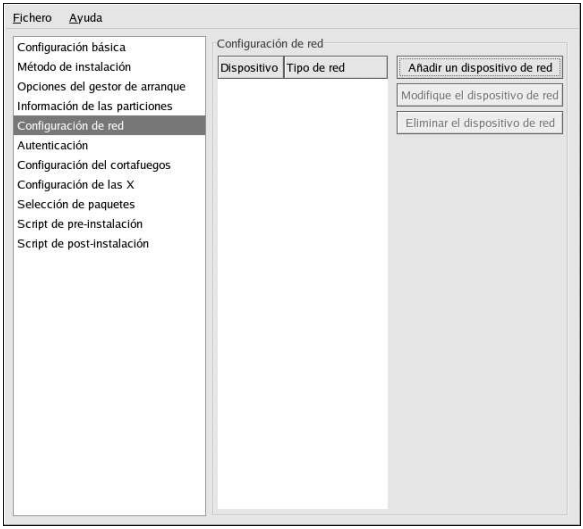

Figura 8-8. Configuración de red

Si el sistema a ser instalado a través de kickstart no tiene una tarjeta Ethernet, no configure una en la página **Configuración de red**.

Sólo se requiere el servicio de red si selecciona un método de instalación basado en red (NFS, FTP, o HTTP). El servicio de red siempre se puede configurar después de la instalación con la **Herramienta de administración de redes** (`redhat-config-network`). Consulte el Capítulo 12 para más detalles.

Por cada tarjeta Ethernet en el sistema, haga click en **Añadir dispositivo de red** y seleccione el dispositivo de red y el tipo de red del dispositivo. Seleccione **eth0** como el dispositivo de red para la primera tarjeta, seleccione **eth1** para la segunda tarjeta Ethernet y así sucesivamente.

8.6. Autenticación

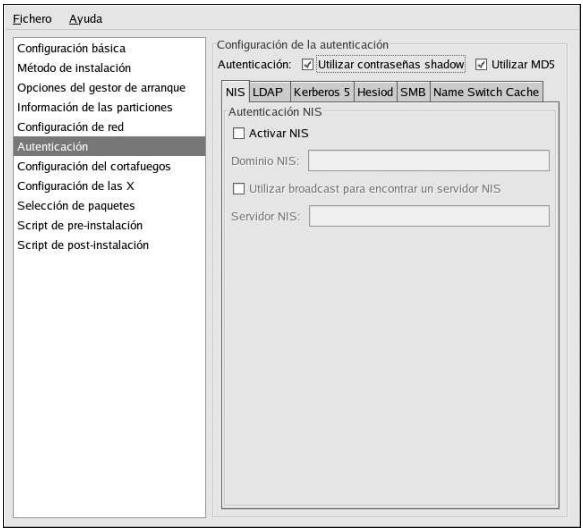

Figura 8-9. Autenticación

En la sección **Autenticación**, seleccione si quiere usar contraseñas shadow y encriptación md5 para contraseñas de usuario. Estas opciones están recomendadas por defecto.

Las opciones de **Configuración de la autenticación** le permiten configurar los siguientes métodos de autenticación:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

Estos métodos no están activados por defecto. Para activar uno o más de estos métodos, haga click en la pestaña apropiada luego click en la casilla de verificación al lado de **Activar**, e introduzca la información correspondiente para el método de autenticación.

8.7. Configuración del cortafuegos

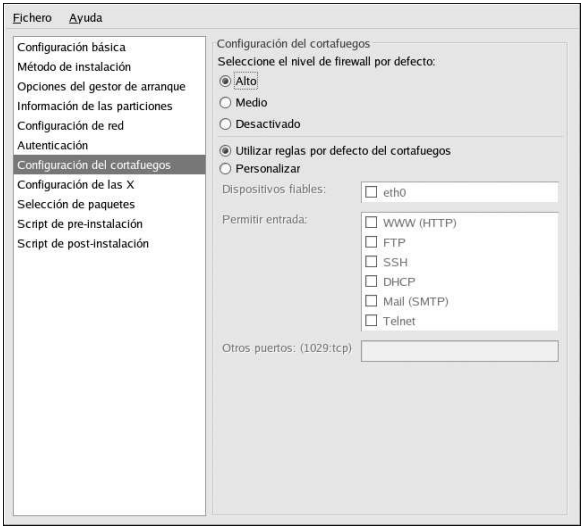

Figura 8-10. Configuración del cortafuegos

La pantalla **Configuración del cortafuegos** es idéntica a la pantalla del programa de instalación Red Hat Linux y de la **Herramienta de configuración de nivel de seguridad**, proporcionando la misma funcionalidad. Escoja entre los niveles de seguridad **Alto**, **Medio** y **Desactivado**. Remítase a la Sección 13.1 para obtener información más detallada sobre los niveles de seguridad.

8.8. Configuración de las X

Si está instalando el sistema X Window, puede configurarlo durante la instalación de kickstart marcando la opción **Configurar el sistema X Window** en la ventana **Configuración de X** como se muestra en la Figura 8-11. Si esta opción no es seleccionada, las opciones de la configuración de X serán inhabilitadas y la opción `skipx` será escrita al archivo kickstart.

8.8.1. General

El primer paso para la configuración de X es seleccionar la profundidad de color y la resolución. Selecciónelo desde sus respectivos menús desplegables. Asegúrese de especificar el color y resolución compatible con la tarjeta de vídeo y monitor del sistema.

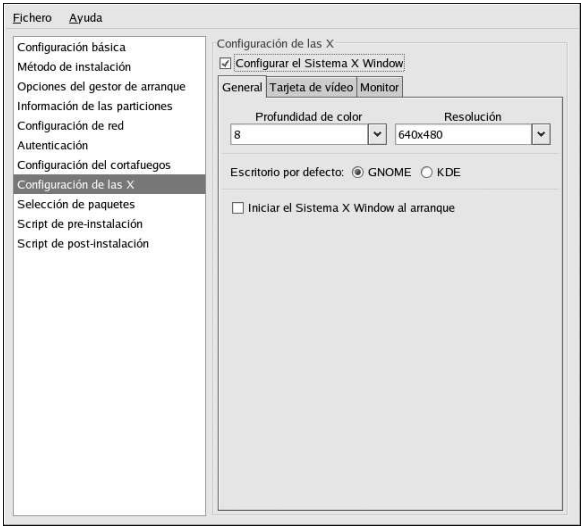

Figura 8-11. Configuración de X - General

Si está instalando los escritorios GNOME y KDE, es necesario que escoja qué escritorio desea por defecto. Si tan sólo instala un escritorio, asegúrese de escogerlo. Una vez que el sistema sea instalado, los usuarios podrán escoger qué escritorio desean tener por defecto. Para más información sobre GNOME y KDE, remítase al *Manual de instalación de Red Hat Linux* y al *Manual del principiante de Red Hat Linux*.

A continuación, escoja si desea iniciar o no el sistema X Window cuando el sistema arranca. Esta opción iniciará el sistema a un nivel de ejecución 5 con la pantalla gráfica de login. Una vez que el sistema se haya instalado, esto se puede cambiar modificando el archivo de configuración `/etc/inittab`.

8.8.2. Tarjeta de vídeo

Probar la tarjeta de vídeo es seleccionado por defecto. Acepte este opción para que el programa de instalación verifique la tarjeta de vídeo durante la instalación. La verificación funciona para la mayoría de las tarjetas de vídeo. Si se selecciona esta opción y el programa de instalación no puede probar su tarjeta de vídeo, el programa de instalación se detendrá en la pantalla de configuración de la tarjeta de vídeo. Para continuar el proceso de instalación, seleccione su tarjeta de vídeo desde la lista y haga click en **Siguiente**.

Alternativamente, puede seleccionar la tarjeta de vídeo desde la lista en la pestaña **Tarjeta de vídeo** como se muestra en la Figura 8-12. Especifique la cantidad de RAM para el vídeo que tiene la tarjeta desde el menú desplegable **RAM de la tarjeta de vídeo**. Estos valores son usados por el programa de instalación para configurar el sistema X Window.

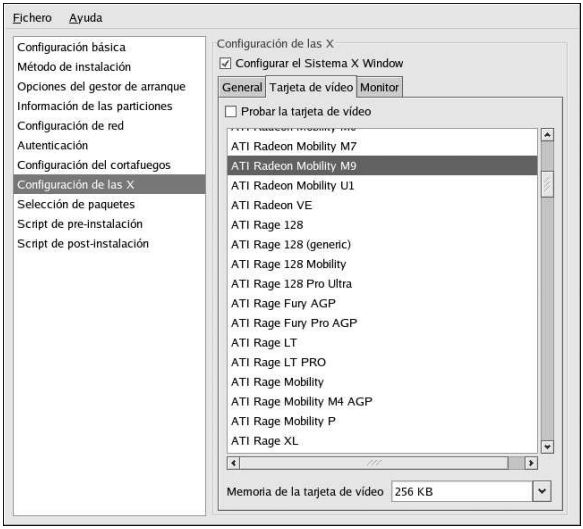

Figura 8-12. Configuración- Tarjeta de vídeo

8.8.3. Monitor

Después de configurar la tarjeta de vídeo, haga click en la pestaña **Monitor** como se muestra en la Figura 8-13.

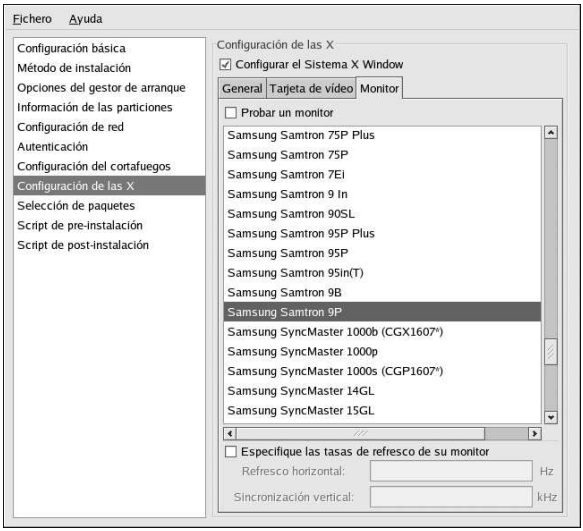

Figura 8-13. Configuración de X - Monitor

La opción **Probar un monitor** aparece seleccionada por defecto. Si desea que el programa de instalación busque el monitor durante la instalación acepte esta opción predeterminada. En general, este proceso tiene éxito pero si el programa de instalación no encuentra el monitor, el programa de instalación se detendrá en la pantalla de la configuración del monitor. Para continuar el proceso de instalación, seleccione su monitor de la lista y haga click en **Siguiente**.

Alternativamente puede seleccionar su monitor desde la lista. También puede especificar los rangos de sincronización horizontal y vertical en vez de especificar un monitor al pulsar la opción **Especifique hysnc y vsync en vez de monitor**. Esta opción es útil si el monitor para el sistema no aparece listado. Observe que cuando esta opción está activada, la lista de monitores está desactivada.

8.9. Selección de paquetes

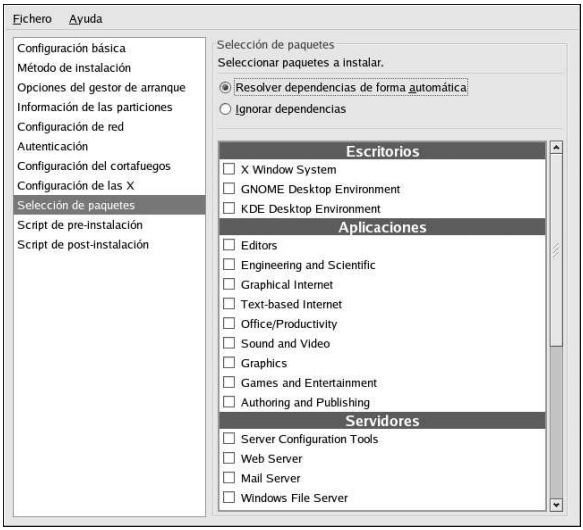

Figura 8-14. Selección de paquetes

La página **Selección de paquetes** le permite escoger qué categoría de paquetes instalar.

También hay opciones disponibles para resolver e ignorar dependencias de paquetes automáticamente.

Actualmente, el **Configurador de Kickstart** no permite que usted seleccione paquetes individuales. Para instalar paquetes individuales, modifique la sección `%packages` del archivo kickstart después que lo haya guardado. Consulte la Sección 7.5 para más detalles.

8.10. Script de pre-instalación

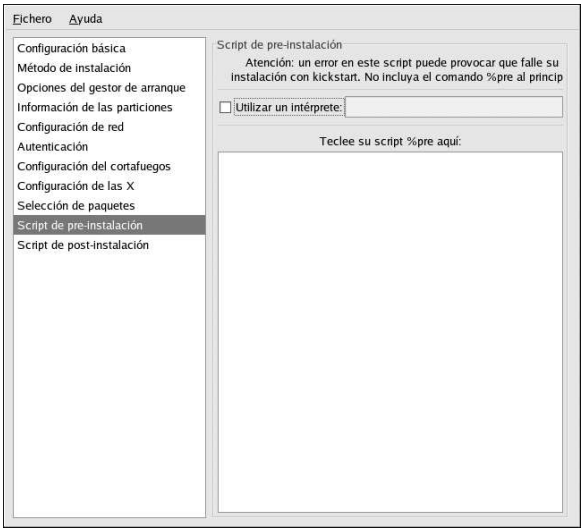

Figura 8-15. Script de pre-instalación

Puede añadir comandos para ejecutar el sistema inmediatamente después de que el archivo kickstart haya sido analizado y antes de que empiece la instalación. Si ha configurado la red en el archivo kickstart, la red se habilita antes de que se procese esta sección. Si desea incluir un script de pre-instalación, escriba en la siguiente zona.

Si desea especificar el lenguaje de scripting para ejecutar el script, haga click en **Usar un intérprete** e introducirlo en el espacio de texto al lado de dicho botón. Por ejemplo, **`/usr/bin/python2.2`** se puede especificar para el script Python. Esta opción equivale a usar `%pre --interpreter /usr/bin/python2.2` en el archivo kickstart.

Atención

No incluya el comando `%pre`. Se incluirá directamente.

8.11. Script de post-instalación

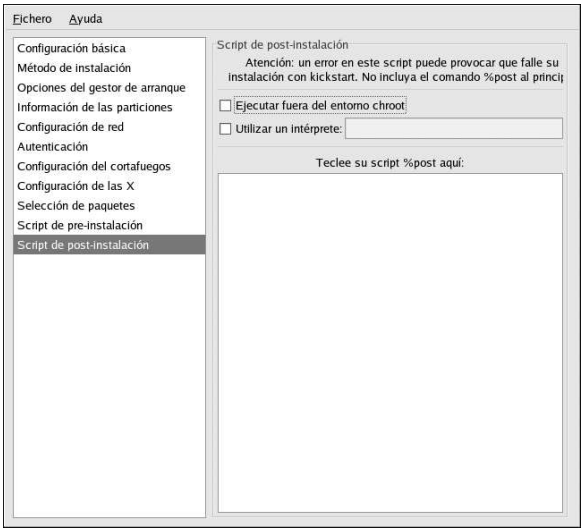

Figura 8-16. Script de post-instalación

Puede añadir comandos para ejecutar en el sistema después de que la instalación se haya completado. Si ha configurado adecuadamente la red en el archivo kickstart, la red será habilitada. Si desea incluir un script de post-instalación, tecléelo en la zona de texto.


Atención

No incluya el comando `%post`. Se añadirá directamente.

Por ejemplo, para cambiar el mensaje del día para el sistema que acaba de instalar, añada el siguiente comando para ver la sección `%post`:

```
echo "Hackers will be punished!" > /etc/motd
```


Sugerencia

Se pueden encontrar más ejemplos en la Sección 7.7.1.

8.11.1. Entorno Chroot

Si desea un script de post-instalación para ejecutar fuera del entorno chroot, haga click en el botón de verificación cercano a esta opción al inicio de la página **Post-Instalación**. Esto es el equivalente a utilizar la opción `--nochroot` en la sección `%post`.

Si quiere hacer cambios en el sistema que acaba de instalar en la sección de post-instalación fuera del entorno chroot, es necesario que añada el nombre del directorio a `/mnt/sysimage/`.

Por ejemplo, si pulsa el botón **Ejecutar fuera del chroot**, en el ejemplo anterior debería cambiarse de la siguiente manera:

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. Uso de un intérprete

Si desea especificar un lenguaje de script para usar en la ejecución de su script, haga click en el botón **Utilizar un intérprete** e introduzca el intérprete en la casilla de texto cercana al botón. Por ejemplo, **`/usr/bin/python2.2`** puede especificarse para un script de Python. Esta opción corresponde a usar `%post --interpreter` *`/usr/bin/python2.2`* en su archivo kickstart.

8.12. Guardar archivo

Después de que haya finalizado de escoger las opciones de kickstart, haga click en el botón **Fichero => Vista preliminar** para ver los contenidos de su archivo kickstart.

Figura 8-17. Confirmar las opciones

Si está satisfecho de sus elecciones, haga click en el botón **Guardar archivo** en la ventana de diálogo. Para guardar el archivo sin visualizarlo antes, seleccione **Fichero => Guardar fichero** o presione [Ctrl]-[S]. Aparecerá una ventana de diálogo. Seleccione dónde guardar el archivo.

Tras haber guardado el archivo, remítase a la Sección 7.10 para la información sobre el modo de iniciar la instalación de kickstart.

redhat.

Capítulo 9.

Recuperación básica del sistema

Cuando las cosas salen mal, siempre hay formas de corregir los problemas. Sin embargo, estos métodos requieren que usted comprenda muy bien cómo funciona el sistema. Este capítulo describe como iniciar el sistema en modo de rescate, modo de usuario único y modo de emergencia, donde podrá utilizar todos sus conocimientos para reparar el sistema.

9.1. Problemas comunes

Puede que necesite arrancar en uno de los modos de recuperación por alguna de las razones siguientes:

- No puede arrancar normalmente en Red Hat Linux (nivel de ejecución 3 o 5).
- Está teniendo problemas con el hardware o con el software, y quiere recuperar algunos archivos importantes y sacarlos del disco duro de su sistema.
- Se le olvidó su contraseña de root.

9.1.1. No puede arrancar en Red Hat Linux

Este tipo de problemas suele estar relacionado con la instalación de otro sistema operativo después de haber instalado Red Hat Linux. Algunos sistemas operativos asumen que no existe ningún otro sistema operativo en su ordenador y sobreescriben el Master Boot Record (MBR) que en un principio contenía los gestores de arranque LILO o GRUB. Si se sobreescribe el gestor de arranque de esta manera, no podrá iniciar Red Hat Linux a no ser que entre en modo de rescate y reconfigure el gestor de arranque.

Otro problema habitual se produce si utiliza una herramienta de particionamiento para redimensionar una partición o crear una nueva partición desde el espacio libre tras la instalación y se cambia el orden de sus particiones. Si el número de su partición `/` cambia, el gestor de arranque no será capaz de encontrarlo y montar la partición. Para solventar este problema, arranque en modo de rescate y modifique `/boot/grub/grub.conf` si está utilizando GRUB o `/etc/lilo.conf` si está utilizando LILO. Usted *debe* también correr el comando `/sbin/lilo` cada vez que modifique el archivo de configuración de LILO.

9.1.2. Problemas de Hardware/Software

Esta categoría contiene una amplia variedad de situaciones diferentes. Dos ejemplos serían un disco duro que se ha caído y ha dejado de funcionar, o que se especifique un kernel o dispositivo root inválido en el archivo de configuración del gestor de arranque. Si cualquiera de estos casos ocurre, puede ser que no pueda reiniciar en Red Hat Linux. Sin embargo, si arranca en alguno de estos modos de recuperación, quizás podrá resolver el problema o al menos obtener copias de los archivos más importantes.

9.1.3. Contraseña de Root

Qué puede hacer si se le olvida la contraseña de root? Para reconfigurarla a una contraseña diferente, debe arrancar en modo de rescate o en modo monousuario y usar el comando `passwd` para reestablecer una contraseña para root.

9.2. Arrancar en modo de rescate

El modo de rescate proporciona la habilidad de arrancar una pequeña parte del ambiente Red Hat Linux desde un disquete, CD-ROM, o algún otro método de arranque en vez del disco duro.

Tal y como su nombre indica, el modo de rescate se proporciona para que usted rescate algo. En el modo de operación normal, su sistema Red Hat Linux utiliza los archivos que se encuentran en el disco duro de su sistema para realizar todo — ejecutar programas, almacenar sus archivos, y mucho más.

Sin embargo, hay veces en las que no logrará que Red Hat Linux se ejecute lo suficiente para poder acceder a los archivos de su disco duro. Usando el modo de rescate, puede acceder a los archivos almacenados en el disco duro de su sistema, aún cuando quizás no pueda ejecutar Red Hat Linux desde ese disco duro.

Para arrancar su sistema en modo de rescate, debe ser capaz de arrancar el sistema usando alguno de los métodos siguientes:

- Arrancar el sistema desde un disquete de instalación hecho a partir de una imagen `bootdisk.img`. [1]
- Arrancar el sistema desde un CD-ROM de instalación. [2]
- Arrancar el sistema desde el CD-ROM #1 de Red Hat Linux.

Una vez que haya arrancado en alguno de los métodos descritos, introduzca el comando siguiente en el intérprete de comandos:

```
linux rescue
```

Se le pedirá que conteste algunas preguntas básicas, incluyendo cúal idioma utilizar. También se le pedirá que seleccione dónde está ubicada una imagen válida de rescate. Seleccione desde **CD-ROM local**, **Disco duro**, **imagen NFS**, **FTP**, o **HTTP**. La ubicación seleccionada debe contener un árbol de instalación válido y el árbol de instalación debe ser de la misma versión de Red Hat Linux que el CD-ROM #1 de Red Hat Linux desde el cual arrancó. Si usó un CD-ROM o disquete de arranque para iniciar el modo de rescate, el árbol de instalación debe ser desde el mismo árbol desde el cual fue creada la media. Para más información sobre como configurar un árbol de instalación en un disco duro, servidor NFS, servidor FTP, o servidor HTTP, consulte el *Manual de instalación de Red Hat Linux*.

Si seleccionó una imagen que no requiere una conexión de red, se le preguntará si desea establecer una conexión de red. Una conexión de red es muy útil si necesita respaldar archivos a una computadora diferente o instalar algunos paquetes desde una ubicación de red compartida, por ejemplo.

Verá el siguiente mensaje:

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage.  You can then make any changes required to your
system.  If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

1. Para crear un disquete de instalación, introduzca un disco en blanco y use el archivo `images/bootdisk.img` en el CD-ROM #1 de Red Hat Linux con el comando `dd if=bootdisk.img of=/dev/fd0`.
2. Para crear un CD-ROM de instalación, consulte las instrucciones en el *Manual de instalación de Red Hat Linux*.

Si selecciona **Continuar**, intentará montar su sistema de archivos bajo el directorio `/mnt/sysimage`. Si no consigue montar una partición, le será notificado. Si selecciona **Sólo lectura**, intentará montar el sistema de archivos bajo el directorio `/mnt/sysimage`, pero en modo de solamente lectura. Si selecciona **Saltar**, su sistema de archivos no será montado. Escoja **Saltar** si piensa que su sistema de archivos está corrupto.

Una vez que tenga su sistema en modo de rescate, aparece un intérprete de comandos en VC (consola virtual) 1 y VC 2 (utilice la combinación de teclas [Ctrl]-[Alt]-[F1] para acceder a VC 1 y la combinación [Ctrl]-[Alt]-[F2] para acceder a VC 2):

```
-/bin/sh-2.05b#
```

Si ha seleccionado **Continuar** para montar sus particiones automáticamente y éstas se han montado con éxito, está en modo monousuario.

Aún si su sistema de archivos está montado, la partición root predeterminada en modo de rescate es una partición root temporal, no la partición root del sistema de archivos usado durante el modo de usuario normal (nivel de ejecución 3 o 5). Si seleccionó montar su sistema de archivos y se montó exitósamente, puede cambiar la partición del ambiente de modo de rescate a la partición root de su sistema de archivos ejecutando el comando siguiente:

```
chroot /mnt/sysimage
```

Esto es útil si necesita ejecutar comandos tales como `rpm` que requieren que su partición root esté montada como `/`. Para salir del ambiente chroot, escriba `exit`, y volverá al intérprete de comandos.

Si seleccionó **Saltar**, todavía puede tratar de montar una partición manualmente dentro del modo de rescate creando un directorio tal como */foo*, y escribiendo el comando siguiente:

```
mount -t ext3 /dev/hda5
/foo
```

En el comando anterior, */foo* es un directorio que usted ha creado y */dev/hda5* es la partición que usted desea montar. Si la partición es del tipo `ext2`, reemplace `ext3` con `ext2`.

Si no conoce los nombres de las particiones, utilice el siguiente comando para listarlas:

```
fdisk -l
```

Desde el intérprete de comandos, puede ejecutar muchos comandos útiles tales como

- `list-harddrives` para listar los discos duros del sistema
- `ssh`,`scp`, y `ping` si la red está iniciada
- `dump` y `restore` para usuarios con unidades de cinta
- `parted` y `fdisk` para administrar particiones
- `rpm` para instalar o actualizar software
- `joe` para modificar archivos de configuración (Si intenta iniciar otros editores populares tales como `emacs`, `pico`, o `vi`, el editor `joe` se arrancará.)

9.3. Arrancar en modo monousuario

Una de las ventajas del modo monousuario es que no necesita un disquete o CD-ROM de arranque; sin embargo, no le dá la opción de montar sistemas de archivos como sólo lectura o de no montar ninguno.

En el modo monousuario, su computador arranca en el nivel de ejecución 1. Se montan sus sistemas de archivos locales, pero no se activa la red. Tiene una shell utilizable para hacer el mantenimiento del sistema. A diferencia del modo de rescate, el modo monousuario automáticamente intenta montar su sistema de archivos; *no utilice* el modo monousuario si su sistema de archivos no se pueda montar exitósamente. No puede usar el nivel de ejecución 1 si la configuración de su sistema está corrupta.

Si su sistema arranca, pero no le permite conectarse cuando ha terminado de arrancar, inténtelo con el modo monousuario.

Si está utilizando GRUB, siga los siguientes pasos para arrancar en modo monousuario:

1. Si ha configurado una contraseña GRUB, teclee `p` e introduzca la contraseña.
2. Seleccione **Red Hat Linux** con la versión del kernel que desee arrancar y escriba `e` para editar. Se le presentará una lista de items en el archivo de configuración para el título que haya seleccionado.
3. Seleccione la línea que inicia con `kernel` y teclee `e` para modificar la línea.
4. Vaya al final de la línea y teclee **`single`** como una palabra por separado (pulse [Barra espaciadora] y teclee **`single`**). Pulse [Intro] para salir del modo modificar.
5. De vuelta en la pantalla de GRUB, escriba `b` para arrancar en el modo monousuario.

Si está usando LILO, en la línea de comandos de LILO (si está usando el LILO gráfico, debe presionar [Ctrl]-[x] para salir de la pantalla gráfica y vaya a la línea de comandos `boot:` prompt) escriba:

```
linux single
```

9.4. Arranque en modo de emergencia

En el modo de emergencia, usted está arrancando en el ambiente más mínimo posible. El sistema de archivos raíz será montado como de sólo lectura y casi nada estará configurado. La mayor ventaja del modo de emergencia respecto al modo monousuario es que los archivos `init` no son cargados. Si `init` está corrupto o no funciona, puede montar el sistema de archivos para recuperar los datos que podrían haberse perdido durante la reinstalación.

Para arrancar en modo de emergencia, use el mismo método descrito para el modo monousuario en Sección 9.3 con una excepción, reemplace la palabra **`single`** con la palabra **`emergency`**.

Capítulo 10.

Configuración de Software RAID

Lea primero el Capítulo 3 para ver las diferencias entre RAID por hardware y RAID por software y las diferencias entre RAID 0, 1 y 5.

El Software RAID puede configurarse durante la instalación gráfica de Red Hat Linux o durante una instalación de inicio rápido (kickstart). Este capítulo discute como configurar el software RAID durante la instalación, usando la interfaz **Disk Druid**.

Antes de poder crear un dispositivo RAID, lo primero es crear las particiones RAID, usando las siguientes instrucciones paso a paso:

1. En la pantalla **Configuración de la partición del disco**, seleccione **Partición manual con Disk Druid**.
2. En **Disk Druid**, elija **Nuevo** para crear una nueva partición.
3. No le será posible introducir un punto de montaje (deberá poder hacer esto una vez que haya creado el dispositivo RAID).
4. Seleccione **software RAID** desde el menú **Tipo de sistema de archivos** como se muestra en la Figura 10-1.

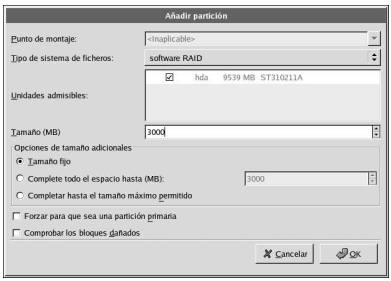

Figura 10-1. Creación de una nueva partición RAID

5. Para **Unidades admisibles**, seleccione el(los) disco(s) donde quiere crear RAID. Si tiene varios discos, todos los discos podrán ser seleccionados desde aquí y deberá anular la selección de los discos que *no* tengan un arreglo RAID.
6. Introduzca el tamaño que desea para la partición.
7. Seleccione **Tamaño fijo** para hacer la partición de un tamaño especificado, seleccione **Complete todo el espacio hasta (MB)** e introduzca un tamaño en MBs para dar alcance para el tamaño de la partición, o seleccione **Completar hasta el tamaño máximo permitido** para hacerlo crecer hasta ocupar todo el tamaño disponible en el disco duro. Si hace crecer a más de una partición, éstas compartirán el espacio libre disponible en el disco.
8. Seleccione **Forzar para que sea una partición primaria** si desea que la partición sea una partición primaria.
9. Seleccione **Comprobar los bloques dañados** si desea que el programa de instalación compruebe los bloques erróneos en el disco duro antes de formatearlo.
10. Haga click en **OK** para volver a la pantalla principal.

Repita estos pasos para crear tantas particiones como necesita para su configuración RAID. Tenga en cuenta que no todas las particiones tienen porqué ser RAID. Por ejemplo, puede configurar tan sólo la partición `/home` como un dispositivo RAID por software.

Una vez que haya creado todas sus particiones como particiones **software RAID**, siga los pasos siguientes:

1. Seleccione el botón **RAID** en la pantalla principal de particionamiento **Disk Druid** (vea la Figura 10-3).
2. A continuación, aparecerá la Figura 10-2 donde puede crear un dispositivo RAID.

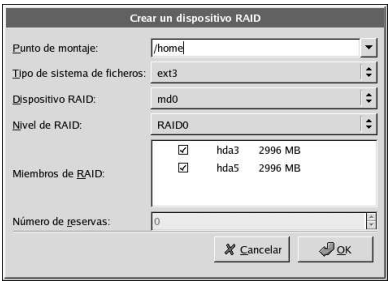

Figura 10-2. Creación de un dispositivo RAID

3. Introduzca un punto de montaje.
4. Seleccione el tipo de sistema de archivos para la partición.
5. Seleccione un nombre de dispositivo tal como **md0** para el dispositivo RAID.
6. Escoja el tipo de RAID. Puede elegir entre **RAID 0**, **RAID 1** y **RAID 5**.

Nota

Si está creando una partición RAID de `/boot`, deberá elegir RAID de nivel 1 y debería utilizar una de las dos primeras unidades (IDE primario, IDE secundario). Si no está creando una partición RAID de `/boot`, y quiere hacer una partición RAID de `/`, deberá ser de tipo RAID nivel 1 y debería estar situada en una de las dos primeras unidades (IDE primario, SCSI secundario).

7. Las particiones RAID que acaba de crear aparecerán en la lista **Miembros RAID**. Seleccione cuáles particiones de éstas deben ser usadas para crear el dispositivo RAID.
8. Si está configurando RAID 1 o RAID 5, especifique el número de particiones de repuesto. Si una partición de software RAID falla, la de repuesto será usada automáticamente como reemplazo. Para cada partición de repuesto que desee especificar, deberá crear una partición de software RAID adicional (además de las particiones para el dispositivo RAID). En el paso anterior, seleccione las particiones para el dispositivo RAID y la(s) particion(es) de repuesto.
9. Después de hacer click en **OK**, el dispositivo RAID aparecerá en la lista **Descripción de la unidad** como se muestra en la Figura 10-3. Llegados a este punto, puede continuar con su proceso de instalación. Remítase al *Manual de instalación de Red Hat Linux* para obtener más información.

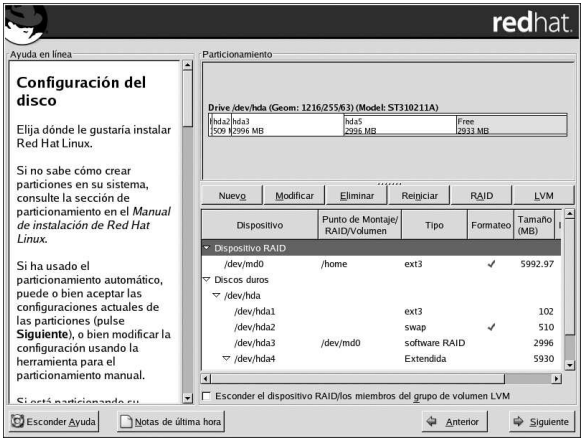

Figura 10-3. Creación de un arreglo RAID

Capítulo 11.

Configuración de LVM

LVM puede ser configurado durante la instalación gráfica de Red Hat Linux o durante la instalación de kickstart. Puede usar las utilidades desde el paquete `lvm` para crear su configuración de LVM, pero estas instrucciones enfocarán el uso de **Disk Druid** durante la instalación de Red Hat Linux para completar esta tarea.

Lea el Capítulo 4 sobre LVM en primer lugar. A continuación se presenta una vista preliminar de los pasos necesarios para configurar LVM:

- Crear *volúmenes físicos* desde las unidades de disco duro.
- Crear *grupos de volúmenes* desde los volúmenes físicos.
- Crear *volúmenes lógicos* desde el grupo de volúmenes y asignar los puntos de montaje de volúmenes lógicos.

Nota

Tan sólo puede modificar los grupos de volumen LVM en el modo de instalación GUI. En una instalación en modo texto, puede asignar los puntos de montaje para los volúmenes lógicos existentes.

Para crear un grupo de volumen lógico con los volúmenes lógicos durante la instalación de Red Hat Linux:

1. En la pantalla **Configuración del particionamiento del disco**, seleccione **Particionamiento manual con Disk Druid**.
2. Seleccione **Nuevo**.
3. No podrá introducir un punto de montaje (podrá efectuarlo una vez que haya creado su grupo de volumen).
4. Seleccione **volumen físico (LVM)** desde el menú **Tipo de sistema de archivos** como se muestra en la Figura 11-1.

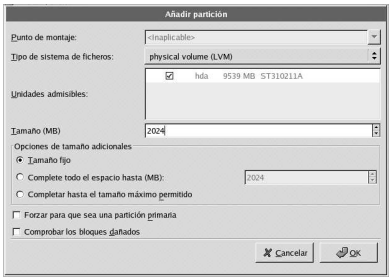

Figura 11-1. Creación de un volumen físico

5. Se debe constreñir un volumen físico a una unidad. Para las **Unidades disponibles**, seleccione la unidad en la que creará el volumen físico. Si posee múltiples unidades, todas las unidades serán seleccionadas aquí y deberá anular la selección de todas, a excepción de una.
6. Introduzca el tamaño que desea que posea el volumen físico.
7. Seleccione **Tamaño fijo** para crear el tamaño específico del volumen físico, seleccione **Completar todo el espacio hasta (MB)** e introduzca un tamaño en MBs para dar un ratio para el tamaño de volumen físico, o seleccione **Completar el tamaño máximo disponible** para hacer que crezca para rellenar todo el espacio disponible en el disco duro. Si ha creado más uno, compartirán el espacio libre del disco.
8. Seleccione **Forzar para que sea una partición primaria** si desea que la partición sea una partición primaria.
9. Seleccione **Controlar los bloques dañados** si desea que el programa de instalación controle los bloques dañados en el disco duro antes de formatearlo.
10. Pulse **OK** para volver a la pantalla principal.

Repita este paso para crear tantos volúmenes físicos como necesite para la configuración de LVM. Por ejemplo, si desea que su grupo de volumen abarque más de una unidad, cree un volumen físico para cada una de las unidades.

Aviso

La partición `/boot` no puede estar en un grupo de volumen porque el gestor de arranque no puede leerlo. Si desea poseer su partición de root en un volumen lógico, necesitará crear una partición `/boot` que no sea una parte de un grupo de volumen.

Una vez que haya creado los volúmenes físicos, siga estos pasos:

1. Pulse el botón **LVM** para recolectar los volúmenes físicos en grupos de volúmenes. Un grupo de volumen es básicamente una colección de volúmenes físicos. Puede poseer grupos múltiples de volumen lógico, pero un volumen físico tan sólo puede estar en un grupo de volumen lógico.

Nota

Existe un espacio de disco reservado en el grupo de volumen lógico. La suma de los volúmenes lógicos no será igual al tamaño del grupo de volumen; sin embargo, el tamaño de los volúmenes lógicos mostrados es correcto.

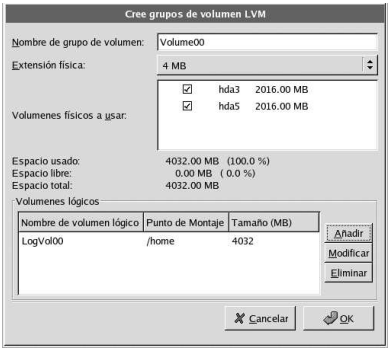

Figura 11-2. Creación de un dispositivo LVM

2. Cambiar el **Nombre del grupo de volumen** si lo desea.
3. Todos los volúmenes lógicos dentro del grupo de volumen deben estar localizados en las unidades *extensión física*. Por defecto, la extensión física está configurada en 4 MB; de este modo, el tamaño del volumen lógico debe ser divisible por 4 MBs. Si introduce un tamaño que no sea una unidad de 4MBs, el programa de instalación seleccionará automáticamente el tamaño más próximo en unidades de 4 MBs. Se le recomienda que cambie esta configuación.
4. Seleccione los volúmenes físicos a usar para el grupo de volumen.
5. Crear volúmenes lógicos con puntos de montaje tales como `/home`. Recuerde que `/boot` no puede ser un volumen lógico. Para añadir volúmenes lógicos, pulse el botón **Añadir** en la sección **Volúmenes lógicos**. Aparecerá una ventana de diálogo como se muestra en la Figura 11-3.

Figura 11-3. Creación de un volumen lógico

Repita estos pasos para cada grupo de volumen que desee crear.

Sugerencia

Deseará dejar espacio libre en el grupo de volumen lógico de manera que pueda ampliar los volúmenes lógicos a posteriori.

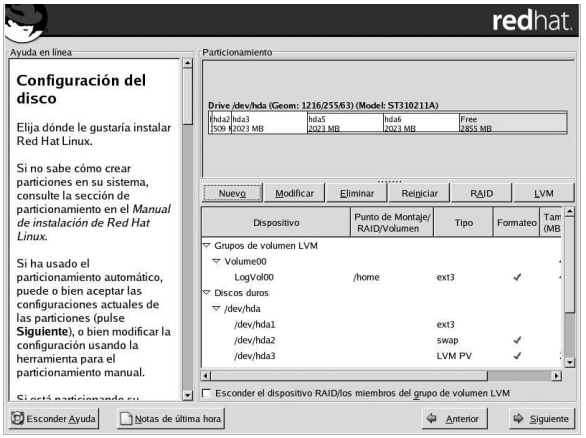

Figura 11-4. Volúmenes lógicos creados

III. Configuración relacionada a la red

Después de explicar cómo configurar la red, este capítulo discute tópicos relacionados a redes tales como formas de permitir conexiones remotas, compartir archivos y directorios sobre la red y la configuración de un servidor Web.

Tabla de contenidos

Capítulo 12.

Configuración de la red

Para que los ordenadores se puedan comunicar entre ellos es necesaria una conexión de red. Esto es posible gracias a que los sistemas operativos reconocen dispositivos de red como Ethernet, el módem RDSI o el token ring y a que estas interfaces de red están configuradas para conectarse a la red.

La **Herramienta de administración de redes** sirve para configurar los siguientes tipos de dispositivos de red:

- Ethernet
- RDSI
- módem
- xDSL
- token ring
- CIPE
- dispositivos inalámbricos

Para usar la **Herramienta de administración de redes**, debe tener privilegios de usuario root. Para arrancar la aplicación, vaya al **Botón de menú principal** (en el Panel) => **Configuración del sistema** => **Red**, o escriba el comando `redhat-config-network` en el intérprete de comandos (por ejemplo, en un **XTerm** o en un terminal **GNOME terminal**). Si escribe el comando, la versión gráfica es desplegada si se está ejecutando X, de lo contrario, se despliega la versión basada en texto. Para forzar a que se ejecute la versión basada en texto, use el comando `redhat-config-network-tui`.

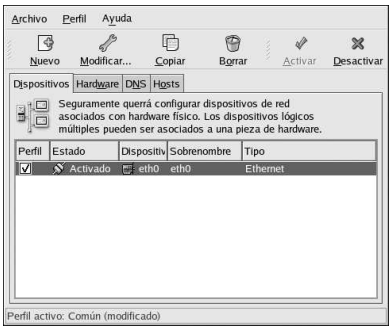

Figura 12-1. Herramienta de administración de redes

Si prefiere modificar los archivos de configuración manualmente, consulte el *Manual de referencia de Red Hat Linux* para información sobre su ubicación y contenidos.

Sugerencia

Vaya a la Lista de compatibilidad de hardware de Red Hat (http://hardware.redhat.com/hcl/) para ver si Red Hat Linux soporta su hardware.

12.1. Resumen

Para configurar una conexión de red con la **Herramienta de administración de redes**, siga los pasos siguientes:

1. Añada dispositivos hardware a la lista del hardware.
2. Añada dispositivos de red asociados al hardware anterior.
3. Configure el nombre del host y los parámetros DNS.
4. Configure cualquier hosts que no pueda ser encontrado a través de DNS.

Este capítulo discute cada uno de estos pasos para cada tipo de conexión de red.

12.2. Conexión Ethernet

Para establecer una conexión Ethernet, necesita una interfaz de red (NIC), un cable de red (usualmente un cable CAT5)y una red a la cual conectarse. Diferentes redes se configuran para velocidades diferentes; asegúrese de que su tarjeta NIC es compatible con la red a la cual se quiere conectar.

Siga los siguientes pasos:

1. Haga click en **Dispositivos**.
2. Haga click en el botón **Añadir**.
3. Seleccione **Conexión Ethernet** en la lista de **Seleccionar el tipo de dispositivo** y haga click en **Siguiente**.
4. Si ya ha añadido el dispositivo de red a la lista de hardware, selecciónelo de la lista **Dispositivo**. Sino, añada otros dispositivos de hardware seleccionándolo en **Otros dispositivos Ethernet**.

Nota

El programa de instalación normalmente detecta los dispositivos Ethernet y le pregunta si desea configurarlos. Si ya ha configurado algún dispositivo Ethernet durante la instalación, aparecerán en la lista de hardware en la pestaña **Hardware**.

5. Si ha seleccionado **Otros dispositivos de red**, aparecerá la pantalla **Seleccionar adaptador de Ethernet**. Seleccione el fabricante y el modelo del dispositivo Ethernet. Seleccione el nombre del dispositivo. Si se trata del primer dispositivo Ethernet del sistema, seleccione **eth0** como nombre del dispositivo, si es el segundo **eth1** (y así sucesivamente). La **Herramienta de administración de redes** también le permite configurar los recursos para NIC. Haga click en **Siguiente** para continuar.
6. En la pantalla **Configuración de parámetros de red** como se muestra en la Figura 12-2, elija entre DHCP y la dirección estática IP. Si el dispositivo recibe una dirección IP diferente cada vez que se arranca la red, no especifique el nombre del host. Haga click en **Siguiente** para continuar.
7. Haga click en **Aplicar** en la página **Crear dispositivo Ethernet**.

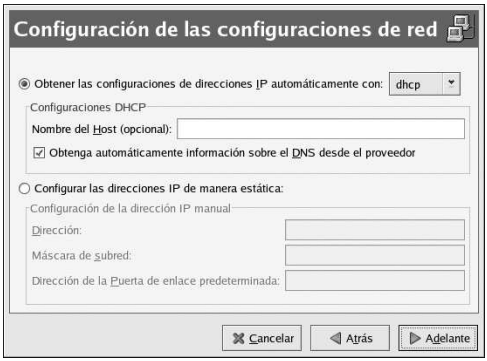

Figura 12-2. Parámetros de Ethernet

Después de haber configurado el dispositivo Ethernet, aparece en la lista de los dispositivos como se muestra en la Figura 12-3.

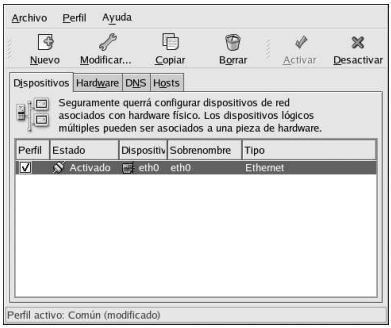

Figura 12-3. Dispositivo Ethernet

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de añadir el dispositivo Ethernet, puede modificar su configuración seleccionando el dispositivo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, cuando el dispositivo se añade, se configura para que arranque por defecto en el momento de arranque. Para modificar la configuración de este parámetro, seleccione el dispositivo y cambie el valor **Activar el dispositivo cuando se inicia el ordenador** y guarde sus cambios.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

Si asocia más de un dispositivo con una tarjeta Ethernet, los dispositivos subsecuentes serán *aliases de dispositivos*. Un alias de dispositivo le permite configurar múltiples dispositivos virtuales a un dispositivo físico, por tanto dándole más de una dirección IP. Por ejemplo, puede configurar un dispositivo eth1 y un dispositivo eth1:1. Para más detalles, refiérase a la Sección 12.13.

12.3. Conexión RDSI

Una conexión RDSI es una conexión a Internet con un módem a través de una línea de teléfono especial instalada por la compañía de teléfonos. Las conexiones RDSI son muy famosas en Europa.

Para establecer una conexión RDSI, siga los siguientes pasos:

1. Haga click en **Dispositivos**.
2. Haga click en el botón **Añadir** en la barra de herramientas.
3. Seleccione la **Conexión RDSI** en la lista de los **Seleccionar el tipo de dispositivos** y haga click en **Siguiente**.
4. Seleccione el adaptador RDSI del menú desplegable. Después configure los recursos y el protocolo del canal D para el adaptador. Haga click en **Siguiente** para continuar.

Figura 12-4. Parámetros RDSI

5. Si su proveedor Internet Service Provider (ISP) esta en la lista de las cuentas preconfiguradas, selecciónela. Sino, introduzca la información necesaria sobre la cuenta ISP. Si no sabe los valores, contacte a su ISP. Haga click en **Siguiente**.
6. En la ventana **Configuraciones IP**, seleccione **Modo de encapsulación** y si se debe obtener una dirección IP a través de DHCP o si se debe configurar una manualmente. Haga click en **Siguiente** cuando termine.
7. En la pantalla **Crear conexón telefónica** haga click en **Aplicar**.

Después de configurar el dispositivo RDSI, aparece en la lista de los dispositivos como un dispositivo **RDSI** como se muestra en la Figura 12-5.

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de añadir el dispositivo RDSI, puede modificar su configuración seleccionando el dispositivo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, cuando el dispositivo se añade, se configura para que no arranque en el tiempo de arranque predeterminado. Modifique la configuración modificando este parámetro. Se puede cambiar también la compresión, las opciones PPP, el nombre de conexión, la contraseña, etc.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

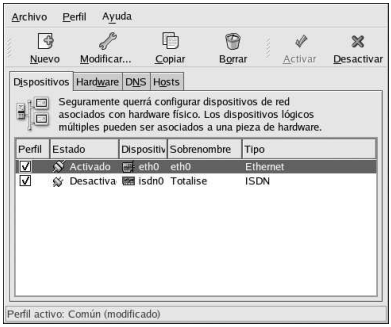

Figura 12-5. Dispositivo RDSI

12.4. Conexión vía módem

Un módem se puede usar para configurar una conexión a Internet con una línea telefónica activa. Se necesita una cuenta ISP, también llamada cuenta de conexión.

Para llevar a cabo una conexión via módem, siga los siguientes pasos:

1. Haga click en **Dispositivos**.
2. Haga click en el botón **Añadir** en la barra de herramientas.
3. Seleccione **Conexión via módem** en **Seleccionar tipos de dispositivos** y haga click en **Siguiente**.
4. Si ya tiene un módem configurado y aparece en la lista de hardware (en la pestaña **Hardware**), la **Herramienta de administración de redes** supone que desea usarla para establecer una conexión via módem. Si no hay módems ya configurados, tratará de detectarlos en el sistema. Esta búsqueda puede tardar un rato. Si no encuentra un módem, se mostrará un mensaje para advertirlo de que las configuraciones mostradas no son valores encontrados en la prueba.
5. Después aparecerá la pantalla como en la Figura 12-6.

Figura 12-6. Parámetros del módem

6. Configure el dispositivo módem, rata de baudios, el control del flujo y el volumen del módem. Si no conoce estos valores, acepte los valores si el módem fue probado exitósamente. Si no recibe el tono cuando marca el número, quite el ok de la casilla. Haga click en el botón **Siguiente**.
7. Si su ISP aparece en la lista de las cuentas predeterminadas, selecciónela; sino, introduzca la información de la cuenta ISP. Si no conoce los valores, contacte con su ISP. Haga click en **Siguiente**.
8. En la página **Configuración IP**, seleccione si desea obtener una dirección IP a través de DHCP o si la desea configurar de forma estática. Haga click en **Siguiente** cuando termine.
9. En la pantalla **Crear conexión telefónica** haga click en **Aplicar**.

Después de haber configurado el módem, aparece en la lista de los dispositivos con el tipo `Modem` como se muestra en la Figura 12-7.

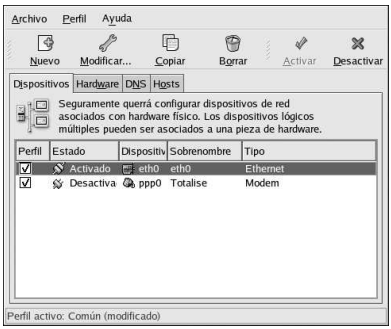

Figura 12-7. Dispositivo del módem

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de haber añadido el dispositivo del módem, puede modificar la configuración seleccionándolo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, cuando se añade un dispositivo, se configura para que no arranque en el tiempo de arranque predeterminado. Modifique la configuración para modificar este parámetro. También se puede cambiar la compresión, las opciones PPP, el nombre de login, la contraseña, etc.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

12.5. Conexión xDSL

DSL viene de las siglas de Digital Subscriber Lines. Hay diferentes tipos de DSL tales como ADSL, IDSL, y SDSL. La **Herramienta de administración de redes** usa el término xDSL para incluir todos los tipos de conexiones de DSL.

Algunos proveedores DSL requieren que el sistema esté configurado para obtener una dirección IP a través de DHCP con una tarjeta Ethernet. Algunos proveedores DSL requieren que configure una conexión PPPoE (Point-to-Point Protocol over Ethernet) con una tarjeta Ethernet. Pregúntele a su proveedor DSL cúal método usar.

Si tiene que usar DHCP, consulte la Sección 12.2 para configurar el dispositivo Ethernet.

Si usa el PPPoE, siga los pasos siguientes:

1. Haga click en **Dispositivos**.
2. Haga click en el botón **Nuevo**.
3. Seleccione **conexión xDSL** en la lista de los **Seleccionar el tipo de dispositivos** y haga click en **Siguiente**.
4. Si su tarjeta Ethernet está en la lista de hardware, seleccione el **Dispositivo Ethernet** desde el menú desplegable desde la página como se muestra en la Figura 12-8. De lo contrario, aparecerá la ventana **Seleccionar adaptador Ethernet**.

Nota

El programa de instalación normalmente detecta los dispositivos Ethernet soportados y le pregunta si los quiere configurar. Si ya ha configurado algún dispositivo Ethernet durante la instalación, aparecerá en la lista de hardware en la pestaña **Hardware**.

Figura 12-8. Parámetros xDSL

5. Si aparece la ventana **Seleccionar adaptador Ethernet**, seleccione el fabricante y el modelo del dispositivo Ethernet. Seleccione el nombre del dispositivo. Si es el primer dispositivo Ethernet del sistema llámelo **eth0**; si es el segundo llámelo **eth1** (y así sucesivamente). La **Herramienta de administración de redes** también le permite configurar los recursos para la NIC. Presione **Siguiente** para continuar.
6. Introduzca el **Nombre del proveedor**, **Nombre de conexión**, y **Contraseña**. Si tiene una cuenta T-Online, en vez de ingresar un **Nombre de conexión** y **Contraseña** en la ventana por defecto, haga click en el botón **Configuración de cuenta T-Online** e introduzca la información requerida. Haga click en **Siguiente** para continuar.
7. En la pantalla **Crear una conexión DSL** haga click en **Aplicar**.

Después de haber configurado la conexión DSL, aparece la lista de los dispositivos como se muestra en la Figura 12-7.

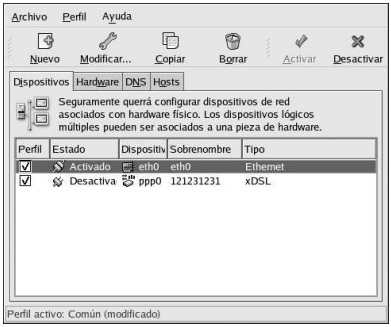

Figura 12-9. Dispositivo xDSL

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de haber establecido la conexión xDSL, puede modificar la configuración seleccionando el dispositivo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, cuando un dispositivo se añade, se configura para que no arranque en el tiempo de arranque predeterminado. Modifique la configuración modificando este parámetro.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

12.6. Conexión Token Ring

Una red token ring es una red en la que los ordenadores están conectados como si formasen un círculo. Un *token* o paquete especial de red, viaja a través del anillo y permite que los ordenadores se intercambien información.

Sugerencia

Para más información sobre el uso de token ring bajo Linux, consulte el sitio web de *Linux Token Ring Project* en http://www.linuxtr.net/.

Para llevar a cabo una conexión token ring, siga los siguientes pasos:

1. Haga click en **Dispositivos**.
2. Haga click en el botón **Añadir** en la barra de herramientas.
3. Seleccione **Conexión Token Ring** desde la lista de **Seleccionar tipos de dispositivos** y haga click en **Siguiente**.
4. Si ya tiene una tarjeta token ring configurada en la lista del hardware, selecciónela de la lista de las **Tarjeta token ring**. Sino, seleccione **Otro dispositivo Token ring** para añadirlo a la lista del hardware.
5. Si seleccionó **Otra tarjeta Tokenring**, aparecerá la ventana **Seleccionar adaptador Token Ring** como se muestra en la Figura 12-10. Seleccione el nombre del fabricante y el modelo del adaptador. Seleccione el nombre del dispositivo. Si es el primer token ring del sistema llámelo **tr0**; si es el segundo token ring, seleccione **tr1** (y así sucesivamente). La **Herramienta de**

administración de redes también permite al usuario configurar los recursos para el adaptador. Haga click en **Siguiente** para continuar.

Figura 12-10. Parámetros Token Ring

6. En la pantalla **Configurar parámetros de la red**, escoja entre DHCP y la dirección IP. Debe especificar un nombre del host para el dispositivo. Si el dispositivo recibe una dirección IP cada vez que se arranca la red, no especifique este nombre. Haga click en **Siguiente** para continuar.
7. Haga click en **Aplicar** en la página **Crear dispositivo Tokenring**.

Después de configurar el dispositivo token ring, aparece en la lista de los dispositivos como se muestra en la Figura 12-11.

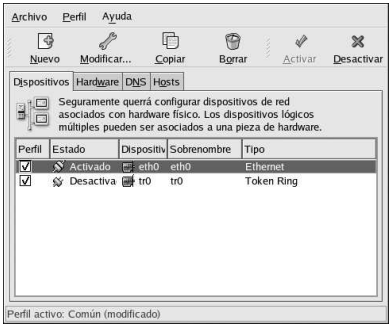

Figura 12-11. Dispositivo Token Ring

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de añadir el dispositivo, puede modificar la configuración seleccionándolo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, puede configurar el tiempo de arranque del dispositivo.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

12.7. Conexión CIPE

CIPE significa Crypto IP Encapsulation. Se utiliza para configurar dispositivos de túnel de IP. Por ejemplo, CIPE puede utilizarse para conceder acceso desde fuera a una Red privada virtual (VPN). Si necesita configurar un dispositivo CIPE, póngase en contacto con el administrador del sistema para obtener los valores correctos.

Figura 12-12. Parámetros CIPE

Sugerencia

Para más información sobre CIPE y su configuración, consulte el *Manual de seguridad de Red Hat Linux*.

12.8. Conexión de tipo inalámbrica

Los dispositivos Ethernet inalámbricos cada vez son más famosos. La configuración es parecida a la configuración de los dispositivos Ethernet salvo que permite configurar el SSID y la clave del dispositivo inalámbrico.

Para establecer una conexión Ethernet inalámbrica, siga los pasos siguientes:

1. Haga click en **Dispositivos**.
2. Haga click en **Añadir** en la barra de herramientas.
3. Seleccione **Conexión inalámbrica** desde **Seleccionar el tipo de dispositivo** y haga click en **Siguiente**.
4. Si ya ha agregado una tarjeta de red inalámbrica a la lista de hardware, selecciónela de la lista **Tarjeta inalámbrica**. De lo contrario, seleccione **Otra tarjeta inalámbrica** para añadir el dispositivo de hardware.

Nota

El programa de instalación normalmente detecta los dispositivos inalámbricos Ethernet soportados y le pregunta si desea configurarlos. Si ya ha configurado algún dispositivo inalámbrico durante la instalación, aparecerán en la lista de hardware en la pestaña **Hardware**.

5. Si ha seleccionado **Otro tarjeta inalámbrica**, aparece la ventana **Seleccionar el adaptador Ethernet**. Seleccione el nombre del fabricante y el modelo del adaptador y del dispositivo. Si es el primer dispositivo del sistema llámelo **eth0**; si es la segunda tarjeta Ethernet para el sistema, seleccione **eth1** (y así sucesivamente). La **Herramienta de administración de redes** también permite al usuario configurar los recursos para el dispositivo de red inalámbrico. Haga click en **Siguiente** para continuar.
6. En la página **Configurar conexión inalámbrica** como se muestra en la Figura 12-13, configure las propiedades para el dispositivo inalámbrico.

Figura 12-13. Parámetros de la conexión inalámbrica

7. En la pantalla **Configurar parámetros de la red**, escoja entre DHCP y la dirección IP. Debe especificar un nombre del host para el dispositivo. Si el dispositivo recibe una dirección IP cada vez que se arranca la red, no especifique este nombre. Haga click en **Siguiente** para continuar.
8. Haga click en **Aplicar** en la pantalla **Crear dispositivo inalámbrico**.

Después de configurar el dispositivo inalámbrico, aparece en la lista de dispositivos como se muestra en la Figura 12-14.

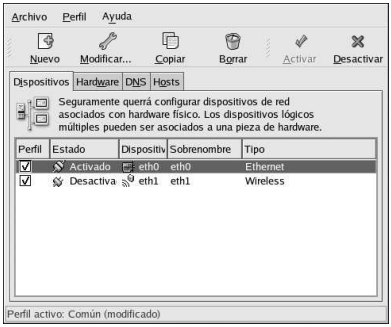

Figura 12-14. Dispositivo inalámbrico

Asegúrese de seleccionar **Archivo => Guardar** para guardar los cambios.

Después de añadir el dispositivo inalámbrico, puede modificar la configuración seleccionándolo de la lista de dispositivos y haciendo click en **Modificar**. Por ejemplo, puede configurar el dispositivo para que se active durante el tiempo de arranque.

Cuando se añade un dispositivo, este no se activa inmediatamente, como se puede ver en su estado **Inactivo**. Para activar el dispositivo, selecciónelo desde la lista de dispositivos y luego presione el botón **Activar**. Si el sistema está configurado para activar el dispositivo cuando la máquina arranca (por defecto), este paso no tiene que volverse a ejecutar.

12.9. Administración de los parámetros DNS

La pestaña **DNS** le permite configurar el nombre host del sistema, el dominio, los servidores de nombres y buscar el dominio. Los servidores de nombres se usan para buscar otros hosts en la red.

Si los nombres de servidores de DNS son obtenidos desde DHCP o PPPoE (o recuperados desde el ISP), no añada servidores DNS primarios, secundarios o terciarios.

Si el nombre del host es recuperado dinámicamente desde DHCP o PPPoE (o desde el ISP), no lo cambie.

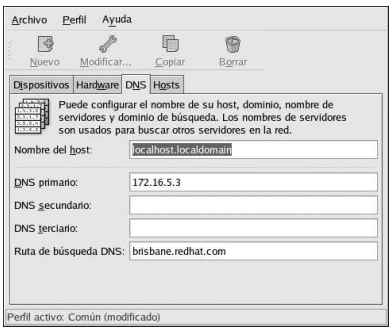

Figura 12-15. Configuración DNS

Nota

La sección de los servidores de nombres no configura el sistema para que sea un servidor de nombres. En su lugar, configura los servidores de nombres para que se usen cuando se resuelven direcciones IP a host y viceversa.

12.10. Administración de hosts

La pestaña **Hosts** le permite agregar, modificar o eliminar hosts del archivo `/etc/hosts`. Este archivo contiene las direcciones IP y sus nombres de hosts correspondientes.

Cuando el sistema intente resolver un nombre de host en una dirección IP, o determinar el nombre de host de una dirección IP, hará referencia al archivo `/etc/hosts` antes de usar los servidores de nombre (si usa la configuración por defecto del sistema Red Hat Linux). Si aparece la dirección IP en el archivo `/etc/hosts`, no se utilizarán los servidores de nombres. Si la red contiene ordenadores cuyas direcciones IP no aparecen en los DNS, se recomienda añadirlas al archivo `/etc/hosts`.

Para añadir una entrada al archivo `/etc/hosts`, vaya a la pestaña **Hosts**, haga click en el botón **Añadir** y proporcione la información que se le solicita y luego haga click en **OK**. Seleccione **Archivo => Guardar** o presione [Ctrl]-[S] para guardar los cambios al archivo `/etc/hosts`. La red o los servicios de la red no necesitan ser reiniciados ya que la versión actual del archivo es referenciada cada vez que se resuelve una dirección.

Aviso

No elimine la entrada `localhost`. Aún si el sistema no tiene una conexión de red o tiene una conexión de red ejecutándose constantemente, algunos programas necesitan conectarse al sistema a través de la interfaz de loopback de la máquina.

Figura 12-16. Configuración de los hosts

Sugerencia

Para cambiar el orden de búsqueda, modifique el archivo `/etc/host.conf`. La línea `order hosts, bind` especifica que `/etc/hosts` toma precedencia sobre los servidores de nombres. Si se cambia la línea a `order bind, hosts` se configura el sistema a que resuelva los nombres de host y direcciones IP usando los servidores de nombres primero. Si las direcciones IP no se pueden resolver a través de los servidores de nombres, el sistema entonces busca por la dirección IP en el archivo `/etc/hosts`.

12.11. Activación de dispositivos

Los dispositivos de red pueden configurarse para activarse en el momento del arranque o no. Por ejemplo, un dispositivo de red para una conexión de módem usualmente no está configurado para arrancar en el momento del arranque, mientras que una conexión Ethernet está configurada para iniciar el momento del arranque. Si su dispositivo de red está configurado para no iniciarse en el momento del arranque, puede usar **Red Hat Control Network** para activarlo a posteriori del arranque. Para iniciarlo, seleccione **Botón del menú principal** (en el Panel) => **Herramientas del sistema** => **Control de dispositivos de red** o escriba el comando `redhat-control-network`.

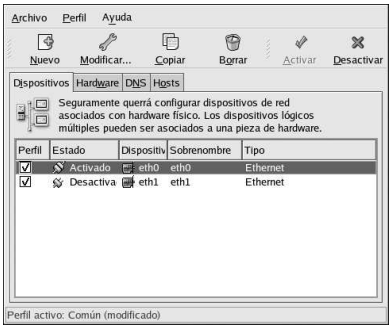

Figura 12-17. Activación de dispositivos

Para activar un dispositivo, selecciónelo de la lista y pulse el botón **Activar**. Para parar un dispositivo, selecciónelo desde la lista y pulse **Desactivar**.

Si esta configurado más de un perfil de red, estos son listados en la interfaz y se pueden activar. Consulte la Sección 12.12 para más detalles.

12.12. Funcionamiento con perfiles

Muchos dispositivos lógicos de red pueden ser creados para cada dispositivo de hardware físico. Por ejemplo, si tiene una tarjeta Ethernet en su sistema (eth0), puede crear dispositivos lógicos de red con apodos diferentes y opciones de configuración diferentes, todos a que estén asociados específicamente a eth0.

Los dispositivos lógicos de red son diferentes de los alias de dispositivos. Los dispositivos lógicos de red asociados con el mismo dispositivo físico deben existir en perfiles diferentes y no pueden ser activados simultáneamente. Los alias de dispositivo están asociados con el mismo dispositivo de

hardware físico, pero los alias asociados al mismo hardware físico pueden ser activados al mismo tiempo. Remítase a la Sección 12.13 para más detalles sobre la creación de alias.

Los *Perfiles* se pueden usar para crear grupos de configuración múltiple para las diferentes redes. Un grupo de configuraciones puede incluir dispositivos lógicos así como hosts y configuraciones DNS. Tras haber configurado los perfiles, puede usar la **Herramienta de administración de redes** para cambiar de uno a otro.

Existe por defecto, un perfil llamado **Common**. Para crear un nuevo perfil, pulse el botón **Perfil => Nuevo** desde el menú e introduzca un nombre único para el perfil.

Ahora esta modificando el nuevo perfil como se indica por la barra de estado en la parte inferior de la pantalla.

Haga click en un dispositivo ya existente en la lista y haga click en el botón **Copiar** para copiar un dispositivo existente a un dispositivo de red lógico. Si usa el botón **Nuevo**, se creará un alias de red, lo cual es incorrecto. Para cambiar las propiedades del dispositivo lógico, selecciónelo desde la lista y haga click en **Modificar**. Por ejemplo, el apodo se puede cambiar a un nombre más descriptivo, tal como **`eth0_office`**, para que sea reconocido más fácilmente.

En la lista de dispositivos existe una columna de casillas de verificación etiquetada como **Perfil**. Para cada perfil, puede comprobar o no dispositivos. Tan sólo los dispositivos comprobados están incluidos en el perfil seleccionado. Por ejemplo, si creó un dispositivo lógico llamado **`eth0_office`** en un perfil de nombre **`Office`** y quiere activar el dispositivo lógico si se selecciona el perfil, quite la marca del dispositivo `eth0` y seleccione `eth0_office`.

Por ejemplo, la Figura 12-18 le muestra un perfil llamado **Office** con el dispositivo lógico **eth0_office**. Está configurado para activar la primera tarjeta Ethernet usando DHCP.

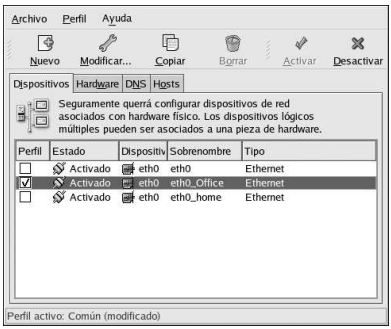

Figura 12-18. Perfil Office

Observe que el perfil **Home** como se muestra en la Figura 12-19 activa el dispositivo lógico **eth0_home**, el cual está asociado con `eth0`.

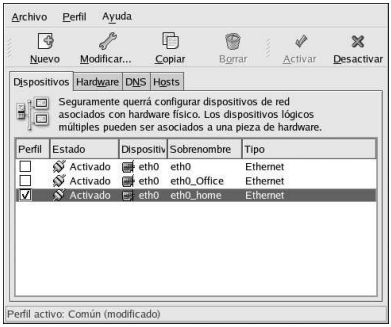

Figura 12-19. Home Profile

También puede configurar `eth0` para que se active en el perfil **Office** solamente y activar un dispositivo ppp (modem) en el perfil **Home** solamente. Otro ejemplo es tener el perfil **Common** activado `eth0` y un perfil **Away** para activar un dispositivo ppp para ser usado mientras se esté de viaje.

Un perfil no puede ser activado en el momento del arranque. Tan sólo los dispositivos en el perfil **Common** que están configurados para activarse en el momento de arranque. Una vez que el sistema haya arrancado, vaya al **Menú principal** (en el Panel) => **Herramientas de sistema** => **Control del dispositivo de red** (o escriba el comando `redhat-control-network`) para seleccionar un perfil y activarlo. La sección de activar perfiles sólo aparece en la interfaz **Control del dispositivo de red** si existen más interfaces además de **Common**.

Alternativamente, puede ejecutar el comando siguiente para activar un perfil (reemplace *<profilename>* con el nombre del perfil):

```
redhat-config-network-cmd --profile
<profilename> --activate
```

12.13. Alias de dispositivo

Los *Alias de dispositivo* son dispositivos virtuales asociados con el mismo hardware físico, pero pueden ser activados al mismo tiempo para tener diferentes direcciones IP. Están representados generalmente como el nombre del dispositivo seguido de dos puntos y un número (por ejemplo eth0:1). Son útiles si desea tener más de una dirección IP para un sistema, pero el sistema posee tan sólo una tarjeta de red.

Después de configurar el dispositivo Ethernet, tal como `eth0`, para usar una dirección estática IP (DHCP no funciona con aliases), vaya a la pestaña **Dispositivos** y haga click en **Nuevo**. Seleccione la tarjeta Ethernet a configurar con un alias, configura la dirección IP estática para el alias y haga click en **Aplicar** para crearlo. Puesto que ya existe un dispositivo para la tarjeta Ethernet, la que se acaba de crear es el alias tal como `eth0:1`.

Aviso

Si está configurando un dispositivo Ethernet para tener un alias, ni el dispositivo ni el alias pueden ser configurados para usar DHCP. Debe configurar las direcciones IP manualmente.

La Figura 12-20 muestra un ejemplo de un alias para el dispositivo `eth0`. Observe el dispositivo `eth0:1` — el primer alias para `eth0`. El segundo alias para `eth0` tendrá el nombre de dispositivo

`eth0:2`, y así sucesivamente. Para modificar los parámetros para el alias del dispositivo tal como si se debe activar en el momento de arranque y el número de alias, selecciónelo de la lista y haga click en el botón **Modificar**.

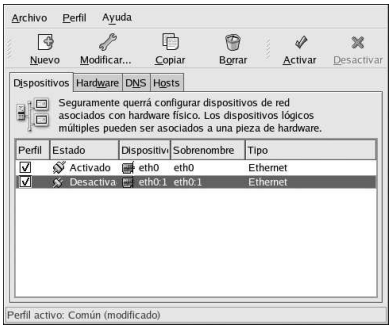

Figura 12-20. Ejemplo de alias del dispositivo de red

Seleccione el alias y pulse el botón **Activar** para activar el alias. Si ha configurado perfiles múltiples, seleccione qué perfiles incluir.

Para verificar que el alias ha sido activado, utilice el comando `/sbin/ifconfig`. La salida debería mostrar el dispositivo y el alias de dispositivo con direcciones IP diferentes:

```
eth0      Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.5  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
          TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:475 txqueuelen:100
          RX bytes:55075551 (52.5 Mb)  TX bytes:178108895 (169.8 Mb)
          Interrupt:10 Base address:0x9000

eth0:1    Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.42  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:10 Base address:0x9000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1627579 (1.5 Mb)  TX bytes:1627579 (1.5 Mb)
```

Capítulo 13.

Configuración básica de firewall

Un firewall o cortafuegos evita que los virus se esparzan por su ordenador y evita que los usuarios no autorizados accedan a su ordenador. El firewall está ubicado entre su ordenador y la red. Determina los servicios a los que pueden acceder los usuarios remotos en su red. Un firewall que haya sido configurado debidamente puede aumentar la seguridad de su sistema. Se le recomienda que configure un firewall para cualquier sistema con una conexión de Internet.

13.1. Herramienta de configuración de nivel de seguridad

Durante la instalación de Red Hat Linux en la pantalla de **configuración del firewall**, se le ha dado la posibilidad de escoger el nivel de seguridad alto, medio o ninguno así como también de permitir dispositivos específicos, servicios entrantes y puertos.

Después de la instalación, puede cambiar el nivel de seguridad de su sistema utilizando la **Herramienta de configuración de nivel de seguridad**. Si prefiere una aplicación basada en un asistente, consulte la Sección 13.2.

Para iniciar la aplicación, seleccione **Botón de menú principal** (en el panel) => **Configuración del sistema => Seguridad** o escriba el comando `redhat-config-securitylevel` desde un indicador de comandos de shell (por ejemplo, en una terminal XTerm o GNOME).

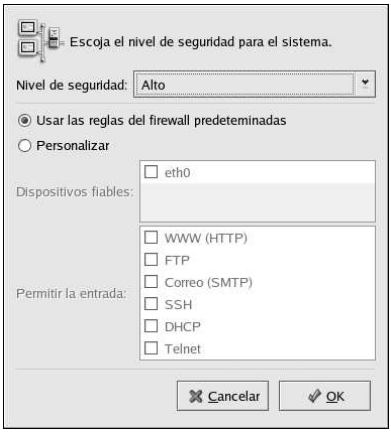

Figura 13-1. Herramienta de configuración de nivel de seguridad

Seleccione el nivel de seguridad deseado desde el menú despegable.

Alto

Si elige **Alto**, su sistema no aceptará conexiones (que no sean parámetros por defecto) que usted no haya definido específicamente. Por defecto, sólo las siguientes conexiones están permitidas:

- respuestas de DNS

- DHCP — de modo que cualquier interfaz de la red que use DHCP se puede configurar correctamente

Si elige **Alto**, su firewall no permitirá lo siguiente:

- Modo activo FTP (modo pasivo FTP, usado por defecto en la mayoría de clientes sí debería funcionar)
- transferencias de archivos IRC DCC
- RealAudio™
- Clientes remotos del sistema X Window

Si va a conectar su sistema a Internet, pero no desea ejecutar un servidor, ésta es la opción más segura. Si necesita servicios adicionales, puede elegir **Personalizar** para permitir servicios específicos a través del firewall.

Nota

Si selecciona un firewall medio o alto, los métodos de autenticación de red (NIS y LDAP) no funcionarán.

Medio

Si elige **Medio**, su firewall no permitirá que máquinas remotas tengan acceso a ciertos recursos de su sistema. Por defecto, el acceso a los siguientes recursos no está permitido:

- Puertos por debajo del 1023 — los puertos reservados estándar, usados por la mayoría de servicios de sistema, tales como **FTP**, **SSH**, **telnet**, **HTTP**, y **NIS**.
- El puerto de servidor NFS (2049) — NFS se deshabilita tanto para servidores remotos como para clientes locales.
- El modo de pantalla local del sistema X Window para clientes X remotos.
- El puerto de servidor X Font (por defecto, **xfs** no se escucha en la red; está deshabilitado en el servidor fuente).

Si quiere permitir recursos tales como **RealAudio™** a la vez que bloquea el acceso a los servicios normales del sistema, elija **Medio**. Seleccione **Personalizar** para permitir servicios específicos a través del firewall.

Nota

Si selecciona un firewall medio o alto, los métodos de autenticación de red (NIS y LDAP) no funcionarán.

Ningún Firewall

Ningún firewall proporciona acceso completo a su sistema y no realiza comprobaciones de seguridad. La Comprobación de seguridad es la deshabilitación del acceso a ciertos servicios. Esto debería estar seleccionado únicamente si usted está conectado a una red de confianza (no Internet) o si desea hacer más configuraciones de firewall en otro momento.

Elija **Personalizar** para añadir dispositivos de confianza o para permitir servicios de entrada adicionales.

Dispositivos fiables

Al seleccionar cualquiera de los **Dispositivos fiables** se permite el acceso a su sistema a todo el tráfico de ese dispositivo; queda excluido de las reglas del firewall. Por ejemplo, si está ejecutando una red local, pero está conectado a Internet por medio de un acceso remoto PPP, puede comprobar **eth0** y el tráfico proveniente de su red local será permitido. Seleccionar **eth0** como de confianza significa que todo el tráfico a través de Ethernet está permitido, pero la interfaz ppp0 sigue teniendo un firewall. Si desea restringir el tráfico en una interfaz, déjela sin marcar.

No es recomendable que haga cualquier dispositivo conectado a redes públicas, como Internet, un **Dispositivo fiable**.

Permitir la entrada

Activar estas opciones permite que los servicios especificados pasen a través del firewall. Nota, durante la instalación de la estación de trabajo, la mayoría de estos servicios *no* están instalados en el sistema.

DHCP

Si permite preguntas y respuestas DHCP de entrada, está permitiendo que cualquier interfaz de red que use DHCP determine sus direcciones IP. Normalmente DHCP está activado. Si DHCP no está activado, su ordenador no podrá obtener una dirección IP.

SSH

*S*ecure *SH*ell (SSH) es un conjunto de herramientas para conectarse y ejecutar comandos en una máquina remota. Si desea utilizar herramientas SSH para acceder a su máquina a través de un firewall, active esta opción. Para acceder a su máquina remotamente, utilizando herramientas SSH, necesita tener instalado el paquete `openssh-server`

Telnet

Telnet es un protocolo para conectarse a máquinas remotas. Las comunicaciones Telnet no son cifradas y no proporcionan seguridad ante la posibilidad de que alguien husmee la red. No se recomienda permitir el acceso Telnet de entrada. Si quiere permitir el acceso de entrada a Telnet, tendrá que instalar el paquete `telnet-server`.

WWW (HTTP)

Apache (y otros servidores Web) utilizan el protocolo HTTP para servir páginas web. Si está planeando hacer su servidor Web accesible para todos, active esta opción. No se requiere esta opción para visualizar páginas localmente o para desarrollar páginas web. Tendrá que instalar el paquete `apache` si quiere servir páginas web.

Al activar **WWW (HTTP)** no se abrirá un puerto para HTTPS. Para activar HTTPS, especifíquelo en el campo **Otros puertos**.

Mail (SMTP)

Si quiere permitir la entrega de correo a través de su firewall, de modo que hosts remotos puedan conectarse directamente a su máquina para entregar correo, active esta opción. No necesita activarla si recoge el correo desde su servidor de ISP utilizando POP3 o IMAP, o si usa una herramienta como por ejemplo **fetchmail**. Tenga en cuenta que un servidor SMTP que no esté configurado adecuadamente puede permitir que máquinas remotas usen su servidor para enviar correo basura.

FTP

El protocolo FTP se utiliza para transferir archivos entre máquinas en red. Si quiere hacer su servidor FTP accesible para todos, active esta opción. Necesita instalar el paquete `wu-ftpd` para que esta opción sea de utilidad.

Haga click en **OK** para activar el firewall. Después de presionar **OK**, las opciones seleccionadas son traducidas a comandos `iptables` y escritos al archivo `/etc/sysconfig/iptables`. El servicio `iptables` es también iniciado para que el cortafuegos se active inmediatamente después de guardar las opciones seleccionadas.

Aviso

Si tiene un firewall configurado o cualquier regla de firewall en el archivo `/etc/sysconfig/iptables`, el archivo será borrado si selecciona **Ningún Firewall** y luego presiona **OK** para guardar los cambios.

Las opciones seleccionadas son también escritas al archivo `/etc/sysconfig/redhat-config-securitylevel` para que así la configuración pueda ser recuperada la próxima vez que se arranque la aplicación. No modifique este archivo manualmente.

Para activar el servicio `iptables` para que se inicie automáticamente en el momento de arranque, consulte la Sección 13.3 para más detalles.

13.2. GNOME Lokkit

GNOME Lokkit le permite a un usuario medio configurar los parámetros del firewall mediante la creación de reglas de red `iptables` básicas. En lugar de tener que escribir las reglas, este programa le formula una serie de preguntas sobre cómo utiliza el sistema y, a continuación, escribe por usted las reglas en el archivo `/etc/sysconfig/iptables`.

No intente usar **GNOME Lokkit** para generar reglas de firewall complejas. Está diseñado para usuarios medios que deseen una protección en las conexiones por módem, cable o DSL. Para configurar reglas de firewall específicas, consulte el capítulo *Firewall con `iptables`* del *Manual de referencia de Red Hat Linux*.

Para desactivar servicios específicos, y denegar hosts y usuarios concretos, consulte el Capítulo 14.

Para arrancar la versión gráfica de **GNOME Lokkit**, seleccione **Botón de menú principal => Herramientas del sistema => Más herramientas del sistema => Lokkit**, o escriba el comando `gnome-lokkit` en el intérprete de comandos como root. Si no tiene acceso al sistema X Window o si prefiere usar un programa basado en texto, escriba el comando `lokkit` en el intérprete de comandos para arrancar la versión en modo texto.

13.2.1. Básico

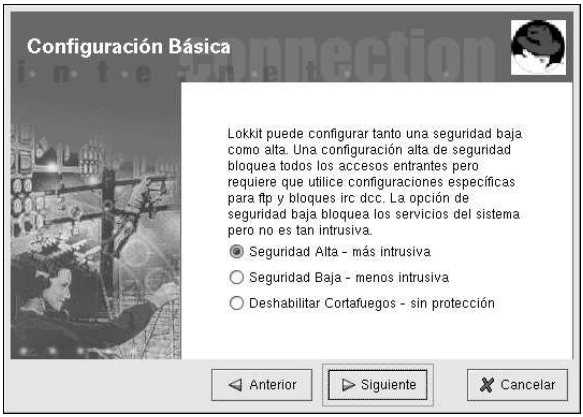

Figura 13-2. Básico

Después de arrancar el programa, elija el nivel de seguridad adecuado para el sistema:

- **Seguridad Alta** — Esta opción desactiva la mayoría de las conexiones de red, excepto las respuestas de DNS y DHCP para que se puedan activar las interfaces de la red. IRC, ICQ y otros servicios de mensajería instantáneo, así como RealAudio™ no funcionan sin un proxy.
- **Seguridad Baja** — Esta opción no permite conexiones remotas en el sistema, incluidas las conexiones NFS y las sesiones remotas de un sistema X Window. Los servicioes que se ejecutan en el puerto 1023 no aceptan las conexiones, incluidas las realizadas con FTP, SSH, Telnet y HTTP.
- **Deshabilitar Cortafuegos** — Esta opción no crea ninguna regla de seguridad. Sólo se recomienda seleccionar esta opción si el sistema se encuentra en una red de confianza (no en Internet), si el sistema tiene instalado un firewall grande o si escribe sus propias reglas personalizadas del firewall. Si elige esta opción y hace click en **Siguiente**, pase a Sección 13.3. No se cambiará la seguridad del sistema.

13.2.2. Hosts locales

Si hay dispositivos Ethernet en el sistema, la página de **Hosts Locales** le permitirá configurar si las reglas de firewall se utilizan en las peticiones de conexión enviadas a cada dispositivo. Si el dispositivo conecta el sistema a una área local con un firewall y no se conecta directamente a Internet, pulse **Sí**. Si la tarjeta Ethernet conecta el sistema a un módem DSL o por cable, se recomienda seleccionar **No**.

Figura 13-3. Hosts locales

13.2.3. DHCP

Si utiliza el protocolo DHCP para activar las interfaces de Ethernet en el sistema, debe responder **Sí** a la pregunta sobre DHCP. Si contesta no, no podrá conectar con una interfaz Ethernet. Muchos proveedores de Internet por DSL y cable requieren el uso del protocolo DHCP para las conexiones de Internet.

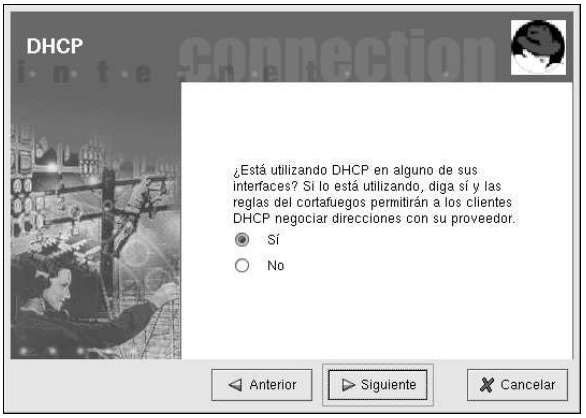

Figura 13-4. DHCP

13.2.4. Configuración de servicios

GNOME Lokkit también le permite activar y desactivar servicios comunes. Si responde **Sí** a la configuración de servicios, se le pedirá información sobre los servicios siguientes:

- **Servidor web** — Active esta opción si desea que los usuarios se conecten a un servidor Web, como Apache, que se ejecuta en el sistema. No es necesario que seleccione esta opción si desea ver las páginas en el sistema o en otros servidores de la red.
- **Correo entrante** — Active esta opción si el sistema debe aceptar el correo entrante. No necesitará usar esta opción si recupera el correo electrónico mediante IMAP, POP3 o fetchmail.
- **Shell segura** — Secure Shell, o SSH, es un conjunto de herramientas para el registro y ejecución de comandos en una máquina remota a través de una conexión cifrada. Si necesita tener acceso a la máquina de forma remota a través de ssh, active esta opción.
- **Telnet** — Telnet le permite registrarse en la máquina remotamente; sin embargo, no es un método seguro. Envía texto plano (incluidas las contraseñas) a través de la red. Se recomienda utilizar SSH para registrarse en la máquina remotamente. Si necesita tener acceso al sistema vía telnet, active esta opción.

Para desactivar otros servicios que no necesite, use **Serviceconf** (consulte la Sección 14.3) o **ntsysv**, (consulte la Sección 14.4), o `chkconfig` (vea la Sección 14.5).

13.2.5. Activación del firewall

Al hacer click en **Terminar** se registrarán las reglas del firewall en `/etc/sysconfig/iptables` y se iniciará el firewall al arrancar el servicio `iptables`.

Aviso

Si tiene un firewall configurado o alguna regla de firewall en el archivo `/etc/sysconfig/iptables`, el archivo será borrado si selecciona **Desactivar el firewall** y luego click en **Terminar** para guardar los cambios.

Es muy recomendable que ejecute **GNOME Lokkit** desde la máquina, no desde una sesión X remota. Si desactiva el acceso remoto al sistema, no podrá tener acceso al mismo ni desactivar las reglas del firewall.

Haga click en **Cancelar** si no desea escribir reglas de firewall.

13.2.5.1. Mail Relay

Mail Relay es un sistema que permite a otros sistemas enviar correo a través de él. Si el sistema es un mail relay, algunos usuarios podrían usarlo para enviar correo basura a otros desde su máquina.

Si decide activar los servicios de correo, después de hacer click en **Terminar** en la página **Activar el Firewall**, se le pedirá que compruebe el sistema de mail relay. Si pulsa **Sí** para comprobarlo, **GNOME Lokkit** intentará conectarse al sitio Web de *Mail Abuse Prevention System* en la dirección URL http://www.mail-abuse.org/ y ejecutará un programa de comprobación de mail relay. Los resultados de la comprobación se mostrarán cuando haya acabado. Si el sistema permite mail relay, es muy recomendable que configure Sendmail para evitar su uso.

13.3. Activación del servicio `iptables`

Las reglas de firewall sólo estarán activas si se está ejecutando el servicio `iptables`. Para arrancar manualmente el servicio, use el comando:

```
/sbin/service iptables restart
```

Para asegurarse de que se ha iniciado al arrancar el sistema, escriba el comando:

```
/sbin/chkconfig --level 345 iptables on
```

El servicio `ipchains` no se puede ejecutar junto al servicio `iptables`. Para asegurarse de que el servicio `ipchains` está desactivado, ejecute el comando:

```
/sbin/chkconfig --level 345 ipchains off
```

La **Herramienta de configuración de servicios** puede ser usada para configurar los servicios `iptables` e `ipchains`. Consulte la Sección 14.3 para más detalles.

redhat.

Capítulo 14.

Control de acceso a servicios

El mantenimiento de la seguridad en su sistema Red Hat Linux es extremadamente importante. Una forma de administrar la seguridad en el sistema es mediante una gestión minuciosa del acceso a los servicios del sistema. Probablemente su sistema deberá proporcionar acceso a determinados servicios (por ejemplo, `httpd` si ejecuta un servidor Web). Sin embargo, si no necesita proveer este servicio, debería desactivar esta función para que de este modo se minimice la exposición a potenciales fallos.

Hay diferentes métodos de administrar el acceso a los servicios del sistema. Debe decidir qué método le gustaría usar en función del servicio, la configuración del sistema y el nivel de conocimientos que tenga de Linux.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. Tanto los servicios administrados con `xinetd` (discutidos más adelante en esta sección) y los servicios en la jerarquía `/etc/rc.d` se pueden configurar para iniciarse o detenerse con tres aplicaciones diferentes:

- **Herramienta de configuración de servicios** — una aplicación gráfica que muestra una descripción de cada servicio, muestra si los servicios se han iniciado en el momento del arranque (para los niveles de ejecución 3, 4, y 5), y permite que los servicios sean arrancados, detenidos o reiniciados.
- **ntsysv** — una aplicación basada en texto que permite configurar cuáles servicios son arrancados al momento de arranque para cada nivel de ejecución. Los cambios no toman efecto de inmediato para los servicios no `xinetd`. Los servicios que no son `xinetd` no pueden ser arrancados, detenidos o reiniciados usando este programa.
- `chkconfig` — utilidad de línea de comandos permite activar o desactivar servicios para los diferentes niveles de ejecución. Los cambios no toman efecto de inmediato para los servicios no `xinetd`. Los servicios no `xinetd` no pueden ser arrancados, detenidos o reiniciados usando esta utilidad.

Pronto descubrirá que estas herramientas son más fáciles de usar que las alternativas — modificación manual de los numerosos vínculos simbólicos ubicados en los directorios bajo `/etc/rc.d` o la modificación de los ficheros de configuración `xinetd` en `/etc/xinetd.d`.

Otra forma de administrar el acceso a los servicios del sistema es mediante el uso de `iptables` para configurar un firewall IP. Si es un usuario nuevo de Linux, tenga en cuenta que `iptables` puede que no sea la mejor solución para usted. La configuración de `iptables` puede ser complicada y es mejor que la realicen administradores de sistemas Linux experimentados.

Por otro lado, la ventaja de utilizar `iptables` es flexibilidad. Por ejemplo, si necesita una solución personalizada que proporcione a determinados hosts el acceso a servicios concretos, `iptables` puede ser la herramienta que necesita. Consulte el *Manual de referencia de Red Hat Linux* y el *Manual de seguridad de Red Hat Linux* para más información sobre `iptables`.

Alternativamente, si está buscando una utilidad que establezca reglas de acceso generales para su máquina, y/o es un nuevo usuario de Linux, pruebe con **GNOME Lokkit**. **GNOME Lokkit** es una aplicación tipo GUI que le hará preguntas sobre cómo desea usar el equipo. Basado en sus respuestas, configurará un cortafuegos sencillo por usted. También puede usar la **Herramienta de configuración de nivel de seguridad** (`redhat-config-securitylevel`), la cual le permite seleccionar el nivel de seguridad para su sistema, similar a la pantalla de **Nivel de seguridad** en el programa de instalación de Red Hat Linux. Refiérase al Capítulo 13 para ver más información sobre estas herramientas.

14.1. Niveles de ejecución

Antes de configurar el acceso a servicios, deberá entender qué son los niveles de ejecución en Linux. Un nivel de ejecución es un estado o un *modo* que los servicios incluídos en el directorio `/etc/rc.d/rc`*<x>*`.d` definen, donde *<x>* es el número del nivel de ejecución.

Red Hat Linux utiliza los siguientes niveles de ejecución:

- 0 — Parada
- 1 — Modo de un usuario
- 2 — No se utiliza (definido por el usuario)
- 3 — Modo completo de multiusuarios
- 4 — No se utiliza (definido por el usuario)
- 5 — Modo completo de multiusuarios (con una pantalla de conexión basada en X)
- 6 — Rearranque

Si usa una pantalla de texto para el ingreso al sistema, estará operando a nivel de ejecución 3. Si usa una pantalla gráfica para ingresar al sistema, estará operando a nivel de ejecución 5.

El nivel de ejecución por defecto se puede cambiar si se modifica el fichero `/etc/inittab`, que contiene una línea junto a la parte superior del fichero con el siguiente aspecto:

```
id:5:initdefault:
```

Cambie el número de esta línea para reflejar el nivel de ejecución que desee. El cambio no tendrá efecto hasta rearrancar el sistema.

Para cambiar el nivel de ejecución inmediatamente, use el comando `telinit` seguido del número del nivel de ejecución. Debe ser usuario root para poder usar este comando.

14.2. TCP Wrappers

Muchos administradores de sistemas UNIX están acostumbrados a usar TCP wrappers para administrar el acceso a determinados servicios de red. Cualquier servicio de red que se administre con `xinetd` (así como también cualquier programa con soporte incorporado para libwrap) puede usar un TCP-wrapper para administrar el acceso. `xinetd` puede usar los ficheros `/etc/hosts.allow` y `/etc/hosts.deny` para configurar el acceso a los servicios del sistema. Como se deduce de los propios nombres `hosts.allow` contiene una lista de reglas que le permiten a los clientes accesar los servicios de red controlados por `xinetd`, y `hosts.deny` a su vez, con reglas para denegar el acceso. El fichero `hosts.allow` toma precedencia sobre el archivo `hosts.deny`. Los permisos que conceden o deniegan el acceso se pueden basar en una dirección IP individual (o nombres de hosts) o en un modelo de clientes. Vea el *Manual de referencia de Red Hat Linux* y la página del manual `hosts_access` en la sección 5 (`man 5 hosts_access`) para más detalles.

14.2.1. `xinetd`

Para controlar el acceso a los servicios de Internet, use `xinetd`, que es un sustituto seguro del comando `inetd`. El demonio `xinetd` conserva los recursos del sistema, proporciona control y registro de acceso, y sirve para arrancar servidores de uso especial. `xinetd` puede ser usado para proveer acceso a host particulares, denegar el acceso a determinados hosts, proporcionar acceso a un servicio en horas concretas, limitar el número de conexiones de entrada y/o la carga que se crea con las conexiones, etc.

`xinetd` se ejecuta de forma permanente y escucha todos los puertos de los servicios que administra. Cuando recibe una petición de conexión de uno de los servicios que administra, `xinetd` arranca el servidor apropiado a dicho servicio.

El archivo de configuración para `xinetd` es `/etc/xinetd.conf`, pero el archivo sólo contiene unos pocos valores por defecto y una instrucción para incluir el directorio `/etc/xinetd.d`. Para activar o desactivar un servicio `xinetd`, modifique el archivo de configuración en el directorio `/etc/xinetd.d`. Si el atributo `disable` está definido como **`yes`**, el servicio está desactivado. Si el

atributo `disable` está definido a **no**, el servicio estará activado. Puede editar cualquiera de los archivos de configuración `xinetd` o cambiar el estado usando la **Herramienta de configuración de servicios**, **ntsysv**, o `chkconfig`. Para una lista de los servicios de red controlados por `xinetd`, revise los contenidos del directorio `/etc/xinetd.d` con el comando `ls /etc/xinetd.d`.

14.3. Herramienta de configuración de servicios

La **Herramienta de configuración de servicios** es una aplicación gráfica desarrollada por Red Hat para configurar qué servicios SysV en `/etc/rc.d/init.d` se inician en el momento del arranque (para los niveles de ejecución 3, 4, y 5) y cuáles servicios `xinetd` están activados. También le permite arrancar, detener y rearrancar servicios SysV así como rearrancar `xinetd`.

Para arrancar la **Herramienta de configuración de servicios** desde el escritorio, vaya al botón **Menú principal** (en el Panel) **=> Configuración del servidor => Servicios** o escriba el comando `redhat-config-services` en el intérprete de comandos (por ejemplo, en un **XTerm** o un **terminal de GNOME**).

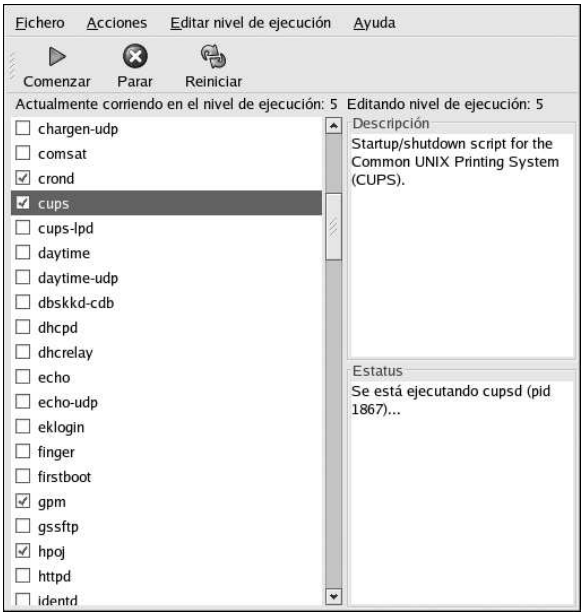

Figura 14-1. Herramienta de configuración de servicios

La **Herramienta de configuración de servicios** muestra el nivel de ejecución así como también el nivel de ejecución en el cual está modificando actualmente. Para modificar otro nivel de ejecución, seleccione **Editar nivel de ejecución** desde el menú desplegable y seleccione los niveles 3, 4, o 5. Refiérase a la Sección 14.1 para obtener una descripción de los niveles de ejecución.

La **Herramienta de configuración de servicios** muestra los servicios de `/etc/rc.d/init.d` y los servicios controlados por `xinetd`. Haga click en un servicio para mostrar una breve descripción del servicio y también para ver el estado del mismo. Si el servicio no es `xinetd`, la ventana de estado

muestra si el servicio se está ejecutando o no. Si el servicio es controlado por `xinetd`, la ventana de estado mostrará la frase **servicio xinetd**.

Para arrancar, detener o rearrancar un servicio inmediatamente, seleccione el servicio y haga click en el botón adecuado (o elija la acción correspondiente en el menú desplegable **Acciones**). Si el servicio es `xinetd`, los botones de acción estarán desactivados porque no pueden ser arrancados o detenidos individualmente.

Si activa o desactiva un servicio `xinetd` marcando o desmarcando la casilla de verificación al lado del nombre del servicio, debe seleccionar **Archivo => Guardar cambios** desde el menú desplegable para reiniciar `xinetd` e inmediatamente activar/desactivar el servicio `xinetd` que usted cambió. También se configura `xinetd` para recordar la configuración. Puede activar/desactivar más de un servicio `xinetd` a la vez y guardar los cambios cuando haya terminado.

Por ejemplo, imagine que verifica `rsync` para activarlo a nivel de ejecución 3 y luego guarda los cambios. El servicio `rsync` se activará de inmediato. La próxima vez que arranque `xinetd`, `rsync` estará todavía activado.

Aviso

Cuando guarde los cambios de los servicios `xinetd`, `xinetd` es reiniciado y los cambios toman efecto de inmediato. Cuando guarda cambios a otros servicios, el nivel de ejecución es reconfigurado, pero los cambios no serán efectivos de inmediato.

Para activar un servicio no `xinetd` para que se inicie en el momento de arranque del sistema para el nivel de ejecución seleccionado actualmente, marque la casilla de verificación al lado del nombre del servicio en la lista. Después de configurar el nivel de ejecución, aplique los cambios seleccionando **Archivo => Guardar cambios** desde el menú desplegable. La configuración del nivel de ejecución es modificada, pero el nivel de ejecución no es reiniciado; por tanto los cambios no toman efecto de inmediato.

Por ejemplo, asuma que está configurando un nivel de ejecución 3. Si cambia el valor para el servicio `anacron` de marcado a desmarcado y luego selecciona **Guardar cambios**, el nivel de ejecución 3 cambia y entonces `anacron` no es iniciado al momento de arranque. Sin embargo, el nivel de ejecución 3 no es reinicializado, por tanto `anacron` todavía estará ejecutándose. Llegados a este punto, seleccione una de las siguientes opciones:

1. Detener el servicio `anacron` — Detenga el servicio seleccionándolo de la lista y haciendo click en el botón **Parar el servicio**. Aparecerá un mensaje para indicar que se ha detenido correctamente el servicio.
2. Reinicializar el nivel de ejecución — Reinicializar el nivel de ejecución escribiendo en el intérprete de comandos del shell el comando `telinit 3` (donde 3 es el número de nivel de ejecución). Esta opción es recomendada si cambia el valor **Comenzar al arrancar** de más de un servicio y quiere activar los cambios inmediatamente.
3. No es necesario que detenga el servicio `anacron`. Puede esperar a que se rearranque el sistema para detener el servicio. La próxima vez que se arranque el sistema, se inicializará el nivel de ejecución sin que se ejecute el servicio `anacron`.

14.4. ntsysv

La utilidad **ntsysv** provee una interfaz sencilla para activar y desactivar servicios. Puede usar **ntsysv** para activar o desactivar un servicio `xinetd`. También puede usar **ntsysv** para configurar los niveles de ejecución. Por defecto, únicamente el nivel de ejecución actual es configurado. Para configurar un

nivel de ejecución diferente, especifique uno o más niveles con la opción `--level`. Por ejemplo, el comando `ntsysv --level 345` configura los niveles de ejecución 3, 4, y 5.

La interfaz **ntsysv** funciona de forma similar al programa de instalación en modo texto. Utilice las flechas arriba y abajo para desplazarse por la lista. La barra espaciadora selecciona o anula la selección de servicios, y también sirve para "pulsar" los botones **Aceptar** y **Cancelar**. Para desplazarse en la lista de servicios y entre los botones **Aceptar** y **Cancelar**, use la tecla [Tab]. Un asterisco, *****, significa que el servicio está activado. Con la tecla [F1] se mostrará una breve descripción de cada servicio.

Aviso

Los servicios manejados por `xinetd` son afectados de inmediato por **ntsysv**. Para todos los demás servicios, los cambios no toman efecto de inmediato. Usted debe detener o arrancar el servicio individual con el comando `service` *`daemon`* `stop`. En el ejemplo anterior, sustituya *`daemon`* por el nombre del servicio que desee detener, por ejemplo `httpd`. Reemplace `stop` por `start` o `restart` para arrancar o reiniciar el servicio.

14.5. `chkconfig`

El comando `chkconfig` puede ser usado para activar y desactivar servicios. Si usa el comando `chkconfig --list`, verá una lista de los servicios del sistema y si están iniciados (`on`) o detenidos (`off`) en los niveles de ejecución 0-6. Al final de la lista, verá una sección para los servicios manejados por `xinetd`.

Si usa `chkconfig --list` para realizar una consulta a un servicio manejado por `xinetd`, verá si el servicio `xinetd` está activado (`on`) o desactivado (`off`). Por ejemplo, el comando `chkconfig --list finger` retorna la salida siguiente:

```
finger          on
```

Como se muestra, `finger` está activado como un servicio `xinetd`. Si `xinetd` está ejecutándose, `finger` estará activo.

Si usa `chkconfig --list` para consultar un servicio `/etc/rc.d`, verá las configuraciones del servicio para cada nivel de ejecución. Por ejemplo, el comando `chkconfig --list anacron` devuelve la siguiente salida:

```
anacron         0:off   1:off   2:on    3:on    4:on    5:on
6:off
```

`chkconfig` también puede ser usado para configurar un servicio para que comience (o no) en un nivel de ejecución específico. Por ejemplo, desactive `nscd` en los niveles de ejecución 3, 4, y 5, usando el comando siguiente:

```
chkconfig --level 345 nscd off
```

Aviso

Los servicios gestionados por `xinetd` están afectados por `chkconfig`. Por ejemplo, si se está ejecutando `xinetd`, `finger` está deshabilitado y se ejecuta el comando `chkconfig finger on` y se activa de inmediato `finger` sin tener que reiniciar `xinetd` de forma manual. El resto de los cambios no se producen inmediatamente tras haber usado `chkconfig` manualmente. Deberá parar y reiniciar el servicio individual con el comando `service` *`daemon`* `stop`. En el ejemplo anterior, reemplace

daemon con el nombre del servicio que desea parar; por ejemplo, `httpd`. Reemplace `stop` `start` o con `restart` para iniciar o reiniciar el sistema .

14.6. Recursos adicionales

Para más información, refiérase a los recursos siguientes.

14.6.1. Documentación instalada

- Las páginas del manual para `ntsysv`, `chkconfig`, `xinetd`, y `xinetd.conf`
- `man 5 hosts_access` — Página del manual para el formato de ficheros de control de acceso al host (en la sección 5 de las páginas de manual).

14.6.2. Sitios Web útiles

- http://www.xinetd.org — Página Web sobre `xinetd`. Contiene una lista detallada de funciones y archivos de configuración de ejemplo.

Capítulo 15.

OpenSSH

OpenSSH es una implementación gratuita y de código libre de los protocolos SSH (*S*ecure *SH*ell). Esto sustituye a `telnet`, `ftp`, `rlogin`, `rsh`, y `rcp` con herramientas seguras y de conectividad de la red encriptada. OpenSSH soporta las versiones 1.3, 1.5, y 2 del protocolo SSH. Desde la versión 2.9 de OpenSSH, el protocolo por defecto es versión 2, el cual usa las claves RSA por defecto.

15.1. ¿Por qué usar OpenSSH?

Si utiliza las utilidades OpenSSH, estará incrementando la seguridad de su máquina. Todas las comunicaciones que utilizan las herramientas OpenSSH, incluyendo contraseñas, son encriptadas. `Telnet` y `ftp` utilizan contraseñas de texto plano y envían toda la información sin encriptar. La información puede ser interceptada, las contraseñas pueden ser recuperadas y cualquier persona no autorizada puede entrar al sistema, toda la seguridad puede estar comprometida. El conjunto de herramientas OpenSSH debe ser usado siempre que sea posible a la hora de abordar estos problemas de seguridad.

Otra razón por la que se recomienda usar OpenSSH es que automáticamente reenvía la variable `DISPLAY` a la máquina cliente. En otras palabras, si está ejecutando el sistema X Window en su máquina local, e ingresa a una máquina remota usando el comando `ssh`, cuando ejecute un programa en la máquina remota que requiera X, será visualizado en su equipo local. Esta característica, es conveniente si prefiere utilizar las herramientas gráficas del sistema pero no siempre tiene acceso al servidor.

15.2. Configurar un servidor OpenSSH

Para poner en funcionamiento un servidor OpenSSH, debe asegurarse primero que su sistema tiene los paquetes RPM instalados. Se requiere el paquete `openssh-server` que depende a su vez del paquete `openssh`.

El demonio OpenSSH usa el archivo de configuración `/etc/ssh/sshd_config`. Por defecto, el archivo de configuración instalado con Red Hat Linux debería ser suficiente para la mayoría de las configuraciones. Si quiere configurar su propio demonio de otra manera que no sea la proporcionada por defecto en el `sshd_config`, lea la página del manual `sshd` para una lista de palabras reservadas que pueden ser definidas en su archivo de configuración.

Para iniciar un servicio OpenSSH, use el comando `/sbin/service sshd start`. Para detener el servidor OpenSSH, use el comando `/sbin/service sshd stop`. Si desea que el demonio arranque automáticamente en el momento de inicio, refiérase al Capítulo 14 para más información sobre la administración de servicios.

Si reinstala un sistema Red Hat Linux, y clientes conectados a este, antes de reinstalar con cualquiera de las herramientas OpenSSH, después de la reinstalación, los usuarios del cliente verán el siguiente mensaje:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

El sistema reinstalado crea un nuevo set de claves de identificación para el sistema; de ahí, el aviso de que la clave del host RSA ha cambiado. Si desea mantener las claves del host generadas para

el sistema, haga una copia de seguridad de los archivos `/etc/ssh/ssh_host*key*` y restáurelos después de reinstalar. Este proceso retiene la identidad del sistema, y cuando los clientes traten de conectarse al sistema después de la instalación, estos no recibirán el mensaje de aviso.

15.3. Configuración de un cliente OpenSSH

Para conectarse a un servidor OpenSSH desde una máquina cliente, debe tener los paquetes `openssh-clients` y `openssh` instalados en la máquina cliente.

15.3.1. Uso del comando `ssh`

El comando `ssh` es un reemplazo seguro para los comandos `rlogin`, `rsh`, y `telnet`. Le permite inicar sesiones y ejecutar comandos en máquinas remotas.

Inicie una sesión en una máquina remota con `ssh` que es muy parecido a utilizar el comando `telnet`. Para iniciar una sesión remota a una máquina llamada penguin.example.net, escriba el comando siguiente en el intérprete de comandos del shell:

```
ssh penguin.example.net
```

La primera vez que ejecute `ssh` a una máquina remota, verá un mensaje similar al siguiente:

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

Escriba **`yes`** para continuar. Esto le permitirá agregar el servidor en su lista de host conocidos como se muestra en el siguiente mensaje:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known
hosts.
```

Luego, verá un indicador de comandos preguntándole por su contraseña. Después de ingresar su contraseña, se encontrará en el indicador de comandos de la máquina remota. Si no especifica un nombre de usuario, el nombre de usuario con el que se ha validado como la máquina local se validará en la máquina remota. Si quiere especificar un nombre de usuario use el comando siguiente:

```
ssh username@penguin.example.net
```

También puede usar la sintaxis `ssh -l username penguin.example.net`.

El comando `ssh` se puede utilizar para ejecutar un comando en una máquina remota sin acceder al indicador de comandos. La sintaxis es `ssh hostname command`. Por ejemplo, si quiere ejecutar el comando `ls /usr/share/doc` en la máquina remota penguin.example.net, escriba el comando siguiente en la línea de comandos del shell:

```
ssh penguin.example.net ls /usr/share/doc
```

Una vez que introduzca la contraseña correcta, visualizará el contenido del directorio `/usr/share/doc`, y regresará al shell de su equipo local.

15.3.2. Usando el comando `scp`

El comando `scp` puede ser usado para transferir archivos entre máquinas sobre una conexión encriptada y segura. Es parecido al comando `rcp`.

La sintaxis general para transferir el archivo local a un sistema remoto es como sigue a continuación:

```
scp localfile
username@tohostname:/newfilename
```

localfile especifica la fuente, y *username@tohostname:/newfilename* especifica el destino.

Para transferir un archivo local `shadowman` a su cuenta penguin.example.net, escriba en la línea de comandos (reemplace *username* con su nombre de usuario):

```
scp shadowman
username@penguin.example.net:/home/username
```

Esto transferirá el archivo local `shadowman` a `/home/`*username*`/shadowman` en penguin.example.net.

La sintaxis general para transferir un archivo remoto al sistema local es como sigue:

```
scp username@tohostname:/remotefile
/newlocalfile
```

remotefile especifica la fuente, y *newlocalfile* especifica el destino.

Se puede especificar múltiples archivos como las fuentes. Por ejemplo, para transferir el contenido del directorio `/downloads` a un directorio existente llamado `uploads` en la máquina remota penguin.example.net, teclee lo siguiente desde el intérprete de comandos:

```
scp /downloads/*
username@penguin.example.net:/uploads/
```

15.3.3. Uso del comando `sftp`

La utilidad `sftp` puede ser usada para abrir una sesión segura interactiva de FTP. Es similar a `ftp` excepto que ésta utiliza una conexión encriptada segura. La sintaxis general es *sftp username@hostname.com*. Una vez autentificado, podrá utilizar un conjunto de comandos similar al conjunto utilizado por el comando FTP. Consulte las páginas del manual de `sftp` para obtener un listado de todos estos comandos. Para consultar el manual ejecute el comando `man sftp` en el intérprete de comandos. La utilidad `sftp` sólo está disponible en las versiones 2.5.0p1 de OpenSSH y superiores.

15.3.4. Generar pares de claves

Si no quiere introducir su contraseña cada vez que se conecte a una máquina remota con `ssh`, `scp`, o `sftp`, puede generar un par de claves de autorización.

Las claves deben ser generadas para cada usuario. Para generar las claves de un usuario, debe seguir los siguientes pasos como el usuario que quiere conectarse a máquinas remotas. Si completa los siguentes pasos como root, sólo root será capaz de utilizar estas claves.

Arrancar con la versión 3.0 deOpenSSH, `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2`, y `/etc/ssh_known_hosts2` se ha quedado obsoletas. Los protocolos 1 y 2 de SSH comparten los archivos `~/.ssh/authorized_keys`, `~/.ssh/known_hosts`, y `/etc/ssh/ssh_known_hosts`.

Red Hat Linux 9 usa el protocolo 2 de SSH y claves RSA por defecto.

Sugerencia

Si reinstala Red Hat Linux y quiere guardar los pares de claves generados, haga una copia de respaldo del directorio `.ssh` en su directorio principal (home). Después de la reinstalación, copie este directorio de vuelta a su directorio principal. Este proceso puede realizarse para todos los usuarios de su sistema, incluyendo root.

15.3.4.1. Generar un par de claves RSA para la versión 2

Siga los siguientes pasos para generar un par de claves RSA para la versión 2 del protocolo SSH. Esto es lo predeterminado para iniciar con OpenSSH 2.9.

1. Para generar un par de claves RSA para trabajar con la versión 2 del protocolo, teclee el siguiente comando desde el indicador de comandos de la shell:
   ```
   ssh-keygen -t rsa
   ```
   Acepte la localización por defecto del archivo `~/.ssh/id_rsa`. Introduzca una palabra de paso diferente de la contraseña de su cuenta y confírmela introduciéndola nuevamente.

   La clave pública se escribe a `~/.ssh/id_rsa.pub`. La clave privada está escrita a `~/.ssh/id_rsa`. No distribuya la clave privada a nadie.
2. Cambie los permisos de su directorio `.ssh` usando el comando `chmod 755 ~/.ssh`.
3. Copie el contenido de `~/.ssh/id_rsa.pub` a `~/.ssh/authorized_keys` en la máquina en la que se quiere conectar. Si el archivo `~/.ssh/authorized_keys` no existe, puede copiar el archivo `~/.ssh/id_rsa.pub` al archivo `~/.ssh/authorized_keys` en la otra máquina.
4. Si está ejecutando GNOME, salte a la Sección 15.3.4.4. Si no está ejecutando el sistema X Window, salte a la Sección 15.3.4.5.

15.3.4.2. Generación de un par de claves DSA para la versión 2

Use los siguientes pasos para generar un par de claves DSA para la versión 2 del protocolo SSH.

1. Para generar un par de claves DSA para trabajar con la versión 2 del protocolo, escriba el siguiente comando en el intérprete de comandos de la shell:
   ```
   ssh-keygen -t dsa
   ```
   Acepte la localización por defecto del archivo `~/.ssh/id_dsa`. Introduzca una palabra de paso diferente a la contraseña de su cuenta y confirme ésta introduciéndola de nuevo.

   

   Sugerencia

   Una palabra de paso es una cadena de caracteres o palabras utilizadas para autentificar a un usuario. Las palabras de paso se diferencian de las contraseñas en que se pueden utilizar espacios o tabuladores en la palabra de paso. Las palabras de paso son generalmente más largas que las contraseñas porque ellas son habitualmente frases.

   La clave pública es escrita a `~/.ssh/id_dsa.pub`. La clave privada es escrita a `~/.ssh/id_dsa`. Es de suma importancia que no de la clave privada a nadie.
2. Cambie los permisos de su directorio `.ssh` usando el comando `chmod 755 ~/.ssh`.
3. Copie el contenido de `~/.ssh/id_dsa.pub` a `~/.ssh/authorized_keys` en la máquina en la cual quiere conectarse. Si el archivo `~/.ssh/authorized_keys` no existe, puede copiar el archivo `~/.ssh/id_dsa.pub` al archivo `~/.ssh/authorized_keys` en la otra máquina.

4. Si está ejecutando GNOME, salte a la Sección 15.3.4.4. Si no está ejecutando el sistema X Window, salte a la Sección 15.3.4.5.

15.3.4.3. Generación de un par de claves RSA para la versión 1.3 y 1.5

Siga los siguientes pasos para generar un par de claves RSA la cual es usada por la versión 1 del protocolo SSH. Si sólo se está conectando entre sistemas que usan DSA, no necesita una par de claves de versión RSA 1.3 o RSA versión 1.5.

1. Para generar un par de claves RSA (para la versión de protocolos 1.3 y 1.5), escriba el comando siguiente en la línea de comandos del shell:
   ```
   ssh-keygen -t rsa1
   ```
   Acepte la localización por defecto del archivo (`~/.ssh/identity`). Introduzca una palabra de paso diferente a la contraseña de su cuenta y confirme ésta introduciéndola de nuevo.

   La clave pública está escrita en `~/.ssh/identity.pub`. La clave privada está escrita a `~/.ssh/identity`. No entregue su clave a nadie.
2. Cambie los permisos de su directorio `.ssh` y su clave con los comandos `chmod 755 ~/.ssh` y `chmod 644 ~/.ssh/identity.pub`.
3. Copie los contenidos de `~/.ssh/identity.pub` al archivo `~/.ssh/authorized_keys` en la máquina a la cual se desea conectar. Si el archivo `~/.ssh/authorized_keys` no existe, puede copiarlo desde `~/.ssh/identity.pub` al archivo `~/.ssh/authorized_keys` en el equipo remoto.
4. Si está ejecutando GNOME, salte a la Sección 15.3.4.4. Si no está corriendo GNOME, salte a la Sección 15.3.4.5.

15.3.4.4. Configurar ssh-agent con GNOME

La utilidad `ssh-agent` puede ser usada para guardar su palabra de paso, de manera que no tendrá que ingresarla cada vez que inicie una conexión `ssh` o `scp`. Si está usando GNOME, la utilidad `openssh-askpass-gnome` puede ser usada para pedirle la palabra de paso cuando inicie una conexión con GNOME y guardarla hasta que salga de GNOME. No tendrá que ingresar su contraseña o palabra de paso para ninguna conexión `ssh` o `scp` realizada durante una sesión GNOME. Si no está usando GNOME, refiérase a la Sección 15.3.4.5.

Para guardar su palabra de paso durante una sesión GNOME, siga los pasos siguientes:

1. Necesitará tener instalado el paquete `openssh-askpass-gnome`; puede usar el comando `rpm -q openssh-askpass-gnome` para determinar si está instalado o no. Si no está instalado, hágalo desde su conjunto de CD de Red Hat Linux, desde un sitio espejo FTP de Red Hat, o usando Red Hat Network.
2. Seleccione **Botón del menú principal** (en el Panel) => **Extras** => **Preferencias** => **Sesión**, y haga click en la pestaña de **Programas de inicio**. Pulse en **Añadir** e introduzca **`/usr/bin/ssh-add`** en el cuadro de texto **Comando de inicio**. Establezca un número de prioridad más alto que cualquiera de los comandos existentes para asegurárse de que se ejecute de último. Un buen número de prioridad para `ssh-add` es 70 o superior. Mientras más alto el número, más baja la prioridad. Si tiene otros programas listados, este debería tener la prioridad más baja. Haga click en **Cerrar** para salir del programa.
3. Cierre la sesión y luego vuelva a GNOME; en otras palabras, reinicie X. Después de arrancar GNOME, aparecerá una ventana de diálogo pidiéndole su palabra(s) de paso. Introduzca la palabra de paso que se le pide. Si tiene pares de claves DSA y RSA, ambas configuradas, lo estará

ejecutando para ambas. A partir de este momento, no debería introducir ninguna contraseña para `ssh`, `scp`, o `sftp`.

15.3.4.5. Configuración de `ssh-agent`

`ssh-agent` se puede utilizar para almacenar sus palabras de paso para que así no tenga que ingresarlas cada vez que realice una conexión `ssh` o `scp`. Si no está ejecutando el sistema X Window, siga los pasos siguientes desde el intérprete de comandos del shell. Si está ejecutando GNOME pero no quiere configurarlo para que le solicite la palabra de paso cuando se conecte (vea la Sección 15.3.4.4), este procedimiento trabajará en una ventana de terminal como por ejemplo XTerm. Si está ejecutando X pero no GNOME, este procedimiento trabajará en una ventana de terminal. Sin embargo, sus palabras de paso sólo pueden ser recordadas en este terminal; no es una configuración global.

1. Desde el indicador de comandos de la shell, teclee el siguiente comando:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. Luego escriba el comando:
   ```
   ssh-add
   ```
   e ingrese su palabra de paso. Si tiene más de un par de claves configuradas, se le pedirá información para ambas.
3. Cuando termine la sesión, su palabra de paso será olvidada. Debe ejecutar estos dos comandos cada vez que abra una consola virtual o abra una ventana de terminal.

15.4. Recursos adicionales

Los proyectos OpenSSH y OpenSSL están en constante desarrollo, y la información más actualizada está disponible desde sus sitios web. Las páginas de manuales para las herramientas OpenSSH y OpenSSL también son una buena fuente de información detallada.

15.4.1. Documentación instalada

- Páginas de manual de `ssh`, `scp`, `sftp`, `sshd`, y `ssh-keygen` — estas páginas incluyen información sobre cómo usar estos comandos así como también los parámetros que se puede usar con ellos.

15.4.2. Sitios web útiles

- http://www.openssh.com — La página principal de OpenSSH, con una sección FAQ, informe de errores (bugs), listas de correo, objetivos del proyecto y una explicación más técnica de las características de seguridad.
- http://www.openssl.org — La página FAQ de OpenSSL, con listas de correo y una descripción del objetivo del proyecto.
- http://www.freessh.org — software de cliente SSH para otras plataformas.

Capítulo 16.

Network File System (NFS)

Network File System (NFS) es un método de compartición de archivos entre máquinas de una red de tal forma que tenemos la impresión de trabajar en nuestro disco duro local. Red Hat Linux puede trabajar como servidor o como cliente de NFS (o ambos), lo que implica que puede exportar sistemas de archivos a otros sistemas, así como montar los sistemas de archivos que otras máquinas exportan.

16.1. ¿Por qué utilizar NFS?

NFS resulta útil para compartir directorios de archivos entre múltiples usuarios de la misma red. Por ejemplo, un grupo de usuarios que trabajan en un mismo proyecto pueden tener acceso a los archivos de ese proyecto usando una porción compartida del sistema de archivos NFS (conocido como NFS share), que se ha montado en un directorio determinado, como puede ser `/myproject`. Para acceder a los archivos compartidos; el usuario accede al directorio `/myproject` de su máquina local. No tendrá que introducir contraseñas o memorizar comandos especiales. El usuario podrá trabajar como si el directorio estuviese en su máquina local.

16.2. Montar sistemas de archivos NFS

Utilice el comando `mount` para montar directorio de NFS compartido desde otra máquina:

```
mount shadowman.example.com:/misc/export
/misc/local
```

Aviso

Debe existir el directorio del punto de montaje en una máquina local (`/misc/local` en el ejemplo de arriba).

En este comando, `shadowman.example.com` es el nombre del servidor de archivos NFS, `/misc/export` es el nombre del sistema de archivos que `shadowman` está exportando y `/misc/local` es el directorio en la máquina local donde queremos que se monte el sistema de archivos. Una vez hayamos ejecutado el comando `mount` (siempre que tengamos los permisos adecuados en el servidor NFS `shadowman.example.com`), podremos teclear `ls /misc/local` y obtener un listado de los archivos que se encuentran en el directorio `/misc/export` de `shadowman.example.com`.

16.2.1. Montar sistemas de archivos NFS usando `/etc/fstab`

Un método alternativo para montar datos compartidos mediante NFS es añadir una línea en el archivo `/etc/fstab`. La línea debe incluir el nombre del servidor NFS, el directorio que el servidor está exportando y el directorio de nuestra máquina local donde queremos montar el sistema de archivos. Deberá ser administrador (root) para poder modificar el archivo `/etc/fstab`.

La sistaxis general de esta línea del archivo `/etc/fstab` es la siguiente:

```
server:/usr/local/pub    /pub    nfs    rsize=8192,wsize=8192,timeo=14,intr
```

El punto de montaje `/pub` debe existir en su máquina. Una vez que haya modificado esta línea en `/etc/fstab` en el sistema cliente, podrá teclear el comando `mount /pub` en la línea del indicador de comandos y el punto de montaje, `/pub` será montado desde el servidor.

16.2.2. Montar un sistema de archivos NFS usando autofs

La tercera opción para montar datos compartidos con NFS es utilizar autofs. Autofs utiliza el demonio automount para controlar los puntos de montaje dinámicamente tan sólo montándolos cuando sea necesario.

Autofs consulta el mapa maestro del archivo de configuración `/etc/auto.master` para ver qué puntos de montaje se han definido. Luego arranca un proceso automount con los parámetros adecuados para cada punto de montaje. Cada línea del mapa maestro define un punto de montaje y un archivo de mapa separado que define el sistema de archivos que se tiene que montar en este punto de montaje. Por ejemplo, el archivo `/etc/auto.misc` define los puntos de montaje en el directorio `/misc`; esta relación debe ser definida en el archivo `/etc/auto.master`.

Cada entrada del archivo `auto.master` tiene tres campos. El primero es el punto de montaje. El segundo es la localización del archivo de mapas y el tercero es opcional. El tercer campo puede contener información variada, como pueda ser el tiempo de expiración.

Por ejemplo, para montar el directorio `/proj52` en la máquina remota penguin.example.net en el punto de montaje `/misc/myproject` en su máquina, agregue la línea siguiente a `auto.master`:

```
/misc   /etc/auto.misc --timeout 60
```

Añada la siguiente línea a `/etc/auto.misc`:

```
myproject  -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

El primer campo del archivo `/etc/auto.misc` es el nombre del subdirectorio de `/misc`. Este directorio suele crearse dinámicamente con automount. No debería existir en la máquina cliente. El segundo campo contiene las opciones de montaje, como puede ser `rw` para tener acceso de lectura y escritura. El tercer campo es la localización de los datos exportados por el servidor de NFS, incluyendo el nombre del servidor y del directorio.

Nota

El directorio `/misc` debe existir en el sistema de archivos local. No debería haber ningún subdirectorio hijo de `/misc` en el sistema de archivos local.

Autofs es un servicio. Para iniciarlo, en la línea de comandos, teclee los siguientes comandos:

```
/sbin/service autofs restart
```

Para ver los puntos de montaje activos, teclee el siguiente comando en la línea de comandos:

```
/sbin/service autofs status
```

Si modifica el archivo de configuración `/etc/auto.master` mientras se ejecuta autofs, deberá decirle al demonio automount que vuelva a cargar la configuración mediante el siguiente comando:

```
/sbin/service autofs reload
```

Para aprender cómo hacer que autofs se inicie durante el arranque de su sistema, consulte el Capítulo 14 para obtener información sobre las utilidades de gestión del sistema.

16.3. Exportar sistemas de archivos NFS

Compartir archivos desde un servidor NFS es conocido como exportar directorios. La **Herramienta de configuración del servidor NFS** se puede usar para configurar un sistema como un servidor NFS.

Para usar la **Herramienta de configuración del servidor NFS**, debe estar ejecutando el sistema X Window, tener privilegios como root y tener el paquete RPM `redhat-config-nfs` instalado. Para iniciar la aplicación, seleccione **Botón de menú principal** (en el Panel) **=> Configuración del sistema => Configuración de servidores => Servidor NFS**, o escriba el comando `redhat-config-nfs`.

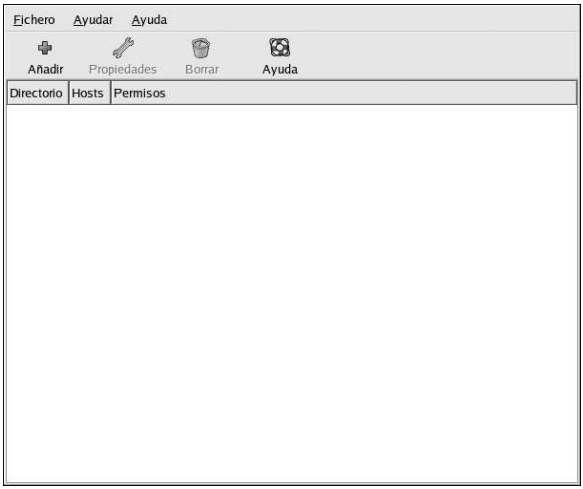

Figura 16-1. Herramienta de configuración del servidor NFS

Para añadir una partición NFS, pulse el botón **Añadir**. Aparecerá una casilla de diálogo mostrada en la Figura 16-2.

La pestaña **Básico** requiere la siguiente información:

- **Directorio** — Especifique el directorio a compartir, por ejemplo `/tmp`.
- **Host(s)** — Especifique el host(s) en el que compartir el directorio. Remítase a la Sección 16.3.2 para una explicación de formatos posibles.
- **Permisos básicos** — Especifique si el directorio debería tener permisos de sólo lectura o sólo escritura.

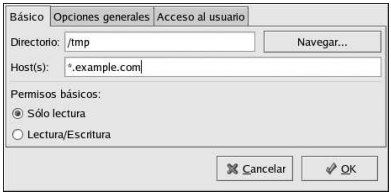

Figura 16-2. Añadir particiones

La pestaña **Opciones generales** permite configurar las siguientes opciones:

- **Permitir conexiones desde un puerto 1024 o superior** — Los servicios iniciados en los puertos con números inferiores a 1024 deben iniciarse como root. Seleccione esta opción para permitir que el servicio NFS sea iniciado por un usuario regular y no root. Esta opción corresponde a `insecure`.
- **Permitir el bloqueo de archivos inseguros** — No realiza una petición de bloqueo. Esta opción corresponde a `insecure_locks`.
- **Deshabilite el control del subárbol** — Si se exporta un subdirectorio de un sistema de archivos, pero no se exporta el sistema de archivos completo, el servidor comprueba si el archivo en cuestión está en el subdirectorio exportado. A este control se le conoce como *control de subárbol*. Seleccione esta opción para deshabilitar el control del subárbol. Si se exporta el sistema de archivos completo, seleccionar la deshabilitación del control del subárbol puede incrementar el ratio de transferencia. Esta opción corresponde a `no_subtree_check`.
- **Operaciones de escritura sincronizada a petición** — Habilitada por defecto, esta opción no deja que el servidor responda a las peticiones antes de que los cambios hechos a petición sean escritos en el disco. Esta opción corresponde a `sync`. Si no la ha seleccionado, se usará la opción `async`.
  - **Forzar la sincronización de operaciones de escritura inmediatamente** — No retrase la escritura en disco. Esta opción corresponde a `no_wdelay`.

La pestaña **Acceso al usuario** le permite configurar las opciones siguientes:

- **Trate el usuario de root remoto como root local** — Por defecto, el usuario y los IDs de grupo del usuario de root son 0. Root ubica el ID de usuario en 0 y el ID de grupo en 0 para los IDs de grupo y de usuario anónimos de manera que root en un cliente no posee privilegios de root en el servidor NFS. La selección de esta opción puede aminorar la seguridad del sistema. No lo seleccione a menos que sea absolutamente necesario. Esta opción corresponde a `no_root_squash`.
- **Trate a todos los usuarios de clientes como usuarios anónimos** — Si selecciona esta opción, todos los IDs de usuarios y de grupos están ubicados en el usuario anónimo. Esta opción corresponde a `all_squash`.
  - **Especificar el ID del usuario local para los usuarios anónimos** — Si selecciona **Tratar a todos los usuarios de clientes como usuarios anónimos**, esta opción le permite especificar un ID de usuario para el usuario anónimo. Esta opción corresponde a `anonuid`.
  - **Especificar el ID del grupo local para los usuarios anónimos** — Si selecciona **Tratar todos los usuarios de clientes como usuarios anónimos**, esta opción le permite especificar un ID de grupo para el usuario anónimo. Esta opción corresponde a `anongid`.

Para modificar una partición NFS ya existente, selecciónela desde la lista y pulse el botón **Propiedades**. Para borrar un share NFS ya existente, selecciónelo desde la lista y pulse el botón **Eliminar**.

Después de pulsar **OK** para añadir, modificar o eliminar un share NFS desde la lista, los cambios tendrán efecto inmediatamente — el demonio del servidor es reiniciado y el archivo de configuración viejo es guardado como `/etc/exports.bak`. La nueva configuración es escrita a `/etc/exports`.

La **Herramienta de configuración del servidor NFS** lee y escribe directamente al archivo de configuración `/etc/exports`. Por tanto, el archivo puede ser modificado manualmente después de usar la herramienta y la herramienta se puede usar después de modificar el archivo manualmente (asumiendo que el archivo fué modificado con la sintaxis correcta).

16.3.1. Configuración desde la línea de comandos

Si prefiere modificar archivos de configuración usando un editor de texto o si no tiene el sistema X Window instalado, puede modificar el archivo de configuración directamente.

El archivo `/etc/exports` controla qué directorios exporta el servidor NFS. Su formato es como puede ver a continuación:

```
directory
hostname(options)
```

La única opción que se debe especificar es una de `sync` o `async` (se recomienda `sync`). Si se especifica `sync`, el servidor no responde a las peticiones antes de que los cambios realizados sean escritos al disco.

Por ejemplo:

```
/misc/export
speedy.example.com(sync)
```

permitirá a los usuarios desde `speedy.example.com` montar `/misc/export` con los permisos por defecto de sólo lectura, pero:

```
/misc/export
speedy.example.com(rw,sync)
```

permitirá a los usuarios desde `speedy.example.com` montar `/misc/export` con privilegios de lectura/escritura.

Remítase a la Sección 16.3.2 para obtener una explicación de los posibles formatos de nombre de host.

Remítase al *Manual de referencia de Red Hat Linux* para obtener una lista de opciones que puedan ser especificadas.

Atención

Esté atento a los espacios en el archivo `/etc/exports`. Si no existen espacios entre el nombre del host y las opciones en paréntesis, las opciones se aplican sólo al nombre del host. Si existe un espacio entre el nombre del host y las opciones, las opciones se aplican al resto del mundo. Por ejemplo, examine las líneas siguientes:

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

La primera línea otorga acceso de lectura/escritura a los usuarios desde `speedy.example.com` y niega acceso a todos los otros usuarios. La segunda línea otorga acceso de sólo lectura a los usuarios desde `speedy.example.com` (predeterminado) y permite al resto del mundo acceso de lectura/escritura.

Cada vez que cambie `/etc/exports`, debe informar al demonio NFS del cambio, o recargar el archivo de configuración con el siguiente comando:

```
/sbin/service nfs reload
```

16.3.2. Formatos del nombre de host

El host(s) puede ser de las siguientes maneras:

- Máquina única — Nombre de dominio altamente cualificado, nombre del host (que puede ser resuelto por el servidor) o dirección IP.
- Series de máquinas especificadas con comodines — Use el caracter * o ? para especificar una cadena de caracteres que coincida. Por ejemplo, `192.168.100.*` especifica cualquier dirección IP que comience con 192.168.100. Cuando se usan comodines en nombres de dominio completos, los puntos (.) no son incluídos en el comodin. Por ejemplo, `*.example.com` incluye one.example.com pero no incluye one.two.example.com.
- Redes IP — Use *`a.b.c.d/z`*, donde *`a.b.c.d`* es la red y *`z`* es el número de bits en la máscara de red (por ejemplo 192.168.0.0/24). Otro formato aceptables es *`a.b.c.d/netmask`*, donde *`a.b.c.d`* es la red y *`netmask`* es la máscara de red (por ejemplo, 192.168.100.8/255.255.255.0).
- Grupos de red — En el formato *`@group-name`*, donde *`group-name`* es el grupo de red de NIS.

16.3.3. Inicio y parada del servidor

En el servidor que exporta el sistema de archivos NFS, el servicio `nfs` debe estar ejecutándose.

Vea el estado del demonio NFS con el siguiente comando:

```
/sbin/service nfs status
```

Lance el demonio NFS daemon con el comando

```
/sbin/service nfs start
```

Pare el demonio NFS con el siguiente comando:

```
/sbin/service nfs stop
```

Para comenzar el servicio `nfs` en el arranque, use el comando:

```
/sbin/chkconfig --level 345 nfs on
```

También puede usar **chkconfig**, **ntsysv** o la **Herramienta de configuración de servicios** para configurar qué servicios lanzar en el arranque. Vea el Capítulo 14 para más detalles.

16.4. Recursos adicionales

Este capítulo trata sobre la utilización de NFS. Para obtener información más detallada, consulte los siguientes recursos.

16.4.1. Documentación instalada

- Las páginas del manual de `nfsd`, `mountd`, `exports`, `auto.master`, y `autofs` (en las secciones del manual 5 y 8) — Estas páginas del manual le muestran la sintaxis correcta de los archivos de configuración de NFS y autofs.

16.4.2. Sitios Web útiles

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — *Linux NFS-HOWTO* del Linux Documentation Project.

16.4.3. Libros sobre el tema

- *Managing NFS and NIS Services* de Hal Stern; O'Reilly & Associates, Inc.

Capítulo 17.

Samba

Samba usa el protocolo SMB para compartir archivos e impresoras en la red. Los sistemas operativos que soportan este protocolo son, entre otros, Microsoft Windows (en el **Entorno de Red**), OS/2, y Linux.

17.1. ¿Por qué usar Samba?

Samba es útil si tiene una red con máquinas Windows y Linux. Samba permite compartir archivos e impresoras con todos los sistemas que tenga en la red. Si desea compartir archivos sólo entre máquinas Red Hat Linux, use NFS como se discutió en el Capítulo 16. Si desea compartir impresoras sólo entre máquinas Red Hat Linux no necesita usar Samba; consulte el Capítulo 27.

17.2. Configuración del servidor Samba

Samba usa por defecto el archivo de configuración (`/etc/samba/smb.conf`) que permite a los usuarios visualizar sus directorios principales en Red Hat Linux como una partición Samba (Samba share). También comparte impresoras configuradas para Red Hat Linux como impresoras compartidas de Samba. En otras palabras, puede conectar, por ejemplo una impresora al sistema Red Hat Linux e imprimir desde un ordenador de la red que tenga instalado el sistema Windows.

17.2.1. Configuración gráfica

Para configurar Samba usando una interfaz gráfica, use la **Herramienta de configuración del servidor Samba**. Para una configuración desde la línea de comandos, salte a la Sección 17.2.2.

La **Herramienta de configuración del servidor Samba** es una interfaz gráfica para el manejo de comparticiones Samba, usuarios y configuraciones básicas. Modifica los archivos de configuración en el directorio `/etc/samba/`. Cualquier cambio que no se haya realizado usando esta aplicación a estos archivos, se mantienen.

Para usar esta aplicación, debe estar ejecutando el sistema X Window, tener privilegios de root, y tener el paquete RPM `redhat-config-samba` instalado. Para arrancar la **Herramienta de configuración del servidor Samba** desde el escritorio, vaya al **Botón de menú principal** (en el Panel) => **Configuración del sistema** => **Configuración de servidores** => **Servidor Samba** o escriba el comando `redhat-config-samba` en el intérprete de comandos (por ejemplo, desde un terminal XTerm o GNOME).

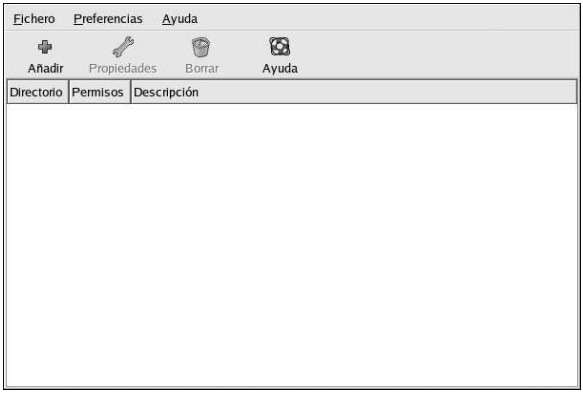

Figura 17-1. Herramienta de configuración del servidor Samba

Nota

La **Herramienta de configuración del servidor Samba** no muestra las impresoras compartidas o la estancia por defecto que permite a los usuarios ver sus propios directorios principales en el Servidor Samba.

17.2.1.1. Configuración de las propiedades del servidor

El primer paso para configurar un servidor Samba es configurar las propiedades básicas y algunas opciones de seguridad. Después de arrancar la aplicación, seleccione **Preferencias => Configuración de servidores** desde el menú. En la Figura 17-2 se muestra la pestaña **Básica**.

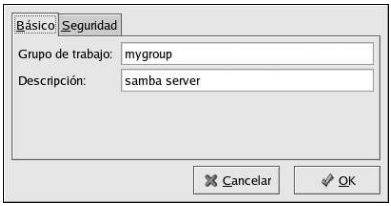

Figura 17-2. Configuración de las propiedades básicas del servidor

En la pestaña **Básica**, especifique en cual grupo debería estar el computador así como también una breve descripción del computador. Esto corresponde a las opciones `grupo de trabajo` y `server string` en `smb.conf`.

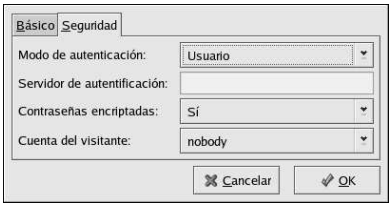

Figura 17-3. Configuración de las propiedades de seguridad

La pestaña de **Seguridad** contiene las opciones siguientes:

- **Modo de autenticación** — Esto corresponde a la opción `seguridad`. Seleccione uno de los siguientes tipos de autenticación.
  - **Dominio** — El servidor Samba confía en un Controlador de Dominio Windows NT Primario o de Backup para verificar un usuario. El servidor pasa el nombre del usuario y la contraseña al Controlador y espera para que éste la devuelva. Especifique el nombre del NetBIOS del Controlador de dominio primario o de backup en el campo **Servidor de autentificación**.

    La opción **Contraseñas encriptadas** debe estar colocada a **Si** si esto es seleccionado.
  - **Servidor** — El servidor Samba intenta verificar la combinación del nombre de usuario y la contraseña pasándolos a otro servidor Samba. Si no puede, el servidor intenta verificar usando el modo de autentificación del usuario. Especifique el nombre del NetBIOS del otro servidor Samba en el campo **Servidor de autentificación**.
  - **Partición** — Los usuarios Samba no tienen que ingresar un nombre de usuario y contraseña para cada servidor. No se les pide un nombre de usuario y contraseña hasta que ellos traten de conectarse a un directorio compartido específico desde el servidor Samba.
  - **Usuario** — (Por defecto) Los usuarios Samba deben proporcionar un nombre de usuario y contraseña válidos por servidor Samba. Seleccione esta opción si desea que la opción **Nombre de usuario Windows** funcione. Consulte la Sección 17.2.1.2 para más detalles.

- **Contraseñas encriptadas** — (Valor por defecto es **Si**) Esta opción debe estar activada si los clientes se están conectando desde Windows 98, Windows NT 4.0 con el Service Pack 3 o otras versiones más recientes de Microsoft Windows. Las contraseñas se transfieren entre el servidor y el cliente en un formato encriptado en vez de texto plano el cual puede ser fácilmente interceptado. Esto corresponde a la opción `Contraseñas encriptadas`. Consulte la Sección 17.2.3 para más información sobre contraseñas encriptadas Samba.
- **Cuenta del visitante** — Cuando los usuarios o invitados se conectan a un servidor Samba, ellos deben ser comparados con un usuario válido en el servidor. Seleccione uno de los nombres de usuarios válidos en el sistema para que sea la cuenta de invitados de Samba. Cuando los invitados se conectan a un servidor Samba, ellos tienen los mismos privilegios que este usuario. Esto corresponde a la opción `Cuenta del visitante`.

Después de pulsar **OK**, los cambios serán escritos en el archivo de configuración y el demonio es reiniciado; de este modo los cambios toman efecto de inmediato.

17.2.1.2. Administración de usuarios Samba

La **Herramienta de configuración del servidor Samba** requiere que haya una cuenta activa de usuarios en el sistema Red Hat Linux actuando como el servidor Samba antes de que se pueda agregar un usuario Samba. El usuario Samba está asociado con la cuenta de usuario existente Red Hat Linux.

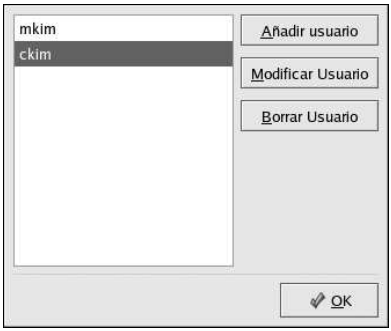

Figura 17-4. Administrando usuarios Samba

Para añadir un usuario Samba, seleccione **Preferencias => Usuarios Samba** desde el menú y haga click en el botón **Añadir usuario**. En la ventana **Crear un nuevo usuario Samba** seleccione **Nombre de usuario Unix** desde la lista de usuarios existentes en el sistema local.

Si el usuario tiene un nombre diferente en una máquina Windows y será conectado en un servidor Samba desde una máquina Windows, especifique ese nombre de usuario Windows en el campo **Nombre de usuario Windows**. El **Modo de autenticación** en la pestaña **Seguridad** de las preferencias **Configuraciones de servidores** debe estar colocado a **Usuario** para que esta opción funcione.

También configure una **Contraseña Samba** para el usuario Samba y confírmela escribiéndola nuevamente. Aún si selecciona usar contraseñas encriptadas para Samba, se recomienda que las contraseñas Samba para todos los usuarios sean diferentes que sus contraseñas de sistema Red Hat Linux.

Para modificar un usuario existente, seleccione el usuario desde la lista y haga click en **Modificar usuario**. Para eliminar un usuario Samba existente, seleccione el usuario, y haga click en el botón **Eliminar usuario**. Cuando borra un usuario Samba no está borrando la cuenta Red Hat Linux asociada.

Los usuarios son modificados inmediatamente después de hacer click en el botón **OK**.

17.2.1.3. Añadir una partición Samba

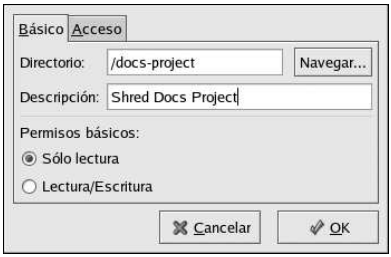

Figura 17-5. Añadir una partición Samba

Para añadir una partición Samba, haga click en el botón **Añadir**. La pestaña **Básica** configura las opciones siguientes:

- **Directorio** — El directorio a compartir vía Samba. El directorio debe existir.
- **Descripción** — Una breve descripción de la compartición.
- **Permisos básicos** — Especifica si los usuarios sólo podrán leer los archivos en el directorio compartido o si pueden leer y escribir al mismo.

En la pestaña de **Acceso**, seleccione si desea que sólo usuarios específicos accesen la compartición o si quiere que todos los usuarios Samba tengan acceso a la partición. Si selecciona permitir el acceso a usuarios específicos, seleccione a los usuarios desde la lista de usuarios Samba disponibles.

La compartición es añadida inmediatamente luego de presionar **OK**.

17.2.2. Configuración de línea de comandos

Samba usa el archivo `/etc/samba/smb.conf`. Si cambia el archivo de configuración, los cambios no tienen efecto hasta que no reinicie el demonio Samba con el comando `service smb restart`.

Para especificar el grupo de trabajo Windows y una breve descripción del servidor Samba, modifique las líneas siguientes en su archivo `smb.conf`:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

Reemplace *`WORKGROUPNAME`* con el nombre del grupo de trabajo Windows al cual debería pertenecer la máquina. El *`BRIEF COMMENT ABOUT SERVER`* es opcional y es usado como el comentario de Windows sobre el sistema Samba.

Para crear un directorio compartido Samba en su sistema Linux, agregue la siguiente sección a su archivo `smb.conf` (después de modificarlo para reflejar las necesidades de su sistema):

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

El ejemplo de arriba permite a los usuarios tfox y carole leer y escribir el directorio `/home/share`, en el servidor Samba, desde un cliente Samba.

17.2.3. Contraseñas encriptadas

En Red Hat Linux 9 las contraseñas encriptadas son activadas por defecto porque así es más seguro. Si las contraseñas encriptadas no son usadas, se usan las contraseñas de texto plano, las cuales pueden ser interceptadas usando un huzmeador de paquetes de red. Se recomienda que se usen las contraseñas encriptadas.

El protocolo Microsoft SMB originalmente usaba contraseñas de texto plano. Sin embargo, Windows NT 4.0 con el Service Pack 3 o superior, Windows 98, Windows 2000, Windows ME, y Windows XP requieren contraseñas encriptadas Samba. Para usar Samba entre un sistema Red Hat Linux y un sistema ejecutando uno de estos sistemas operativos, puede modificar su registro Windows o bien usar contraseñas de texto plano o configurar Samba en su sistema Linux para usar contraseñas encriptadas. Si selecciona modificar su registro, debe hacerlo para todas sus máquinas Windows — esto es un poco riesgoso y puede causar conflictos. Se recomienda que use contraseñas encriptadas para mayor seguridad.

Para configurar Samba en su sistema Red Hat Linux para usar contraseñas encriptadas, siga los pasos siguientes:

1. Cree un archivo de contraseñas separado para Samba. Para crear uno basado en su archivo existente `/etc/passwd`, en el intérprete de comandos, escriba el comando siguiente:
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Si el sistema usa NIS, escriba el comando siguiente:
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   El script `mksmbpasswd.sh` es instalado en su directorio `/usr/bin` con el paquete `samba`.
2. Cambie los permisos del archivo de contraseñas Samba para que sólo root tenga privilegios de leer y escribir:
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. El script no copia las contraseñas al nuevo archivo, y una cuenta de usuario Samba no esta activa hasta que se configure una contraseña para ella. Para mayor seguridad, se recomienda que la contraseña de usuario Samba sea diferente de la contraseña del usuario Red Hat Linux. Para configurar cada contraseña de usuario, use el comando siguiente (reemplace *`username`* con cada nombre de usuario):
   ```
   smbpasswd username
   ```
4. Las contraseñas encriptadas deben estar activadas en el archivo de configuración Samba. En el archivo `smb.conf`, verifique que las siguientes líneas esten presentes y no se encuentren dentro de comentarios:
   ```
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
   ```
5. Asegúrese de que el servicio `smb` sea arrancado escribiendo el comando `service smb restart` en el intérprete de comandos de la shell.
6. Si desea que el servicio `smb` se arranque automáticamente, use **ntsysv**, `chkconfig`, o la **Herramienta de configuración de servicios** para activarlo en tiempo de ejecución. Consulte el Capítulo 14 para más detalles.

Sugerencia

Lea `/usr/share/doc/samba-`*<version>*`/docs/htmldocs/ENCRYPTION.html` para más detalles sobre las contraseñas encriptadas. (reemplace *<version>* con el número de versión de Samba que tiene instalado).

El módulo PAM `pam_smbpass` se puede usar para sincronizar las contraseñas Samba con sus contraseñas del sistema cuando el comando `passwd` es usado. Si un usuario invoca el comando `passwd`, la contraseña que use para conectarse en el sistema Red Hat Linux así como también la contraseña que debe proporcionar para conectarse a la partición Samba, son cambiadas.

Para activar esta característica, añada la siguiente línea `/etc/pam.d/system-auth` debajo de la llamada de `pam_cracklib.so`:

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

17.2.4. Arrancar y detener el servidor

En el servidor que esta compartiendo directorios a través de Samba, el servicio `smb` debe estar ejecutándose.

Visualice el estado del demonio Samba con el comando siguiente:

```
/sbin/service smb status
```

Puede arrancar el demonio con el comando siguiente:

```
/sbin/service smb start
```

Detenga el demonio con el comando siguiente:

```
/sbin/service smb stop
```

Para iniciar el servicio `smb` al momento de arranque, use el comando:

```
/sbin/chkconfig --level 345 smb on
```

También puede usar `chkconfig`, **ntsysv** o la **Herramienta de configuración de servicios** para configurar cuáles servicios iniciar en el momento de arranque. Consulte el Capítulo 14 para más detalles.

17.3. Conexión a una compartición Samba

Para conectarse a una compartición Linux Samba desde un ordenador Microsoft Windows, use el **Entorno de red** o el administrador de archivos.

Para conectarse a una compartición Samba desde un sistema Linux, escriba en la línea de comandos de la shell el comando:

```
smbclient
//hostname/sharename -U
username
```

Tendrá que reemplazar *`hostname`* por el nombre de la máquina o la dirección IP del servidor Samba al que desee conectarse, *`sharename`* por el nombre del directorio compartido al que quiera acceder y *`username`* por el nombre del usuario para el sistema Samba. Introduzca la contraseña correcta o presione [Intro] si no se requiere contraseña.

Si ve `smb:\>` en la pantalla, la conexión se habrá realizado sin ningún problema. Una vez que se haya conectado, escriba **`help`** para ver la lista de comandos. Si desea ver los contenidos de su directorio principal, reemplace *`sharename`* por su nombre del usuario. Si la opción `-U` no es usada, el nombre de usuario del usuario actual es pasado al servidor Samba.

Para salir de `smbclient`, escriba **`exit`** en la inea de comandos `smb:\>`.

Puede usar también **Nautilus** para ver las comparticiones de Samba disponibles en su red. Seleccione **Botón de menú principal** (en el Panel) => **Servidores de red** para visualizar la lista de los grupos de trabajo Samba en su red. También puede escribir **`smb:`** en la barra **Location:** de Nautilus para ver los grupos de trabajo.

Como se muestra en la Figura 17-6, aparece un icono para cada grupo de trabajo SMB disponible en la red.

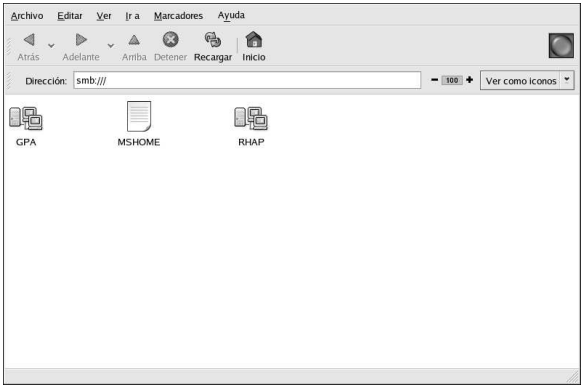

Figura 17-6. Grupos de trabajo SMB en Nautilus

Haga doble-click en uno de los iconos de los grupos de trabajo para ver una lista de las computadoras dentro del grupo.

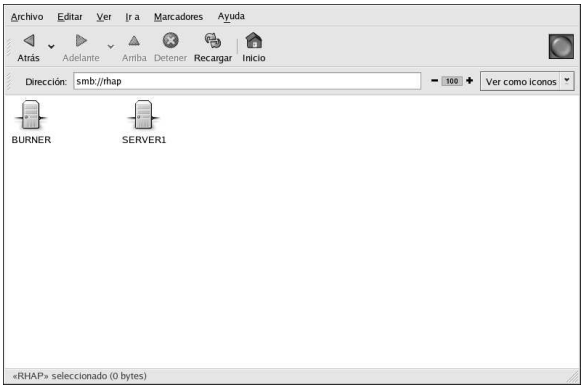

Figura 17-7. Máquinas SMB en Nautilus

Como puede ver desde la Figura 17-7, hay un icono para cada máquina dentro del grupo de trabajo. Haga doble-click en un icono para ver las comparticiones Samba en la máquina. Si se requiere una combinación de nombre de usuario y contraseña, se le pedirá.

Alternativamente, puede especificar una combinación de nombre de usuario y contraseña en **Location:** usando la sintaxis siguiente (sustituya *`user`*, *`password`*, *`servername`*, y *`sharename`* con los valores apropiados):

```
smb://user:password@servername/sharename/
```

17.4. Recursos adicionales

Para tener más información sobre las opciones de configuración que no se han tratado aquí, consulte los siguientes recursos.

17.4.1. Documentación instalada

- La página man de `smb.conf` — explica cómo configurar el archivo de configuración de Samba
- La página man de `smbd` — describe cómo funciona el demonio Samba
- `/usr/share/doc/samba-<version-number>/docs/` — HTML y archivos texto de ayuda incluídos con el paquete `samba`

17.4.2. Sitios web útiles

- http://www.samba.org — La página web de Samba contiene documentación útil, información sobre las listas de correo y una lista de las interfaces GUI.

Capítulo 18. Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP), Protocolo de configuración dinámica de servidor, es un protocolo de red para asignar automáticamente información TCP/IP a equipos cliente. Cada cliente DHCP se conecta un servidor DHCP centralizado que devuelve la configuración de red del cliente, incluida la dirección IP, el gateway y los servidores DNS.

18.1. Motivos para usar el protocolo DHCP

DHCP es útil para proporcionar de un modo rápido la configuración de red del cliente. Al configurar el sistema cliente, el administrador puede seleccionar el protocolo DHCP y no especificar una dirección IP, una máscara de red, un gateway o servidor DNS. El cliente recupera esta información desde el servidor DHCP. DHCP también es útil si un administrador desea cambiar las direcciones IP de muchos sistemas. En lugar de volver a configurar todos los sistemas, puede modificar un archivo de configuración DHCP en el servidor para establecer el nuevo conjunto de direcciones IP. Si los servidores DNS de una organización cambian, los cambios también se aplicarán en el servidor DHCP, no en todos los clientes DHCP. Una vez que se reinicie la red en los clientes (o rearranquen los clientes), se aplicarán los cambios.

Además, si un portátil o cualquier tipo de equipo móvil se configura para DHCP, podrá desplazarse entre distintas oficinas sin tener que volver a configurarlo, siempre y cuando cada oficina tenga un servidor DHCP que permita su conexión a la red.

18.2. Configuración de un servidor DHCP

Puede configurar un servidor DHCP mediante el archivo de configuración `/etc/dhcpd.conf`.

DHCP también usa el archivo `/var/lib/dhcp/dhcpd.leases` para almacenar la base de datos de arrendamiento de clientes. Consulte Sección 18.2.2 para más información.

18.2.1. Archivo de configuración

El primer paso al configurar un servidor DHCP es crear el archivo de configuración que almacena la información de red de los clientes. Se pueden declarar opciones globales para todos los clientes, o bien opciones para cada sistema cliente.

El archivo de configuración puede contener tabulaciones o líneas en blanco adicionales para facilitar el formato. Las palabras clave no distinguen entre mayúsculas y minúsculas, y las líneas que empiezan con una almohadilla o símbolo numeral (#) se consideran comentarios.

Hay dos tipos de esquemas DNS de actualización implementados actualmente — el modo de actualización DNS ad-hoc y el modo de actualización de interacción DHCP-DNS. Si y cuando estos dos son aceptados como parte del proceso estándar de IETF, habrá un tercer modo — el método estándar de actualización DNS. El servidor DHCP tiene que estar configurado para usar uno de estos dos tipos de actualización. La versión 3.0b2p111 y las versiones anteriores usaban el modo ad-hoc, pero ya no se usan. Si quiere conservar el mismo comportamiento, añada la siguiente línea al inicio del archivo de configuración: file:

```
ddns-update-style ad-hoc;
```

Para usar el modo recomendado, añada la siguiente línea al inicio del archivo de configuración:

```
ddns-update-style interim;
```

Lea la página man de `dhcpd.conf` para más detalles sobre los diferentes modos.

El archivo de configuración posee dos tipos de información:

- Parámetros — establece cómo se realiza una tarea, si debe llevarse a cabo una tarea o las opciones de configuración de red que se enviarán al cliente.
- Declaraciones — describen la topología de la red, describen los clientes, proporcionan direcciones para los clientes o aplican un grupo de parámetros a un grupo de declaraciones.

Algunos parámetros deben empezar con la palabra clave `option`. Algunas opciones configuran DHCP y los parámetros definen valores no opcionales o que controlan el comportamiento del servidor DHCP.

Los parámetros (incluidas las opciones) declarados antes de una sección encerrada entre paréntesis ({ }) se consideran parámetros globales. Los parámetros globales se aplican a todas las secciones situadas debajo de ellos.

Importante

Si cambia el archivo de configuración, los cambios no se aplicarán hasta reiniciar el demonio DHCP con el comando `service dhcpd restart`.

En Ejemplo 18-1, las opciones `routers`, `subnet-mask`, `domain-name`, `domain-name-servers`, y `time-offset` son usadas para cualquier sentencia `host` declarada debajo de ellas.

Como se muestra en el Ejemplo 18-1, puede declarar una `subnet`. Debe incluir una declaración `subnet` para cada subred en su red. Si no lo hace, el servidor DHCP no podrá arrancarse.

En este ejemplo, hay opciones globales para cada cliente DHCP en la subred y un `range` declarado. A los clientes se les asigna una dirección IP dentro del `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;

        option time-offset              -18000;     # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

Ejemplo 18-1. Ejemplo de declaración de Subred

Todas las subredes que comparten la misma red física deben especificarse dentro de una declaración `shared-network` como se muestra en Ejemplo 18-2. Los parámetros dentro de `shared-network` pero fuera del cerco de las declaraciones `subnet` se consideran parámetros globales. El nombre de `shared-network` debe ser el título descriptivo de la red, como, por ejemplo, test-lab, para describir todas las subredes en un entorno de laboratorio de pruebas.

```
shared-network name {
    option domain-name              "test.redhat.com";
    option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
    option routers                  192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

Ejemplo 18-2. Ejemplo de declaración de red compartida

Como se muestra en el Ejemplo 18-3, la declaración `group` puede utilizarse para aplicar parámetros globales a un grupo de declaraciones. Puede agrupar redes compartidas, subredes, hosts u otros grupos.

```
group {
   option routers                  192.168.1.254;
   option subnet-mask              255.255.255.0;

   option domain-name              "example.com";
   option domain-name-servers       192.168.1.1;

   option time-offset              -18000;     # Eastern Standard Time

   host apex {
      option host-name "apex.example.com";
      hardware ethernet 00:A0:78:8E:9E:AA;
      fixed-address 192.168.1.4;
   }

   host raleigh {
      option host-name "raleigh.example.com";
      hardware ethernet 00:A1:DD:74:C3:F2;
      fixed-address 192.168.1.6;
   }
}
```

Ejemplo 18-3. Declaración de Group

Para configurar un servidor DHCP que arrenda una dirección IP dinámica a un sistema dentro de una subred, modifique Ejemplo 18-4 con sus valores. Declara un tiempo de arrendamiento por defecto, un tiempo de arrendamiento máximo y los valores de configuración de red para los clientes. Este ejemplo asigna una dirección IP en el `range` 192.168.1.10 y 192.168.1.100 a los sistemas clientes.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.10 192.168.1.100;
}
```

Ejemplo 18-4. Parámetro Range (Rango)

Para asignar una dirección IP a un cliente según la dirección MAC de la tarjeta de interfaz de red, use el parámetro `hardware ethernet` dentro de la declaración `host`. Como se muestra en el Ejemplo 18-5, la declaración `host apex` especifica que la interfaz de red con una dirección MAC 00:A0:78:8E:9E:AA siempre recibe la dirección IP 192.168.1.4.

Tenga en cuenta que también puede usar el parámetro opcional `host-name` para asignar un nombre host al cliente.

```
host apex {
   option host-name "apex.example.com";
   hardware ethernet 00:A0:78:8E:9E:AA;
   fixed-address 192.168.1.4;
}
```

Ejemplo 18-5. Ejemplo de dirección IP estática con DHCP

Sugerencia

Puede usar el archivo de configuración de ejemplo de Red Hat Linux 9 como punto de partida y, a continuación, agregarle opciones de configuración personalizadas. Cópielo en la ubicación adecuada con el comando

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(donde <*version-number*> es la versión de DHCP que está usando).

Para obtener una lista completa de sentencias de opciones e información relacionada, consulte la página del manual de dhcp-options.

18.2.2. Base de datos de arrendamiento

En el servidor DHCP, el archivo `/var/lib/dhcp/dhcpd.leases` almacena la base de datos de arrendamiento del cliente DHCP. Este archivo no debe modificarse manualmente. La información sobre arrendamiento de DHCP de cada dirección IP asignada recientemente se almacena de modo automático en la base de datos de arrendamiento. La información incluye la longitud del arrendamiento, a quién se ha asignado la dirección IP, las fechas iniciales y finales de la renta, y la dirección MAC de la tarjeta de interfaz de red utilizada para recuperar el arrendamiento.

Todas las horas de la base de datos de arrendamiento se expresan según GMT, no con la hora local.

La base de datos de arrendamiento se crea nuevamente de vez en cuando para que su tamaño no sea excesivo. En primer lugar, se guardan todas las concesiones conocidas en una base de datos de renta temporal. El archivo `dhcpd.leases` es renombrado a `dhcpd.leases~`, y la base de datos temporal se registra en `dhcpd.leases`.

El demonio DHCP puede borrarse porque, de otro modo, el sistema puede quedarse inestable después de cambiar el nombre de la base de datos por el archivo de copia de seguridad, antes de escribir el nuevo archivo. Si ocurre esto, no se necesitará ningún archivo `dhcpd.leases` para arrancar el servicio. No cree un nuevo archivo de arrendamiento si ocurre esto. Si lo hace, se perderán las versiones anteriores del arrendamiento y podrían generarse problemas. La solución correcta consiste en cambiar el nombre del archivo de copia de seguridad `dhcpd.leases~` de nuevo a `dhcpd.leases` y, a continuación, arrancar el demonio.

18.2.3. Arranque y parada del servidor

Importante

Antes de arrancar por primera vez el servidor DHCP, asegúrese de que existe un archivo `dhcpd.leases` para que no falle el arranque. Use el comando `touch /var/lib/dhcp/dhcpd.leases` para crear el archivo en caso de que no exista.

Para arrancar el servicio DHCP, use el comando `/sbin/service dhcpd start`. Para detener el servidor DHCP, use el comando `/sbin/service dhcpd stop`. Si desea que el demonio se arranque automáticamente en el momento de arranque, consulte el Capítulo 14 para obtener información sobre cómo administrar los servicios.

Si tiene más de una interfaz de red conectada al sistema, pero sólo desea que el servidor DHCP arranque en una de las interfaces, puede configurar el servidor DHCP para que sólo arranque en ese dispositivo. En `/etc/sysconfig/dhcpd`, agregue el nombre de la interfaz a la lista de `DHCPDARGS`:

```
# Command line options here
DHCPDARGS=eth0
```

Esto es útil si tiene una máquina firewall con dos tarjetas de red. Se puede configurar una tarjeta de red como cliente DHCP para recuperar una dirección IP en Internet y la otra tarjeta de red puede utilizarse como servidor DHCP para la red interna detrás del firewall. Su sistema será más seguro si especifica la tarjeta de red conectada a la red interna ya que los usuarios no pueden conectarse al demonio vía Internet.

Otras opciones de línea de comandos que pueden ser especificadas en `/etc/sysconfig/dhcpd` incluyen:

- `-p <portnum>` — Especifique el número de puerto udp en el que dhcpd debería escuchar. Está predeterminado 67. El servidor DHCP transmite las respuestas al cliente a un puerto con un número más grande que el puerto udp especificado. Por ejemplo, si acepta el puerto predeterminado, 67, el servidor escucha en el puerto 67 y responde en el puerto 68. Si especifica un puerto en este momento y usa el agente de transmisión, debería especificar el mismo puerto en el que el agente debería escuchar. Consulte la Sección 18.2.4 para más detalles.
- `-f` — Ejecutar el demonio como un proceso de en primer plano. Casi siempre se usa para la depuración.
- `-d` — Registrar el demonio del servidor DCHP en el descriptor de errores estándar. Casi siempre se usa para el depurado. Si no está especificado, el registro será escrito en `/var/log/messages`.

- `-cf filename` — Especifica la localización del archivo de configuración. La configuración por defecto es `/etc/dhcpd.conf`.
- `-lf filename` — Especifica la ubicación de la base de datos de arrendamiento. Si ya existe el archivo de la base de datos de arrendamiento, es muy importante que el mismo archivo sea usado cada vez que el servidor DHCP se inicia. Se le recomienda que use esta opción sólo para propósitos de depuración en máquinas que no estén en producción. La ubicación por defecto es `/var/lib/dhcp/dhcpd.leases`.
- `-q` — No imprima el mensaje de copyright entero cuando inicie el demonio.

18.2.4. Agente de transmisión DHCP

El agente de transmisión DHCP (`dhcrelay`) le permite transmitir las peticiones DHCP y BOOTP desde una subred sin un servidor DHCP para uno o más servidores en otras subredes.

Cuando un cliente DHCP pide información, el agente de transmisión DHCP reenvía la petición a la lista de servidores DHCP especificada cuando se inicia el agente de transmisión DHCP. Cuando un servidor DHCP devuelve una respuesta, la respuesta puede ser broadcast o unicast en la red que ha enviado la petición original.

El agente de transmisión escucha las peticiones DHCP en todas las interfaces a menos que las interfaces estén especificadas en `/etc/sysconfig/dhcrelay` con la directiva `INTERFACES`.

Para iniciar el agente de transmisión DHCP, use el comando `service dhcrelay start`.

18.3. Configuración de un cliente DHCP

El primer paso al configurar un cliente DHCP es asegurarse de que el kernel reconoce la tarjeta de la interfaz de red. La mayoría de las tarjetas se reconocen durante el proceso de instalación y el sistema se configura para utilizar el módulo de kernel correcto para la tarjeta. Si instala una tarjeta después de la instalación, la aplicación **Kudzu** [1] debería reconocerla y solicitarle que configure el módulo del kernel correspondiente para ésta. Asegúrese de comprobar la Lista de compatibilidad de hardware de Red Hat Linux disponible en http://hardware.redhat.com/hcl/. Si el programa de instalación o la aplicación **Kudzu** no configuran la tarjeta de red y sabe qué módulo de kernel debe cargarse, consulte el Capítulo 31 para obtener más información sobre la carga de módulos de kernel.

Para configurar un cliente DHCP manualmente, debe modificar el archivo `/etc/sysconfig/network` para habilitar el uso del archivo de configuración y de red en los dispositivos de red del directorio `/etc/sysconfig/network-scripts`. En este directorio, cada dispositivo debería tener un archivo de configuración llamado `ifcfg-eth0` donde `eth0` es el nombre del dispositivo de red.

El archivo `/etc/sysconfig/network` debería contener la línea siguiente:

```
NETWORKING=yes
```

Puede disponer de más información en este archivo. Sólo debe asegurarse de que la variable `NETWORKING` esté colocada a `yes` si quiere que se inicie la red en el momento de arranque.

El archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` debería contener las líneas siguientes:

```
DEVICE=eth0
```

1. **Kudzu** es una herramienta de prueba del hardware que se ejecuta en el momento de arrancar el sistema para determinar qué hardware ha sido añadido o eliminado del sistema.

```
BOOTPROTO=dhcp
ONBOOT=yes
```

Necesita un archivo de configuración para cada dispositivo que desee configurar para el uso de DHCP.

Si prefiere usar una interfaz gráfica para configurar el cliente DHCP, consulte el Capítulo 12 para obtener más información sobre **Herramienta de administración de redes** para configurar la interfaz de red para usar DHCP.

18.4. Recursos adicionales

Para obtener más información sobre otras opciones, consulte los recursos siguientes.

18.4.1. Documentación instalada

- Página del manual `dhcpd` — describe cómo funciona el demonio DHCP
- Página del manual `dhcpd.conf` — explica cómo configurar el archivo de configuración de DHCP; incluye algunos ejemplos
- Página del manual `dhcpd.leases` — explica cómo configurar el archivo de arrendamiento DHCP; incluye también algunos ejemplos
- Página del manual `dhcp-options` — explica la sintaxis para la declaración de opciones DHCP en `dhcpd.conf`; incluye ejemplos
- Página del manual `dhcrelay` — explica el Agente de transmisión DHCP y sus opciones de configuración.

Capítulo 19.

Configuración del Servidor Apache HTTP

En Red Hat Linux 8.0, el Servidor Apache HTTP fué actualizado a la versión 2.0, la cual tiene opciones diferentes. También se le ha dado otro nombre al paquete, es decir, ahora se llama `httpd`. Si desea migrar de un fichero de configuración existente a mano, consulte el manual de la migración en `/usr/share/doc/httpd-<ver>/migration.html` o el *Manual de referencia de Red Hat Linux* para más detalles.

Si ha configurado el Servidor Apache HTTP con la **Herramienta de configuración de HTTP** en anteriores versiones de Red Hat Linux y después ha llevado a cabo una actualización, puede usar la aplicación para migrar el fichero de configuración al nuevo formato de la versión 2.0. Arranque la **Herramienta de configuración de HTTP**, haga los cambios y sálvelo. El fichero de configuración salvado será compatible con la versión 2.0.

La **Herramienta de configuración de HTTP** le permite configurar el fichero de configuración `/etc/httpd/conf/httpd.conf` para su Servidor Apache HTTP. No use los antiguos ficheros de configuración `srm.conf` o `access.conf`; déjelos vacíos. Podrá configurar las directivas de Apache tales como hosts virtuales, atributos de registro y número máximo de conexiones a través de la interfaz gráfica.

Sólo se pueden configurar con la **Herramienta de configuración de HTTP** aquellos módulos que estén incluídos en el paquete de Red Hat Linux. Si se instalan otros módulos, no se podrá hacer usando esta herramienta.

Los paquetes RPM `httpd` y `redhat-config-httpd` necesitan estar instalados para usar la **Herramienta de configuración de HTTP**. También se requiere el sistema X Window y acceso como root. Para iniciar la aplicación, vaya al **Botón de Menú principal => Configuración del sistema => Configuración de servidores => Servidor HTTP** o escriba el comando `redhat-config-httpd` en el intérprete de comandos (por ejemplo, en un terminal XTerm o GNOME).

Atención

No modifique el fichero el fichero de configuración de Apache `/etc/httpd/conf/httpd.conf` manualmente si desea utilizar esta herramienta. La **Herramienta de configuración de HTTP** crea este fichero después de que haya grabado los cambios y haya salido del programa. Si desea añadir módulos u opciones que no se encuentren en la **Herramienta de configuración de HTTP**, no podrá usarla.

Los pasos que debe seguir para configurar el servidor Servidor Apache HTTP con la **Herramienta de configuración de HTTP** son los siguientes:

1. Configure las posiciones básicas que se encuentran en la pestaña **Principal**.
2. Haga click en **Hosts Virtuales** y configure las opciones predeterminadas.
3. Si desea servir a más de una URL, añada las máquinas virtuales adicionales.
4. Configure las posiciones del servidor que se encuentran en **Servidor**.
5. Configure las conexiones en **Mejoras de las prestaciones**.
6. Copie todos los ficheros necesarios a los directorios DocumentRoot y cgi-bin y grabe las posiciones en la **Herramienta de configuración de HTTP**.
7. Copie todos los ficheros necesarios a los directorios `DocumentRoot` y `cgi-bin`.

8. Salga de la aplicación y seleccione guardar sus configuraciones.

19.1. Configuraciones básicas

Use la pestaña **Principal** para establecer las configuraciones básicas.

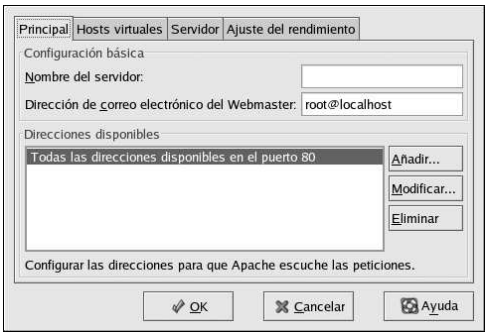

Figura 19-1. Configuraciones básicas

Introduzca el nombre del dominio completo que tenga derecho a usar en **Nombre del servidor**. Esta opción corresponde a la directiva `ServerName` en `httpd.conf`. La directiva `ServerName` establece el nombre de la máquina del servidor de web. Se usa cuando se crean redireccionamientos de URLs. Si usted no introduce el Nombre del servidor, Apache intentará resolverlo desde una dirección IP del sistema. El Nombre del servidor no tiene porqué ser igual al nombre DNS del servidor. Por ejemplo, a lo mejor el nombre del servidor es www.su_dominio.com cuando el verdadero nombre DNS es en realidad foo_su__dominio.com.

Introduzca la dirección de correo electrónico de la persona que mantiene el servidor web en **Dirección de correo electrónico del Webmaster**. Esta opción corresponde a la directiva `ServerAdmin` en `httpd.conf`. Si configura la página de errores del servidor para que contenga una dirección de correo electrónico, dicha dirección se usará para que los usarios puedan informar sobre algún problema que tengan mandando un correo electrónico al administrador del servidor. El valor predeterminado es root@localhost.

Use el área **Direcciones disponibles** para definir los puertos de escucha del servidor Apache. Esta opción corresponde a la directiva `Listen` en `httpd.conf`. El valor predeterminado de escucha para Servidor Apache HTTP es el puerto 80 para las comunicaciones Web no-seguras.

Haga click en el botón **Añadir** para definir puertos de escucha adicionales. Aparecerá una ventana en la Figura 19-2. Puede tanto elegir la opción de **Escuchar todas las direcciones** para escuchar todas las direcciones IP del puerto definido o bien especificar la dirección en la que el servidor aceptará las conexiones en el campo **Direcciones**. Especifique sólo una dirección IP por número de puerto. Si quiere especificar más de una dirección con el mismo número de puerto, cree una entrada para cada una de ellas. Si esto es posible, utilice una única dirección IP en vez de un nombre de dominio para así evitar que falle la búsqueda del DNS. Consulte http://httpd.apache.org/docs-2.0/dns-caveats.html para más información sobre *Problemas relacionados con DNS y Apache*.

Si introduce un asterisco (*) en el campo **Direcciones** equivaldrá a elegir la opción **Escuchar todas las direcciones**. Haga click en el botón **Modificar** en el recuadro de **Direcciones disponibles** muestra la misma ventana que el botón **Añadir** excepto los campos de la entrada seleccionada. Para borrar una entrada, pulse el botón **Eliminar**.

Sugerencia

Si configuró el servidor para escuchar en el puerto 1024, deberá ser root para arrancarlo. Para el puerto 1024 y superiores, se puede arrancar `httpd` como un usuario normal.

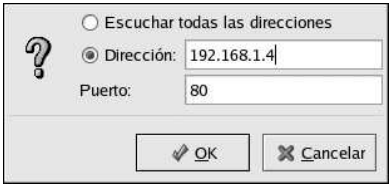

Figura 19-2. Direcciones disponibles

19.2. Configuraciones predeterminadas

Después de definir el **Nombre del servidor**, la **Dirección de correo electrónico del Webmaster**, y las **Direcciones disponibles**, haga click en la pestaña **Hosts virtuales** y click en el botón **Modificar configuraciones predeterminadas**. Aparecerá la ventana mostrada en la Figura 19-3. Configure los valores por defecto para su servidor Web en esta ventana. Si agrega un virtual host, las configuraciones que establezca para el servidor virtual tendrán precedencia para ese host. Para una directiva que no esté definida dentro de las configuraciones del host virtual, se usarán los valores predeterminados.

19.2.1. Configuración del sitio

Los valores predeterminados de **Lista de búsqueda de página de directorio** y **Páginas de error**, funcionarán para la mayoría de los servidores. Si no está seguro de estos valores, no los modifique.

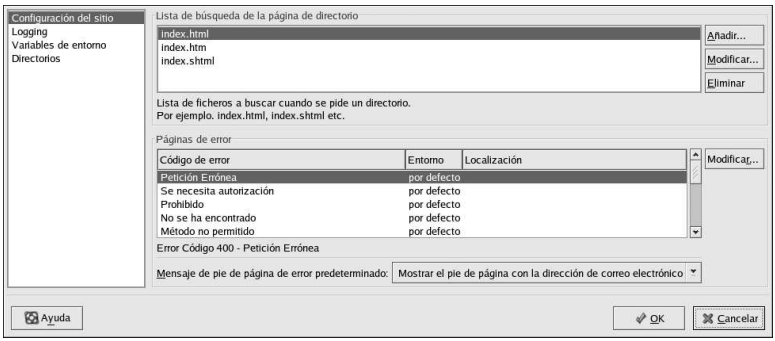

Figura 19-3. Configuración del sitio

Las entradas que aparecen en la **Lista de búqueda de página de directorio** definen la directiva `DirectoryIndex`. El `DirectoryIndex` es la página predeterminada que el servidor da a un usuario que pide el índice de un directorio escribiendo la barra inclinada (/) al final del nombre del directorio.

Por ejemplo, cuando un usuario pide la página http://*www.ejemplo.com/este_directorio/*, el servidor le da bien sea la página `DirectoryIndex` si existe o la lista de directorios generada por el servidor. El servidor intentará encontrar uno de los ficheros que se encuentran en la lista de la directiva `DirectoryIndex` y le entregará el primero que encuentre. Si no encuentra ninguno de los ficheros y si ese directorio contiene los `Índices de opciones`, el servidor generará y devolverá una lista, en formato HTML de los subdirectorios y ficheros de ese directorio.

Use la sección **Código de Error** para configurar Servidor Apache HTTP a que redireccione el cliente a un URL local o externo en el evento de un problema o error. Esta opción responde a la directiva `ErrorDocument`. Si ocurre un problema o error cuando un cliente intenta conectarse al Servidor Apache HTTP, la acción por defecto es mostrar un mensaje corto de error como se muestra en la columna **Código de Error**. Para ignorar esta configuración por defecto, seleccione el código del error y haga click en **Modificar**. Seleccione **Predeterminado** para desplegar un mensaje corto de error. Escoja **URL** para redirigir el cliente a un URL externo e introduzca un URL completo incluyendo http:// en el campo **Ubicación**. Seleccione **Archivo** para redirigir el cliente a un URL interno e introduzca la ubicación de un archivo bajo el documento raíz para el servidor Web. La ubicación debe comenzar con un símbolo de barra oblícua (/) y ser relativo al Documento raíz (Document Root).

Por ejemplo, para redirigir un código de error 404 Not Found a una página web que usted ha creado en un archivo llamado `404.html`, copie `404.html` a *`DocumentRoot`*`/errors/404.html`. En este caso, *`DocumentRoot`* es el directorio del documento raíz que ha definido (el valor por defecto es `/var/www/html`). Luego, elija **Archivo** como el Comportamiento para el código de error **404 - Not Found** e introduzca `/errors/404.html` como la **Ubicación**.

Desde el menú **Pie de página de Error por defecto**, escoja una de las siguientes opciones:

- **Mostrar el pie de página con la dirección de correo electrónico** — Esta opción muestra el pie de página predeterminado en todas las páginas de error junto con la dirección de correo electrónico del encargado del sitio web especificado por la directiva `ServerAdmin`. Para mayor información sobre la configuración de la directiva `ServerAdmin` consulte la Sección 19.3.1.1.
- **Muestra el pie de página** — Esta opción le muestra el pie de página predeterminado en todas las páginas de error.
- **Ningún pie de página** — No muestra el pie de página.

19.2.2. Registro

Por defecto, el servidor escribe el registro de transferencias en el fichero `/var/log/httpd/access_log` y el registro de errores en el fichero `/var/log/httpd/error_log`.

El registro de transferencia contiene una lista de todos los intentos de accesar el servidor Web. Registra la dirección IP del cliente que está intentando conectarse, la fecha y hora del intento, y el archivo en el servidor Web que está tratando de recuperar. Introduzca el nombre de la ruta y el archivo en el cual almacenar la información. Si la ruta y el nombre del archivo no comienzan con una barra oblícua (/), la ruta es relativa al directorio raíz del servidor. Esta opción corresponde a la directiva `TransferLog`.

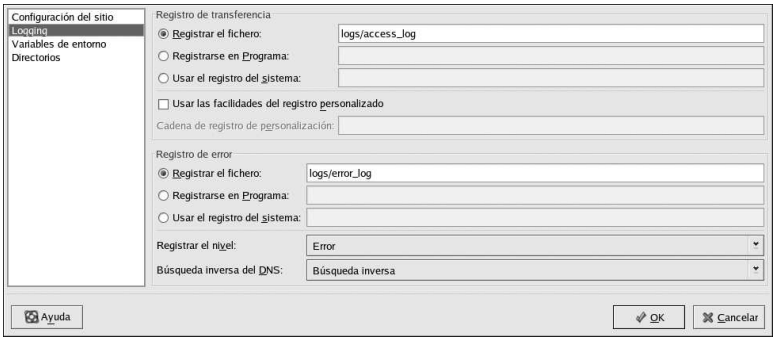

Figura 19-4. Registro

Puede configurar un registro con formato personalizado chequeando **Usar las facilidades de registro personalizado** e introduciendo una cadena personalizada en el campo **Cadena de registro personalizada**. Esto configura la directiva `LogFormat`. Para mayor información sobre los detalles del formato de la directiva consulte http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats.

El registro de errores contiene la lista de los errores que ocurren en el servidor. Introduzca el nombre del recorrido y del fichero en el que quiera guardar estos datos. Si ambos no comienzan con (/), se entenderá que el recorrido pertenece al directorio raíz del servidor tal y como se configuró. Esta opción corresponde a la directiva `ErrorLog`.

Use el menú **Registrar el nivel** para configurar que niveles de detalles tendrán los mensajes de error en el registro. Se puede establecer (de menor a mayor cantidad de detalles) a emergencias, alertas, críticos, error, advertencias, notificaciones, informes o depuración. Esta opción corresponde a la directiva `LogLevel` en http://httpd.apache.org/docs-2.0/mod/core.html#loglevel.

El valor escogido en el menú **Búsqueda inversa del DNS** define la directiva `HostnameLookups` en http://httpd.apache.org/docs-2.0/mod/core.html#hostnamelookups. Si escoge **Ninguna búsqueda inversa** se desactiva el valor, si escoge **Búsqueda inversa** el valor está activado y si escoge **Doble búsqueda inversa** éste se duplica.

Al elegir la opción **Búsqueda inversa**, el servidor resuelve automáticamente la dirección IP para cada conexión que requiera un documento del servidor web. Esto quiere decir que el servidor lleva a cabo más de una conexión a la DNS hasta encontrar el nombre de la máquina a la que le corresponda una dirección IP determinada.

Si elige la opción **Doble búsqueda inversa**, el servidor realizará un DNS inverso doble. En otras palabras, después de una búsqueda inversa, hace una normal al resultado. Al menos una de las direcciones encontrada en esta segunda búsqueda debe coincidir con la primera.

Generalmente, esta opción debería de estar en **Ninguna búsqueda inversa** porque sino se sobrecarga al servidor y disminuye el ritmo de trabajo. Si su servidor tiene mucha carga, al tratar de realizar estas búsquedas, los efectos serán bastante notables.

Tanto las búsquedas inversas como las dobles son también un problema para la Internet en general. Todas las conexiones individuales para buscar cada máquina se suman. Por tanto, para beneficio de su propio servidor Web, así como también para beneficio de la Internet, debería dejar esta opción en **Ninguna búsqueda inversa**.

19.2.3. Variables de entorno

Algunas veces es necesario modificar las variables del entorno para scripts CGI o páginas server-side include (SSI). El Servidor Apache HTTP puede usar el módulo `mod_env` para configurar las variables

del ambiente que son pasadas a los scripts CGI y a las páginas SSI. Use la página **Variables de entorno** para configurar las directivas para este modulo.

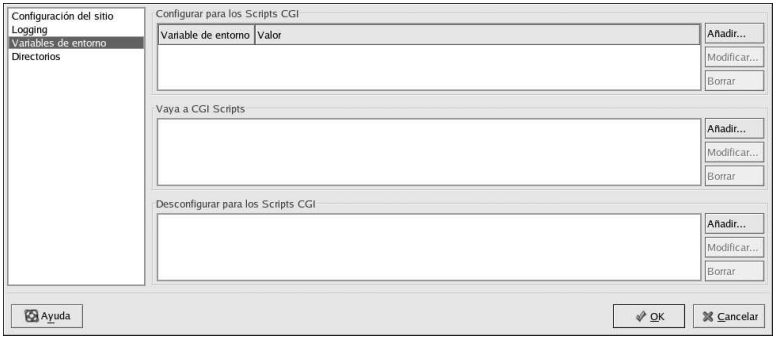

Figura 19-5. Variables de entorno

Use la sección **Configuración de los Scripts CGI** para establecer una variable de entorno que se pasa a los scripts CGI y a las páginas SSI. Por ejemplo, para establecer la variable de entorno `MAXNUM` en `50`, haga click en el botón **Añadir** dentro de la sección **Configuración de los Scripts CGI** como muestra la Sección 19.2.3 y teclee **`MAXNUM`** en el campo **Variables de entorno** y **`50`** en el campo **Valor a configurar:**. Haga click en **OK**. La sección **Configuración de los Scripts CGI** configura la directiva `SetEnv`.

Use la sección **Acceder a scripts CGI** para pasar el valor de una variable de entorno cuando el servidor fue arrancado para los scripts CGI. Para ver la variable teclee el comando `env` en la línea de comandos de la shell. Haga click en **Añadir** en la sección **Acceder a scripts CGI** e introduzca el nombre de la variable de entorno que aparece en la ventana de diálogo. Después haga click en **OK** para agregarlo a la lista. La sección **Acceder a Scripts CGI** configura la directiva `PassEnv` .

Si desea eliminar el valor de la variable de entorno para que no pase ni al script CGI ni a las páginas SSI, use la sección **Quitar configuración para scripts CGI**. Haga click en **Añadir** en la sección **Elimina la configuración de los Scripts CGI**, e introduzca el nombre de la variable de entorno que ha decidido eliminar. Haga click en **OK** para añadirlo a la lista. Esta opción corresponde a la directiva `UnsetEnv`.

Para modificar cualquiera de estas variables de entorno, selecciónela desde la lista y haga click en el botón **Modificar**. Para eliminar una entrada de la lista, selecciónela y haga click en el correspondiente botón **Eliminar**.

Para saber más sobre las variables de entorno en el Servidor Apache HTTP, refiérase a:

`http://httpd.apache.org/docs-2.0/env.html`

19.2.4. Directorios

Use la página **Directorios** para configurar opciones para directorios específicos. Esto corresponde a la directiva `<Directory>`.

Figura 19-6. Directorios

Haga click en el botón **Modificar** que se encuentra en la esquina superior derecha para configurar las **Opciones de directorio por defecto** para todos los directorios que no están especificados en la lista de **Directorio**. Las opciones que elija se encuentran listadas como la directiva Opciones dentro de `<Directory>`. Puede configurar las opciones siguientes:

- **ExecCGI** — Permite la ejecución de los scripts CGI. Los scripts no se ejecutan si no elige esta opción.
- **FollowSymLinks** — Permite que se sigan enlaces simbólicos.
- **Includes** — Permite las inclusiones en el servidor (SSI).
- **IncludesNOEXEC** — Permite las inclusiones en el servidor pero anula los comandos `#exec` y `#include` en los scripts CGI.
- **Indexes** — Muestra una lista formateada de los contenidos de un directorio si la opción `DirectoryIndex` (como por ejemplo `index.html`) existe en el directorio pedido.
- **Multiview** — Soporta las visualizaciones múltiples de los contenidos; esta opción no está activada por defecto.
- **SymLinksIfOwnerMatch** — Permite seguir un enlace simbólico solamente si el fichero o el directorio en cuestión tienen el mismo propietario que el enlace.

Para especificar las opciones para directorios determinados, haga click en **Añadir** que se encuentra al lado de la lista **Directorio**. Aparecerá la ventana que se muestra en la Figura 19-7. Introduzca el directorio para configurarlo en el campo **Directorio** que se encuentra en la parte de abajo de la ventana. Seleccione las opciones de la lista de la derecha y configure la directiva `Order` con las opciones de la izquierda. Esta directiva controla el orden según el cual se permiten o se deniegan las directivas. En los campos **Permitir los hosts desde** y **Negar los hosts desde:**, puede especificar uno de las siguientes:

- Permitir todas los hosts — Escriba **`all`** para permitir el acceso a todas la máquinas.
- Nombre parcial de dominio — Permite todas las máquinas cuyos nombres coincidan o terminen con una cadena determinado.
- Dirección IP completa — Permite el acceso a una determinada dirección IP.
- Una subred — Tal como **`192.168.1.0/255.255.255.0`**
- Una especificación CIDR de red — como por ejemplo **`10.3.0.0/16`**

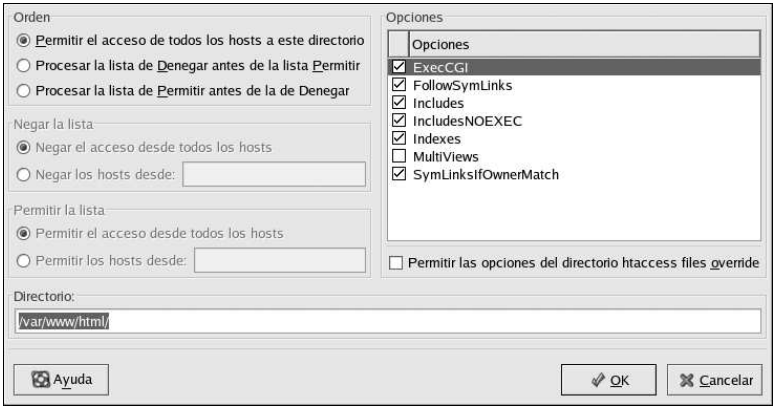

Figura 19-7. Configuraciones del directorio

Si marca **Permitir que los archivos .htaccess pasen por encima de las opciones del directorio**, las directivas de configuración en el archivo `.htaccess` toman precedencia.

19.3. Configuraciones de las máquinas virtuales

Puede usar la **Herramienta de configuración de HTTP** para configurar máquinas virtuales. Los hosts virtuales le permiten ejecutar diferentes servidores para direcciones IP diferentes, nombres de hosts diferentes o puertos diferentes en la misma máquina. Por ejemplo, puede correr el sitio web para http://www.example.com y http://www.anotherexample.com en el mismo servidor Web usando hosts virtuales. Esta opción corresponde a la directiva <VirtualHost> para el host virtual por defecto y hosts vistuales basados en IP. Corresponde a la directiva `<NameVirtualHost>` para un host virtual basado en nombre.

Las directivas establecidas para una máquina virtual son sólo aplicables a ésta. Si se establece una directiva con alcance de servidor usando el botón **Modificar las configuraciones por defecto** pero no se definen dentro de las configuraciones de la máquina virtual, se usará el valor predeterminadod. Por ejemplo, se puede definir una **Dirección de correo electrónico del webmaster** en la pestaña **Principal** y no definir las direcciones de correo electrónico individuales para cada una de las máquinas virtuales.

La **Herramienta de configuración de HTTP** incluye una máquina virtual predeterminada como se muestra en la Figura 19-8.

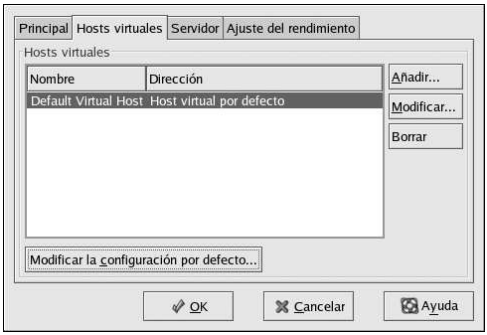

Figura 19-8. Máquinas virtuales

http://httpd.apache.org/docs-2.0/vhosts/ y la documentación de Servidor Apache HTTP de su máquina le proporcionan más información sobre los hosts virtuales.

19.3.1. Añadir y modificar máquinas virtuales

Para añadir una máquina virtual, haga click en la pestaña **Hosts virtuales** y presione el botón **Añadir**. También puede modificar una máquina virtual seleccionando en la lista y después haciendo click en **Modificar**.

19.3.1.1. Opciones generales

Las configuraciones **Opciones generales** sólo se aplican a la máquina virtual que esté configurando. Escriba el nombre de la máquina virtual en el área de texto **Nombre del Host Virtual**. Este nombre es usado por la **Herramienta de configuración de HTTP** para distinguir entre hosts virtuales.

Establezca el valor del **Directorio raíz de documentos** en el directorio que contenga el documento raíz (tal como index.html) para la máquina virtual. Esta opción corresponde a la directiva `DocumentRoot` dentro de `<VirtualHost>`. Antes de Red Hat Linux 7, el Servidor Apache HTTP proporcionado con Red Hat Linux usaba `/home/httpd/html` como el `DocumentRoot`. En Red Hat Linux 9, sin embargo, el `DocumentRoot` predeterminado es `/var/www/html`.

La **Dirección email del Webmaster** corresponde a la directiva `ServerAdmin` dentro de la directiva `VirtualHost`. Esta dirección de correo es usada en el pie de las páginas de errores si selecciona mostrar un pie de página con una dirección de correo en las páginas de errores.

En la sección **Información del Host**, seleccione **Host virtual por defecto**, **Host virtual basado en IP**, o **Host virtual basado en el nombre**.

Host virtual por defecto

Sólo debe configurar una máqina virtual predeterminada (recuerde que hay una configurada por defecto). Las configuraciones de la máquina virtual predeterminada se usan cuando la dirección IP requerida no aparece explícitamente en la lista de otra máquina virtual. Si no existe ninguna máquina virtual por defecto definida, se usan las configuraciones del servidor principal.

Host virtual basado en IP

Si selecciona **Host virtual basado en IP**, aparecerá una ventana para configurar la directiva <VirtualHost> basada en la dirección IP del servidor. Especifique esta dirección IP en el campo **Dirección IP**. Para especificar más de una dirección IP, separe cada dirección IP con espacios. Para especificar un puerto, use la sintaxis *`Dirección IP:Puerto`*. Use :* para configurar

todos los puertos para la dirección IP. Especifique el nombre del host para la máquina virtual en el campo **Nombre de servidor Host**.

Host virtual basado en el nombre

Si escoge la opción **Host virtual basado en el nombre**, aparecerá una pantalla para configurar la directiva `NameVirtualHost` basada en el nombre de la máquina del servidor. Especifique la dirección IP en el campo **Dirección IP**. Para especificar más de una dirección IP, sepárelas con espacios. Para un puerto, use la sintaxis *`Dirección IP:Puerto`*. Use :* para configurar todos los puertos de esa dirección IP. Especifique el nombre de la máquina para la máquina virtual en el campo **Nombre del servidor Host**. En la sección **Aliases** haga click en **Añadir** para agregar un alias al nombre de la máquina. Añadir un alias aquí agrega una directiva `ServerAlias` dentro de la directiva `NameVirtualHost`.

19.3.1.2. SSL

Nota

No puede usar host virtuales basados en nombre con SSL, porque el 'handshake' de SSL (cuando el navegador acepta el certificado del servidor web seguro) tiene lugar antes de que se solicite una página en HTTP la cual identifica la apropiada máquina virtual basada en el nombre. Si quiere usar máquinas de este tipo, tendrá que utilizar un servidor de web no seguro.

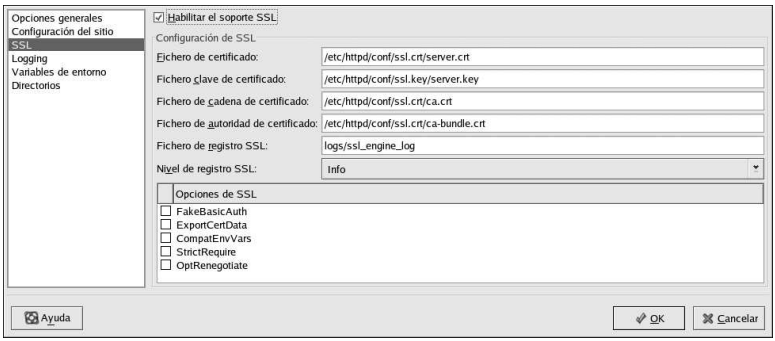

Figura 19-9. Soporte SSL

Si un servidor Servidor Apache HTTP no está configurado con el soporte SSL, las comunicaciones entre un Servidor Apache HTTP y sus clientes no estará encriptada. Esto es apropiado para los sitios web que no contengan información confidencial. Por ejemplo, un sitio "open source" que se encarga de distribuir software y documentación no necesita comunicaciones seguras cosa que no ocurre cuando se trata de un sitio que se encarga del comercio electrónico el cual necesita el soporte SSL para el manejo de información sobre tarjetas de crédito, por ejemplo. En este caso se requiere el soporte Apache SSL para encriptar las comunicaciones. Al activar el soporte Apache SSL se habilita el uso del módulo de seguridad `mod_ssl`. Para activarlo a través de **Herramienta de configuración de HTTP** debe permitir el acceso a través del puerto 443 bajo la pestaña **Principal => Direcciones disponibles**. Consulte la Sección 19.1 para más detalles. Luego, seleccione el nombre del host virtual en la pestaña **Hosts Virtuales**, haga click en **Modificar**, seleccione **SSL** desde el menú del lado izquierdo y marque

la opción **Habilitar el soporte SSL** como se muestra en Figura 19-9. La sección **Configuración SSL** está pre-configurada con el certificado digital. El certificado digital proporciona la validación para su servidor Web seguro e identifica el servidor seguro a los navegadores clientes. Tiene que comprar su propio certificado digital. No utilice el que viene con Red Hat Linux para su sitio Web. Para mayor información sobre cómo comprar un certificado digital aprobado por la CA, consulte el Capítulo 20.

19.3.1.3. Opciones adicionales de los host virtuales

Las opciones **Configuración del sitio**, **Variables de entorno**, y **Directorios** para las máquinas virtuales son las mismas directivas que estableció cuando presionó el botón **Modificar la configuración por defecto**, excepto que las opciones aquí establecidas son para cada una de las máquinas virtuales que está configurando. Consulte la Sección 19.2 para más detalles sobre estas opciones.

19.4. Propiedades del servidor

La pestaña **Servidor** le permite configurar las propiedades básicas. Las propiedades por defecto para estas opciones son apropiadas para la mayoria de los casos.

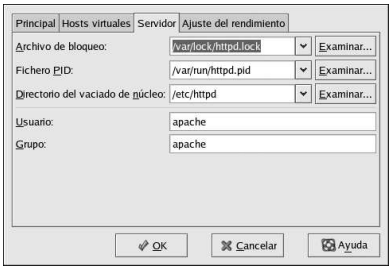

Figura 19-10. Configuración del servidor

El valor **Archivo de bloqueo** corresponde a la directiva `LockFile`. Esta directiva establece el recorrido hacia el archivo de bloqueo que se utiliza cuando se compila el servidor con USE_FCNTL_SERIALIZED_ACCEPT o con USE_FLOCK_SERIALIZED_ACCEPT. Se debe almacenar en un disco local. Este valor no se debe de cambiar a no ser que el directorio `logs` esté localizado en la compartición NFS. Si fuese este el caso, se debería cambiar el valor predeterminado a un disco local y a un directorio que sólo se pueda leer si se es root.

El valor del **Archivo PID** corresponde a la directiva `PidFile`. Esta directiva establece el fichero en el que el servidor graba sus procesos ID (pid). Este fichero se puede leer sólo si se es root. En la mayoría de los casos, se debería de dejar a su valor predeterminado.

El valor **Directorio de volcado del núcleo** corresponde a la directiva `CoreDumpDirectory`. El Servidor Apache HTTP intenta cambiarse a este directorio antes de volcar el núcleo. El valor predeterminado es el `ServerRoot`. Sin embargo, si el usuario no puede escribir en este directorio, entonces el volcado del núcleo no se puede escribir. Cambie este valor a un directorio que se pueda escribir por el usuario, si desea escribir los vaciados de núcleo en el disco para propósitos de depuración.

El valor **Usuario** corresponde a la directiva `User`. Establece el userid que utiliza el servidor para responder a las peticiones. Las configuraciones del usuario determinan el acceso del servidor. Todo

fichero al que el usuario no tenga acceso será también inaccesible a los visitantes del sitio web. El valor predeterminado para `User` es apache.

El usuario debe de tener sólo privilegios de tal manera que pueda acceder a ficheros que supuestamente puede ver el resto de los usuarios. El usuario es también el propietario de cualquier proceso CGI distribuido por el servidor. El usuario no debería tener permitido ejecutar ningún código cuyo fin no sea responder a las peticiones HTTP.

Aviso

A menos que no sepa bien lo que está haciendo, no configure la directiva `User` como root. El uso de root como `User` provocará la pérdida de seguridad de su servidor Web.

El proceso padre `httpd` primero se ejecuta como root durante las operaciones normales pero luego pasa a las manos del usuario apache. El servidor debe arrancarse como root porque necesita un puerto cuyo valor sea inferior a 1024. Los puertos con valores inferiores a 1024 están reservados al sistema, por lo tanto no los puede usar cualquiera. Una vez que el servidor se haya conectado a su puerto, pasa el proceso al usuario apache antes de aceptar alguna petición de conexión.

El valor **Grupo** corresponde a la directiva `Group`. La directiva `Group` es similar a la directiva `User`. `Group` configura el grupo bajo el cual el servidor responderá a las peticiones. El grupo por defecto es apache.

19.5. Ajuste del rendimiento

Haga click en la pestaña **Ajuste del rendimiento** para configurar el máximo número de procesos hijos que desea y configurar las opciones de Servidor Apache HTTP para las conexiones del cliente. Las propiedades por defecto para estas opciones son adecuadas para la mayoría de los casos. El cambiar estos valores podría afectar el rendimiento general de su servidor Web.

Figura 19-11. Ajuste del rendimiento

Coloque el **Máximo número de conexiones** al número máximo de conexiones que su servidor puede manejar simultáneamente. Para cada conexión, se crea un proceso hijo `httpd`. Cuando se alcanza este número máximo de conexiones, nadie más puede conectarse al servidor Web hasta que se libere un proceso hijo del servidor. Este valor no puede ser superior a 256 a menos que recompile Apache. Esta opción corresponde a la directiva `MaxClients`.

Tiempo máximo de expiración de la conexión define, en segundos, la cantidad de tiempo que su servidor esperará para recibir y transmitir durante las comunicaciones. Específicamente, **Tiempo máximo de expiración de la conexión** define cuánto tiempo su servidor esperará para recibir una petición GET, cuanto esperará para recibir paquetes TCP en una petición POST o PUT y cuanto

esperará entre ACKs que responda a paquetes TCP. El valor predeterminado para el **Tiempo máximo de expiración de la conexión** es 300 segundos, que se adapta a la mayoría de las situaciones. Esta opción corresponde a la directiva `TimeOut`.

Configure **Máximo número de peticiones por conexión** al máximo número de peticiones permitidas para una conexión persistente. El valor por defecto es 100, que normalmente se adapta a todas las situaciones. Esta opción corresponde a la directiva `MaxRequestsPerChild`.

Si selecciona la opción **Admitir peticiones ilimitadas por conexión** el valor de la directiva `MaxKeepAliveRequests` es 0, que significa que se pueden llevar a cabo un número ilimitado de conexiones.

Si no selecciona la opción **Permitir las conexiones persistentes**, la directiva `KeepAlive` se coloca a falso. Pero si la selecciona, aparecerá como verdadera y la directiva `KeepAliveTimeout` le indicará el valor seleccionado para la opción **Tiempo máximo de espera para la próxima conexión**. Esta directiva establece los segundos que el servidor espera entre una petición y otra antes de que se cierre la conexión. Una vez que se ha recibido la petición, se aplica la opción **Tiempo máximo de expiración de la conexión**.

Si se configura **Conexiones persistentes** a un valor alto el servidor realiza sus tareas más lentamente dependiendo del número de usuarios que estén intentando conectarse en ese momento. Cuanto mayor sea el valor, mayor será el tiempo de espera entre una conexión y otra.

19.6. Grabar configuraciones

Si no desea grabar la configuración de su servidor Servidor Apache HTTP, haga click en **Cancelar** que se encuentra en la parte de abajo a la derecha de la ventana de la **Herramienta de configuración de HTTP**. Se le pedirá que confirme su decisión. Si hace click en **Sí** para confirmar su decisión, no se guardarán sus configuraciones.

En cambio, si desea grabar la configuración de Servidor Apache HTTP, haga click en **OK** en la esquina inferior derecha de la ventana de la **Herramienta de configuración de HTTP**. Aparecerá una ventana de diálogo, si contesta **Sí**, se guardarán sus configuraciones en `/etc/httpd/conf/httpd.conf`. Recuerde que se sobreescribirá el fichero de configuración original.

Si esta es la primera vez que ha utilizado la **Herramienta de configuración de HTTP**, aparecerá una ventana de diálogo en la que se le advertirá que el fichero de configuración se ha modificado manualmente. Si la **Herramienta de configuración de HTTP** detecta que el archivo de configuración `httpd.conf` se ha modificado manualmente, grabará el fichero modificado con el nombre `/etc/httpd/conf/httpd.conf.bak`.

Importante

Después de grabar las configuraciones, debe de reiniciar el demonio `httpd` con el comando `service httpd restart`. Tiene que haberse conectado al sistema como root para poder llevar a cabo esta operación.

19.7. Recursos adicionales

Para mayor información sobre el Servidor Apache HTTP, consulte los recursos siguientes:

19.7.1. Documentación instalada

- Documentación Servidor Apache HTTP — Si tiene instalado el paquete `httpd-manual` y está ejecutando el demonio Servidor Apache HTTP (`httpd`), puede visualizar la documentación sobre el Servidor Apache HTTP. Abra el nevagador de web y vaya al URL http://localhost en el servidor que esté ejecutando el Servidor Apache HTTP. Luego, pulse el enlace **Documentación**.
- `/usr/share/docs/httpd-`*<version>* — El documento *Apache Migration HOWTO* contiene una lista de los cambios que se han realizado desde la versión 1.3 a la versión 2.0 así como también información sobre cómo migrar el fichero de configuración manualmente.

19.7.2. Sitios web útiles

- http://www.apache.org — *La Fundación del software de Apache*.
- http://httpd.apache.org/docs-2.0/ — La documentación de La Fundación del software de Apache del Servidor Apache HTTP versión 2.0, incluyendo el *Manual del usuario de Servidor Apache HTTP Versión 2.0*.
- http://localhost/manual/index.html — Después de haber ejecutado el Servidor Apache HTTP en el sistema local, puede visualizar la documentación del Servidor Apache HTTP Versión 2.0 en su sistema local usando este URL.
- http://www.redhat.com/support/resources/web_ftp/apache.html — El soporte Red Hat mantiene una lista de enlaces útiles de Servidor Apache HTTP.
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — La base centralizada de conocimientos de Apache de Red Hat Linux compilada por Red Hat.

19.7.3. Libros relacionados

- *Apache: The Definitive Guide* por Ben Laurie y Peter Laurie; O'Reilly & Associates, Inc.
- *Manual de referencia de Red Hat Linux*; Red Hat, Inc. — Este manual incluye instruciones sobre cómo migrar desde Servidor Apache HTTP versión 1.3 a Servidor Apache HTTP versión 2.0 manualmente, más detalles sobre las directivas del Servidor Apache HTTP e instrucciones para añadir módulos al Servidor Apache HTTP.

redhat.

Capítulo 20.

Configuración del Servidor Seguro Apache HTTP

20.1. Introducción

Este capítulo proporciona información básica sobre Servidor Apache HTTP con el módulo se seguridad `mod_ssl` activado para usar la librería y el conjunto de herramientas OpenSSL. La combinación de estos tres componentes, proporcionados con Red Hat Linux, se conocen en este capítulo como el servidor seguro Web o simplemente como el servidor seguro.

El módulo `mod_ssl` es un módulo de seguridad para el Servidor Apache HTTP. El módulo `mod_ssl` usa las herramientas proporcionadas por el Proyecto OpenSSL para añadir una característica muy importante al Servidor Apache HTTP — la habilidad de tener comunicaciones encriptadas. En contraste, usando HTTP normal, las comunicaciones entre el navegador y el servidor Web son enviadas en texto plano, lo cual puede ser interceptado y leído por alguna persona no autorizada.

Este capítulo no está diseñado para ser una guía completa de ninguno de estos programas. Siempre que sea posible, esta guía le indicará los lugares apropiados donde puede encontrar información más detallada sobre estos temas.

Este capítulo le mostrará como instalar estos programas. También aprenderá los pasos necesarios para generar una clave privada y una petición de certificado, cómo generar su propio certificado firmado, y cómo instalar un certificado para usarlo con su servidor web seguro.

El archivo de configuración `mod_ssl` está ubicado en `/etc/httpd/conf.d/ssl.conf`. Para que este archivo sea cargado, y por ende para que `mod_ssl` funcione, debe tener la sentencia `Include conf.d/*.conf` en `/etc/httpd/conf/httpd.conf`. Esta sentencia es incluida por defecto en el archivo de configuración Servidor Apache HTTP en Red Hat Linux 9.

20.2. Vista preliminar de los paquetes relacionados con la seguridad

Para activar el servidor seguro, necesita, como mínimo, tener instalados los siguientes tres paquetes:

`httpd`

El paquete `httpd` contiene el demonio `httpd` y otras utilidades relacionadas, archivos de configuración, iconos, Servidor Apache HTTP módulos, páginas de manual y otros archivos utilizados por Servidor Apache HTTP.

`mod_ssl`

El paquete `mod_ssl` incluye el módulo `mod_ssl`, que proporciona criptografía fuerte para el servidor web Servidor Apache HTTP a través de los protocolos SSL, Secure Sockets Layer y TLS, Transport Layer Security.

`openssl`

El paquete `openssl` contiene el conjunto de herramientas de OpenSSL. El conjunto de herramientas de OpenSSL implementa los protocolos SSL y TLS y también incluye una librería criptográfica de propósito general.

Adicionalmente, otros paquetes de software incluídos con Red Hat Linux pueden proporcionar ciertas funcionalidades de seguridad (pero que no son requeridas por el servidor seguro para funcionar):

`httpd-devel`

El paquete `httpd-devel` contiene el Servidor Apache HTTP, incluye archivos, cabeceras de archivos y la utilidad APXS. Necesitará todo esto si intenta cargar cualquier módulo extra, aparte de los proporcionados con este producto. Por favor, vea el *Manual de referencia de Red Hat Linux* para ver más información sobre la carga de módulos en su servidor seguro usando las funcionalidades DSO de Apache.

Si no tiene intención de cargar otros módulos en su servidor Apache, no necesita instalar este paquete.

`httpd-manual`

El paquete `httpd-manual` contiene el *Manual del usuario Apache* del Proyecto Apache en formato HTML. Este manual también esta disponible en el Web en http://httpd.apache.org/docs-2.0/.

Paquetes OpenSSH

Los paquetes OpenSSH proporcionan el conjunto OpenSSH de herramientas de conectividad para conectarse y ejecutar comandos en una máquina remota. Las herramientas OpenSSH encriptan todo el tráfico (incluyendo contraseñas), para que así pueda evitar que otros escuchen detras de las puertas, el secuestro de conexiones y otros ataques a las comunicaciones entre su máquina y la máquina remota.

El paquete `openssh` incluye los paquetes del núcleo necesarios por los programas clientes OpenSSH y el servidor OpenSSH. El paquete `openssh` también contiene `scp`, una versión segura de `rcp` (para copiar archivos entre máquinas).

El paquete `openssh-askpass` muestra una ventana de diálogo que pide una contraseña durante el uso del agente OpenSSH.

El paquete `openssh-askpass-gnome` puede ser usado con el ambiente de escritorio gráfico GNOME para mostrar una ventana de diálogo cuando los programas OpenSSH solicitan una contraseña. Si está ejecutando GNOME y está utilizando las utilidades OpenSSH, debería instalar este paquete.

El paquete `openssh-server` contiene el demonio seguro del shell `sshd` y otros archivos relacionados. Dicho demonio es la parte servidor del conjunto OpenSSH, y debe ser instalado en su máquina si quiere permitir que clientes SSH se conecten a ella.

El paquete `openssh-clients` contiene los programas clientes necesarios para hacer conexiones encriptadas a servidores SSH, incluyendo lo siguiente: `ssh`, una versión segura de `rsh`; `sftp`, una versión segura de `ftp` (para transferir archivos entre máquinas); y `slogin`, la versión segura de `rlogin` (para conexión remota) y `telnet` (para comunicarse con otra máquina a través del protocolo Telnet).

Para más información sobre OpenSSH, consulte el Capítulo 15, el *Manual de referencia de Red Hat Linux* y la página web de OpenSSH en http://www.openssh.com.

`openssl-devel`

El paquete `openssl-devel` contiene las librerías estáticas y los archivos de inclusión necesarios para compilar aplicaciones con soporte de varios algoritmos y protocolos criptográficos. Sólo necesita instalar éste paquete si está desarrollando aplicaciones que incluyan soporte SSL — No necesita éste paquete para usar SSL.

`stunnel`

El paquete `stunnel` proporciona el Stunnel SSL wrapper. Stunnel soporta la encriptación SSL de conexiones TCP, así puede proporcionar encriptación para demonios no-SSL y protocolos (como POP, IMAP y LDAP) sin que requiera cambiar el código del demonio.

Tabla 20-1 muestra un resúmen de los paquetes de servidor seguro y si cada paquete es opcional para la instalación del servidor seguro.

Nombre del paquete	Opcional?
`httpd`	no
`mod_ssl`	no
`openssl`	no
`httpd-devel`	yes
`httpd-manual`	yes
`openssh`	yes
`openssh-askpass`	yes
`openssh-askpass-gnome`	yes
`openssh-clients`	yes
`openssh-server`	yes
`openssl-devel`	yes
`stunnel`	yes

Tabla 20-1. Paquetes de seguridad

20.3. Vista preliminar de certificados y seguridad

Su servidor proporciona seguridad usando una combinación del protocolo SSL Secure Sockets Layer y (en la mayoría de los casos) un certificado digital de una Autoridad de Certificación (CA). SSL maneja las comunicaciones encriptadas y la mutua autentificación entre navegadores y su servidor seguro. El certificado digital aprobado por una CA proporciona autentificación para su servidor seguro (el CA pone su reputación detrás de la certificación de la identidad de su organización). Cuando su navegador se esté comunicando usando la encriptación SSL, verá el prefijo `https://` al principio de la URL (Localizador de Recursos Uniforme - la dirección de internet) en la barra de navegación.

La encriptación depende del uso de claves (imagínelas como anillos codificador/decodificador en formato de datos). En criptografía convencional o simétrica, ambas partes de la transacción tienen la misma clave, la cual usan para decodificar la transmisión del otro. En criptografía pública o asimétrica, coexisten dos claves: una pública y una privada. Una persona o una organización guarda su clave privada en secreto, y publica su clave pública. Los datos codificados con la llave pública sólo pueden ser decodificados con la clave privada; y los datos codificados con la clave privada sólo pueden ser decodificados con la llave pública.

Para configurar su servidor seguro, usará criptografía pública para crear un par de claves pública y privada. En muchos casos, enviará su petición de certificado (incluyendo su clave pública), demostrando la identidad de su compañía y pago a la CA. La CA verificará la petición del certificado y su identidad, y entonces mandará un certificado para su servidor seguro.

Un servidor seguro usa un certificado para identificarse a sí mismo a los navegadores web. Puede generar su propio certificado (llamado certificado autofirmado) o puede conseguirlo de una Autoridad de Certificación o CA. Un certificado de una CA con buena reputación garantiza que un sitio web está asociado a una compañía u organización particular.

Alternativamente, puede crear su propio certificado autofirmado. Note, sin embargo, que estos certificados autofirmados no deben ser usados en muchos entornos de producción. Dichos

certificados pueden no ser aceptados automáticamente por el navegador de un usuario — el usuario será preguntado por el navegador si quiere aceptar el certificado y crear la conexión segura. Vea la Sección 20.5 para más información sobre las diferencias entre certificados autofirmados y firmados por una CA.

Una vez que tenga un certificado autofirmado o firmado por la CA de su elección, necesitará instalarlo en su servidor seguro.

20.4. Uso de claves y certificados preexistentes

Si ya tiene una clave y certificado preexistente (por ejemplo, si ha instalado un servidor seguro para reemplazar un servidor web seguro de otra compañía), probablemente sea capaz de usar su clave y certificado existente con el servidor seguro. En las dos siguientes situaciones, no será capaz de usar su clave y certificado existente:

- *Si está cambiando su dirección IP o su nombre de dominio* — No podrá usar su vieja clave y certificado si está cambiando la dirección IP o el nombre de dominio. Los certificados se emiten para un par concreto de dirección IP y nombre de dominio. Necesitará un nuevo certificado si los cambia.
- *Si tiene un certificado de VeriSign y está cambiando el software de su servidor* — VeriSign es un CA ampliamente usado. Si ya tiene un certificado VeriSign para otro propósito, puede estar considerando usar su certificado VeriSign existente con su nuevo servidor seguro. Sin embargo, no podrá hacerlo, ya que los certificados VeriSign se emiten para un software servidor determinado y una combinación de dirección IP y nombre de dominio.

  Si cambia uno de estos parámetros (por ejemplo, si previamente ha usado otro producto de servidor web seguro, el certificado VeriSign que obtuvo para usar con la configuración previa, no funcionará con la nueva configuración. Necesitará obtener un nuevo certificado.

Si ya tiene una clave y un certificado existente que quiera usar, no tendrá que generar una nueva clave ni obtener un nuevo certificado. Sin embargo, necesitará mover y renombrar los archivos que contienen su clave y su certificado.

Mueva su archivo de claves existente a:

```
/etc/httpd/conf/ssl.key/server.key
```

Mueva su archivo de certificado existente a:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Después de haber movido su clave y su certificado, salte a la Sección 20.9.

Si está actualizando desde el Servidor Web seguro Red Hat, su vieja clave (`httpsd.key`) y certificado (`httpsd.crt`) estarán localizados en `/etc/httpd/conf/`. Necesitará moverlos y renombrarlos para que el servidor seguro pueda usarlos. Utilize los siguientes dos comandos para hacerlo:

```
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
```

Entonces, lance su servidor seguro con el comando:

```
/sbin/service httpd start
```

Para un servidor seguro, se le pedirá que introduzca su contraseña. Después de que la haya introducido y presione [Intro], el servidor arrancará.

20.5. Tipos de certificados

Si ha instalado su servidor seguro desde el paquete RPM proporcionado en Red Hat Linux, una clave aleatoria y un certificado de prueba son generados y puestos en sus directorios apropiados. Antes de que empiece a usar su servidor seguro, sin embargo, necesitará generar su propia clave y obtener un certificado que identifique correctamente su servidor.

Necesita una clave y un certificado para operar su servidor seguro — lo cual significa que puede generar un certificado autofirmado o adquirir uno firmado por una CA. ¿Cuáles son las diferencias entre los dos?

Un certificado firmado por una CA proporciona dos importantes capacidades para su servidor:

- Los navegadores (normalmente) reconocen automáticamente el certificado y permiten establecer la conexión segura sin preguntar al usuario.
- Cuando una CA emite un certificado firmado, ellos garantizan la identidad de la organización que está proporcionando las páginas web al navegador.

Si a su servidor seguro está siendo accesado por todo el mundo, necesitará un certificado firmado por una CA, así la gente que acceda a su sitio web sabrá que dicho sitio es propiedad de la organización que proclama ser la dueña. Antes de firmar un certificado, una CA verifica que la organización peticionaria de dicho certificado es realmente quien proclama ser.

Muchos navegadores web que soportan SSL tienen una lista de CAs cuyos certificados admiten automáticamente. Si el navegador encuentra un certificado autorizado por una CA que no está en la lista, el navegador preguntará al usuario si desea aceptar o rechazar la conexión.

Puede generar un certificado autofirmado para su servidor seguro, pero tenga claro que dicho certificado no proporciona la misma funcionalidad que uno firmado por una CA. Un certificado autofirmado no será reconocido automáticamente por los navegadores de los usuarios, además de no proporcionar ninguna garantía concerniente a la identidad de la organización que provee el sitio web. Un certificado firmado por una CA proporciona ambas importantes características a un servidor seguro. Si su servidor seguro será usado en un ambiente de producción, probablemente necesite un certificado firmado por una CA.

El proceso para conseguir un certificado de una CA es bastante sencillo. A continuación un vistazo rápido a dicho proceso:

1. Crear un par de claves encriptadas, pública y privada.
2. Crear una petición de certificado basada en la clave pública. La petición contiene información sobre su servidor y la compañía que lo hospeda.
3. Mande la petición de certificado, junto con los documentos que prueben su identidad, a una CA. No le diremos qué Autoridad de Certificación elegir. Su elección puede basarse en experiencias previas, experiencias de sus amigos o conocidos o simplemente en factores monetarios.

   Una vez que haya decidido sobre el CA, necesitará seguir las instrucciones que se le indiquen para obtener un certificado.
4. Cuando la CA esté satisfecha de que usted es en realidad quién dice ser, le enviarán su certificado digital.
5. Instale este certificado en su servidor seguro y comience a manejar transacciones seguras.

Si está consiguiendo un certificado de una CA o generando su propio certificado autofirmado, el primer paso es generar una clave. Vea la Sección 20.6 para conseguir instrucciones de como hacerlo.

20.6. Generar una clave

Tiene que ser root para generar una clave.

Primero, cámbiese al directorio `/etc/httpd/conf`. Elimine la clave y el certificado simulados que se generaron durante la instalación con los siguientes comandos:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

A continuación, necesita crear su propia clave aleatoria. Cambie al directorio `/usr/share/ssl/certs` y escriba el comando siguiente:

```
make genkey
```

Su sistema mostrará 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:
```

Necesita teclear una palabra de paso. Para mayor seguridad, su palabra de paso debe incluir, al menos, ocho caracteres, incluyendo números y símbolos de puntuación, y no ser una palabra que esté incluida en un diccionario. También, recuerde que su palabra de paso es sensible a las mayúsculas.

Nota

Necesitará acordarse de su palabra de paso para poder introducirla cada vez que inicie su servidor Web seguro; así que no la olvide.

Le será requerido que reintroduzca su contraseña, para verificar que es correcta. Una vez que la haya tecleado correctamente, será creado un archivo llamado `/etc/httpd/conf/ssl.key/server.key`, que contendrá dicha clave.

Observe que si no quiere teclear la palabra de paso cada vez que comience su servidor seguro, necesitará usar los dos comandos siguientes en vez de `make genkey` para crear su clave.

Utilice el siguiente comando para crear su clave:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Luego, utilice el comando siguiente para asegurarse que los permisos de su clave están correctamente asignados:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Después de usar los comandos anteriores para crear su clave, no necesitará utilizar una contraseña para comenzar su servidor Web seguro.

Atención

El desactivar la contraseña para su servidor web seguro es un riesgo de seguridad. NO le recomendamos que lo haga.

Los problemas asociados con no usar la contraseña están directamente relacionados al mantenimiento de la seguridad en el sistema de la máquina. Si por ejemplo, un individuo sin escrúpulos compromete la seguridad UNIX estándar de la máquina, ésta persona podrá obtener su clave privada (el contenido de su archivo `server.key`). La clave podría ser usada para servir páginas web que aparenten estar en su servidor web.

Si las labores de seguridad de UNIX son rigurosamente mantenidas en el sistema (todos los parches y actualizaciones del sistema operativo son instalados tan pronto como están disponibles, no se ejecutan servicios innecesarios o peligrosos, etc.), la contraseña del servidor seguro puede parecer innecesaria. Sin embargo, desde que su servidor Web seguro no necesita ser reiniciado muy a menudo, la seguridad extra proporcionada por la introducción de la contraseña es un pequeño esfuerzo que vale la pena en muchos casos.

El archivo `server.key` debe ser propiedad del usuario root de su sistema y no debe ser accesible por nadie más. Haga una copia de seguridad de dicho archivo y guárdela en un lugar seguro. Necesitará la copia de seguridad por que si pierde el archivo `server.key` después de haberlo usado para crear su certificado, el susodicho certificado no funcionará más y la CA no podrá ayudarle. Su única solución será pedir (y volver a pagar por ello) un nuevo certificado.

Si va a adquirir un certificado de una CA, continue con la Sección 20.7. Si va a generar su propio certificado autofirmado, vaya a la Sección 20.8.

20.7. Generar una petición de certificado para enviarla a un CA

Una vez creada la clave, el siguiente paso es generar la petición de certificado que necesitaremos enviar al CA de nuestra elección. Asegúrese de estar en el directorio `/usr/share/ssl/certs` y teclee el siguiente comando:

```
make certreq
```

Su sistema mostrará la siguiente salida y le preguntará por su contraseña (a menos que desactivara dicha opción):

```
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:
```

Teclee la palabra de paso que eligió cuando generó su clave. Su sistema mostrará algunas instrucciones y le requerirá una serie de respuestas. Dichas respuestas serán incorporadas a la petición del certificado. La pantalla, con respuestas de ejemplo, será similar a esta:

```
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) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Las respuestas por defecto aparecerán entre corchetes `[]` inmediatamente después de cada petición de entrada. Por ejemplo, la primera información requerida es el nombre del país dónde el certificado será usado, parecido a:

```
Country Name (2 letter code) [GB]:
```

La entrada por defecto, entre corchetes, es `GB`. Para aceptarla, pulse [Intro], o relléne con el código de dos letras de su país.

Tendrá que introducir el resto de las entradas. Todas estas entradas son autoexplicativas, pero necesitará seguir estas directrices:

- No abrevie la localidad o el estado. Escríbalas enteras (por ejemplo, St. Louis debe escribirse como Saint Louis).
- Si está mandando esta información de un CSR a un CA, sea cuidadoso en proporcionar la información correcta en todos los campos, pero especialmente en el `Nombre de la Organización` y el `Nombre común`. Las CAs verifican los datos para determinar si su organización es responsable de quién proporcionó como `Nombre común`. Las CAs rechazarán las peticiones que incluyan información que ellos perciban como inválida.
- Para `Nombre común`, asegúrese que teclea el *verdadero* nombre de su servidor Web seguro (un nombre de DNS válido) y no un alias que el servidor tenga.
- La `Dirección email` debe ser la del webmaster o administrador del sistema.
- Evite caracteres especiales como @, #, &, !, etc. Algunas CAs rechazarán una petición de certificado que contenga un caracter especial. Así, si el nombre de su compañía contiene una "y" comercial (&), escríbalo como "y" en vez de "&".
- No use los atributos extra (`Otra Contraseña` y `Nombre opcional de la compañía`). Para continuar sin introducir estos campos, simplemente pulse [Intro] para aceptar los valores en blanco por defecto.

El archivo `/etc/httpd/conf/ssl.csr/server.csr` es creado cuando termine de introducir su información. Este archivo es su petición de certificado, listo para enviar a su CA.

Después de haber decidido una CA, siga las instrucciones que ellos proporcionen en su sitio web. Estas instrucciones le dirán como mandar su petición de certificado, cualquier otra documentación que ellos requieran, y como pagarles.

Después de haber satisfecho los requisitos de la CA, ellos le mandarán un certificado para usted (normalmente por email). Guarde (o copie y pegue) el certificado que le manden como `/etc/httpd/conf/ssl.crt/server.crt`. Asegúrese de hacer una copia de respaldo.

20.8. Creación de un certificado autofirmado

Usted puede crear su propio certificado autofirmado. Por favor, tenga en cuenta que un certificado autofirmado no proporciona las garantías de seguridad que un certificado firmado por una CA sí proporciona. Consulte la Sección 20.5 para ver más detalles sobre los certificados.

Si quiere crear su propio certificado autofirmado, necesitará primero crear una clave aleatoria usando las instrucciones proporcionadas en la Sección 20.6. Una vez que tenga la clave y que se asegure de estar en el directorio `/usr/share/ssl/certs`, utilice el siguiente comando:

```
make testcert
```

Verá la siguiente salida, se le pedirá que introduzca su palabra de paso (a menos que haya generado una clave sin 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
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Después de que introduzca su contraseña (o sin la petición, si ha creado una clave sin ella), se le pedirá más información. La salida del ordenador y el conjunto de peticiones será parecido al siguiente (necesitará dar la información correcta de su organización y de su máquina):

```
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) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

Después que proporcione la información correcta, un certificado autofirmado será creado y colocado en `/etc/httpd/conf/ssl.crt/server.crt`. Necesitará reiniciar su servidor seguro, después de generar el certificado, con el comando:

```
/sbin/service httpd restart
```

20.9. Probar su certificado

Para probar el certificado instalado por defecto, un certificado de una CA o un certificado autofirmado, apunte su navegador Web a la siguiente página web (reemplazando *`server.example.com`* con el nombre de su dominio):

`https://`*`server.example.com`*

Nota

Observe la `s` después de `http`. el prefijo `https:` es usado para las transacciones HTTP seguras.

Si ha comprado un certificado de una CA bien conocida, su navegador probablemente aceptará el certificado automáticamente (sin pedirle información adicional) y creará una conexión segura. Su navegador no reconocerá automáticamente un certificado de prueba o un certificado autofirmado, porque el certificado no es firmado por una CA. Si no está usando un certificado de una CA, siga las instrucciones proporcionadas por su navegador para aceptar el certificado.

Una vez que su navegador acepte el certificado, su servidor seguro mostrará una página de inicio predeterminada.

20.10. Acceder a su servidor seguro

Para acceder a su servidor seguro, use una URL como esta:

`https://`*`server.example.com`*

Su servidor no seguro puede ser accedido usando una URL como la siguiente:

`http://`*`server.example.com`*

El puerto estándar para las comunicaciones web seguras es el 443. El puerto estándar para las comunicaciones web no seguras es el 80. La configuración predeterminada del servidor seguro escucha en ambos puertos. Por lo tanto, no necesita especificar el número del puerto en la URL (el número del puerto es asumido).

Sin embargo, si configura su servidor para escuchar en un puerto no estándar (por ejemplo, en cualquiera que no sea el 80 o el 443), necesitará especificar el número de puerto en cada URL que intente conectarse al servidor por el puerto no estándar.

Por ejemplo, puede tener configurado su servidor para que tenga un host virtual no seguro corriendo en el puerto 12331. Cualquier URL que intente conectarse a este host virtual debe especificar el puerto en el URL. El siguiente URL de ejemplo intentará conectarse a un servidor web no seguro que escucha en el puerto 12331:

`http://`*`server.example.com`*`:12331`

20.11. Recursos adicionales

Consulte la Sección 19.7 para encontrar recursos adicionales sobre el Servidor Apache HTTP.

20.11.1. Documentación instalada

- `mod_ssl documentation` — Abra un navegador web, y vaya a la URL http://localhost/manual/mod/mod_ssl.html en el servidor en el que está ejecutándose Servidor Apache HTTP y tiene el paquete `httpd-manual` instalado.

20.11.2. Sitios web útiles

- Lista de correo http://www.redhat.com/mailing-lists/ — Se puede suscribir a la lista de correo de redhat-secure-server en este URL.

  También puede mandar un correo electrónico a <redhat-secure-server-request@redhat.com> e incluir la palabra *subscribe* en el asunto del e-mail.

- http://www.modssl.org — El sitio web de `mod_ssl` es la fuente definitiva sobre información concerniente a `mod_ssl`. El sitio web incluye abundante documentación, incluyendo un *Manual del usuario* at http://www.modssl.org/docs.

20.11.3. Libros relacionados

- *Apache: The Definitive Guide*, 2nd edition, por Ben Laurie and Peter Laurie, O'Reilly & Associates, Inc.

Capítulo 21.

Configuración de BIND

Este capítulo asume que usted ya tiene unas nociones básicas de BIND y de DNS; por lo tanto, no se explicarán estos conceptos. Este capítulo describe cómo utilizar la **Herramienta de configuración de Bind** (`redhat-config-bind`) para configurar las zonas básicas del servidor de BIND en la versión 8 de BIND. La **Herramienta de configuración BIND** crea el archivo de configuración `/etc/named.conf` y los archivos de configuración de zona en el directorio `/var/named` cada vez que se aplican los cambios.

Importante

No edite el archivo de configuración `/etc/named.conf`. La **Herramienta de configuración de Bind** genera este archivo después de aplicar los cambios. Si desea configurar determinados parámetros que no se pueden configurar usando la **Herramienta de configuración de Bind**, añádalos a `/etc/named.custom`.

La **Herramienta de configuración de Bind** requiere el uso del sistema X Window y acceso como root. Para arrancar la **Herramienta de configuración de Bind**, vaya al **Menú principal** (en el Panel) => **Configuración del sistema** => **Configuración de servidores** => **Servicio de nombres de dominio** o escriba el comando `redhat-config-bind` en el intérprete de comandos (por ejemplo, en una ventana de terminal XTerm o GNOME).

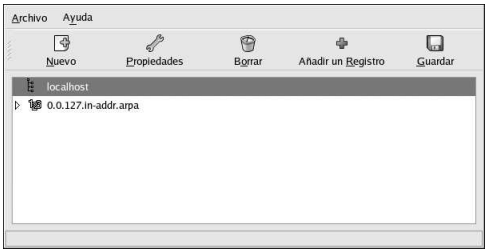

Figura 21-1. Herramienta de configuración de Bind

La **Herramienta de configuración de Bind** configura el directorio de zona predeterminado a `/var/named`. Todos los archivos de zona especificados son relativos a este directorio. La **Herramienta de configuración de Bind** también incluye una función de comprobación de sintaxis básica cuando se introducen los valores. Por ejemplo, si una entrada válida es una dirección IP, el usuario solamente podrá escribir los números y el carácter de punto (.) en el área de texto.

La **Herramienta de configuración de Bind** le permite agregar una zona maestra de redireccionamiento, una zona maestra inversa y una zona esclava. Tras agregar las zonas, puede editarlas o eliminarlas desde la ventana principal como se muestra en la Figura 21-1.

Después de agregar, editar o eliminar una zona, debe hacer click en el botón **Guardar** o seleccionar **Archivo** => **Guardar** para escribir el archivo de configuración `/etc/named.conf` y todos los archivos de zona individuales en el directorio `/var/named`. Al aplicar los cambios, el servicio `named` también volverá a cargar los archivos de configuración. También puede seleccionar **Archivo** => **Salir** y guardará los cambios antes de salir de la aplicación.

21.1. Agregar una zona maestra de redireccionamiento

Para agregar una zona maestra de redireccionamiento (también denominada maestra principal), pulse el bótón **Añadir**, seleccione **Zona Maestra de Reenvío** e introduzca el nombre de dominio de la zona maestra en el área de texto **Nombre de Dominio**.

Aparecerá una nueva ventana como se muestra en la Figura 21-2 con las siguientes opciones:

- **Nombre** — Nombre del dominio que se acaba de introducir en la ventana anterior.
- **Nombre del archivo** — Nombre del archivo de la base de datos DNS, relacionada con `/var/named`. Está programado para el nombre de dominio y se le ha añadido `.zone`.
- **Contacto** — Dirección de correo electrónico del contacto principal de la zona maestra.
- **Servidor de nombres primario (SOA)** — Registro de estado de autoridad (SOA). Indica el servidor de nombres considerado como el mejor recurso de información para este dominio.
- **Número de serie** — Número de serie del archivo de la base de datos DNS. Este número irá aumentando cada vez que cambie el archivo; de este modo, los servidores de nombres esclavos de la zona podrán recuperar los últimos datos. La **Herramienta de configuración de Bind** incrementa este número cada vez que cambia la configuración. También se puede aumentar manualmente si se pulsa el botón **Configurar** que se encuentra junto al valor **Número serie**.
- **Configuración del tiempo** — Los valores TTL (Time to Live) **Refrescar**, **Reintentar**, **Expirar**, y **Mínimo** que se almacenan en el archivo de la base de datos DNS. Todos los valores son en segundos.
- **Registros** - Agrega, edita y elimina recursos de registros de tipo **Host**, **Alias** y **Nombre del servidor**.

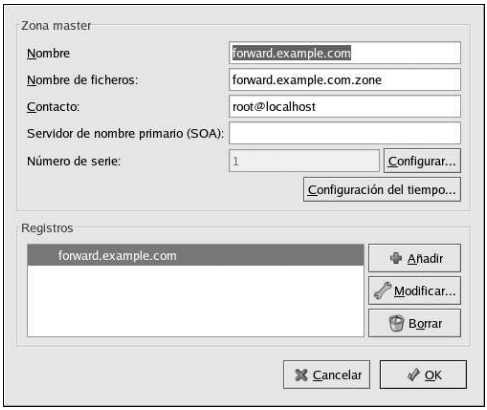

Figura 21-2. Agregar una zona maestra de redireccionamiento

Se debe especificar un **Nombre de servidor primario (SOA)**, y al menos un registro de nombre de servidor se debe especificar haciendo click en el botón **Añadir** en la sección **Registros**.

Después de configurar la Zona maestra de redireccionamiento, haga click en **OK** para volver a la pantalla principal como se muestra en la Figura 21-1. Desde el menú, haga click en **Guardar** para escribir el archivo de configuración `/etc/named.conf`, escribir todos los archivos de zona individuales en el directorio `/var/named` y hacer que el demonio recargue los archivos de configuración.

La configuración crea una entrada similar a lo siguiente en el archivo `/etc/named.conf`:

```
zone  "forward.example.com" {
 type master;
 file  "forward.example.com.zone";
};
```

También crea el archivo `/var/named/forward.example.com.zone` con la siguiente información:

```
$TTL 86400
@       IN      SOA     ns.example.com.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )


        IN      NS      192.168.1.1.
```

21.2. Agregar una zona maestra inversa

Para agregar una zona maestra inversa, haga click en **Añadir** y seleccione **Zona maestra inversa**. Introduzca los tres primeros octetos del rango de direcciones IP que desee configurar. Por ejemplo, si está configurando el rango de direcciones IP 192.168.10.0/255.255.255.0, introduzca 192.168.10 en el área de texto **Dirección IP (primeros tres octetos)**.

Aparecerá una nueva ventana, tal como se muestra en la Figura 21-3, con la siguientes opciones:

1. **Dirección IP** — Los tres primeros grupos numéricos que acaba de introducir en la ventana anterior.
2. **Dirección IP inversa** — No se puede editar. Se completa automáticamente según la dirección IP especificada.
3. **Contacto** — Dirección de correo electrónico del contacto principal para la zona maestra.
4. **Nombre de archivo** — Nombre del archivo de la base de datos DNS en el directorio `/var/named`.
5. **Servidor de nombres primario (SOA)** — Registro de estado de autoridad (SOA). Indica el servidor de nombres considerado como el mejor recurso de información para este dominio.
6. **Número de serie** — Número de serie del archivo de la base de datos DNS. Este número irá aumentando cada vez que cambie el archivo; de este modo, los servidores de nombres esclavos de la zona podrán recuperar los últimos datos. La **Herramienta de configuración de Bind** incrementa este número cada vez que cambia la configuración. También se puede aumentar manualmente si se pulsa el botón **Configurar** que se encuentra junto al valor **Número serie**.
7. **Configuración del tiempo** — Se trata de los valores TTL (**Refrescar**, **Reenviar**, **Expirar** y **Mínimo** que se almacenan en el archivo de la base de datos DNS.
8. **Servidores de nombre** — Agrega, edita y elimina los servidores de nombres para la zona maestra inversa. Se necesita, como mínimo, un servidor de nombres.
9. **Tabla de dirección inversa** — Lista de direcciones IP que hay en la zona maestra inversa y sus nombres host. Por ejemplo, para la zona maestra inversa 192.168.10, puede agregar 192.168.10.1 en la **Tabla de dirección inversa** con el nombre de host one.example.com. Este nombre debe terminar con un punto (.) para indicar que se trata de un nombre de host completo.

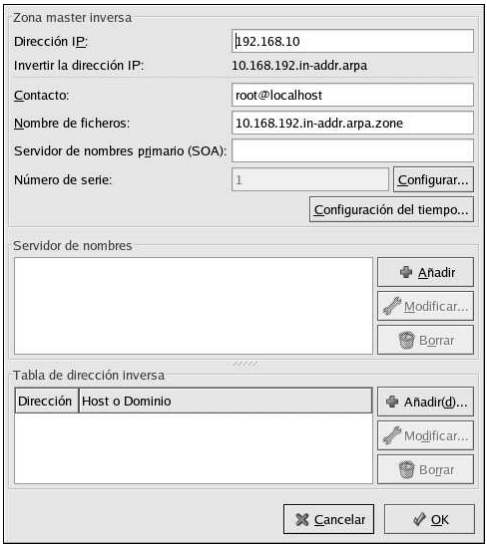

Figura 21-3. Agregar una zona maestra inversa

Se debe especificar un **Nombre de servidor primario (SOA)** y al menos un registro de nombre de servidor haciendo click en el botón **Añadir** en la sección **Nombre de servidores**.

Después de configurar la zona maestra inversa, pulse en **OK** para volver a la ventana principal, tal como se muestra en la Figura 21-1. En el menú desplegable, seleccione **Guardar** para escribir el archivo de configuración `/etc/named.conf`, escribir todos los archivos de zona individuales en el directorio `/var/named`, y hacer que el demonio vuelva a cargar los archivos de configuración.

La configuración creará una entrada similar a lo siguiente en el archivo `/etc/named.conf`:

```
zone  "10.168.192.in-addr.arpa" {
        type master;
        file  "10.168.192.in-addr.arpa.zone";
};
```

También crea el archivo `/var/named/10.168.192.in-addr.arpa.zone` con la siguiente información:

```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      ns2.example.com.

1       IN      PTR     one.example.com.
2       IN      PTR     two.example.com.
```

21.3. Agregar una zona esclava

Para agregar una zona esclava (también conocida como maestra secundaria), haga click en el botón **Añadir** y seleccione **Zona esclava**. Introduzca el nombre de dominio de la zona esclava en el área de texto **Nombre de dominio**.

Aparecerá una nueva ventana como se muestra en la Figura 21-4, con las siguientes opciones:

- **Nombre** — Nombre del dominio que se acaba de introducir en la ventana anterior.
- **Lista de maestros** — Los nombres de servidores a partir del cual la zona esclava recupera los datos. Este valor debe ser una dirección IP válida. Solamente puede introducir números y puntos (.) en el área de texto.
- **Nombre del archivo** — Nombre del archivo de la base de datos DNS del directorio `/var/named`.

Figura 21-4. Agregar una zona esclava

Después de configurar la zona esclava, haga click en **Aceptar** para volver a la ventana principal como se muestra en la Figura 21-1. Haga click en **Guardar** para escribir el archivo de configuración `/etc/named.conf` y que el demonio recargue los archivos de configuración.

La configuración crea una entrada similar a lo siguiente en el archivo `/etc/named.conf`:

```
zone "slave.example.com" {
        type slave;
        file "slave.example.com.zone";
        masters {
                 1.2.3.4;
                };
};
```

El servicio `named` crea el archivo de configuración `/var/named/slave.example.com.zone` al descargar los datos de la zona desde el servidor o servidores maestros.

Capítulo 22.
Configuración de la autenticación

Cuando un usuario se conecta a un sistema Red Hat Linux, se verifican el nombre de usuario y la contraseña, o en otras palabras se *autentifican*, como un usuario activo válido. Algunas veces la información para verificar el usuario está localizada en el sistema local, otras veces el sistema delega la validación a una base de datos de usuarios en un sistema remoto.

La **Herramienta de configuración de autenticación** proporciona una interfaz gráfica para configurar NIS, LDAP y Hesiod para recuperar información del usuario así como también para configurar LDAP, Kerberos y SMB como protocolos de autentificación.

Nota

Si configuró un nivel de seguridad medio o alto durante la instalación con la **Herramienta de configuración de nivel de seguridad** (o seleccionó alta o baja seguridad con el programa **GNOME Lokkit**), los métodos de autentificación de red, incluyendo NIS y LDAP, no son permitidos a través del cortafuegos.

Este capítulo no explica cada uno de los tipos diferentes de autenticación en detalle. En vez de eso explica cómo usar la **Herramienta de configuración de autenticación** para configurarlos.

Para arrancar la versión gráfica de la **Herramienta de configuración de autenticación** desde el escritorio, seleccione **Botón de menú principal** (en el Panel) => **Configuración del sistema** => **Autentificación** o escriba el comando `authconfig-gtk` en el intérprete de comandos (por ejemplo en un terminal **XTerm** o **GNOME**). Para arrancar la versión basada en texto, escriba el comando `authconfig` en el intérprete de de comandos.

Importante

Después de salir del programa de autenticación, los cambios tendrán efecto de inmediato.

22.1. Información del usuario

La pestaña de **Información del usuario** tiene muchas opciones. Para habilitar una opción, haga click en la casilla de verificación al lado de ella. Para inhabilitarla, haga click en la casilla para limpiarla. Luego haga click en **OK** para salir del programa y aplicar los cambios.

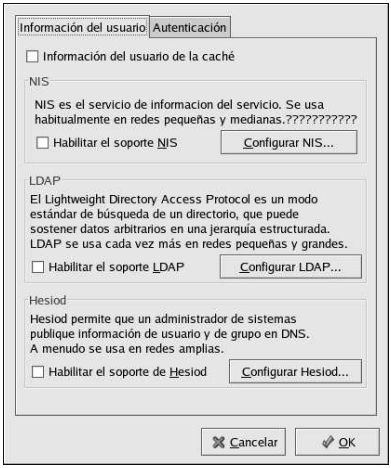

Figura 22-1. Información del usuario

La lista siguiente explica lo que configura cada una de las opciones:

- **Información del usuario de la cache** — Seleccione esta opción para habilitar el demonio de cache de servicio de nombre (`nscd`) y configurarlo para que se inicie al momento de arranque.

  El paquete `nscd` debe estar instalado para que esta opción funcione.

- **Habilitar soporte NIS** — Seleccione esta opción para configurar el sistema como un cliente NIS el cual se conecta a un servidor NIS para la autentificación de usuarios y contraseñas. Haga click en el botón **Configurar NIS** para especificar el dominio NIS y el servidor NIS. Si no se especifica el servidor NIS, el demonio intentará buscarlo vía difusión (broadcast).

  Debe tener el paquete `ypbind` instalado para que esta opción funcione. Si el soporte NIS esta activado, los servicios `portmap` y `ypbind` serán iniciados y también estarán habilitados para arrancar en el momento de inicio del sistema.

- **Habilitar el soporte LDAP** — Seleccione esta opción para configurar el sistema a que recupere la información del usuario a través de LDAP. Haga click en el botón **Configurar LDAP** para especificar el **DN de base de búsqueda LDAP** y el **Servidor LDAP**. Si **Utilice TLS para encriptar conexiones** esta activado, se usará el Transport Layer Security para encriptar las contraseñas enviadas al servidor LDAP.

  Debe tener instalado el paquete `openldap-clients` para que esta opción funcione.

  Para información adicional sobre LDAP, consulte el *Manual de referencia de Red Hat Linux*.

- **Habilitar el soporte Hesiod** — Seleccione esta opción para configurar el sistema a que recupere la información desde una base de datos Hesiod remota, incluyendo la información del usuario.

  El paquete `hesiod` debe estar instalado.

22.2. Autenticación

La pestaña de **Autenticación** permite la configuración de los métodos de autenticación de red. Para activar una opción haga click sobre la casilla de verificación al lado de la misma. Para desactivarla, haga click nuevamente sobre la casilla para desmarcarla o limpiarla.

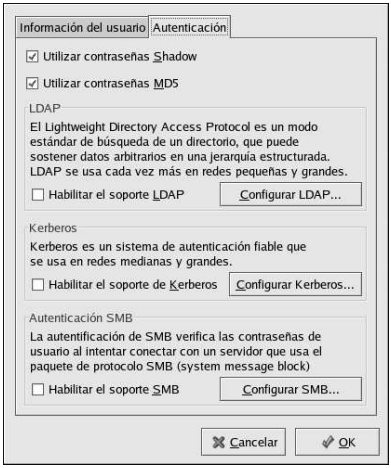

Figura 22-2. Autenticación

A continuación se explica lo que configura cada opción:

- **Utilizar contraseñas shadow** — Seleccione esta opción para guardar las contraseñas en formato de contraseñas shadow en el archivo `/etc/shadow` en vez de en `/etc/passwd`. Las contraseñas shadow son activadas por defecto durante la instalación y se recomiendan para incrementar la seguridad del sistema.

  Debe estar instalado el paquete `shadow-utils` para que esta opción funcione. Para más detalles sobre las contraseñas shadow, refiérase al capítulo *Usuarios y grupos* en el *Manual de referencia de Red Hat Linux*.
- **Utilizar contraseñas MD5** — Seleccione esta opción para activar contraseñas MD5, lo que permite que las contraseñas tengan hasta 256 en vez de 8 o menos. Esta opción seleccionada por defecto durante la instalación y se recomienda su uso para mayor seguridad.
- **Habilitar el soporte LDAP** — Seleccione esta opción para que las aplicaciones PAM estándar usen LDAP para la autenticación. Haga click en el botón **Configurar LDAP** para especificar lo siguiente:
  - **Utilice TLS para encriptar conexiones** — Utiliza Transport Layer Security, TLS, para encriptar las contraseñas enviadas al servidor LDAP.
  - **DN de base de búsqueda LDAP** — Recupera la información del usuario por su nombre distinguido, Distinguished Name (DN).
  - **Servidor LDAP** — Especifique la dirección IP del servidor LDAP.

  El paquete `openldap-clients` debe estar instalado para que esta opción funcione. Refiérase al *Manual de referencia de Red Hat Linux* para más información sobre LDAP.
- **Habilitar el soporte Kerberos** — Seleccione esta opción para activar la autenticación Kerberos. Haga click en el botón **Configurar Kerberos** para configurar:
  - **Entorno** — Configure el entorno para el servidor de Kerberos. El entorno o reino es la red que usa Kerberos, compuesta de uno o más KDCs y un número potencial de muchos clientes.
  - **KDC** — Define el Centro de distribución de claves, Key Distribution Center (KDC), el cual es el servidor que emite los tickets Kerberos.

- **Servidores de administración** — Especifica el o los servidores de administración ejecutando `kadmind`.

  Debe tener instalados los paquetes `krb5-libs` y `krb5-workstation` para que esta opción funcione. Consulte el *Manual de referencia de Red Hat Linux* para más información sobre Kerberos.

- **Habilitar el soporte SMB** — Esta opción configura PAM para usar un servidor SMB para autentificar a los usuarios. Haga click en el botón **Configurar SMB** para especificar:
  - **Grupo de trabajo** — Especifique el grupo de trabajo SMB a usar.
  - **Controladores de dominio** — Especifique los controladores de dominio SMB a utilizar.

22.3. Versión de línea de comandos

La **Herramienta de configuración de autenticación** también se puede ejecutar como una herramienta de línea de comandos. La versión de línea de comandos se puede utilizar en un script de configuración de kickstart. Las opciones de autenticación son resumidas en la Tabla 22-1.

Opción	Descripción
`--enableshadow`	Habilitar contraseñas shadow
`--disableshadow`	Desactivar contraseñas shadow
`--enablemd5`	Habilitar contraseñas MD5
`--disablemd5`	Inhabilitar contraseñas MD5
`--enablenis`	Habilitar NIS
`--disablenis`	Inhabilitar NIS
`--nisdomain=<`*`domain`*`>`	Especifica el dominio NIS
`--nisserver=<`*`server`*`>`	Especifica el servidor NIS
`--enableldap`	Habilitar LDAP para información del usuario
`--disableldap`	Inhabilitar LDAP para información del usuario
`--enableldaptls`	Habilitar el uso de TLS con LDAP
`--disableldaptls`	Inhabilitar el uso de TLS con LDAP
`--enableldapauth`	Habilitar LDAP para la autenticación
`--disableldapauth`	Inhabilitar LDAP para la autenticación
`--ldapserver=<`*`server`*`>`	Especifica un servidor LDAP
`--ldapbasedn=<`*`dn`*`>`	Especifica un DN de base LDAP
`--enablekrb5`	Habilita Kerberos
`--disablekrb5`	Inhabilita Kerberos
`--krb5kdc=<`*`kdc`*`>`	Especifica un KDC de Kerberos
`--krb5adminserver=<`*`server`*`>`	Especifica un servidor de administración Kerberos
`--krb5realm=<`*`realm`*`>`	Especifica el entorno Kerberos

Opción	Descripción
`--enablesmbauth`	Habilita SMB
`--disablesmbauth`	Inhabilita SMB
`--smbworkgroup=<`*`workgroup`*`>`	Specify SMB workgroup
`--smbservers=<`*`server`*`>`	Especifica servidores SMB
`--enablehesiod`	Habilita Hesiod
`--disablehesiod`	Inhabilita Hesiod
`--hesiodlhs=<`*`lhs`*`>`	Especifica Hesiod LHS
`--hesiodrhs=<`*`rhs`*`>`	Especifica Hesiod RHS
`--enablecache`	Habilita `nscd`
`--disablecache`	Inhabilita `nscd`
`--nostart`	No arranca o detiene los servicios `portmap`, `ypbind` o `nscd` aún si ellos están configurados
`--kickstart`	No muestra la interfaz del usuario
`--probe`	Verifica y muestra las fallas de red

Tabla 22-1. Opciones de línea de comandos

Sugerencia

Estas opciones también se pueden encontrar en la página del manual de `authconfig` o escribiendo `authconfig --help` en el intérprete de comandos.

Capítulo 23.

Configuración del Agente de Transporte de Correo (MTA)

Un *Agente de Transporte de Correo* (MTA, del inglés Mail Transport Agent) es indispensable para enviar correos electrónicos desde un sistema Red Hat Linux. Se usan *Agentes de correo de usuario* (MUA) tales como **Evolution**, **Mozilla Mail**, y **Mutt**, para leer y escribir correos. Cuando un usuario envia un email desde un MUA, los mensajes se entregan al MTA, que los envía a una serie de MTAs hasta que llega a su destino.

Si un usuario no tiene previsto enviar un email desde el sistema, algunas tareas automatizadas o programas del sistema usarán el comando `/bin/mail` para enviar un correo que contenga mensajes de registro para el usuario root del sistema local.

Red Hat Linux 9 tiene dos MTAs: Sendmail y Postfix. Si ambos están instalados, `sendmail` es el MTA predeterminado. **Conmutador de agente de transporte de correo** permite a un usuario seleccionar o `sendmail` o `postfix` como el MTA predeterminado para el sistema.

El paquete `redhat-switch-mail` RPM debe estar instalado para usar la versión basada en texto del programa **Conmutador de agente de transporte de correo**. Si desea usar la versión gráfica, el paquete `redhat-switch-mail-gnome` también debe estar instalado. Para más información sobre la instalación de paquetes RPM, consulte Parte V.

Para iniciar el **Conmutador de agente de transporte de correo**, seleccione **Botón de menú principal** (en el Panel) => **Extras** => **Herramientas del sistema** => **Conmutador de agente de transporte de correo**, o escriba el comando `redhat-switch-mail` en la línea de comandos de la shell (por ejemplo, en una terminal XTerm o GNOME).

El programa detecta automáticamente si está funcionando el sistema X Window. En tal caso, el programa empieza en modo gráfico como se muestra en la Figura 23-1. Si no se detecta X, arranca en modo texto. Para forzar a que el **Conmutador de agente de transporte de correo** funcione en modo texto, use el comando `redhat-switch-mail-nox`.

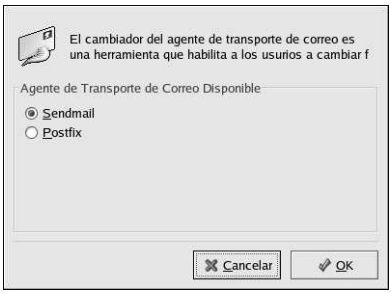

Figura 23-1. Conmutador de agente de transporte de correo

Si ha seleccionado **OK** para cambiar el MTA, el demonio seleccionado estará activado para iniciarse al momento de arranque, y el demonio de correo que no está marcado estará desactivado y así no se ejecutará en el momento del arranque. Se arranca el demonio seleccionado, y el otro demonio es detenido; y así los cambios tendrán efecto de inmediato.

Para más información sobre los protocolos de correo electrónico y MTAs, consulte el *Manual de referencia de Red Hat Linux*. Para más información sobre los MUAs, refiérase al *Manual del principiante de Red Hat Linux*.

IV. Configuración del sistema

Después de discutir el acceso desde la consola y cómo reunir información de software y del hardware desde un sistema Red Hat Linux, esta parte explica las tareas comunes de configuración del sistema.

Tabla de contenidos

redhat.

Capítulo 24.

Acceso a consola

Cuando los usuarios normales (no root) se registran en un equipo localmente, se les conceden dos tipos de permisos especiales:

1. Pueden ejecutar ciertos programas que de otra forma no podrían ejecutar
2. Pueden tener acceso a ciertos archivos (normalmente archivos de dispositivos especiales usados para accesar disquetes, CD-ROMs, etc) a los que no tendrían acceso de otro modo

Puesto que un equipo tiene varias consolas y varios usuarios pueden registrarse a la vez localmente, uno de los usuarios debe tener "prioridad" en la carrera por acceder a los archivos. El primer usuario que se registra en la consola será el propietario de dichos archivos. Una vez que el primer usuario sale de la sesión, el siguiente usuario que se registra pasa a ser el propietario de los archivos.

En contraste, *cada* usuario que se registra en la consola podrá ejecutar programas que realizan tareas normalmente restringidas para ser ejecutadas por usuario root. Si se ejecuta el sistema X, estas acciones se pueden incluir como elementos de menú en una interfaz gráfica de usuario. Tal y como se distribuyen, los programas accesibles desde una consola incluyen los comandos `halt`, `poweroff`, y `reboot`.

24.1. Desactivación del apagado con la combinación de teclas Ctrl-Alt-Del

Por defecto, `/etc/inittab` especifica que su sistema se ha establecido para apagarse y rearrancar el sistema si se utiliza la combinación de teclas [Ctrl]-[Alt]-[Del] en la consola. Si desea desactivar completamente esta opción, deberá crear un comentario en la línea `/etc/inittab` colocando un símbolo de numeral o almohadilla (`#`) en frente a ella:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Opcionalmente, puede estar interesado en permitir a algunos usuarios no root a que tengan derechos para apagar el sistema desde la consola con la combinación de teclas [Ctrl]-[Alt]-[Del]. Para limitar este privilegio a determinados usuarios, siga los pasos siguientes:

1. Agregue la opción `-a` a la línea `/etc/inittab` mostrada arriba, de modo que se lea lo siguiente:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   La bandera `-a` indica al comando `shutdown` que debe buscar el archivo `/etc/shutdown.allow`, que creará en el paso siguiente.
2. Cree un archivo denominado `shutdown.allow` en `/etc`. El archivo `shutdown.allow` debe mostrar los nombres de los usuarios que pueden apagar el sistema con la combinación de teclas [Ctrl]-[Alt]-[Del]. El formato del archivo `/etc/shutdown.allow` es una lista de nombres de usuario en cada línea. Por ejemplo:
   ```
   stephen
   jack
   sophie
   ```

Según el archivo `shutdown.allow` de ejemplo, los usuarios stephen, jack, y sophie pueden apagar el sistema desde la consola con [Ctrl]-[Alt]-[Del]. Cuando se utiliza esta combinación de teclas, el archivo `shutdown -a` en `/etc/inittab` comprueba si alguno de los usuarios en `/etc/shutdown.allow` (o root) están registrados en una consola virtual. Si alguno de ellos lo está,

continuará el apagado del sistema; en caso contrario, se registrará un mensaje de error en la consola del sistema.

Para más información sobre `shutdown.allow`, consulte la página del manual para `shutdown`.

24.2. Desactivación del acceso a programas de la consola

Para desactivar el acceso de los usuarios a los programas de la consola, debe ejecutar este comando como root:

```
rm -f /etc/security/console.apps/*
```

En los entornos en los que la consola tiene otro sistema de seguridad (se han establecido contraseñas en la BIOS y en el gestor de arranque, se ha desactivado la combinación de teclas [Ctrl]-[Alt]-[Delete], se han desabilitado los interruptores de encendido y reinicio, etc.), probablemente no desee que ningún usuario que trabaje en una consola ejecute los comandos `poweroff`, `halt`, y `reboot`, a los que de manera predeterminada se puede tener acceso desde la consola.

Para quitar estas opciones, ejecute los comandos siguientes como root:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. Desactivación de todos los accesos a la consola

El módulo `pam_console.so` de PAM, gestiona los permisos y la autentificación de los archivos de la consola. (Consulte el *Manual de referencia de Red Hat Linux* para obtener más información sobre la configuración de PAM.) Si desea desactivar todos los accesos a la consola, incluyendo el acceso a programas y a archivos, coloque en comentarios todas las líneas que se refieren a `pam_console.so` en el directorio `/etc/pam.d`. Como usuario root, el siguiente script puede ayudarle:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo
$i
done
```

24.4. Definición de la consola

El módulo `pam_console.so` usa el archivo `/etc/security/console.perms` para determinar los permisos que tienen los usuarios en la consola del sistema. La sintaxis del archivo es muy flexible; puede modificar el archivo para que estas instrucciones dejen de ser válidas. Sin embargo, el archivo por defecto tiene una línea similar a la siguiente:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Cuando los usuarios se registran, se conectan a algún terminal, bien sea un servidor X con un nombre como `:0` o `mymachine.example.com:1.0` o un dispositivo como `/dev/ttyS0` o `/dev/pts/2`. La opción por defecto es definir esas consolas virtuales locales y que los servidores X locales se consideren locales, pero si desea considerar también el terminal serial próximo en el puerto `/dev/ttyS1` puede cambiar la línea para que muestre:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

```
/dev/ttyS1
```

24.5. Colocar los archivos accesibles desde la consola

En `/etc/security/console.perms`, hay una sección con líneas similares:

```
<floppy>=/dev/fd[0-1]* \
         /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

Puede agregar, si lo necesita, sus propias líneas a esta sección. Asegúrese de que todas las líneas que agregue hacen referencia al dispositivo pertinente. Por ejemplo, puede agregar la línea siguiente:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(Por supuesto, asegúrese de que `/dev/scanner` es realmente su scanner y no el disco duro, por ejemplo.)

Este es el primer paso. El segundo paso consiste en definir lo que se realiza con estos archivos. Observe la última sección de `/etc/security/console.perms` para buscar 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
```

Luego, cuando se registre en la consola, tendrá derechos de propiedad sobre el dispositivo `/dev/scanner` y los permisos serán 0600 (permiso exclusivo de lectura y escritura). Cuando cierre la sesión, el dispositivo será propiedad del root y seguirá teniendo permisos 0600 (ahora: permiso exclusivo de lectura y escritura para el usuario root).

24.6. Activación del acceso a la consola para otras aplicaciones

Si desea que los usuarios de la consola puedan acceder a otras aplicaciones tendrá que realizar un poco más de trabajo.

En primer lugar, el acceso a la consola *sólo* funciona para las aplicaciones que residen en `/sbin` o `/usr/sbin`, de modo que la aplicación que desee ejecutar deberá estar ubicada en este lugar. Después de verificar esto, siga los pasos siguientes:

1. Cree un vínculo del nombre de la aplicación, como el programa ejemplo *foo*, en 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/`. Un modo sencillo de realizar esto es empezar con una copia del archivo de configuración del servicio detenido y luego modificar el archivo si desea cambiar su comportamiento:

```
cp /etc/pam.d/halt
/etc/pam.d/foo
```

Ahora, cuando ejecute `/usr/bin/`*foo*, se llamará al comando `consolehelper`, el cual validará al usuario con la ayuda de `/usr/sbin/userhelper`. Para validar al usuario, `consolehelper` solicitará una contraseña del usuario si `/etc/pam.d/`*foo* es una copia de `/etc/pam.d/halt` (en caso contrario, hará precisamente lo que se haya especificado en `/etc/pam.d/`*foo*) y a continuación ejecutará `/usr/sbin/`*foo* con permisos de root.

En el archivo de configuración PAM, una aplicación puede ser configurada para usar el módulo *pam_timestamp* para recordar (caché) un intento de conexión exitoso. Cuando una aplicación inicia y se proporciona una autentificación adecuada (la contraseña de root), se crea un archivo timestamp. Por defecto, una validación con éxito está cacheada durante cinco minutos. Durante este tiempo, cualquier otra aplicación que sea configurada para usar `pam_timestamp` y ejecutar desde la misma sesión, está automáticamente autenticada para el usuario — el usuario no introduce la contraseña de root de nuevo.

Este módulo está incluido en el paquete `pam`. Para activar esta característica, el archivo de configuración PAM en `etc/pam.d/` debe incluir las líneas siguientes:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

La primera línea que inicie con `auth` debería estar tras cualquier otra línea `auth sufficient` y la línea que empieza con `session` debería estar tras cualquier otra línea `session optional`.

Si una aplicación configurada para usar `pam_timestamp` es validada exitósamente desde el **Botón de Menú Principal** (en el Panel), el  icono es desplegado en el área de notificación del panel si está ejecutando el entorno de escritorio GNOME. Después que la autentificación caduca (por defecto cinco minutos), el icono desaparece.

El usuario puede seleccionar olvidar la autentificación cacheada al pulsar el icono y seleccionar la opción de olvidar la autentificación.

24.7. El Grupo `floppy`

Si, por cualquier motivo, el acceso a la consola no es adecuado para usted y necesita conceder acceso a los usuarios no root a la unidad de disquete del sistema, puede hacerlo con el grupo `floppy`. Simplemente agregue el usuario(s) al grupo `floppy` usando la herramienta de su preferencia. A continuación se incluye un ejemplo mostrando cómo utilizar `gpasswd` para añadir un usuario fred al grupo `floppy`:

```
[root@bigdog root]# gpasswd -a fred
floppy
Adding user fred to group floppy
[root@bigdog root]#
```

A partir de este momento, el usuario fred podrá acceder a la unidad de disquete del sistema desde la consola.

Capítulo 25.

Configuración de grupos y de usuarios

El **Administrador de usuarios** le permite visualizar, modificar, añadir y borrar los usuarios y grupos locales.

Para usar el **Administrador de usuarios**, debe estar ejecutando el sistema X Window y tener privilegios de root y tener el paquete RPM `redhat-config-users` instalado. Para iniciar el **Administrador de usuarios** desde el escritorio, vaya a **Botón del menú principal** (en el Panel) => **Configuración del sistema** => **Gestor de usuarios** o escriba el comando `redhat-config-users` en el intérprete del shell (en un terminal XTerm o GNOME, por ejemplo).

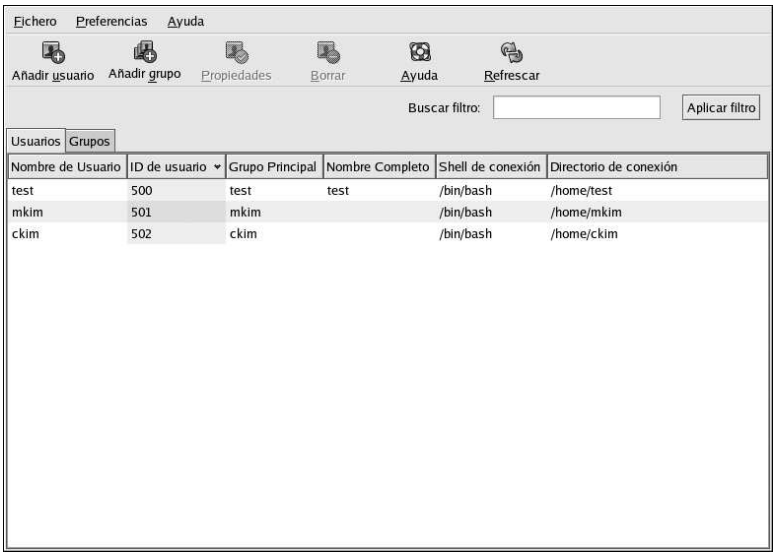

Figura 25-1. Administrador de usuarios

Para visualizar una lista de usuarios locales del sistema, haga click en la pestaña **Usuarios**. Para visualizar una lista de todos los grupos locales del sistema, haga click en la pestaña **Grupos**.

Si necesita encontrar un usuario o grupo específico, teclee las primeras letras del nombre en el campo **Buscar filtro**. Pulse [Intro] o haga click en el botón **Aplicar filtro**. Aparecerá la lista filtrada.

Para clasificar usuarios y grupos, haga click en el nombre de la columna. Usuarios y grupos serán clasificados por el valor de la columna.

Red Hat Linux reserva los IDs de usuario por debajo de 500 para los usuarios del sistema. Por defecto, el **Administrador de usuarios** no visualiza los usuarios del sistema. Para visualizar todos los usuarios, incluyendo los usuarios del sistema, anule la selección **Preferencias** => **Sistema de filtrado de usuarios y grupos** desde el menú desplegable.

Para más información sobre usuarios y grupos, remítase al *Manual de referencia de Red Hat Linux* y al *Manual de administración del sistema de Red Hat Linux*.

25.1. Añadir un nuevo usuario

Para añadir un nuevo usuario, haga click en el botón **Añadir usuario**. Aparecerá una ventana como la que se muestra en la Figura 25-2. Escriba el nombre de usuario y el nombre completo para el nuevo usuario en los campos apropiados. Teclee la contraseña de usuario en los campos **Contraseña** y **Confirmar contraseña**. La contraseña debe contar al menos con seis caracteres.

Aviso

Cuanto más larga sea una contraseña, más difícil es que alguien la adivine y se registre en la cuenta de usuario sin permiso. Es aconsejable que la contraseña no sea una palabra sino una combinación de letras, números y caracteres especiales.

Seleccione una shell de registro. Si no está seguro de qué shell seleccionar, acepte el valor por defecto de `/bin/bash`. El directorio principal por defecto es `/home/`*`nombredeusuario`*. Puede cambiar el directorio principal que se ha creado para el usuario o puede escoger no crear el directorio principal anulando la selección **Crear directorio de conexión**.

Si seleccionó crear el directorio principal, los archivos de configuración por defecto son copiados desde el directorio `/etc/skel` en el nuevo directorio.

Red Hat Linux utiliza un esquema *grupo de usuario privado* (UPG). El esquema UPG no añade ni cambia nada en el modo estándar de UNIX de gestionar grupos; simplemente ofrece una nueva convención. Siempre que cree un nuevo usuario, por defecto, se crea un grupo único con el mismo nombre que el del usuario. Si no desea crear este grupo, anule la selección **Crear un nuevo grupo para este usuario**.

Para especificar el ID del usuario, seleccione **Especificar el ID del usuario manualmente**. Si la opción no ha sido seleccionada, se asignará al nuevo usuario el próximo ID del usuario disponible que empiece con el número 500. Red Hat Linux se reserva los IDs de usuario por debajo de 500 para los usuarios de sistemas.

Pulse **OK** para crear el usuario.

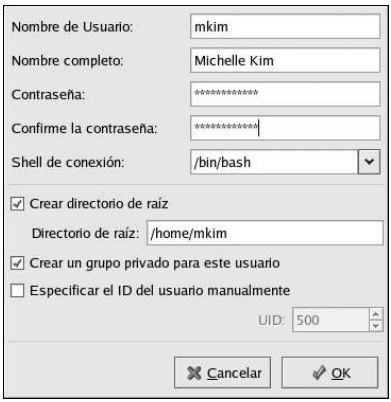

Figura 25-2. Nuevo usuario

Para configurar las propiedades de usuario más avanzadas como la caducidad de la contraseña, modifique las propiedades del usuario tras añadir el usuario. Remítase a la Sección 25.2 para más información.

Para añadir el usuario a otros muchos grupos, haga click en la pestaña **Usuarios**, seleccione el usuario pulse **Propiedades**. En la ventana de **Propiedades de usuarios**, seleccione la pestaña **Grupos** Seleccione los grupos de los que desea que el usuario forme parte, seleccione el grupo primario y haga click en **OK**.

25.2. Modificar las propiedades del usuario

Para ver las propiedades de un usuario ya existente, haga click en la pestaña **Usuarios**, seleccione el usuario de la lista de usuarios y haga click en **Propiedades** desde el menú de botones (o escoja **Fichero => Propiedades** desde el menú desplegable). Aparecerá una ventana parecida a la Figura 25-3.

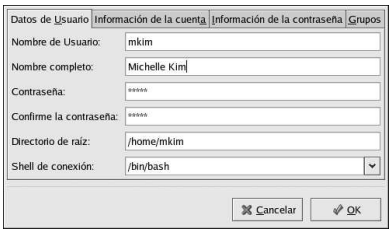

Figura 25-3. Propiedades del usuario

La ventana **Propiedades de los usuarios** está dividida en dos páginas:

- **Datos de Usuario** — Información básica del usuario configurada cuando ha añadido el usuario. Utilice esta pestaña para cambiar el nombre completo del usuario, la contraseña, el directorio principal o la shell de registro.
- **Información de la cuenta** — Seleccione **Activar expiración de cuenta** si quiere que la cuenta caduque en una fecha determinada. Introduzca la fecha en los campos pertinentes. Seleccione **La cuenta del usuario está bloqueada** para bloquear la cuenta de usuario de manera que el usuario no pueda entrar en el sistema.
- **Información de la contraseña** — Esta pestaña muestra la fecha en que el usuario cambió la contraseña por última vez. Para hacer que el usuario cambie la contraseña después de unos cuantos días, seleccione **Activar expiración de contraseña**. Podrá establecer el número de días antes de que al usuario se le permita cambiar su contraseña, el número de días previos al aviso al usuario para que cambie su contraseña y los días anteriores a que la cuenta pase a ser inactiva.
- **Grupos** — Seleccione los grupos de los que desea que el usuario sea miembro.

25.3. Añadir un nuevo grupo

Para añadir un nuevo grupo de usuarios, pulse el botón **Añadir Grupo**. Aparecerá una ventana parecida a la Figura 25-4. Escriba el nombre del grupo nuevo que desea crear. Para especificar un ID de grupo para el nuevo grupo seleccione **Especificar el ID de grupo manualmente** y seleccione el GID. Red Hat Linux reserva los IDs de grupo menores de 500 para los grupos de sistemas.

Pulse **OK** para crear el grupo. Aparecerá un grupo nuevo en la lista.

Figura 25-4. Nuevo grupo

Para añadir usuarios al grupo, remítase a la Sección 25.4.

25.4. Modificar las propiedades del grupo

Para ver las propiedades de un grupo ya existente, seleccione el grupo desde la lista de grupos y pulse **Propiedades** desde el menú (o seleccione **Archivo => Propiedades** desde el menú desplegable). Aparecerá una ventana similar a la Figura 25-5.

Figura 25-5. Propiedades del grupo

La pestaña **Usuarios de grupo** visualiza qué usuarios son miembros del grupo. Seleccione los usuarios adicionales para añadirlos al grupo y anule la selección de los usuarios para eliminarlos. Haga click en **OK** o **Aplicar** para modificar los usuarios en el grupo.

25.5. Configuración de usuarios desde la línea de comandos

Si prefiere las herramientas de línea de comandos o no tiene el sistema X Window instalado, use este capítulo para configurar usuarios y grupos.

25.5.1. Añadir un usuario

Para añadir un usuario al sistema:

1. Emita el comando `useradd` para crear una cuenta de usuario bloqueada:
   `useradd <username>`
2. Desbloquee la cuenta ejecutando el comando `passwd` para asignar una contraseña y configurar el vencimiento de la misma:
   `passwd <username>`

Las opciones de línea de comandos para `useradd` están en la Tabla 25-1.

Opción	Descripción
`-c` *`comentario`*	Comentario para el usuario
`-d` *`home-dir`*	Directorio principal a ser usado en vez del directorio predeterminado `/home/`*`nombredeusuario`*
`-e` *`fecha`*	Fecha en que la cuenta será desactivada usando el formato de fecha YYYY-MM-DD
`-f` *`días`*	Número de días que pasarán después que la contraseña ha caducado hasta que la cuenta se desactivará (Si se especifica **`0`**, la cuenta será desactivada inmediatamente después que la contraseña expire. Si se especifica **`-1`**, la cuenta no se desactivará después que la contraseña caduque.)
`-g` *`nombredegrupo`*	Nombre o número del grupo para el grupo predeterminado del usuario (El grupo debe existir.)
`-G` *`listadegrupo`*	Lista de nombres de los grupos adicionales (además del predeterminado), separados por comas, de los cuales el usuario es miembro (Los grupos deben existir.)
`-m`	Crea el directorio principal si no existe
`-M`	No crea el directorio principal
`-n`	No crea un grupo de usuario privado para el usuario
`-r`	Crea una cuenta de sistema con un UID menor que 500 y dentro del directorio principal.
`-p` *`contraseña`*	La contraseña encriptada con `crypt`
`-s`	Línea de comando de conexión del usuario, predeterminada a `/bin/bash`
`-u` *`uid`*	ID de usuario, el cual debe ser único y mayor que 499

Tabla 25-1. Opciones de línea de comandos para `useradd`

25.5.2. Añadir un grupo

Para agregar un grupo al sistema, use el comando `groupadd`:

`groupadd <`*`nombredegrupo`*`>`

Las opciones de línea de comando para `groupadd` están en la Tabla 25-2.

Opción	Descripción
`-g` *`gid`*	ID para el grupo, el cual debe ser único y mayor que 499.
`-r`	Crea un grupo de sistema con un GID menor que 500.
`-f`	Sale con un error si el grupo ya existe. (El grupo no es alterado.) Si se especifica `-g` y `-f`, pero el grupo ya existe, la opción `-g` es ignorada.

Tabla 25-2. Opciones de línea de comando para `groupadd`

25.5.3. Vencimiento de la contraseña

Si las contraseña dentro de la organización son creadas centralmente por el administrador, al agregar nuevos usuarios significa que el administrador debe configurar la cuenta del usuario de manera que cuando el usuario se conecte por primera vez, el sistema le pedirá que cree una contraseña. Esto se puede hacer cuando se añade o modifica un usuario en la pestaña **Información de contraseña** del **Administrador de usuarios**.

Para configurar el vencimiento de la contraseña para un usuario desde el intérprete de comandos, use el comando `chage`, seguido de una opción desde la Tabla 25-3, seguido por el 'nombredeusuario' del usuario.

Importante

La contraseña oculta debe estar activada para poder usar el comando `chage`.

Opción	Descripción
`-m` *días*	Especifica el número mínimo de días entre los cuales el usuario debe cambiar su contraseña. Si el valor es 0, la contraseña no caduca.
`-M` *días*	Especifica el número máximo de días durante los cuales la contraseña es válida. Cuando el número de días especificado por esta opción más el número de días especificado con la opción `-d` es menor que el día actual, el usuario debe cambiar su contraseña antes de usar la cuenta.
`-d` *días*	Especifica el número de días desde Enero 1, 1970 que la contraseña fué cambiada.
`-I` *días*	Especifica el número de días inactivos después de la expiración de la contraseña antes de bloquear la cuenta. Si el valor es 0, la cuenta no es bloqueada después que la contraseña caduca.
`-E` *fecha*	Especifica la fecha en la cual la cuenta es bloqueada, en el formato YYYY-MM-DD. También se puede usar el número de días transcurridos desde Enero 1, 1970 en lugar de la fecha.
`-W` *días*	Especifica el número de días antes de la fecha de expiración de la contraseña para advertir al usuario.

Tabla 25-3. Opciones de línea de comando de `change`

Sugerencia

Si el comando `chage` está seguido directamente por un nombre de usuario (sin opciones), se visualizará los valores de vencimiento de la contraseña actual y le permite cambiar estos valores.

Si el administrador del sistema desea que un usuario configure su contraseña la primera vez que éste se conecte, la contraseña del usuario puede ser configurada a que expire de inmediato, obligando al usuario a cambiarla inmediatamente después de conectarse la primera vez.

Para obligar al usuario a configurar su contraseña la primera vez que se conecte en la consola, siga los pasos siguientes. Este proceso no funciona si el usuario se conecta usando el protocolo SSH.

1. *Bloquear la contraseña del usuario* — Si el usuario no existe, use el comando `useradd` para crear la cuenta del usuario, pero no le de la contraseña para que así permanezca bloqueada.

   Si la contraseña ya está activa, bloquéela con el comando:
   `usermod -L nombredeusuario`

2. *Obligar el vencimiento inmediato de la contraseña* — Escriba el comando siguiente:
   `chage -d 0 nombredeusuario`

   Este comando coloca el valor para la fecha en que la contraseña fué cambiada la última vez (Enero 1, 1970). Este valor obliga a la expiración inmediata de la contraseña sin tomar en cuenta la política de vencimiento, si existe alguna.

3. *Desbloquear la cuenta* — Hay dos formas comunes para realizar este paso. El administrador puede asignar una contraseña inicial o puede asignar una contraseña nula.

   
   Aviso

   No use `passwd` para configurar una contraseña porque desactivará el vencimiento inmediato que se acaba de configurar.

   Para asignar una contraseña inicial, siga los pasos siguientes:

   - Arranque el intérprete de línea de comandos `python` con el comando `python`. Se mostrará lo siguiente:
     ```
     Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
     [GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
     Type "help", "copyright", "credits" or "license" for more information.
     >>>
     ```
   - En la línea de comandos, escriba lo siguiente (sustituyendo *`contraseña`* con la contraseña a encriptar y *`salt`* con una combinación de exáctamente 2 caracteres en mayúsculas o minúsculas, números, y el caractes punto (.) o la barra (/)):
     ```
     import crypt; print
     crypt.crypt("password","salt")
     ```
     La salida es la contraseña encriptada similar a `12CsGd8FRcMSM`.
   - Presione [Ctrl]-[D] para salir del intérprete Python.
   - Corte o pegue la salida exacta de la contraseña encriptada, sin dejar espacios en blanco al principio o final, en el siguiente comando:
     ```
     usermod -p "contraseña-encriptada"
     nombredeusuario
     ```

   En vez de asignar una contraseña inicial, se puede asignar una contraseña nula con el comando:
   `usermod -p "" username`

   
   Atención

   A pesar de que el uso de una contraseña nula es conveniente tanto para el administrador como para el usuario, existe el pequeño riesgo de que un tercero se conecte primero y accese el sistema. Para minimizar esta amenaza, se recomienda que los administradores verifiquen que el usuario está listo para conectarse cuando desbloqueen la cuenta.

   En cualquier caso, luego de la conexión inicial, se le pedirá al usuario una nueva contraseña.

25.6. Explicación del proceso

Los siguientes pasos describen lo que ocurre si se ejecuta el comando `useradd juan` en un sistema que tiene contraseñas ocultas activadas:

1. Se crea una nueva línea para `juan` en `/etc/passwd`. La línea tiene las características siguientes:
   - Comienza con el nombre del usuario, `juan`.
   - Hay una `x` para el campo de contraseña indicando que es sistema está usando contraseñas ocultas.
   - Se crea un UID en o sobre 500. (Bajo Red Hat Linux UIDs y GIDs debajo de 500 son reservados para uso del sistema.)
   - Se crea un GID en o por encima de 500.
   - La información para el GECOS óptimo se deja en blanco.
   - El directorio principal se configura a `/home/juan/`.
   - El intérprete de comandos predeterminado se configura a `/bin/bash`.

2. Se crea una nueva línea para `juan` en `/etc/shadow`. La línea tiene las características siguientes:
   - Comienza con el nombre del usuario, `juan`.
   - Aparecen dos símbolos de exclamación (`!!`) en el campo de la contraseña del archivo `/etc/shadow`, lo cual bloquea la cuenta.

     

     Nota

     Si se pasa una contraseña encriptada usando la opción `-p`, se colocará en el archivo `/etc/shadow` en la nueva línea para el usuario.

   - Se configura la contraseña para que no caduque nunca.

3. Se crea una nueva línea para un grupo llamado `juan` en `/etc/group`. Un grupo con el mismo nombre del usuario se conoce como un *grupo de usuario privado*. Para más información sobre los grupos de usuario privados, consulte la Sección 25.1.

   La línea creada en `/etc/group` tiene las características siguientes:
   - Comienza con el nombre del grupo, `juan`.
   - Aparece una `x` en el campo de contraseña indicando que el sistema está usando contraseñas de grupo oculta.
   - El GID coincide con el listado para el usuario `juan` en `/etc/passwd`.

4. Es creada una nueva línea para un grupo llamado `juan` en `/etc/gshadow`. La línea tiene las siguientes características:
   - Comienza con el nombre del grupo, `juan`.
   - Aparece un símbolo de exclamación (`!`) en el campo de contraseña del archivo `/etc/gshadow`, lo cual bloquea el grupo.
   - Todos los otros campos quedan en blanco.

5. Se crea un directorio para el usuario `juan` en el directorio `/home/`. Este directorio tiene como dueño al usuario `juan` y al grupo `juan`. Sin embargo, tiene privilegios para leer, escribir y ejecutar *sólo* para el usuario `juan`. Todos los demás permisos son denegados.
6. Los archivos dentro del directorio `/etc/skel/` (lo cual contiene configuraciones predeterminadas del usuario) son copiadas en el nuevo directorio `/home/juan/`.

En este punto, existe una cuenta bloqueda llamada `juan` en el sistema. Para activarla, el administrador debe asignar una contraseña a la cuenta usando el comando `passwd` y, opcionalmente, especificar las pautas de vencimiento de la misma.

Capítulo 26.

Reunir información del sistema

Antes de aprender a configurar su sistema, debería aprender cómo obtener la información esencial sobre su sistema. Por ejemplo, debería saber como encontrar información sobre cuánta memoria tiene disponible, el tamaño de su disco duro, cómo está particionado y qué procesos se están ejecutando. Esta capítulo trata sobre cómo recuperar este tipo de información a partir de sus sistema Red Hat Linux utilizando comandos fáciles y algunos programas.

26.1. Procesos del sistema

El comando `ps ax` muestra una lista de los procesos que se encuentran actualmente en el sistema, incluyendo los procesos que pertenecen a otros usuarios. Para mostrar el propietario de un proceso, utilice el comando `ps aux`. Esto es una lista estática de información, es decir, es una representación instantánea de los procesos que están en ejecución en el momento de invocar el comando. Si quiere obtener una lista de los procesos en ejecución de su sistema, utilice el comando `top` tal y como se describe más adelante.

La salida `ps` puede ser larga. Para evitar que haga scroll fuera de la pantalla, puede canalizarla a través de less:

```
ps aux | less
```

Puede utilizar el comando `ps` en combinación con el comando `grep` para ver si un proceso en concreto está en ejecución. Por ejemplo, para ver si **emacs** se esta ejecutando, utilice el comando:

```
ps ax | grep emacs
```

El comando `top` muestra los procesos que se encuentran actualmente en ejecución así como información importante sobre los mismos, como la memoria que utilizan y el tiempo de CPU que consumen. El resultado se muestra en una lista en tiempo real e interactiva. Un ejemplo de la salida en pantalla de `top` sería:

```
 00:53:01  up 6 days, 14:05,  3 users,  load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states:  18.0% user   0.1% system   16.0% nice   0.0% iowait  80.1% idle
Mem:  1030244k av,  985656k used,   44588k free,       0k shrd,  138692k buff
                    424252k actv,   23220k in_d,  252356k in_c
Swap: 2040212k av,  330132k used, 1710080k free                   521796k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
15775 joe        5   0 11028  10M  3192 S     1.5  4.2   0:46 emacs
14429 root      15   0 63620  62M  3284 R     0.5 24.7  63:33 X
17372 joe       11   0  1056 1056   840 R     0.5  0.4   0:00 top
17356 joe        2   0  4104 4104  3244 S     0.3  1.5   0:00 gnome-terminal
    1 root       0   0   544  544   476 S     0.0  0.2   0:06 init
    2 root       0   0     0    0     0 SW    0.0  0.0   0:00 kflushd
    3 root       1   0     0    0     0 SW    0.0  0.0   0:24 kupdate
    4 root       0   0     0    0     0 SW    0.0  0.0   0:00 kpiod
    5 root       0   0     0    0     0 SW    0.0  0.0   0:29 kswapd
  347 root       0   0   556  556   460 S     0.0  0.2   0:00 syslogd
  357 root       0   0   712  712   360 S     0.0  0.2   0:00 klogd
  372 bin        0   0   692  692   584 S     0.0  0.2   0:00 portmap
  388 root       0   0     0    0     0 SW    0.0  0.0   0:00 lockd
  389 root       0   0     0    0     0 SW    0.0  0.0   0:00 rpciod
  414 root       0   0   436  432   372 S     0.0  0.1   0:00 apmd
```

```
  476 root       0   0   592  592   496 S     0.0  0.2   0:00 automount
```

Para salir de `top`, presione la tecla [q].

Existen comandos interactivos que puede usar con `top` entre los que se incluye:

Comando	Descripción
[Espacio]	Realiza un refresco de la pantalla
[h]	Muestra la pantalla de ayuda
[k]	Mata un proceso. Se le pedirá que introduzca el ID del proceso así como la señal que hay que enviarle.
[n]	Cambia el número de procesos que se muestran en pantalla. Se le pedirá que introduzca un número.
[u]	Ordena por usuario.
[M]	Ordena por uso de memoria.
[P]	Ordena por uso del CPU.

Tabla 26-1. Comando interactivos de `top`

Sugerencia

Aplicaciones como **Mozilla** y **Nautilus** son del tipo *thread-aware* — se crean enlaces o hilos (thread) múltiples para gestionar usuarios múltiples y peticiones múltiples y a cada enlace se le da un proceso ID. Por defecto, `ps` y `top` tan sólo visualizan el enlace principal (inicial). Para ver todos los enlaces, use el comando `ps -m` o escriba [Shift]-[H] en `top`.

Si prefiere una interfaz gráfica para `top`, puede usar el **Monitor del sistema GNOME**. Para arrancarlo desde el escritorio, seleccione **Botón de menú principal** (en el Panel) => **Herramientas del sistema** => **Monitor del sistema** o escriba `gnome-system-monitor` en el intérprete de comandos de la shell dentro del sistema X Window. Luego seleccione la pestaña **Listado de procesos**.

El **Monitor del sistema GNOME** le permite buscar el proceso en la lista de procesos en ejecución así como visualizar todos los procesos, sus procesos o los procesos activos.

Para obtener más información sobre un proceso, selecciónelo y haga click en el botón **Más Info**. Visualizará los detalles sobre el proceso en la parte inferior de la pantalla.

Para detener un proceso, selecciónelo y haga click en **Finalizar Proceso**. Esta función es útil para procesos que no respondan a la entrada del usuario.

Para ordenar por la información de una columna específica, haga click en el nombre de la columna. La columna en la que la información ha sido clasificada aparece en un color más oscuro.

Por defecto, el **Monitor del sistema de GNOME** no visualiza enlaces (hilos). Para cambiar preferencias, seleccione **Editar => Preferencias**, haga click en la pestaña **Listado de procesos** y seleccione **Mostrar hilos**. Las preferencias le permitirán configurar el intervalo de actualización, qué tipo de información visualizar sobre cada proceso por defecto y los colores de los gráficos del monitor del sistema.

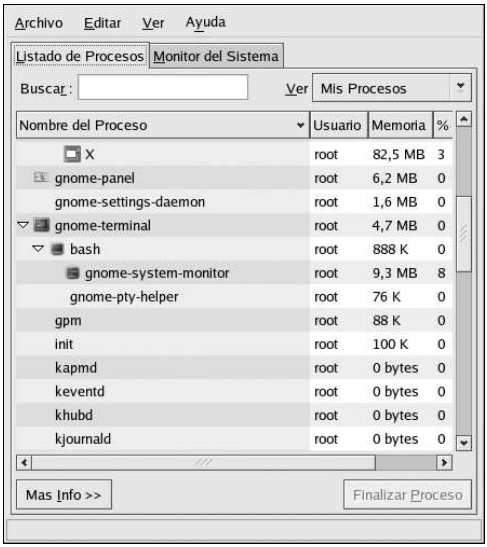

Figura 26-1. El Monitor del sistema de GNOME

26.2. Utilización de memoria

El comando `free` muestra el total de la memoria física y swap del sistema así como las cantidades de memoria que estamos utilizando, que queda libre, que está siendo compartida en buffers del kernel y cacheada.

```
             total       used       free     shared    buffers     cached
Mem:        256812     240668      16144     105176      50520      81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

El comando `free -m` muestra la misma información, pero en megabytes, lo cual es más fácil de leer.

```
             total       used       free     shared    buffers     cached
Mem:           250        235         15        102         49         79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

Si quiere utilizar una interfaz gráfica para `free`, puede usar el **Monitor del sistema de GNOME**. Para iniciarla desde el escritorio, vaya a **Botón de menú principal** (en el Panel) **=> Herramientas del sistema => Monitor del sistema** o en el intérprete de comandos de la shell, escriba `gnome-system-monitor`. A continuación escoja la pestaña **Monitor del sistema**.

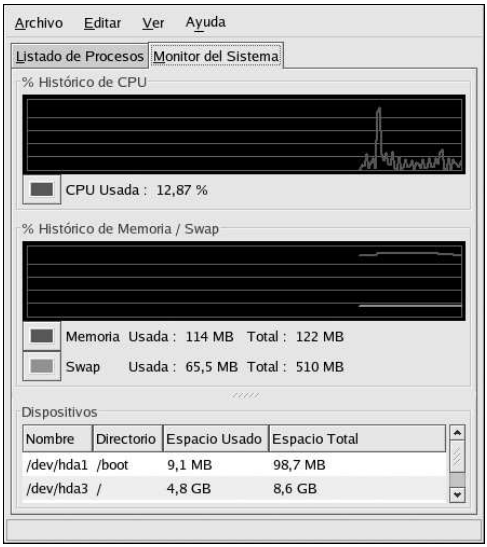

Figura 26-2. El Monitor del sistema de GNOME

26.3. Sistemas de archivos

El comando `df` le informa sobre la ocupación de disco que realiza el sistema. Si teclea el comando `df` en la línea del indicador de comandos, obtendrá la siguiente salida en pantalla:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda2             10325716   2902060   6899140  30% /
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

Por defecto, esta utilidad muestra el tamaño de las particiones en bloques de 1 kilobyte y el tamaño del espacio libre en kilobytes. Para ver esta información en megabytes y gigabytes, utilice el comando `df -h`. El argumento `-h` se utiliza para especificar un formato "legible" (human-readable format). La salida que obtendríamos en este caso sería tal y como se muestra a continuación:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

En la lista de particiones, existe una entrada para `/dev/shm`. Esta entrada representa el sistema de archivos de memoria virtual del sistema.

El comando `du` muestra la cantidad estimada de espacio que está siendo utilizado por los ficheros de un directorio. Si teclea `du` en la línea de comandos, la ocupación de disco de cada uno de los subdirectorios se mostrará por pantalla. Se mostrará también el espacio total ocupado en el directorio actual y en los subdirectorios del mismo en la última línea de la lista. Si no quiere ver los totales para

todos los subdirectorios, teclee `du -hs` y verá tan sólo el espacio total ocupado del directorio. Use el comando `du --help` para ver más opciones.

Para ver las particiones del sistema y el uso del espacio del disco en un formato gráfico, use la pestaña **Monitor del sistema** como se muestra en la Figura 26-2.

Sugerencia

Para más información sobre la implementación de quotas de disco, consulte el Capítulo 6.

26.3.1. Supervisión de sistemas de archivos

Red Hat Linux proporciona una utilidad llamada `diskcheck` que monitoriza la cantidad de espacio libre de disco en el sistema. Basándose en el fichero de configuración, puede mandar un email al administrador del sistema cuando uno o más discos alcanzan una determinada capacidad. Para usar esta utilidad, debe tener instalado el paquete RPM `diskcheck`.

Este utilidad se ejecuta como una tarea cron cada hora [1].

Las siguientes variables pueden ser definidas en `/etc/diskcheck.conf`:

- `defaultCutoff` — Cuando el disco llega al tanto por ciento de ocupación indicado, mandará un informe. Por ejemplo, si `defaultCutoff = 90`, se enviará un email cuando el disco monitorizado se llene al 90% de su capacidad.
- `cutoff[`*`/dev/partition`*`]` — Ignora el `defaultCutoff` para una partición. Por ejemplo, si especificamos `cutoff['/dev/hda3'] = 50`, `diskcheck` alertará al administrador del sistema cuando la partición `/dev/hda3` alcance el 50% de su capacidad.
- `cutoff[`*`/mountpoint`*`]` — Ignora el `defaultCutoff` para el punto de montaje. Por ejemplo, si especificamos `cutoff['/home'] = 50`, `diskcheck` alertará al administrador del sistema cuando el punto de montaje `/home` alcance el 50% de su capacidad.
- `exclude` — Especifica una o más particiones que `diskcheck` ignorará. Por ejemplo, si se especifica `exclude = "/dev/sda2 /dev/sda4"`, `diskcheck` no avisará al administrador del sistema si `/dev/sda2` o `/dev/sda4` llegan al porcentaje de ocupación especificado.
- `ignore` — Especifica uno o más tipos de sistemas de ficheros a ignorar en el formato `-x` *`filesystem-type`*. Por ejemplo, si se especifica `ignore = "-x nfs -x iso9660"`, el administrador del sistema no será alertado sobre los sistemas de ficheros nfs o iso9660.
- `mailTo` — Especifica la dirección de correo del administrador del sistema para avisarle cuando las particiones y puntos de montaje alcancen la capacidad especificada. Por ejemplo, si se especifica `mailTo = "webmaster@example.com"`, recibirá las alertas en webmaster@example.com.
- `mailFrom` — Especifica la identidad del emisor del email. Esto es útil si el administrador del sistema quiere filtrar el mail enviado por `diskcheck`. Por ejemplo, si se especifica `mailFrom = "Disk Usage Monitor"`, el email será enviado al administrador del sistema con el emisor "Monitorización de discos".
- `mailProg` — Especifica el programa de correo que se usará para enviar las alertas por email. Por ejemplo, si se especifica `mailProg = "/usr/sbin/sendmail"`, será usado Sendmail como el programa de mail.

No necesita reiniciar el servicio si cambia el archivo de configuración, ya que es leida cada vez que el cron lanza dicho servicio. Debería tener el servicio ejecutándose `crond` para que las tareas cron sean ejecutadas. Para determinar si el demonio se está ejecutando, utilice el comando `/sbin/service`

1. Consulte el Capítulo 28 para más información sobre cron.

`crond status`. Se le recomienda que inicie el servicio en el tiempo de arranque. Remítase al Capítulo 14 para obtener más detalles para iniciar el servicio cron de manera automática en el momento de arranque.

26.4. Hardware

Si tiene problemas con la configuración de su hardware o simplemente desea conocer qué hardware está en su sistema, puede utilizar la aplicación **Navegador de Hardware** para visualizar el hardware que se puede probar. Para iniciar el programa desde el escritorio, seleccione **Botón de menú principal => Herramientas del sistema => Navegador de Hardware** o escriba `hwbrowser` en el intérprete de comandos. Como se muestra en la Figura 26-3, se visualizarán los dispositivos en CD-ROM, los disquetes, los discos duros y sus particiones, los dispositivos de red, dispositivos puntero y las tarjetas de vídeo. Haga click en el nombre de la categoría en el menú de la izquierda y visualizará toda la información.

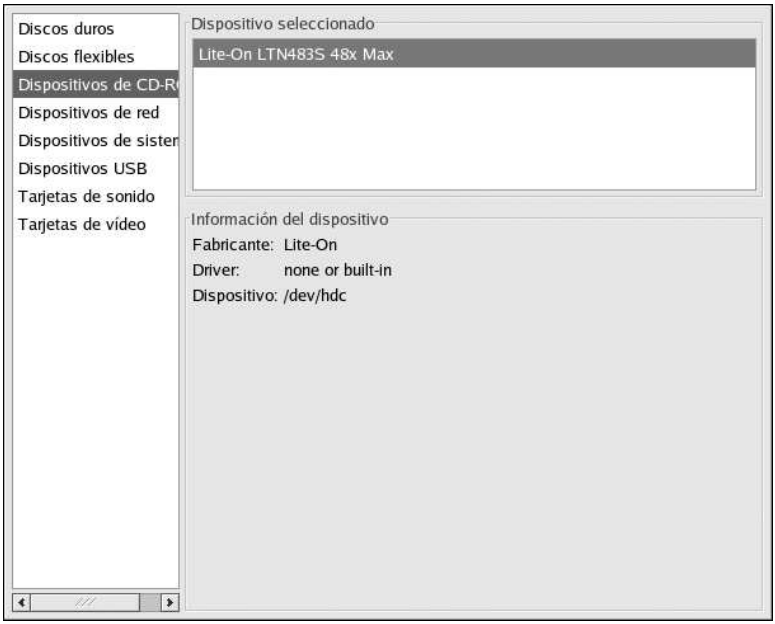

Figura 26-3. Navegador de Hardware

También puede utilizar el comando `lspci` para listar todos los dispositivos PCI. Use el comando `lspci -v` para ver información ampliada o `lspci -vv` para una salida de pantalla muy ampliada.

Por ejemplo, `lspci` puede usarse para determinar el fabricante, el modelo y el tamaño de la memoria de una tarjeta de vídeo:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-
if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
```

```
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

`lspci` es útil a la hora de determinar la tarjeta de red de su sistema si no conoce el fabricante o el número de modelo.

26.5. Recursos adicionales

Para aprender más sobre cómo obtener información del sistema, consulte los siguientes recursos.

26.5.1. Documentación instalada

- `ps --help` — Despliega una lista de opciones que pueden utilizarse con `ps`.
- Página del manual de `top` — Escriba `man top` para aprender más de `top` y sus muchas opciones.
- Página del manual de `free` — escriba `man free` para más detalles sobre `free` y sus opciones.
- Página del manual `df` — Escriba `man df` para más detalles sobre `df` y sus otras opciones.
- Página del manual de `du` — Utilice el comando `man du` para más información sobre `du` y sus opciones.
- Página del manual de `lspci` — Utilice el comando `man lspci` para ver más información sobre `lspci` y sus opciones.
- `/proc` — Los contenidos del directorio `/proc` pueden ser usados para reunir más información del sistema. Refiérase al *Manual de referencia de Red Hat Linux* para información adicional sobre el directorio `/proc`.

26.5.2. Libros relacionados

- *Manual de administración del sistema de Red Hat Linux*; Red Hat, Inc. — Incluye un capítulo sobre la monitorización de recursos.

Capítulo 27.

Configuración de la impresora

La **Herramienta de configuración de impresoras** permite a los usuarios configurar una impresora en Red Hat Linux. Esta herramienta ayuda a mantener el archivo de configuración de la impresora, los directorios spool y los filtros de impresión.

Desde la versión 9, Red Hat Linux, CUPS es el sistema de impresión predeterminado. Sin embargo, todavía se proporciona el sistema de impresión por defecto anterior, LPRng. Si el sistema fue actualizado desde una versión anterior de Red Hat Linux que usaba LPRng, el proceso de actualización no reemplaza LPRng con CUPS; el sistema continuará usando LPRng.

Si un sistema fue actualizado desde una versión anterior de Red Hat Linux que usaba CUPS, el proceso de actualización mantiene las colas configuradas y el sistema continuará usando CUPS.

La **Herramienta de configuración de impresoras** configura ambos sistemas de impresión CUPS y LPRng, dependiendo de cual se configure a usar en el sistema. Cuando aplique los cambios, configurará el sistema de impresión activo.

Para usar la **Herramienta de configuración de impresoras** debe tener privilegios como root. Para iniciar la aplicación, seleccione **Botón de menú principal** (en el Panel) => **Configuración del sistema => Impresión**, o escriba el comando `redhat-config-printer`. Este comando determina automáticamente si ejecutará la versión gráfica o la versión basada en texto dependiendo de si el comando es ejecutado desde el ambiente gráfico X Window o desde una consola basada en texto.

Puede forzar a la **Herramienta de configuración de impresoras** a ejecutarse como una aplicación basada en texto usando el comando `redhat-config-printer-tui` desde el intérprete de comandos.

Importante

No modifique el archivo `/etc/printcap` o los archivos en el directorio `/etc/cups/`. Cada vez que el demonio de impresión (`lpd` o `cups`) es iniciado o reiniciado, se crean dinámicamente nuevos archivos de configuración. Los archivos son creados dinámicamente cuando se aplican cambios con la **Herramienta de configuración de impresoras** también.

Si está usando LPRng y desea añadir una impresora sin usar la **Herramienta de configuración de impresoras**, modifique el archivo `/etc/printcap.local`. Las entradas en `/etc/printcap.local` no son desplegadas en la **Herramienta de configuración de impresoras** pero son leídas por el demonio de impresión. Si actualizó su sistema desde una versión anterior de Red Hat Linux, su archivo de configuración existente fue convertido al nuevo formato usado por esta aplicación. Cada vez que se genera un nuevo archivo de configuración, el archivo viejo es guardado como `/etc/printcap.old`.

Si está usando CUPS, la **Herramienta de configuración de impresoras** no despliega las colas o comparticiones que no hayan sido configuradas con la **Herramienta de configuración de impresoras**; sin embargo, no las eliminará de los archivos de configuración.

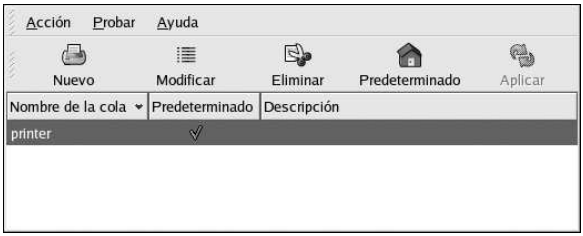

Figura 27-1. Herramienta de configuración de impresoras

Se pueden configurar los siguientes tipos de colas de impresión:

- **Conectada-localmente** — una impresora directamente conectada al computador a través de un puerto paralelo o USB.
- **Conectada CUPS (IPP)** — una impresora conectada a un sistema CUPS diferente que puede ser accesada sobre una red TCP/IP (por ejemplo, una impresora conectada a otro sistema Red Hat Linux corriendo CUPS en la red).
- **Conectada UNIX (LPD)** — una impresora conectada a un sistema UNIX diferente que puede ser accesada sobre una red TCP/IP (por ejemplo, una impresora conectada a otro sistema Red Hat Linux corriendo LPD en la red).
- **Conectada Windows (SMB)** — una impresora conectada a un sistema diferente el cual está compartiendo una impresora sobre una red SMB (por ejemplo, una impresora conectada a una máquina Microsoft Windows™).
- **Conectada Novell (NCP)** — una impresora conectada a un sistema diferente el cual usa la tecnología de red Novell NetWare.
- **Conectada JetDirect** — una impresora connectada directamente a la red a través de HP JetDirect en vez de a un computador.

Importante

Si agrega una nueva cola de impresión o modifica una existente, debe aplicar los cambios para que tomen efecto.

Al hacer click en el botón **Aplicar** guarda cualquier cambio que haya realizado y reinicia el demonio de impresión. Los cambios no son escritos al archivo de configuración hasta que el demonio de impresión no sea reiniciado. Alternativamente, puede seleccionar **Acción => Aplicar**.

27.1. Añadir una impresora local

Para añadir una impresora local, tal como una conectada al puerto paralelo o USB en su computador, haga click en **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras** para mostrar la ventana en la Figura 27-2. Haga click en **Siguiente** para proceder.

Figura 27-2. Añadir una impresora

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

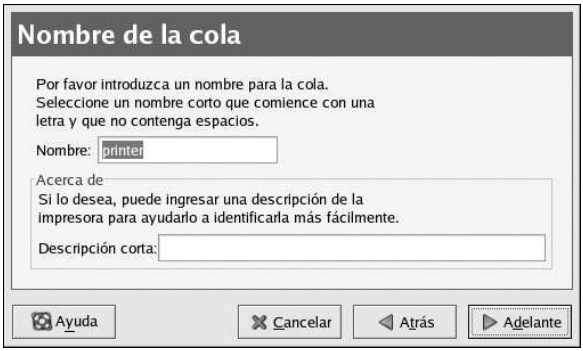

Figura 27-3. Seleccionar un nombre de cola

Después de hacer click en **Siguiente**, aparecerá la Figura 27-4. Seleccione **Conectado localmente** desde el menú **Seleccionar el tipo de cola** y seleccione el dispositivo. El dispositivo es usualmente `/dev/lp0` para una impresora paralela o `/dev/usb/lp0` para una impresora USB. Si no aparece ningún dispositivo en la lista, haga click en **Volver a escanear dispositivos** para revisar nuevamente la máquina o haga click en **Dispositivo personalizado** para especificarlo manualmente. Haga click en **Siguiente** para continuar.

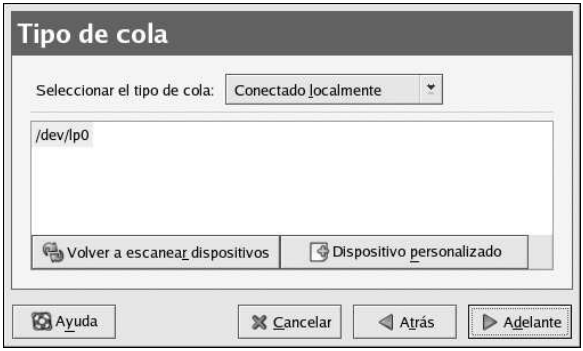

Figura 27-4. Añadir una impresora local

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

27.2. Añadir una impresora IPP

Una impresora de red IPP es una impresora conectada a un sistema Linux diferente en la misma red ejecutando CUPS o una impresora configurada para usar IPP en otro sistema operativo. Por defecto, la **Herramienta de configuración de impresoras** navega la red en busca de impresoras compartidas IPP. (Esta opción se puede cambiar seleccionando **Acción => Compartir** desde el menú.) Cualquier impresora IPP compartida aparecerá en la ventana principal.

Si tiene un cortafuegos (firewall) configurado en el servidor de impresión, este debe ser capaz de enviar y recibir conexiones en el puerto de entrada UDP 631. Si tiene un cortafuegos configurado en el cliente (la computadora enviando la petición de impresión), se le debe permitir enviar y aceptar conexiones en el puerto 631.

Si desactivó la característica automática de navegación, todavía puede agregar una impresora de red IPP haciendo click en el botón **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras** para desplegar la ventana en la Figura 27-2. Haga click en **Siguiente** para proceder.

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

Después de hacer click en **Siguiente**, aparecerá la Figura 27-5. Seleccione **Conectada CUPS (IPP)** desde el menú **Seleccionar un tipo de cola**.

Figura 27-5. Añadir una impresora de red IPP

Aparecen los campos de texto para las opciones siguientes:

- **Servidor** — El nombre de la máquina o dirección IP de la máquina remota a la cual la impresora está conectada.
- **Ruta** — La ruta de la cola de impresión en la máquina remota.

Haga click en **Siguiente** para continuar.

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

Importante

El servidor de impresión de red IPP debe permitir conexiones desde el sistema local. Consulte la Sección 27.13 para más información.

27.3. Añadir una impresora UNIX (LPD) remota

Para agregar una impresora UNIX remota, tal como una conectada a un sistema Linux diferente en la misma red, haga click en el botón **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras**. Aparecerá la ventana mostrada en la Figura 27-2. Haga click en **Siguiente** para proceder.

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

Seleccione **Conectada UNIX (LPD)** desde el menú **Seleccionar el tipo de cola** y haga click en **Siguiente**.

Figura 27-6. Añadir una impresora LPD remota

Aparecen los campos de texto para las opciones siguientes:

- **Servidor** — El nombre de la máquina o la dirección IP de la máquina remota a la cual la impresora está conectada.
- **Cola** — La cola de impresión remota. La impresora por defecto es usualmente `lp`.

Haga click en **Siguiente** para continuar.

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

Importante

El servidor de impresión remoto debe poder aceptar trabajos de impresión desde el sistema local. Consulte Sección 27.13.1 para más detalles.

27.4. Añadir una impresora Samba (SMB)

Para añadir una impresora que es accesada usando el protocolo SMB (tal como una impresora conectada a un sistema Microsoft Windows), haga click en el botón **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras**. Aparecerá la ventana mostrada en la Figura 27-2. Haga click en **Siguiente** para proceder.

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

Seleccione **Conectada a Windows (SMB)** desde el menú **Seleccionar un tipo de cola**, y haga click en **Siguiente**. Si la impresora está conectada a un sistema Microsoft Windows, seleccione este tipo de cola.

Figura 27-7. Añadir una impresora SMB

Como se muestra en la Figura 27-7, las comparticiones SMB son detectadas y listadas automáticamente. Haga click en la flecha al lado de cada nombre de compartición para ampliar la lista. Desde la lista ampliada, seleccione una impresora.

Si la impresora que está buscando no aparece en la lista, haga click en el botón **Especificar** a la derecha. Aparecerán los campos de texto para las siguientes opciones:

- **Grupo de trabajo** — El nombre del grupo de trabajo Samba para la impresora compartida.
- **Servidor** — El nombre del servidor compartiendo la impresora.
- **Compartir** — El nombre de la impresora compartida en la cual desea imprimir. Este nombre debe ser el mismo que el definido como la impresora Samba en la máquina Windows remota.
- **Nombre de usuario** — El nombre de usuario con el que debe conectarse para acceder a la impresora. Este usuario debe existir en el sistema Windows y el usuario debe tener permiso para accesar la impresora. El nombre de usuario predeterminado es típicamente **`guest`** para los servidores Windows, o **`nobody`** para los servidores Samba.
- **Contraseña** — La contraseña (si se necesita) para el usuario especificado en el campo **Nombre de usuario**.

Haga click en **Siguiente** para continuar. La **Herramienta de configuración de impresoras** luego intenta conectarse a la impresora compartida. Si la impresora compartida requiere un nombre de usuario y contraseña, aparecerá una ventana de diálogo pidiéndole que proporcione un nombre de usuario válido y contraseña. Si se especificó un nombre de compartición incorrecto, puede cambiarlo aquí también. Si un nombre de grupo de trabajo es requerido para conectarse a la compartición, se puede especificar en esta caja de diálogo. Esta ventana de diálogo es la misma que la mostrada cuando se hace click sobre el botón **Especificar**.

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

Aviso

Si requiere un nombre de usuario y una contraseña, estos son almacenados descifrados en archivos que sólo pueden ser accesados por root y lpd. Por tanto, es posible para otros conocer el nombre de usuario y la contraseña si ellos tienen acceso root. Para evitar esto, el nombre de usuario y la contraseña para accesar a la impresora deberían ser diferentes del nombre de usuario y la contraseña usados por la cuenta de usuario en el sistema local Red Hat Linux. Si son diferentes, entonces el único riesgo de seguridad posible será el uso no autorizado de la impresora. Si hay comparticiones de archivo del servidor, se recomienda que ellos también tengan una contraseña diferente de la de la cola de impresión.

27.5. Añadir una impresora Novell NetWare (NCP)

Para añadir una impresora Novell NetWare (NCP), haga click en el botón **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras**. Aparecerá la ventana mostrada en Figura 27-1. Haga click en **Siguiente** para proceder.

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

Seleccione **Conectada Novell (NCP)** del menú **Seleccionar un tipo de cola**.

Figura 27-8. Añadir una impresora NCP

Aparecerán campos de texto para las opciones siguientes:

- **Servidor** — El nombre de la máquina o dirección IP del sistema NCP al cual la impresora está conectada.
- **Cola** — La cola remota para la impresora en el sistema NCP.
- **Usuario** — El nombre del usuario que debe conectarse para accesar la impresora.
- **Contraseña** — La contraseña para el usuario especificado en el campo **Usuario**.

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

Aviso

Si requiere un nombre de usuario y una contraseña, estos son almacenados descifrados en archivos que sólo pueden ser accesados por root y lpd. Por tanto, es posible para otros conocer el nombre de usuario y la contraseña si ellos tienen acceso root. Para evitar esto, el nombre de usuario y la contraseña para accesar a la impresora deberían ser diferentes del nombre de usuario y la contraseña usados por la cuenta de usuario en el sistema local Red Hat Linux. Si son diferentes, entonces el único riesgo de seguridad posible será el uso no autorizado de la impresora. Si hay comparticiones de archivo del servidor, se recomienda que ellos también tengan una contraseña diferente de la de la cola de impresión.

27.6. Añadir una impresora JetDirect

Para agregar una impresora JetDirect, haga click en el botón **Nuevo** en la ventana principal de la **Herramienta de configuración de impresoras**. Aparecerá la ventana mostrada en la Figura 27-1. Haga click en **Siguiente** para proceder.

En la ventana mostrada en Figura 27-3, introduzca un nombre único para la impresora en el campo de texto **Nombre**. El nombre de la impresora no puede contener espacios y debe comenzar con una letra. El nombre de la impresora puede contener letras, números, guiones (-), y rayas (_). Opcionalmente, introduzca una descripción corta para la impresora, la cual puede contener espacios.

Seleccione **Conectada JetDirect** desde el menú **Seleccionar un tipo de cola**, y haga click en **Siguiente**.

Figura 27-9. Añadir una impresora JetDirect

Aparecerán los campos de texto para las siguientes opciones:

- **Impresora** — El nombre de la máquina o dirección IP de la impresora JetDirect.
- **Puerto** — El puerto en la impresora JetDirect que está escuchando por trabajos de impresión. El puerto predeterminado es 9100.

El próximo paso es seleccionar el tipo de impresora. Vaya a la Sección 27.7 para continuar.

27.7. Selección del modelo de impresora

Después de seleccionar el tipo de cola de impresión, el próximo paso es seleccionar el modelo de la impresora.

Verá una ventana similar a la Figura 27-10. Si no fue detectado automáticamente, seleccione el modelo de la lista. Las impresoras son divididas por fabricantes. Seleccione el nombre del fabricante desde el menú. Los modelos de impresoras son actualizados cada vez que un nuevo fabricante es seleccionado. Seleccione el modelo de impresora de la lista.

Figura 27-10. Selección del modelo de impresora

El controlador de la impresora recomendado es escogido basado en el modelo de impresora seleccionado. El controlador de la impresora procesa los datos que desea imprimir en un formato que la impresora pueda entender. Puesto que hay una impresora local conectada a su computador, necesita un controlador de impresora para procesar los datos que son enviados a la misma.

Si está configurando una impresora remota (IPP, LPD, SMB, or NCP), el servidor de impresión remoto usualmente tiene su propio controlador de impresión. Si selecciona un controlador de impresión adicional en su computador local, los datos son filtrados múltiples veces y convertido a un formato que la impresora no puede entender.

Para asegurarse de que los datos no son filtrados más de una vez, primero trate de seleccionar **Genérico** como el fabricante y **Cola de impresora sin formato** o **Impresora Postscript** como el modelo de impresora. Después de aplicar los cambios, imprima una página de prueba para probar la nueva configuración. Si la prueba falla, el servidor de impresión remoto puede que no tenga un controlador de impresora configurado. Intente seleccionando un controlador de acuerdo al fabricante y modelo de la impresora remota, aplique los cambios e imprima una página de prueba.

Sugerencia

Puede seleccionar un controlador de impresora diferente después de añadir una impresora iniciando la **Herramienta de configuración de impresoras**, seleccione la impresora desde la lista, y haga click en **Modificar**. Luego haga click en la pestaña **Controlador**, seleccione un controlador diferente y luego aplique los cambios.

27.7.1. Confirmación de la configuración de la impresora

El último paso es confirmar la configuración de su impresora. Haga click en **Aplicar** para agregar la cola de impresión si las configuraciones son correctas. Haga click en **Anterior** para modificar la configuración de la impresora.

Presione el botón **Aplicar** en la ventana principal para guardar sus cambios y reiniciar el demonio de impresión. Después de aplicar los cambios, imprima una página de prueba para asegurarse de que la configuración es correcta. Refiérase a la Sección 27.8 para más detalles.

Si necesita imprimir caracteres fuera del conjunto ASCII básico (incluyendo aquellos usados por idiomas tal como el Japonés), debe revisar las opciones de su controlador y seleccionar **Preparar Postscript**. Consulte la Sección 27.9 para más detalles. También puede configurar opciones tales como el tamaño del papel si modifica la cola de impresión después de haberla agregado.

27.8. Imprimiendo una página de prueba

Después de haber configurado su impresora, debería imprimir una página de prueba para asegurarse de que su impresora funciona perfectamente. Para imprimir una página de prueba, seleccione la impresora que desea probar desde la lista de impresoras, luego seleccione la página de prueba apropiada desde el menú **Probar**.

Si cambia el controlador de la impresora o modifica las opciones de la impresora, debería imprimir una página de prueba para verificar la nueva configuración.

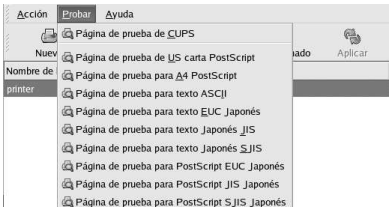

Figura 27-11. Opciones de la página de prueba

27.9. Modificar impresoras existentes

Para borrar una impresora existente, seleccione la impresora y haga click en el botón **Eliminar** en la barra de herramientas. La impresora será eliminada de la lista de impresoras. Haga click en **Aplicar** para guardar los cambios y reiniciar el demonio de impresión.

Para establecer la impresora por defecto, seleccione la impresora desde la lista y presione el botón **Predeterminado** en la barra de herramientas. Aparecerá el icono de la impresora por defecto en la columna **Predeterminado** de la impresora predeterminada en la lista.

Después de agregar una impresora, las propiedades se pueden modificar seleccionando la impresora desde la lista de impresoras y haciendo click en el botón **Modificar**. Se muestra la ventana con pestañas mostrada en Figura 27-12. La ventana contiene los valores actuales para la impresora seleccionada. Efectúe los cambios necesarios, y luego pulse el botón **OK**. Haga click **Aplicar** en la ventana principal de la **Herramienta de configuración de impresoras** para guardar los cambios y reiniciar el demonio de impresión.

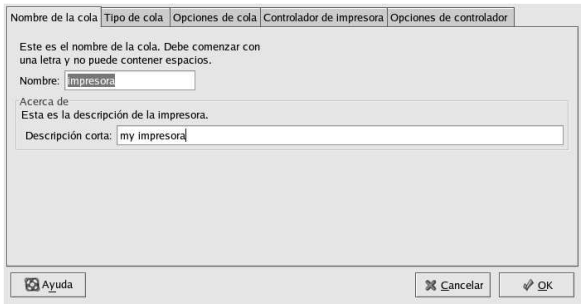

Figura 27-12. Modificar una impresora

27.9.1. Nombre de la cola

Para renombrar una impresora o cambiar su descripción, cambie el valor en la pestaña **Nombre de la cola**. Presione **OK** para volver a la ventana principal. El nombre de la impresora debería cambiar en la lista de impresoras. Haga click en **Aplicar** para guardar los cambios y reiniciar el demonio de impresión.

27.9.2. Tipo de cola

La pestaña **Tipo de cola** muestra el tipo de cola que fue seleccionada cuando se agregó la impresora y sus propiedades. El tipo de cola de la impresora se puede cambiar o simplemente las propiedades. Después de realizar las modificaciones, haga click en **OK** para volver a la ventana principal. Pulse **Aplicar** para guardar los cambios y reiniciar el demonio de impresión.

Dependiendo del tipo de cola escogido, se desplegarán opciones diferentes. Consulte la sección apropiada sobre Añadir impresoras para una descripción de las opciones.

27.9.3. Controlador de impresoras

La pestaña **Controlador de impresoras** muestra cúal controlador de impresora está siendo usado actualmente. Si se cambia, haga click en **OK** para volver a la pantalla principal. Pulse el botón **Aplicar** para guardar los cambios y reiniciar el demonio de impresión.

27.9.4. Opciones del controlador

La pestaña **Opciones de controladores** muestra las opciones avanzadas del controlador. Las opciones varían para cada controlador de impresoras. Las opciones comunes incluyen:

- **Envie Form-Feed (FF)** debería ser seleccionada si la última página del trabajo de impresión no sale de la impresora (por ejemplo, la luz de 'form feed' está brillando). Si esto no funciona, intente seleccionando **Envie un End-of-Transmission (EOT)**. Algunas impresoras requieren que ambos **Envie Form-Feed (FF)** y **Envie un End-of-Transmission (EOT)** esten seleccionados para expulsar la página. Esta opción sólo está disponible con el sistema de impresión LPRng.
- **Envie un End-of-Transmission (EOT)** debería ser seleccionado si 'form-feed' no funciona. Consulte **Envie Form-Feed (FF)** mostrado arriba. Esta opción sólo está disponible con el sistema de impresión LPRng.
- **Asume que los datos desconocidos son texto** debería estas seleccionado si el controlador de impresora no reconoce algunos de los datos enviados a él. Solamente seleccione esta opción si hay problemas imprimiendo. Si esta opción es seleccionada, el controlador de impresión asume que cualquier dato que no pueda reconocer es texto e intenta imprimirlo como texto. Si esta opción es seleccionada junto con **Convertir texto a Postscript**, el controlador de impresión asume que los datos desconocidos son texto y lo convierte a PostScript. Esta opción está disponible sólo con el sistema de impresión LPRng.
- **Preparar Postscript** debería estar seleccionado si se están enviando caracteres fuera del conjunto básico ASCII a la impresora pero no se están imprimiendo correctamente (tal como caracteres japoneses). Esta opción traduce las fuentes no-estándar PostScript para que se puedan imprimir correctamente.

  Si la impresora no soporta las fuentes que usted está tratando de imprimir, inténtelo seleccionando esta opción. Por ejemplo, seleccione esta opción para imprimir fuentes japonesas a una impresora no-japonesa.

  Se requiere tiempo adicional para realizar esta acción. No la seleccione a menos que tenga problemas imprimiendo las fuentes correctas.

También seleccione esta opción si la impresora no puede manejar PostScript de nivel 3. Esta opción lo convierte a PostScript de nivel 1.

- **Prefiltrado GhostScript** — le permite seleccionar **Sin prefiltrado**, **Convertir a PS de nivel 1**, o **Convertir a PS de nivel 2** en caso de que la impresora no pueda manejar ciertos niveles de PostScript. Esta opción sólo está disponible si el controlador de PostScript es usado con el sistema de impresión CUPS.
- **Convertir texto a Postscript** está seleccionado por defecto. Si la impresora puede imprimir texto plano, intente quitar esta opción cuando esté imprimiendo documentos de texto plano para reducir el tiempo que toma en imprimir. Si está usando el sistema CUPS, esto no es una opción porque el texto siempre se convierte a PostScript.
- **Tamaño de la página** le permite seleccionar el tamaño del papel. Las opciones incluyen Carta US, Legal, A3, y A4.
- **Localización del filtro efectivo** por defecto es **C**. Si se está imprimiendo caracteres japoneses, seleccione **ja_JP**. De lo contrario, accepte el valor por defecto de **C**.
- **Fuente de medios** por defecto está en **Impresora predeterminada**. Cambie esta opción para usar papel desde una bandeja diferente.

Para modificar las opciones de los controladores, haga click en **OK** para volver a la pantalla principal. Pulse **Aplicar** para guardar los cambios y reiniciar el demonio de impresión.

27.10. Guardar el archivo de configuración

Cuando la configuración de la impresora es guardada usando la **Herramienta de configuración de impresoras**, la aplicación crea su propio archivo de configuración que es usado para crear los archivos en el directorio `/etc/cups` (o el archivo `/etc/printcap` que `lpd` lee). Puede usar las opcioens de línea de comando para guardar o restaurar el archivo de la **Herramienta de configuración de impresoras**. Si el directorio `/etc/cups` o el archivo `/etc/printcap` es guardado y restaurado a las mismas ubicaciones, la configuración de la impresora no es restaurada porque cada vez que el demonio de impresión es iniciado, crea un nuevo archivo `/etc/printcap` desde el archivo especial de configuración **Herramienta de configuración de impresoras**. Cuando se esté haciendo un respaldo de los archivos de configuración del sistema, use el método siguiente para guardar los archivos de configuración de la impresora(s). Si el sistema está usando LPRng y se han añadido configuraciones personalizadas en el archivo `/etc/printcap.local`, debería guardarse como parte del respaldo también.

Para guardar la configuración de su impresora, escriba este comando como root:

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

Su configuración es guardada al archivo `settings.xml`.

Si se guarda este archivo, se puede usar para restaurar las configuraciones de la impresora. Esto es muy útil si la configuración de la impresora es borrada, si Red Hat Linux es reinstalado o si se necesita la misma configuración de impresoras en múltiples sistemas. El archivo debería guardarse en un sistema diferente antes de ser reinstalado. Para restaurar la configuración, escriba este comando como root:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

Si ya tiene un archivo de configuración (ya ha configurado una o más impresoras en el sistema) e intenta importar otro archivo de configuración, el archivo de configuración existente será sobreescrito. Si quiere conservar su configuración existente y agregar la configuración en el archivo guardado, puede mezclar los archivos con el comando siguiente (como root):

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

Su lista de impresoras consistirá de las impresoras que ha configurado en el sistema así como también las impresoras que importó desde el archivo de configuración guardado. Si el archivo de configuración importado tiene una cola de impresión con el mismo nombre de una cola existente en el sistema, la cola de impresión desde el archivo importado sobreescribirá la impresora existente.

Después de importar el archivo de configuración (con o sin el comando `merge`), debe reiniciar el demonio de impresión. Si está usando CUPS, escriba el comando:

```
/sbin/service cups restart
```

Si está usando LPRng, use el comando:

```
/sbin/service lpd restart
```

27.11. Configuración de línea de comandos

Si no tiene instalado el sistema X y no desea usar la versión basada en texto, puede añadir una impresora a través de la línea de comandos. Este método es muy útil si desea añadir una impresora desde un script o en la sección %post de una instalación de arranque rápido (kickstart).

27.11.1. Añadir una impresora local

Para agregar una impresora:

```
redhat-config-printer-tui --Xadd-local opciones
```

Opciones:

--device=*nodo*

(Requerido) El nodo dispositivo a ser usado. Por ejemplo, `/dev/lp0`.

--make=*make*

(Requerido) La cadena de caracteres IEEE 1284 MANUFACTURER o el nombre del fabricante de la impresora como en la base de datos foomatic si la cadena de caracteres del fabricante no está disponible.

--model=*modelo*

(Requerido) La cadena de caracteres IEEE 1284 MODEL o el modelo de la impresora listada en la base de datos foomatic si la cadena de caracteres no está disponible.

--name=*nombre*

(Opcional) El nombre dado a la nueva cola. Si alguno no está dado, será usado un nombre basado en el nodo dispositivo (tal como “lp0”).

--as-default

(Opcional) Configure esto como la cola predeterminada.

Si está usando CUPS como el sistema de impresión (predeterminado), después de añadir la impresora, use el comando siguiente para iniciar/reiniciar el demonio de impresión:

```
service cups restart
```

Si está usando LPRng como el sistema de impresión, después de agregar la impresora, use el comando siguiente para iniciar/reiniciar el demonio de impresión:

```
service lpd restart
```

27.11.2. Eliminar una impresora local

Una cola de impresión también se puede eliminar a través de la línea de comandos.

Como usuario root, para eliminar la cola de impresión:

```
redhat-config-printer-tui --Xremove-local opciones
```

Opciones:

--device=*nodo*

(Requerido) El nodo dispositivo usado tal como `/dev/lp0`.

--make=*make*

(Requerido) La cadena de caracteres de IEEE 1284 MANUFACTURER, o (si no hay ninguna disponible) el nombre del fabricante como aparece en la base de datos foomatic.

--model=*modelo*

(Requerido) La cadena de caracteres de IEEE 1284 MODEL, o (si no hay ninguna disponible) el modelo de la impresora como aparece listado en la base de datos foomatic.

Si está usando el sistema de impresión CUPS (predeterminado), después de eliminar la impresora de la configuración de la **Herramienta de configuración de impresoras**, reinicie el demonio de impresión para que los cambios tengan efecto:

```
service cups restart
```

Si está usando el sistema de impresión LPRng, después de eliminar la impresora desde la configuración en la **Herramienta de configuración de impresoras**, reinicie el demonio de impresión para que los cambios tengan efecto:

```
service lpd restart
```

Si está usando CUPS, ha removido todas las impresoras y no desea ejecutar el demonio de impresión otra vez, ejecute el comando siguiente:

```
service cups stop
```

Si está usando LPRng, ha eliminado todas las impresoras y no desea ejecutar el demonio de impresión otra vez, ejecute el comando:

```
service lpd stop
```

27.12. Administración de trabajos de impresión

Cuando usted envía un trabajo de impresión al demonio de impresión, tal como imprimir un archivo de texto desde **Emacs** o imprimir una imagen desde **El GIMP**, el trabajo de impresión es añadido al spool de la cola de impresión. El spool de la cola de impresión es una lista de los trabajos de impresión que han sido enviados a la impresora e información acerca de cada petición de impresión, tal como el estado de la petición, el nombre del usuario de la persona que envió la petición, el nombre de la máquina que lo envió, el número de trabajo, etc.

Si está ejecutando un ambiente gráfico de escritorio, haga click en el icono **Administrador de impresión** en el panel para arrancar el **Administrador de impresión GNOME** como se muestra en la Figura 27-13.

Figura 27-13. Administrador de impresión GNOME

También se puede arrancar seleccionando **Botón de menú principal** (en el Panel) => **Herramientas del sistema => Administrador de impresión**.

Para cambiar las configuraciones de la impresora, presione sobre el icono de la impresora con el botón derecho del ratón y seleccione **Propiedades**. La **Herramienta de configuración de impresoras** es iniciada.

Haga doble click sobre una impresora configurada para ver el spool de la cola como se muestra en la Figura 27-14.

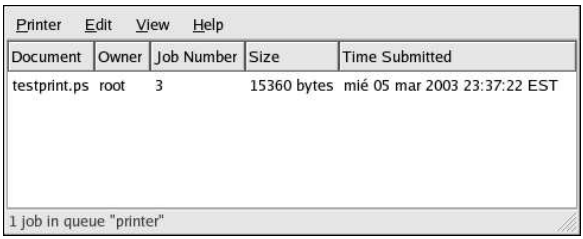

Figura 27-14. Lista de los trabajos de impresión

Para cancelar un trabajo específico de impresión listado en el **Administrador de impresión GNOME**, selecciónelo desde la lista y pulse **Modificar => Cancelar documentos** desde el menú desplegable.

Si hay trabajos activos de impresión en el spool, aparecerá un icono de notificación de impresión en el **Área de notificación del panel** del panel del escritorio, como se muestra en la Figura 27-15. Debido a que se verifica por trabajos de impresión activos cada cinco segundos, puede que no sea desplegado el icono para trabajos de impresión cortos.

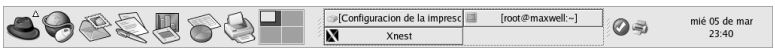

Figura 27-15. Icono de notificación de impresión

Haciendo click en el icono de notificación de impresión inicia el **Administrador de impresión GNOME** para mostrar una lista de los trabajos de impresión actuales.

También ubicado en el Panel está un icono **Administrador de impresión**. Para imprimir un archivo desde **Nautilus**, navegue hasta la ubicación del archivo y arrastre y suéltelo en el icono de **Administrador de impresión** en el Panel. Se despliega la ventana mostrada en la Figura 27-16. Haga click en **OK** para comenzar a imprimir el archivo.

Figura 27-16. Ventana de verificación de impresión

Para ver una lista de los trabajos de impresión en el spool de impresión desde el intérprete de comandos, escriba el comando `lpq`. Las últimas pocas líneas de la salida de este comando, serán similares a lo siguiente:

```
Rank    Owner/ID            Class  Job Files       Size Time
active user@localhost+902     A    902 sample.txt  2050 01:20:46
```

Ejemplo 27-1. Ejemplo de salida de `lpq`

Si desea cancelar un trabajo de impresión, encuentre el número del trabajo de la petición con el comando `lpq` y luego use el comando `lprm` *`número de trabajo`*. Por ejemplo, `lprm 902` cancelará el trabajo en Ejemplo 27-1. Debe tener los permisos adecuados para poder cancelar un trabajo de impresión. Usted no puede cancelar trabajos de impresión que fueron iniciados por otros usuarios a menos que usted se haya conectado como root en la máquina a la cual la impresora está conectada.

También puede imprimir un archivo directamente desde el intérprete de comandos. Por ejemplo, el comando `lpr sample.txt` imprimirá el archivo de texto `sample.txt`. El filtro de impresión determina qué tipo de archivos es y lo convierte a un formato de impresión que la impresora pueda entender.

27.13. Compartir una impresora

La habilidad de la **Herramienta de configuración de impresoras** de compartir las opciones de configuración sólo puede ser usada si está usando el sistema de impresión CUPS. Para configurar impresoras compartidas en un sistema LPRng, consulte Sección 27.13.1.

El permitir a otros usuarios en un computador diferente en la red imprimir a una impresora configurada para su sistema se llama *compartir* la impresora. Por defecto, las impresoras configuradas con la **Herramienta de configuración de impresoras** no están compartidas.

Para compartir una impresora configurada, arranque la **Herramienta de configuración de impresoras** y seleccione una impresora desde la lista. Luego seleccione **Acción => Compartir** desde el menú desplegable.

Nota

Si una impresora no está seleccionada, **Acción** => **Compartir** sólo muestra las opciones de compartir en el sistema mostradas normalmente bajo la pestaña **General**.

En la pestaña **Cola**, seleccione la opción para hacer la cola disponible a otros usuarios.

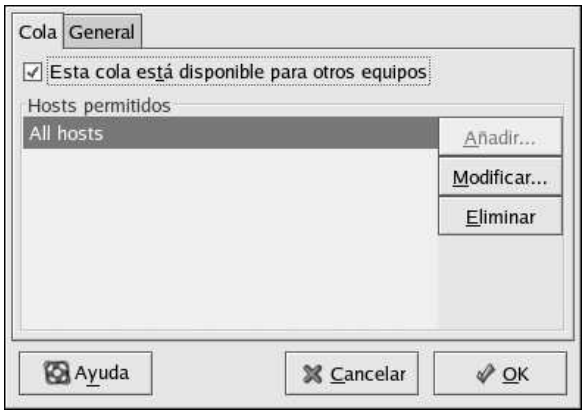

Figura 27-17. Opciones de la cola

Después de seleccionar compartir la cola, por defecto, *todas* las máquinas pueden imprimir a la impresora compartida. Permitir a todos los sistemas en la red imprimir a la cola puede ser un poco peligroso, especialmente si el sistema está directamente conectado a la Internet. Se recomienda que esta opción sea cambiada seleccionando la entrada **Todas las máquinas** y haciendo click en el botón **Modificar** para desplegar la ventana mostrada en la Figura 27-18.

Si tiene un cortafuegos (firewall) configurado en el servidor de impresión, éste debe ser capaz de enviar y recibir conexiones en el puerto UDP, 631. Si tiene un cortafuego configurado en el cliente (la computadora enviando la petición de impresión), éste debe poder enviar y aceptar conexiones en el puerto 631.

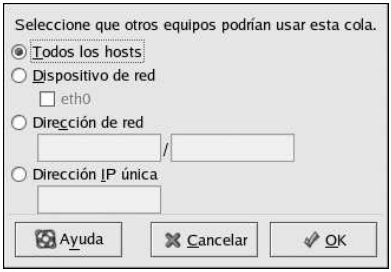

Figura 27-18. Hosts permitidos

La pestaña **General** establece configuraciones para todas las impresoras, incluyendo aquellas que no son visualizadas con la **Herramienta de configuración de impresoras**. Hay dos opciones:

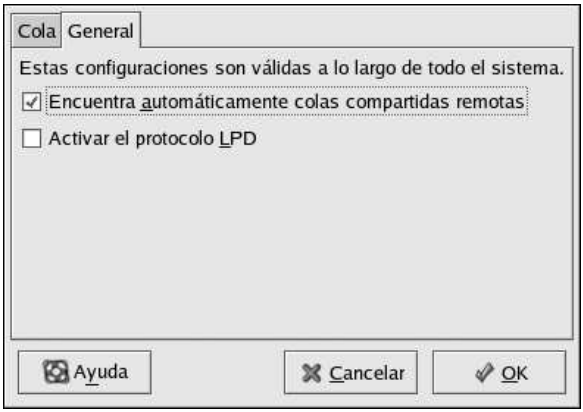

Figura 27-19. Opciones de ámbito del sistema para la impresión compartida

- **Encuentra automáticamente colas compartidas remotas** — Seleccionada como predeterminada, esta opción activa la navegación IPP, lo cual significa que cuando otras máquinas en la red difunden las colas que tienen, las colas son automáticamente agregadas a la lista de impresoras disponibles en el sistema; no se requiere configuración adicional para una impresora que es encontrada desde la navegación IPP. Esta opción no comparte automáticamente las impresoras configuradas en el sistema local.
- **Activar el protocolo LPD** — Esta opción permite a la impresora recibir trabajos de impresión de clientes configurados para usar el protocolo LPD usando el servicio `cups-lpd`, el cual es un servicio `xinetd`.

Aviso

Si esta opción está activada, todos los trabajos de impresión son aceptados desde todas las máquinas si son recibidos desde un cliente LPD.

27.13.1. Compartir una impresora con LPRng

Si está ejecutando el sistema de impresión LPRng, compartir debe ser configurado manualmente. Para permitir a los sistemas en la red imprimir a una impresora configurada en un sistema Red Hat Linux, siga los pasos siguientes:

1. Cree el archivo `/etc/accepthost`. En este archivo, añada la dirección IP o el nombre de la máquina al que desea permitir el acceso a la impresión, con una línea por IP o nombre de máquina.
2. Quite los comentarios de la siguiente línea en `/etc/lpd.perms`:
   ```
   ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
   ```
3. Reinicie el demonio para que los cambios tengan efecto:
   ```
   service lpd restart
   ```

27.14. Intercambiando sistemas de impresión

Para cambiar sistemas de impresión, ejecute la aplicación **Conmutador del sistema de impresión**. Iníciela seleccionando el **Botón de menú principal** (en el Panel) => **Configuración del sistema** => **Más configuraciones del sistema** => **Conmutador del sistema de impresión**, o escriba el comando `redhat-switch-printer` en la línea de comandos de la shell (por ejemplo, en un terminal XTerm o GNOME).

El programa detectará automáticamente si el sistema X Window se está ejecutando. Si es así, el programa arrancará en modo gráfico como se muestra en Figura 27-20. Si no se detecta X, arrancará en modo texto. Para forzarlo a que se ejecute en modo texto, use el comando `redhat-switch-printer-nox`.

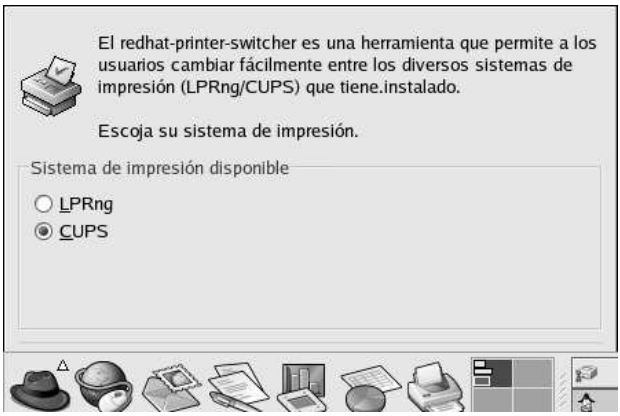

Figura 27-20. Conmutador del sistema de impresión

Seleccione bien sea **LPRng** o el sistema de impresión **CUPS**. En Red Hat Linux 9, CUPS es el sistema predeterminado. Si sólo tiene un sistema de impresión instalado, será la única opción mostrada.

Si selecciona **OK** para cambiar el sistema de impresión, el demonio de impresión seleccionado es activado para iniciarse en el momento de arranque y el demonio de impresión no seleccionado estará

desactivado para que no se inicie en el momento de arranque. El demonio de impresión seleccionado es iniciado y el otro demonio es detenido; así los cambiós tomarán efecto de inmediato.

27.15. Recursos adicionales

Para saber un poco más sobre la impresión en Red Hat Linux, puede consultar los recursos siguientes.

27.15.1. Documentación instalada

- `man printcap` — La página del manual para el archivo de configuración `/etc/printcap`.
- `map lpr` — La página del manual para el comando `lpr` que le permite imprimir archivos desde la línea de comandos.
- `man lpd` — La página del manual para el demonio de impresión LPRng.
- `man lprm` — La página del manual para la utilidad para eliminar los trabajos de impresión desde la cola del spool LPRng.
- `man mpage` — La página del manual para la utilidad de línea de comandos para imprimir múltiples páginas en una hoja de papel.
- `man cupsd` — La página del manual para el demonio de impresión CUPS.
- `man cupsd.conf` — La página del manual para el archivo de configuración del demonio de impresión CUPS.
- `man classes.conf` — La página del manual para el archivo de configuración de clases para CUPS.

27.15.2. Sitios Web de utilidad

- http://www.linuxprinting.org — *GNU/Linux Printing* contiene una gran cantidad de información sobre la impresión en Linux.
- http://www.cups.org/ — Documentación, lista de preguntas más frecuentes (FAQs) y grupos de noticias sobre CUPS.

redhat.

Capítulo 28.

Tareas automáticas

En Linux, las tareas pueden configurarse para que se ejecuten de forma automática en un período de tiempo concreto y en las fechas indicadas. El sistema Red Hat Linux se distribuye preconfigurado para ejecutar determinadas tareas del sistema de modo que el sistema se mantenga actualizado. Por ejemplo, la base de datos slocate se actualiza diariamente. Un administrador del sistema puede utilizar las tareas automáticas para realizar copias de seguridad periódicas, controlar el sistema y ejecutar scripts personalizados, entre otras tareas.

Red Hat Linux contiene cuatro utilidades de tareas automáticas: `cron`, `anacron`, `at` y `batch`.

28.1. Cron

Cron es un demonio que sirve para ejecutar tareas programadas según una combinación de la hora, día del mes, mes, día de la semana y semana.

Cron asume que el sistema está activo de forma continua. Si el sistema no está activo cuando está programada una tarea, Cron no se ejecuta. Para configurar las tareas en función de los períodos, en vez de según horas exactas, consulte la Sección 28.2. Para programar las tareas contemporáneas, remítase a la Sección 28.3.

Para usar el servicio cron, debe de tener el paquete RPM `vixie-cron`instalado y el servicio `crond` debe estar en funcionamiento. Para determinar si el paquete está instalado, use el comando `rpm -q vixie-cron`. Para determinar si el servicio está funcionando, utilice el comando `/sbin/service crond status`.

28.1.1. Configuración de una tarea Cron

El fichero de configuración principal de cron, `/etc/crontab`, contiene las líneas siguientes:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Las primeras cuatro líneas son variables que se usan para configurar el entorno en el que se ejecutan las tareas cron. El valor de la variable `SHELL` indica al sistema el entorno de shell que deberá utilizarse (en este ejemplo, el shell de bash) y la variable `PATH` define la ruta usada para ejecutar los comandos. El resultado de las tareas cron se envía por correo electrónico al nombre de usuario definido con la variable `MAILTO`. Si la variable `MAILTO` se define como una cadena vacía (`MAILTO=""`), no se enviará correo electrónico. La variable `HOME` puede utilizarse para establecer el directorio principal que deberá usarse al ejecutar los comandos o scripts.

Cada línea del fichero `/etc/crontab` tiene el formato siguiente:

```
minute   hour   day   month   dayofweek   command
```

- `minute` — número entero entre 0 y 59
- `hour` — número entero entre 0 y 23
- `day` — número entero entre 1 y 31 (debe ser un día válido si se especifica un mes)
- `month` — número entero entre 1 y 12 (o nombre corto del mes, por ejemplo, ene, feb, etc.)
- `dayofweek` — número entero entre 0 y 7, donde 0 o 7 corresponde a Domingo (o el nombre corto del día de la semana, por ejemplo, dom, lun, etc.)
- `command` — el comando a ejecutar (el comando puede ser uno tal como `ls /proc >> /tmp/proc` o el comando para ejecutar un script personalizado que usted haya escrito.)

En cualquiera de los valores antes indicados, se puede utilizar un asterisco (*) para especificar todos los valores válidos. Por ejemplo, un asterisco para el valor de mes significa que el comando se ejecutará cada mes dentro de las limitaciones del resto de los valores.

Un guión (-) entre los números enteros indica un intervalo de números enteros. Por ejemplo, **`1-4`** significa los números enteros 1, 2, 3 y 4.

Una lista de valores separados por comas (,) especifica una lista. Por ejemplo, **`3, 4, 6, 8`** indica esos cuatro números enteros.

La barra (/) puede utilizarse para especificar valores de pasos. El valor de un número entero se puede omitir dentro de un intervalo si se indica a continuación del intervalo lo siguiente **`/`*`<número entero>`***. Por ejemplo, **`0-59/2`** puede usarse para definir el resto de los minutos del campo minuto. Los valores de pasos también pueden utilizarse con un asterisco. Por ejemplo, el valor **`*/3`** puede usarse en el campo de mes para omitir el tercer mes.

Las líneas que empiezan por almohadilla (#) son comentarios y no se procesan.

Como podrá observar en el archivo `/etc/crontab`, usa el script `run-parts` para ejecutar los scripts en los directorios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly`, y `/etc/cron.monthly` cada hora, diariamente, semanalmente o mensualmente, respectivamente. Los ficheros de estos directorios deben ser scripts de shell.

Si las tareas cron deben ejecutarse según una programación distinta a la hora, día, semana o mes, esto puede agregarse en el directorio `/etc/cron.d`. Todos los ficheros de este directorio utilizan la misma sintaxis que `/etc/crontab`. Remítase al Ejemplo 28-1 para más ejemplos.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

Ejemplo 28-1. Ejemplos de Crontab

Los usuarios no root pueden configurar las tareas cron tasks con la utilidad `crontab`. Todos los crontabs definidos por el usuario se almacenan en el directorio `/var/spool/cron` y se ejecutan utilizando los nombres de los usuarios que los han creado. Para crear un crontab como un usuario, inicie la sesión como ese usuario y escriba el comando `crontab -e` para modificar el crontab del usuario con el editor especificado por la variable de entorno `VISUAL` o `EDITOR`. El fichero usa el mismo formato que `/etc/crontab`. Cuando se guardan los cambios en crontab, el crontab se almacena según el nombre de usuario, y se escribe en el fichero `/var/spool/cron/`*`username`*.

El demonio cron controla el fichero `etc/crontab`, el directorio `etc/cron.d/` y el directorio `/var/spool/cron` cada minuto para cada cambio. Si se encuentra algún cambio, estos se descargan en la memoria. De este modo, el demonio no necesita ser reiniciado si se cambia un fichero crontab.

28.1.2. Control de acceso a Cron

Los ficheros `/etc/cron.allow` y `/etc/cron.deny` se usan para restringir el acceso a cron. El formato de los dos ficheros de acceso es un nombre de usuario en cada línea. No está permitido espacio en blanco en ninguno de los ficheros. El demonio cron (`crond`) no deberá ser reiniciado si los ficheros de control de acceso se modifican. Los ficheros de control de acceso se leen cada vez que el usuario intenta añadir o borrar una tarea cron.

El usuario root puede utilizar siempre cron, sin prestar atención a los nombres de usuarios listados en los ficheros de control de acceso.

Si existe el fichero `cron.allow`, tan sólo se permitirá a los usuarios presentes en la lista utilizar cron y el fichero `cron.deny` se ignorará.

Si `cron.allow` no existe, todos los usuarios listados en `cron.deny` no se les permite usar cron.

28.1.3. Iniciar y finalizar el servicio

Para iniciar el servicio cron, use el comando `/sbin/service crond start`. Para parar el servicio, use el comando `/sbin/service crond stop`. Se le recomienda que inicie el servicio en el tiempo de arranque. Remítase al Capítulo 14 para más detalles sobre cómo iniciar el servicio cron automáticamente al arrancar el sistema.

28.2. Anacron

Anacron es un programador de tareas similar a cron, con la diferencia de que no necesita que el sistema esté en ejecución. Se puede utilizar para ejecutar los procesos que cron ejecuta normalmente de forma diaria, semanal y mensual.

Para usar el servicio Anacron, debe tener instalado el paquete RPM `anacron`. Para determinar si está instalado este paquete, utilice el comando `rpm -q anacron`. Si quiere comprobar que el servicio está en ejecución, utilice el comando `/sbin/service anacron status`.

28.2.1. Configuración de las tareas de Anacron

Las tareas Anacron están incluidas en el fichero de configuración `/etc/anacrontab`. Cada línea del fichero de configuración corresponde a una tarea y tiene el formato siguiente:

```
period   delay   job-identifier  command
```

- `period` — frecuencia (en días) con la que se ejecuta el comando
- `delay` — tiempo de retraso en minutos
- `job-identifier` — descripción de las tareas, usados en los mensajes Anacron y como el nombre del identificador de la estampilla del proceso, puede contener cualquier caracter no en blanco (excepto barras oblicuas)
- `command` — comando que debe ejecutarse

Por cada tarea, Anacron determina si la tarea ha sido ejecutada dentro del período especificado en el campo `period` del archivo de configuración. Si no se ha ejecutado dentro de ese período, Anacron ejecutará el comando especificado en el campo `command` después de esperar la cantidad de tiempo especificado en el campo `delay`.

Una vez finalizada la tarea, Anacron registra la fecha en el fichero de marca de fecha que se encuentra en el directorio `/var/spool/anacron`. Sólo se utiliza la fecha (no la hora), y se usa el valor de `job-identifier` como nombre de fichero del fichero de marca de hora.

Las variables de entorno, como `SHELL` y `PATH` , pueden definirse en la parte superior de `/etc/anacron`, de forma similar al fichero de configuración de cron.

El aspecto del fichero de configuración por defecto es similar a como se indica a continuación:

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1       5       cron.daily              run-parts /etc/cron.daily
7       10      cron.weekly             run-parts /etc/cron.weekly
30      15      cron.monthly            run-parts /etc/cron.monthly
```

Figura 28-1. Anacrontab por defecto

Tal como puede ver en la Figura 28-1, anacron para Red Hat Linux se configura de modo que queda garantizada la ejecución diaria, semanal y mensual de las tareas cron.

28.2.2. Iniciar y finalizar el servicio

Para arrancar el servicio anacron, use el comando `/sbin/service anacron start`. Para detener el servicio, use el comando `/sbin/service anacron stop`. Se recomienda arrancar el servicio en el momento del arranque. Remítase al Capítulo 14 para más detalles sobre el inicio del servicio anacron de manera automática al momento de arranque.

28.3. At y Batch

Mientras que cron y anacron se usan para programar tareas, el comando `at` se usa para programar una única tarea en un tiempo específico. El comando `batch` se usa para programar que se ejecute una sóla tarea cuando los sistemas cargan las caídas promedio por debajo de 0.8.

Para poder usar `at` or `batch` debe tener el paquete RPM `at` instalado y el sistema `atd` en funcionamiento. Para determinar si el servicio se está ejecutando, utilice el comando `/sbin/service atd status`.

28.3.1. Configuración de tareas

Para programar una tarea no repetitiva en un tiempo específico, escriba el comando `at` *`time`*, en el que *`time`* es el tiempo para ejecutar el comando.

El argumento *`time`* puede ser uno de los siguientes:

- formato HH:MM — Por ejemplo,04:00 especifica 4:00AM. Si se inserta el tiempo, se ejecuta en el tiempo específico el día después.
- midnight — Especifica 12:00AM.
- noon — Especifica 12:00PM.

- teatime — Especifica 4:00PM.
- formato del nombre-mes, día y año — Por ejemplo, Enero 15 del año 2002. El año es opcional.
- formato MMDDYY, MM/DD/YY, o MM.DD.YY — Por ejemplo, 011502 para el día 15 de Enero del año 2002.
- ahora + tiempo — el tiempo está en minutos, horas, días o semanas. Por ejemplo, ahora + 5 días, especifica que el comando debería ser ejecutado a la misma hora en 5 días.

La hora debe ser especificada en primer lugar, seguido por la fecha opcional. Para más información sobre el formato del tiempo, lea el fichero del texto `/usr/share/doc/at-<version>/timespec`.

Tras haber escrito el comando `at` con el argumento del tiempo, el prompt `at>` será visualizado. Escriba el comando a ejecutar, pulse [Intro] y escriba Ctrl-D. Se puede especificar más de un comando escribiendo cada comando seguido de la tecla [Intro]. Después de haber escrito todos los comandos, pulse [Intro] para obtener una línea en blanco y escriba Ctrl-D. Alternativamente, se puede introducir un script de shell en el intérprete de comandos y escribir Ctrl-D en una línea en blanco para salir. Si se introduce un script, la configuración de la shell usada será la configuración de la shell en la SHELL del usuario, la shell de registro del usuario o `/bin/sh` (el primero que se encuentre).

Si la configuración de comandos o el script intentan visualizar información, la salida de datos será enviada vía correo electrónico al usuario.

Use el comando `atq` para visualizar los trabajos pendientes. Remítase a la Sección 28.3.3 para más información.

El uso del comando `at` puede ser restringido. Remítase a la Sección 28.3.5 para más detalles.

28.3.2. Configuración de tareas Batch

Para ejecutar una tarea no repetitiva cuando el promedio de carga está por debajo de 0.8, utilice el comando `batch`.

Tras haber escrito el comando `batch`, se visualiza el intérprete de comandos `at>`. Escriba el comando a ejecutar, pulse [Intro] y escriba Ctrl-D. Se puede especificar más de un comando al escribir cada comando seguido de la tecla [Intro]. Tras haber escrito todos los comandos, pulse [Intro] para acceder a una línea en blanco y escriba Ctrl-D. Se puede introducir de forma alternativa un script de shell en el intérprete de comandos y escribir Ctrl-D en una línea en blanco para salir. Si se introduce un script, la shell usada es la configuración de la she en el entorno SHELL del usuario, la shell de login del usuario, o `/bin/sh` (todo lo que se encuentre en primer lugar). Tan pronto como el promedio de carga está bajo 0.8, se ejecutará la configuración del comando o el script.

Si la configuración de comandos o el script intentan visualizar información, la salida de datos será enviada vía correo electrónico al usuario.

Use el comando `atq` para visualizar los trabajos pendientes. Remítase a la Sección 28.3.3 para más información.

El uso del comando `batch` puede ser restringido. Remítase a la Sección 28.3.5 para más detalles.

28.3.3. Visualización de las tareas pendientes

Para visualizar las tareas pendientes `at` y `batch`, use el comando `atq`. Se muestra una lista de tareas pendientes, con cada línea de trabajo. Cada línea está en el número de tarea del formato, la fecha, la hora, el tipo de tarea y el nombre de usuario. Los usuarios tan sólo pueden ver sus propias tareas. Si el usuario root ejecuta el comando `atq`, se visualizarán todas las tareas para los usuarios.

28.3.4. Opciones adicionales de la línea de comandos

Opciones adicionales de la línea de comandos para `at` y `batch` incluyen:

Opciones	Descripción
`-f`	Lee los comandos o script del shell desde un archivo en vez de ser especificados en el intérprete de comandos.
`-m`	Envía un email al usuario cuando se ha completado la tarea.
`-v`	Muestra la hora en la que la tarea será ejecutada.

Tabla 28-1. Opciones de línea de comandos `at` y `batch`

28.3.5. Control de acceso a At y Batch

Los ficheros `/etc/at.allow` y `/etc/at.deny` pueden ser usados para restringir el acceso a los comandos `at` y `batch`. El formato de ambos ficheros de control de acceso es un nombre de usuario en cada línea. El espacio en blanco no está permitido en ningún fichero. El (`atd`) demonio `at` no deberá ser reiniciado si los ficheros de control de acceso son modificados. Los ficheros de control de acceso se leen cada vez que un usuario intenta ejecutar los comandos `at` y `batch`.

El usuario root siempre puede ejecutar los comandos `at` y `batch`, sin tener en cuenta los ficheros de control de acceso.

Si existe el fichero `at.allow` tan sólo se permitirá a los usuarios listados usar `at` o `batch` y el fichero `at.deny` será ignorado.

Si `at.allow` no existe, a todos los usuarios listados en `at.deny` no se les permitirá usar `at` o `batch`.

28.3.6. Iniciar y finalizar el servicio

Para iniciar el servicio `at`, use el comando `/sbin/service atd start`. Para detener el servicio, use el comando `/sbin/service atd stop`. Se le recomienda que inicie el servicio durante el momento de arranque. Remítase al Capítulo 14 para más detalles sobre como arrancar el servicio cron al momento de arranque.

28.4. Recursos adicionales

Para obtener más información sobre cómo configurar tareas automáticas, consulte los recursos siguientes.

28.4.1. Documentación instalada

- Página del manual de`cron` — descripción general de cron.
- Páginas del manual de `crontab` en las secciones 1 y 5 — la página del manual de la sección 1 contiene una descripción del fichero `crontab`. La página del manual de la sección 5 contiene el formato del fichero y algunos ejemplos de entradas.
- `/usr/share/doc/at-<version>/timespec` contiene el formato del fichero y algunos ejemplos de entradas.

- Página del manual de `anacron` — descripción de anacron y de las opciones de la línea de comandos correspondientes.
- Página del manual de `anacrontab` — breve descripción del fichero de configuración de anacron.
- `/usr/share/doc/anacron-`*<version>*`/README` — describe Anacron y su utilidad.
- Página de manual `at` — descripción de `at` y `batch` y las opciones de la línea de comandos.

Capítulo 29.

Archivos de registro

Los *Archivos de registro* (o archivos de log) son archivos que contienen mensajes sobre el sistema, incluyendo el kernel, los servicios y las aplicaciones que se ejecutan en dicho sistema. Existen diferentes tipos de archivos de log dependiendo de la información. Por ejemplo, existe un archivo de log del sistema, un archivo de log para los mensajes de seguridad y un archivo de log para las tareas cron.

Los archivos de registro pueden ser muy útiles cuando se trate de resolver un problema con el sistema tal como cuando se trata de cargar un controlador del kernel o cuando se este buscando por intentos no autorizados de conexión al sistema. Este capítulo discute donde encontrar estos archivos de registro, cómo visualizarlos y qué buscar en ellos.

Algunos archivos de log están controlados por un demonio llamado `syslogd`. Encontrará una lista de mensajes de log mantenidos por `syslogd` en el archivo de configuración `/etc/syslog.conf`.

29.1. Localizar archivos de registro

La mayoría de archivos de log están localizados en el directorio `/var/log`. Algunas aplicaciones como por ejemplo `httpd` y `samba` poseen un directorio en `/var/log` para sus archivos de log.

Observe los múltiples archivos en el directorio de archivos log seguidos de números. Estos se crean cuando los archivos de log circulan. Los archivos de log circulan de manera que los tamaños de los archivos no sean demasiado amplios. El paquete `logrotate` contiene una tarea de cron que hace circular automáticamente los archivos de log al archivo de configuración `/etc/logrotate.conf` y los archivos de configuración en el directorio `/etc/logrotate.d`. Por defecto, se configura para circular cada semana y mantener la validez de los archivos previos de log durante cuatro semanas.

29.2. Visualizar los archivos de registro

La mayoría de los archivos de registro están en formato de texto plano. Puede visualizarlos con cualquier editor de texto tal como **Vi** o **Emacs**. Algunos archivos log pueden ser leídos por todos los usuarios del sistema; sin embargo se requiere de privilegios como root para visualizar la mayoría de ellos.

Para visualizar los archivos log en una aplicación interactiva en tiempo real, utilice la **Visor de registros del sistema**. Para iniciar la aplicación, vaya a **Botón del menú principal** (en el Panel) **=> Herramientas del sistema => Registros del sistema**, o escriba el comando `redhat-logviewer` en el intérprete de comandos de la shell.

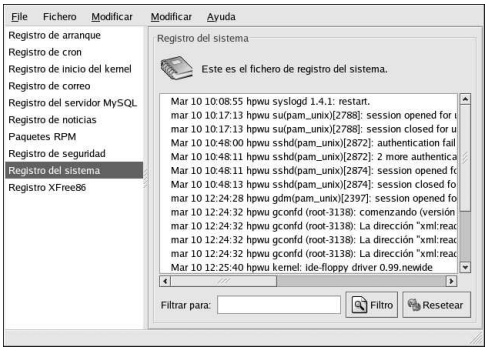

Figura 29-1. Visor de registros del sistema

La aplicación sólo muestra los archivos de registro que existen; por tanto, la lista puede ser diferente a la mostrada en la Figura 29-1. Para ver la lista completa de archivos registro que pueden ser visualizados, consulte el archivo de configuración `/etc/sysconfig/redhat-logviewer`.

Por defecto, el archivo de registro visible actualmente es refrescado cada 30 segundos. Para cambiar el ratio de refrescado, seleccione **Modificar => Preferencias** desde el menú desplegable. Aparecerá la ventana mostrada en la Figura 29-2. En la pestaña **Archivos de registro**, haga click en las flechas al lado del ratio de refrescado para cambiarlo. Haga click en **Cerrar** para volver a la ventana principal. El ratio de refresco es cambiado de inmediato. Para refrescar el archivo visible manualmente, seleccione **Archivo => Refrescar ahora** o presione [Ctrl]-[R].

Para filtrar los contenidos de un archivo de registro por palabras clave, escriba la palabra o palabras en el campo **Filtrar por** y haga click en **Filtrar**. Haga click en **Reset** para limpiar los contenidos.

También puede cambiar el lugar en el que la aplicación busca los archivos de log en la pestaña **Archivos de registro**. Seleccione el archivo de log desde la lista y pulse el botón **Cambiar localización**. Escriba la nueva localización del archivo de log o pulse el botón **Navegar** para localizar la localización del archivo usando un diálogo de selección del archivo. Pulse **OK** para volver a la ventana principal.

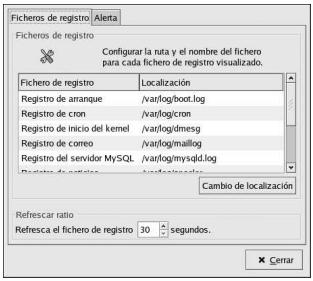

Figura 29-2. Localizaciones de archivos de log

29.3. Examinar los archivos de registro

La **Visor de registros del sistema** se puede configurar para que muestre un icono de alerta al lado de las líneas que contienen palabras clave de alerta. Para añadir palabras de alerta, seleccione **Editar =>**

Preferencias desde el menú desplegable y haga click en la pestaña **Alertas**. Haga click en el botón **Añadir** para agregar una palabra de alerta. Para borrar una palabra de alerta, seleccione la palabra de la lista y haga click en **Borrar**.

Figura 29-3. Alertas

Capítulo 30.

Actualización del Kernel

El kernel que viene con Red Hat Linux está personalizado por el equipo de desarrollo del kernel de Red Hat para asegurar su integridad y compatibilidad con el hardware soportado. Antes que Red Hat libere un kernel, debe pasar un conjunto de evaluaciones rigurosas para asegurar su calidad.

Los kernels Red Hat Linux están empaquetados en formato RPM para así hacerlos más fácil de actualizar y verificar. Por ejemplo, cuando el paquete RPM `kernel` distribuido por Red Hat, Inc. es instalado, una imagen `initrd` es creada; por lo tanto no es necesario usar el comando `mkinitrd` después de instalar un kernel diferente. También modifica el fichero de configuración del gestor de arranque para incluir el nuevo kernel, tanto si se instala LILO o GRUB.

Este capítulo trata sobre los pasos necesarios para actualizar el kernel únicamente en un sistema x86.

El kernel 2.4

La construcción de un kernel personalizado no es soportado por el Equipo de soporte durante la instalación de Red Hat Linux. Para más información sobre cómo hacer un kernel personalizado desde el código fuente, vea el Apéndice A.

30.1. Preparación de la actualización

Red Hat Linux ahora se distribuye con el kernel 2.4. Las características de un kernel 2.4 tal como se distribuye con Red Hat Linux son:

- El directorio de las fuentes del kernel es `/usr/src/linux-2.4/` en vez de `/usr/src/linux/`.
- Soporte para el sistema de ficheros ext3.
- Mejor soporte SMP.
- Compatibilidad multimedia mejorada, incluido el módulo maestro3 para la tarjeta de sonido ESS Allegro.
- Soporte mejorado para USB.

30.2. Preparación para la actualización

Antes de actualizar el kernel, tome algunas precauciones. La primera es asegurarse que tiene un disco de arranque en caso de que haya problemas. Si el gestor de arranque no está configurado apropiadamente para arrancar el nuevo kernel, no será capaz de arrancar su sistema a menos que tenga un disquete de arranque.

Para crear un disco de arranque para su sistema, conéctese como usuario root y en el intérprete de comandos teclee el siguiente comando:

```
/sbin/mkbootdisk `uname -r`
```

Sugerencia

Consulte la página del manual para `mkbootdisk` para ver más opciones.

Reinicie la máquina con el disquete de arranque y verifique que funciona antes de continuar.

Con suerte, no necesitará usar el disquete, pero guárdelo en un lugar seguro por si acaso.

Para determinar cuáles paquetes del kernel están instalados, ejecute el comando siguiente en el intérprete de comandos:

```
rpm -qa | grep kernel
```

La salida contendrá alguno o todos de los siguientes paquetes, dependiendo del tipo de instalación que haya realizado (el número de la versión puede variar):

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

De la anterior salida, puede determinar qué paquetes necesita descargar para actualizar el kernel. El único paquete necesario para un sistema con un único procesador es el `kernel`.

Si tiene un ordenador con más de un procesador, necesita el paquete `kernel-smp` que contiene el soporte para más de un procesador. También se recomienda instalar el paquete `kernel` en el caso de que el kernel con varios procesadores no funcione correctamente con el sistema.

Si tiene un ordenador con una memoria superior a cuatro GB, necesita el paquete `kernel-bigmem` para que el sistema pueda usar más de cuatro gigabytes de memoria. De todas maneras, se recomienda instalar el paquete `kernel` por si ocurriera algún error. El paquete `kernel-bigmem` existe sólo para la arquitectura i686.

Si está actualizando el kernel en un ordenador portátil o está usando PCMCIA, el paquete `kernel-pcmcia-cs` también es necesario.

No necesita el paquete `kernel-source` a menos que vaya a recompilar el kernel por sí mismo o vaya a desarrollarlo.

El paquete `kernel-doc` contiene documentación sobre desarrollo del kernel y no es necesario. Se recomienda si el sistema es usado para desarrollos del kernel.

El paquete `kernel-util` incluye utilidades que pueden ser usadas para controlar el kernel o el hardware del sistema. No es necesario.

Red Hat crea kernels que han sido optimizados para diferentes versiones x86. Las opciones son `athlon` para los sistemas AMD Athlon™ y AMD Duron™, `i686` para sistemas Intel® Pentium® II, Intel® Pentium® III, e Intel® Pentium® 4, y `i586` para sistemas Intel® Pentium® y AMD K6™. Si no sabe cuál es la versión de su sistema x86, use el kernel para la versión `i386` ya que es compatible con todas los sistemas basados en la arquitectura x86.

La versión x86 del paquete RPM se encuentra en el nombre del fichero. Por ejemplo, `kernel-2.4.20-2.47.1.athlon.rpm` se ha optimizado para los sistemas AMD Athlon™ y AMD Duron™ y `kernel-2.4.20-2.47.1.i686.rpm` para los sistemas Intel® Pentium® II, Intel® Pentium® III, e Intel® Pentium® 4. Cuando haya determinado los paquetes necesarios para su kernel, seleccione la arquitectura apropiada para los paquetes `kernel`, `kernel-smp`, y `kernel-bigmem`. Use las versiones `i386` de los otros paquetes.

30.3. Descarga

Hay varias maneras de saber si hay un kernel actualizado disponible para su sistema.

- Vaya a http://www.redhat.com/apps/support/errata/, elija la versión del sistema Red Hat Linux que está usando y busque la errata de ésta. Las erratas del kernel, normalmente están bajo la sección **Security Advisories**. Desde la lista de erratas, pulse kernel errata para ver los informes detallados de erratas. En el informe de erratas, hay una lista de paquetes RPM requeridos y un enlace para descargarlos desde el sitio FTP de Red Hat. También puede descargarlos desde un FTP espejo de Red Hat. Una lista de sitios espejos está disponible desde http://www.redhat.com/download/mirror.html.
- Use Red Hat Network para descargar los paquetes RPM del kernel e instalarlos. Red Hat Network puede descargar el kernel más reciente, actualizarlo en el sistema, crear una imagen de disco RAM inicial si se necesita y configurar el gestor de arranque para arrancar el nuevo kernel. Para más información, consulte *Red Hat Network User Reference Guide* disponible en http://www.redhat.com/docs/manuals/RHNetwork/.

Si los paquetes RPM fueron descargados desde la página de erratas de Red Hat Linux o si se usó Red Hat Network para descargar paquetes, proceda con la Sección 30.4. Si se utilizó Red Hat Network para descargar e instalar el kernel actualizado, siguiendo las instrucciones en la Sección 30.5 y Sección 30.6, excepto no cambie el kernel para arrancar por defecto puesto que Red Hat Network automaticamente cambia el kernel por defecto a la versión más reciente.

30.4. Realizando la actualización

Después de obtener todos los paquetes necesarios, es hora de actualizar el kernel existente. En el intérprete de comandos de la shell como root, cámbiese al directorio que contiene los paquetes RPM y siga los pasos.

Importante

Se recomienda encarecidamente guardar el kernel anterior por si tiene problemas con el kernel nuevo.

Use el argumento `-i` con el comando `rpm` para mantener el viejo kernel. Si la opción `-U` es usada para actualizar el paquete `kernel`, se sobreescribirá el kernel instalado actualmente (la versión del kernel y la versión x86 pueden variar):

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

Si el sistema es un sistema multiprocesador, instale también los paquetes `kernel-smp` (la versión del kernel y la versión x86 pueden variar):

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

Si el sistema esta basado en `i686` y contiene más de 4 gigabytes de RAM, instale el paquete `kernel-bigmem` construido para la arquitectura `i686` así como también (la versión del kernel puede variar):

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

Si los paquetes `kernel-source`, `kernel-docs`, o `kernel-utils` se van a actualizar, las versiones más viejas lo más probable es que no sean necesarias. Use los comandos siguientes para actualizar estos paquetes (las versiones pueden variar):

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

Si está usando PCMCIA (por ejemplo, en un portátil), necesitará también instalar `kernel-pcmcia-cs` y guardar la versión vieja. Si se usa la opción `-i` probablemente tenga un conflicto ya que el kernel antiguo necesita este paquete para reiniciar con soporte PCMCIA. Para trabajar con ello, use la opción `--force` como sigue (la versión puede variar):

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

El próximo paso es verificar que la imagen del disco inicial RAM ha sido creada. Refiérase a la Sección 30.5 para más detalles.

30.5. Verificación de la imagen de disco RAM inicial

Si el sistema usa un controlador SCSI o un sistema de archivos ext3, necesitará un disco RAM inicial. El propósito de dicho disco es permitir a un kernel modular tener acceso a los módulos que son necesarios para arrancar antes de que el kernel tenga acceso a los dispositivos donde los módulos normalmente residen.

El disco RAM inicial puede ser creado con el comando `mkinitrd`. Sin embargo, este paso es ejecutado automáticamente si el kernel y sus paquetes asociados son instalados o actualizados desde los paquetes RPM distribuidos por Red Hat, Inc.; por tanto, no necesita ser ejecutado manualmente. Para verificar que fue creado, use el comando `ls -l /boot` para asegurarse de que el archivo `initrd-2.4.20-2.47.1.img` fue creado (la versión debería coincidir la versión del kernel que acaba de instalar).

Ahora que ya tiene instalado el nuevo kernel, necesita verificar que el gestor de arranque está configurado para cargar el nuevo kernel. Vea la Sección 30.6 para más detalles.

30.6. Configuración del gestor de arranque

El paquete RPM `kernel` configura el gestor de arranque GRUB o LILO para arrancar el nuevo kernel si cualquiera de estos gestores de arranque es instalado. Sin embargo, no configura el gestor de arranque para cargar el nuevo kernel por defecto.

Es una buena idea confirmar que el gestor de arranque se ha configurado correctamente. Esto es un paso crucial. Si el gestor de arranque esta configurado de forma incorrecta, no podrán arrancar el sistema. Si esto ocurre, arranque el sistema con el disquete de arranque que creó anteriormente e intente configurar de nuevo el gestor de arranque.

30.6.1. GRUB

Si selecciona GRUB como gestor de arranque, asegúrese que el fichero `/boot/grub/grub.conf` contenga la sección `title` con la misma versión del paquete `kernel` que acaba de instalar (lo mismo para los paquetes `kernel-smp` o `kernel-bigmem`):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=3
```

```
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
        initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.img
```

Si ha creado una partición separada para `/boot`, el camino al kernel y la imagen initrd será relativo a la partición `/boot`.

Observe que el nuevo kernel no está configurado para ser el kernel por defecto. Para configurar GRUB para que arranque el nuevo kernel por defecto, cambie el valor de la variable `default` al número del título de la sección que contiene el nuevo kernel. La cuenta comienza con 0. Por ejemplo, si el nuevo kernel es el segundo título en la sección, configure `default` a **`1`**.

Comience evaluando el nuevo kernel reiniciando el computador y vigilando los mensajes para asegurarase de que el hardware es detectado adecuadamente.

30.6.2. LILO

Si se utiliza LILO como el gestor de arranque, confirme que el archivo `/etc/lilo.conf` contiene una sección `image` con la misma versión que el paquete `kernel` que acaba de instalar (lo mismo para los paquetes `kernel-smp` o `kernel-bigmem`):

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
        label=2.4.20-2.47.1
        initrd=/boot/initrd-2.4.20-2.47.1.img
        read-only
        append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
        label=2.4.20-2.30
        initrd=/boot/initrd-2.4.20-2.30.img
        read-only
        append="root=LABEL=/"
```

Observe que el nuevo kernel no está configurado para ser el kernel por defecto. Para configurar LILO para que arranque el nuevo kernel por defecto, cambie el valor de la variable `default` al valor de `label` de la sección `image` del nuevo kernel. Debe ejecutar el comando `/sbin/lilo` como root para activar los cambios. Después de ejecutarlo, verá un resultado similar al siguiente:

```
Added 2.4.20-2.47.1 *
Added linux
```

El `*` después de `2.4.20-2.47.1` significa que el kernel en esa sección es el kernel por defecto que LILO arrancará.

Comience evaluando el nuevo kernel reiniciando su ordenador y viendo los mensajes para asegurarse que su hardware es detectado apropiadamente.

Capítulo 31.

Módulos del kernel

El kernel de Linux tiene un diseño modular. En el momento de arranque, sólo se carga un kernel residente mínimo en memoria. Por ello, cuando un usuario solicita alguna característica que no esta presente en el kernel residente, se carga dinámicamente en memoria un *módulo kernel*, también conocido algunas veces como un *controlador*.

Durante la instalación, se prueba el hardware en el sistema. Basado en esta prueba y en la información proporcionada por el usuario, el programa de instalación decide qué módulos necesita cargar en el momento de arranque. El programa de instalación configura el mecanismo de carga dinámica para que funcione de forma transparente.

Si se añade un nuevo hardware después de la instalación y este requiere un módulo kernel, el sistema debe ser configurado para cargar el módulo adecuado para el nuevo hardware. Cuando el sistema es arrancado con el nuevo hardware, se ejecuta el programa **Kudzu** detecta el nuevo hardware si es soportado y configura el módulo necesario para él. El módulo tambíen puede ser especificado manualmente modificando el archivo de configuración del módulo, `/etc/modules.conf`.

Nota

Los módulos de tarjetas de vídeo usados para desplegar la interfaz del sistema X Window son parte del paquete `XFree86`, no del kernel; por lo tanto, este capítulo no se aplica a ellos.

Por ejemplo, si un sistema incluye un adaptador de red SMC EtherPower 10 PCI, el archivo de configuración del módulo contiene la línea siguiente:

```
alias eth0 tulip
```

Si una segunda tarjeta de red es añadida al sistema y es idéntica a la primera tarjeta, añada la línea siguiente al archivo `/etc/modules.conf`:

```
alias eth1 tulip
```

Consulte el *Manual de referencia de Red Hat Linux* para una lista alfabética de módulos de kernel y hardware soportado por los módulos.

31.1. Utilidades del módulo del kernel

Está disponible un grupo de comandos para el manejo de módulos kernel si el paquete `modutils` está instalado. Use estos comandos para determinar si un módulo ha sido cargado exitósamente o cuando se esté probando módulos diferentes para una nueva pieza de hardware.

El comando `/sbin/lsmod` muestra una lista de los módulos cargados actualmente. Por ejemplo:

```
Module                  Size  Used by    Not tainted
iptable_filter          2412   0 (autoclean) (unused)
ip_tables              15864   1 [iptable_filter]
nfs                    84632   1 (autoclean)
lockd                  59536   1 (autoclean) [nfs]
sunrpc                 87452   1 (autoclean) [nfs lockd]
soundcore               7044   0 (autoclean)
```

```
ide-cd                  35836   0 (autoclean)
cdrom                   34144   0 (autoclean) [ide-cd]
parport_pc              19204   1 (autoclean)
lp                       9188   0 (autoclean)
parport                 39072   1 (autoclean) [parport_pc lp]
autofs                  13692   0 (autoclean) (unused)
e100                    62148   1
microcode                5184   0 (autoclean)
keybdev                  2976   0 (unused)
mousedev                 5656   1
hid                     22308   0 (unused)
input                    6208   0 [keybdev mousedev hid]
usb-uhci                27468   0 (unused)
usbcore                 82752   1 [hid usb-uhci]
ext3                    91464   2
jbd                     56336   2 [ext3]
```

Por cada línea, la primera columna es el nombre del módulo, la segunda columna es el tamaño del módulo y la tercera es el recuento de usos.

La información después del recuento de usos varía un poco por módulo. Si se lista `(unused)` en la línea del módulo, el módulo no está siendo usado actualmente. Si `(autoclean)` está en la línea para el módulo, este puede ser limpiado automáticamente por el comando `rmmod -a`. Cuando se ejecuta este comando, cualquier módulo que este etiquetado con autoclean, que no ha sido usado desde la acción previa de autoclean, será cargado. Red Hat Linux no realiza esta acción de autoclean por defecto.

Si el nombre de un módulo esta listado al final de la línea entre corchetes, el módulo entre corchetes es dependiente del módulo listado en la primera columna de la línea. Por ejemplo, en la línea

```
usbcore                 82752   1 [hid usb-uhci]
```

los módulo del kernel hid y usb-uhci dependen del módulo usbcore.

La salida `/sbin/lsmod` es la misma que la salida de `/proc/modules`.

Para cargar un módulo del kernel, use el comando `/sbin/modprobe` seguido del nombre del módulo. Por defecto, `modprobe` intenta cargar el módulo desde los subdirectorios `/lib/modules/<kernel-version>/kernel/drivers/`. Hay un subdirectorio para cada tipo de módulo, tal como el subdirectorio `net/` para los controladores de interfaces de red. Algunos módulos del kernel tienen dependencias, es decir que otros módulos deben ser cargados antes para que el otro se cargue. El comando `/sbin/modprobe` verifica estas dependencias y carga los módulos necesarios antes de cargar el módulo específico.

Por ejemplo, el comando

```
/sbin/modprobe hid
```

carga cualquier dependencia de módulos y luego el módulo `hid`.

Para imprimir a la pantalla todos los comandos a medida en que `/sbin/modprobe` los ejecuta, use la opción `-v`. Por ejemplo:

```
/sbin/modprobe -v hid
```

Se despliega una salida similar a lo siguiente:

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

El comando `/sbin/insmod` también existe para cargar módulos kernel; sin embargo no resuelve dependencias. Por ello se recomienda el uso de `/sbin/modprobe`.

Para descargar módulos del kernel, use el comando `/sbin/rmmod` seguido por el nombre del módulo. La utilidad `rmmod` sólo descarga módulos que ya no son usados y que no son una dependencia de otro módulo en uso.

Por ejemplo, el comando

```
/sbin/rmmod hid
```

baja el módulo del kernel `hid`.

Otra utilidad muy conveniente es `modinfo`. Use el comando `/sbin/modinfo` para mostrar información sobre el módulo del kernel. La sintaxis general es:

```
/sbin/modinfo [options]
<module>
```

Las opciones incluyen `-d`, lo cual muestra una breve descripción del módulo, y `-p` lo que lista los parámetros que el módulo soporta. Para una lista completa de las opciones, consulte la página del manual de `modinfo` (`man modinfo`).

31.2. Recursos adicionales

Para más información en los módulos del kernel y sus utilidades, remítase a las siguientes fuentes de información.

31.2.1. Documentación instalada

- Página del manual de `lsmod` — descripción y explicación de su salida.
- Página del manual de `insmod` — descripción y listado de las opciones de la línea de comandos.
- Página del manual de `modprobe` — descripción y listado de las opciones de la línea de comandos.
- Página del manual de `rmmod` — descripción y listado de las opciones de la línea de comandos.
- Página del manual de `modinfo` — descripción y listado de las opciones de la línea de comandos.
- `/usr/src/linux-2.4/Documentation/modules.txt` — explica como se compilan y usan los módulos del kernel.

31.2.2. Sitios Web de utilidad

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — *Linux Loadable Kernel Module HOWTO* del Proyecto de documentación de Linux.

V. Administración de paquetes

Todo el software en un sistema Red Hat Linux está dividido en paquetes RPM los cuales pueden ser instalados, actualizados o eliminados. Esta parte describe como manejar los paquetes RPM en un sistema Red Hat Linux usando herramientas gráficas y de línea de comandos.

Tabla de contenidos

redhat.

Capítulo 32.

La administración de paquetes con RPM

El Administrador de paquetes (RPM) es un sistema de empaquetado abierto que trabaja en Red Hat Linux además de otros sistemas Linux y UNIX y que está a la disposición de cualquiera. Red Hat, Inc. fomenta el uso de RPM por parte de otros vendedores para sus propios productos. RPM se puede distribuir bajo los términos de GPL.

RPM facilita las actualizaciones de sistema para el usuario final. Es posible instalar, desinstalar y actualizar paquetes RPM por medio de comandos breves. RPM mantiene una base de datos de los paquetes instalados y de sus archivos, y usted puede hacer consultas y verificaciones poderosas en su sistema. Si prefiere una interfaz gráfica, puede utilizar **Herramienta de administración de paquetes** para ejecutar muchos comandos RPM. Para mayor información, consulte el Capítulo 33 para más detalles.

Durante las actualizaciones, RPM maneja cuidadosamente los archivos de configuración para que usted nunca pierda sus modificaciones de personalización — algo que no lograría hacer con archivos `.tar.gz` normales.

RPM permite al desarrollador tomar el código fuente del software y empaquetarlo en paquetes binarios y de fuente para los usuarios finales. Este proceso es bastante sencillo y se controla desde un único archivo y parches opcionales creados por usted mismo. Esta clara delineación de fuentes originarias y sus parches y las instrucciones de construcción facilitan el mantenimiento del paquete al ir apareciendo nuevas versiones del software.

Nota

Ya que RPM efectúa cambios a su sistema, debe ser root para poder instalar, quitar, o actualizar un paquete RPM.

32.1. Metas de diseño RPM

Podría ser útil conocer las metas de diseño de RPM para poder aprender a usar RPM:

Predisposición a la actualización

Al usar RPM es posible actualizar componentes individuales de su sistema sin tener que reinstalarlos completamente. Cuando obtenga una versión nueva de un sistema operativo basado en RPM (como Red Hat Linux), no es necesario efectuar reinstalaciones en su máquina (como debe hacerse con sistemas operativos basados en otros sistemas de empaquetado). RPM permite actualizaciones inteligentes, in situ y completamente automatizadas en su sistema. Los archivos de configuración en los paquetes se conservan no obstante las actualizaciones, y así no perderá sus personalizaciones. No existen archivos de actualización específicos para actualizar un paquete porque se utiliza el mismo archivo RPM para instalar y actualizar el paquete en su sistema.

Consultas poderosas

RPM fue ideado para proporcionar opciones de consulta poderosas. Se pueden efectuar búsquedas por toda su base de datos para encontrar un paquete o sólo algún archivo. También es posible averiguar a cuál paquete pertenece un determinado archivo y de dónde proviene el paquete. Los archivos contenidos en el paquete RPM están en un archivo comprimido, con

un encabezado binario personalizado que contiene información útil sobre el paquete y su contenido, permitiéndole consultar paquetes individuales rápida y sencillamente.

Verificación de sistema

Otra característica poderosa es la de verificar paquetes. Si está preocupado porque borró un archivo importante para algún paquete, verifique el paquete. Se le notificará si hay anomalías. En este punto, puede reinstalar el paquete si es necesario. Cualquier archivo de configuración que haya modificado será preservado durante la reinstalación.

Fuentes originarias

Un objetivo crucial ha sido el de permitir el uso de fuentes de software originario, tal y como ha sido distribuido por los autores originales del software. Con RPM tendrá las fuentes originarias junto con cualquier parche que haya sido usado además de las instrucciones de construcción completas. Esta es una ventaja importante por varios motivos. Si por ejemplo sale una versión nueva de un programa, no necesariamente necesita empezar desde cero para que se compile. Puede revisar el parche para ver lo que *tal vez* necesitaría hacer. Usando esta técnica se ven fácilmente todos los elementos predeterminados y compilados en el programa y todos los cambios que se le han hecho al software para construir adecuadamente.

El objetivo de mantener las fuentes originarias podría parecer importante sólo para los desarrolladores, pero el resultado también sería software de más alta calidad para los usuarios finales. Quisiéramos dar las gracias a la gente de distribución de BOGUS por haber ideado el concepto de la fuente originaria.

32.2. El uso de RPM

RPM tiene cinco modos de operación básicos (sin contar la construcción de paquetes): instalación, desinstalación, actualización, consulta y verificación. Esta sección contiene una visión de conjunto de cada modo. Para obtener detalles y opciones lance el comando `rpm --help`, o diríjase a la Sección 32.5 para obtener más información sobre RPM.

32.2.1. Encontrar paquetes RPM

Antes de usar un RPM debe saber dónde encontrarlo. Con una búsqueda en Internet obtendrá varios depósitos de RPM, pero si está buscando paquetes RPM construidos por Red Hat, se pueden encontrar en los siguientes sitios:

- Los CD-ROMs Red Hat Linux oficiales
- La página de errata de Red Hat a disposición en http://www.redhat.com/apps/support/errata/
- Existe un sitio espejo FTP de Red Hat en http://www.redhat.com/download/mirror.html
- Red Hat Network — consulte el Capítulo 34 para obtener más detalles sobre Red Hat Network

32.2.2. Instalación de RPM

Los paquetes RPM normalmente tienen nombres de archivo como `foo-1.0-1.i386.rpm`. El nombre de archivo incluye el nombre de paquete (`foo`), versión (`1.0`), lanzamiento (`1`) y arquitectura (`i386`). La instalación de un paquete es tan simple como teclear el siguiente comando en el intérprete de comandos de shell:

```
rpm -Uvh foo-1.0-1.i386.rpm
```

Si la instalación es correcta verá lo siguiente:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [100%]
```

Como podrá ver, RPM imprime el nombre del paquete y luego imprime una serie de almohadillas (#) mientras se instala el paquete como una especie de medidor de progreso.

Si empieza con la versión 4.1 del RPM, la firma del paquete se autentica en el momento de la instalación o de la actualización del paquete. Si la verificación de la firma falla, verá el siguiente mensaje de error:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

Si se trata de una nueva firma en el cabezal, verá el siguiente error:

```
error: Header V3 DSA signature: BAD, key ID
0352860f
```

Si no tiene instalada la clave apropiada para verificar la firma, el mensaje dirá `NOKEY` y será como lo siguiente:

```
warning: V3 DSA signature: NOKEY, key ID
0352860f
```

Para mayor información sobre la verificación de la firma del paquete, consulte la Sección 32.3.

Nota

Si está instalando un paquete del kernel, use el comando `rpm -ivh`. Consulte el Capítulo 30 para mayor información.

La instalación de paquetes está ideada para ser sencilla, pero de vez en cuando podría haber errores.

32.2.2.1. Paquete ya instalado

Si ya está instalado un paquete de la misma versión, verá:

```
Preparing...                ########################################### [100%]
package foo-1.0-1 is already installed
```

Si desea instalar el paquete de todos modos y la versión que está intentando instalar ya está instalada, podrá usar la opción `--replacepkgs`, la cual le dirá a RPM que ignore el error:

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

Esta opción es útil si se borraron los archivos instalados del RPM o si desea que se instalen los archivos de configuración originales del RPM.

32.2.2.2. Archivos en conflicto

Si intenta instalar un paquete que contiene un archivo que ya ha sido instalado por otro paquete o una versión más antigua del mismo paquete, verá lo siguiente:

```
Preparing...                ########################################### [100%]
```

```
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package
bar-2.0.20
```

Para hacer que RPM ignore este error, use la opción `--replacefiles`:

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. Dependencias no resueltas

Los paquetes RPM pueden "depender" de otros paquetes, lo cual significa que requieren de la instalación de otros paquetes para poder ejecutarse adecuadamente. Si intenta instalar un paquete que tiene una dependencia no resuelta, verá lo siguiente:

```
Preparing...                ########################################### [100%]
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

Si está instalando un paquete oficial de Red Hat, se le sugerirá resolver la dependencia de este paquete. Encuentre este paquete en los CD-ROMs de Red Hat Linux o en el sitio FTP (o espejo) y añádalo al comando:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

Si se realiza la instalación correctamente, verá lo siguiente:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [ 50%]
   2:bar                    ########################################### [100%]
```

Si no se le suguiere resolver la dependencia, puede intentar usar la opción `--redhatprovides` para determinar el paquete que contenga el archivo requerido. Necesita instalar el paquete `rpmdb-redhat` para usar esta opción.

```
rpm -q --redhatprovides bar.so.2
```

Si el paquete que contiene el archivo `bar.so.2` se encuentra en la base de datos instalada del paquete `rpmdb-redhat` aparecerá el nombre del paquete:

```
bar-2.0.20-3.i386.rpm
```

Si desea forzar la instalación de todas maneras (no es una buena idea ya que el paquete no funcionará correctamente), use la opción `--nodeps`.

32.2.3. Desinstalación

Desinstalar un paquete es tan simple como instalarlo. Teclee el siguiente comando en el intérprete de comandos de la shell:

```
rpm -e foo
```

Nota

Observe que hemos usado el *nombre* `foo` del paquete, no el nombre de *archivo* `foo-1.0-1.i386.rpm` del paquete original. Para desinstalar un paquete necesitará sustituir `foo` con el verdadero nombre de paquete del paquete original.

Podría encontrarse con un error de dependencia cuando esté desinstalando un paquete si otro paquete instalado depende del que está tratando de eliminar. Por ejemplo:

```
Preparing...                ########################################### [100%]
error: removing these packages would break dependencies:
        foo is needed by  bar-2.0.20-3.i386.rpm
```

Para hacer que RPM ignore este error y desinstale el paquete de todos modos (que tampoco es buena idea ya que al hacerlo, el paquete que depende de él probablemente dejará de funcionar correctamente), use la opción `--nodeps`.

32.2.4. Actualización

Actualizar un paquete es parecido a instalarlo. Teclee el siguiente comando en un intérprete de comandos de la shell:

```
rpm -Uvh foo-2.0-1.i386.rpm
```

Lo que no se ve arriba es que RPM ha desinstalado automáticamente cualquier versión antigua del paquete `foo`. De hecho, tal vez desee usar `-U` siempre para instalar paquetes, ya que funcionará aunque no haya versiones precedentes del paquete instaladas.

Ya que RPM lleva a cabo la actualización inteligente de paquetes con archivos de configuración, tal vez vea un mensaje como el siguiente:

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

Este mensaje significa que los cambios hechos al archivo de configuración podrían no ser "compatibles a reenvío" con el archivo de configuración nuevo en el paquete, así que RPM ha almacenado su archivo original y ha instalado uno nuevo. Debería averiguar cuáles son las diferencias entre los dos archivos de configuración y resuelva el problema tan pronto como le sea posible para asegurarse que su sistema continúe funcionando correctamente.

La actualización es en realidad una combinación de las actividades de desinstalación e instalación, así que durante una actualización RPM, podrá encontrar errores de desinstalación e instalación, además de cualquier otro tipo de error. Si RPM cree que usted está tratando de actualizar a un número de versión de paquete *más antiguo*, aparecerá lo siguiente:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

Para hacer que RPM "actualice" de todos modos, use la opción `--oldpackage`:

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. Refrescamiento

Refrescar un paquete es parecido a actualizarlo. Teclee el siguiente comando en un intérprete de comandos shell:

```
rpm -Fvh foo-1.2-1.i386.rpm
```

La opción de refrescamiento RPM compara las versiones de los paquetes especificados en la línea de comandos con las versiones de los paquetes que ya han sido instalados en su sistema. Cuando la opción de refrescamiento de RPM elabora una versión más reciente de un paquete ya instalado, éste será actualizado a la versión más reciente. Sin embargo, la opción de refrescamiento de RPM no instalará un paquete si no existe un paquete previamente instalado del mismo nombre. Esto no es igual a la opción de actualización de RPM, ya que una actualización *sí* instalará paquetes, no importa si ya esté instalada una versión más antigua de un paquete.

La opción de refrescamiento de RPM funciona ya sea para paquetes individuales que para un grupo de paquetes. Si usted acaba de descargar una gran cantidad de paquetes diferentes y sólo desea actualizar los paquetes que ya estaban instalados en su sistema, la solución es el refrescamiento. Si utiliza la opción de refrescamiento, antes de usar RPM no tendrá que eliminar ningún paquete indeseado del grupo que ha descargado.

En este caso, puede ejecutar el comando siguiente:

```
rpm -Fvh *.rpm
```

RPM actualizará automáticamente sólo los paquetes que ya estén instalados.

32.2.6. Consultas

Use el comando `rpm -q` para hacer consultas a la base de datos de los paquetes instalados. El comando `rpm -q foo` imprimirá el nombre de paquete, versión y número de lanzamiento del paquete foo instalado:

```
foo-2.0-1
```

Nota

Observe que hemos utilizado el *nombre* `foo` del paquete. Al hacer una consulta sobre un paquete, necesitará sustituir `foo` con el verdadero nombre del paquete.

En vez de especificar el nombre del paquete, se pueden usar las siguientes opciones con `-q` para especificar lo(s) paquete(s) que desea consultar. Se llaman *Opciones de especificación de paquetes*.

- `-a` consulta todos los paquetes actualmente instalados.
- `-f <file>` consultará el paquete que posea `<file>`. Cuando especifique un archivo, deberá especificar la ruta completa del archivo (`/usr/bin/ls`, por ejemplo).
- `-p <packagefile>` consulta el paquete `<packagefile>`.

Hay varias maneras de especificar qué información mostrar sobre los paquetes consultados. Las siguientes opciones sirven para seleccionar el tipo de información que usted está buscando. Se llaman *Opciones de selección de información*.

- `-i` muestra información del paquete como el nombre, la descripción, la versión, el tamaño, la fecha de construcción, la fecha de instalación, el distribuidor, y otra información miscelánea.
- `-l` muestra la lista de archivos contenidos en el paquete.
- `-s` muestra el estado de todos los archivos en el paquete.

- `-d` muestra una lista de archivos marcados como documentación (páginas de manual, páginas de información, archivos LÉAME, etc.).
- `-c` muestra una lista de archivos marcados como archivos de configuración. Estos son los archivos que usted cambia después de la instalación para adaptar el paquete a su sistema (como `sendmail.cf`, `passwd`, `inittab`, etc.).

Para acceder a opciones que muestran listas de archivos, puede añadir `-v` al comando para que muestre las listas en un formato `ls -l` conocido.

32.2.7. Verificación

La verificación de un paquete tiene que ver con comparar la información sobre archivos instalados de un paquete con la misma información del paquete original. Entre otras cosas, la verificación compara el tamaño, la suma MD5, los permisos, el tipo, el dueño y el grupo de cada archivo.

El comando `rpm -V` verifica un paquete. Usted puede utilizar cualquiera de las *Opciones de selección de paquete* de la lista para pedir que se especifiquen los paquetes que desea verificar. Un modo sencillo de verificar es `rpm -V foo`, que verifica si todos los archivos en el paquete foo se encuentran en el mismo estado en que estaban cuando originalmente fueron instalados. Por ejemplo:

- Para verificar un paquete que contiene un determinado archivo:
  `rpm -Vf /bin/vi`
- Para verificar TODOS los paquetes instalados:
  `rpm -Va`
- Para verificar un paquete instalado contra un archivo de paquete RPM
  `rpm -Vp foo-1.0-1.i386.rpm`

  Este comando puede ser útil si sospecha que sus bases de datos de RPM están dañadas.

Si todo fue verificado correctamente, no habrá salida. Si se encuentran discrepancias, serán mostradas. El formato de la salida es una cadena de ocho caracteres (una `c` identifica un archivo de configuración) seguido por el nombre del archivo. Cada uno de los ocho caracteres señala el resultado de una comparación entre un atributo del archivo al valor de ese atributo escrito en la base de datos de RPM. Un sólo `.` (punto) significa que ha pasado la prueba. Los siguientes caracteres señalan que ciertas pruebas no han sido pasadas:

- `5` — MD5 suma de verificación
- `S` — tamaño de archivo
- `L` — enlace simbólico
- `T` — hora de modificación de archivo
- `D` — dispositivo
- `U` — usuario
- `G` — grupo
- `M` — modo (incluye permisos y tipos de archivos)
- `?` — archivo que no se puede leer

Si ve alguna salida, use su buen juicio para determinar si debería quitar o reinstalar el paquete o resolver el problema de otra manera.

32.3. Verificando la firma del paquete

Si desea verificar si algún paquete ha sido dañado o alterado examine sólo la suma md5 tecleando el siguiente comando en un intérprete de comandos de shell (sustituya *<rpm-file>* con el nombre de archivo de su paquete):

```
rpm -K --nogpg <rpm-file>
```

Aparecerá el mensaje *<rpm-file>*: `md5 OK`. Este breve mensaje significa que el archivo no ha sido dañado al momento de la descarga. Si desea un mensaje más detallado, reemplace `-K` por `-Kvv` en el comando.

Por otra parte, ¿cuánto es de fiable el desarrollador que creó el paquete? Si el paquete está *firmado* con la *clave* **GnuPG** del desarrollador, sabrá que el desarrollador de verdad es quien dice ser.

Se puede firmar un paquete RPM usando la **Gnu Privacy Guard** (o **GnuPG**), para ayudarle a asegurarse que el paquete descargado es de fiar.

GnuPG es una herramienta para comunicación segura; reemplaza completa y gratuitamente la tecnología de encriptación de **PGP**, un programa electrónico de privacidad. Con **GnuPG** usted puede autentificar la validez de los documentos y encriptar/descifrar datos de y hacia otros destinatarios. Además, **GnuPG** es capaz de descifrar y verificar archivos **PGP** 5.*x*.

Durante la instalación de Red Hat Linux, **GnuPG** está instalado por defecto. De este modo podrá usar inmediatamente **GnuPG** para verificar cualquier paquete que reciba desde Red Hat. En primer lugar necesitará importar la clave pública privada de Red Hat.

32.3.1. Importar claves

Para verificar los paquetes de Red Hat tiene que importar las claves de GPG de Red Hat. Para ello, ejecute el siguiente comando en el intérprete de comandos de la shell:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

Para ver la lista de todas las claves isntaladas para la verificación de RPM, ejecute el comando:

```
rpm -qa gpg-pubkey*
```

Para la clave de Red Hat, la salida incluye:

```
gpg-pubkey-db42a60e-37ea5438
```

Para mostrar más detalles sobre una clave determinada, use `rpm -qi` seguido de la salida del anterior comando:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. Verificación de la firma de paquetes

Para controlar la firma **GnuPG** de un archivo RPM después de importar la clave del constructor **GnuPG**, use el siguiente comando (sustituya *<rpm-file>* con el nombre de archivo de su paquete RPM):

```
rpm -K <rpm-file>
```

Si todo va bien, verá el siguiente mensaje: `md5 gpg OK`. Esto significa que el paquete no está dañado.

Sugerencia

Para más información sobre GnuPG, lea el Apéndice B.

32.4. Impresione a sus amigos con RPM

RPM es una herramienta útil ya sea para administrar su sistema que para diagnosticar y solucionar problemas. La mejor manera de comprender todas sus opciones es viendo algunos ejemplos.

- Tal vez usted haya borrado algunos archivos accidentalmente, pero no está seguro de lo que ha eliminado. Si desea verificar su sistema entero y ver lo que podría hacer falta, podría intentarlo con el siguiente comando:
  ```
  rpm -Va
  ```
  Si faltan algunos archivos o parecen dañados, probablemente debería o reinstalar el paquete o desinstalarlo y luego reinstalarlo.
- Tal vez alguna vez verá un archivo que no reconoce. Para saber a qué paquete pertenece, teclearía:
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  La salida es parecida a lo siguiente:
  ```
  gv-3.5.8-22
  ```
- Podemos combinar los dos ejemplos de arriba en la siguiente hipótesis. Digamos que está teniendo problemas con `/usr/bin/paste`. Le gustaría verificar el paquete al cual pertenece ese programa, pero no sabe a cuál paquete pertenece `paste`. Simplemente teclee el siguiente comando:
  ```
  rpm -Vf /usr/bin/paste
  ```
  y se verificará el paquete correcto.
- ¿Desea encontrar más información sobre un determinado programa? Puede intentar el siguiente comando para localizar la documentación que acompañaba el paquete al cual pertenece ese programa:
  ```
  rpm -qdf /usr/bin/free
  ```
  La salida debería ser parecida a la siguiente:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```
- Podría encontrar un RPM nuevo y no saber para qué sirve. Para encontrar información sobre él, use el siguiente comando:
  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```

La salida es parecida a lo siguiente:

```
Name        : crontabs                      Relocations: (not relocateable)
Version     : 1.10                               Vendor: Red Hat, Inc.
Release     : 5                              Build Date: Fri 07 Feb 2003 04:07:32
PM EST
Install date: (not installed)                Build Host: porky.devel.redhat.com
Group       : System Environment/Base        Source RPM: crontabs-1.10-5.src.rpm
Size        : 1004                              License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

- Quizás desea ver qué archivos instala el RPM `crontabs`. Ingrese lo siguiente:

```
rpm -qlp crontabs-1.10-5.noarch.rpm
```

La salida será de la siguiente manera:

```
Name        : crontabs                      Relocations: (not relocateable)
Version     : 1.10                               Vendor: Red Hat, Inc.
Release     : 5                              Build Date: Fri 07 Feb 2003 04:07:32
PM EST
Install date: (not installed)                Build Host: porky.devel.redhat.com
Group       : System Environment/Base        Source RPM: crontabs-1.10-5.src.rpm
Size        : 1004                              License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

Estos son solamente algunos ejemplos. Al usarlo, descubrirá muchos más usos para RPM.

32.5. Recursos adicionales

RPM es una utilidad muy compleja con muchas opciones y métodos para efectuar consultas, instalar, actualizar y eliminar paquetes. Consulte los siguientes recursos para saber más sobre RPM.

32.5.1. La documentación instalada

- `rpm --help` — este comando proporciona una referencia rápida de los parámetros de RPM.
- `man rpm` — las páginas de manual de RPM le proporcionará más detalles sobre los parámetros de RPM que el comando `rpm --help`.

32.5.2. Sitios web útiles

- http://www.rpm.org/ — El sitio web de RPM.
- http://www.redhat.com/mailing-lists/ — la lista de correo RPM está archivada aquí. Para suscribirse, envíe un mensaje de correo electrónico a <rpm-list-request@redhat.com> con la palabra `subscribe` en el espacio del objeto.

32.5.3. Libros relacionados

- *Maximum RPM* por Ed Bailey; Red Hat Press — Tiene a su disposición una versión en línea del libro en http://www.rpm.org/ y en http://www.redhat.com/docs/books/.

Capítulo 33.

Herramienta de administración de paquetes

Durante la instalación, los usuarios seleccionan un tipo de instalación como por ejemplo **Estación de trabajo** o **Servidor**. Los paquetes de software son instalados basándose en esta selección. Ya que los usuarios usan los ordenadores de forma diversa, algunos desearán instalar o eliminar paquetes tras la instalación. La **Herramienta de administración de paquetes** permite a los usuarios ejecutar estas acciones.

Se requiere el sistema X Window para ejecutar la aplicación **Herramienta de administración de paquetes**. Para arrancar la aplicación, vaya al **Botón de menú principal** (en el Panel) => **Configuración del sistema** => **Paquetes**, o escriba el comando `redhat-config-packages` en el intérprete de comandos.

La misma interfaz aparece si usted inserta el CD # 1 de Red Hat Linux en su computador.

Figura 33-1. Herramienta de administración de paquetes

La interfaz para esta aplicación es parecida a la que se usa durante la instalación. Los paquetes están divididos en grupos de paquetes, que contienen una lista de *paquetes estándar* y *paquetes extra* que comparten funcionalidades comunes. Por ejemplo, el grupo **Internet gráfico** contiene un navegador de Web, cliente de correo electrónico y otros programas gráficos usados para conectarse a Internet. Los paquetes estándar no pueden ser seleccionados para eliminar a menos que el grupo de paquetes entero sea eliminado. Los paquetes extra son opcionales y pueden ser seleccionados para la instalación o la eliminación, siempre y cuando el grupo de paquetes sea seleccionado.

La ventana principal muestra una lista de grupos de paquetes. Si el grupo de paquetes está marcado en la casilla de verificación, los paquetes de ese grupo serán los que se instalarán realmente. Para visualizar la lista de paquetes individuales para un grupo, pulse el botón **Detalles**. Los paquetes indivuales marcados con un visto son los que están actualmente instalados.

33.1. Instalación de paquetes

Para instalar los paquetes estándar en un grupo de paquetes que no esté instalado en la actualidad, compruebe la casilla de verificación. Para personalizar los paquetes que van a ser instalados dentro del grupo, haga click en el botón **Detalles**. La lista de paquetes estándar y extra está visualizada, como se muestra en la Figura 33-2. Al pulsar el nombre del paquete se visualiza el espacio en el disco necesario para instalar el paquete en la parte inferior de la ventana. Al controlar la casilla de verificación al lado del paquete lo marca durante la instalación.

Puede seleccionar paquetes individuales de los grupos de paquetes ya instalados al pulsar el botón **Detalles** y marcar la casilla de verificación de cualquier paquete extra que no haya sido instalado.

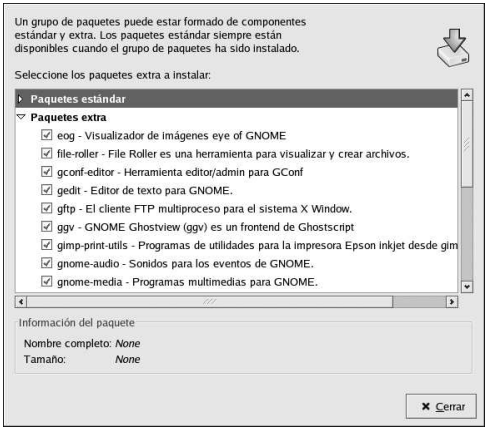

Figura 33-2. Selección individual de paquetes

Tras haber seleccionado los grupos de paquetes y los paquetes individuales a instalar, pulse el botón **Update** en la ventana principal. La aplicación contará la cantidad de espacio necesario para instalar los paquetes así como cualquier dependencia de paquetes y visualizar una ventana de resumen. Si existen dependencias de paquetes, éstas serán añadidas automáticamente a la lista de paquetes a instalar. Pulse el botón **Mostar detalles** para visualizar la lista completa de los paquetes a instalar.

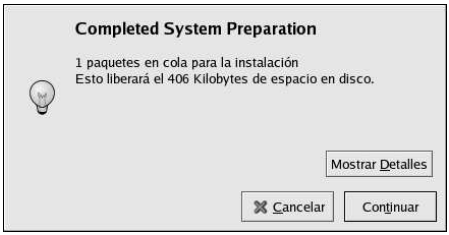

Figura 33-3. Resumen de la instalación de paquetes

Pulse **Continuar** para iniciar el proceso de instalación. Cuando haya acabado, aparecerá el mensaje **Actualización completa**.

Sugerencia

Si usa **Nautilus** para navegar por los ficheros y directorios de su ordenador, puede usarlo para instalar paquetes. En **Nautilus**, vaya al directorio que contiene un paquete RPM (generalmente acaban en `.rpm`), y pulse dos veces el icono RPM.

33.2. Eliminar paquetes

Para eliminar todos los paquetes instalados dentro de un grupo de paquetes, anule la selección de la casilla de verificación. Para eliminar paquetes individuales, pulse el botón **Detalles** al lado del grupo de paquetes y anule la selección de paquetes individuales.

Cuando haya acabado de seleccionar los paquetes a eliminar, pulse el botón **Actualizar** en la ventana principal. La aplicación cuenta la cantidad de espacio en disco que se liberará así como las dependencias del paquete de software. Si otros paquetes dependen de los paquetes que haya seleccionado eliminar, éstos serán añadidos de forma automática a la lista de paquetes a eliminar. Pulse el botón **Mostrar detalles** para ver la lista de paquetes que serán eliminados.

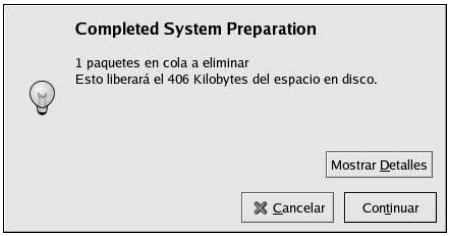

Figura 33-4. Resumen de la eliminación de paquetes

Pulse **Continuar** para iniciar el proceso de eliminación. Cuando haya acabado, aparecerá un mensaje **Update Complete**.

Sugerencia

Puede combinar la instalación y eliminación de paquetes al seleccionar los grupos de paquetes/paquetes que serán instalados/eliminados y pulsar **Actualizar**. La ventana **Preparación del sistema completo** visualizar el número de paquetes a instalar y eliminar.

Capítulo 34.

Red Hat Network

Red Hat Network es una solución de Internet para administrar uno o más sistemas Red Hat Linux. Todos los parches de seguridad, correcciones de errores y mejoras en los paquetes (conocidas usualmente como Alertas de Erratas), pueden ser descargadas directamente desde Red Hat usando la aplicación **Agente de actualización de Red Hat** o a través del sitio web de RHN en http://rhn.redhat.com/.

Figura 34-1. Su RHN

Red Hat Network le ahorra tiempo a los usuarios porque estos reciben un correo electrónico cuando está disponible una actualización de paquetes. Los usuarios no tienen que buscar en la web por los paquetes actualizados o parches de seguridad. Por defecto, Red Hat Network instala los paquetes también, de esta manera, los usuarios no tienen que saber como usar RPM o preocuparse por resolver las dependencias de software; RHN lo hace por ellos.

Cada cuenta Red Hat Network viene con:

- La lista de erratas — que le indica cuándo salen los parches de seguridad, las correcciones de errores y las mejoras de paquetes de los sistemas en su red a través de la interfaz Basic

Figura 34-2. Erratas de importancia

- Notificaciones automáticas de correo — reciba una notificación de correo cuando salen nuevos parches de errores para su sistema.
- Actualizaciones planificadas de errata — planifica la entrega de actualizaciones de errata.
- Instalación de paquetes — Planifica la instalación de paquetes en uno o más sistemas con el click de un botón.
- El **Agente de actualización de Red Hat** — use el **Agente de actualización de Red Hat** para descargar los últimos paquetes de software para su sistema (con instalación de paquetes automática opcional)
- Sitio web Red Hat Network — administre sistemas múltiples, descargue paquetes individuales y planifique acciones tales como Actualización de Errata a través de una conexión segura al web desde cualquier computador.

Para comenzar a usar Red Hat Network, siga estos pasos básicos:

1. Cree un Perfil del sistema usando alguno de los métodos siguientes:
   - Inscriba el sistema con RHN durante el **Agente de configuración** la primera vez que su sistema arranca luego de la instalación.
   - Seleccione el **Botón de menú principal => Herramientas del sistema => Red Hat Network** en su escritorio.
   - Ejecute el comando `up2date` desde el intérprete de comandos shell.

2. Conéctese a RHN en http://rhn.redhat.com/ y pida un determinado servicio para el sistema. Todos reciben una cuenta gratis a Red Hat Network para cada sistema. También se pueden adquirir cuentas adicionales.

3. Inicie la planificación de actualizaciones a través del sitio web de RHN o descargue e instale las Actualizaciones de Errata con el **Agente de actualización de Red Hat**.

Para instrucciones detalladas, lea el *Manual de referencia del usuario de Red Hat Network* disponible en http://www.redhat.com/docs/manuals/RHNetwork/.

Sugerencia

Red Hat Linux incluye la **Herramienta de notificación de Red Hat Network**, un icono del panel muy conveniente que muestra señales visibles cuando hay alguna actualización para su sistema Red Hat Linux disponible. Refiérase al siguiente URL: http://rhn.redhat.com/help/basic/applet.html para más información sobre el applet.

VI. Apéndices

Esta parte contiene instrucciones para la construcción de un kernel personalizado a partir los archivos fuente proporcionados por Red Hat, Inc.. También incluye un capítulo sobre Gnu Privacy Guard, una herramienta que puede ser usada para comunicaciones seguras.

Tabla de contenidos

Apéndice A.

Construcción de un kernel personalizado

Mucha gente nueva en Linux pregunta "¿Por qué construir mi propio kernel?". Dado el avance realizado con el uso de módulos para el kernel, la respuesta más acertada a esta pregunta es, "A menos que sepa por qué construir su propio kernel, probablemente no lo necesite".

El kernel entregado con Red Hat Linux y a través del sistema de Errata de Red Hat Linux proporciona soporte para la mayoría del hardware moderno y características del kernel. Para la mayoría de los usuarios, no necesita ser recompilado. Este apéndice es proporcionado como una guía para aquellos usuarios que deseen recompilar su kernel y aprender un poco más sobre ello, para usuarios que quieren compilar una característica experimental en el kernel, etc.

Para actualizar el kernel usando los paquetes del kernel distribuidos por Red Hat, Inc., consulte el Capítulo 30.

Aviso

La construcción de un kernel personalizado no es soportado por el Equipo de soporte de instalación de Red Hat Linux. Para más información sobre la actualización de su kernel usando los paquetes RPM distribuídos por Red Hat, Inc., consulte el Capítulo 30.

A.1. Preparación para la construcción

Antes de construir un kernel personalizado, es extremadamente importante asegurarse de que tiene un disquete de arranque de emergencia en caso de que se cometa un error. Para crear un disquete de arranque que le permitirá arrancar usando el kernel actual, ejecute el comando:

```
/sbin/mkbootdisk `uname -r`
```

Después de preparar el disquete, prúebelo para asegurarse de que funciona correctamente.

Para recompilar el kernel, debe tener instalado el paquete `kernel-source`. Ejecute el comando

```
rpm -q kernel-source
```

para determinar si lo tiene instalado. Si no está instalado, instálelo desde los CD-ROMs de Red Hat Linux, el sitio FTP de Red Hat FTP disponible en ftp://ftp.redhat.com (hay una lista de espejos disponible en http://www.redhat.com/mirrors.html), o desde Red Hat Network. Para más información sobre la instalación de paquetes RPM, consulte Parte V.

A.2. Construcción del Kernel

Las instrucciones de esta sección se aplican a construir un kernel modularizado. Si está interesado en construir un kernel monolítico, vea la Sección A.3 para una explicación de los diferentes aspectos de su construcción e instalación.

Nota

Este ejemplo usa la versión del kernel 2.4.20-2.47.1 (Su versión del kernel puede diferir). Para determinar su versión del kernel, teclee el comando `uname -r` y reemplace 2.4.20-2.47.1 por su versión del kernel.

Para construir un kernel para la arquitectura x86 (realice todos los pasos como root):

1. Abra un intérprete de comandos y cámbiese al directorio `/usr/src/linux-2.4/`. Todos los comandos desde este punto en adelante deben ser ejecutados desde este directorio.
2. Es importante que empiece la construcción del kernel con el árbol de las fuentes en perfectas condiciones. Esto es, es recomendable que comience con el comando `make mrproper`. Esto borrará cualquier fichero de configuración remanente de configuraciones previas que pueda estar disperso por el árbol de las fuentes. Si ya tiene un fichero de configuración funcional `/usr/src/linux-2.4/.config`, haga una copia de respaldo en un directorio diferente antes de ejecutar este comando.
3. Se recomienda que use la configuración del kernel de Red Hat Linux por defecto como punto de partida. Para hacer esto, copie el archivo de configuración para la arquitectura del sistema desde el directorio `/usr/src/linux-2.4/configs/` a `/usr/src/linux-2.4/.config`. Si el sistema tiene más de cuatro gigabytes de memoria, copie el archivo que contiene la palabra clave `bigmem`.
4. Luego, personalice los parámetros. Si está ejecutando el Sistema X Window, el método recomendado es usar el `make xconfig` para ejecutar la **Linux Kernel Configuration**.

Nota

Para usar la herramienta gráfica iniciada con el comando `make xconfig`, debe estar instalado el paquete `tk`, el cual proporciona el comando `wish`. Para más información sobre la instalación de paquetes RPM, consulte Parte V.

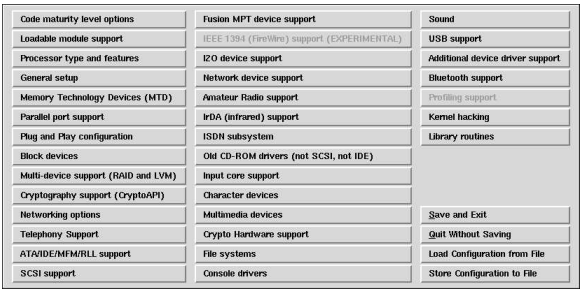

Figura A-1. Configuración de categorías de componentes de Kernel

Como se muestra en la Figura A-1, seleccione una categoría haciendo click sobre ella. Dentro de cada categoría hay componentes. Seleccione **y** (yes), **m** (module), o **n** (no) al lado del componente para compilarlo en el kernel, compilarlo como un módulo kernel o no compilarlo. Para obtener más detalles de un componente, haga click en el botón **Help** que tiene al lado.

Haga click en **Main menu** para volver a la lista de categorías.

Después de terminar la configuracion, haga click en el botón **Save and Exit** en la ventana del menú principal para crear el archivo de configuración `/usr/src/linux-2.4/.config` y salir el programa **Linux Kernel Configuration**.

Aún si no se efectuó ningún cambio en los parámetros, la ejecución del comando `make xconfig` (o alguno de los otros métodos para la configuración del kernel) se requiere antes de continuar.

Los otros métodos disponibles para la confifuración del kernel incluyen:

- `make config` — Un programa de texto interactivo. Los componentes le son presentados de forma lineal y los va respondiendo uno a uno. Este método no requiere el Sistema X Window y no le permite cambiar sus respuestas a preguntas previas.
- `make menuconfig` — Un programa de modo de texto, basado en menú. Los componentes le son presentados en un menú categorizado; seleccione los componentes deseados de la misma manera usada en el programa de instalación en modo texto de Red Hat Linux. Cambie la etiqueta correspondiente al punto que quiera incluir: **[*]** (incorporado), **[ ]** (excluido), **<M>** (modularizado), o **< >** (posibilidad de modularizar). Este método no requiere el Sistema X Window.
- `make oldconfig` — Este es un script no interactivo que configurará su fichero de configuración con los valores predeterminados. Si está usando el kernel predeterminado de Red Hat, creará un fichero de configuración para el kernel que manejará Red Hat Linux en su arquitectura. Esto es útil para configurar su kernel con una configuración predeterminada que funciona, y entonces poder desactivar las características que no quiera usar.

Nota

Para usar `kmod` y los módulos del kernel conteste **`Yes`** a `kmod support` y `module version (CONFIG_MODVERSIONS) support` durante la configuración.

5. Después de crear el archivo `/usr/src/linux-2.4/.config`, use el comando `make dep` para configurar las dependencias correctamente.
6. Use el comando `make clean` para preparar el árbol fuente para construir.
7. Se le recomienda que aporte un número de versión modificada al kernel personalizado de manera que no sobreescriba el kernel ya existente. El método descrito aquí es el más sencillo para recuperar el sistema en caso de problemas. Si está interesado en otras posibilidades, puede encontrar más detalles en http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html o en el `Makefile` en `/usr/src/linux-2.4`.

   Por defecto, `/usr/src/linux-2.4/Makefile` incluye la palabra `custom` al final de la línea que empieza por `EXTRAVERSION`. Añadir a la cadena le permitirá tener contemporaneamente en su sistema el kernel antiguo en funcionamiento y el kernel nuevo (versión 2.4.20-2.47.1 personalizada).

   Si el sistema contiene más de un kernel personalizado, un buen método es anexar la fecha al final (u otro identificador).
8. Compile el kernel con `make bzImage`.
9. Compile cualquier módulo que haya configurado con `make modules`.
10. Use el comando `make modules_install` para instalar los módulos del kernel (aún si no se compiló ninguno). Observe el guión (_) en el comando. Esto instala los módulos kernel en la ruta del directorio `/lib/modules/<KERNELVERSION>/kernel/drivers` (donde *KERNELVERSION* es la versión especificada en el `Makefile`). En este ejemplo sería `/lib/modules/2.4.20-2.47.1custom/kernel/drivers/`.

11. Use `make install` para copiar su nuevo kernel y sus ficheros asociados a los directorios apropiados.

    Además de instalar los ficheros del kernel en el directorio `/boot`, este comando ejecuta el script `/sbin/new-kernel-pkg` que construye una nueva imagen `initrd` y añade nuevas entradas para el fichero de configuración del gestor de arranque.

    Si posee un adaptador SCSI y ha compilado el driver SCSI driver como un módulo o si ha construido un kernel con el soporte ext3 como un módulo (predeterminado en Red Hat Linux), se necesitará la imagen `initrd`.

12. Aunque la imagen `initrd` y las modificaciones del gestor de arranque han sido creadas, debería verificar que ha sido realizado correctamente y también asegurarse de usar la versión del kernel personalizado en vez de la 2.4.20-2.47.1. Consulte la Sección 30.5 y la Sección 30.6 para más detalles.

A.3. Construcción de un kernel monolítico

Para construir un kernel monolítico, sigua los mismos pasos que al compilar un kernel modularizado, con unas pocas excepciones.

- Cuando configure el kernel, no compile nada como módulo. En otras palabras, sólo responda **`Yes`** o **`No`** a las preguntas. También, debería responder **`No`** a `kmod support` y `module version (CONFIG_MODVERSIONS) support`.
- Omita los siguiente pasos:
  ```
  make modules
  make modules_install
  ```
- Añada la línea `kernel` en `grub.conf` con `nomodules` o modifique el archivo `lilo.conf` para incluir la línea `append=nomodules`.

A.4. Recursos adicionales

Para obtener más información sobre el kernel de Linux, consulte las siguientes fuentes.

A.4.1. Documentación instalada

- `/usr/src/linux-2.4/Documentation` — Documentación avanzada sobre el kernel y los módulos. Está dirigida a las personas que deseen contribuir al código fuente del kernel y en profundizar en el funcionamiento del kernel.

A.4.2. Sitios web útiles

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — *The Linux Kernel HOWTO* del Linux Documentation Project.
- http://www.kernel.org/pub/linux/docs/lkml/ — La lista de correo del kernel de Linux.

Apéndice B.

Iniciándose con Gnu Privacy Guard

¿Se ha preguntado alguna vez si su correo electrónico es seguro? Desgraciadamente siempre hay alguien que intercepta los mensajes y los lee.

En el correo tradicional (también conocido como "snail"), las cartas se mandan en un sobre con un sello desde la oficina de correos. Sin embargo, mandar e-mails por Internet no es tan seguro ya que normalmente los mensajes se mandan sin ningún tipo de código de un servidor a otro. No se han tomado ningún tipo de medidas de seguridad especiales para evitar que los correos electrónicos sean interceptados.

Para ayudarle a proteger su privacidad, Red Hat Linux 9 incluye GnuPG, *GNU Privacy Guard*, que ya viene instalada por defecto durante la instalación de Red Hat Linux. También se le conoce como *GPG*.

GnuPG es una herramienta que se usa para las comunicaciones seguras; es un reemplazo gratuito de la tecnología de encriptación PGP (Pretty Good Privacy, una aplicación de encriptación muy conocida). Con GnuPG, puede codificar sus datos y su correspondencia y autentificar ésta con una *firma digital*. GnuPG es también capaz de descifrar y verificar PGP 5.*x*.

Debido a que la herramienta GnuPG es compatible con otros sistemas estándares, su correspondencia segura será también compatible con otras aplicaciones de correo electrónico en otros sistemas operativos, tales como Windows y Macintosh.

GnuPG usa la *criptografía de clave pública* para asegurar a los usuarios un intercambio de datos seguro. En un esquema de criptografía de clave pública, se tiene que crear dos claves: una pública y otra privada. Usted intercambia la clave pública con aquellas personas con las que se comunica o con el servidor de claves pero nunca debe revelar la clave privada.

La encriptación va a depender del uso de las claves. En criptografía tradicional, ambas partes tienen la misma clave que usan para descodificar cada una de las transmisiones de información. En la criptografía de clave pública, co-existen dos claves: una pública y otra privada. Normalmente, una persona o una organización da a conocer su clave pública y se reserva la privada. Los datos codificados con la clave pública sólo pueden ser descifrados con la privada y viceversa.

Importante

Recuerde que puede revelar su clave pública con quien quiera comunicarse de forma segura, pero no debe por ningún motivo hacerlo con la privada.

Una explicación más a fondo sobre criptografía está más allá del ámbito de ésta publicación; pero puede encontrar muchos libros sobre este tópico. Sin embargo, esperamos que en este capítulo encuentre suficiente información para entender GnuPG y comenzar a usar la criptografía en su correspondencia. Si quiere aprender más sobre GnuPG, PGP y la tecnología de encriptación, vea Sección B.8.

B.1. Archivo de configuración

La primera vez que ejecute el comando GnuPG, se creará un directorio `.gnupg` en su directorio principal. Desde la versión 1.2, el nombre del archivo de configuración ha cambiado de `.gnupg/options` a `.gnupg/gpg.conf`. Si no encuentra `.gnupg/gpg.conf` en su directorio principal, será usado `.gnupg/options`. Si solamente usa la versión 1.2 o superior, se recomienda que renombre el archivo de configuración con el siguiente comando:

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

Si está actualizando desde una versión anterior a 1.0.7, puede crear caches de firmas en su llavero para disminuir el tiempo de acceso al llavero. Para realizar esta operación, ejecute el comando siguiente una vez:

```
gpg --rebuild-keydb-caches
```

B.2. Mensajes de advertencia

Cuando ejecute los comandos GnuPG, probablemente verá el siguiente mensaje:

```
gpg: Warning: using insecure memory!
```

Este aviso aparece porque usuarios que no son root no pueden bloquear páginas de memoria. Si los usuarios pudiesen bloquear páginas de memoria, también pueden hacer ataques de rechazo de servicio por falta de memoria, out-of-memory Denial of Service (DoS); y así, un posible problema de seguridad. Para más detalles, refiérase a http://www.gnupg.org/(en)/documentation/faqs.html#q6.1.

Quizás vea el mensaje siguiente:

```
gpg: WARNING: unsafe permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

Este mensaje es mostrado si los permisos de su archivo de configuración permite a otros leerlo. Si ve esta advertencia, se recomienda que ejecute el comando siguiente para cambiar la permisología:

```
chmod 600 ~/.gnupg/gpg.conf
```

Otro mensaje de advertencia común es el siguiente:

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

Este mensaje es mostrado si los permisos de archivo del directorio que contiene el archivo de configuración permite a otros leer su contenido. Si ve esta advertencia, se recomienda que ejecute el comando siguiente para cambiar los permisos de archivos:

```
chmod 700 ~/.gnupg
```

Si ha realizado una actualización de una versión previa de GnuPG, puede que vea el siguiente mensaje:

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated
option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

Esta advertencia se debe a que el archivo `~/.gnupg/gpg.conf` contiene la línea:

```
honor-http-proxy
```

Las versiones 1.0.7 y superiores prefieren una sintaxis diferente. Cambie la línea a lo siguiente:

```
keyserver-options honor-http-proxy
```

B.3. Generar un par de claves

Para comenzar a utilizar GnuPG, debe primero generar un nuevo par de claves: una pública y otra privada.

Para generar un par de claves, en el intérprete de comandos, escriba el comando siguiente:

```
gpg --gen-key
```

Debería realizar esta operación como usuario normal y no como root.

Verá una pantalla de introducción en la que encontrará las opciones y entre ellas la que el sistema le recomienda (por defecto) que se parece a lo siguiente:

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection?
```

De hecho, la mayor parte de las pantallas que le piden escoger una opción le mostrarán las opciones predeterminadas entre paréntesis. Puede aceptar las opciones predeterminadas presionando [Intro].

En la primera pantalla, debería aceptar la opción por defecto: `(1) DSA and ElGamal`. Esta opción le permitirá crear una firma digital y encriptar (o descifrar) con dos tipos de tecnologías. Escriba **1** y luego presione [Intro].

Después, escoja el tamaño de la clave, o que tan larga debería ser la clave. Generalmente, miestras más larga la clave, más resistente serán sus mensajes en contra de ataques. El tamaño por defecto, 1024 bits, debería ser suficientemente fuerte para la mayoría de los usuarios, por lo que puede presionar [Intro].

La próxima opción le pide especificar el tiempo de validez de su clave. Usualmente, basta con el valor por defecto (`0 = la clave no caduca`). Si escoge otra fecha de caducidad, recuerde que se lo debe comunicar a todas aquellas personas con las que intercambia información así como también debe crear una nueva clave pública. Si no selecciona una fecha de caducidad, se le pedirá que confirme su decisión. Presione [y] para confirmar su decisión.

Lo siguiente que tiene que hacer es proporcionar un identificador de usuario que consta de su nombre, su dirección de correo electrónico y un comentario adicional. Cuando termine, se le presentará un resúmen con la información que ha ingresado.

Una vez que acepte sus selecciones, tendrá que suministrar su palabra de paso.

Sugerencia

Como ocurre con las contraseñas normales, debe elegir una buena frase como contraseña para que así pueda tener una seguridad óptima con la herramiente GnuPG. Por ejemplo, combine en la frase letras en mayúscula y minúscula, números, exclamaciones e interrogaciones, etc.

Una vez que haya ingresado y verificado la palabra de paso, se crearán sus claves. Verá un mensaje similar al siguiente:

```
We need to generate a lot of random bytes. It is a good idea to perform
```

```
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++.........................++++
```

Si desaparece esta pantalla quiere decir que ya se han creado las claves y que se encuentran en el archivo `.gnupg` en su directorio principal. Para listar sus claves ejecute:

```
gpg --list-keys
```

Verá algo similar a lo siguiente:

```
/home/username/.gnupg/pubring.gpg
---------------------------------------
pub  1024D/B7085C8A 2000-06-18 Your Name
<you@example.com>
sub  1024g/E12AF9C4 2000-06-18
```

Si ha creado una clave GnuPG con la versión 1.0.6 o anterior, ha exportado su clave privada y la ha importado en una nueva, deberá confiar explícitamente en su clave para firmar items con la versión 1.0.7 o superior. Para confiar su clave, escriba el comando siguiente (reemplace *<user-id>*):

```
gpg --edit-key <user-id>
```

En el intérprete de comandos `Command>` escriba **`trust`** y seleccione `5 = I trust ultimately` para confiar en su propia clave.

B.4. Crear un certificado de revocación

Una vez que haya obtenido el par de claves, debe crear un certificado de revocación para su clave pública. Si olvida su palabra de paso, o si ésta ha sido comprometida, puede publicar este certificado para notificar a los usuarios que su clave pública ya no se debería usar.

Nota

Cuando emite un certificado de revocación, usted no está eliminando la clave que ha creado. Más bien se esta dando una forma segura de anular su clave pública del uso público en caso de que se le olvide su palabra de paso, se cambie de PSI, o sufra algún daño en el disco duro. El certificado de revocación puede ser usado para descalificar su clave pública.

Su firma será válida para aquellos que lean su correspondencia antes de que se revoque su clave y además podrá descifrar los mensajes recibidos antes de la revocación. Para crear el certificado de revocación use la opción `--gen-revoke`:

```
gpg --output revoke.asc --gen-revoke
<you@example.com>
```

Observe que si omite la opción `--output revoke.asc` el certificado de revocación se devuelve al monitor, es decir, a la salida estándar. Aunque puede copiar y pegar el contenido de la salida en cualquier fichero usando un editor de textos, seguramente sea más sencillo mandarlo a su directorio de conexión. De esta manera, puede guardar el certificado para usarlo cuando lo necesite o grabarlo en un disquete y guardarlo en un lugar seguro.

La salida se parecerá a lo siguiente:

```
sec  1024D/823D25A9 2000-04-26  Your Name
<you@example.com>

Create a revocation certificate for this key?
```

Presione [Y] para crear un certificado de revocación para la clave mostrada. Luego, se le pedirá que seleccione la razón de la revocación y que proporcione una descripción opcional. Después de confirmar el motivo, ingrese la palabra de paso para generar la clave.

Una vez creado el certificado de revocación (`revoke.asc`), será colocado en su directorio de conexión. Debería copiar el certificado en un disquete y guardarlo en un lugar seguro (si no sabe cómo se copia un archivo en un disquete con el sistema Red Hat Linux consulte el *Manual del principiante de Red Hat Linux*.)

B.5. Exportar la clave pública

Antes de que pueda usar la criptografía de clave pública, otras personas deben tener una copia de su clave pública. Para enviar su clave a los correspondientes o al servidor de claves, debe *exportar* la clave.

Para exportar su clave de manera que pueda visualizarla en la página web o añadirla al email, escriba el comando:

```
gpg --armor --export
<you@example.com> >
mykey.asc
```

No verá ninguna salida, porque usted no solamente está exportando la clave pública, sino que ha redirigido la salida a un archivo llamado, por ejemplo, `mykey.asc` (sin la adición de `> mykey.asc`, la clave aparecerá en la salida estándar, es decir en la pantalla de su monitor.)

Ahora que la clave se encuentra en el archivo `mykey.asc` puede insertarla en el correo electrónico o exportarlo a un servidor de claves. Para ver la clave, escriba `less mykey.asc` para abrir el archivo en un paginador (escriba [q] para salir del paginador). Debería parecerse a lo siguiente:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lX0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5llluGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
```

```
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. Exportar la clave a un servidor de claves

Si está escribiendo a pocas personas puede exportar la clave pública y mandársela personalmente. Sin embargo, si se trata de muchas personas, ahorra tiempo si usa un servidor de claves.

Un servidor de claves es un depósito que se encuentra en Internet en el que puede almacenar su clave pública y distribuirla a cualquier persona que la requiera. Existen muchos servidores de claves disponibles y muchos de ellos intentan estar sincronizados; mandar la clave a un servidor de claves es como distribuirla a todos. Una persona puede pedir la clave a un servidor, importarla a sus llaveros de los servidores de tal manera que la comunicación que mantenga sea segura.

Sugerencia

Debido a que la mayoría de los servidores están sincronizados, mandar la clave a uno de ellos es como mandársela a todos. Sin embargo, puede ubicar diferentes servidores de claves. Un buen lugar para comenzar su búsqueda de servidores de claves y más información es *Keyserver.Net* disponible en http://www.keyserver.net.

Puede mandar la clave pública desde la línea de comandos o desde un navegador; por supuesto, para poder mandar y recibir claves de un servidor de claves tiene que estar conectado a Internet.

- Desde la línea de comandos, escriba lo siguiente:
  `gpg --keyserver search.keyserver.net --send-key you@example.com`
- Desde el navegador, vaya a Keyserver.Net (http://www.keyserver.net) y seleccione la opción que desea agregar su propia clave pública PGP.

  Lo siguiente que tiene que hacer es copiar y pegar la clave pública en el lugar apropiado de la página web. Si necesita instrucciones para hacer esto, haga lo siguiente:

  - Abra el archivo de su clave pública exportado (tal como *mykey.asc*, que fue creado en Sección B.5) con un paginador — por ejemplo, use el comando `less mykey.asc`.
  - Usando su ratón, copie el archivo resaltando todas las líneas desde `BEGIN PGP` a `END PGP` (vea la Figura B-1).
  - Pegue los contenidos del fichero *mykey.asc* en el área apropiada de la página en Keyserver.Net utilizando el tercer botón de su ratón (o ambos botones simultáneamente si tiene un ratón de sólo dos botones). Luego seleccione el botón **Submit** en la página del servidor de claves. (Si comete un error, presione el botón **Reset** en la página para limpiar su clave copiada.)

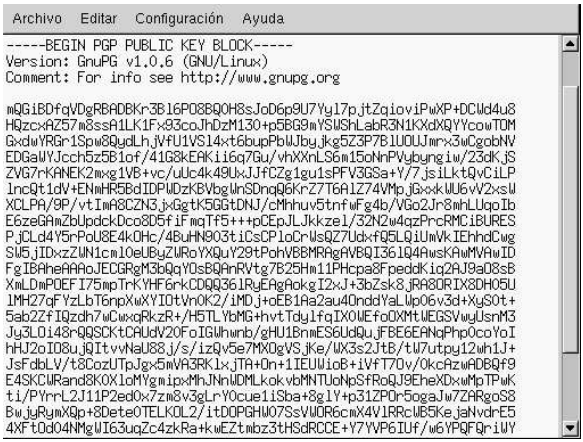

Figura B-1. Copiar la clave pública

Observe que si quiere presentar su clave a otro servidor de claves basado en web, la transacción es esencialmente la misma.

Eso es todo lo que tiene que hacer. Tanto si usa la línea de comandos como la Web, aparecerá un mensaje en la pantalla que le indicará que la transferencia de la clave ha llegado a buen fin — A partir de ahora, todos aquellos que se quieran comunicar con usted de una manera segura no tienen más que importar su clave pública y añadirla a sus llaveros.

B.6. Importar una clave pública

La otra parte del intercambio de claves es la importación de claves de otras personas a su llavero — es tan fácil como la exportación. Cuando importa una clave pública, puede descifrar los mensajes de esa persona y verificar la firma digital contra su clave pública en su llavero.

Una de las maneras más sencillas de importar una clave es descargarla o grabarla desde un sitio Web.

Después de descargarla y guardarla en el fichero *key.asc*, use el comando siguiente para agregarla a su llavero.

```
gpg --import key.asc
```

Otra manera de grabar la clave es usar la opción del navegador **Guardar como**. Si usa un navegador como **Mozilla**, y ubica una clave en un servidor de claves, puede guardar la página como un archivo de texto (vaya a **Archivo => Guardar página como**). En la opción desplegable al lado de **Tipos de archivo**, escoja **Archivos de texto (*.txt)**. Luego, puede importar la clave — pero recuerde del archivo que guardó. Por ejemplo, si guardó una clave como archivo de texto llamado *newkey.txt*, para importar el archivo, en el intérprete de comandos, escriba el siguiente comando:

```
gpg --import newkey.txt
```

La salida será similar a lo siguiente:

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Para verificar que el proceso haya llegado a buen fin, use el comando `gpg --list-keys`; debería ver la clave importada listada en su llavero.

Cuando usted importa una clave, la está agregando a su *llavero* (un archivo en el cual se guardan las claves públicas y privadas). Luego, cuando descargue un documento o archivo desde esa entidad, puede verificar la validez del documento comparándolo con la clave en su llavero.

B.7. ¿Qué son las firmas digitales?

Las firmas digitales son como las firmas normales. A diferencia de las firmas tradicionales, las firmas digitales no se pueden imitar. Esto se debe a que la firma se ha creado con su clave privada y sólo puede verificarse con su clave pública.

Una firma digital coloca también una marca de tiempo en el documento; se puede decir entonces que la hora en la que firmó el documento es parte de la firma. Así, si alguien quiere modificar el documento, no podrá verificar la firma. Algunas aplicaciones para el correo electrónico, tales como **Exmh** o KDE's **KMail**, incluyen la habilidad de firmar documentos con GnuPG dentro de la interfaz de la aplicación.

Dos tipos útiles de firmas digitales son: *clearsigned* y *detached signatures*. Ambos tipos de firmas incorporan la misma seguridad de autenticidad, ya que no requieren que el destinatario del mensaje descifre el mensaje al completo.

En un mensaje clearsigned, su firma aparecerá como un bloque de texto dentro del contexto de su mensaje; en detached signatures será enviada una firma como un archivo separado con la correspondencia.

B.8. Recursos adicionales

Hay mucho más sobre la tecnología de encriptación de lo que se puede presentar en una introducción de GnuPG. He aquí algunos recursos donde puede obtener más información.

B.8.1. Documentación instalada

- `man gpg` and `info gpg` — Referencia rápida de comandos y opciones de GnuPG.

B.8.2. Sitios web útiles

- http://www.gnupg.org — El sitio web de GnuPG con enlaces a las últimas versiones de GnuPG, una guía completa para el usuario y otros recursos de criptografía.
- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html — Visite el *Encryption Tutorial* desde Webmonkey para aprender más sobre criptografía y las técnicas de aplicación.
- http://www.eff.org/pub/Privacy — La Electronic Frontier Foundation, archivos de "Privacy, Security, Crypto, & Surveillance".

B.8.3. Libros relacionados

- *The Official PGP User's Guide* por Philip R. Zimmerman; MIT Press
- *PGP: Pretty Good Privacy* de Simson Garfinkel; O'Reilly & Associates, Inc.

- *E-Mail Security: How to Keep Your Electronic Messages Private* por Bruce Schneier; John Wiley & Sons

Índice

Símbolos

A

B

C

D

E

F

G

H

I

K

L

M

N

R

S

T

U

V

W

X

Y

Colophon

Los manuales de Red Hat Linux son escritos en formato DocBook SGML v4.1. Los formatos HTML y PDF son producidos usando hojas de estilos personalizados DSSSL y scripts personalizados jade wrapper. Los archivos DocBook SGML son escritos en **Emacs** con la ayuda del modo PSGML.

Garrett LeSage creó los gráficos de admonición (nota, sugerencia, importante, aviso y atención). Pueden ser distribuídos gratuitamente con la documentación de Red Hat.

El Equipo de Documentación del producto Red Hat Linux está formado por las siguientes personas:

Sandra A. Moore — Escritor inicial y mantenedora del *Manual de instalación de Red Hat Linux para x86*; Colaboradora en la escritura del *Manual del principiante de Red Hat Linux*

Tammy Fox — Escritora inicial y mantenedora del *Manual de personalización de Red Hat Linux*; Colaboradora en la escritura del *Manual del principiante de Red Hat Linux*; Escritora inicial y mantenedora de las hojas de estilo personalizadas DocBook y los scripts

Edward C. Bailey — Escritor inicial y mantenedor del *Manual de administración del sistema de Red Hat Linux*; Colaborador en la escritura del *Manual de instalación de Red Hat Linux para x86*

Johnray Fuller — Escritor inicial y mantenedor del *Manual de referencia de Red Hat Linux*; Co-escritor y co-mantenedor del *Manual de seguridad de Red Hat Linux*; Colaborador en la escritura del *Manual de administración del sistema de Red Hat Linux*

John Ha — Escritor inicial y mantenedor del *Manual del principiante de Red Hat Linux*; Co-escritor y co-mantenedor del *Manual de seguridad de Red Hat Linux*; Colaborador en la escritura del *Manual de administración del sistema de Red Hat Linux*

Yelitza Louzé — Traductor técnico al Español del *Manual de instalación de Red Hat Linux para x86*; el *Manual del principiante de Red Hat Linux*; el *Manual de personalización de Red Hat Linux* y del *Manual de referencia de Red Hat Linux*