Red Hat Enterprise Linux 5.0.0

Manual de implementación de Red Hat Enterprise Linux

Red Hat Enterprise Linux 5.0.0: Manual de implementación de Red Hat Enterprise Linux

Este manual de implementación documenta toda la información relevante concerniente a la implementación, configuración y administración de Red Hat Enterprise Linux 5.0.0.

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

Documentation-Deployment

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Tabla de contenidos

Introducción

Bienvenido al *Manual de implementación de Red Hat Enterprise Linux*.

El Manual de implementación de Red Hat Enterprise Linux contiene información sobre cómo personalizar su sistema Red Hat Enterprise Linux para satisfacer sus necesidades. Si está buscando una guía completa, orientada a tareas para la configuración y personalización de su sistema, este es el manual que está buscando.

Esta manual asume que usted comprende los conceptos básicos relacionados con su sistema Red Hat Enterprise Linux. Si necesita ayuda para instalar Red Hat Enterprise Linux, consulte el *Manual de instalación de Red Hat Enterprise Linux*.

1. Convenciones del documento

En este manual ciertas palabras utilizan diferentes tipos de letras, tamañosy pesos. Este énfasis es sistemático; diferentes palabras se representan con el mismo estilo para indicar su inclusión en una categoria específica. Los tipos de palabras que se representan de esta manera son:

`comandos`
: Los comandos en Linux (y comandos de otros sistemas operativos, cuando estos se utilicen) 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 invocar el comando. A veces un comando contiene palabras que aparecerían con un estilo diferente si estuvieran solas (por ejemplo, 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.

`nombres de archivos`
: 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. 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.

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

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

tecla

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

Para utilizar la completación con **Tab** para enumerar los archivos en particular en un directorio, escriba `ls` luego un caracter y finalmente pulse la tecla **Tab**. Aparecerá una lista de archivos en el directorio que empiezan con esa letra.

tecla-combinación

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

La combinación de teclas **Ctrl**-**Alt**-**Retroceso** terminará la sesión gráfica y lo llevará a la pantalla gráfica de inicio de sesión o a la consola.

texto de una interfaz gráfica (GUI)

Un título, palabra o frase encontrada en una pantalla o ventana en la interfaz gráfica aparecerá en este estilo. La finalidad del texto escrito en este estilo es la de identificar una pantalla GUI particular o un elemento en una pantalla gráfica (p.ej. 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 clic sobre la palabra en la pantalla GUI, aparecerá el resto del menú. Por ejemplo:

Bajo **Archivo** en una terminal de GNOME, la opción **Nueva solapa** le permite abrir múltiples intérpretes de comandos de la shell en la misma ventana.

Las instrucciones para escribir una secuencia de comandos desde un menú GUI aparecerán como en el siguiente ejemplo:

Vaya a **Aplicaciones** (el menú principal en el panel) => **Programación** => **Editor de texto Emacs** para iniciar el editor de texto **Emacs**.

botón en una pantalla o ventana GUI

Este estilo indica que el texto puede encontrarse en un botón que se puede pulsar en una pantalla GUI. Por ejemplo:

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

`salida del computador`

El texto en este estilo indica el texto desplegado en un intérprete de comandos de la shell, tales como mensajes de error y respuestas a comandos. Por ejemplo:

Utilice el comando `ls` para visualizar los contenidos de un directorio. Por ejemplo:

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

La salida de pantalla que un comando retorna (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 algo, aparecerá con el siguiente estilo. Ejemplos:

```
$

#

[stephen@maturin stephen]$

leopard login:
```

`entrada de 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 presenta en este estilo:

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

`<reemplazable>`

El texto usado en los ejemplos, que se supone debe ser reemplazado con datos proporcionados por el usuario, se representa en este estilo. En el siguiente ejemplo, *`<número-versión>`* se mostrará en este estilo:

El directorio para la fuente del kernel es `/usr/src/kernels/`*`<número-versión>`*`/`, donde *`<número-versión>`* es la versión del kernel instalado en este sistema.

Adicionalmente, usamos diferentes tipos de estrategias para llamar su atención sobre determinados tipos de información. Dependiendo de la importancia de esta información, estos elementos serán marcados como nota, sugerencia, importante, 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 de los paquetes instalados en su sistema.

Importante

Si modifica el archivo de configuración de DHCP, los cambios no surtirán efecto

sino hasta que reinicie el demonio DHCP.

Advertencia

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

Aviso

Tenga cuidado de borrar solamente las particiones necesaria. Remover otras particiones puede resultar en perdida de datos o en un entorno de sistema corrupto.

2. Envíenos su opinión

Si encuentra algún error en el *Manual de implementación de Red Hat Enterprise Linux*, o si se le ha ocurrido una manera de mejorar este manual, nos encantaría escuchar sus comentarios. Por favor envíe un informe a Bugzilla (`http://bugzilla.redhat.com/bugzilla/`) contra el componente `Deployment_Guide`.

Si tiene alguna sugerencia para mejorar la documentación, trate de ser tan específico como sea posible. Si ha encontrado un error, por favor incluya el número de la sección y parte del texto alrededor del error para que así lo podamos localizar rápidamente.

Parte I. Configuración relacionada a la red

Después de explicar cómo configurar la red, esta parte discute temas relacionados a redes, tales como permitir las conexiones remotas, compartir archivos y directorios sobre la red y la configuración de un servidor Web.

Capítulo 1. Interfaces de red

Bajo Red Hat Enterprise Linux, todas las comunicaciones de red acontecen entre *interfaces* de software configuradas y *dispositivos de red físicos* conectados al sistema.

Los archivos de configuración para las interfaces de red y los scripts para activarlas o desactivarlas están ubicados en el directorio `/etc/sysconfig/network-scripts`. Aún cuando el número y tipo de archivos de interfaces pueden diferir de sistema a sistema, hay tres categorías de archivos que existen en este directorio.

1. *Archivos de configuración de interfaz*
2. *Scripts de control de interfaz*
3. *Archivos de funciones de red*

Los archivos en cada una de estas categorías trabajan juntos para habilitar varios dispositivos de red.

Este capítulo explora la relación entre estos archivos y cómo son utilizados.

1. Archivos de configuración de red

Antes de ahondar en los archivos de configuración de interfaz, hagamos una lista de los principales archivos de configuración usados en la configuración de la red. La comprensión del papel que desempeñan estos archivos en la configuración de la red puede ser de ayuda a la hora de personalizar un sistema Red Hat Enterprise Linux.

Los principales archivos de configuración de la red son los siguientes:

`/etc/hosts`
: El principal propóposito de este archivo es resolver los nombres de hosts que no pueden ser resueltos de otra manera. También se puede usar para resolver nombres de hosts en pequeñas redes sin servidor DNS. Sin tener en cuenta el tipo de red en que se encuentre el ordenador, este archivo debe contener un línea que especifica la dirección IP del dispositivo loopback (`127.0.0.1`) como por ejemplo `localhost.localdomain`. Para mayor información consulte la página man de `hosts`.

`/etc/resolv.conf`
: Este archivo especifica las direcciones IP de los servidores DNS y el dominio de búsqueda. A menos que se haya configurado para algo diferente, los scripts de inicialización de la red llenan este archivo. Para mayor información consulte la página man de `resolv.conf`.

`/etc/sysconfig/network-scripts/ifcfg-<nombre-de-interfaz>`
: Para cada interfaz de red existe un script de configuración de interfaz correspondiente. Cada uno de estos archivos proporciona información específica para una interfaz de red determinada. Consulte la Sección 2, “Archivos de configuración de interfaz” para obtener mayor información sobre este tipo de archivo y las directrices que acepta.

Aviso

La **Herramienta de administración de red** (`system-config-network`) utiliza el directorio `/etc/sysconfig/networking/`. Sus contenidos **no** deberían modificarse manualmente. Se recomienda utilizar solamente un método para la configuración de red debido al riesgo que se corre de borrar la configuración.

2. Archivos de configuración de interfaz

Los archivos de configuración de interfaz controlan las interfaces de software para dispositivos de red individuales. Cuando su sistema arranca, utiliza estos archivos para saber qué interfaces debe activar y cómo deben ser configuradas. Estos archivos habitualmente se conocen como `ifcfg-<nombre>`, donde `<nombre>` hace referencia al nombre del dispositivo que controla el archivo de configuración.

2.1. Interfaces Ethernet

Uno de los archivos de interfaz más comunes es `ifcfg-eth0`, que controla la primera *tarjeta de interfaz de red* Ethernet o *NIC* en el sistema. Un sistema con múltiples NICs tendrá varios archivos `ifcfg-eth<X>`, (donde `<X>` es un número único correspondiente a una interfaz específica). Como cada dispositivo tiene su propio archivo de configuración, un administrador podrá controlar la forma como cada interfaz funciona individualmente.

El siguiente es un ejemplo de un archivo `ifcfg-eth0` para un sistema que usa una dirección IP fija:

```
DEVICE=eth0 BOOTPROTO=none ONBOOT=yes NETWORK=10.0.1.0 NETMASK=255.255.255.0 IPADDR=10.0.1.27 USERCTL=no
```

Los valores requeridos en un archivo de configuración de interfaz pueden cambiar basándose en otros valores. Por ejemplo, el archivo `ifcfg-eth0` para una interfaz que use DHCP se verá bastante diferente ya que la información IP es proporcionada por el servidor DHCP:

```
DEVICE=eth0 BOOTPROTO=dhcp ONBOOT=yes
```

Sin embargo, también es posible modificar manualmente los archivos de configuración para una interfaz de red dada.

Abajo hay un listado de los parámetros configurables en un archivo de configuración de interfaz Ethernet.

`BOOTPROTO=<protocolo>`
: donde `<protocolo>` es uno de los siguientes:

- `none` — No se debería utilizar ningún protocolo de tiempo de arranque.
- `bootp` — Se debería utilizar el protocolo BOOTP.
- `dhcp` — Se debería utilizar el protocolo DHCP.

`BROADCAST=<dirección>`
: donde `<dirección>` es la dirección de difusión. Esta directriz ha sido descontinuada, pues el valor es calculado automáticamente con `ifcalc`.

`DEVICE=<nombre>`
: donde `<nombre>` es el nombre del dispositivo físico (a excepción de los dispositivos PPP asignados de forma dinámica en donde éste es el *nombre lógico*).

`DHCP_HOSTNAME`
: Solamente utilice esta opción si el servidor DHCP requiere que el cliente especifique un nombre de host antes de recibir una dirección IP.

`DNS{1,2}=<dirección>`
: donde `<dirección>` es la dirección del servidor de nombres que se tiene que colocar en `/etc/resolv.conf` si la directriz `PEERDNS` es `yes`.

`ETHTOOL_OPTS=<opciones>`
: donde `<opciones>` son cualquiera de las opciones específicas del dispositivo soportadas por `ethtool`. Por ejemplo, si desea forzar a 100Mb, full duplex:

```
ETHTOOL_OPTS="autoneg off speed 100 duplex full"
```

Nota

Tenga en cuenta que para cambiar la velocidad o las configuraciones de dúplex se necesita desactivar la negociación automática con la opción `autoneg off`. Es necesario iniciar esta opción primero, pues las entradas para las opciones dependen del orden.

`GATEWAY=<dirección>`
: donde `<dirección>` es la dirección IP del enrutador o dipositivo de puerta de enlace (si existe).

`HWADDR=<dirección-MAC>`
: donde `<dirección-MAC>` es la dirección de hardware del dispositivo Ethernet en la forma de `AA:BB:CC:DD:EE:FF`. Esta directriz es útil en las máquinas con múltiples NICs para asegurarse de que a las interfaces se les asignen los nombres correctos de dispositivos sin importar el orden de carga configurado para cada módulo NIC. Esta directriz **no** debería ser usada en conjunto con `MACADDR`.

`IPADDR=<dirección>`
: donde `<dirección>` es la dirección IP.

`MACADDR=<dirección-MAC>`
: donde `<dirección-MAC>` es la dirección de hardware del dispositivo Ethernet en la forma de `AA:BB:CC:DD:EE:FF`. Esta directriz es utilizada para asignar una dirección MAC a una interfaz, ignorando la asignada a la NIC física. Esta directriz *no* debería ser usada en conjunto con `HWADDR`.

`MASTER=<interfaz-vínculo>`
donde `<interfaz-vínculo>` es la interfaz de unión de canales a la cual la interfaz Ethernet está vinculada.

Esta directriz es usada en conjunto con la directriz `SLAVE`.

Consulte la Sección 2.3, “Interfaces de unión de canales” para obtener mayor información sobre las interfaces de unión de canales.

`NETMASK=<máscara>`
donde `<máscara>` es el valor de la máscara de red.

`NETWORK=<dirección>`
donde `<dirección>` es la dirección de red. Esta directriz ya no se usa, el valor es calculado automáticamente con `ifcalc`.

`ONBOOT=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — El dispositivo debería activarse en el momento de arranque.
- `no` — Este dispositivo no debería activarse en el momento de arranque.

`PEERDNS=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — Modifica `/etc/resolv.conf` si está activada la directriz DNS. Si está usando DCHP, la opción `yes` es la predeterminada.
- `no` — No modificar `/etc/resolv.conf`.

`SLAVE=<interfaz-vínculo>`
donde `<interfaz-vínculo>` es una de las siguientes:

- `yes` — Este dispositivo es controlado por la interfaz de unión de canales especificado en la directriz `MASTER`.
- `no` — Este dispositivo *no* es controlado por la interfaz de unión de canales especificada en la directriz `MASTER`.

Esta directriz es usada en conjunto con la directriz `MASTER`.

Consulte la Sección 2.3, “Interfaces de unión de canales” para obtener más detalles sobre las interfaces de unión de canales.

`SRCADDR=<dirección>`
donde `<dirección>` es la dirección IP de la fuente específica para los paquetes salientes.

`USERCTL=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — Los usuarios que no sean root pueden controlar este dispositivo.

- `no` — No se les permite controlar este dispositivo a los usuarios que no sean root.

2.2. Interfaces IPsec

El ejemplo siguiente muestra un archivo `ifcfg` para una conexión de red-a-red IPsec para la LAN A. El nombre único para identificar la conexión en este ejemplo es `ipsec1`, por lo que el archivo resultante se llama `/etc/sysconfig/network-scripts/ifcfg-ipsec1`.

```
TYPE=IPsec ONBOOT=yes IKE_METHOD=PSK SRCNET=192.168.1.0/24 DSTNET=192.168.2.0/24 DST=X.X.X.X
```

En el ejemplo anterior, *`X.X.X.X`* es la dirección IP enrutable públicamente del enrutador IPsec de destino.

A continuación se presenta un listado de los parámetros configurables para una interfaz IPsec:

`DST=<dirección>`
: donde `<dirección>` es la dirección IP del host o enrutador IPsec destino. Esto se utiliza tanto para configuraciones IPsec host-a-host como para configuraciones red-a-red.

`DSTNET=<red>`
: donde `<red>` es la dirección de red de la red IPsec destino. Esto solamente se utiliza para configuraciones de red-a-red IPsec.

`SRC=<dirección>`
: donde `<dirección>` es la dirección IP del enrutador o host fuente IPsec. Esta configuración es opcional y solamente es utilizada para las configuraciones IPsec host-a-host.

`SRCNET=<red>`
: donde `<red>` es la dirección de red de la red IPsec fuente. Esto solamente se utiliza para las configuraciones IPsec de red-a-red.

`TYPE=<tipo-interfaz>`
: donde `<tipo-interfaz>` es `IPSEC`. Ambas aplicaciones son parte del paquete `ipsec-tools`.

Si se utiliza la encriptación de llaves manual con IPsec, consulte `/usr/share/doc/initscripts-<número-versión>/sysconfig.txt` (reemplace `<número-versión>` con la versión del paquete `initscripts` instalado) para los parámetros de la configuración.

El demonio de manejo de llaves IKEv1 `racoon` negocia y configura un conjunto de parámetros para IPSec. Puede utilizar llaves previamente compartidas, firmas RSA o GSS-API. Si se utiliza `racoon` para manejar automáticamente la encriptación de llaves, se requieren las opciones siguientes:

`IKE_METHOD=<método-encriptación>`
: donde `<método-encriptación>` es, o bien `PSK`, `X509` o `GSSAPI`. Si se especifica `PSK`, también se debe configurar el parámetro `IKE_PSK`. Si se especifica `X509`, se debe especificar el parámetro `IKE_CERTFILE`.

`IKE_PSK=<llave-compartida>`
: donde `<llave-compartida>` es el valor secreto y compartido para el método PSK (llaves precompartidas).

`IKE_CERTFILE=<archivo-cert>`
donde `<archivo-cert>` es un archivo de certificado `X.509` válido para el host.

`IKE_PEER_CERTFILE=<archivo-cert>`
donde `<archivo-cert>` es un certificado `X.509` válido para el host *remoto*.

`IKE_DNSSEC=<respuesta>`
donde `<respuesta>` es `yes`. El demonio `racoon` recupera el certificado `X.509` del host remoto a través de DNS. Si se especifica `IKE_PEER_CERTFILE`, *no* incluya este parámetro.

Para más información sobre los algoritmos de encriptación disponibles para IPsec, consulte la página man de `setkey`. Para más información sobre `racoon`, consulte las páginas man de `racoon` y de `racoon.conf`.

2.3. Interfaces de unión de canales

Red Hat Enterprise Linux permite a los administradores vincular múltiples interfaces juntas en un canal único usando el módulo del kernel `bonding` y una interfaz de red especial llamada la *interfaz de unión de canales*. La unión de canales habilita a dos o más interfaces de red a actuar como una sola, incrementando simultáneamente el ancho de banda y proporcionando redundancia.

Para crear una interfaz de unión de canales, cree un archivo en el directorio `/etc/sysconfig/network-scripts/` llamado `ifcfg-bond<N>`, reemplazando `<N>` con el número para la interfaz, tal como `0`.

Los contenidos del archivo pueden ser idénticos al tipo de interfaz que se esté vinculando, tal como una interfaz Ethernet. La única diferencia es que la directriz `DEVICE=` debe ser `bond<N>`, reemplazando `<N>` con el número para la interfaz.

A continuación se muestra un ejemplo de un archivo de configuración de unión de canales:

```
DEVICE=bond0 BOOTPROTO=none ONBOOT=yes NETWORK=10.0.1.0 NETMASK=255.255.255.0 IPADDR=10.0.1.27 USERCTL=no
```

Después de crear la interfaz de unión de canales, las interfaces de red a ser unidas se deben configurar añadiendo las directrices `MASTER=` y `SLAVE=` a sus archivos de configuración. Los archivos de configuración para cada interfaz de unión de canales pueden ser casi idénticos.

Por ejemplo, si se tiene un canal uniendo dos interfaces Ethernet, ambas `eth0` y `eth1` pueden verse como en el ejemplo siguiente:

```
DEVICE=eth<N> BOOTPROTO=none ONBOOT=yes MASTER=bond0 SLAVE=yes USERCTL=no
```

En este ejemplo, reemplace `<N>` con el valor numérico para la interfaz.

Para que una interfaz de unión de canales sea válida, se debe cargar el módulo del kernel. Para asegurar que el módulo esté cargado cuando se suba la interfaz de unión, añada la línea siguiente a `/etc/modprobe.conf`:

```
alias bond<N> bonding
```

Reemplace `<N>` con el número de la interfaz, tal como `0`. Para cada interfaz de unión de canales ya configurada, debe haber una entrada correspondiente en `/etc/modprobe.conf`.

Una vez que `/etc/modprobe.conf` esté configurado — así como la interfaz de unión de canales y las interfaces de red— puede utilizar el comando `ifup` para activar la interfaz de unión de canales.

2.4. Archivos alias y clon

Dos tipos menos usados de archivos de configuración de interfaz son los archivos *alias* y *clon*.

Los archivos de configuración Alias, que se utilizan para enlazar direcciones múltiples a una sola interfaz, siguen este esquema de nombres `ifcfg-<nombre-if>:<valor-alias>`.

Por ejemplo, un archivo `ifcfg-eth0:0` podría estar configurado para especificar `DEVICE=eth0:0` y una dirección IP estática de 10.0.0.2, que sirva como un alias de una interfaz Ethernet que ya haya sido configurada para recibir la información IP a través de DHCP en `ifcfg-eth0`. Bajo esta configuración, el dispositivo `eth0` está ligado a una dirección IP dinámica, pero la misma tarjeta de red física puede recibir peticiones a través de la dirección fija 10.0.0.2.

Atención

Los alias de interfaces no soportan DHCP.

Un archivo de configuración de interfaz clon debería seguir la siguiente convención de nombres: `ifcfg-<nombre-if>-<nombre-clone>`. Mientras que un archivo alias permite múltiples direcciones para una interfaz existente, un archivo clon se usa para especificar opciones adicionales para una interfaz. Por ejemplo, una interfaz Ethernet DHCP estándar llamada `eth0`, se verá de una forma similar a:

```
DEVICE=eth0 ONBOOT=yes BOOTPROTO=dhcp
```

Puesto que el valor predeterminado para la directriz `USERCTL` es `no` si no está especificado, los usuarios no pueden activar y desactivar esta interfaz. Para que los usuarios gocen de esta habilidad, cree un clon copiando `ifcfg-eth0` a `ifcfg-eth0-user` y añada la línea siguiente a `ifcfg-eth0-user`:

```
USERCTL=yes
```

De esta forma un usuario puede activar la interfaz `eth0` mediante el comando `/sbin/ifup eth0-user`, porque las opciones de configuración desde `ifcfg-eth0` y `ifcfg-eth0-user` se usan conjuntamente. Aunque este ejemplo es muy sencillo, este método puede ser utilizado con una variedad de opciones e interfaces.

2.5. Interfaces de acceso telefónico

Si se conecta a una red, como Internet, a través de la conexión de acceso telefónico, necesitará un archivo de configuración para la interfaz.

Los archivos de interfaz PPP son nombrados utilizando el siguiente formato:

`ifcfg-ppp<X>`
En este ejemplo, reemplace `<X>` con el valor numérico para la interfaz.

El archivo de configuración de la interfaz PPP es creado automáticamente cuando se usa `wvdial`, la **Herramienta de administración de red** o **Kppp** para crear una cuenta de marcado telefónico. También es posible crear y modificar este archivo manualmente.

A continuación se presenta un archivo `ifcfg-ppp0` típico:

```
DEVICE=ppp0 NAME=test WVDIALSECT=test MODEMPORT=/dev/modem LINESPEED=115200 PAPNAME=test USERCTL=true ONBO
```

El *Protocolo SLIP (siglas en inglés de Serial Line Internet Protocol)* es otra interfaz de acceso telefónico menos usada. Los archivos SLIP tienen nombres de archivos de configuración de interfaz tales como `ifcfg-sl0`.

Otras opciones que se pueden utilizar en estos archivos incluyen:

`DEFROUTE=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — Establece esta interfaz como la ruta por defecto.
- `no` — No establece la interfaz como la ruta por defecto.

`DEMAND=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — Esta interfaz permitirá que `pppd` inicie una conexión cuando alguien está intentando utilizarla.
- `no` — Se debe establecer una conexión de forma manual para esta interfaz.

`IDLETIMEOUT=<valor>`
donde `<valor>` es el número de segundos de inactividad antes de que la interfaz se desconecte a sí misma.

`INITSTRING=<cadena>`
donde `<cadena>` es la cadena de inicialización que pasa al dispositivo del módem. Esta opción se usa principalmente en conjunto con las interfaces SLIP.

`LINESPEED=<valor>`
donde `<valor>` es la tasa de baudios del dispositivo. Los posibles valores estándar incluyen `57600`, `38400`, `19200` y `9600`.

`MODEMPORT=<dispositivo>`
donde `<dispositivo>` es el nombre del dispositivo serial que se usa para establecer la conexión para la interfaz.

`MTU=<valor>`
donde `<valor>` es la *unidad máxima de transferencia (MTU)* configurada para la interfaz. La MTU hace referencia al mayor número de bytes de datos que puede abarcar un bloque, sin

contar la información de encabezamiento. En algunas situaciones, la configuración de esta opción a un valor de `576` dará un resultado de pocos paquetes caídos y mejorará un poco el rendimiento para una conexión.

`NAME=<nombre>`
donde `<nombre>` es la referencia al título que se le da a un grupo de configuraciones de conexiones de acceso telefónico.

`PAPNAME=<nombre>`
donde `<nombre>` es el nombre de usuario dado durante el intercambio del *Protocolo de autenticación de contraseña (PAP)* que ocurre para permitir conectarse a un sistema remoto.

`PERSIST=<respuesta>`
donde `<respuesta>` es una de las siguientes:

- `yes` — Esta interfaz debería mantenerse siempre activa, incluso si se desactiva tras una desconexión del módem.
- `no` — Esta interfaz no debería mantenerse siempre activa.

`REMIP=<dirección>`
donde `<dirección>` es la dirección IP del sistema remoto. Generalmente no se especifica.

`WVDIALSECT=<nombre>`
donde `<nombre>` asocia esta interfaz con una configuración de marcado en `/etc/wvdial.conf`. Este archivo contiene el número de teléfono a marcar y otra información importante para la interfaz.

2.6. Otras interfaces

Los siguientes son otros archivos de configuración de interfaces comunes:

`ifcfg-lo`
A menudo se usa una *interfaz loopback* para realizar pruebas y con una variedad de aplicaciones que requieren una dirección IP que apunte al mismo sistema. Todos los datos que se mandan al dispositivo loopback vuelven inmediatamente a la capa de red del host.

Aviso

El script de la interfaz loopback `/etc/sysconfig/network-scripts/ifcfg-lo` nunca debe ser editado manualmente. Esto puede causar que el sistema deje de funcionar correctamente.

`ifcfg-irlan0`
Una *interfaz de infrarrojo* permite que se transmita información a través de un enlace infrarrojo entre dispositivos, tal como un portátil y una impresora. Esto funciona de forma similar a un dispositivo Ethernet excepto que se da comúnmente en una conexión punto a punto.

`ifcfg-plip0`

La conexión *Protocolo de interfaz de línea paralela (PLIP)* funciona casi de la misma manera que un dispositivo Ethernet, solamente que usa un puerto paralelo.

`ifcfg-tr0`
Las topologías *Token Ring* no son tan frecuentes en las *Redes de área local* (*LANs*), como lo eran antes, ya que Ethernet las ha opacado.

3. Scripts de control de interfaz

Los scripts de control de interfaz controlan la activación y desactivación de las interfaces del sistema. Existen dos scripts de control de la interfaz primaria que llaman a los scripts de control ubicados en el directorio `/etc/sysconfig/network-scripts`: `/sbin/ifdown` y `/sbin/ifup`.

Los scripts de interfaz `ifdown` y `ifup` son enlaces simbólicos a los scripts en el directorio `/sbin`. Cuando se solicita cualquiera de estos scripts se debe especificar el valor de la interfaz, como por ejemplo:

```
ifup eth0
```

Atención

Los scripts de interfaz `ifup` y `ifdown` son los únicos scripts que el usuario debe utilizar para subir y bajar las interfaces de red.

Los siguientes scripts son descritos como referencia únicamente.

Dos archivos utilizados para llevar a cabo una variedad de tareas de inicialización de la red durante el proceso de activación de una interfaz de red son `/etc/rc.d/init.d/functions` y `/etc/sysconfig/network-scripts/network-functions`. Consulte la Sección 4, “Archivos de funciones de red” para obtener mayor información.

Tras haber verificado que se ha especificado una interfaz y que al usuario que ha ejecutado la petición se le permite controlar la interfaz, el script correcto activa o desactiva la interfaz. Los siguientes scripts de control de interfaz son bastante comunes y se encuentran en el directorio `/etc/sysconfig/network-scripts/`:

`ifup-aliases`
Configura los alias IP desde los archivos de configuración de la interfaz cuando se asocia más de una dirección IP con una interfaz.

`ifup-ippp` y `ifdown-ippp`
Activa y desactiva una interfaz ISDN.

`ifup-ipsec` y `ifdown-ipsec`
Activa y desactiva una interfaz IPsec.

`ifup-ipv6` y `ifdown-ipv6`
Se usa para activar y desactivar una interfaz IPv6.

`ifup-ipx`
Activa y desactiva una interfaz IPX.

`ifup-plip`
Activa y desactiva una interfaz PLIP.

`ifup-plusb`
Activa y desactiva una interfaz USB para conexiones de red.

`ifup-post` y `ifdown-post`
Contiene comandos que son ejecutados después de que una interfaz ha sido activada o desactivada.

`ifup-ppp` y `ifdown-ppp`
Activa o desactiva una interfaz PPP.

`ifup-routes`
Añade rutas estáticas para un dispositivo como si se activase su interfaz.

`ifdown-sit` y `ifup-sit`
Contiene llamadas de funciones relacionadas con la activación y desactivación de un túnel IPv6 dentro de una conexión IPv4.

`ifup-sl` y `ifdown-sl`
Activa o desactiva una interfaz SLIP.

`ifup-wireless`
Activa una interfaz inalámbrica.

Aviso

Tenga en cuenta que si elimina o modifica cualquier script en el directorio `/etc/sysconfig/network-scripts/` puede provocar que las conexiones de interfaz funcionen de forma extraña o incluso fallen. Solo los usuarios avanzados deberían modificar los scripts relacionados con una interfaz de red.

La forma más fácil de manipular todos los scripts de red simultáneamente es con el comando `/sbin/service` en el servicio de red (`/etc/rc.d/init.d/network`), como se ilustra en el comando siguiente:

```
/sbin/service network <acción>
```

En este ejemplo `<acción>` puede ser `start`, `stop` o `restart`.

Para ver una lista de los dispositivos configurados y las interfaces de red actualmente activas, utilice el comando:

```
/sbin/service network status
```

4. Archivos de funciones de red

Red Hat Enterprise Linux utiliza varios archivos que contienen funciones importantes que se usan para activar o desactivar interfaces. En vez de forzar cada archivo de control de interfaz para que contenga estas funciones, éstas están agrupadas convenientemente en algunos archivos que se pueden llamar cuando sea necesario.

El archivo `/etc/sysconfig/network-scripts/network-functions` contiene las funciones IPv4 más comunes que son útiles para muchos scripts de control de interfaz. Estas funciones incluyen: contactar con programas en ejecución que han solicitado información sobre cambios en el estado de una interfaz, configurar los nombres del host, encontrar dispositivos de puerta de enlace, ver si un dispositivo en particular está o no activado y añadir una ruta por defecto.

Debido a que las funciones solicitadas por las interfaces IPv6 son diferentes de las interfaces IPv4, existe específicamente un archivo `/etc/sysconfig/network-scripts/network-functions-ipv6` para guardar esta información. Las funciones en este archivo configuran y borran las rutas IPv6 estáticas, crean y borran túneles, añaden y eliminan direcciones IPv6 para una interfaz y comprueban la existencia de una dirección IPv6 en una interfaz.

5. Recursos adicionales

Los siguientes son recursos que explican más detalladamente las interfaces de red.

5.1. Documentación instalada

`/usr/share/doc/initscripts-<versión>/sysconfig.txt`
: Un manual que estudia las opciones disponibles para los archivos de configuración de red, incluidas las opciones IPv6 que no son cubiertas en este capítulo.

`/usr/share/doc/iproute-<versión>/ip-cref.ps`
: Este archivo contiene mucha información sobre el comando `ip`, que se usa, entre otras cosas, para manipular las tablas de enrutamiento. Use la aplicación **ggv** o **kghostview** para ver este archivo.

Capítulo 2. 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, módem RDSI o token ring) y a que estas interfaces de red están configuradas para conectarse a la red.

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

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

También se puede usar para configurar conexiones IPsec, administrar configuraciones de DNS y manejar el archivo `/etc/hosts` para almacenar nombres de host adicionales y combinaciones de direcciones IP.

Para usar la **Herramienta de administración de red**, debe tener privilegios de usuario root. Para arrancar la aplicación, vaya a Applications (the main menu on the panel) => **Configuración del sistema** => **Red**, o escriba el comando `system-config-network` en el intérprete de comandos (por ejemplo, en un **XTerm** o en un terminal **GNOME terminal**). Si escribe el comando mientras ejecuta X, la versión gráfica es desplegada, de lo contrario se inicia la versión basada en texto.

Para usar la versión de línea de comandos, ejecute el comando `system-config-network-cmd --help` como usuario root para ver todas las opciones disponibles.

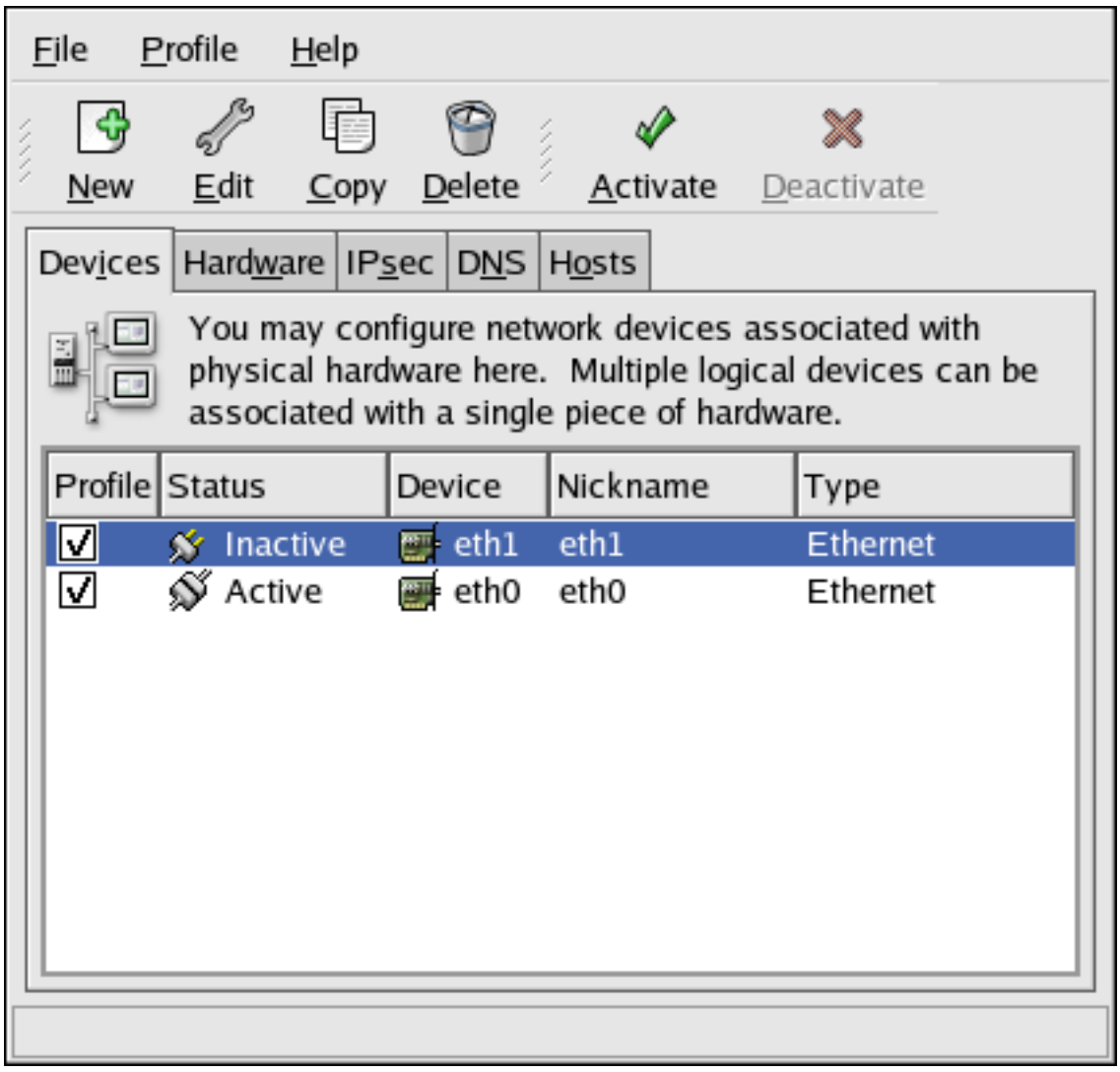


Figura 2.1. Herramienta de administración de red

Sugerencia

Consulte la lista de compatibilidad de hardware de Red Hat (http://hardware.redhat.com/hcl/) para ver si Red Hat Enterprise Linux soporta su dispositivo de hardware.

1. Resumen

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

1. Añada dispositivos de red asociados al hardware anterior.

2. Añada el dispositivo de hardware a la lista del hardware si aún no existe.
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.

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** en la barra de herramientas.
3. Seleccione **Conexión Ethernet** en la lista **Tipo de dispositivo** y haga click en **Adelante**.
4. Si ya ha añadido el dispositivo de red a la lista de hardware, selecciónelo de la lista **Dispositivo**. De lo contrario, 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, éstos 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. Luego 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 red** también le permite configurar los recursos para NIC. Haga clic en **Adelante** para continuar.
6. En la pantalla **Configuración de parámetros de red** como se muestra en la Figura 2.2, “Parámetros de Ethernet”, 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 **Adelante** para continuar.
7. Haga click en **Aplicar** en la página **Crear dispositivo Ethernet**.

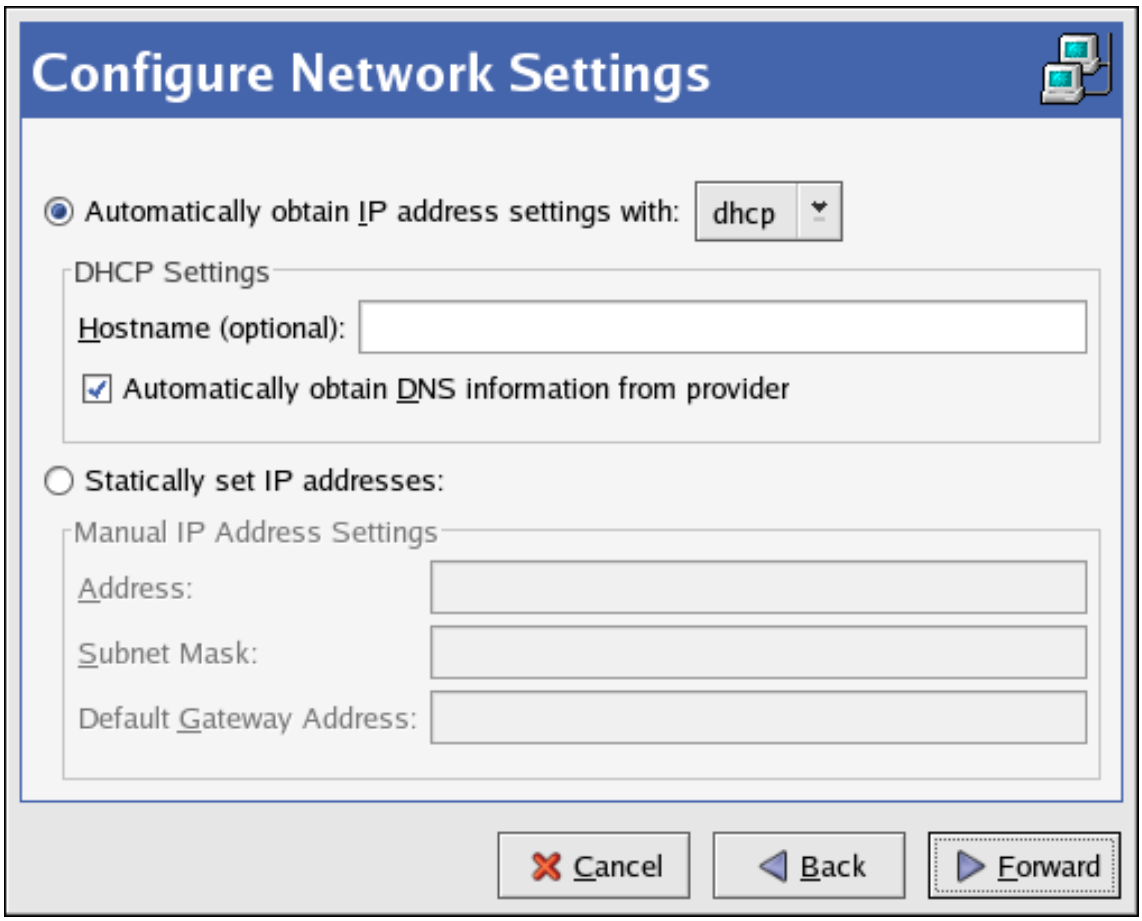


Figura 2.2. Parámetros de Ethernet

Después de haber configurado el dispositivo Ethernet, éste aparece en la lista de los dispositivos como se muestra en la Figura 2.3, “Dispositivo Ethernet”.

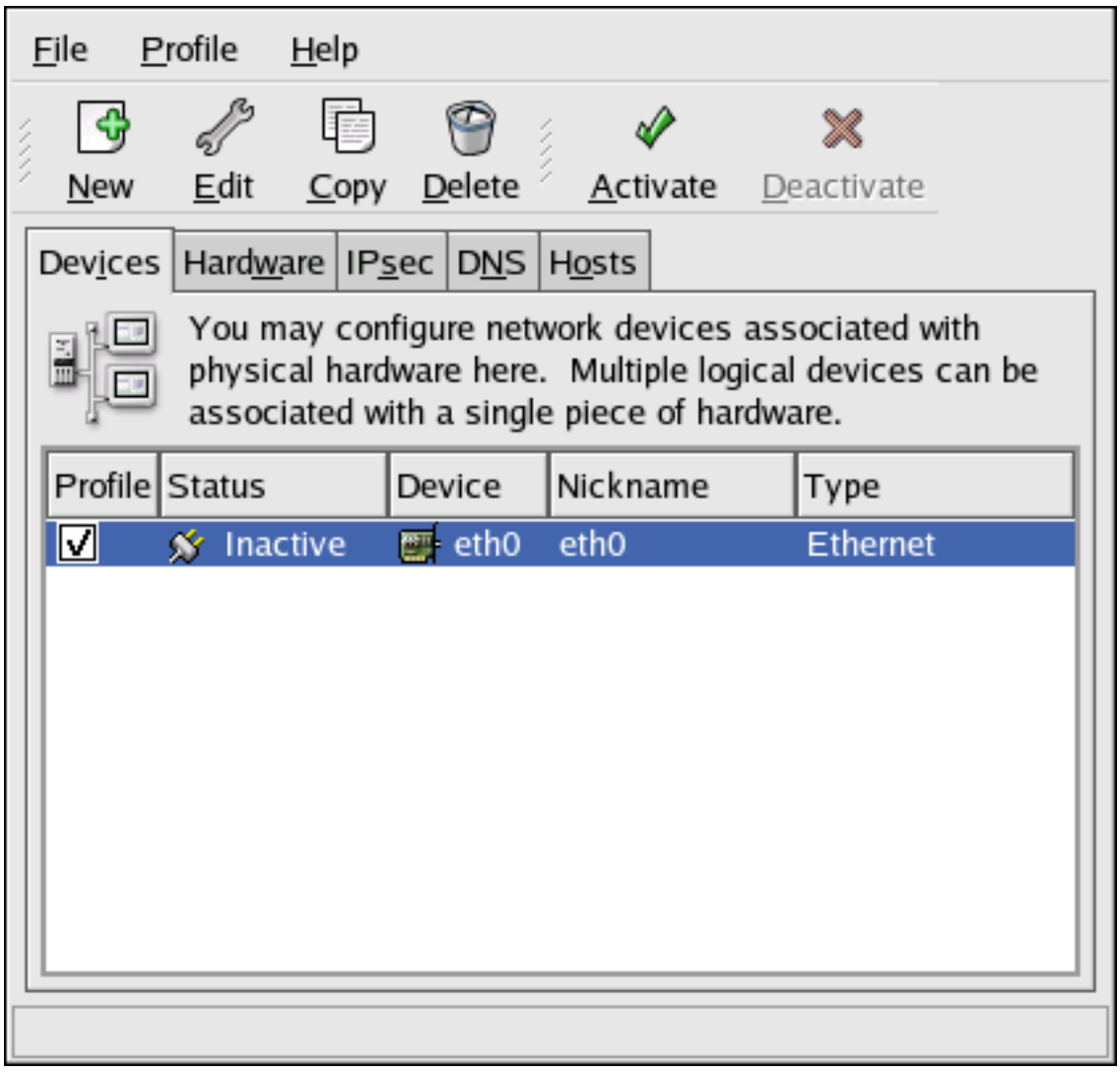


Figura 2.3. Dispositivo Ethernet

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 dándole así más de una dirección IP. Por ejemplo, puede configurar un dispositivo eth1 y un dispositivo eth1:1. Para obtener mayor información consulte la Sec-

ción 11, “Alias de dispositivo”.

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 **Adelante**.
4. Seleccione el adaptador RDSI del menú desplegable. Después configure los recursos y el protocolo del canal D para el adaptador. Haga click en **Adelante** para continuar.

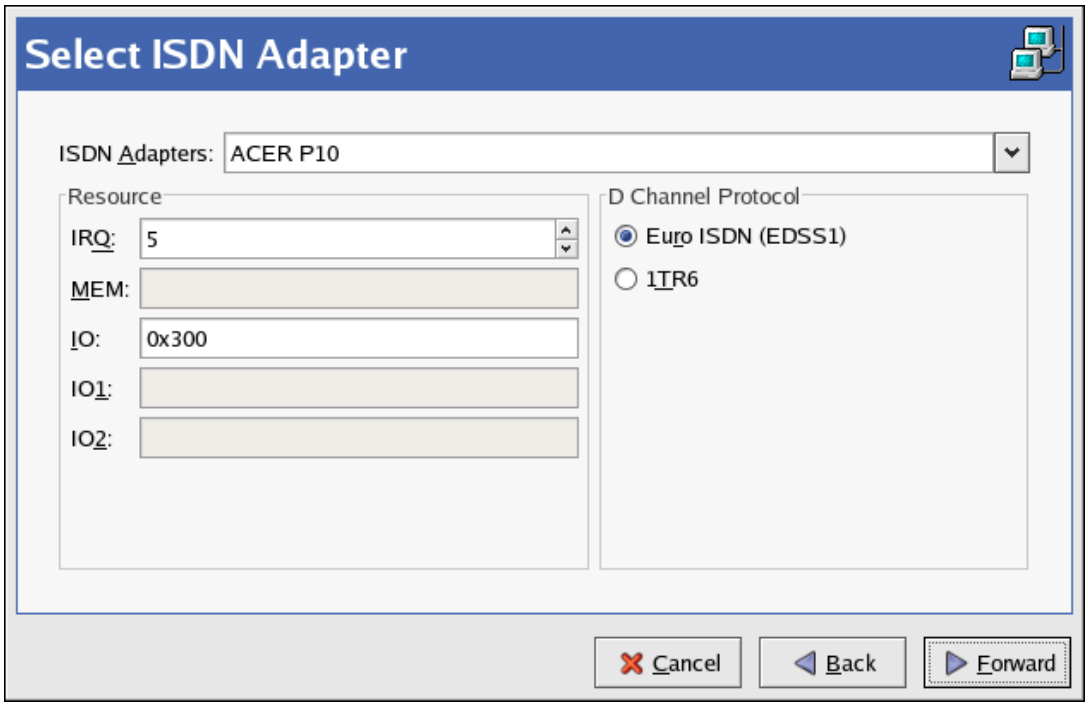


Figura 2.4. Parámetros RDSI

5. Si su proveedor ISP (siglas en inglés de Internet Service Provider) está en la lista de las cuentas preconfiguradas, selecciónela. De lo contrario, introduzca la información necesaria sobre la cuenta ISP. Si no sabe los valores, contacte a su ISP. Haga click en **Adelante**.
6. En la ventana **Configuraciones IP**, seleccione **Modo de encapsulación** y si se debe obtener una dirección IP o si se debe configurar una estáticamente. Haga clic en **Adelante** al finalizar.

7. En la pantalla **Crear conexión telefónica** haga clic en **Aplicar**.

Después de configurar el dispositivo RDSI, éste aparece en la lista de los dispositivos como un dispositivo de tipo **RDSI** como se muestra en la Figura 2.5, “Dispositivo RDSI”.

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 clic en **Modificar**. Por ejemplo, cuando el dispositivo se añade, se configura para que no inicie en el tiempo de arranque predeterminado. Modifique la configuración cambiando 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.

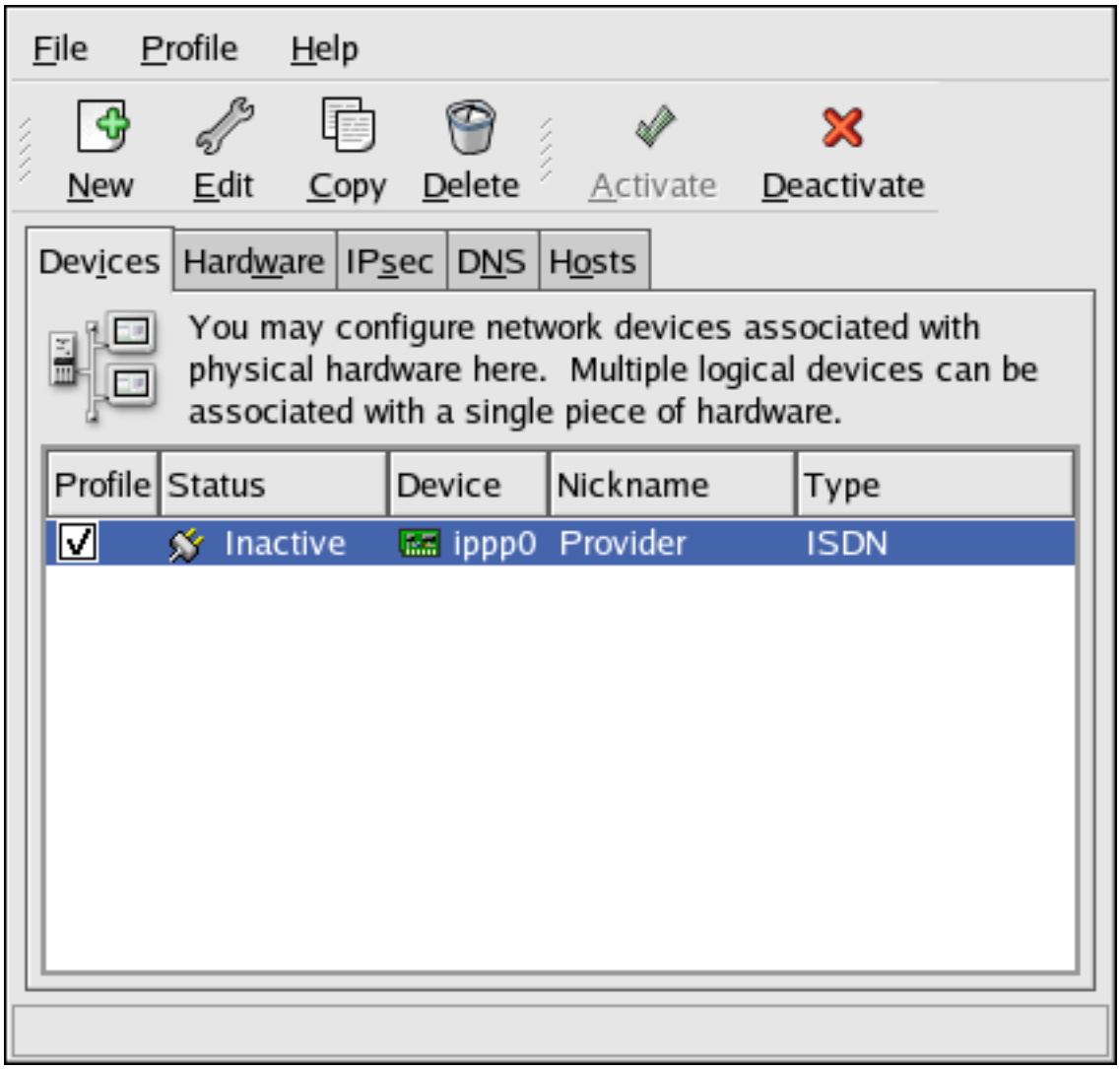


Figura 2.5. Dispositivo RDSI

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 del módem** en **Tipo de dispositivo** y haga click en **Adelante**.
4. Si ya tiene un módem configurado y aparece en la lista de hardware (en la pestaña **Hardware**), la **Herramienta de administración de red** 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 advertirle de que las configuraciones mostradas no son valores encontrados en la prueba.
5. Después de verificar, aparecerá la Figura 2.6, “Propiedades del módem”.

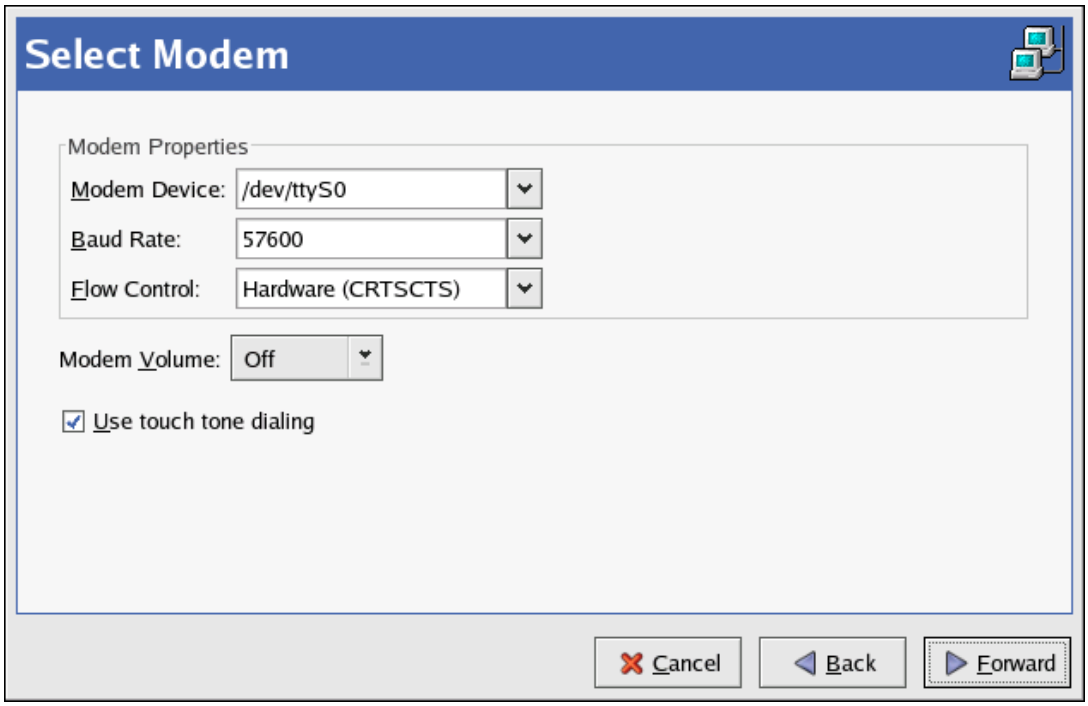


Figura 2.6. Propiedades del módem

6. Configure el dispositivo módem, velocidad 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 **Adelante**.
7. Si su ISP aparece en la lista de las cuentas predeterminadas, selecciónela; sino, introduz-

ca la información de la cuenta ISP. Si no conoce los valores, contacte con su ISP. Haga click en **Adelante**.

8. En la página **Configuración IP**, seleccione si desea obtener una dirección IP automáticamente o si la desea configurar de forma estática. Haga clic en **Adelante** cuando termine.

9. En la pantalla **Crear conexión telefónica** haga clic en **Aplicar**.

Después de haber configurado el módem, éste aparece en la lista de los dispositivos con el tipo `Modem` como se muestra en la Figura 2.7, “Dispositivo del módem”.

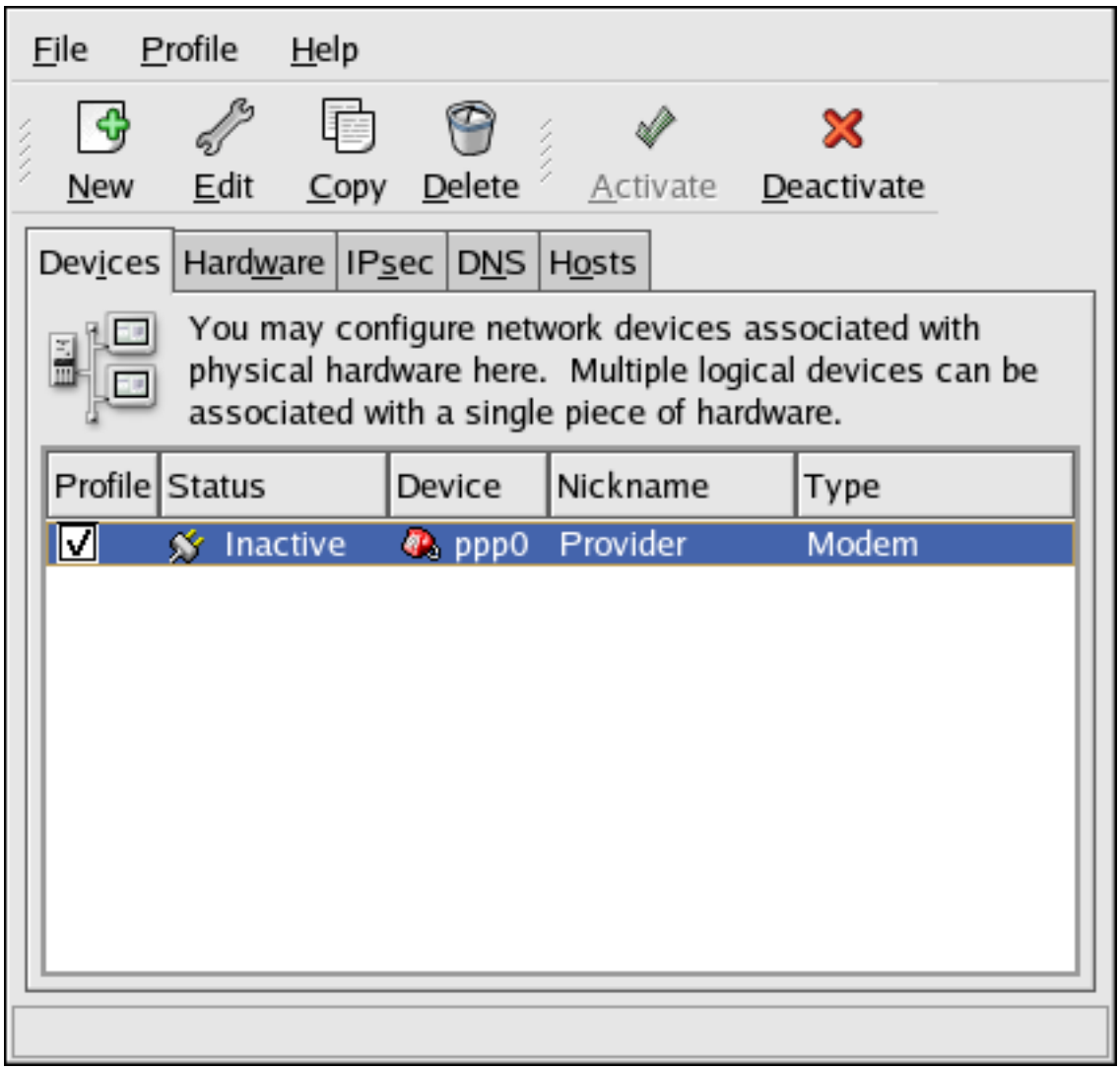


Figura 2.7. Dispositivo del módem

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 cambiar 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.

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 red** usa el término xDSL para incluir todos los tipos de conexiones 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 2, “Conexión Ethernet” 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 **Tipo de dispositivo** y haga click en **Adelante**.
4. Si su tarjeta Ethernet está en la lista de hardware, seleccione el **Dispositivo Ethernet** desde el menú desplegable desde la página mostrada en la Figura 2.8, “Parámetros xDSL”. De lo contrario, aparecerá la ventana **Seleccionar adaptador 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, éstos aparecerán en la lista de hardware en la pestaña **Hardware**.

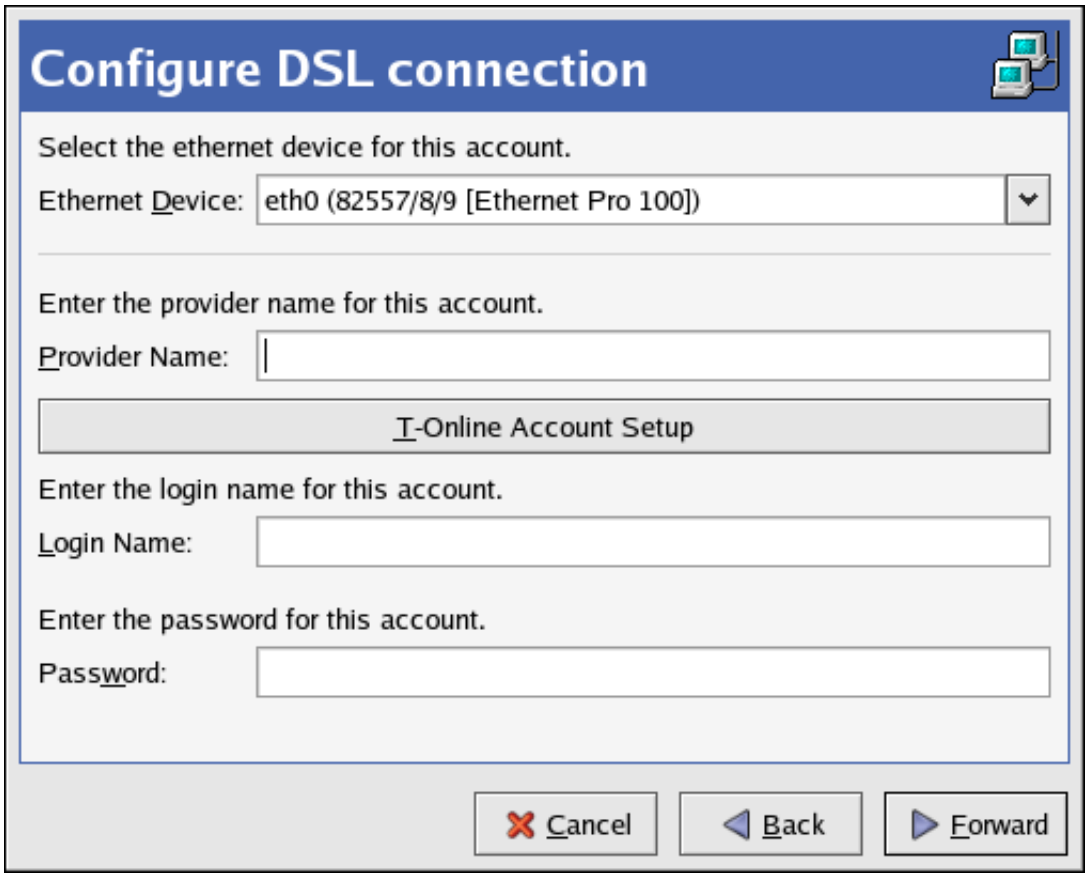


Figura 2.8. Parámetros xDSL

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 red** también le permite configurar los recursos para la NIC. Presione **Adelante** 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 **Adelante** para continuar.

7. En la pantalla **Crear una conexión DSL** haga click en **Aplicar**.

Después de haber configurado la conexión DSL, esta aparece en la lista de los dispositivos como se muestra en la Figura 2.7, “Dispositivo del módem”.

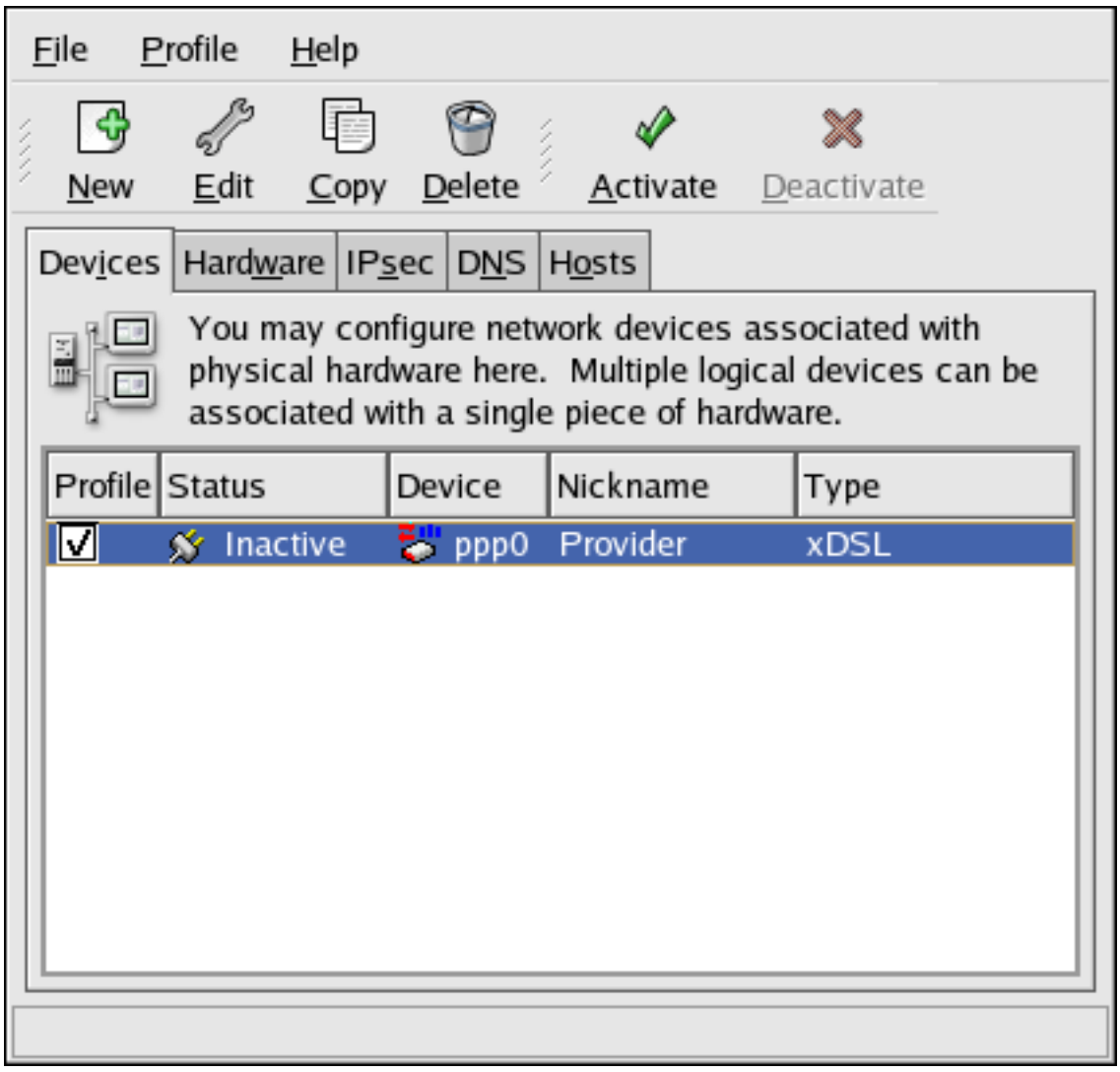


Figura 2.9. Dispositivo xDSL

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 cambiando 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.

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 orde-

nadores 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 **Tipo de dispositivo** y haga click en **Adelante**.
4. Si ya tiene una tarjeta token ring configurada en la lista del hardware, selecciónela de la lista **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 2.10, “Parámetros Token Ring”. 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 red** también permite que el usuario pueda configurar los recursos para el adaptador. Haga clic en **Adelante** para continuar.

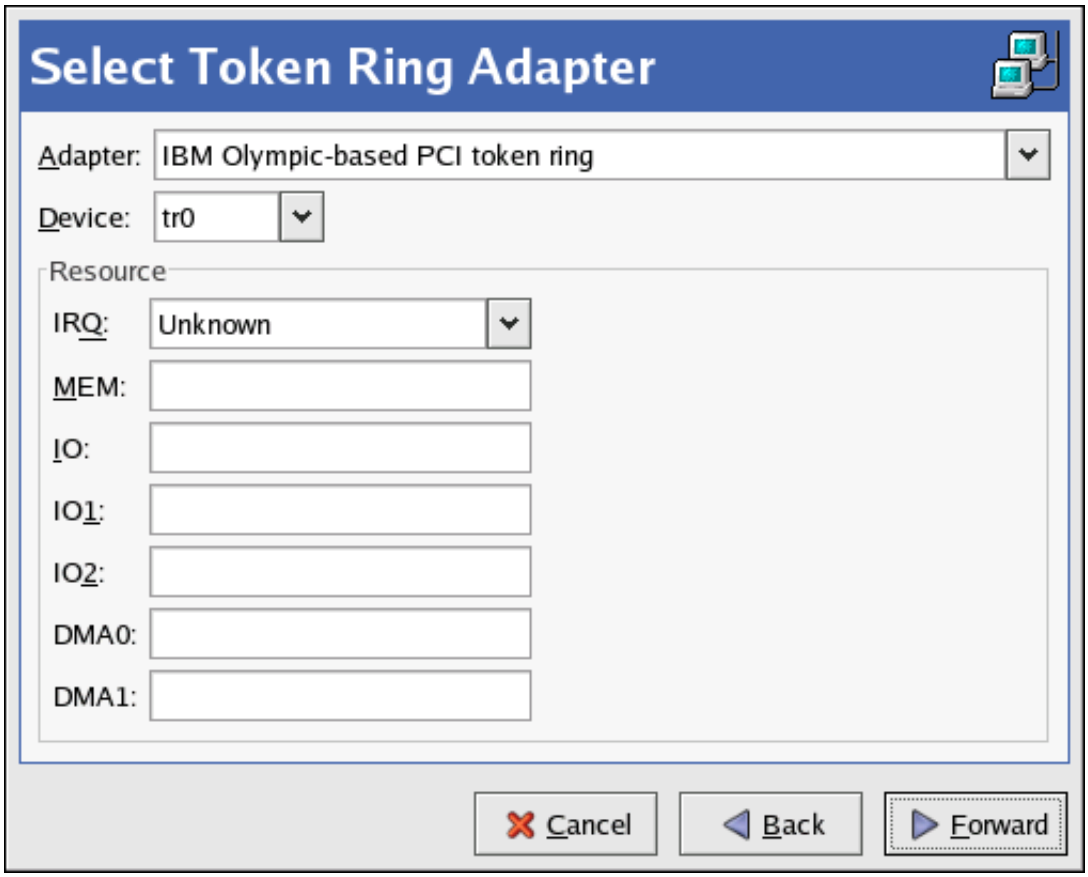


Figura 2.10. Parámetros Token Ring

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 **Adelante** para continuar.

7. Haga click en **Aplicar** en la página **Crear dispositivo Token ring**.

Después de configurar el dispositivo token ring, éste aparece en la lista de los dispositivos como se muestra en la Figura 2.11, “Dispositivo Token Ring”.

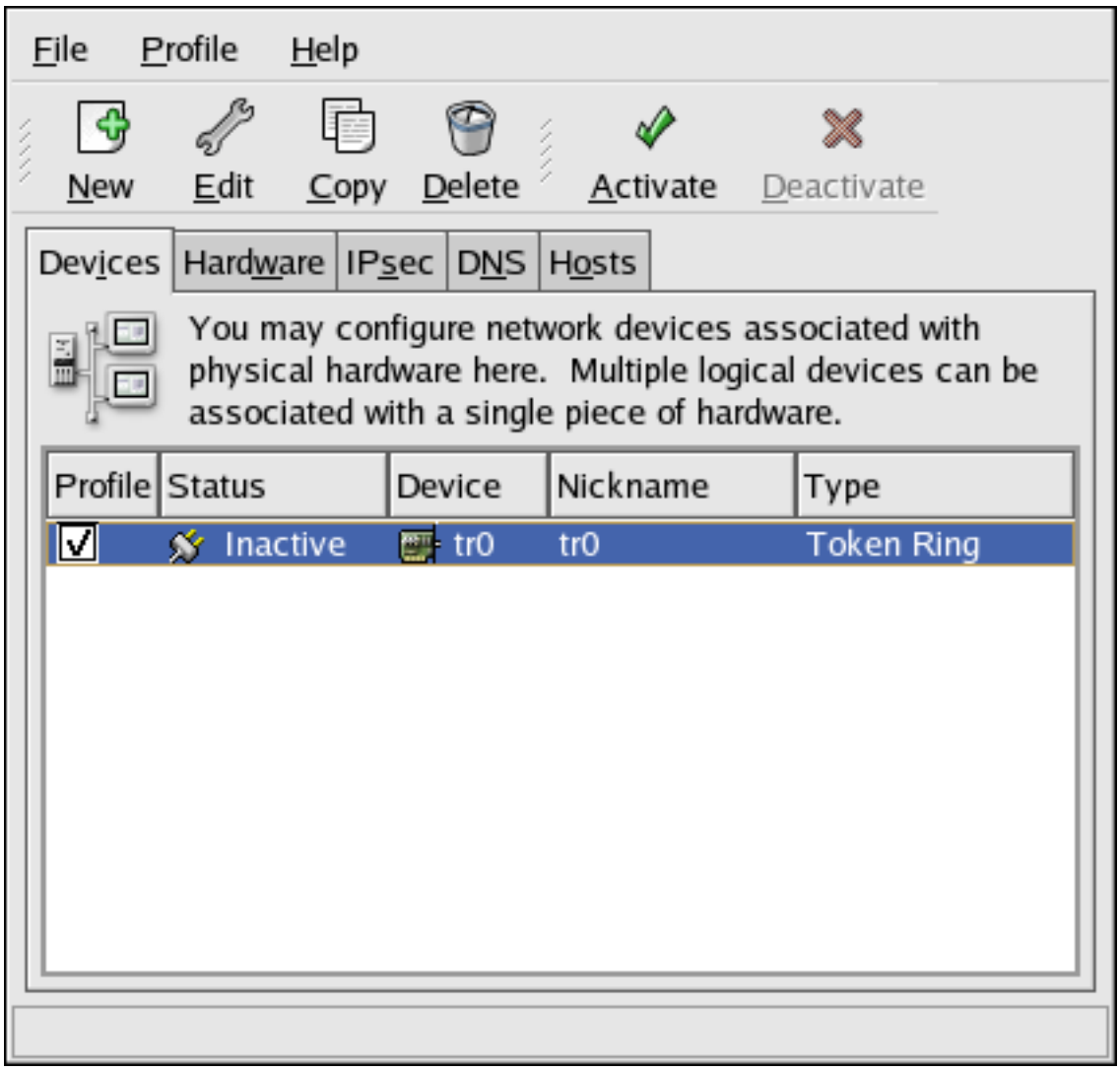


Figura 2.11. Dispositivo Token Ring

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.

7. 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 el botón **Añadir** en la barra de herramientas.
3. Seleccione **Conexión inalámbrica** desde la lista **Tipo de dispositivo** y haga clic en **Adelante**.
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 red** también permite al usuario configurar los recursos para el dispositivo de red inalámbrico. Haga click en **Adelante** para continuar.
6. En la página **Configurar conexión inalámbrica** como se muestra en la Figura 2.12, “Parámetros de la conexión inalámbrica”, configure las propiedades para el dispositivo inalámbrico.

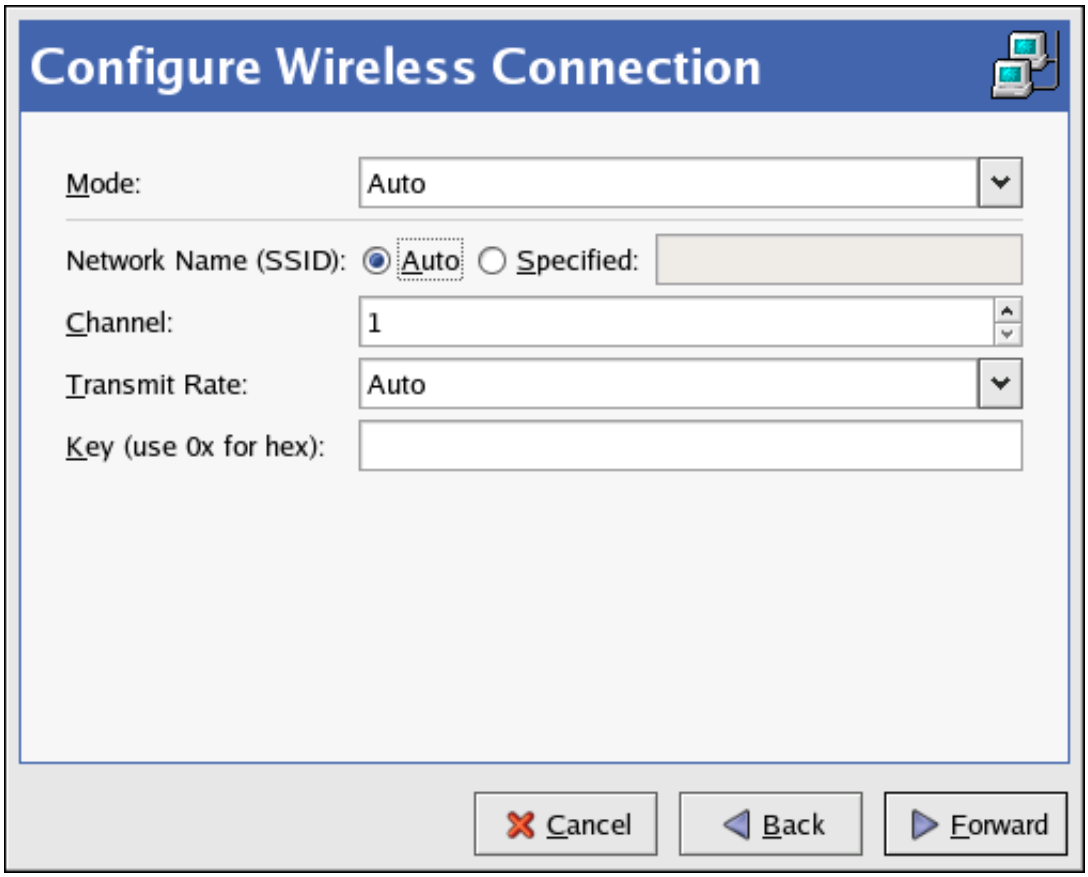


Figura 2.12. Parámetros de la conexión inalámbrica

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 **Adelante** para continuar.

8. Haga click en **Aplicar** en la pantalla **Crear dispositivo inalámbrico**.

Después de configurar el dispositivo inalámbrico, aparecerá en la lista de dispositivos como se muestra en la Figura 2.13, “Dispositivo inalámbrico”.

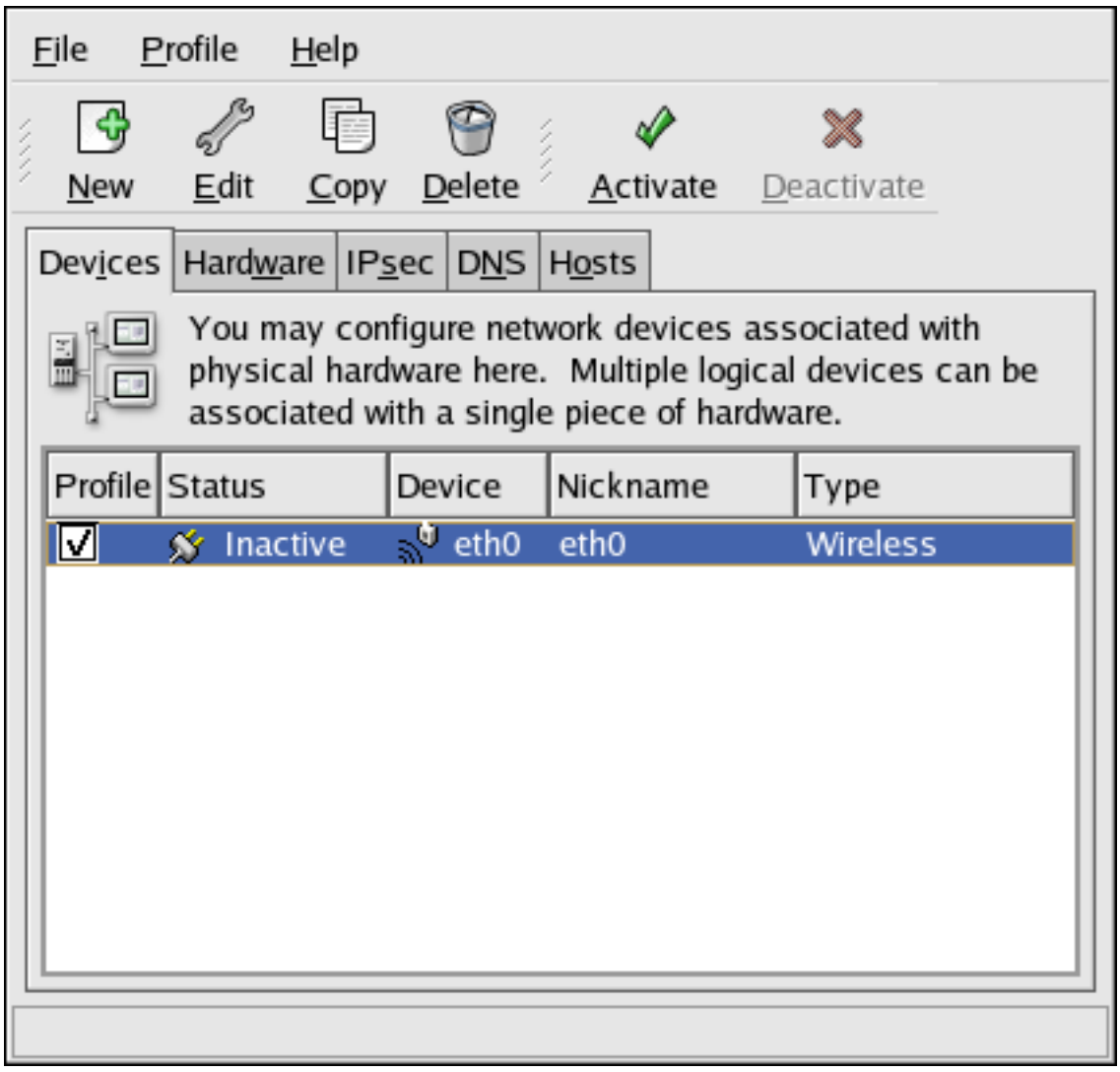


Figura 2.13. Dispositivo inalámbrico

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.

8. Administración de los parámetros DNS

La pestaña **DNS** le permite configurar el nombre host del sistema, el dominio, los servidores de nombres y el dominio de búsqueda. 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.

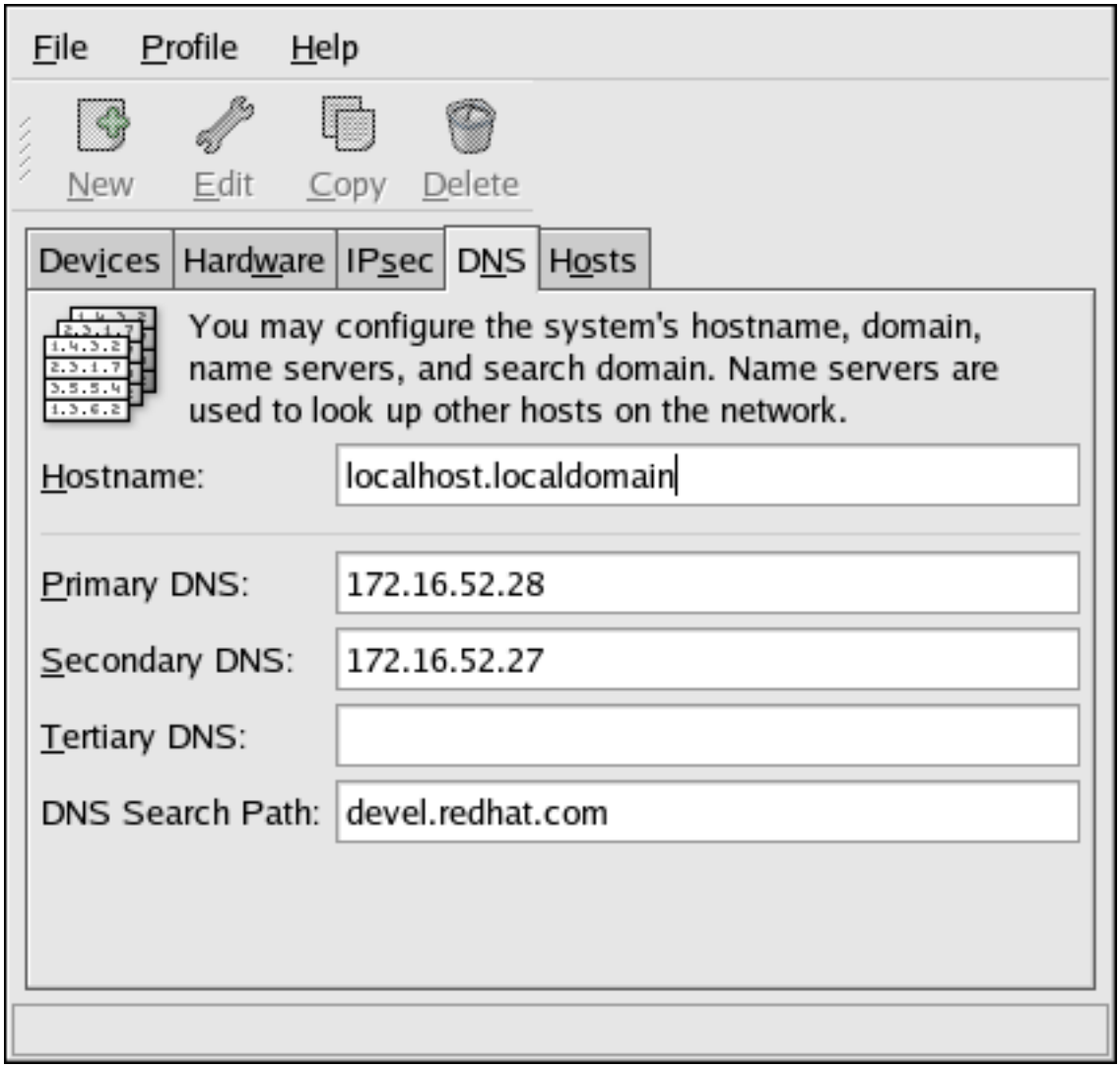


Figura 2.14. Configuración DNS

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.

Aviso

Si el nombre de host ha cambiado y `system-config-network` es iniciado en el host local, otra aplicación **X11** podría no poder ser iniciada. Para ello, usted tendría que iniciar una nueva sesión de escritorio.

9. 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 a una dirección IP, o de determinar el nombre de host para una dirección IP, hará referencia al archivo `/etc/hosts` antes de usar los servidores de nombres (si usa la configuración por defecto de Red Hat Enterprise 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 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.

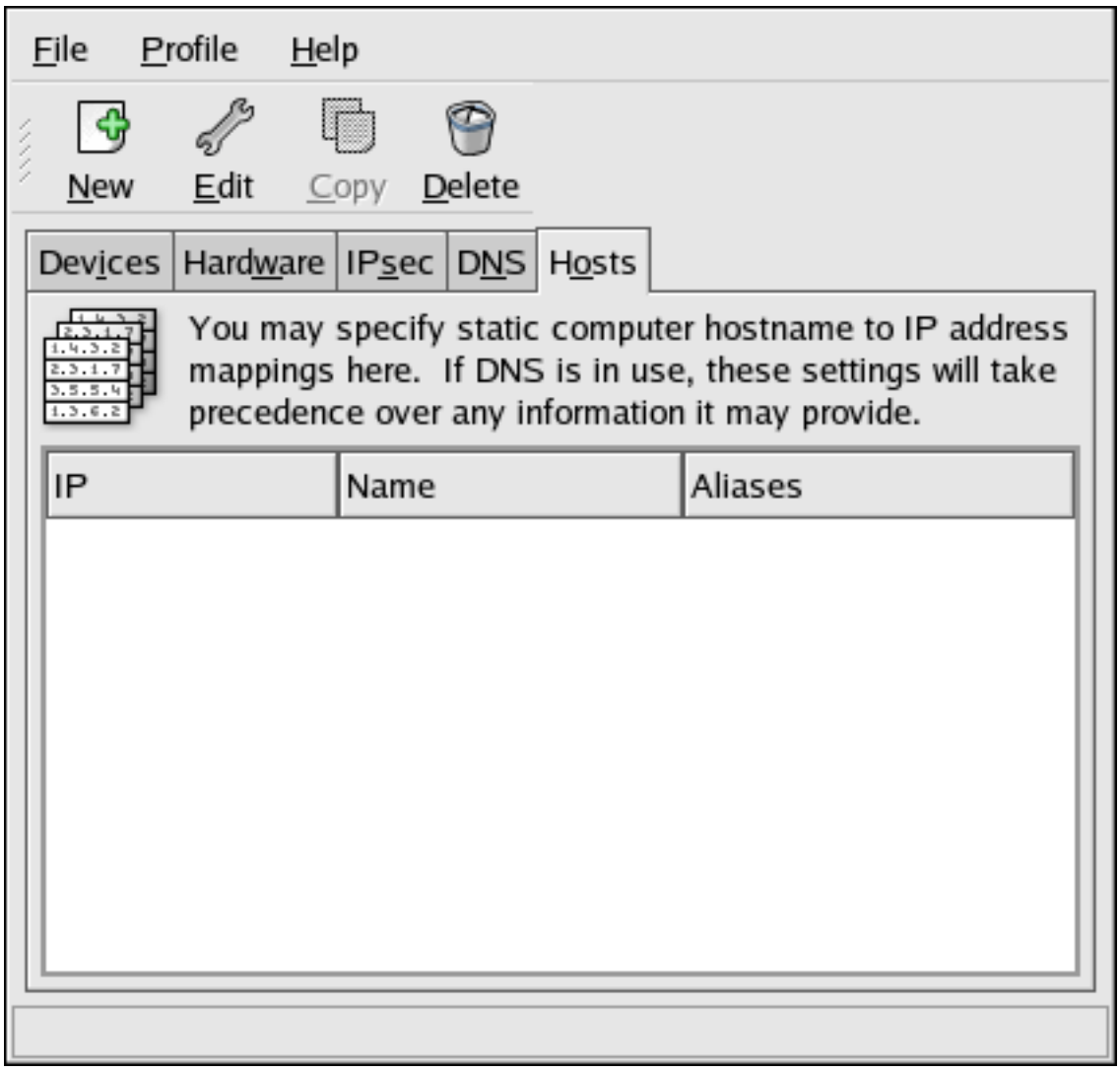


Figura 2.15. Configuración de los hosts

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`.

10. Funcionamiento con perfiles

Muchos dispositivos lógicos de red pueden ser creados para cada dispositivo de hardware físi-

co. 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 ellos 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. Consulte la Sección 11, “Alias de dispositivo” para obtener 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 red** 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 seleccionar o deseleccionar los dispositivos. Tan sólo los dispositivos seleccionados 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 2.16, “Perfil Office” le muestra un perfil llamado **Office** con el dispositivo lógico **eth0_office**. Está configurado para activar la primera tarjeta Ethernet usando DHCP.

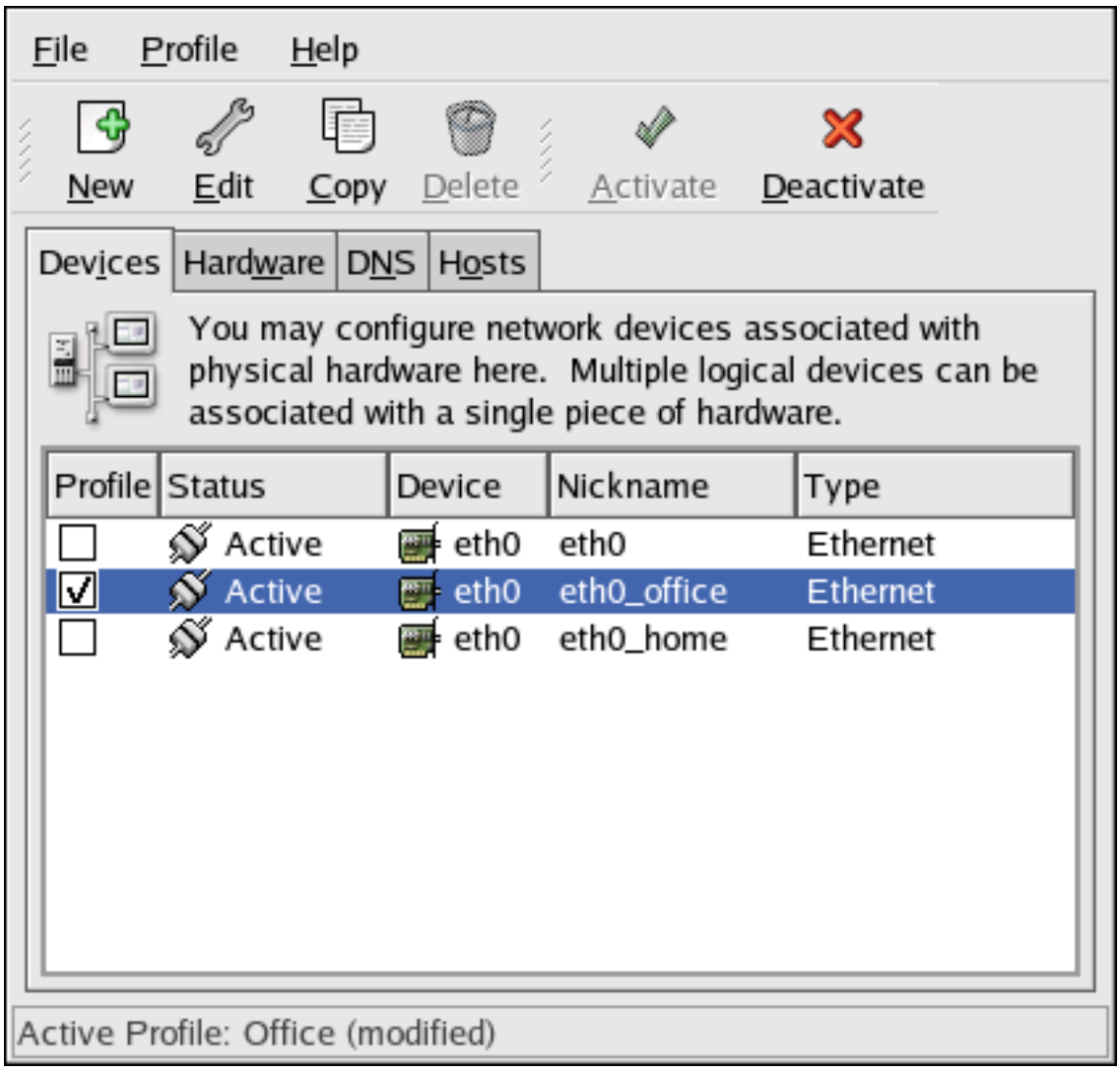


Figura 2.16. Perfil Office

Observe que el perfil **Home** como se muestra en la Figura 2.17, “Home Profile” activa el dispositivo lógico **eth0_home**, el cual está asociado con `eth0`.

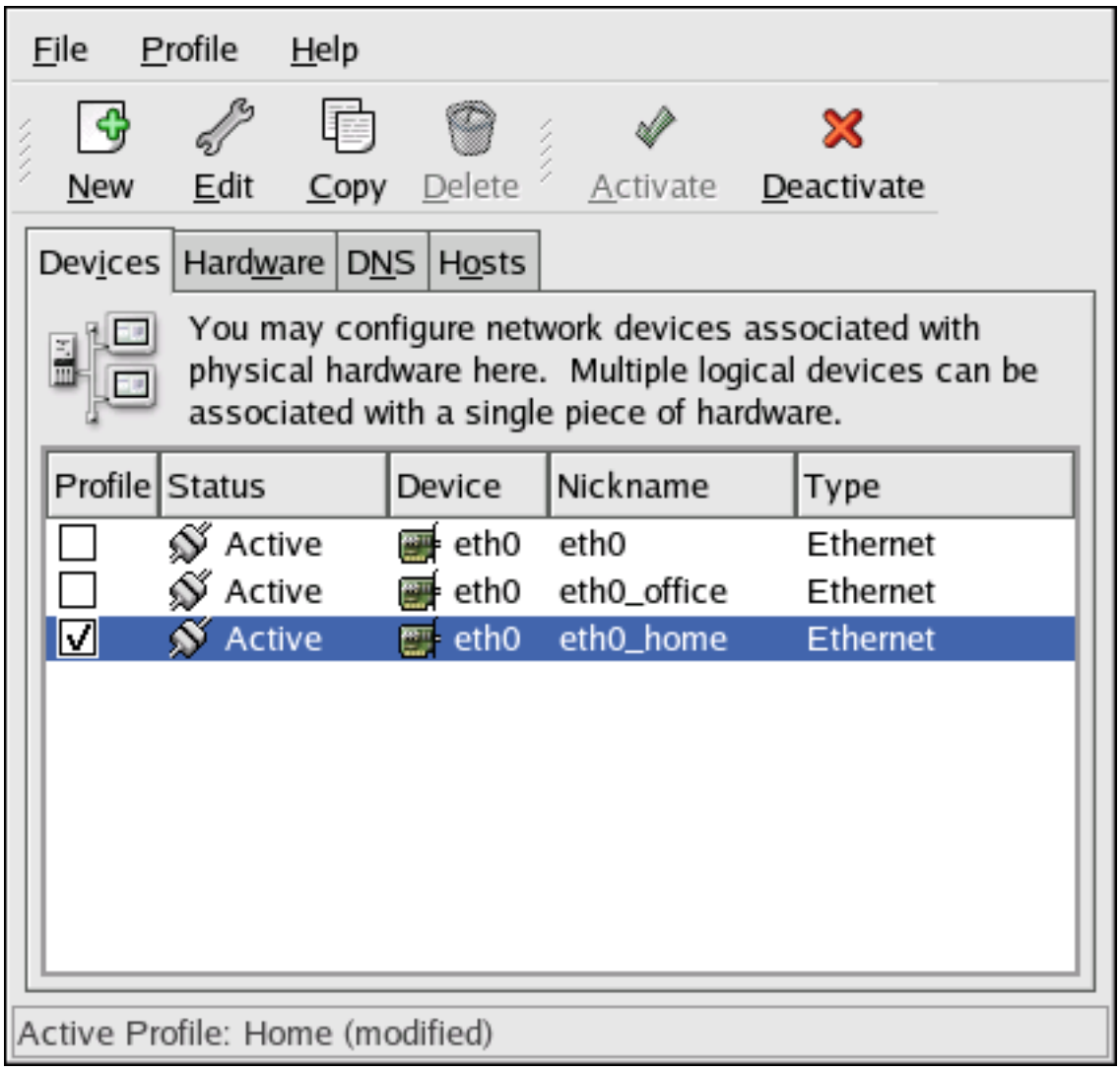


Figura 2.17. Home Profile

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.

Para activar un perfil al momento del arranque, modifique el archivo de configuración del gestor de arranque para incluir la opción `netprofile=<nombre-perfil>`. Por ejemplo, si el sistema utiliza GRUB como gestor de arranque y `/boot/grub/grub.conf` contiene:

```
title Red Hat Enterprise Linux (2.6.9-5.EL) root (hd0,0) kernel /vmlinuz-2.6.9-5.EL ro root=/dev/VolGroup0
```

Modifíquelo a lo siguiente (donde `<nombre-perfil>` es el nombre del perfil a ser activado durante el arranque):

```
title Red Hat Enterprise Linux (2.6.9-5.EL) root (hd0,0) kernel /vmlinuz-2.6.9-5.EL ro root=/dev/VolGroup0
```

Para cambiar perfiles después de iniciado el sistema, vaya al Applications (the main menu on

the panel) => **Herramientas de sistema** => **Control del dispositivo de red** (o escriba el comando `system-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 **Común**.

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

```
system-config-network-cmd --profile <nombre-perfil> --activate
```

11. 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 generalmente representados 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 que tan sólo tiene 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.

Figura 2.18, “Ejemplo de alias del dispositivo de red” 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 la activación de éste durante el arranque y el número de alias, selecciónelo de la lista y haga click en el botón **Modificar**.

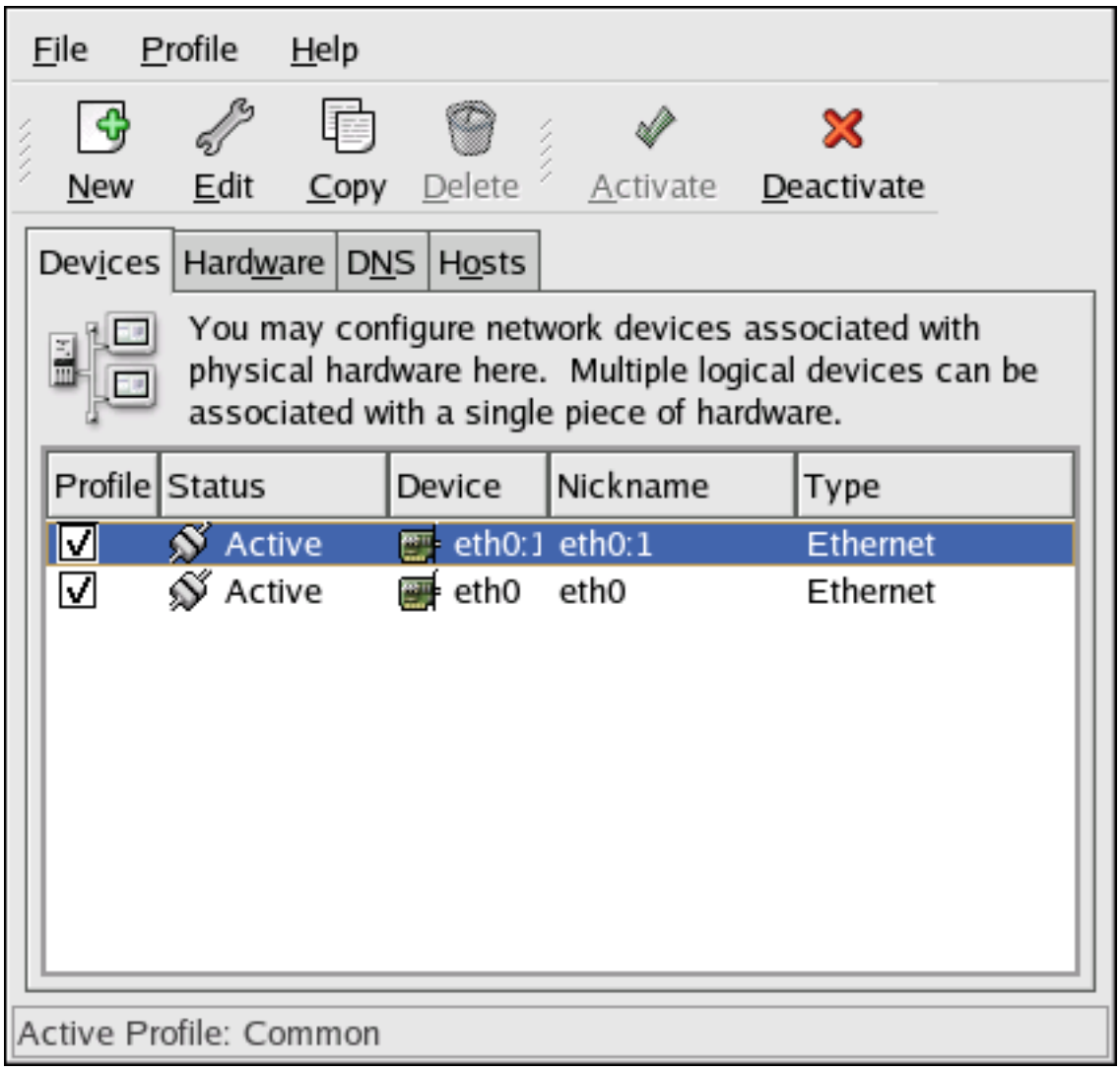


Figura 2.18. Ejemplo de alias del dispositivo de red

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:255.25
```

12. Guardar y recuperar la configuración de la red

La versión de línea de comandos de la **Herramienta de administración de red** puede ser utilizada para guardar la configuración de la red del sistema a un archivo. Este archivo se puede utilizar porteriormente para restaurar la configuración de la red a un sistema Red Hat Enterprise Linux.

Esta funcionalidad se puede usar como parte de un script de respaldo automático, para guardar la configuración antes de actualizar o reinstalar, o para copiar la configuración a un sistema Red Hat Enterprise Linux diferente.

Para guardar o *exportar* la configuración del sistema a un archivo `/tmp/network-config`, ejecute el comando siguiente como root:

```
system-config-network-cmd -e > /tmp/network-config
```

Para restaurar o *importar* la configuración de la red desde un archivo creado desde el comando anterior, ejecute el comando siguiente como root:

```
system-config-network-cmd -i -c -f /tmp/network-config
```

La opción `-i` significa importar datos, la opción `-c` significa limpiar la configuración existente antes de importar y la opción `-f` especifica que el archivo a importar es como el dado después de la opción.

Capítulo 3. Control de acceso a servicios

La seguridad del sistema es un tema muy importante, y una de las aproximaciones para esta tarea es la cuidadosa administración del acceso a los servicios del sistema. Su sistema podría tener que proporcionar acceso a algunos servicios en particular (por ejemplo `httpd` se está ejecutando un servidor de Web). Sin embargo, si usted no tiene que proporcionar un servicio, debería minimizar su exposición a posibles ataques.

Hay diferentes métodos de administrar el acceso a los servicios del sistema. Debe decidir el método que 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 negar el acceso a un servicio es desactivandolo. Tanto los servicios administrados por `xinetd` como los servicios en `/etc/rc.d/init.d` (también conocidos como servicios SysV) pueden ser activados o desactivados utilizando tres diferentes aplicaciones:

Herramienta de configuración de servicios
: Ésta es 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
: Esta es una aplicación de la línea de comandos que permite configurar los servicios que deben ser iniciados durante el arranque del sistema para cada nivel de ejecución. Los servicios que no son controlados por `xinetd` no pueden ser iniciados, detenidos o reiniciados utilizando este programa.

`chkconfig`
: Esta es una utilidad de la línea de comandos que le permite activar o desactivar servicios en los diferentes niveles de ejecución. Los servicios que no son controlados por `xinetd` no pueden ser iniciados, detenidos o reiniciados utilizando 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 cortafuegos de 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.

Además, si está buscando una utilidad para establecer reglas de acceso generales para su máquina personal, y/o si usted es nuevo en Linux, intente la **Herramienta de configuración del nivel de seguridad** (`system-config-selinux`), el cual le permite seleccionar el nivel de seguridad para su sistema de una forma similar al realizado en la pantalla **Configuración del cortafuegos** en el programa de instalación.

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.

Existen 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 en esta línea con el nivel de ejecución deseado. El cambio no tiene efecto hasta que reinicie el sistema.

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 TCP-wrappers 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. `hosts.allow` contiene una lista de reglas que le permiten a los clientes acceder los servicios de red controlados por `xinetd` y `hosts.deny`, a su vez, contiene reglas para denegar el acceso. El archivo `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 la página man `hosts_access` en la sección 5 (`man 5 hosts_access`) para obetener más detalles.

2.1. `xinetd`

Para controlar el acceso a los servicios de Internet, use `xinetd`. Éste es un sustituto seguro del comando `inetd`. El demonio `xinetd` conserva los recursos del sistema, proporciona control y re-

gistro 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 en todos los puertos para 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 es desactivado. Si el atributo `disable` está definido a **no**, el servicio es 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 obtener 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`.

3. Herramienta de configuración de servicios

La **Herramienta de configuración de servicios** es una aplicación gráfica desarrollada por Red Hat para configurar los servicios SysV en `/etc/rc.d/init.d` que 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 usar la **Herramienta de configuración de servicios**, debe tener privilegios de usuario root. Para arrancar la aplicación, vaya al Applications (the main menu on the panel) => **Configuración del sistema** => **Configuración de servidores** => **Servicios** o escriba el comando `system-config-services` en el intérprete de comandos (por ejemplo, en un **XTerm** o en un terminal **GNOME terminal**).

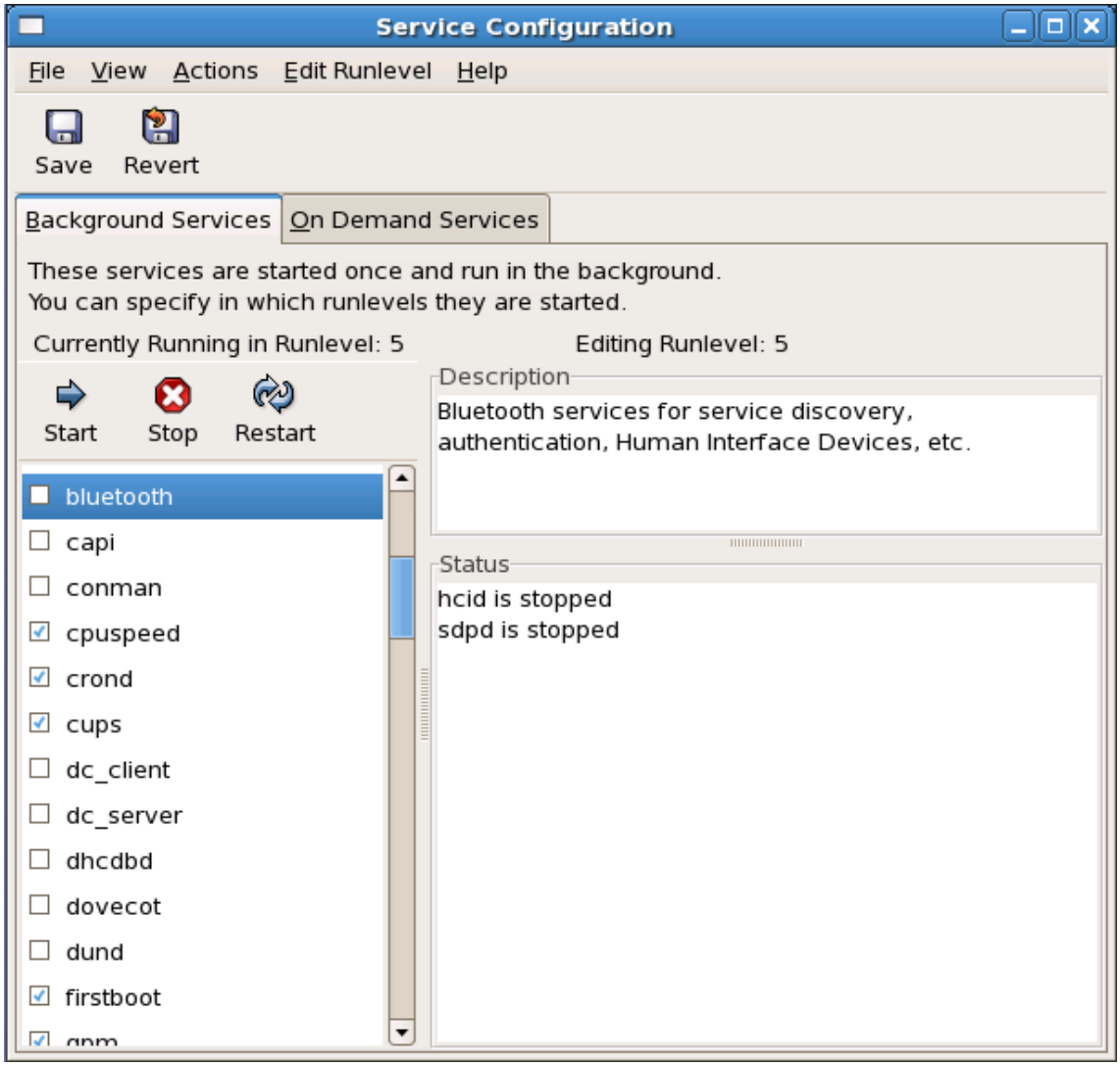


Figura 3.1. Herramienta de configuración de servicios

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. Consulte la Sección 1, “Niveles de ejecución” 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. `xinetd` se configura 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.

Nota

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 que no es controlado por `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 `httpd` de marcado a desmarcado y luego selecciona **Guardar cambios**, el nivel de ejecución 3 cambia y entonces `httpd` no es iniciado al momento de arranque. Sin embargo, el nivel de ejecución 3 no es reinicializado, por tanto `httpd` todavía estará ejecutándose. Llegados a este punto, seleccione una de las siguientes opciones:

1. Detener el servicio `httpd` — 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 de shell el comando `telinit` *`x`* (donde *`x`* 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 hacer nada — No tiene que detener el servicio `httpd`. Puede esperar a que se rearranque el sistema para que el servicio se detenga. La próxima vez que se arranque el sistema, se inicializará el nivel de ejecución sin que se ejecute el servicio `httpd`.

Para añadir un servicio a un nivel de ejecución, seleccione el nivel de ejecución desde el menú desplegable **Modificar nivel de ejecución** y seleccione **Acciones** => **Añadir servicio**. Para borrar un servicio de un nivel de ejecución, seleccione el nivel de ejecución desde el menú desplegable **Modificar nivel de ejecución**, seleccione el servicio a eliminar de la lista a la izquierda y seleccione **Acciones** => **Eliminar servicio**.

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 de **ntsysv** funciona como el programa de instalación en modo texto. Utilice las flechas del teclado para navegar a través de la lista. La barra espaciadora es utilizada para seleccionar/deseleccionar los servicios y también para presionarlos botones **Ok** y **Cancelar**. Para moverse a través de los servicios y los botones **Ok** y **Cancelar** utilice la tecla **Tab**. Un asterisco (*****) significa que el servicio está activado. Al presionar la tecla **F1** muestra una descripción de los servicios seleccionados.

Figura 3.2. La utilidad ntsysv

Aviso

Los servicios manejados por `xinetd` son afectados de inmediato por **ntsysv**. Para todos los demás servicios, los cambios no tienen efecto de inmediato. Usted debe detener o arrancar el servicio individual con el comando `service <demonio> stop`.

En el ejemplo anterior, sustituya *<demonio>* con el nombre del servicio que desee detener, por ejemplo `httpd`. Reemplace `stop` por `start` o `restart` para arrancar o reiniciar el servicio.

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 rsync` muestra:

```
rsync on
```

Como se muestra, `rsync` está activado como un servicio `xinetd`. Si `xinetd` está ejecutándose, `rsync` 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 httpd` muestra:

```
httpd 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` son afectados por `chkconfig`. Por ejemplo, si se está ejecutando `xinetd`, `rsync` está deshabilitado y se ejecuta el comando `chkconfig rsync on` y se activa de inmediato `rsync` 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 <demonio> stop`. En el ejemplo anterior, reemplace *<demonio>* con el nombre del servicio que desea parar; por ejemplo, `httpd`. Reemplace `stop` con `start` o con `restart` para iniciar o reiniciar el servicio.

6. Recursos adicionales

Para más información, refiérase a los recursos siguientes.

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).

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 4. Berkeley Internet Name Domain (BIND)

En la mayoría de las redes modernas, incluyendo la Internet, los usuarios localizan otras máquinas por su nombre. Esto libera a los usuarios de la pesada tarea de recordar la dirección numérica de los recursos de red. La forma más efectiva de configurar una red para permitir tales conexiones basadas en nombres es configurando un *servidor de nombres* o *DNS* (siglas en inglés de *Domain Name Service*), el cual resuelve los nombres de hosts en la red a direcciones numéricas y viceversa.

Este capítulo revisa el servidor de nombres incluido en Red Hat Enterprise Linux, el servidor DNS *Berkeley Internet Name Domain* (*BIND*), con énfasis en la estructura de sus archivos de configuración y en cómo deberían ser administrados tanto local como remótamente.

Nota

BIND es también conocido como el servicio `named` en Red Hat Enterprise Linux. Puede administrarlo a través de la Herramienta de configuración de servicios (`system-config-service`).

1. Introducción a DNS

DNS asocia nombres de hosts con sus respectivas direcciones IP. Así, los usuarios pueden utilizar el nombre de host cuando desean conectarse a otras máquinas en la red sin tener que recordar las direcciones IP.

El uso de nombres de un dominio completamente cualificado (FQDN) y DNS brinda varias ventajas a los administradores de sistemas, ofreciéndoles flexibilidad a la hora de cambiar las direcciones IP para máquinas individuales sin afectar las peticiones a nombres en las máquinas. Por otro lado, los administradores pueden intercambiar las máquinas que manejan consultas basadas en nombre.

DNS es normalmente implementado usando servidores centralizados que autorizan algunos dominios y remiten a otros servidores DNS para otros dominios.

Cuando un host cliente solicita información desde un servidor de nombres, usualmente se conecta al puerto 53. El servidor de nombres intenta luego resolver el FQDN basado en su librería de resolución, la cual puede contener información de autorización sobre el host solicitado o datos en caché de una consulta anterior. Si el nombre del servidor no tiene la respuesta en su librería de resolución, consultará a otros servidores de nombres, llamados *servidores de nombres de root*, para determinar cuáles servidores de nombres son fidedignos para el FQDN en cuestión. Luego, con esa información, consulta los servidores de nombres autoritarios para determinar la dirección IP del host solicitado. Si se está realizando una búsqueda inversa, se usa el mismo procedimiento, excepto que la consulta es realizada con una dirección IP desconocida en vez de un nombre.

1.1. Zonas de servidores de nombres

En Internet, el FQDN de un host se puede dividir en diversas secciones. Estas secciones son organizadas en orden jerárquico (como un árbol), con un tronco, ramas principales, ramas secundarias, etc. Por ejemplo, considere el siguiente FQDN:

```
bob.sales.example.com
```

Para leer cómo un FQDN es resuelto para encontrar la dirección IP que se relaciona a un sistema particular, lea el nombre de derecha a izquierda, con cada nivel de la jerarquía dividido por puntos (`.`). En nuestro ejemplo, `com` define el *dominio de nivel superior* para este FQDN. El nombre `example` es un subdominio bajo `com`, mientras que `sales` es un subdominio bajo `example`. El nombre a la izquierda, `bob`, identifica el nombre de una máquina específica.

Aparte del nombre del dominio, cada sección se llama *zona*, la cual define un *espacio de nombre* particular. Un espacio de nombre, controla los nombres de los subdominios de la izquierda. Aunque en el ejemplo solamente hay dos subdominios, un FQDN tiene que contener al menos un subdominio, pero puede incluir muchos más dependiendo de la organización del espacio de nombres elegido.

Las zonas son definidas en servidores de nombres autorizados a través del uso de *archivos de zona* (los cuales describen el espacio de nombres de esa zona), los servidores de correo a ser utilizados por un dominio particular o sub-dominio y más. Los archivos de zona son almancenados en *servidores de nombres primarios* (también llamados *servidores de nombres maestros*), los cuales son autorizados y en donde los cambios se hacen a los archivos, y los *servidores de nombres secundarios* (también llamados *servidores de nombres esclavos*), que reciben sus archivos de zona desde los servidores de nombres primarios. Cualquier servidor de nombres puede ser un servidor primario y secundario para zonas diferentes al mismo tiempo, y también pueden ser considerados autoritarios para múltiples zonas. Todo depende de cómo se configure el servidor de nombres.

1.2. Tipos de servidores de nombres

Existen cuatro tipos de configuración de servidores de nombres primarios:

maestro
: Almacena los registros de las zonas originales y de autoridad para un cierto espacio de nombres. Asimismo responde a consultas sobre el espacio de nombres de otros servidores de nombres.

esclavo
: Responde a las peticiones que provienen de otros servidores de nombres y que se refieren a los espacios de nombres sobre los que tiene autoridad. Sin embargo, los servidores esclavos obtienen la información de sus espacios de nombres desde los servidores maestros.

de sólo caché
: Ofrece servicios de resolución de nombres a direcciones IP pero no tiene ninguna autoridad sobre ninguna zona. Las respuestas en general se introducen en un caché por un período de tiempo fijo, el cual es especificado por el registro de zona recuperado.

reenvío

Reenvía las peticiones a una lista específica de servidores de nombres para la resolución de nombres. Si ninguno de los servidores de nombres especificados puede resolver los nombres, la resolución falla.

Un servidor de nombres puede ser uno o más de estos tipos. Por ejemplo, un servidor de nombres puede ser un maestro para algunas zonas, un esclavo para otras y sólo ofrecer el reenvío de resoluciones para otras.

1.3. BIND como un servidor de nombres

BIND realiza la resolución de nombres a través del demonio `/usr/sbin/named`. BIND también incluye una utilidad de administración llamada `/usr/sbin/rndc`. Se puede encontrar más información sobre `rndc` en Sección 4, “Uso de rndc”.

BIND almacena sus archivos de configuración en los siguientes lugares:

`/etc/named.conf`
El archivo de configuración para el demonio `named`.

directorio `/var/named/`
El directorio de trabajo `named` el cual almacena zonas, estadísticas y archivos de caché.

Nota

Si tiene instalado el paquete `bind-chroot`, el servicio BIND será ejecutado en el entorno `/var/named/chroot`. Todos los archivos serán desplazados allí. Así, `named.conf` será ubicado en `/var/named/chroot/etc/named.conf`.

Consejo

Si ha instalado el paquete `caching-nameserver`, el archivo de configuración predeterminado es `/etc/named.caching-nameserver.conf`. Para sobreescribir esta configuración, usted puede crear su propio archivo de configuración en `/etc/named.conf`. Una vez reiniciado, BIND usará el archivo personalizado `/etc/named.conf` en vez del archivo de configuración predeterminado.

Las próximas secciones revisan los archivos de configuración de BIND en más detalle.

2. `/etc/named.conf`

El archivo `named.conf` es una colección de declaraciones que utilizan opciones anidadas rodeadas por corchetes, `{ }`. Los administradores deben tener mucho cuidado cuando estén modificando `named.conf` para evitar errores sintácticos, puesto que hasta el error más pequeño puede impedir que el servicio `named` arranque.

Un archivo típico de `named.conf` está organizado de forma similar al siguiente ejemplo:

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] { <option-1>; <option-2>; <option-N>; }; <state
```

2.1. Tipos de declaraciones comúnes

Los siguientes tipos de declaraciones son usadas a menudo en `/etc/named.conf`:

2.1.1. Declaración `acl`

La sentencia `acl` (o sentencia de control de acceso) define grupos de hosts a los que se les puede permitir o negar el acceso al servidor de nombres.

Una declaración `acl` tiene la siguiente forma:

```
acl <acl-name> { <match-element>; [<match-element>; ...] };
```

En esta declaración, sustituya *`<acl-name>`* con el nombre de la lista de control de acceso y reemplace *`<match-element>`* con una lista de direcciones IP separada por puntos y comas. La mayoría de las veces, una dirección IP individual o notación de red IP (tal como `10.0.1.0/24`) es usada para identificar las direcciones IP dentro de la declaración `acl`.

Las siguientes listas de control de acceso ya están definidas como palabras claves para simplificar la configuración:

- `any` — Coincide con todas las direcciones IP.
- `localhost` — Coincide con cualquier dirección IP usada por el sistema local.
- `localnets` — Coincide con cualquier dirección IP en cualquier red en la que el sistema local esté conectado.
- `none` — No concuerda con ninguna dirección IP.

Cuando lo utilice con otras pautas (tales como las declaraciones `options`), las declaraciones `acl` pueden ser muy útiles para asegurar el uso correcto de su servidor de nombres BIND.

El ejemplo siguiente define dos listas de control de acceso y utiliza una declaración `options` para definir cómo son tratadas en el servidor de nombres:

```
acl black-hats { 10.0.2.0/24; 192.168.0.0/24; }; acl red-hats { 10.0.1.0/24; }; options { blackhole { blac
```

Este ejemplo contiene dos listas de control de acceso, `black-hats` y `red-hats`. A los hosts en la lista `black-hats` se les niega el acceso al servidor de nombres, mientras que a los hosts en la lista `red-hats` se les dá acceso normal.

2.1.2. Declaración `include`

La declaración `include` permite incluir archivos en un `named.conf`. De esta forma los datos de configuración confidenciales (tales como `llaves`) se pueden colocar en un archivo separado con permisos restringidos.

Una declaración `include` tiene la forma siguiente:

```
include "<file-name>"
```

En esta declaración, `<file-name>` es reemplazado con la ruta absoluta de un archivo.

2.1.3. Declaración `options`

La declaración `options` define opciones de configuración de servidor globales y configura otras declaraciones por defecto. Puede ser usado para especificar la ubicación del directorio de trabajo `named`, los tipos de consulta permitidos y más.

La declaración `options` tiene la forma siguiente:

```
options { <option>; [<option>; ...] };
```

En esta declaración, las directivas `<option>` son reemplazadas con una opción válida.

Las siguientes son opciones usadas a menudo:

`allow-query`
: Especifica cuáles hosts tienen permitido consultar este servidor de nombres. Por defecto, todos los hosts tienen derecho a realizar consultas. Una lista de control de acceso, o una colección de direcciones IP o redes se puede usar aquí para sólo permitir a hosts particulares hacer consultas al servidor de nombres.

`allow-recursion`
: Parecida a la opción `allow-query`, salvo que se aplica a las peticiones recursivas. Por defecto, todos los hosts están autorizados a presentar peticiones recursivas en un servidor de nombres.

`blackhole`
: Especifica cuáles hosts no tienen permitido consultar al servidor de nombres.

`directory`
: Especifica el directorio de trabajo `named` si es diferente del valor predeterminado `/var/named`.

`forwarders`
: Especifica una lista de direcciones IP válidas para los servidores de nombres donde las peticiones deben ser reenviadas para ser resueltas.

`forward`
: Especifica el comportamiento de reenvío de una directiva `forwarders`.

  Se aceptan las siguientes opciones:

  - `first` — Indica que los servidores de nombres especificados en la directiva `forwarders` sean consultados antes de que `named` intente resolver el nombre por sí mismo.
  - `only` — Especifica que `named` no intente la resolución de nombres por sí mismo cuando las consultas a los servidores de nombres especificados en la directriz `forwarders` fallen.

`listen-on`
: Especifica la interfaz de red en la cual `named` escucha por solicitudes. Por defecto, todas las

interfaces son usadas.

Al usar esta directiva en un servidor DNS que también actúa como un gateway, BIND puede ser configurado para sólo contestar solicitudes que se originan desde algunas de las redes.

El siguiente es un ejemplo de la directiva `listen-on`:

```
options { listen-on { 10.0.1.1; }; };
```

En este ejemplo, las peticiones que llegan desde la interfaz de red sirviendo a la red privada (`10.0.1.1`) son las únicas que se aceptan.

`notify`
Controla si `named` notifica a los servidores esclavos cuando una zona es actualizada. Acepta las opciones siguientes:

- `yes` — Notifica a los servidores esclavos.
- `no` — No notifica a los servidores esclavos.
- `explicit` — Solamente notifica a los servidores esclavos especificados en una lista de `also-notify` dentro de la declaración de una zona.

`pid-file`
Especifica la ubicación del archivo del proceso ID creado por `named`.

`root-delegation-only`
Activa la implementación de las propiedades de delegación en dominios de nivel superior (TLDs) y zonas raíz con una lista opcional de exclusión. La *delegación* es el proceso de separar una zona sencilla en múltiples zonas. Para poder crear una zona delegada, se utilizan elementos conocidos como *registros NS*. Los registros de servidor de nombres (registros de delegación) declaran los servidores de nombres autorizados para una zona particular.

El siguiente ejemplo de `root-delegation-only` especifica una lista excluyente de los TDLs desde los que se esperan respuestas no delegadas:

```
options { root-delegation-only exclude { "ad"; "ar"; "biz"; "cr"; "cu"; "de"; "dm"; "id"; "lu"; "lv"; "
```

`statistics-file`
Permite especificar la localización alternativa de los archivos de estadísticas. Por defecto, las estadísticas de `named` son guardadas al archivo `/var/named/named.stats`.

Existen numerosas opciones disponibles, muchas de ellas dependen unas de otras para poder funcionar correctamente. Consulte el *Manual de referencia para el administrador de BIND 9* en la Sección 7.1, “Documentación instalada” y la página man para `bind.conf` para más detalles.

2.1.4. Declaración `zone`

Una declaración `zone` define las características de una zona, tal como la ubicación de su archivo de configuración y opciones específicas de la zona. Esta declaración puede ser usada para ignorar las declaraciones globales `options`.

Una declaración `zone` tiene la forma siguiente:

```
zone <zone-name><zone-class> { <zone-options>; [<zone-options>; ...] };
```

En esta declaración, *<zone-name>* es el nombre de la zona, *<zone-class>* es la clase opcional de la zona, y *<zone-options>* es una lista de opciones que caracterizan la zona.

El atributo *<zone-name>* para la declaración de zona es particularmente importante, pues es el valor por defecto asignado para la directriz `$ORIGIN` usada dentro del archivo de zona correspondiente localizado en el directorio `/var/named/`. El demonio `named` anexa el nombre de la zona a cualquier nombre de dominio que no esté completamente cualificado listado en el archivo de zona.

Nota

Si ha instalado el paquete `caching-nameserver`, el archivo de configuración predeterminado estará en `/etc/named.rfc1912.zones`.

Por ejemplo, si una declaración `zone` define el espacio de nombres para `example.com`, utilice `example.com` como el *<zone-name>* para que sea colocado al final de los nombres de hosts dentro del archivo de zona `example.com`.

Para obtener mayor información sobre los archivos de zona, consulte Sección 3, “Archivos de zona”.

Las opciones más comunes para la declaración `zone` incluyen lo siguiente:

`allow-query`
: Especifica los clientes que se autorizan para pedir información sobre una zona. Por defecto, todas las peticiones de información son autorizadas.

`allow-transfer`
: Especifica los servidores esclavos que están autorizados para pedir una transferencia de información de la zona. Por defecto, todas las peticiones se autorizan.

`allow-update`
: Especifica los hosts que están autorizados para actualizar dinámicamente la información en sus zonas. Por defecto, no se autoriza la actualización dinámica de la información.

  Tenga cuidado cuando autorice a los hosts para actualizar la información de su zona. No habilite esta opción si no tiene confianza en el host que vaya a usar. Es mejor que el administrador actualice manualmente los registros de zona y que vuelva a cargar el servicio `named`.

`file`
: Especifica el nombre del archivo en el directorio de trabajo `named` que contiene los datos de configuración de zona.

`masters`

Especifica las direcciones IP desde las cuales solicitar información autorizada. Solamente se usa si la zona está definida como `typeslave`.

`notify`
Controla si `named` notifica a los servidores esclavos cuando una zona es actualizada. Esta directiva sólo acepta las opciones siguientes:

- `yes` — Notifica a los servidores esclavos.
- `no` — No notifica a los servidores esclavos.
- `explicit` — Solamente notifica a los servidores esclavos especificados en una lista de `also-notify` dentro de la declaración de una zona.

`type`
Define el tipo de zona.

Abajo se muestra una lista de las opciones válidas:

- `delegation-only` — Refuerza el estado de delegación de las zonas de infraestructura tales como COM, NET u ORG. Cualquier respuesta recibida sin una delegación explícita o implícita es tratada como `NXDOMAIN`. Esta opción solamente es aplicable en TLDs o en archivos raíz de zona en implementaciones recursivas o de caché.
- `forward` — Dice al servidor de nombres que lleve a cabo todas las peticiones de información de la zona en cuestión hacia otros servidores de nombres.
- `hint` — Tipo especial de zona que se usa para orientar hacia los servidores de nombres root que sirven para resolver peticiones de una zona que no se conoce. No se requiere mayor configuración que la establecida por defecto en una zona `hint`.
- `master` — Designa el servidor de nombres actual como el servidor autoritativo para esa zona. Una zona se puede configurar como tipo `master` si los archivos de configuración de la zona residen en el sistema.
- `slave` — Designa el servidor de nombres como un servidor esclavo para esa zona. También especifica la dirección IP del servidor de nombres maestro para la zona.

`zone-statistics`
Configura `named` para mantener estadísticas concerniente a esta zona, escribiéndola a su ubicación por defecto (`/var/named/named.stats`) o al archivo listado en la opción `statistics-file` en la declaración `server`. Consulte la Sección 2.2, “Otros tipos de declaraciones” para más información sobre la declaración `server`.

2.1.5. Ejemplo de declaraciones de `zone`

La mayoría de los cambios al archivo `/etc/named.conf` de un servidor de nombres maestro o esclavo envuelven agregar, modificar o borrar declaraciones `zone`. Mientras que estas declaraciones `zone` pueden contener muchas opciones, la mayoría de los servidores de nombres requieren sólo un pequeño subconjunto para funcionar efectivamente. Las siguientes declaraciones `zone` son ejemplos muy básicos que ilustran la relación de servidores de nombres maestro-esclavo.

A continuación se muestra un ejemplo de una declaración de `zone` para un servidor de nombres primario hospedando `example.com` (`192.168.0.1`):

```
zone "example.com" IN { type master; file "example.com.zone"; allow-update { none; }; };
```

En la declaración, la zona es identificada como `example.com`, el tipo es configurado a `master` y el servicio `named` se instruye para leer el archivo `/var/named/example.com.zone`. También le dice a `named` que no permita a ningún otro host que realice actualizaciones.

Una declaración `zone` de servidor esclavo para `example.com` se ve un poco diferente comparado con el ejemplo anterior. Para un servidor esclavo, el tipo se coloca a `slave` y en lugar de la línea `allow-update` está una directiva diciéndole a `named` la dirección IP del servidor maestro.

A continuación se muestra un ejemplo de una declaración `zone` para un servidor esclavo para la zona `example.com`:

```
zone "example.com" { type slave; file "example.com.zone"; masters { 192.168.0.1; }; };
```

Esta declaración `zone` configura `named` en el servidor esclavo para que busque el servidor maestro en la dirección IP `192.168.0.1` para obtener información sobre la zona `example.com`. La información que el servidor esclavo recibe desde el servidor maestro es guardada en el archivo `/var/named/example.com.zone`.

2.2. Otros tipos de declaraciones

La lista siguiente muestra tipos de declaraciones usadas con menos frecuencia disponibles dentro de `named.conf`:

`controls`
: Configura varios requerimientos de seguridad necesarios para usar el comando `rndc` para administrar el servicio `named`.

  Consulte la Sección 4.1, “Configuración de /etc/named.conf” para obtener mayor información sobre la estructura de la declaración `controls` y de las opciones que están disponibles.

`key "<key-name>"`
: Define una llave particular por nombre. Las claves son usadas para autenticar varias acciones, tales como actualizaciones seguras o el uso del comando `rndc`. Se usan dos opciones con `key`:

  - `algorithm <algorithm-name>` — El tipo de algoritma usado, tal como `dsa` o `hmac-md5`.
  - `secret "<key-value>"` — La clave encriptada.

  Consulte la Sección 4.2, “Configuración de /etc/rndc.conf” para instrucciones sobre cómo escribir una declaración `key`.

`logging`
: Permite el uso de múltiples tipos de registro, llamados *channels*. Usando la opción `channel` dentro de la declaración `logging`, se puede construir un tipo de registro personalizado — con su propio nombre de archivo (`file`), tamaño límite (`size`), versión (`version`), y nivel de

importancia (`severity`). Una vez el canal personalizado ha sido definido, se usa una opción `category` para clasificar el canal y comenzar las conexiones cuando se reinicie `named`.

Por defecto, `named` registra mensajes estándar al demonio `syslog`, que les sitúa en `/var/log/messages`. Esto se debe a que varios canales estándares se encuentran incorporados a BIND junto con varios niveles de severidad, tales como `default_syslog` (el cual maneja la información de mensajes de registros) y `default_debug` (que maneja mensajes de depuración). Una categoría por defecto, llamada `default`, usa los canales incorporados para hacer conexiones normales sin ninguna configuración especial.

La personalización del proceso de conexión es un proceso con muchos detalles que está más allá del objetivo de este capítulo. Para información sobre la creación de registros personalizados BIND, consulte el *Manual de referencia del administrador de BIND 9* mencionado en la Sección 7.1, “Documentación instalada”.

`server`
Define opciones particulares que afectan como `named` debería actuar con respecto a servidores de nombres remotos, especialmente en lo que respecta a las notificaciones y transferencias de zonas.

La opción `transfer-format` controla si un registro de recursos es enviado con cada mensaje (`one-answer`) o si registros de múltiples recursos son enviados con cada mensaje (`many-answers`). Mientras que `many-answers` es más eficiente, sólo los nuevos servidores de nombres BIND lo entienden.

`trusted-keys`
Contiene llaves públicas utilizadas por DNS seguro, DNSSEC. Para mayor información sobre la seguridad de BIND, consulte la Sección 5.3, “Seguridad”.

`view "<view-name>"`
Crea vistas especiales dependiendo de la en la cual está el host que contacta el servidor de nombres. Esto permite a determinados hosts recibir una respuesta que se refiere a una zona particular mientras que otros hosts reciben información completamente diferente. Alternativamente, algunas zonas pueden estar disponibles para ciertos hosts de confianza únicamente mientras que otros hosts menos autorizados sólo pueden hacer peticiones a otras zonas.

Se pueden usar múltiples visualizaciones, siempre y cuando sus nombres sean únicos. La opción `match-clients` especifica las direcciones IP que aplican a una vista particular. Cualquier declaración de `options` puede también ser usada dentro de una vista, ignorando las opciones globales ya configuradas por `named`. La mayoría de las declaraciones `view` contienen múltiples declaraciones `zone` que aplican a la lista `match-clients`. El orden en que las declaraciones `view` son listadas es importante, pues la primera declaración `view` que coincida con una dirección IP de cliente particular es usada.

Consulte la Sección 5.2, “Vistas múltiples” para obtener mayor información sobre la declaración `view`.

2.3. Etiquetas de comentarios

La siguiente es una lista de las etiquetas de comentarios válidas usadas dentro de `named.conf`:

- `//` — Cuando se coloca al comienzo de una línea, esa línea es ignorada por `named`.
- `#` — Cuando se coloca al comienzo de una línea, esa línea es ignorada por `named`.
- `/*` y `*/` — Cuando el texto se coloca entre estas etiquetas, se ignora el bloque de texto por `named`.

3. Archivos de zona

Los *Archivos de zona* contienen información sobre un espacio de nombres particular. Éstos son almacenados en el directorio de trabajo `named`, por defecto `/var/named/`. Cada archivo de zona es nombrado de acuerdo a la opción `file` en la declaración `zone`, usualmente en una forma que relaciona al dominio en cuestión e identifica el archivo como un archivo que contiene datos de zona, tal como `example.com.zone`.

Nota

Si ha instalado el paquete `bind-chroot`, el servicio BIND será ejecutado en el entorno `/var/named/chroot`. Todos los archivos de configuración serán desplazados allí. Así, usted podrá encontrar los archivos de zona en `/var/named/chroot/var/named`.

Cada archivo de zona contiene *directivas* y *registros de recursos*. Las directivas le dicen al servidor de nombres que realice tareas o aplique configuraciones especiales a la zona. Los registros de recursos definen los parámetros de la zona y asignan identidades a hosts individuales. Las directivas son opcionales, pero los registros de recursos se requieren para proporcionar servicios de nombres a la zona.

Todas las directivas y registros de recursos deberían ir en sus propias líneas individuales.

Los comentarios se pueden colocar después de los punto y comas (`;`) en archivos de zona.

3.1. Directivas de archivos de zona

Las directivas comienzan con el símbolo de dollar (`$`) seguido del nombre de la directiva. Usualmente aparecen en la parte superior del archivo de zona.

Las siguientes son directivas usadas a menudo:

`$INCLUDE`
: Configura a `named` para que incluya otro archivo de zona en el archivo de zona donde se usa la directiva. Así se pueden almacenar configuraciones de zona suplementarias aparte del archivo de zona principal.

`$ORIGIN`
: Anexa el nombre del dominio a registros no cualificados, tales como aquellos con el nombre de host solamente.

Por ejemplo, un archivo de zona puede contener la línea siguiente:

```
$ORIGIN example.com.
```

Cualquier nombre utilizado en registros de recursos que no terminen en un punto (.) tendrán `example.com` anexado.

Nota

El uso de la directiva `$ORIGIN` no es necesario si la zona es especificada en `/etc/named.conf` porque la zona es usada como el valor de la directiva `$ORIGIN` por defecto.

`$TTL`

Ajusta el valor *Time to Live (TTL)* predeterminado para la zona. Este es el tiempo, en segundos, que un registro de recurso de zona es válido. Cada recurso puede contener su propio valor TTL, el cual ignora esta directiva.

Cuando se decide aumentar este valor, permite a los servidores de nombres remotos hacer caché a la información de zona para un período más largo de tiempo, reduciendo el número de consultas para la zona y alargando la cantidad de tiempo requerido para proliferar cambios de registros de recursos.

3.2. Registros de recursos de archivos de zona

El componente principal de un archivo de zona es su registro de recursos.

Hay muchos tipos de registros de recursos de archivos de zona. A continuación le mostramos los tipos de registros más frecuentes:

`A`

Registro de dirección que especifica una dirección IP que se debe asignar a un nombre, como en el siguiente ejemplo:

```
<host> IN A <IP-address>
```

Si el valor `<host>` es omitido, el registro `A` apunta a una dirección IP por defecto para la parte superior del espacio de nombres. Este sistema es el objetivo para todas las peticiones no FQDN.

Considere el siguiente ejemplo de registro `A` para el archivo de zona `example.com`:

```
server1 IN A 10.0.1.3 IN A 10.0.1.5
```

Las peticiones para `example.com` apuntan a 10.0.1.3 o 10.0.1.5.

`CNAME`

Se refiere al Registro del nombre canónico, el cual enlaza un nombre con otro. Esta clase de registros es también conocido como un *alias record*.

El próximo ejemplo indica a named que cualquier petición enviada a <*alias-name*> apuntará al host, <*real-name*>. Los registros CNAME son usados normalmente para apuntar a servicios que usan un esquema de nombres común, tal como www para servidores Web.

```
<alias-name> IN CNAME <real-name>
```

En el ejemplo siguiente, un registro A vincula un nombre de host a una dirección IP, mientras que un registro CNAME apunta al nombre host www comúnmente utilizado para éste.

```
server1 IN A 10.0.1.5 www IN CNAME server1
```

MX

Registro de Mail eXchange, el cual indica dónde debería ir el correo enviado a un espacio de nombres particular controlado por esta zona.

```
 IN MX <preference-value><email-server-name>
```

En este ejemplo, <*preference-value*> permite una clasificación numérica de los servidores de correo para un espacio de nombres, dando preferencia a algunos sistemas de correo sobre otros. El registro de recursos MX con el valor más bajo <*preference-value*> es preferido sobre los otros. Sin embargo, múltiples servidores de correo pueden tener el mismo valor para distribuir el tráfico de forma pareja entre ellos.

El <*email-server-name*> puede ser un nombre de servidor o FQDN.

```
 IN MX 10 mail.example.com. IN MX 20 mail2.example.com.
```

En este ejemplo, el primer servidor de correo mail.example.com es preferido al servidor de correo mail2.example.com cuando se recibe correo destinado para el dominio example.com.

NS

Se refiere al Registro NameServer, el cual anuncia los nombres de servidores con autoridad para una zona particular.

El siguiente ejemplo es un ejemplo de un registro NS:

```
 IN NS <nameserver-name>
```

Aquí, el <*nameserver-name*> debería ser un FQDN.

Luego, dos nombres de servidores son listados como servidores con autoridad para el dominio. No es importante si estos nombres de servidores son esclavos o maestros; ambos son todavía considerados como servidores con autoridad.

```
 IN NS dns1.example.com. IN NS dns2.example.com.
```

PTR

Registro PoinTeR (puntero), diseñado para apuntar a otra parte del espacio de nombres.

Los registros PTR son usados principalmente para la resolución inversa de nombres, pues ellos apuntan direcciones IP de vuelta a un nombre particular. Consulte la Sección 3.4, “Archivos de zona de resolución de nombres inversa” para más ejemplos de registros PTR en uso.

SOA

Registro de recursos Start Of Authority, que declara información importante de autoridad relacionada con espacios de nombres al servidor de nombres.

Está situado detrás de las directivas, un registro SOA es el primer registro en un archivo de zona.

El ejemplo siguiente muestra la estructura básica de un registro de recursos SOA:

```
@ IN SOA <primary-name-server><hostmaster-email> ( <serial-number><time-to-refresh><time-to-retry><time
```

El símbolo @ coloca la directiva $ORIGIN (o el nombre de la zona, si la directiva $ORIGIN no está configurada) como el espacio de nombres que esta siendo definido por este registro de recursos SOA. El nombre del host del servidor de nombres que tiene autoridad para este dominio es la directiva <*primary-name-server*> y el correo electrónico de la persona a contactar sobre este espacio de nombres es la directiva <*hostmaster-email*>.

La directiva <*serial-number*> es un valor numérico que es incrementado cada vez que se cambia el archivo de zona para así indicar a named que debería recargar esta zona. La directiva <*time-to-refresh*> es el valor numérico que los servidores esclavos utilizan para determinar cuánto tiempo debe esperar antes de preguntar al servidor de nombres maestro si se han realizado cambios a la zona. El valor <*serial-number*> es usado por los servidores esclavos para determinar si esta usando datos de la zona desactualizados y si debería refrescarlos.

La directiva <*time-to-retry*> es un valor numérico usado por los servidores esclavos para determinar el intervalo de tiempo que tiene que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no responda. Si el servidor maestro no ha respondido a una petición de actualización de datos antes de que se acabe el intervalo de tiempo <*time-to-expire*>, los servidores esclavos paran de responder como una autoridad por peticiones relacionadas a ese espacio de nombres.

La directiva <*minimum-TTL*> es la cantidad de tiempo que otros servidores de nombres guardan en caché la información de zona.

Cuando se configura BIND, todos los tiempos son siempre referenciados en segundos. Sin embargo, es posible usar abreviaciones cuando se especifiquen unidades de tiempo además de segundos, tales como minutos (M), horas (H), días (D) y semanas (W). La Tabla 4.1, “Segundos comparados a otras unidades de tiempo” le muestra la cantidad de tiempo en segundos y el tiempo equivalente en otro formato.

Segundos	Otras unidades de tiempo
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H

Segundos	Otras unidades de tiempo
86400	1D
259200	3D
604800	1W
31536000	365D

Tabla 4.1. Segundos comparados a otras unidades de tiempo

El ejemplo siguiente ilustra la forma que un registro de recursos SOA puede tomar cuando es configurado con valores reales.

```
@ IN SOA dns1.example.com. hostmaster.example.com. ( 2001062501 ; serial 21600 ; refresh after 6 hours
```

3.3. Ejemplo de archivo de zonas

Vistos individualmente, las directivas y registros de recursos pueden ser difíciles de comprender. Sin embargo, cuando se colocan juntos en un mismo archivo, se vuelven más fáciles de entender.

El ejemplo siguiente muestra un archivo de zona muy básico.

```
$ORIGIN example.com. $TTL 86400 @ IN SOA dns1.example.com. hostmaster.example.com. ( 2001062501 ; serial 2
```

En este ejemplo, las directivas estándar y los valores SOA son usados. Los servidores de nombres con autoridad se configuran como `dns1.example.com` y `dns2.example.com`, que tiene registros A que los relacionan con `10.0.1.1` y `10.0.1.2`, respectivamente.

Los servidores de correo configurados con los registros MX apuntan a `server1` y `server2` a través de registros CNAME. Puesto que los nombres `server1` y `server2` no terminan en un punto (.), el dominio `$ORIGIN` es colocado después de ellos, expandiéndolos a `server1.example.com` y a `server2.example.com`. A través de registros de recursos relacionados A, se puede determinar sus direcciones IP.

Los servicios FTP y Web, disponibles en los nombres estándar `ftp.example.com` y `www.example.com`, son apuntados a los servidores apropiados usando registros CNAME.

Este archivo de zona se colocará en funcionamiento con una declaración `zone` en el archivo `named.conf` el cual se ve similar a lo siguiente:

```
zone "example.com" IN { type master; file "example.com.zone"; allow-update { none; }; };
```

3.4. Archivos de zona de resolución de nombres inversa

Se usa un archivo de zona de resolución inversa de nombres para traducir una dirección IP en un espacio de nombres particular en un FQDN. Se vé muy similar a un archivo de zona estándar, excepto que se usan registros de recursos PTR para enlazar las direcciones IP a un nombre de dominio completamente cualificado.

El ejemplo siguiente muestra la estructura básica de un registro de recursos PTR:

```
<last-IP-digit> IN PTR <FQDN-of-system>
```

El valor *<last-IP-digit>* se refiere al último número en una dirección IP que apunta al FQDN de un sistema particular.

En el ejemplo siguiente, las direcciones IP de la 10.0.1.1 a la 10.0.1.6 apuntan a los FQDNs correspondientes. Pueden ser ubicadas en /var/named/example.com.rr.zone.

```
$ORIGIN 1.0.10.in-addr.arpa. $TTL 86400 @ IN SOA dns1.example.com. hostmaster.example.com. ( 2001062501 ; s
```

Este archivo de zona se colocará en funcionamiento con una declaración zone en el archivo named.conf el cual se ve similar a lo siguiente:

```
zone "1.0.10.in-addr.arpa" IN { type master; file "example.com.rr.zone"; allow-update { none; }; };
```

Hay muy poca diferencia entre este ejemplo y una declaración de zone estándar, excepto por el nombre de la zona. Observe que una zona de resolución de nombres inversa requiere que los primeros tres bloques de la dirección IP estén invertidos seguido por .in-addr.arpa. Esto permite asociar con la zona a un bloque único de números IP usados en el archivo de zona de resolución de nombres inversa.

4. Uso de rndc

BIND incluye una utilidad llamada rndc que permite la administración a través de la línea de comandos del demonio named desde el host local o desde un host remoto.

Para prevenir el acceso no autorizado al demonio named, BIND utiliza un método de autenticación de llave secreta compartida para otorgar privilegios a hosts. Esto significa que una llave idéntica debe estar presente en los archivos de configuración /etc/named.conf y en el /etc/rndc.conf de rndc.

Nota

Si ha instalado el paquete bind-chroot, el servicio BIND será ejecutado en el entorno /var/named/chroot. Todos los archivos de configuración serán desplazados allí. Así, el archivo rndc.conf estará ubicado en /var/named/chroot/etc/rndc.conf.

Tenga en cuenta que la utilidad rndc no se ejecuta en un entorno chroot, por lo cual /etc/rndc.conf es un enlace simbólico a /var/named/chroot/etc/rndc.conf.

4.1. Configuración de /etc/named.conf

Para que rndc se pueda conectar a un servicio named, debe haber una declaración controls en el archivo de configuración del servidor BIND /etc/named.conf.

La declaración controls mostrada abajo en el ejemplo siguiente, permite a rndc conectarse desde un host local.

```
controls { inet 127.0.0.1 allow { localhost; } keys { <key-name>; }; };
```

Esta declaración le dice a `named` que escuche en el puerto por defecto TCP 953 de la dirección loopback y que permita comandos `rndc` provenientes del host local, si se proporciona la llave correcta. El valor *<key-name>* especifica un nombre en la declaración `key` dentro del archivo `/etc/named.conf`. El ejemplo siguiente ilustra la declaración `key`.

```
key "<key-name>" { algorithm hmac-md5; secret "<key-value>"; };
```

En este caso, el *<key-value>* utiliza el algoritmo HMAC-MD5. Utilice el comando siguiente para generar llaves usando el algoritmo HMAC-MD5:

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Es aconsejable crear una llave con al menos 256-bit de longitud. La llave que debería ser colocada en el área *<key-value>* se puede encontrar en el archivo *<key-file-name>* generado por este comando.

Advertencia

Debido a que `/etc/named.conf` es universalmente accesible, es aconsejable colocar la declaración `key` en un archivo separado que sólo sea accesible por root y luego utilizar una declaración `include` para referenciarlo. Por ejemplo:

```
include "/etc/rndc.key";
```

4.2. Configuración de `/etc/rndc.conf`

La declaración `key` es la más importante en `/etc/rndc.conf`.

```
key "<key-name>" { algorithm hmac-md5; secret "<key-value>"; };
```

<key-name> y *<key-value>* deberían ser exáctamente los mismos que sus configuraciones en `/etc/named.conf`.

Para hacer coincidir las claves especificadas en el archivo de configuración del servidor objetivo `/etc/named.conf`, agregue las líneas siguientes a `/etc/rndc.conf`.

```
options { default-server localhost; default-key "<key-name>"; };
```

Este directriz configura un valor de llave global por defecto. Sin embargo, el archivo de configuración `rndc` también puede usar llaves diferentes para servidores diferentes, como en el ejemplo siguiente:

```
server localhost { key "<key-name>"; };
```

Importante

Asegúrese de que sólo el usuario root pueda leer y escribir al archivo `/etc/rndc.conf`.

Para más información sobre el archivo `/etc/rndc.conf`, vea la página man de `rndc.conf`.

4.3. Opciones de línea de comandos

Un comando `rndc` tiene la forma siguiente:

`rndc <options><command><command-options>`

Cuando esté ejecutando `rndc` en una máquina local configurada de la forma correcta, los comandos siguientes están disponibles:

- `halt` — Detiene inmediatamente el servicio `named`.
- `querylog` — Registra todas las peticiones hechas a este servidor de nombres.
- `refresh` — Refresca la base de datos del servidor de nombres.
- `reload` — Recarga los archivos de zona pero mantiene todas las respuestas precedentes situadas en caché. Esto le permite realizar cambios en los archivos de zona sin perder todas las resoluciones de nombres almacenadas.

  Si los cambios sólo afectaron una zona específica, vuelva a cargar esa zona añadiendo el nombre de la zona después del comando `reload`.
- `stats` — Descarga las estadísticas actuales de `named` al archivo `/var/named/named.stats`.
- `stop` — Detiene al servidor salvando todas las actualizaciones dinámicas y los datos de las *Transferencias de zona incremental* (*IXFR*) antes de salir.

Ocasionalmente, puede ser necesario ignorar las configuraciones por defecto en el archivo `/etc/rndc.conf`. Están disponibles las siguientes opciones:

- `-c <configuration-file>` — Especifica la ubicación alterna de un archivo de configuración.
- `-p <port-number>` — Especifica la utilización de un número de puerto diferente del predeterminado 953 para la conexión del comando `rndc`.
- `-s <server>` — Especifica un servidor diferente al `default-server` listado en `/etc/rndc.conf`.
- `-y <key-name>` — Le permite especificar una llave distinta de la opción `default-key` en el archivo `/etc/rndc.conf`.

Se puede encontrar información adicional sobre estas opciones en la página del manual de `rndc`.

5. Características avanzadas de BIND

La mayoría de las implementaciones BIND solamente utilizan `named` para proporcionar servicios de resolución de nombres o para actuar como una autoridad para un dominio particular o subdominio. Sin embargo, la versión 9 de BIND tiene un número de características avanzadas que permiten un servicio DNS más seguro y avanzado.

Atención

Algunas de estas propiedades avanzadas, tales como DNSSEC, TSIG e IXFR (las cuales se definen en la sección siguiente), solamente se deberían usar en los entornos de red que tengan servidores de nombres que soporten estas propiedades. Si su entorno de red incluye servidores de nombres no-BIND o versiones anteriores de BIND, verifique que cada característica avanzada sea soportada antes de intentar utilizarla.

Todas las propiedades citadas aquí se describen en detalle en el *Manual de referencia para el administrador de BIND 9* referenciado en la Sección 7.1, “Documentación instalada”.

5.1. Mejoras al protocolo DNS

BIND soporta Transferencias de zona incremental (Incremental Zone Transfers, IXFR), donde un servidor de nombres esclavo sólo descargará las porciones actualizadas de una zona modificada en un servidor de nombres maestro. El proceso de transferencia estándar requiere que la zona completa sea transferida a cada servidor de nombres esclavo hasta por el cambio más pequeño. Para dominios muy populares con archivos de zona muy largos y muchos servidores de nombres esclavos, IXFR hace que la notificación y los procesos de actualización sean menos exigentes en recursos.

Observe que IXFR solamente está disponible cuando utiliza la *actualización dinámica* para realizar los cambios en los registros de zona maestra. Si cambia los archivos de zona manualmente, se utilizará AXFR (Automatic Zone Transfer). Encontrará más información sobre la actualización dinámica en el *Manual de referencia para el administrador de BIND 9*. Consulte la Sección 7.1, “Documentación instalada” para más información.

5.2. Vistas múltiples

A través del uso de la declaración `view` en `named.conf`, BIND puede presentar información diferente dependiendo de la red desde la cual se esté realizando la petición.

Esta característica es básicamente utilizada para negar entradas DNS confidenciales a clientes fuera de la red local, mientras se permiten consultas desde clientes dentro de la red local.

La declaración `view` usa la opción `match-clients` para coincidir direcciones IP o redes completas y darles opciones especiales y datos de zona.

5.3. Seguridad

BIND soporta un número de métodos diferentes para proteger la actualización y zonas de transferencia, en los servidores de nombres maestro y esclavo:

DNSSEC
: Abreviación de *DNS SECurity*, esta propiedad permite firmar criptográficamente las zonas con una *clave de zona*.

  De esta manera puede verificar que la información de una zona provenga de un servidor de nombres que la ha firmado con una llave privada, siempre y cuando el recipiente tenga esa llave pública del servidor de nombres.

  La versión 9 de BIND también soporta el método SIG(0) de llave pública/privada de autenticación de mensajes.

TSIG
: Abreviación para *Transaction SIGnatures*, esta característica permite una transferencia desde el maestro al esclavo solamente después de verificar que una llave secreta compartida existe tanto en el servidor maestro como en el esclavo.

  Esta característica fortalece el método estándar basado en direcciones IP de transferencia de autorización. Un intruso no solamente necesitará acceso a la dirección IP para transferir la zona, sino también necesitará conocer la clave secreta.

  BIND versión 9 también soporta *TKEY*, el cual es otro método de autorización de zonas de transferencia basado en clave secreta compartida.

5.4. IP versión 6

BIND versión 9 puede proporcionar servicios de nombres en ambientes IP versión 6 (IPv6) a través del uso de registros de zona `A6`.

Si el entorno de red incluye hosts IPv4 e IPv6, use el demonio ligero de resolución `lwresd` en todos los clientes de la red. Este demonio es muy eficiente, funciona solamente en caché y además entiende los nuevos registros `A6` y `DNAME` usados bajo IPv6. Consulte la página de manual para `lwresd` para más información.

6. Errores comunes que debe evitar

Es normal que los principiantes cometan errores modificando los archivos de configuración de BIND. Asegúrese de evitar los siguientes errores:

- *Incremente el número de serie cuando esté modificando un archivo de zona.*

  Si no se incrementa el número de serie, el servidor de nombres maestro tendrá la información nueva correcta, pero los servidores esclavos nunca serán notificados del cambio ni intentarán actualizar sus datos de esa zona.

- *Preste atención a la utilización correcta de las llaves y de los puntos y comas en el archivo `/etc/named.conf`.*

  La omisión de un punto y coma o de una llave en una sección causará que `named` se niegue

a arrancar.

- *Recuerde colocar puntos (.) en los archivos de zona después de todos los FQDNs y omítalos en los nombres de máquinas.*

  Un punto al final de un nombre de dominio denota un nombre de dominio completamente cualificado. Si el punto es omitido, entonces `named` añade el nombre de la zona o el valor `$ORIGIN` para completarlo.

- *Si un cortafuegos está bloqueando las conexiones con el programa `named` a otros servidores de nombres, modifique su archivo de configuración.*

  Por defecto, la versión 9 de BIND usa los puertos aleatorios por encima de 1024 para consultar otros servidores de nombres. Algunos cortafuegos, sin embargo, esperan que todos los servidores de nombres se comuniquen usando solamente el puerto 53. Puede forzar `named` a que use el puerto 53 añadiendo la línea siguiente a la declaración `options` de `/etc/named.conf`:

  ```
  query-source address * port 53;
  ```

7. Recursos adicionales

Las siguientes fuentes de información le proporcionarán recursos adicionales relacionados a BIND.

7.1. Documentación instalada

BIND contiene una larga variedad de documentación que cubre diferentes tópicos, cada uno de ellos ubicado en su propio directorio. Por cada elemento, reemplace `<version-number>` con la versión de `bind` instalada en el sistema:

`/usr/share/doc/bind-<version-number>/`
: Este directorio enumera las características más recientes.

`/usr/share/doc/bind-<version-number>/arm/`
: Este directorio contiene una versión en HTML y SGML del *Manual de referencia para el administrador de BIND 9*, el cual detalla los requerimientos de recursos de BIND, cómo configurar diferentes tipos de servidores de nombres, balancear cargas y otros temas avanzados. Para la mayoría de los usuarios nuevos de BIND, este es el mejor lugar para comenzar.

`/usr/share/doc/bind-<version-number>/draft/`
: Este directorio contiene documentos técnicos ordenados concernientes al servicio DNS y que proponen métodos para abordarlo.

`/usr/share/doc/bind-<version-number>/misc/`
: Este directorio contiene documentos diseñados para referenciar problemas avanzados. Los usuarios de la versión 8 de BIND deberían consultar el documento `migration` para cambios específicos que se deben hacer cuando se esté moviendo a BIND 9. El archivo `options` lista todas las opciones implementadas en BIND 9 que son usadas en el archivo `/`

`etc/named.conf`.

`/usr/share/doc/bind-<version-number>/rfc/`
Este directorio proporciona cada documento RFC relacionado con BIND.

Hay un gran número de páginas man para las diferentes aplicaciones y archivos de configuración referentes a BIND. La siguiente es una lista de algunas de las páginas importantes.

Aplicaciones administrativas

- La página `man rndc` — Explica las diferentes opciones disponibles cuando se utilice el comando `rndc` para controlar un servidor de nombres BIND.

Aplicaciones de servidor

- La página `man named` — Explora argumentos varios que se pueden usar para controlar el demonio de servidor de nombres BIND.
- `man lwresd` — Describe las opciones disponibles y el propósito para el demonio lightweight resolver.

Archivos de configuración

- La página `man named.conf` — Una lista completa de las opciones disponibles dentro del archivo de configuración `named`.
- La página `man rndc.conf` — Una lista completa de opciones disponibles dentro del archivo de configuración `rndc`.

7.2. Sitios web de utilidad

- http://www.isc.org/index.pl?/sw/bind/ — La página principal del proyecto BIND contiene información sobre los lanzamientos recientes y la versión PDF del *Manual de referencia para el administrador de BIND 9*.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Cubre el uso de BIND como un servidor de nombres de caché y la configuración de varios archivos de zona necesarios para servir como el servidor de nombres principal de un dominio.

7.3. Libros relacionados

- *DNS y BIND* por Paul Albitz y Cricket Liu; O'Reilly & Associates — Una referencia popular que explica opciones de configuración comunes y esotéricas de BIND, así como también proporciona estrategias para asegurar su servidor DNS.
- *The Concise Guide to DNS and BIND* por Nicolai Langfeldt; Que — Hace referencia a la conexión entre servicios de red múltiples y BIND, haciendo énfasis en los tópicos técnicos orientados a tareas.

Capítulo 5. OpenSSH

SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar aplicaciones de terminal anteriores y menos seguras que eran utilizadas para registrarse remotamente, tales como `telnet` o `rsh`. Un programa relacionado, el `scp`, reemplaza otros programas diseñados para copiar archivos entre hosts como `rcp`. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas en lo posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

1. Características de SSH

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremadamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de reenviar aplicaciones X11 [1] desde el servidor. Esta técnica, llamada *reenvío por X11*, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para asegurar los protocolos inseguros, como por ejemplo POP, mediante el uso de una técnica llamada *reenvío por puerto*. Utilizando este método se incrementa la seguridad del sistema en general y la seguridad de los datos.

El servidor y cliente OpenSSH pueden también ser configurados para crear un túnel similar a una red privada virtual para el tráfico entre el cliente y el servidor.

Red Hat Enterprise Linux contiene el paquete general de OpenSSH (`openssh`) así como también los paquetes del servidor OpenSSH (`openssh-server`) y del cliente (`openssh-clients`). Tenga en cuenta que los paquetes OpenSSH requieren el paquete OpenSSL (`openssl`). OpenSSL instala varias bibliotecas criptográficas importantes, permitiendo que OpenSSH pueda proporcionar comunicaciones encriptadas.

1.1. ¿Por qué usar SSH?

[1] X11 se refiere al sistema de visión por ventanas X11R7, tradicionalmente llamado Sistema de ventanas X o simplemente X. Red Hat Enterprise Linux incluye X11R7, un sistema de ventanas X de código abierto.

Los usuarios malignos tienen a su disposición una variedad de herramientas que les permiten interceptar y redirigir el tráfico de la red para ganar acceso al sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

- *Intercepción de la comunicación entre dos sistemas* — En este escenario, el atacante puede estar en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. El atacante puede interceptar y conservar la información o puede modificar la información y luego enviarla al recipiente al cual estaba destinada.

  Este ataque se puede realizar a través del uso de un paquete sniffer —una utilidad de red muy común.

- *Personificación de un determinado host* — Con esta estrategia, el sistema de un atacante se configura para fingir ser el recipiente a quien está destinado un mensaje. Si funciona la estrategia, el sistema del usuario no se da cuenta del engaño y continúa la comunicación con el host incorrecto.

  Este ataque puede realizarse con técnicas como el envenenamiento del DNS [2] o spoofing de IP (engaño de direcciones IP) [3]

Ambas técnicas interceptan información potencialmente confidencial y si esta intercepción se realiza con propósitos hostiles, el resultado puede ser catastrófico.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar archivos, se pueden disminuir notablemente estas amenazas a la seguridad. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada. No servirá de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una llave conocida sólo por el sistema local y el remoto.

2. Versiones del protocolo SSH

El protocolo SSH permite a cualquier programa cliente y servidor construido según las especificaciones del protocolo comunicarse de forma segura y de forma intercambiable.

En la actualidad existen dos variedades de SSH (versión 1 y versión 2). La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de llaves mejorado que no es vulnerable al hueco de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.

Importante

Se recomienda que sólo se utilicen servidores y clientes compatibles con la versión 2 de SSH siempre que sea posible.

[2] El envenenamiento del DNS ocurre cuando un intruso entra en el servidor de DNS, apuntando sistemas hacia hosts intencionalmente duplicados.
[3] IP spoofing ocurre cuando un intruso manda paquetes de red que parecen provenir de hosts de confianza de la red.

3. Secuencia de eventos de una conexión SSH

La siguiente serie de eventos lo ayudan a proteger la integridad de la comunicación SSH entre dos host.

1. Se lleva a cabo un "apretón de manos" encriptado para que el cliente pueda verificar que se está comunicando con el servidor correcto.
2. La capa de transporte de la conexión entre el cliente y la máquina remota es encriptada mediante un código simétrico.
3. El cliente se autentica ante el servidor.
4. El cliente remoto interactúa con la máquina remota a través de la conexión encriptada.

3.1. Capa de transporte

El papel principal de la capa de transporte es facilitar una comunicación segura entre los dos hosts durante la autenticación y la subsecuente comunicación. La capa de transporte lleva a cabo esta tarea manejando la encriptación y decodificación de datos y proporcionando protección de integridad de los paquetes de datos mientras son enviados y recibidos. La capa de transporte proporciona compresión de datos, lo que acelera la transmisión de la información.

Al contactar un cliente a un servidor por medio del protocolo SSH se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente. Durante el intercambio se producen los siguientes pasos:

- Intercambio de claves
- Se determina el algoritmo de encriptación de la clave pública
- Se determina el algoritmo de la encriptación simétrica
- Se determina el algoritmo autenticación de mensajes
- Se determina el algoritmo del hash

El servidor se identifica ante el cliente con una *llave de host* única durante el intercambio de llaves. Obviamente, si este cliente nunca se había comunicado antes con este determinado servidor, la llave del servidor le resultará desconocida al cliente y no lo conectará. OpenSSH evita este problema permitiendo que el cliente acepte la llave del host del servidor después de que el usuario es notificado y verifica la aceptación de la nueva llave del host. Para las conexiones posteriores, la llave del host del servidor se puede verificar con la versión guardada en el cliente, proporcionando la confianza de que el cliente se está comunicando con el servidor deseado. Si en el futuro, la llave del host ya no coincide, el usuario debe eliminar la versión guardada antes de que una conexión pueda ocurrir.

Precaución

Un atacante podría enmascararse como servidor SSH durante el contacto inicial ya que el sistema local no conoce la diferencia entre el servidor en cuestión y el servidor falso configurado por un agresor. Para evitar que esto ocurra, debería verificar la integridad del nuevo servidor SSH contactando con el administrador del servidor antes de conectarse por primera vez o en el evento de que no coincidan las claves.

SSH fue ideado para funcionar con casi cualquier tipo de algoritmo de clave pública o formato de codificación. Después del intercambio de claves inicial se crea un valor hash usado para el intercambio y un valor compartido secreto, los dos sistemas empiezan inmediatamente a calcular claves y algoritmos nuevos para proteger la autenticación y los datos que se enviarán a través de la conexión en el futuro.

Después de que una cierta cantidad de datos haya sido transmitida con un determinado algoritmo y clave (la cantidad exacta depende de la implementación de SSH), ocurre otro intercambio de claves, el cual genera otro conjunto de valores de hash y un nuevo valor secreto compartido. De esta manera aunque un agresor lograse determinar los valores de hash y de secreto compartido, esta información sólo será válida por un periodo de tiempo limitado.

3.2. Autenticación

Cuando la capa de transporte haya construido un túnel seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autenticación soportados, tales como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autenticarse ante el servidor mediante el uso de cualquiera de los métodos soportados.

Los servidores y clientes SSH se pueden configurar para permitir varios tipos de autenticación, lo cual le concede a cada lado la cantidad óptima de control. El servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad; el cliente puede elegir el orden en que intentará utilizar los métodos de autenticación entre las opciones a disposición.

3.3. Canales

Luego de una autenticación exitosa sobre la capa de transporte SSH, se abren múltiples canales a través de la técnica llamada *multiplexing*[4]. Cada uno de estos canales manejan la conexión para diferentes sesiones de terminal y para sesiones de reenvío X11.

Ambos clientes y servidores pueden crear un canal nuevo. Luego se le asigna un número diferente a cada canal en cada punta de la conexión. Cuando el cliente intenta abrir un nuevo canal, los clientes envían el número del canal junto con la petición. Esta información es almacenada por el servidor y usada para dirigir la comunicación a ese canal. Esto es hecho para que diferentes tipos de sesión no afecten una a la otra y así cuando una sesión termine, su canal pueda ser cerrado sin interrumpir la conexión SSH primaria.

[4] Una conexión multiplexada consiste de muchas señales que se envian sobre un medio común, compartido. Con SSH, canales diferentes son enviados sobre una conexión común segura.

Los canales también soportan el *control de flujo*, el cual les permite enviar y recibir datos ordenadamente. De esta manera, los datos no se envían a través del canal sino hasta que el host haya recibido un mensaje avisando que el canal está abierto y puede recibirlos.

El cliente y el servidor negocian las características de cada canal automáticamente, dependiendo del tipo de servicio que el cliente solicita y la forma en que el usuario está conectado a la red. Esto otorga una gran flexibilidad en el manejo de diferentes tipos de conexiones remotas sin tener que cambiar la infraestructura básica del protocolo.

4. Configurar un servidor OpenSSH

Para poner en funcionamiento un servidor OpenSSH, primero debe asegurarse de 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`. El archivo de configuración por defecto debería ser suficiente para la mayoría de los propósitos. 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 de `sshd` para una lista de palabras reservadas que pueden ser definidas en su archivo de configuración.

Si reinstala un sistema, el sistema reinstalado crea un nuevo conjunto de llaves de identificación. Cualquier cliente que se haya conectado al sistema con alguna de las herramientas OpenSSH, verán el siguiente mensaje antes de la reinstalación:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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.
```

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.

4.1. Requiriendo SSH para conexiones remotas

Para que SSH sea realmente eficaz, el uso de protocolos de conexión inseguros, como por ejemplo FTP y Telnet, deberían ser prohibidos. De lo contrario, una contraseña de usuario puede estar protegida usando SSH para una sesión, para luego ser capturada cuando establece una conexión Telnet.

Algunos servicios a deshabilitar incluyen:

- `telnet`
- `rsh`
- `rlogin`

- `vsftpd`

Para desactivar métodos de conexión inseguros al sistema, use el programa de línea de comandos `chkconfig`, el programa basado en ncurses **ntsysv**, o la **Herramienta de configuración de servicios** (`system-config-services`). Todas estas herramientas requieren prioridades de root.

5. Archivos de configuración de OpenSSH

OpenSSH tiene dos conjuntos diferentes de archivos de configuración: uno para clientes (`ssh`, `scp` y `sftp`) y otro para el demonio del servidor (`sshd`).

La información de configuración SSH para todo el sistema está almacenada en el directorio `/etc/ssh/`:

- `moduli` — Contiene grupos Diffie-Hellman usados para el intercambio de la clave Diffie-Hellman que es imprescindible para la construcción de una capa de transporte seguro. Cuando se intercambian las claves al inicio de una sesión SSH, se crea un valor secreto y compartido que no puede ser determinado por ninguna de las partes individualmente. Este valor se usa para proporcionar la autenticación del host.
- `ssh_config` — El archivo de configuración del sistema cliente SSH por defecto. Este archivo se sobreescribe si hay alguno ya presente en el directorio principal del usuario (`~/.ssh/config`).
- `sshd_config` — El archivo de configuración para el demonio `sshd`
- `ssh_host_dsa_key` — La clave privada DSA usada por el demonio `sshd`.
- `ssh_host_dsa_key.pub` — La clave pública DSA usada por el demonio `sshd`.
- `ssh_host_key` — La clave privada RSA usada por el demonio `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_key.pub` — La clave pública RSA usada por el demonio `sshd` para la versión 1 del protocolo SSH.
- `ssh_host_rsa_key` — La clave privada RSA usada por el demonio `sshd` para la versión 2 del protocolo SSH.
- `ssh_host_rsa_key.pub` — La clave pública RSA usada por el demonio `sshd` para la versión 2 del protocolo SSH.

La información para la configuración SSH específica para el usuario está almacenada en el directorio `~/.ssh/` del usuario:

- `authorized_keys` — Este archivo contiene una lista de claves públicas autorizadas. Cuando un cliente se conecta al servidor, el servidor autentica al cliente chequeando su clave pública firmada almacenada dentro de este archivo.
- `id_dsa` — Contiene la clave privada DSA del usuario.

- `id_dsa.pub` — la clave pública DSA del usuario.
- `id_rsa` — La clave RSA privada usada por `ssh` para la versión 2 del protocolo SSH.
- `id_rsa.pub` — La clave pública RSA usada por `ssh` para la versión 2 del protocolo SSH.
- `identity` — La clave privada RSA usada por `ssh` para la versión 1 del protocolo SSH.
- `identity.pub` — La clave pública RSA usada por `ssh` para la versión 1 del protocolo SSH.
- `known_hosts` — Este archivo contiene las claves de host DSA de los servidores SSH a los cuales el usuario ha accedido. Este archivo es muy importante para asegurar que el cliente SSH está conectado al servidor SSH correcto.

Importante

Si se ha cambiado una llave de host del servidor SSH, el cliente notificará al usuario que la conexión no puede proceder hasta que la llave del host del servidor sea borrada del archivo `known_hosts` usando un editor de texto. Antes de hacer esto, sin embargo, contacte al administrador del sistema del servidor SSH para verificar que no se ha comprometido al servidor.

Consulte las páginas man para `ssh_config` y `sshd_config` para obtener información acerca de las directivas disponibles en los archivos de configuración SSH.

6. 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.

6.1. 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 de la 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 añadirá el servidor en su lista de host conocidos (`~/.ssh/known_hosts/`) como se muestra en el siguiente mensaje:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

Luego, verá un intérprete de comandos preguntándole por su contraseña. Después de ingresar su contraseña, se encontrará en el intérprete de comandos de la máquina remota. Si no especifica un nombre de usuario, el nombre de usuario con el que se ha validado en la máquina local se utilizará en la máquina remota. Si quiere especificar un nombre de usuario use el comando siguiente:

```
ssh nombre-usuario@penguin.example.net
```

También puede usar la sintaxis `ssh -l nombre-usuario penguin.example.net`.

El comando `ssh` se puede utilizar para ejecutar un comando en una máquina remota sin acceder al intérprete de comandos. La sintaxis es `ssh nombre-hostcommand`. 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 de la shell:

```
ssh penguin.example.net ls /usr/share/doc
```

Una vez que introduzca la contraseña correcta, verá el contenido del directorio `/usr/share/doc`, y regresará a la shell de su equipo local.

6.2. 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 <archivo-local>nombre-usuario@tohostname:<archivo-remoto>
```

`<archivo-local>` especifica la fuente incluyendo la ruta al archivo, tal como `/var/log/maillog`. `<archivo-remoto>` especifica el destino, el cual puede ser un nuevo archivo tal como `/tmp/hostname-maillog`. Para el sistema remoto, si no tiene un barra oblícua (`/`) en frente, la ruta será relativa al directorio principal de *`nombre-usuario`*, usualmente `/home/username/`.

Para transferir un archivo local `shadowman` al directorio principal de su cuenta en penguin.example.net, escriba en la línea de comandos (reemplace *`nombre-usuario`* con su nombre de usuario):

```
scp shadowman nombre_usuario@penguin.example.net:shadowman
```

Esto transferirá el archivo local `shadowman` a `/home/`*`nombre_usuario`*`/shadowman` en penguin.example.net. También puede dejar por fuera la parte final de `shadowman` en el comando `scp`.

La sintaxis general para transferir un archivo remoto al sistema local es como sigue:

```
scp nombre_usuario@tohostname:<archivoremoto><nuevoarchivolocal>
```

`<archivoremoto>` especifica la fuente incluyendo la ruta y `<nuevoarchivolocal>` especifica el destino con su ruta.

Se pueden 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/* nombre_usuario@penguin.example.net:uploads/
```

6.3. 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 nombre-usuario@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.

7. Más que un Shell seguro

Una interfaz de línea de comandos segura es sólo el inicio de las muchas maneras de usar SSH. Dada una cantidad apropiada de ancho de banda, las sesiones X11 se pueden dirigir por un canal SSH. O usando reenvío TCP/IP, se pueden asignar conexiones de puerto entre sistemas que previamente eran inseguras a canales SSH específicos.

7.1. Reenvío por X11

Abrir una sesión X11 a través de una conexión SSH es tan fácil como conectarse a un servidor SSH utilizando la opción `-Y` y ejecutar un programa X en una máquina local.

```
ssh -Y <usuario>@example.com
```

Cuando un programa X se ejecuta desde un intérprete de comandos de shell segura, el cliente y el servidor SSH crean un nuevo canal seguro; los datos del programa X se envían a través de ese canal a la máquina cliente de forma transparente.

El reenvío por X11 puede ser muy útil. Por ejemplo, se puede usar el reenvío por X11 para crear una sesión segura e interactiva de la **Herramienta de configuración de la impresora**. Para hacer esto, conéctese al servidor usando **ssh** y escriba:

```
system-config-printer &
```

Después de proporcionar la contraseña de root para el servidor, la **Herramienta de configuración de la impresora** aparecerá y le permitirá al usuario remoto configurar de una forma segura la impresora en el sistema remoto.

7.2. Reenvío del puerto

Con SSH puede asegurar los protocolos TCP/IP a través del reenvío de puertos. Cuando use esta técnica, el servidor SSH se convierte en un conducto encriptado para el cliente SSH.

El reenvío de puertos funciona mediante el mapeado de un puerto local en el cliente a un puer-

to remoto en el servidor. SSH le permite mapear cualquier puerto desde el servidor a cualquier puerto en el cliente; los números de puerto no necesitan coincidir para que esto funcione.

Para crear un canal de reenvío de puerto TCP/IP que escucha conexiones del localhost, utilice el siguiente comando:

```
ssh -L local-port:remote-hostname:remote-portusername@hostname
```

Nota

La configuración del reenvío de puertos para escuchar puertos bajo 1024 requiere acceso de root.

Para verificar correo-e en un servidor llamado `mail.example.com` usando POP3 a través de una conexión encriptada, use el comando siguiente:

```
ssh -L 1100:mail.example.com:110 mail.example.com
```

Una vez que el canal de reenvío de puerto está entre la máquina cliente y el servidor de correo, puede direccionar su cliente de correo POP3 para usar el puerto 1100 en su host local para comprobar el nuevo correo. Cualquier petición enviada al puerto 1100 en el sistema cliente será dirigida seguramente al servidor `mail.example.com`.

Si `mail.example.com` no está ejecutando un servidor SSH, pero otra máquina en la misma red si, SSH todavía puede ser usado para asegurar parte de la conexión. Sin embargo, un comando ligeramente diferente es necesario:

```
ssh -L 1100:mail.example.com:110 other.example.com
```

En este ejemplo, se está reenviando las peticiones POP3 desde el puerto 1100 en la máquina cliente a través de una conexión SSH en el puerto 22 al servidor SSH, `other.example.com`. Luego, `other.example.com` se conecta al puerto 110 en `mail.example.com` para verificar correo nuevo. Observe que usando esta técnica, sólo la conexión entre el sistema cliente y el servidor SSH `other.example.com` es segura.

El reenvío del puerto se puede usar para obtener información segura a través de los cortafuegos de red. Si el cortafuegos está configurado para permitir el tráfico SSH a través del puerto estándar (22) pero bloquea el acceso a través de otros puertos, es posible todavía una conexión entre dos hosts usando los puertos bloqueados al redireccionar la comunicación sobre una conexión SSH establecida.

Nota

Si se utiliza el reenvío de puerto para reenviar conexiones de este modo, cualquier usuario en el sistema cliente puede conectarse a ese servicio. Si el cliente está en riesgo o está comprometido, un agresor puede también acceder a los servicios reenviados.

Los administradores de sistemas pueden desactivar la funcionalidad de reenvío de puerto en el servidor si especifican `No` en la línea `AllowTcpForwarding` en `/etc/ssh/sshd_config`. El servicio `sshd` debe ser reiniciado después de esta modificación.

7.3. 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 de OpenSSH, `~/.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 Enterprise Linux 5.0.0 utiliza el protocolo 2 de SSH y llaves RSA por defecto.

Sugerencia

Si reinstala y quiere guardar los pares de llaves 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.

7.3.1. 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 intérprete de comandos de la shell:

   ```
   ssh-keygen -t rsa
   ```

   Acepte la localización por defecto del archivo `~/.ssh/id_rsa`. Introduzca una contraseña 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 siguiente:

   ```
   chmod 755 ~/.ssh
   ```

3. Copie los contenidos de `~/.ssh/id_rsa.pub` al archivo `~/.ssh/authorized_keys` en la máquina en la que se quiere conectar. Si el archivo `~/.ssh/authorized_keys` existe, puede añadir los contenidos del archivo `~/.ssh/id_rsa.pub` al archivo `~/.ssh/authorized_keys` en la otra máquina.

4. Cambie los permisos del archivo `authorized_keys` usando el comando siguiente:

   ```
   chmod 644 ~/.ssh/authorized_keys
   ```

5. Si está ejecutando GNOME o está ejecutando un escritorio gráfico con las bibliotecas GTK2+, vaya a la Sección 7.3.4, “Configurando ssh-agent con una interfaz gráfica”. Si no está ejecutando el sistema de ventanas X, vaya a la Sección 7.3.5, “Configuración de ssh-agent”.

7.3.2. 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 frase secreta diferente a la contraseña de su cuenta y confirme ésta introduciéndola de nuevo.

   ### Sugerencia

   Una frase secreta es una cadena de caracteres o palabras utilizadas para autentificar a un usuario. Las frases secretas se diferencian de las contraseñas en que se pueden utilizar espacios o tabuladores en la primera. Las frases secretas son generalmente más largas que las contraseñas porque ellas son habitualmente frases. Algunas veces estos dos términos se usan indistintamente.

   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 siguiente:

   ```
   chmod 755 ~/.ssh
   ```

3. Copie los contenidos de `~/.ssh/id_dsa.pub` a `~/.ssh/authorized_keys` en la máquina a la cual quiere conectarse. Si el archivo `~/.ssh/authorized_keys` existe, añada los contenidos del archivo `~/.ssh/id_dsa.pub` al archivo `~/.ssh/authorized_keys` en la otra máquina.

4. Cambie los permisos del archivo `authorized_keys` usando el comando siguiente:

   ```
   chmod 644 ~/.ssh/authorized_keys
   ```

5. Si está ejecutando GNOME o un entorno gráfico con las bibliotecas GTK2+ instaladas, vaya a la Sección 7.3.4, “Configurando ssh-agent con una interfaz gráfica”. Si no está ejecutando el sistema de ventanas X, vaya a la Sección 7.3.5, “Configuración de ssh-agent”.

7.3.3. 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 de la shell:

   ```
   ssh-keygen -t rsa1
   ```

   Acepte la localización por defecto del archivo (`~/.ssh/identity`). Introduzca una contraseña 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 copiar el archivo `~/.ssh/identity.pub` al archivo `~/.ssh/authorized_keys` en el equipo remoto.

4. Si está ejecutando GNOME, vaya a la Sección 7.3.4, “Configurando ssh-agent con una interfaz gráfica”. Si no está corriendo GNOME, salte a la Sección 7.3.5, “Configuración de ssh-agent”.

7.3.4. Configurando `ssh-agent` con una interfaz gráfica

La utilidad `ssh-agent` puede ser usada para guardar su contraseña, de manera que no tendrá que ingresarla cada vez que inicie una conexión `ssh` o `scp`. Si está usando GNOME, la utilidad `openssh-askpass` puede ser usada para pedirle la contraseña cuando inicie una conexión con GNOME y guardarla hasta que salga de GNOME. No tendrá que ingresar su contraseña para ninguna conexión `ssh` o `scp` realizada durante una sesión GNOME. Si no está usando GNOME consulte la Sección 7.3.5, “Configuración de ssh-agent”.

Para guardar su contraseña durante una sesión GNOME, siga los pasos siguientes:

1. Verifique que el paquete `openssh-askpass-gnome` esté instalado usando el comando `rpm -q openssh-askpass`. Si no está instalado, hágalo desde su conjunto de CDs de Red Hat Enterprise 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 clic 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 asegurarse 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 clic 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 frase secreta. Introduzca ésta. 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`.

7.3.5. Configuración de `ssh-agent`

`ssh-agent` se puede utilizar para almacenar su contraseña para que así no tenga que ingresarlas cada vez que realice una conexión `ssh` o `scp`. Si no está ejecutando el sistema de ventanas X, siga los pasos siguientes desde el intérprete de comandos de la shell. Si está ejecutando GNOME pero no quiere configurarlo para que le solicite la contraseña cuando se conecte (vea la Sección 7.3.4, “Configurando ssh-agent con una interfaz gráfica”), este procedimiento trabajará en una ventana de terminal como por ejemplo XTerm. Si está ejecutando X pero no GNOME, este procedimiento funcionará en una ventana de terminal. Sin embargo, su contraseña sólo será recordada en ese terminal; no es una configuración global.

1. Desde el intérprete 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 contraseña. Si tiene más de un par de claves configuradas, se le pedirá información para ambas.

3. Su contraseña será olvidada cuando termine la sesión. Debe ejecutar estos dos comandos cada vez que abra una consola virtual o abra una ventana de terminal.

8. Recursos adicionales

Los proyectos OpenSSH y OpenSSL están en constante desarrollo. 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.

8.1. Documentación instalada

- Páginas man 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.

8.2. Sitios web útiles

- http://www.openssh.com — La página de FAQ de OpenSSH, 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 6. Protocolo de Configuración Dinámica de Hosts (DHCP)

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red para asignar automáticamente información TCP/IP a equipos cliente. Cada cliente DHCP se conecta a un servidor DHCP centralizado que devuelve la configuración de red del cliente (incluyendo la dirección IP, la puerta de enlace y los servidores DNS).

1. Motivos para usar el protocolo DHCP

DHCP es útil para proporcionar de un modo rápido la configuración de la interfaz 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, una puerta de enlace o servidores 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 son hechos en el servidor DHCP, no en los clientes DHCP. Una vez que se reinicie la red en los clientes (o se reinicien los clientes), se aplicarán los cambios.

Si una organización tiene un servidor DHCP funcional conectado correctamente a una red, los usuarios de portátiles pueden mover estas máquinas de oficina a oficina.

2. Configuración de un servidor DHCP

Para configurar un servidor DHCP se debe crear el archivo de configuración `dhcpd.conf` en el directorio `/etc/`. Se puede encontrar un archivo de ejemplo en `/usr/share/doc/dhcp-<version>/dhcpd.conf.sample`.

DHCP también usa el archivo `/var/lib/dhcp/dhcpd.leases` para almacenar la base de datos de arrendamiento de clientes. Consulte la Sección 2.2, “Base de datos de arrendamiento” para más información.

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 para los clientes. Utilice este archivo para declarar opciones, globales o no, para los sistemas clientes.

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. Las líneas que empiezan con una almohadilla o símbolo numeral (#) se consideran comentarios.

Hay dos tipos de esquemas de actualización DNS implementados actualmente — el modo de

actualización DNS ad-hoc y el modo de actualización intermedio de boceto 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 esquemas actuales. La versión 3.0b2pl11 y las versiones anteriores usaban el modo ad-hoc, el cual no es utilizado en la actualidad. Si quiere conservar el mismo comportamiento, añada la siguiente línea al inicio del archivo de configuración:

```
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 ésta se debe llevar a cabo 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.

Los parámetros que inician con la palabra clave `option` son conocidos como *opciones*. Estas opciones controlan las opciones de DHCP mientras que los parámetros configuran valores que no son 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`.

Sugerencia

En vez de cambiar un archivo de configuración DHCP y reiniciar el equipo cada vez, el comando `omshell` proporciona una manera interactiva de conectarse, preguntar y cambiar la configuración de un servidor DHCP. Al utilizar `omshell`, todos los cambios pueden realizarse mientras el servidor está en ejecución. Para obtener mayor información sobre `omshell`, consulte la página man `omshell`.

En el Ejemplo 6.1, “Ejemplo de declaración de Subred”, las opciones `routers`, `subnet-mask`, `domain-name`, `domain-name-servers`, y `time-offset` son usadas para cualquier sentencia `host` declarada debajo de ellas.

Adicionalmente, se puede declarar una `subnet`. Debe incluir una declaración `subnet` para cada subred en la red. Si no lo hace, el servidor DHCP no podrá ser iniciado.

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 6.1. 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 el Ejemplo 6.2, “Ejemplo de declaración de red compartida”. 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                  192.168.0.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.252.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.254;
    }
    subnet 192.168.2.0 netmask 255.255.252.0 {
        parameters for subnet
        range 192.168.2.1 192.168.2.254;
    }
}
```

Ejemplo 6.2. Ejemplo de declaración de red compartida

Como se muestra en el Ejemplo 6.3, “Declaración de Group”, la declaración `group` puede utilizarse para aplicar parámetros globales a un grupo de declaraciones. Por ejemplo, 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 6.3. Declaración de Group

Para configurar un servidor DHCP que arrienda una dirección IP dinámica a un sistema dentro de una subred, modifique el Ejemplo 6.4, “Parámetro Range (Rango)” con sus valores. Así se 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 6.4. 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 6.5, “Ejemplo de dirección IP estática con DHCP”, 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 6.5. Ejemplo de dirección IP estática con DHCP

Sugerencia

Puede usar el archivo de configuración de ejemplo proporcionado como punto de partida y, a continuación, agregarle opciones de configuración personalizadas. Para copiar el archivo en la ubicación adecuada, use 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`.

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 el Tiempo Universal Coordinado (UTC por sus siglas en inglés), no con la hora local.

Cada cierto tiempo, la base de datos de arrendamiento es nuevamente creada para controlar su tamaño. 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 podría ser terminado o el sistema puede fallar después de que la base de datos ha sido renombrada al archivo de copia de seguridad pero antes de que el nuevo archivo haya sido escrito. Si ocurre esto, el archivo `dhcpd.leases` no existirá a pesar de ser requerido para arrancar el servicio. No cree un nuevo archivo de arrendamiento si esto ocurre. Si lo hace, se perderán las versiones anteriores del arrendamiento y podrían generarse muchos 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.

2.3. Iniciar y detener el servidor

Importante

Cuando el servidor DHCP arranca por primera vez, fallará si no existe un archivo `dhcpd.leases`. Use el comando `touch /var/lib/dhcp/dhcpd.leases` para crear el archivo en caso de que no exista.

Si el mismo servidor está utilizando BIND con servidor DNS, este paso no será necesario, ya que al iniciar el servicio `named` se revisa automáticamente la existencia del archivo `dhcpd.leases`.

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 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`:

```
# Opciones de línea de comandos
DHCPDARGS=eth0
```

Esto es útil si tiene una máquina cortafuegos 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 cortafuegos. Su sistema será más seguro si sólo 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 cual `dhcpd` debería escuchar. El puerto predeterminado es el 67. El servidor DHCP transmite las respuestas al cliente DHCP a un puerto con un número más grande que el puerto UDP especificado. Por ejemplo, si se usa el puerto predeterminado, el servidor escucha peticiones en el puerto 67 y responde al cliente en el puerto 68. Si especifica un puerto en este momento y usa el agente de transmisión DHCP, se debería especificar el mismo puerto en el que el agente DHCP debería escuchar. Consulte la Sección 2.4, “Agente de transmisión DHCP” para más detalles.
- `-f` — Ejecuta el demonio como un proceso en primer plano. Casi siempre se usa para la depuración.
- `-d` — Registra 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 ubicación por defecto es `/etc/dhcpd.conf`.
- `-lf <filename>` — Especifica la ubicación de la base de datos de arrendamiento. Si ya exis-

te 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.

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 a uno o más servidores DHCP 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`.

3. Configuración de un cliente DHCP

Para configurar un cliente DHCP manualmente, debe modificar el archivo `/etc/sysconfig/network` para habilitar redes y el uso del archivo de configuración para cada dispositivo de red en el 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
```

Si quiere que se inicie la red en el momento de arranque debe asegurarse de que la variable `NETWORKING` sea `yes`.

El archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` debería contener las líneas siguientes:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Necesita un archivo de configuración para cada dispositivo que desee configurar para el uso de DHCP.

Otras opciones para el script de la red incluyen:

- `DHCP_HOSTNAME` — Utilice esta opción solamente si el servidor DHCP requiere que el cliente especifique un nombre de host antes de recibir una dirección IP. (El demonio del servidor DHCP en Red Hat Enterprise Linux no soporta esta característica.)

- `PEERDNS=<answer>`, donde `<answer>` es uno de los siguientes:
  - `yes` — Modifica `/etc/resolv.conf` con información desde el servidor. Si se está usando DHCP, entonces `yes` es el valor por defecto.
  - `no` — No modifica `/etc/resolv.conf`.
- `SRCADDR=<address>`, donde `<address>` es la dirección IP fuente especificada para los paquetes salientes.
- `USERCTL=<answer>`, donde `<answer>` es uno de los siguientes:
  - `yes` — Los usuarios que no sean root pueden modificar este dispositivo.
  - `no` — Los usuarios no root no tienen derecho a controlar este dispositivo.

Si prefiere usar una interfaz gráfica, consulte el Capítulo 2, *Configuración de la red* para obtener más información sobre la **Herramienta de administración de red** para configurar la interfaz de red para usar DHCP.

Sugerencia

Para configurar opciones avanzadas de clientes DHCP tal como tiempo del protocolo, requerimientos y peticiones de asignación, soporte dinámico DNS, aliases y una amplia gama de valores para sobreescribir o añadir a la configuración del lado del cliente, consulte `dhclient` y las páginas man de `dhclient.conf`

4. Recursos adicionales

Para obtener mayor información sobre otras opciones, consulte los recursos siguientes.

4.1. Documentación instalada

- La página del manual `dhcpd` — describe cómo funciona el demonio DHCP
- La página del manual `dhcpd.conf` — explica cómo configurar el archivo de configuración de DHCP; incluye algunos ejemplos.
- La página del manual `dhcpd.leases` — explica cómo configurar el archivo de arrendamiento DHCP; incluye también algunos ejemplos.
- La página del manual `dhcp-options` — explica la sintaxis para la declaración de opciones DHCP en `dhcpd.conf`; incluye ejemplos.
- La página del manual `dhcrelay` — explica el Agente de transmisión DHCP y sus opciones de configuración.
- `/usr/share/doc/dhcp-<version>/` — Contiene archivos de ejemplo, archivos README y las

notas de lanzamiento para la versión específica del servicio DHCP.

Capítulo 7. Servidor HTTP Apache

El Servidor HTTP Apache es un servidor Web de tecnología Open Source sólido y para uso comercial desarrollado por Apache Software Foundation (http://www.apache.org/). Red Hat Enterprise Linux incluye el Servidor HTTP Apache versión 2.2 así como también una serie de módulos de servidor diseñados para mejorar su funcionalidad.

El archivo de configuración predeterminado instalado en el Servidor HTTP Apache funciona sin necesidad de modificarlo, en la mayor parte de los casos. Este capítulo da una idea general de las directrices dentro de este archivo de configuración (`/etc/httpd/conf/httpd.conf`) para ayudar a aquellos que requieren una configuración personalizada o que necesitan convertir un archivo de configuración del formato más antiguo del Servidor HTTP Apache versión 1.3.

Advertencia

Si utiliza la **Herramienta de configuración HTTP** (*system-config-httpd*), *no* cambie el archivo de configuración del Servidor Apache HTTP manualmente porque la **Herramienta de configuración HTTP** vuelve a generar este archivo cada vez que se usa.

1. Servidor HTTP Apache Versión 2.2

Existen diferencias importantes entre el Servidor HTTP Apache Versión 2.2 y la versión 2.0 (la versión 2.0 incluida con Red Hat Enterprise Linux 4 y las versiones anteriores). Esta sección revisa algunas de las características del Servidor HTTP Apache Versión 2.2 y esboza los cambios principales. Si necesita actualizar desde la versión 1.3 también debe leer las instrucciones sobre como migrar desde la versión 1.3 a la 2.0. Para obtener las instrucciones sobre como migrar un archivo de configuración versión 1.3 al formato 2.0 refiérase a Sección 2.2, “Migración de los Archivos de Configuración del Servidor HTTP Apache de la Versión 1.3 a la 2.0”.

1.1. Características del Servidor HTTP Apache Versión 2.2

El Servidor HTTP Apache Versión 2.2 presenta las siguientes mejoras sobre las versión 2.0:

- Módulos de cacheo mejorados (mod_cache, mod_disk_cache, mod_mem_cache).
- Una nueva estructura para el soporte de autenticación y autorización que remplaza los módulos de autenticación proporcionados en las versiones anteriores.
- Soporte para balanceo de carga proxy (mod_proxy_balancer)
- soporte para manejo de archivos grandes (más grandes de 2 GB) en plataformas de 32 bits.

Se han realizado los siguientes cambios a la configuración httpd predeterminada:

- Los módulos mod_cern_meta y mod_asis ya no se cargan por defecto.

- Ahora el módulo mod_ext_filter se carga por defecto.

Si actualiza desde un lanzamiento previo de Red Hat Enterprise Linux, la configuración httpd necesitará actualizarse para httpd 2.2. Para obtener más información refiérase a http://httpd.apache.org/docs/2.2/upgrading.html.

2. Migración de los Archivos de Configuración del Servidor HTTP Apache

2.1. Migración de los Archivos de Configuración del Servidor HTTP Apache Versión 2.0.

Esta sección esboza la migración desde la versión 2.0 a la 2.2. Si está migrando desde la versión 1.3 por favor refiérase a Sección 2.2, “Migración de los Archivos de Configuración del Servidor HTTP Apache de la Versión 1.3 a la 2.0”.

- Los archivos de configuración y los scripts de inicialización de la versión 2.0 necesitan ajustes mínimos particularmente en los nombres de los módulos los cuales pueden haber cambiado. Los módulos de terceros que servían en la versión 2.0 también sirven en la versión 2.2 pero necesitan ser recompilados antes de que los cargue. Los módulos claves que se deben observar son los módulos de autenticación y autorización. Para cada unos de los módulos que ha sido renombrado será necesario actualizar la línea `LoadModule` [http://httpd.apache.org/docs/2.2/mod/mod_so.html#loadmodule].

- El módulo `mod_userdir` sólamente actuará bajo pedidos si proporciona una directiva `UserDir` indicando un nombre de directorio. Si desea mantener los procedimientos utilizados en la versión 2.0 añada la directiva `UserDir public_html` en su archivo de configuración.

- Para habilitar SSL, edite el archivo `httpd.conf` añadiendo las directivas necesarias `mod_ssl`. Utilice `apachectl start` ya que `apachectl startssl` no se encuentra disponible en la versión 2.2. Puede ver un ejemplo de la configuración SSL para httpd en `conf/extra/httpd-ssl.conf`.

- Para probar su configuración se le aconseja que utilice `service httpd configtest` la cual detectará errores de configuración.

Para obtener más información sobre como actualizar desde la versión 2.0 a la 2.2 puede ir a http://httpd.apache.org/docs/2.2/upgrading.html.

2.2. Migración de los Archivos de Configuración del Servidor HTTP Apache de la Versión 1.3 a la 2.0

Esta sección detalla la migración de un archivo de configuración del Servidor HTTP Apache versión 1.3 para el Servidor HTTP Apache versión 2.0 lo pueda utilizar.

Si está actualizando a Red Hat Enterprise Linux 5 desde Red Hat Enterprise Linux 2.1 tenga en cuenta que el nuevo archivo de configuración para el paquete del Servidor HTTP Apache versión 2.0 es instalado como `/etc/httpd/conf/httpd.conf.rpmnew` y no se toca la versión original

1.3 `httpd.conf`. Depende absolutamente de usted si decide utilizar el nuevo archivo de configuración y migrar los viejos cambios o si utilizar el archivo ya existente como base y modificarlo para que se adapte; sin embargo, algunas partes del archivo se han cambiado más que otras y lo mejor es llegar a un punto intermedio. Los archivos de configuración para ambas versiones la 1.3 y la 2.0 están divididos en tres secciones.

Si el archivo `/etc/httpd/conf/httpd.conf` es una versión modificada de la versión por defecto recién instalada y ha guardado una copia del original, entonces le será más fácil invocar el comando `diff`, como se muestra a continuación (conectándose como root):

```
diff -u httpd.conf.orig httpd.conf | less
```

Este comando subraya los cambios realizados. Si no tiene una copia del archivo original, cójalo del paquete RPM usando los comandos `rpm2cpio` y `cpio`, como en el ejemplo siguiente:

```
rpm2cpio apache-<version-number>.i386.rpm | cpio -i --make
```

En el comando de arriba, sustituya `<version-number>` con el número de versión para el paquete `apache`.

Finalmente, es útil saber que el Servidor HTTP Apache tiene un modo de prueba para verificar si hay errores en la configuración. Para ello, escriba el siguiente comando:

```
apachectl configtest
```

2.2.1. Configuración del entorno a nivel global

La sección del entorno global del archivo de configuración contiene directrices que afectan la operación general del Servidor HTTP Apache como por ejemplo el número de peticiones que puede manejar al mismo tiempo y la ubicación de varios archivos que usa. Esta sección requiere un gran número de cambios y por ello se recomienda que base esta sección en el archivo de configuración del Servidor HTTP Apache versión 2.0 y que migre sus configuraciones anteriores a este.

2.2.1.1. Interfaces y vinculación de puertos

Ya no existen las directrices `BindAddress` y `Port`; porque quedan recogidas en la directriz `Listen`.

Si tenía configurado el `Puerto 80` en el archivo de configuración de la versión 1.3, debe cambiarlo a `Listen 80` en el archivo de configuración 2.0. Si el valor del `Puerto` estaba configurado a un valor *diferente que 80*, tiene que poner el número del puerto a los contenidos de la directriz `ServerName`.

Por ejemplo, el siguiente es un ejemplo de la directtriz de Servidor HTTP Apache de la versión 1.3:

```
Port 123 ServerName www.example.com
```

Para migrar esta configuración al Servidor HTTP Apache versión 2.0 utilice la siguiente estructura:

```
Listen 123 ServerName www.example.com:123
```

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

2.2.1.2. Regulación del tamaño del pool de servidores

Cuando el Servidor HTTP Apache acepta peticiones, este despacha procesos hijo o hilos para que los manejen. Este grupo de procesos o hilos es conocido como un *pool de servidores*. Bajo el Servidor HTTP Apache versión 2.0 se ha abstraído la responsabilidad de crear y mantener estos pool de servidores a un grupo de módulos llamados *Módulos de Procesos Múltiples* (*MPMs*). A diferencia de otros módulos, el Servidor HTTP Apache sólamente puede cargar un módulo del grupo MPM. Hay tres módulos MPM incluidos con la versión 2.0: `prefork`, `worker`, y `perchild`. Actualmente, únicamente están disponibles los MPMs `prefork` y `worker`, aunque el MPM `perchild` estará disponible más adelante.

El comportamiento del Servidor HTTP Apache 1.3 original ha sido movido al MPM `prefork`. El MPM `prefork` acepta las mismas directrices que el Servidor HTTP Apache versión 1.3 por tanto, las siguientes directrices se pueden migrar directamente:

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

El MPM `worker` implementa un servidor multi-proceso y multi-hilos proporcionando una mayor escalabilidad. Cuando este utilizando este MPM, los hilos manejan las peticiones conservando recursos del sistema y permitiendo servir a grandes números de peticiones de manera eficiente. Aún cuando algunas de las directrices aceptadas por el MPM `worker` son las mismas que aquellas aceptadas por el MPM `prefork` los valores para esas directrices no deberían ser transferidos directamente desde una instalación del Servidor HTTP Apache versión 1.3. Es mejor utilizar los valores por defecto como una guía y luego experimentar para determinar los valores que funcionan mejor.

Importante

Para utilizar el MPM `worker`, cree el archivo `/etc/sysconfig/httpd` y añada la directriz siguiente:

```
HTTPD=/usr/sbin/httpd.worker
```

Para mayor información sobre el tema de MPMs, consulte la documentación siguiente en el sitio web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mpm.html

2.2.1.3. Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)

Se tienen que realizar muchos cambios aquí, por eso se recomienda que para modificar la configuración del Servidor HTTP Apache 1.3 para adaptarse a la versión 2.0 (al contrario de migrar los cambios en la configuración de la versión 2.0) copie esta sección del archivo de configuración del Servidor HTTP Apache 2.0.

Aquellos que no deseen copiar la sección desde la configuración del Servidor HTTP Apache versión 2.0 deberían tomar en cuenta lo siguiente:

- Las directrices `AddModule` y `ClearModuleList` ya no existen. Estas directrices eran usadas para asegurarse de que se pudiesen activar los módulos en el orden correcto. El Servidor HTTP Apache versión 2.0 permite a los módulos especificar su orden, eliminando la necesidad de estas dos directrices.
- El orden de las líneas `LoadModule` ya no es relevante en la mayoría de los casos.
- Se han añadido muchos módulos, otros han sido eliminados, renombrado, dividido o incorporados con otros.
- Ya no son necesarias las líneas `LoadModule` para los módulos empaquetados en sus propios RPMs (`mod_ssl`, `php`, `mod_perl` y similares) ya que se pueden encontrar en sus archivos relevantes dentro del directorio `/etc/httpd/conf.d/`.
- Las definiciones `HAVE_XXX` ya no existen.

Importante

Si se está modificando el archivo original, por favor tenga en cuenta que es de suma importancia que `httpd.conf` contenga la directriz siguiente:

```
Include conf.d/*.conf
```

La omisión de esta directriz podría resultar en la falla de todos los módulos enpaquetados en sus propios RPMs (tales como `mod_perl`, `php` y `mod_ssl`).

2.2.1.4. Otros cambios en el entorno global

Se han eliminado las siguientes directrices de la configuración del Servidor HTTP Apache 2.0:

- *`ServerType`* — El Servidor HTTP Apache se puede ejecutar sólamente como `ServerType standalone` por lo que esta directriz es irrelevante.
- *`AccessConfig`* y *`ResourceConfig`* — Se han eliminado estas directrices porque su funcionalidad aparece ya en la directriz `Include`. Si las directrices `AccessConfig` y `ResourceConfig` son configuradas, entonces reemplácelas por las directrices `Include`.

Para asegurarse que estos archivos se lean en el orden de las antiguas directrices, las directrices `Include` se deberían colocar al final de `httpd.conf`, con la correspondiente a `ResourceConfig` precediendo la que corresponde a `AccessConfig`. Si se estan usando los valores por defecto, inclúyalos explícitamente como archivos `conf/srm.conf` y `conf/access.conf`.

2.2.2. Configuración del servidor principal

La sección de la configuración del servidor principal del archivo de configuración configura el servidor principal que responde a todas aquellas peticiones que no maneja un host virtual definido dentro de un contenedor `<VirtualHost>`. Los valores aquí también proporcionan valores por defecto para cualquier contenedor `<VirtualHost>` definido.

Las directrices utilizadas en esta sección han cambiado ligeramente respecto a las del Servidor HTTP Apache versión 1.3 y la versión 2.0. Si la configuración del servidor principal está altamente personalizada, le será más fácil modificar el archivo de configuración existente para que se adapte a la versión 2.0 del Servidor HTTP Apache. Los usuarios con secciones del servidor principal ligeramente personalizadas deberían migrar sus cambios al archivo de configuración 2.0 predeterminado.

2.2.2.1. Asignaciones `UserDir`

La directriz `UserDir` se usa para habilitar URLs tales como `http://example.com/~bob/` para mapear a un subdirectorio dentro del directorio home del usuario `bob` tal como `/home/bob/public_html/`. Un efecto secundario de esta característica es que un potencial atacante puede determinar si un nombre de usuario dado se encuentra en el sistema; por esta razón la configuración por defecto para el Servidor HTTP Apache desactiva esta directriz.

Para habilitar la asignación de `UserDir`, cambie la directriz en `httpd.conf` desde:

```
UserDir disable
```

a lo siguiente:

```
UserDir public_html
```

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir

2.2.2.2. Conexión

Se han eliminado las siguientes directrices de conexión:

- `AgentLog`
- `RefererLog`
- `RefererIgnore`

Sin embargo, las conexiones agent y referrer estan disponibles usando las directrices `CustomLog` y `LogFormat`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

2.2.2.3. Índice de directorios

Se ha eliminado la directriz `FancyIndexing`. La misma funcionalidad se encuentra ahora en `FancyIndexing`*option* dentro de la directriz `IndexOptions`.

La opción `VersionSort` para la directriz `IndexOptions` causa que los archivos conteniendo números de versiones sean ordenados de una forma más natural. Por ejemplo, `httpd-2.0.6.tar` aparece antes de `httpd-2.0.36.tar` en una página de índices de directorio.

Las directrices predeterminadas `ReadmeName` y `HeaderName` han sido cambiadas desde `README` y `HEADER` a `README.html` y `HEADER.html`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

2.2.2.4. Negociación de contenido

La directriz `CacheNegotiatedDocs` toma ahora el argumento `on` o `off`. Las instancias existentes de `CacheNegotiatedDocs` deberían ser cambiadas con `CacheNegotiatedDocs on`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

2.2.2.5. Documentos de error

Para utilizar un mensaje codificado con la directriz `ErrorDocument` el mensaje tiene que aparecer en un par de comillas dobles `"` en vez de estar simplemente precedido por las comillas como en el Servidor HTTP Apache 1.3.

Por ejemplo, el siguiente es un ejemplo de la directtriz de Servidor HTTP Apache de la versión 1.3:

```
ErrorDocument 404 "The document was not found
```

Para migrar la configuración de `ErrorDocument` al Servidor HTTP Apache versión 2.0, utilice la siguiente estructura:

```
ErrorDocument 404 "The document was not found"
```

Observe las dobles comillas en la directriz `ErrorDocument` del ejemplo anterior.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

2.2.3. Configuración de host virtuales

Los contenidos de todos los contenedores `<VirtualHost>` se deben migrar de la misma manera que en la sección del servidor principal como se describió en Sección 2.2.2, “Configuración del servidor principal”.

Importante

Observe que la configuración de las máquinas virtuales SSL/TLS se han quitado del archivo de configuración del servidor principal al archivo `/etc/httpd/conf.d/ssl.conf`.

- http://httpd.apache.org/docs-2.0/vhosts/

2.2.4. Módulos y el Servidor HTTP Apache 2.0

En la versión 2.0 del Servidor HTTP Apache el sistema de módulos se ha cambiado para permitir que los módulos se encadenen o se combinen en maneras nuevas e interesantes. Los scripts CGI (*Common Gateway Interface*), por ejemplo, pueden generar documentos HTML interpretados por el servidor que luego pueden ser procesados por `mod_include`. Esto abre una gran cantidad de posibilidades en lo que se refiere a cómo los módulos pueden combinarse para lograr una meta determinada.

La forma en que esto funciona es que cada petición es servida por exáctamente un módulo *handler* seguido por cero o más módulos *filtro*.

Bajo el Servidor HTTP Apache 1.3, por ejemplo, un script Perl es manejado completamente por el módulo Perl (`mod_include`). En la versión 2.0 del Servidor HTTP Apache la petición la *gestiona* inicialmente el módulo principal — que sirve archivos estáticos — y que es luego *filtrado* por `mod_perl`.

Exactamente cómo utilizar esto y otras de las nuevas características del Servidor HTTP Apache 2.0, están más allá del alcance de este documento; sin embargo, el cambio tiene ramificaciones si ha usado la directriz `PATH_INFO` para un documento que es gestionado por un módulo que ahora se implementa como un filtro, pues cada uno contiene información del recorrido del nombre del archivo verdadero. El módulo principal, que inicialmente manejaba la petición, no entiende por defecto `PATH_INFO` y devuelve el error `404 Not Found` para las peticiones que contienen dicha información. Como alternativa puede utilizar la directriz `AcceptPathInfo` para obligar al módulo principal a que acepte peticiones con `PATH_INFO`.

A continuación se presenta un ejemplo de esta directriz:

```
AcceptPathInfo on
```

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

2.2.4.1. El módulo `suexec`

En el Servidor HTTP Apache 2.0, el módulo `mod_suexec` utiliza la directriz `SuexecUserGroup` en vez de las directrices `User` y `Group`, la cual se utiliza para configurar hosts virtuales. Las directrices `User` y `Group` también se pueden utilizar en general, pero no para la configuración de hosts virtuales.

Por ejemplo, el siguiente es un ejemplo de la directtriz de Servidor HTTP Apache de la versión 1.3:

```
<VirtualHost vhost.example.com:80> User someone Group somegroup </VirtualHost>
```

Para migrar esta configuración al Servidor HTTP Apache versión 2.0 utilice la siguiente estructura:

```
<VirtualHost vhost.example.com:80> SuexecUserGroup someone somegroup </VirtualHost>
```

2.2.4.2. El módulo `mod_ssl`

La configuración para `mod_ssl` se ha cambiado desde `httpd.conf` al archivo `/etc/httpd/conf.d/ssl.conf`. Para cargar este archivo y hacer que `mod_ssl` funcione, tiene que tener la declaración `Include conf.d/*.conf` en `httpd.conf` como se describe en la Sección 2.2.1.3, “Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)”.

Las directrices `ServerName` en las máquinas virtuales SSL tienen que especificar el número del puerto.

Por ejemplo, el siguiente es un ejemplo de la directtriz de Servidor HTTP Apache de la versión 1.3:

```
<VirtualHost _default_:443> # General setup for the virtual host ServerName ssl.example.name ... </VirtualH
```

Para migrar esta configuración al Servidor HTTP Apache versión 2.0 utilice la siguiente estructura:

```
<VirtualHost _default_:443> # General setup for the virtual host ServerName ssl.host.name:443 ... </Virtua
```

También es importante tener en cuenta que ambas directrices `SSLLog` y `SSLLogLevel` han sido eliminadas. El módulo `mod_ssl` obedece las directrices `ErrorLog` y `LogLevel` . Para más información sobre estas directrices, consulte la ErrorLog y LogLevel

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

- http://httpd.apache.org/docs-2.0/vhosts/

2.2.4.3. El módulo `mod_proxy`

Las declaraciones de control del acceso proxy se encuentran ahora en el bloque `<Proxy>` en vez de en `<Directory proxy:>`.

La funcionalidad de caché del antiguo `mod_proxy` se ha dividido en tres módulos siguientes:

- `mod_cache`
- `mod_disk_cache`
- `mod_mem_cache`

Estos generalmente usan directrices similares a las versiones anteriores del módulo `mod_proxy`, pero se recomienda que verifique cada directriz antes de migrar cualquier configuración caché.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

2.2.4.4. El módulo `mod_include`

El módulo `mod_include` ahora es implementado como un filtro y por lo tanto se activa de una forma diferente. Consulte la Sección 2.2.4, “Módulos y el Servidor HTTP Apache 2.0” para obtener más información sobre filtros.

Por ejemplo, el siguiente es un ejemplo de la directtriz de Servidor HTTP Apache de la versión 1.3:

```
AddType text/html .shtml AddHandler server-parsed .shtml
```

Para migrar esta configuración al Servidor HTTP Apache versión 2.0 utilice la siguiente estructura:

```
AddType text/html .shtml AddOutputFilter INCLUDES .shtml
```

Observe que la directriz `Options +Includes` aún es requerida para el contenedor `<Directory>` o en el archivo `.htaccess`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

2.2.4.5. Los módulos `mod_auth_dbm` y `mod_auth_db`

El Servidor HTTP Apache 1.3 soportaba dos módulos de autenticación, `mod_auth_db` y `mod_auth_dbm` que usaba las bases de datos Berkeley y DBM respectivamente. Estos módulos se han combinado en un único módulo que se llama `mod_auth_dbm` en el Servidor HTTP Apache 2.0, que puede acceder a diferentes formatos de bases de datos. Para migrar desde `mod_auth_db` los archivos de configuración se tienen que ajustar reemplazando `AuthDBUserFile` y

`AuthDBGroupFile` con los equivalentes: `AuthDBMUserFile` y `AuthDBMGroupFile`. También, se debe añadir la directriz `AuthDBMType DB` para indicar el tipo de archivo de base de datos en uso.

El siguiente ejemplo muestra una configuración `mod_auth_db` de ejemplo para el Servidor HTTP Apache 1.3:

```
<Location /private/> AuthType Basic AuthName "My Private Files" AuthDBUserFile /var/www/authdb require val
```

Para migrar esta configuración a la versión 2.0 del Servidor HTTP Apache 2.0 utilice la siguiente estructura:

```
<Location /private/> AuthType Basic AuthName "My Private Files" AuthDBMUserFile /var/www/authdb AuthDBMTyp
```

Observe que la directriz `AuthDBMUserFile` también puede ser usada en archivos `.htaccess`.

El script Perl `dbmmanage` que se utiliza para manipular bases de datos de nombres de usuarios y contraseñas ha sido reemplazado por `htdbm` en el Servidor HTTP Apache 2.0. El programa `htdbm` ofrece una funcionalidad equivalente y como `mod_auth_dbm` puede operar en una variedad de formatos de bases de datos; la opción `-T` se puede usar en la línea de comandos para especificar el formato a utilizar.

Tabla 7.1, “Migración del dbmmanage a htdbm” muestra cómo migrar desde un formato de base de datos DBM al formato `htdbm` utilizando g `dbmmanage`.

Acción	comando dbmmanage (1.3)	comando equivalente htdbm (2.0)
Añade un usuario a la base de datos (usando la contraseña dada)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Añade un usuario a la base de datos (le pide la contraseña)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Eliminar el usuario de la base de datos	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Listar usuarios en la base de datos	`dbmmanage authdb view`	`htdbm -l -TDB authdb`
Verificar una contraseña	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tabla 7.1. Migración del `dbmmanage` a `htdbm`

Las opciones `-m` y `-s` trabajan con `dbmmanage` y con `htdbm`, permitiendo el uso de los algortimos MD5 o SHA1 para las contraseñas hashing, respectivamente.

Cuando cree una nueva base de datos con `htdbm`, use la opción `-c`.

Para mayor información, consulte los siguientes sitios web de la Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

2.2.4.6. El módulo `mod_perl`

La configuración para `mod_perl` se ha pasado del `httpd.conf` al archivo `/etc/httpd/conf.d/perl.conf`. Para cargar este archivo, y hacer funcionar `mod_perl` se debe incluir la declaración `Include conf.d/*.conf` en el `httpd.conf` como se describe en la Sección 2.2.1.3, “Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)”.

Las ocurrencias del `Apache::` en el `httpd.conf` tienen que ser sustituídas por `ModPerl::`. Además, se ha cambiado el modo en que se registran los manejadores.

Ejemplo de configuración del Servidor HTTP Apache 1.3 `mod_perl`:

```
<Directory /var/www/perl> SetHandler perl-script PerlHandler Apache::Registry Options +ExecCGI </Directory>
```

Este es el equivalente del `mod_perl` para el Servidor HTTP Apache 2.0:

```
<Directory /var/www/perl> SetHandler perl-script PerlResponseHandler ModPerl::Registry Options +ExecCGI </
```

La mayoría de los módulos para `mod_perl` 1.x deberían funcionar sin modificación con los módulos `mod_perl` 2.x. Los módulos XS requieren recompilación y quizás algunas modificaciones menores de Makefile.

2.2.4.7. El módulo `mod_python`

La configuración para `mod_python` ha sido movida desde `httpd.conf` al archivo `/etc/httpd/conf.d/python.conf`. Para que se cargue este archivo y por lo tanto para que funcione `mod_python` se debe incluir la declaración `Include conf.d/*.conf` en el `httpd.conf` como se describe en la Sección 2.2.1.3, “Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)”.

2.2.4.8. PHP

La configuración del PHP ha sido movida de `httpd.conf` al archivo `/etc/httpd/conf.d/php.conf`. Para cargar este archivo, tiene que tener la declaración `Include conf.d/*.conf` en `httpd.conf` tal y como se describe en la Sección 2.2.1.3, “Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)”.

Nota

Cualquier directriz de configuración PHP utilizada en el Servidor HTTP Apache 1.3 ahora es completamente compatible cuando se migra al Servidor HTTP Apache 2.0 en Red Hat Enterprise Linux 5.

En PHP 4.2.0 y posterior, el conjunto predeterminado de variables predefinidas que están disponibles en el ámbito global, han cambiado. Las entradas individuales y las variables del servidor, por defecto, ya no se colocan directamente en el ámbito global. Este cambio puede hacer que se rompan los scripts. Cámbiese al antiguo comportamiento colocando `register_globals` a `On` en el archivo `/etc/php.ini`.

Para mayor información sobre estos temas, consulte los siguientes sitios web:

- http://www.php.net/release_4_1_0.php

2.2.4.9. El módulo `mod_authz_ldap`

Red Hat Enterprise Linux 5. se entrega con el módulo `mod_authz_ldap` para el Servidor HTTP Apache. Este módulo utiliza la forma corta del nombre distinguido para un sujeto y el emisor del certificado de cliente SSL para determinar el nombre distinguido de un usuario dentro de un directorio LDAP. También es capaz de autorizar usuarios basado en los atributos de esa entrada del usuario del directorio LDAP, determinando el acceso a los activos basado en los privilegios de usuario y de grupo de ese activo y negando el acceso a los usuarios con contraseñas caducadas. Se requiere el módulo `mod_ssl` cuando se utilice el módulo `mod_authz_ldap`.

Importante

El módulo `mod_authz_ldap` no valida un usuario a un directorio LDAP usando un hash de contraseña encriptada. Esta funcionalidad es proporcionada por el módulo experimental `mod_auth_ldap`. Consulte la documentación en línea de `mod_auth_ldap` en http://httpd.apache.org/docs-2.0/mod/mod_auth_ldap.html para más detalles sobre el estatus de este módulo.

El archivo `/etc/httpd/conf.d/authz_ldap.conf` configura al módulo `mod_authz_ldap`.

Consulte el `/usr/share/doc/mod_authz_ldap-<version>/index.html` (reemplazando `<version>` con el número de versión del paquete) o http://authzldap.othello.ch/ para más información sobre la configuración del módulo `mod_authz_ldap`.

3. Arrancar y detener `httpd`

Después de instalar el paquete `httpd` revise la documentación del Servidor HTTP Apache disponible en línea en http://httpd.apache.org/docs/2.2/.

El RPM de `httpd` instala el script `/etc/init.d/httpd`, el cual se puede acceder usando el comando `/sbin/service`.

Iniciando `httpd` utilizandoel script de control `apachectl` configura las variables del entorno en `/etc/sysconfig/httpd` e inicia `httpd`. También puede configurar las variables del entorno utilizando el script de inicialización.

Para arrancar el servidor utilizando el script de control `apachectl` como tipo root:

```
apachectl start
```

También puede arrancar `httpd` utilizando `/sbin/service httpd start`. Esto inicia `httpd` pero no configura las variables del entorno. Si está utilizando la directriz predeterminada `Listen` en `httpd.conf`, la cual es el puerto 80, necesitará contar con privilegios de usuario root para iniciar el servidor apache.

Para detener el servidor, como root escriba:

```
apachectl stop
```

También puede detener `httpd` utilizando `/sbin/service httpd stop`. La opción `restart` es una manera más rápida de detener y luego iniciar el Servidor HTTP Apache.

Para reiniciar el servidor como root escriba:

```
apachectl restart
or:/sbin/service httpd restart
```

Apache presentará un mensaje en la consola o en el `ErrorLog` si encuentra un error al iniciar.

Por defecto, el servicio `httpd`*no* inicia automáticamente al momento de arranque. Si quiere que Apache inicie al momento de arranque necesitará añadir una llamada a `apachectl` en sus archivos de inicalización dentro de su directorio `rc.local`. Un archivo que se utiliza típicamente es `rc.local`. Ya que esto inicia Apache como usuario root se recomienda que configure apropiadamente su seguridad y autenticación antes de añadir esta llamada.

También puede configurar el servicio `httpd` para iniciar en tiempo de arranque utilizando una herramienta script de inicialización tal como `/sbin/chkconfig`, **/usr/sbin/ntsysv**, o el programa **Services Configuration Tool**.

También puede visualizar el estado de su servidor httpd escribiendo:

```
apachectl status
```

Sin embargo, el módulo de estado `mod_status` necesita ser habilitado en su archivo de configuración `mod_status` para que esto funcione. Para obtener más detalles sobre `mod_status` vaya a http://httpd.apache.org/docs/2.2/mod/mod_status.html.

Nota

Si esta ejecutando el Servidor HTTP Apache como un servidor seguro, se le pedirá la contraseña del servidor seguro después de que la máquina arranca cuando se utilice una llave privada SSL encriptada.

Puede encontrar más información en http://httpd.apache.org/docs/2.2/ssl

4. Configuración del Servidor HTTP Apache

La **Herramienta de Configuración HTTP** le permite configurar el archivo de configuración `/etc/httpd/conf/httpd.conf` para el Servidor HTTP Apache. No utiliza los antiguos archivos de configuración `srm.conf` o `access.conf`, déjelos vacíos. Podrá configurar las directrices tales como hosts virtuales, atributos de registro y número máximo de conexiones a través de la interfaz gráfica. Para iniciar la Herramienta de Configuración HTTD haga clic en `System => Administration => Server Settings => HTTP`.

Sólo se pueden configurar con la **Herramienta de Configuración HTTP**aquellos módulos que estén incluídos con Red Hat Enterprise Linux. Si se instalan otros módulos, no se podrán configurar utilizando esta herramienta.

Advertencia

No modifique el archivo de configuración `/etc/httpd/conf/httpd.conf` manualmente si desea utilizar esta herramienta. La **Herramienta de Configuración HTTP** genera este archivo después de que haya grabado los cambios y haya salido del programa. Si desea añadir módulos u opciones de configuración que no se encuentran en la **Herramienta de Configuración HTTP** no podrá usarla.

Los pasos generales para configurar el Servidor HTTP Apache utilizando la **Herramienta de Configuración HTTP** son los siguientes:

1. Configure los aspectos básicos que se encuentran en la pestaña **Principal**
2. Haga clic en **Hosts Virtuales**y configure las opciones predeterminadas.
3. Bajo la pestaña **Hosts Virtuales** configure el Host Virtual Predeterminado.
4. Para servir más de una URL o más de un host virtual, añada cualquier host virtual adicional.
5. Configure las características del servidor bajo la pestaña **Servidor**.
6. Configure la configuración de las conexiones bajo la pestaña **Ajuste de Rendimiento**.
7. Copie todos los archivos necesarios a los directorios `DocumentRoot` y `cgi-bin`
8. Salga de la aplicación y seleccione guardar sus configuraciones.

4.1. Configuración Básica

Use la pestaña **Principal** para establecer las configuraciones básicas del servidor.

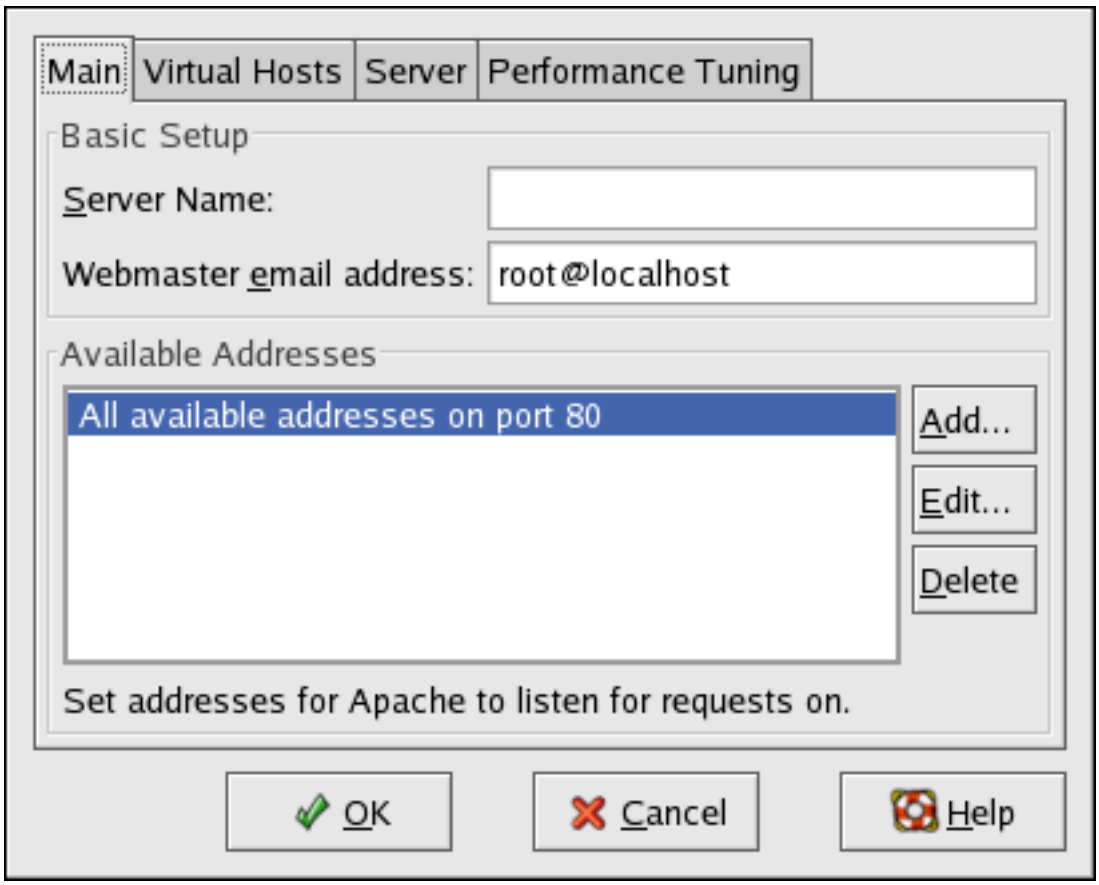


Figura 7.1. Configuración Básica

Ingrese un nombre de dominio completamente calificado al que tenga derecho de utilizar en el área de texto **Server Name**. Esta opción corresponde a la directriz `ServerName` [http://httpd.apache.org/docs/2.2/mod/core.html#servername] en `httpd.conf`. La directriz `ServerName` establece el nombre del host del servidor web. Se utiliza cuando se crea la redirecciém de URLs. Si no define un nombre de servidor, el servidor web intenta resolverlo desde la dirección IP del sistema. El nombre del servidor no tiene que ser el nombre del dominio resuelto desde la dirección IP del servidor. Por ejemplo, usted puede establecer el nombre del servidor como www.example.com mientras que el nombre DNS real del servidor es foo.example.com.

Ingrese la dirección de correo electrónico de la persona que mantiene el servidor web en el área de texto **Dirección de correo electrónico del webmaster**. Esta opción corresponde a la directriz `ServerAdmin` [http://httpd.apache.org/docs/2.2/mod/core.html#serveradmin] en `httpd.conf`. Si configura las páginas de error del servidor para que incluyan una dirección de correo electrónico, esta se utilizará para que los usuarios puedan reportar un problema al administrador del servidor. El valor predeterminado es root@localhost.

Utilice el área **Direcciones Disponibles** para definir los puertos en los que el servidor acepta pedidos entrantes. Esta opción corresponde a la directriz `Listen` [http://httpd.apache.org/docs/2.2/mod/mpm_common.html#listen] en `httpd.conf`. Por defecto, Red Hat configura el Servidor HTTP Apache para que escuche el puerto 80 para comunicaciones de web no seguras.

Haga clic en el botón **Añadir** para definir puertos adicionales sobre los cuales se aceptan pedidos. Aparecerá una ventana como lo muestra Figura 7.2, “Direcciones Disponibles”. Puede escoger la opción **Escuchar todas las direcciones** para escuchar a todas IP en el puerto definido o especificque una dirección IP en particular sobre la cual el servidor acepta las conexiones en el campo **Dirección**. Especifique sólamente una dirección IP por número de puerto. Para especificar más de una dirección IP con el mismo número de puerto cree una entrada para cada dirección IP. Si es posible utilice una dirección IP en vez de un nombre d edominio para evitar una falla de búsqueda DNS. Refiérase a http://httpd.apache.org/docs/2.2/dns-caveats.html para obtener más información sobre *Asuntos 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, seleccionela y haga clic en 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.

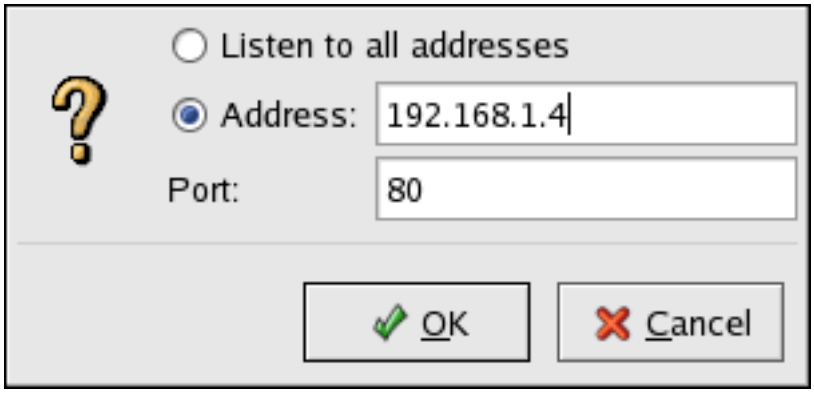


Figura 7.2. Direcciones Disponibles

4.2. Configuraciones predeterminadas

Después de definir el **Nombre del Servidor**, **Dirección de correo eletrónico del webmaster** y **Direcciones Disponibles** haga clic en la pestaña **Hosts Virtuales**. La figura a continuación ilustra la pestaña **Hosts Virtuales**.

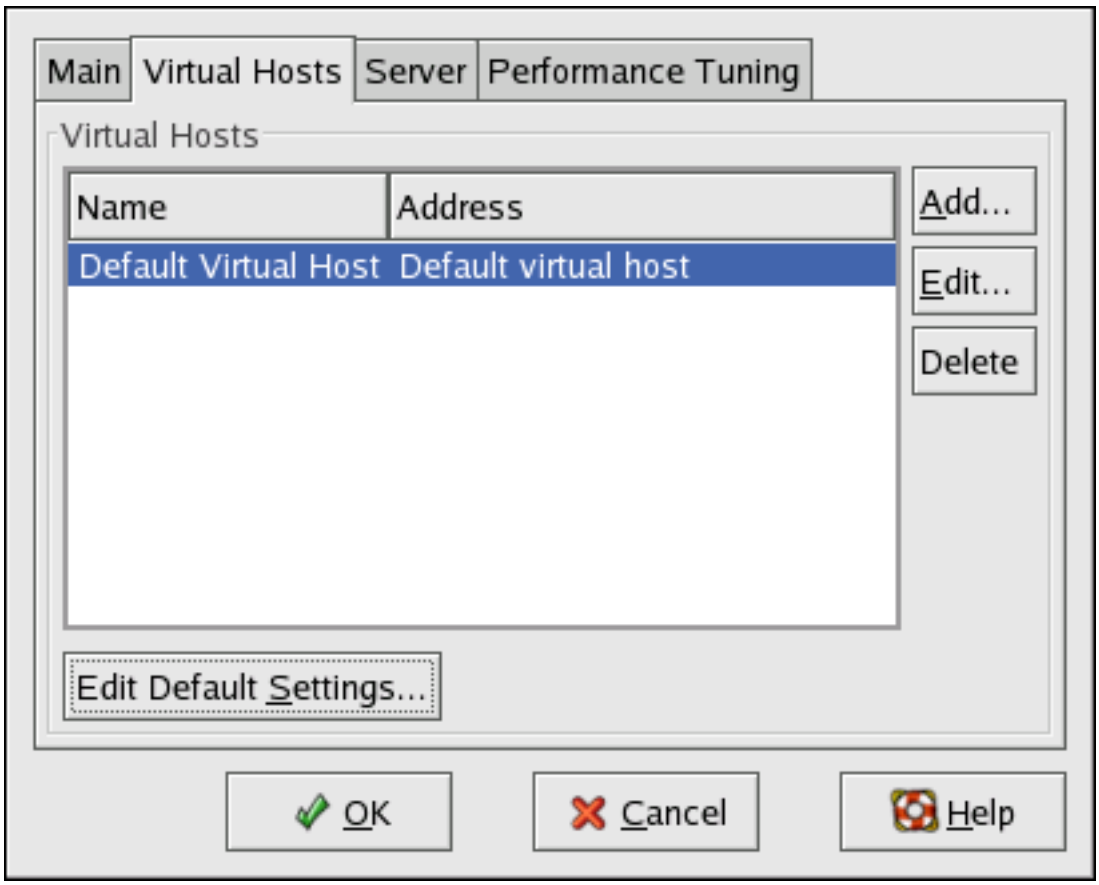


Figura 7.3. Pestaña Hosts Virtuales

Al hacer clic en **Modificar** presentará la ventana de las **Propiedades del Host Virtual** desde donde usted puede configurarlo como desee. Para añadir nuevas configuraciones haga clic en el botón **Añadir**, el cual también presentará la ventana **Propiedades del Host Virtual**. Al hacer clic en el botón **Modificar Configuración Predeterminada** aparecerá una ventana **Propiedades del Host Virtual** sin la pestaña **Opciones Generales**.

En la pestaña **Opciones Generales** puede cambiar el nombre del host, el directorio root del documento y también puede establecer la dirección de correo electrónico del webmaster. En la información del Host puede establecer la Dirección IP del Host Virtual y el Nombre del Host. La figura a continuación ilustra la pestaña **Opciones Generales**.

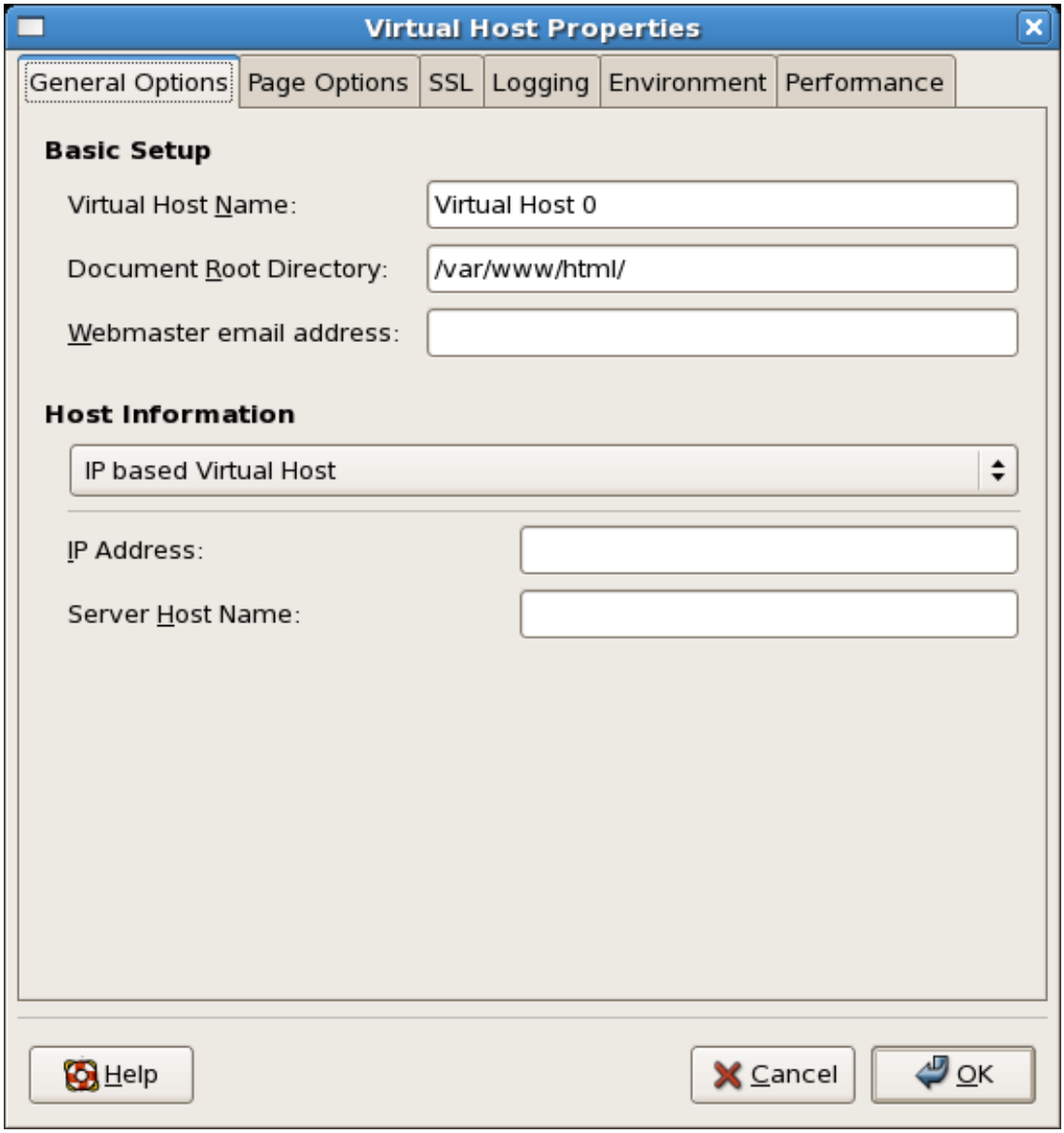


Figura 7.4. Opciones Generales

Si añade un host virtual, la configuración del host virtual tiene prioridad para ese host virtual. Para una directriz no definida dentro de la configuración del host virtual se utiliza el valor predeterminado.

4.2.1. Configuración del Sitio

La figura a continuación ilustra la pestaña **Opciones de Página** desde la cual puede configurar la **Lista de Páginas del Directorio** y **Páginas de Error**. Si no está seguro de esta configuración no la modifique.

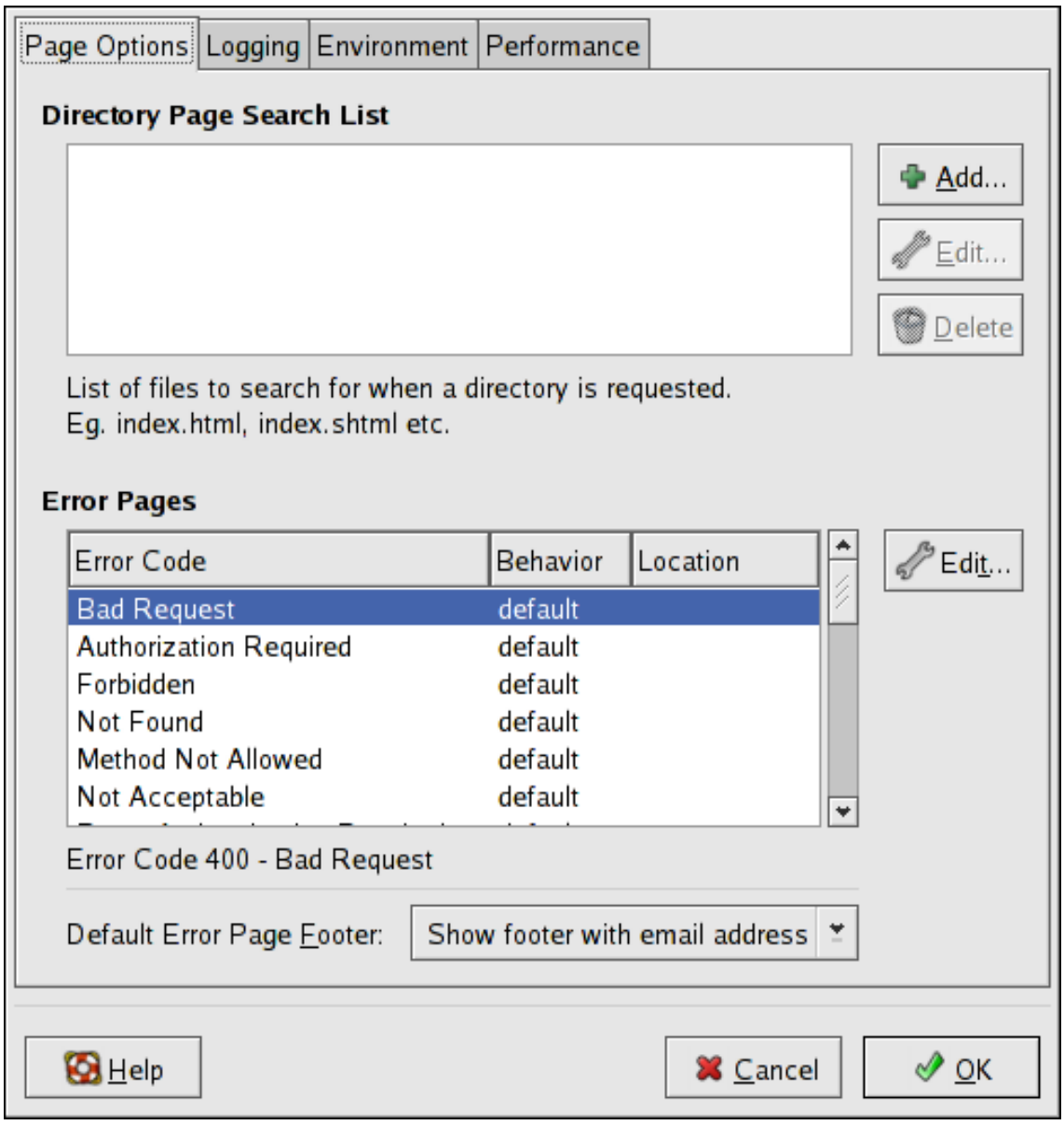


Figura 7.5. Configuración del Sitio

Las entradas que aparecen en la **Lista de Búsqueda de Página de Directorio** definen la directiva `DirectoryIndex` [http://httpd.apache.org/docs/2.2/mod/mod_dir.html#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.example.com/this_directory/` recibe la página del índice del directorio, `DirectoryIndex`, si existe, o un listado de directorios generado por el servidor. El servidor intentará encontrar uno de los archivos incluidos en `DirectoryIndex` y entregará el primero que encuentre. Si no encuentra ninguno de estos archivos y si`Options Indexes` está configurado para ese directorio, el servidor genera y devuelve una lista, en formato HTML, de los subdirectorios y archivos dentro del directorio.

Utilice la sección **Código Error** para configurar el Servidor HTTP Apache para redireccionar el cliente a una URL local o externa en el caso de que haya un error o un problema. Esta opción

corresponde a la directriz `ErrorDocument` [http://httpd.apache.org/docs/2.2/mod/core.html#errordocument]. Si ocurre un error o si se presenta un problema cuando un clienta trata de conectarse al Servidor HTTP Apache, la acción predeterminada es presentar un corto mensaje de error en la columna **Código Error**. Para cancelar esta configuración predeterminada seleccione el código error y haga clic en el botón **Modificar**. Seleccione **Predeterminado** para visualizar el mensaje corto de error predeterminado. Elija **URL** para redireccionar el cliente a la URL externa e ingresar una URL completa incluyendo el `http://` en el campo **Location**. Seleccione **File** para redireccionar el cliente a una URL interna e ingresar la ubicación de un archivo bajo la raíz del documento para el servidor Web. La ubicación debe comenzar con la barra inclinada (/) y debe estar relacionada con la Raíz del Documento.

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`*`/../error/404.html`. En este caso, *`DocumentRoot`* es el directorio del documento raíz que ha definido (el valor por defecto es `/var/www/html/`). Si se deja el documento raíz como la ubicación por defecto, el archivo debería ser copiado a `/var/www/error/404.html`. Luego, elija **Archivo** como el Comportamiento para el código de error **404 - Not Found** e introduzca `/error/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 directriz `ServerAdmin` [http://httpd.apache.org/docs/2.2/mod/core.html#serveradmin].
- **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 en las páginas de error.

4.2.2. Soporte SSL

El `mod_ssl` le permite encriptar el protocolo HTTP sobre SSL. El protocolo SSL(Secure Sockets Layer) se utiliza para comunicación y para encriptar sobre redes TCP/IP. La pestaña SSL le permite configurar SSL para su servidor. Para configurar SSL necesita proporcionar la ruta a su:

- Archivo de certificado - equivalente a utilizar la directriz `SSLCertificateFile` la cual apunta la ruta al archivo de certificado de servidor codificado PEM (Privacy Enhanced Mail).
- Archivo de la llave - equivalente a utilizar la directriz `SSLCertificateKeyFile` la cual apunta la ruta al archivo de la llave privada del servidor codificado PEM.
- Archivo de cadena del certificado - equivalente a utilizar la directriz `SSLCertificateChainFile` la cual apunta la ruta al archivo del certificado que incluye todos los certificados de cadena del servidor.
- Archivo de autoridad del certificado - es un archivo encriptado utilizado para confirmar la autenticidad o identidad de las partes que se comunican con el servidor.

Puede encontrar más información sobre las directrices de configuración para SSL en

http://httpd.apache.org/docs/2.2/mod/directives.html#S [http://httpd.apache.org/docs/2.2/mod/directives.html#S]. También necesita determinar que opciones SSL debe habilitar. Estas son equivalentes a utilizar `SSLOptions` con las siguientes opciones:

- FakeBasicAuth - habilita los métodos de autenticación estándares utilizados por Apache. Esto significa que el Nombre Distinguido del Sujeto del certificado del Cliente X509 es traducido a un nombre de usuario HTTP básico.
- ExportCertData - crea variables de entorno CGI en `SSL_SERVER_CERT`, `SSL_CLIENT_CERT` y `SSL_CLIENT_CERT_CHAIN_n` en donde n es un número 0,1,2,3,4... Los scripts CGI utilizan estos archivos para más chequeos de certificados.
- CompatEnvVars - habilita una compatibilidad retroactiva para Apache SSL añadiendo variables de entorno CGI.
- StrictRequire - habilita acceso estricto el cual obliga a denegar acceso cuando las directrices `SSLRequireSSL` y `SSLRequire` indican que es prohibido el acceso.
- OptRenegotiate - permite eludir los apretones de manos de `mod_ssl` el cual también realiza chequeos de parámetros seguros. Se recomienda que habilite OptRenegotiate con base en el directorio.

Para obtener más información sobre las opciones SSL mencionadas anteriormente vaya a http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#ssloptions [http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#ssloptions]. La figura a continuación ilustra la pestaña SSL y las opciones que se discutieron anteriormente.

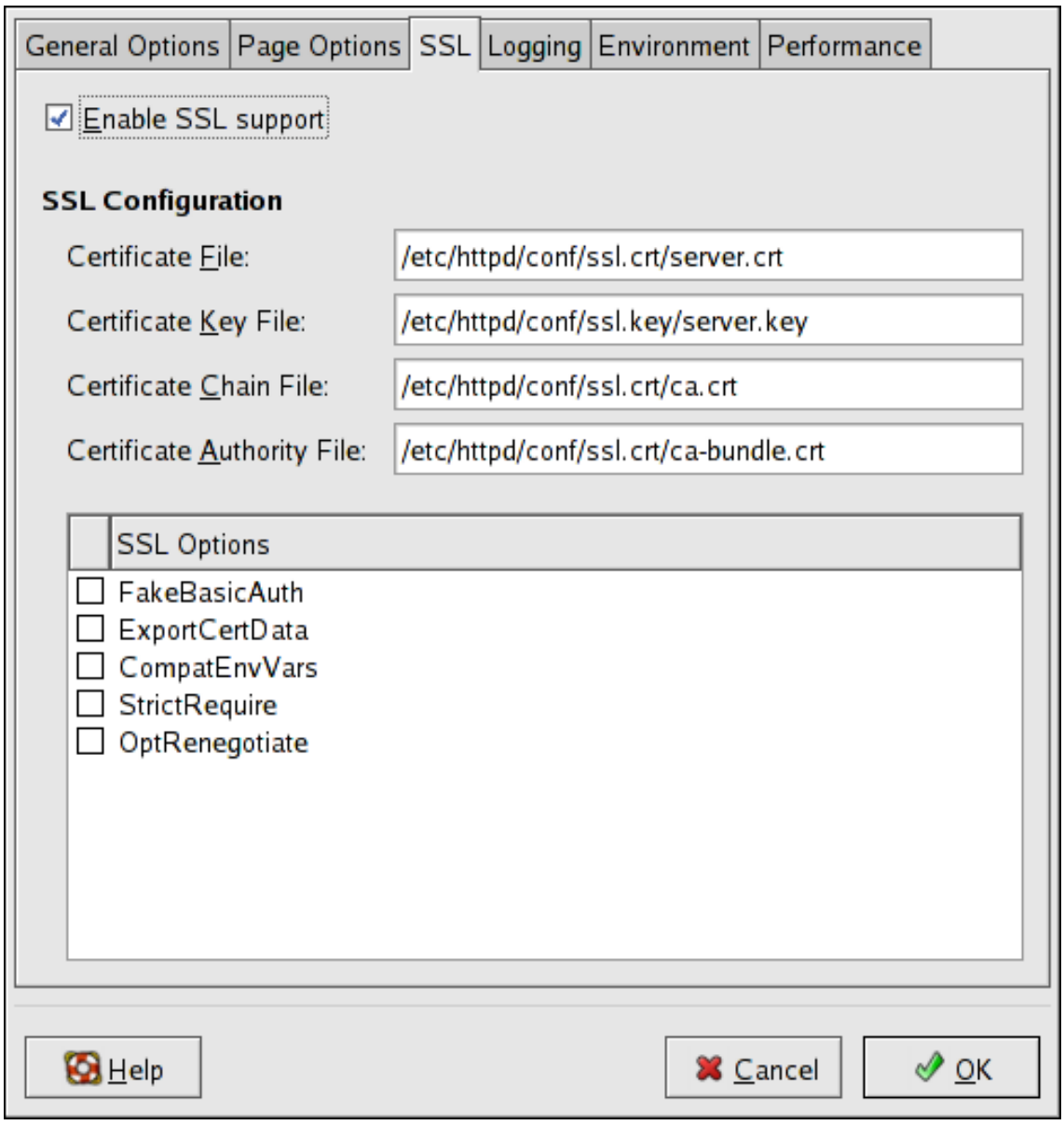


Figura 7.6. SSL

4.2.3. Conexión

Utilice la pestaña **Registro** para configurar las opciones para registro de errores y transferencia específica.

Por defecto, el servidor escribe el registro de transferencia en el archivo `/var/log/httpd/access_log` y el registro de error en el archivo `/var/log/httpd/error_log`.

El registro de transferencias contiene una lista de todos los intentos para acceder al servidor web. Graba las direcciones IP del cliente que está tratande de conectarse, la fecha y hora en que intentó, y el archivo en el servidor web que está tratando de recuperar. Introduzca el nombre de la ruta y del archivo en donde se alamacenará esta información. Si el nombre de la ruta y del archivo no comienzan con una barra inclinada (/), la ruta es relativa al directorio root del servidor como se configurá. Esta opción corresponde a la directriz `TransferLog`

[http://httpd.apache.org/docs/2.2/mod/mod_log_config.html#transferlog].

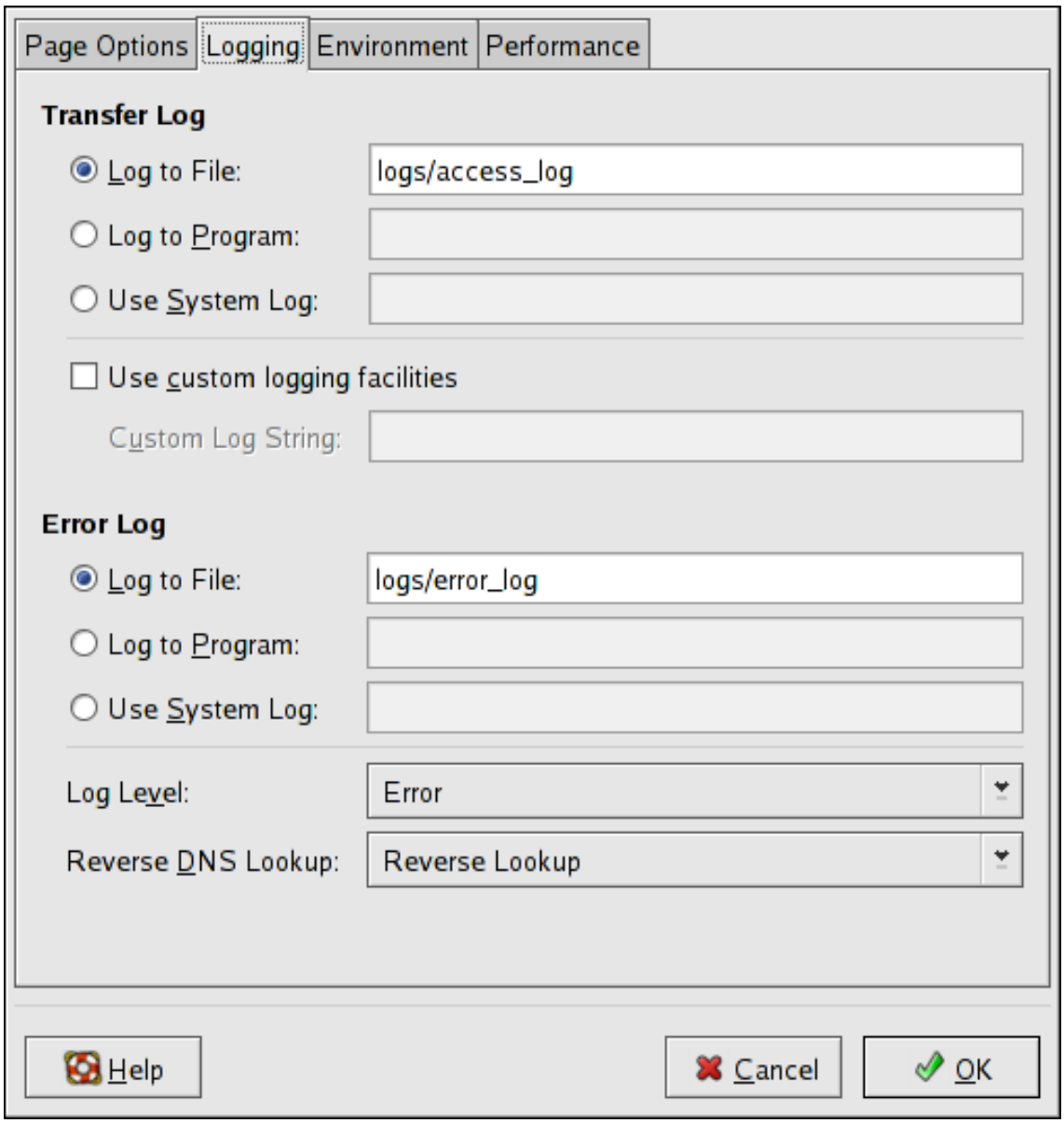


Figura 7.7. Conexión

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 directriz `LogFormat` [http://httpd.apache.org/docs/2.2/mod/mod_log_config.html#logformat]. Para mayor información sobre los detalles del formato de la directiva consulte http://httpd.apache.org/docs/2.2/mod/mod_log_config.html#logformat [http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats].

El registro de transferencia incluye una lista de los errores del servidor. Introduzca el nombre de la ruta y del archivo en donde se debe almacenar esta información. Si el nombre de la ruta y del archivo no empiezan con una barra inclinada (/), la ruta es relativa al directorio root del servidor como se configuró. Esta opción corresponde a la directriz `ErrorLog`

[http://httpd.apache.org/docs/2.2/mod/core.html#errorlog].

Utilice el menú **Nivel de Registro** para establecer la verbosidad de los emnsajes de error en los registrs de error. Se puede configurar (del menos verbos al más verboso) como emerg, alerta, crit, error, advert, aviso, info o depurar. Esta opción corresponde a la directriz `LogLevel` [http://httpd.apache.org/docs/2.2/mod/core.html#loglevel].

El valor escogido en el menú **Búsqueda inversa del DNS** define la directiva `HostnameLookups` [http://httpd.apache.org/docs/2.2/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.

Si escoje **Búsuqeda Inversa** su servidor resuelve automáticamente la dirección IP para cada conexión la cual pide un documento de su servidor web. El resolver una dirección IP significa que su servidor realiza una o más conexiones al DNS para encontrar el nombre del host que corresponde a una dirección IP en particular.

Si elije **Búsqueda Inversa Doble** su servidor realiza un DNS inverso doble. Es decir, después de que se realiza una búsqueda inversa, se realiza una búsqueda avanzada en el resultado. Por lo menos una de las direcciones IP en la búsqueda vanazada debe coincidir con la dirección de la primera búqieda inversa.

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.

Las búsquedas inversas y las búsquedas inversas dobles también son un problema para el internet en general. Cada conexión individual que se realiza para buscar cada nombre de host se va sumando. Por lo tanto, para el beneficio de su propio servidor web así como para el beneficio de internet, usted debe dejar configurada esta opción como **No Búsqueda Inversa**.

4.2.4. Variables del entorno

Utilice la pestaña **Entorno** para configurar las opciones para variables específicas para establecer, pasar o desconfigurar para scripts CGI.

Algunas veces es necesario modificar las variables del entorno para scripts CGI o páginas server-side include (SSI). El Servidor HTTP Apache puede usar el módulo `mod_env` para configurar las variables del ambiente que son pasadas a los scripts CGI y a las páginas SSI. Utilice la página **Variables de entorno** para configurar las directivas para este módulo.

Utilice la sección **Configuración para el Script 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` como `50` haga clic en el botón **Añadir** dentro de la sección **Configuración para el Script CGI** como se muestra en Figura 7.8, “Variables del entorno” y escriba **`MAXNUM`** en el campo de texto **Variables de Entorno** y **`50`** en el campo de texto **Valor a establecer**. Haga clic en **OK** para añadirlo a la lista. La sección **Configuración para el Script CGI** configura la directriz `ConfigEnt` [http://httpd.apache.org/docs/2.2/mod/mod_env.html#setenv]

Utilice la sección **Pasar a los Scripts CGI** para pasar el valor de una variable de entorno cuando el servidor se inicia por primera vez en scripts CGI. Para ver esta variable de entrada escriba el comando `env` en un intérprete de comandos. Haga clic en el botón **Añadir** dentro de la sección **Pasar a Scripts CGI** e introduzca el nombre de la variable de entorno en la ventana de

diálogo que aparece. Haga clic en **OK** para añadirla a la lista. La sección **Pass to CGI Scripts** configura la directriz `PasarEnt` [http://httpd.apache.org/docs/2.2/mod/mod_env.html#passenv].

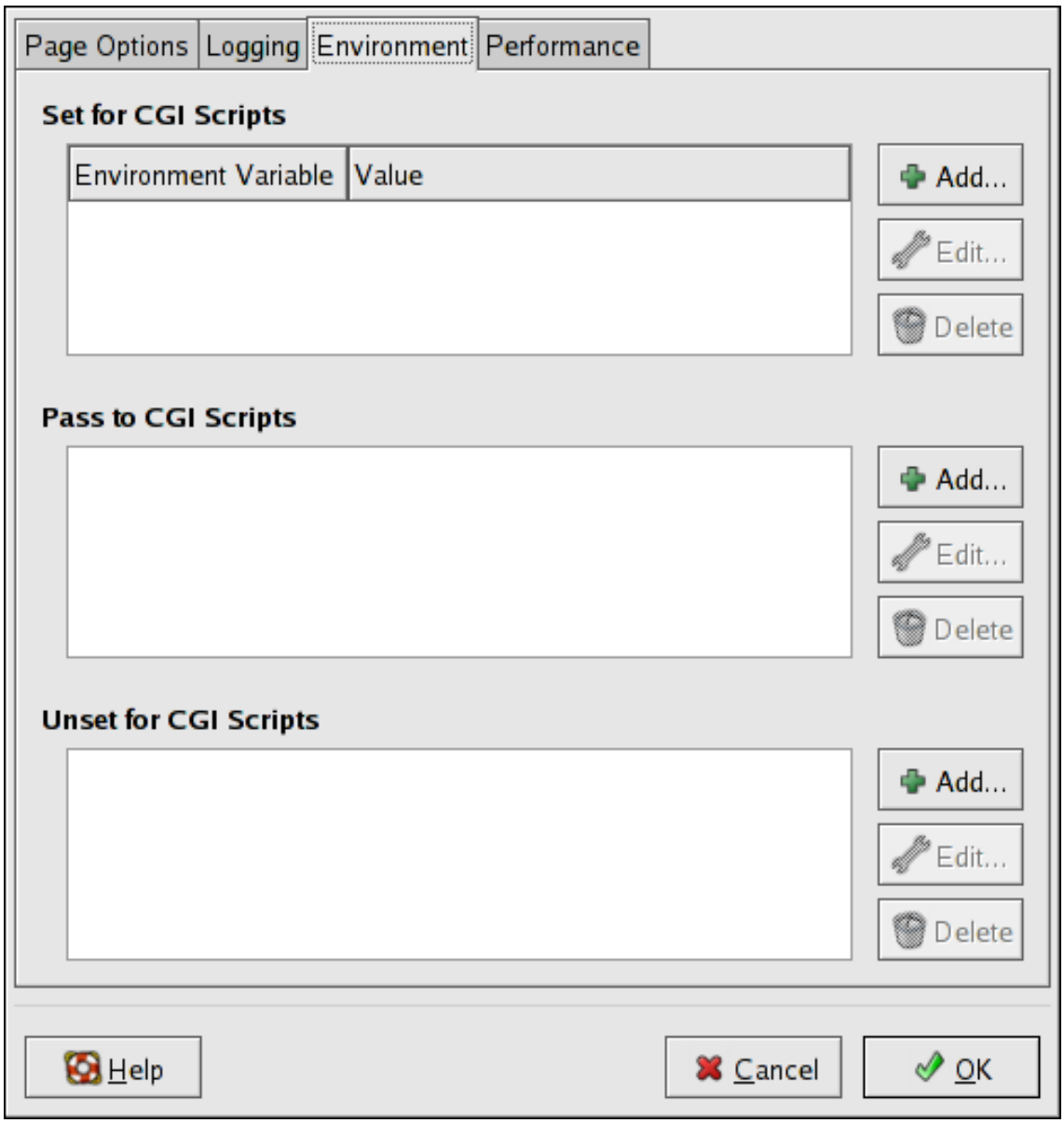


Figura 7.8. Variables del entorno

Para eliminar una variable de entorno de manera que el valor no se pase a a los scripts CGI y a las páginas SSI utilice la sección **Desconfigurar para Scripts CGI**. Haga clic en **Añadir** en la sección **Desconfigurar para Scripts CGI** e introduzca el nombre de la variable de entorno en desconfigurar. Haga clic en **OK** para añadirla a la lista. Esto corresponde a la directriz `DesconfigEnt` [http://httpd.apache.org/docs/2.2/mod/mod_env.html#unsetenv]

Para modificar cualquier de estos valores de entorno selecciónelo de la lista y haga clic en el botón **Modificar** . Para borrar cualquier entrada de la lista selecciónela y haga clic en el botón **Eliminar** correspondiente.

Para obtener más información sobre las variables de entorno en el Servidor HTTP Apache refiérase a: http://httpd.apache.org/docs/2.2/env.html

4.2.5. Directorios

Utilice la página **Directorios** en la pestaña **Rendimiento** para configurar las opciones para directorios específicos. Esto corresponde a la directriz `<Directory>` [http://httpd.apache.org/docs/2.2/mod/core.html#directory].

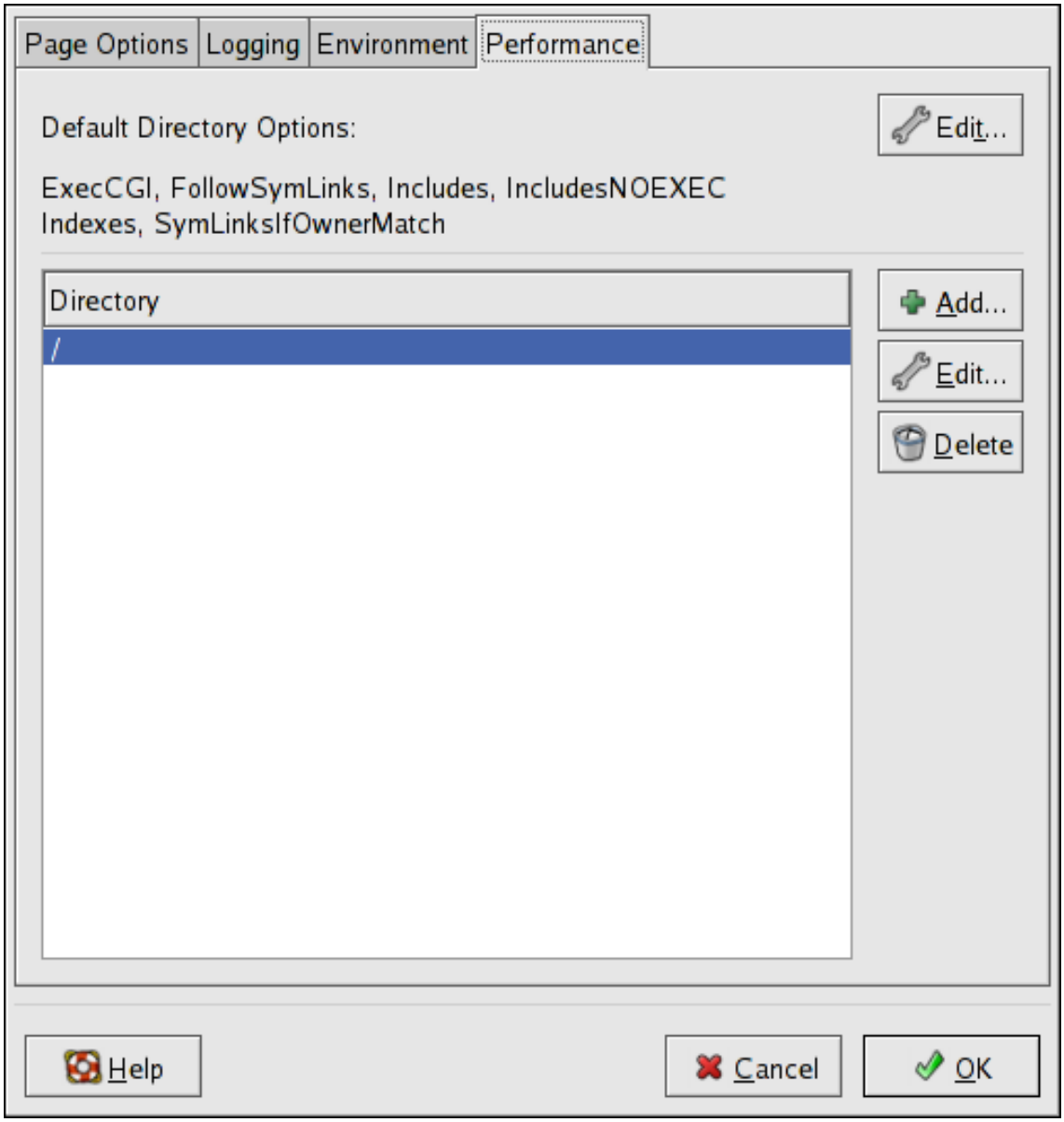


Figura 7.9. Directorios

Haga clic en el botón **Modificar** en la parte de arriba de la esquina derecha para configurar las **Opciones del Directorio Predeterminadas** para todos los directorios que no se especifican en la lista **Directorio** debajo de esta. Las opciones que puede escoger como la directriz `Opciones` [http://httpd.apache.org/docs/2.2/mod/core.html#options] dentro de la directriz `<Directorio>` [http://httpd.apache.org/docs/2.2/mod/core.html#directory]. Puede configurar las siguientes opciones:

- **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.
- `index.html` Soporta las visualizaciones múltiples de los contenidos; esta opción no está activada por defecto.
- **SymLinksIfOwnerMatch** — Permite seguir un enlace simbólico sólamente si el archivo o el directorio en cuestión tienen el mismo propietario que el enlace.

Para especificar opciones para directorios específicos haga clic en el botón **Añadir** al lado de la lista **Directorio**. Aparecerá una ventana como en Figura 7.10, “Configuración de Directorio”. Ingrese el directorio a configurar en el campo de texto Figura 7.10, “Configuración de Directorio” en la parte de abajo de la ventana. Seleccione las opciones en la lista del lado derecho y configure la directriz `Order` [http://httpd.apache.org/docs-2.0/mod/mod_access.html#order] con las opciones que se encuentran del lado izquierdo. La directriz `Orden` controla el orden en que se evaluan las directrices de permiso y de rechazo. En los campos de texto **Permitir Allow hosts de** y **Rechazar hosts de** puede especificar uno de los siguientes:

- Permitir todas los hosts — Escriba **`all`** para permitir el acceso a todos los hosts.
- 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`**

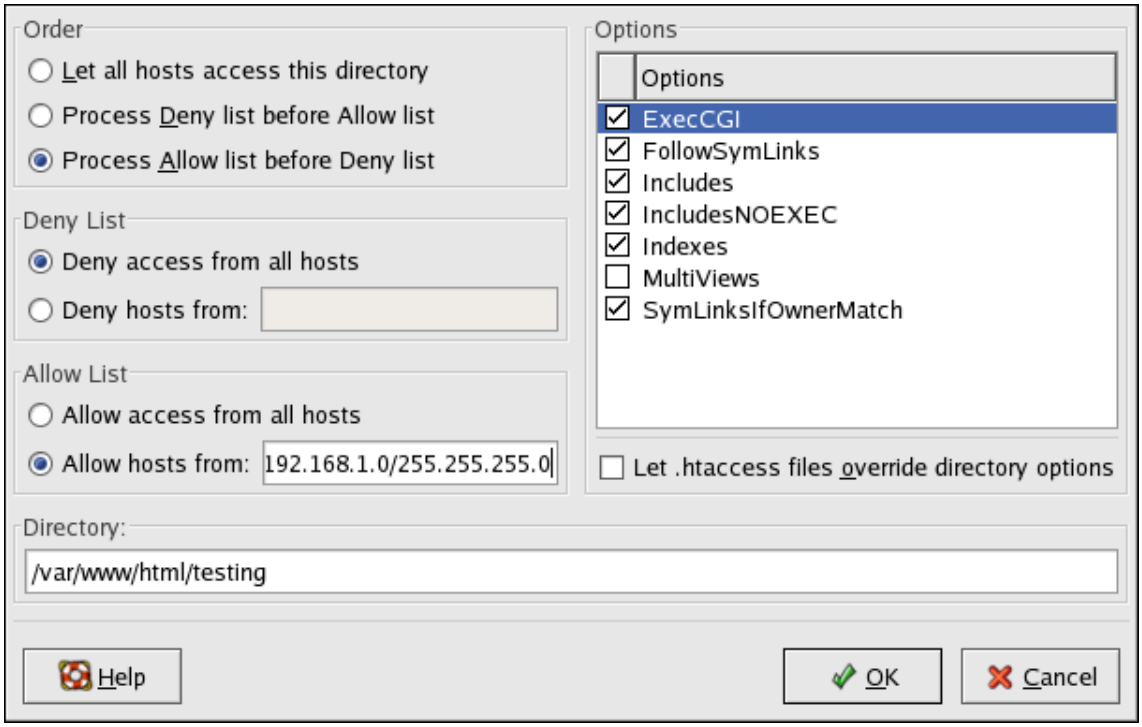


Figura 7.10. Configuración de Directorio

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.

5. Directrices de configuración en `httpd.conf`

El archivo de configuración del Servidor HTTP Apache es `/etc/httpd/conf/httpd.conf`. El archivo `httpd.conf` está bien comentado y en gran parte es autoexplicativo. Su configuración por defecto funciona para la mayoría de los casos; sin embargo, es una buena idea familiarizarse con algunas de las opciones de configuración más importantes.

Advertencia

Con la versión 2.2 del Servidor HTTP Apache han cambiado muchas de las opciones de configuración. Si necesita migrar de la versión 1.3 a la 2.2 primero lea Sección 2.2, “Migración de los Archivos de Configuración del Servidor HTTP Apache de la Versión 1.3 a la 2.0”.

5.1. Sugerencias de configuración generales

Si necesita configurar el Servidor HTTP Apache sólo tiene que modificar el archivo `/etc/httpd/conf/httpd.conf` y después recargar o bien apagar y arrancar el proceso `httpd` como se describe en Sección 3, “Arrancar y detener httpd”.

Antes de modificar el archivo `httpd.conf`, primero haga una copia del archivo original. Al crear una copia de respaldo se hace más fácil recuperarse de posibles errores cometidos mientras se editaba el archivo de configuración.

Si comete un error y su servidor de web no funciona correctamente, lo primero que debe realizar es revisar lo que lo que acaba de modificar en `httpd.conf` para ver si no hay errores de transcripción.

Después consulte el archivo de registro de errores del servidor web, `/var/log/httpd/error_log`. Este puede ser difícil de interpretar, todo depende del nivel de experiencia. Sin embargo, las últimas entradas en el registro deberían de ayudarle a saber lo que ha pasado.

Las siguientes subsecciones proporcionan una breve descripción de muchas de las directrices incluidas en `httpd.conf`. Estas descripciones no son exhaustivas. Para obtener más información consulte la documentación de Apache en línea http://httpd.apache.org/docs/2.2/.

Para obtener mayor información sobre las directrices `mod_ssl` consulte la documentación en http://httpd.apache.org/docs/2.2/mod/mod_ssl.html.

AccessFileName. `AccessFileName` denomina el archivo que el servidor utilizará para información de control de acceso en cada directorio. Por defecto, el servidor utilizará `.htaccess`.

Justo tras `AccessFileName`, un conjunto de indicadores de `Files` aplican el control de acceso a cualquier archivo comenzando con un `.ht`. Estas directrices niegan el acceso Web a cualquier archivo `.htaccess` (o otros archivos que comiencen con `.ht`) por razones de seguridad.

Acción. `Action` especifica parejas tipo contenido MIME y script CGI, para que cuando un archivo de ese tipo de media sea solicitado, se ejecute un script CGI particular.

AddDescription. Cuando utilice `FancyIndexing` como un parámetro de `IndexOptions`, la directriz `AddDescription` se puede usar para mostrar descripciones especificadas por el usuario para ciertos archivos o tipos de archivo en un listado de directorio generado por el servidor. La directriz `AddDescription` soporta el listado de archivos específicos, expresiones con comodines o extensiones de archivos.

AddEncoding. La directriz `AddEncoding` nombra las extensiones de archivos que deberían especificar un tipo particular de codificación. También se puede usar `AddEncoding` para decirle a los navegadores que descompriman ciertos archivos mientras los descargan.

AddHandler. La directriz `AddHandler` hace corresponder extensiones de archivos a manejadores específicos. Por ejemplo, se puede corresponder el manejador `cgi-script` con la extensión `.cgi` para que automáticamente trate a cualquier archivo con un nombre que termine en `.cgi` como un script CGI. A continuación se presenta un ejemplo de una directriz `AddHandler` para la extensión `.cgi`.

```
AddHandler cgi-script .cgi
```

Esta directriz habilita a CGIs fuera del `cgi-bin` para que funcionen en cualquier directorio en el servidor que tenga la opción `ExecCGI` dentro del contenedor de directorios. Refiérase a la Directory para obtener más información sobre la configuración de la opción `ExecCGI` para un directorio.

Además de los scripts CGI, la directriz `AddHandler` es usada para procesar archivos de mapas

de imagen y HTML analizados por el servidor.

AddIcon. `AddIcon` dice al servidor qué icono mostrar en los listados del directorio para ciertos tipos de archivos según la extensión. Por ejemplo, el servidor Web muestra el icono `binary.gif` para archivos con extensiones `.bin` o `.exe`.

AddIconByEncoding. Esta directriz denomina qué iconos se mostrarán con los archivos según su codificación MIME, en los listados de directorio. Por ejemplo, el servidor muestra por defecto el icono `compressed.gif` junto a archivos con codificación MIME x-compress y x-gzip en los listados de directorio.

AddIconByType. Esta directriz denomina qué iconos se mostrarán con los archivos con codificación MIME, en los listados del directorio. Por ejemplo, por defecto, el servidor muestra el icono `text.gif` junto a archivos con tipo MIME `text` en los listados del directorio.

AddLanguage. La directriz `AddLanguage` asocia extensiones de nombres de archivos a idiomas específicos. Esta directriz es útil para los Servidores HTTP Apache, los cuales devuelven contenidos en diferentes idiomas dependiendo de la configuración del idioma del navegador Web del cliente.

AddType. Utilice la directriz `AddType` para definir o suprimir por defecto pares tipo MIME y extensiones de archivos. El siguiente ejemplo de directriz le dice al Servidor HTTP Apache que reconozca la extensión de archivos `.tgz`:

```
AddType application/x-tar .tgz
```

Alias. El valor `Alias` hace accesibles a los directorios fuera del directorio `DocumentRoot`. Cualquier URL que termine en el alias será automáticamente traducido a la ruta del alias. Por defecto, ya existe un alias configurado para un directorio `icons`. El servidor web puede acceder al directorio `icons`, pero el directorio no está en el `DocumentRoot`.

Allow. `Allow` especifica cual cliente puede acceder a un directorio dado. El solicitante puede ser `all`, un nombre de dominio, una dirección IP, una dirección IP parcial, un par de red/máscara de la red, etc. El directorio `DocumentRoot` está configurado para permitir (`Allow`) peticiones desde todos (`all`), es decir, que todos tienen acceso.

AllowOverride. La directriz `AllowOverride` indica si puede o no ignorar cualquiera de las `Options` por las declaraciones en un archivo `.htaccess`. Por defecto, tanto el directorio raíz como `DocumentRoot` están configurados para no se permita ignorar `.htaccess`.

BrowserMatch. La directriz `BrowserMatch` permite al servidor definir variables de entorno y/o tomar acciones según sea el campo de cabecera User-Agent del HTTP, que identifica el tipo de navegador Web del cliente. Por defecto, el servidor usa `BrowserMatch` para denegar la conexión a navegadores con problemas conocidos y para desactivar "keepalives" y vaciados de cabecera de HTTP para navegadores que se sabe tienen problemas con acciones de ese tipo.

Directrices Cache. El archivo de configuración del Servidor HTTP Apache suministra varias directrices de caché comentadas. En la mayoría de los casos, al quitar el comentario de estas líneas mediante la eliminación de las almohadillas (`#`) del principio de la línea es suficiente. Sin embargo, lo siguiente es una lista de algunas de las directrices relacionadas con caché más importantes.

- `CacheEnable` — Especifica si la caché es un disco, memoria o caché de archivo descriptivo. Por defecto `CacheEnable` configura un disco caché para las URLs en o por debajo de `/`.
- `CacheRoot` — pone el nombre del directorio que contiene archivos de caché. El valor predeterminado de `CacheRoot` es el directorio `/var/httpd/proxy/`.
- `CacheSize` — establece cuánto espacio puede usar el caché, en KB. El valor predeterminado de `CacheSize` es `5` KB.

Lo siguiente es una lista de algunas directrices comunes relacionadas con caché.

- `CacheMaxExpire` — Especifica cuanto tiempo se conservan los documentos HTML (sin una recarga desde el servidor Web original) en el caché. El valor por defecto es `24` horas (`86400` segundos).
- `CacheLastModifiedFactor` — Especifica la creación de una fecha de vencimiento para documentos que no venían con caducidad desde el servidor de origen. El valor predeterminado de `CacheLastModifiedFactor` está configurado a `0.1`, es decir que la fecha de vencimiento para tales documentos es igual a un décimo de la cantidad de tiempo desde la última vez que se modificó el documento.
- `CacheDefaultExpire` — Especifica el tiempo de caducidad en horas para un documento que fue recibido usando un protocolo que no soporta fechas de vencimiento. El valor por defecto es configurado a `1` hora (`3600` segundos).
- `NoProxy` — Especifica una lista separada por espacios de subredes, direcciones IP, dominios o hosts cuyos contenidos no están en caché. Este valor es de gran utilidad para sitios de Intranet.

CacheNegotiatedDocs. Por defecto, el servidor Web requiere a los servidores proxy que no hagan caché de los documentos que se negocian en base al contenido (pueden cambiar en el tiempo o según la entrada de quien los solicita). Si se configura `CacheNegotiatedDocs` a `on`, se desactiva la función y se permite acceso a los servidores proxy a tales documentos caché.

CustomLog. `CustomLog` identifica el archivo de registro y su formato. Por defecto, el registro de acceso es guardado al archivo `/var/log/httpd/access_log` mientras que los errores se guardan en el archivo `/var/log/httpd/error_log`.

El formato por defecto `CustomLog` es `combined`, como se ilustra a aquí:

```
remotehost rfc931 user date "request" status bytes referrer user-agent
```

DefaultIcon. `DefaultIcon` especifica el icono desplegado en el listado generado por el servidor para archivos que no tienen otro icono especificado. El archivo de imagen por defecto es `unknown.gif`.

DefaultType. `DefaultType` establece el tipo de contenido por defecto que el servidor utilizará para documentos cuyos tipos MIME no puedan ser determinados. Por defecto es `text/plain`.

Deny. `Deny` funciona igual que `Allow`, excepto que especifica a quién se le niega el acceso. `DocumentRoot` no es configurado para negar (`Deny`) peticiones a ninguno por defecto.

Directory. Las etiquetas `<Directory /path/to/directory>` y `</Directory>` se usan para crear

un contenedor que se utiliza para cercar un grupo de directrices de configuración que sólo se aplican a un directorio y sus subdirectorios específicos. Cualquier directriz aplicable a un directorio puede usarse en las etiquetas `Directory`.

Por defecto, se aplican parámetros muy restrictivos al directorio raíz (`/`) utilizando las directrices `Options` (consulte la Options) y `AllowOverride` (vea la AllowOverride). Con esta configuración, cualquier directorio del sistema que necesite valores más permisivos ha de ser configurado explícitamente con esos valores.

En la configuración predeterminada, otro contenedor `Directory` es configurado para el `DocumentRoot`, el cual asigna parámetros menos rígidos al árbol del directorio para que el Servidor HTTP Apache pueda acceder a los archivos que residan allí.

El contenedor `Directory` también se puede utilizar para configurar directorios adicionales `cgi-bin` para las aplicaciones del servidor fuera del directorio especificado en la directriz `ScriptAlias` (consulte a la ScriptAlias para obtener más información).

Para lograr esto, el contenedor `Directory` debe configurar la opción `ExecCGI` para ese directorio.

Por ejemplo, si los scripts CGI están localizados en `/home/my_cgi_directory`, añada el contenedor siguiente `Directory` al archivo `httpd.conf`:

```
<Directory /home/my_cgi_directory> Options +ExecCGI </Directory>
```

Luego, necesitará anular el comentario de la directriz `AddHandler` para identificar archivos con la extensión `.cgi` como scripts CGI. Consulte la AddHandler para saber cómo configurar el `AddHandler`.

Para que esto funcione, los permisos para los scripts CGI y la ruta completa a los scripts, se deben colocar a 0755.

DirectoryIndex. `DirectoryIndex` es la página por defecto que entrega el servidor cuando hay una petición de índice de un directorio especificado con una barra (/) al final del nombre del directorio.

Cuando un usuario pide la página http://*ejemplo*/*este_directorio*/, recibe la página del índice del directorio, `DirectoryIndex`, si existe, o un listado de directorios generado por el servidor. El valor por defecto para `DirectoryIndex` es `index.html` y el tipo de mapa `index.html.var`. El servidor intentará encontrar cualquiera de estos archivos y entregará el primero que encuentre. Si no encuentra ninguno de estos archivos y `Options Indexes` esta configurado para ese directorio, el servidor genera y devuelve una lista, en formato HTML, de los subdirectorios y archivos dentro del directorio, a menos que la característica de listar directorios esté desactivada.

DocumentRoot. `DocumentRoot` es el directorio que contiene la mayoría de los archivos HTML que se entregarán en respuesta a peticiones. El directorio predeterminado `DocumentRoot` para servidores web seguros y no seguros es `/var/www/html`. Por ejemplo, el servidor puede recibir una petición para el siguiente documento:

```
http://example.com/foo.html
```

El servidor busca por el archivo siguiente en el directorio por defecto:

```
/var/www/html/foo.html
```

Si se quiere cambiar `DocumentRoot` para que no lo compartan los servidores web seguros y los no seguros vea la Sección 7, “Hosts virtuales”.

ErrorDocument. La directriz `ErrorDocument` asocia un código de respuesta HTTP con un mensaje o un URL para que sea devuelto al cliente. Por defecto, el servidor Web produce una salida simple de mensaje de error cuando ocurre alguno. La directriz `ErrorDocument` obliga a que el servidor Web envie una salida de mensaje personalizado o página.

Importante

Para que el mensaje sea válido, éste se *tiene* que estar entre un par de comillas dobles `"`.

ErrorLog. `ErrorLog` especifica el archivo donde se guardan los errores del servidor . Por defecto, esta directriz es configurada a `/var/log/httpd/error_log`.

ExtendedStatus. La directriz `ExtendedStatus` controla si Apache generará información básica del estado del servidor (`off`) o detallada (`on`), cuando se invoca el manejador `server-status`. El manejador `server-status` se llama utilizando la etiqueta `Location`. Para obtener más ifnormación sobre cómo realizar llamadas `server-status` vaya a Location.

Group. Especifica el nombre del grupo de los procesos del Servidor HTTP Apache.

Esta directriz se ha desaprobado para la configuración de hosts virtuales.

Por defecto, `Group` está configurado a `apache`.

HeaderName. La directriz `HeaderName` dicta el archivo (si existe dentro del directorio) que se antepondrá al comienzo de los listados de los directorios. Al igual que con `ReadmeName`, el servidor intentará incluirlo como documento HTML si es posible, o en caso contrario, como texto.

HostnameLookups. `HostnameLookups` se puede configurar a `on`, `off` o `double`. Si se configura `HostnameLookups` a `on`, el servidor automáticamente resuelve las direcciones IP para cada conexión. Resolver las direcciones IP significa que el servidor hace una o más conexiones a un servidor DNS, añadiendo sobrecarga por procesamiento. Si `HostnameLookups` es configurado a `double`, el servidor realiza búsquedas inversa doble del DNS, añadiendo aún más sobrecarga.

Para ahorrar recursos en el servidor, `HostnameLookups` es configurado a `off` por defecto.

Si se requieren nombres de host en los archivos de registro, considere ejecutar una de los muchas herramientas de análisis de log que llevan a cabo las búsquedas de DNS de forma mucho más eficiente y por montones cuando se este rotando los archivos de log del servidor Web.

IfDefine. Las etiquetas `IfDefine` envuelven directrices de configuración que son aplicadas si el "test" establecido en la etiqueta `<IfDefine>` es verdadero. Las directrices no se tienen en cuenta si el test es falso.

El test en las etiquetas `IfDefine` es un nombre de parámetro (por ejemplo, `HAVE_PERL`). Si el parámetro está definido, es decir, si se da como argumento al comando de arranque del servidor, entonces el test es verdadero. En este caso, cuando se arranca el servidor Web, el test es ver-

dadero y se aplican las directrices contenidas en las etiquetas `IfDefine`.

IfModule. Las etiquetas `<IfModule>` y `</IfModule>` crean un contenedor condicional que sólo es activado si el módulo especificado es cargado. Las directrices contenidas entre etiquetas `IfModule` son procesadas bajo una de dos condiciones. Las directrices son procesadas si se carga el módulo entre la etiqueta de comienzo `<IfModule>`. O, si un símbolo de exclamación **!** aparece antes del nombre del módulo, entonces las directrices son procesadas sólo si el módulo especificado en la etiqueta `<IfModule>`*no* es cargado.

Para obtener mayor información sobre los módulos del Servidor HTTP Apache consulte la Sección 6, “Añadir módulos”.

Include. `Include` permite que se incluyan otros archivos de configuración en el tiempo de ejecución.

La ruta a estos archivos de configuración pueden ser absolutas o relativas con respecto al `ServerRoot`.

Importante

Para que el servidor use módulos de paquetes individuales, como `mod_ssl`, `mod_perl` y `php`, tiene que estar la siguiente directriz en `Section 1: Global Environment` del `httpd.conf`:

```
Include conf.d/*.conf
```

IndexIgnore. `IndexIgnore` lista las extensiones de archivo, los nombres de los archivos parciales, las expresiones con comodines o los nombres completos. El servidor Web no incluirá ningún archivo que coincida con estos patrones en los listados de directorios.

IndexOptions. `IndexOptions` controla la apariencia de los listados generados por el servidor, al añadir iconos, texto descriptivo, etc. Si `Options Indexes` está configurado (vea la Options) el servidor Web server genera un listado de directorio cuando el servidor Web recibe una petición HTTP para un directorio sin un índice.

Primero el servidor Web busca en el directorio solicitado un archivo que coincida los nombres listados en la directriz `DirectoryIndex` (usualmente, `index.html`). Si el servidor no encuentra un archivo `index.html` el Servidor HTTP Apache genera un listado del directorio en HTML. La apariencia del listado de este directorio es controlada, en parte, por la directriz `IndexOptions`.

La configuración predeterminada activa `FancyIndexing`. Esto significa que un usuario puede reordenar un listado de directorio haciendo clic en las cabeceras de columnas. Otro clic en la misma cabecera cambiará del orden ascendente al descendente. `FancyIndexing` también muestra iconos diferentes para diferentes archivos, basados en las extensiones de archivos.

La opción `AddDescription`, cuando se utiliza junto con `FancyIndexing`, presenta una descripción corta para el archivo en los listados de directorios generados por el servidor.

`IndexOptions` tiene otros parámetros que pueden activarse para controlar la apariencia de los listados generados por los servidores. Los parámetros `IconHeight` y `IconWidth` requieren que el

servidor incluya etiquetas HTML `HEIGHT` y `WIDTH` para los iconos en las páginas generadas por el servidor. El parámetro `IconsAreLinks` combina el icono con el ancla HTML, la cual contiene el enlace URL objetivo.

KeepAlive. `KeepAlive` determina si el servidor permitirá más de una petición por conexión y se puede usar para prevenir a un cliente consumir demasiados recursos del servidor.

Por defecto `Keepalive` está configurado a `off`. Si `Keepalive` está en `on` y el servidor se vuelve muy ocupado, este puede rápidamente generar el máximo número de procesos hijos. En esta situación, el servidor se volverá significativamente lento. Si se activa `Keepalive` es una buena idea configurar el `KeepAliveTimeout` a un valor bajo (consulte la KeepAliveTimeout para más información sobre la directriz `KeepAliveTimeout`) y controle el archivo de registro `/var/log/httpd/error_log` en el servidor. Este registro informa cuando el servidor se está quedando corto de procesos hijos.

KeepAliveTimeout. La directriz `KeepAliveTimeout` establece el número de segundos que el servidor esperará tras haber dado servicio a una petición, antes de cerrar la conexión. Una vez que el servidor recibe una petición, se aplica la directriz `Timeout` en su lugar. `KeepAliveTimeout` está configurado a 15 segundos por defecto.

LanguagePriority. La directriz `LanguagePriority` permite dar la prioridad para diferentes idiomas en caso de que el navegador Web no especique la preferencia de idioma.

Listen. El comando `Listen` identifica los puertos en los que el servidor Web aceptará las peticiones entrantes. Por defecto, el Servidor HTTP Apache está configurado para escuchar en el puerto 80 para comunicaciones Web no seguras y (en el archivo `/etc/httpd/conf.d/ssl.conf` el cual define cualquier servidor seguro) en el puerto 443 para comunicaciones seguras.

Si el Servidor HTTP Apache está configurado para escuchar en un puerto por debajo del 1024, se necesita al usuario root para iniciarlo. Para los puertos 1024 y superiores, `httpd` puede ser arrancado por cualquier usuario.

La directriz `Listen` también se puede usar para especificar direcciones IP particulares sobre las cuales el servidor aceptará conexiones.

LoadModule. `LoadModule` se utiliza para cargar módulos Dynamic Shared Object (DSO). Se puede encontrar más información sobre el soporte del Servidor HTTP Apache para DSO, incluyendo exáctamente cómo utilizar la directriz `LoadModule` en la Sección 6, “Añadir módulos”. Observe que ya *no es importante* el orden en que se cargan estos módulos con el Servidor HTTP Apache 2.0. Consulte la Sección 2.2.1.3, “Soporte del Dynamic Shared Object (DSO) (Objeto dinámico compartido)” para obtener más información sobre el soporte DSO del Servidor HTTP Apache 2.0 para DSO.

Location. Las etiquetas `<Location>` y `</Location>` permiten crear un contenedor en el cual se puede especificar el control de acceso basado en URL.

Por ejemplo, para permitir a personas conectarse desde dentro del dominio del servidor para ver informes de estado, utilice las directrices siguientes:

```
<Location /server-status> SetHandler server-status Order deny,allow Deny from all Allow from <.example.com
```

Reemplace `<.example.com>` con el nombre de dominio de segundo nivel para el servidor Web.

Para proporcionar informes de configuración del servidor (incluyendo los módulos instalados y las directrices de configuración) a peticiones desde dentro del dominio, utilice las siguientes directrices:

```
<Location /server-info> SetHandler server-info Order deny,allow Deny from all Allow from <.example.com> </
```

Una vez más, reemplace `<.example.com>` con el nombre del dominio de segundo nivel para el servidor Web.

LogFormat. La directriz `LogFormat` configura el formato para los archivos de registro del servidor Web. El comando `LogFormat` utilizado en realidad depende de la configuración dada en la directriz `CustomLog` (consulte la CustomLog).

Las siguientes son las opciones de formato si la directriz `CustomLog` es configurada a `combined`:

`%h` (dirección IP del host remoto o nombre de la máquina)
: Lista la dirección IP de la máquina remota del cliente solicitante. Si `HostnameLookups` es configurada a `on`, el nombre de máquina del cliente es registrado a menos que no este disponible desde el DNS.

`%l` (rfc931)
: No se usa. Un guión **-** aparece en el campo de registro para este campo.

`%u` (usuario autenticado)
: Si se requiere autenticación, lista el nombre del usuario registrado. Usualmente, esto no se utiliza, por tanto aparece un guión **-** en el archivo de registro para este campo.

`%t` (fecha)
: Lista la fecha y hora de la solicitud.

`%r` (cadena de la solicitud)
: Lista la cadena de la solicitud exactamente como viene del navegador o cliente.

`%s` (estado)
: Lista el estado de código HTTP el cual fue devuelto al host cliente.

`%b` (bytes)
: Lista el tamaño del documento.

`%\"%{Referer}i\"` (referencia)
: Lista la dirección URL de la página web que refiere el máquina cliente al servidor Web.

`%\"%{User-Agent}i\"` (agente usuario)
: Lista el tipo de navegador Web que está realizando la solicitud.

LogLevel. `LogLevel` establece la cantidad de detalles que tendrán los registros de mensajes de error. `LogLevel` se puede configurar (desde el que tiene menos detalles a los más detallados) a `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` o `debug`. El valor predeterminado de `LogLevel` es `warn`.

MaxKeepAliveRequests. Esta directriz establece el número máximo de peticiones permitidas por cada conexión persistente. El Proyecto Apache recomienda un valor alto, lo que mejoraría el rendimiento del servidor. El valor predeterminado de `MaxKeepAliveRequests` es de `100` que de-

bería bastar en la mayoría de los casos.

NameVirtualHost. La directriz `NameVirtualHost` asocia una dirección IP y el número de puerto, si es necesario, para cualquier máquina virtual basada en nombres. El hospedaje virtual basado en nombres permite a un Servidor HTTP Apache servir a dominios diferentes sin utilizar múltiples direcciones IP.

Nota

Los hosts virtuales basados en nombre *only* funcionan con conexiones HTTP no seguras. Si está usando host virtuales con un servidor seguro, use host virtuales basados en direcciones IP.

Para habilitar el hospedaje basado en nombres, quite los comentarios de la directriz de configuración `NameVirtualHost` y añada la dirección IP correcta. Luego añada más contenedores `VirtualHost` para cada host virtual como sea necesario para su configuración.

Options. La directriz `Options` controla cuáles características del servidor están disponibles en un directorio en particular. Por ejemplo, en los parámetros restrictivos especificados para el directorio raíz, `Options` sólo permite `FollowSymLinks`. No hay características activadas, salvo que el servidor puede seguir enlaces simbólicos en el directorio raíz.

Por defecto, en el directorio `DocumentRoot`, `Options` se configura para incluir `Indexes` y `FollowSymLinks`. `Indexes` permite al servidor generar un listado de un directorio si no se especifica el `DirectoryIndex` (por ejemplo, `index.html`). `FollowSymLinks` permite al servidor seguir enlaces simbólicos en ese directorio.

Nota

Se tienen que duplicar las declaraciones `Options` de la sección principal de configuración del servidor para cada contenedor `VirtualHost` individualmente. Consulte la VirtualHost para obtener mayor información.

Order. La directriz `Order` controla el orden en el cual las directrices `allow` y `deny` son evaluadas. El servidor es configurado para evaluar las directrices `Allow` antes de las directrices `Deny` para el directorio `DocumentRoot`.

PidFile. `PidFile` nombra el archivo en el que el servidor graba su ID de proceso (pid). Por defecto, el PID es listado en `/var/run/httpd.pid`.

Proxy. Las etiquetas `<Proxy *>` y `</Proxy>` crean un contenedor el cual envuelve un grupo de directrices de configuración solamente para aplicar al servidor proxy. Muchas directrices las cuales son permitidas dentro del contenedor `<Directory>` pueden también ser usadas dentro del contenedor `<Proxy>`.

ProxyRequests. Para configurar el Servidor HTTP Apache para que funcione como un servidor proxy, elimine las marcas de almohadillas o numeral (`#`) del comienzo de la línea `<IfModule`

mod_proxy.c>, las ProxyRequests y cada línea en la estrofa <Proxy>. Configure la directriz ProxyRequests aOn y configure cuáles dominios tienen acceso al servidor en la directriz Allow from de la estrofa <Proxy>.

ReadmeName. La directriz ReadmeName determina el archivo (si existe dentro del directorio) que se adjuntará a los listados de los directorios. El servidor Web intentará primero incluirlo como documento HTML y luego como texto plano. El valor predeterminado de ReadmeName es README.html.

Redirect. Cuando se mueve una página web, se puede utilizar Redirect para crear asignaciones de la ubicación del archivo a un nuevo URL. El formato es como sigue:

Redirect /<*old-path*>/<*file-name*> http://<*current-domain*>/<*current-path*>/<*file-name*>

En este ejemplo, sustituya <*old-path*> con la vieja información de la ruta por <*file-name*> y <*current-domain*> y <*current-path*> con el dominio actual y la información de la ruta para <*file-name*>.

En este ejemplo, cualquier petición <*file-name*> en la vieja ubicación será redirigida automáticamente a la nueva ubicación.

Para técnicas de redireccionamiento más avanzadas, utilice el módulo mod_rewrite incluido con el Servidor HTTP Apache. Para obtener más información sobre la configuración del módulo mod_rewrite refiérase a la documentación de la Apache Software Foundation en http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html [http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html].

ScriptAlias. La directriz ScriptAlias define donde pueden encontrarse los scripts CGI. Normalmente, no es una buena idea colocar los scripts CGI dentro de DocumentRoot, donde podrían, potencialmente, ser visualizados como documentos de texto. Por esta razón, la directriz ScriptAlias diseña un directorio especial fuera del directorio DocumentRoot para contener ejecutables del servidor y scripts. Este directorio es conocido como un cgi-bin y se configura por defecto a /var/www/cgi-bin/.

Es posible establecer directorios para almacenar ejecutables fuera del directorio cgi-bin/. Para obtener más instrucciones sobre cómo hacer esto refiérase a la AddHandler and Directory.

ServerAdmin. Configure la directriz ServerAdmin a la dirección de correo electrónico del administrador del servidor Web. Esta dirección de correo aparecerá en los mensajes de error en las páginas generadas por el servidor Web, de tal manera que los usuarios pueden comunicar errores enviando correo al administrador.

Por defecto, ServerAdmin es configurado a root@localhost.

Una forma típica de configurar ServerAdmin es configurarlo en a webmaster@ejemplo.com. Una vez configurado, cree un alias del webmaster para la persona responsable del servidor Web en /etc/aliases y ejecute /usr/bin/newaliases.

ServerName. Use la directriz ServerName para configurar un nombre de servidor y un número de puerto (que coincida con la directriz Listen) para el servidor. El ServerName no necesita coincidir con el nombre real de la máquina. Por ejemplo, el servidor Web puede ser www.example.com pero el nombre del servidor es en realidad foo.example.com. El valor especificado en ServerName debe ser un nombre del Servicio de Nombres de Dominio (Domain Name

Service, DNS) válido que pueda ser resuelto por el sistema — no invente algo.

Lo siguiente es una directriz `ServerName` de ejemplo:

```
ServerName www.example.com:80
```

Cuando especifique un `ServerName`, asegúrese de que el par de la dirección IP y el nombre del servidor esten incluidos en el archivo `/etc/hosts`.

ServerRoot. La directriz `ServerRoot` especifica el directorio de nivel superior que tiene el contenido web. Por defecto, `ServerRoot` está configurado a `"/etc/httpd"` para servidores seguros y no seguros.

ServerSignature. La directriz `ServerSignature` añade una línea que contiene la versión del Servidor HTTP Apache y el `ServerName` para cualquier documento generado por el servidor, tales como mensajes de error devueltos a los clientes. Por defecto `ServerSignature` está configurada a `on`.

`ServerSignature` se puede configurar como `EMail` el cual añade una etiqueta HTML `mailto:ServerAdmin` a la línea de firma de respuestas auto generadas. También se puede configurar como `Off` para que Apache pare de enviar su número de versión y la información del módulo. Revise también la configuración de `ServerTokens`.

ServerTokens. La directriz `ServerTokens` determina si el encabezamiento de la respuesta del servidor que se devuelve al cliente debe incluir detalles sobre el tipo de Sistema Operativo e información sobre los módulos compilados. Por defecto, `ServerTokens` se encuentra configurado como `Full` y por tanto envía información sobre el tipo del Sistema Operativo y lo módulos compilados. Al configurar `ServerTokens` como `Prod` envía el nombre del producto sólamente y se recomienda un buen número de hackers revise la información en el encabezamiento del servidor en la búsqueda de vulnerabilidades. También puede configurar `ServerTokens` como `Min` (minimal) o como `OS` (sistema operativo).

SuexecUserGroup. La directriz `SuexecUserGroup`, que se origina desde el módulo `mod_suexec`, permite especificar privilegios de ejecución de usuario y grupo para programas CGI. Las solicitudes no CGI también son procesadas con el usuario y el grupo especificado en las directrices `User` y `Group`.

Nota

Desde la versión 2.0, la directriz `SuexecUserGroup` reemplaza la configuración del Servidor HTTP Apache versión 1.3 de utilizar las directrices `User` y `Group` dentro de la configuración de las secciones `VirtualHosts`.

Timeout. `Timeout` define, en segundos, el tiempo que el servidor esperará por recibir y transmitir durante la comunicación. `Timeout` está configurado por defecto a `300` segundos, lo cual es apropiado para la mayoría de las situaciones.

TypesConfig. `TypesConfig` nombra el archivo que configura la lista por defecto de asignaciones tipo MIME (extensiones de nombres de archivo a tipos de contenido). El archivo predeterminado `TypesConfig` es `/etc/mime.types`. En vez de modificar el `/etc/mime.types`, la forma reco-

mendada de añadir asignaciones de tipo MIME es usando la directriz `AddType`.

Para obtener más información sobre `AddType` refiérase a la AddType.

UseCanonicalName. Cuando se configure esta directriz como `on`, se está indicando al Servidor HTTP Apache a que se referencie asímismo utilizando el valor especificado en las directrices `ServerName` y `Port`. Cuando `UseCanonicalName` es configurada como `off`, el servidor usará el valor usado por el cliente solicitante cuando se refiera a él.

`UseCanonicalName` está configurada a `off` por defecto.

User. La directriz `User` establece el nombre de usuario para el proceso del servidor y determina qué archivos pueden acceder al servidor. Cualquier archivo que no esté accesible a este usuario tampoco estará disponible para los clientes conectándose al Servidor HTTP Apache.

Por defecto `User` es configurado a `apache`.

Esta directriz se ha desaprobado para la configuración de hosts virtuales.

Nota

Por razones de seguridad, el Servidor HTTP Apache no se ejecuta como el usuario root.

UserDir. `UserDir` es el nombre del subdirectorio dentro del directorio principal de cada usuario dónde estarán los archivos HTML personal que serán servidos por el servidor de Web. Esta directriz esta configurada por defecto a `disable`.

El nombre para el subdirectorio esta configurado a `public_html` en la configuración por defecto. Por ejemplo, el servidor puede recibir la siguiente petición:

`http://example.com/~username/foo.html`

El servidor buscará por el archivo:

`/home/username/public_html/foo.html`

En el ejemplo de arriba, `/home/username/` es el directorio principal del usuario (observe que la ruta por defecto al directorio principal del usuario puede variar).

Hay que asegurarse que los permisos de los directorios principales de usuario esten configurados correctamente. El valor de los permisos deben ser de 0711. Los bits de lectura (r) y ejecución (x) deben estar activados en el directorio del usuario `public_html` (0755 también funcionará). Los archivos servidos en un directorio principal de usuario `public_html` debe estar configurados, por lo menos, a 0644.

VirtualHost. Las etiquetas `<VirtualHost>` y `</VirtualHost>` crean un contenedor mostrando las características de un host virtual. El contenedor `VirtualHost` acepta la mayoría de las directrices de configuración.

Se proporciona un contenedor `VirtualHost` en comentarios en `httpd.conf`, el cual ilustra el con-

junto mínimo de directrices de configuración necesarias para cada host virtual. Refiérase a la Sección 7, “Hosts virtuales” para obtener más información sobre los host virtuales.

Nota

El contenedor de host virtuales SSL por defecto reside en el archivo `/etc/httpd/conf.d/ssl.conf`.

5.2. Configuración de directrices para SSL

Las directrices en el archivo `/etc/httpd/conf.d/ssl.conf` se pueden configurar para activar las comunicaciones Web seguras usando SSL y TLS.

SetEnvIf. `SetEnvIf` configura las variables del entorno basado en las cabeceras de las conexiones entrantes. *No* es una directriz únicamente de SSL, aunque se presenta en el archivo `/etc/httpd/conf.d/ssl.conf`. En este contexto, su propósito es desactivar el keepalive del HTTP y permitir a SSL cerrar la conexión sin una alerta de notificación desde el navegador del cliente. Esta configuración es necesaria para ciertos navegadores que no cierran de forma confiable la conexión SSL.

Para más información sobre otras directrices dentro del archivo de configuración SSL, consulte los siguientes URLs:

- http://localhost/manual/mod/mod_ssl.html
- http://httpd.apache.org/docs/2.2/mod/mod_ssl.html

Nota

En la mayoría de los casos, las directrices SSL son configuradas apropiadamente durante la instalación de Red Hat Enterprise Linux. Tenga cuidado cuando altere las directrices del Servidor Seguro HTTP de Apache pues un error en la configuración puede provocar que el servidor sea vulnerable en términos de seguridad.

5.3. Directrices MPM específicas al pool de servidores

Como se explicó en la Sección 2.2.1.2, “Regulación del tamaño del pool de servidores” la responsabilidad del manejo de las características del pool de servidores recae sobre un grupo de módulos llamado MPMs bajo el Servidor HTTP Apache versión 2.0. Las características del pool de servidores difieren dependiendo de cual MPM se utiliza. Por esta razón, es necesario un contenedor `IfModule` para poder definir el pool de servidores del MPM en uso.

Por defecto, el Servidor HTTP Apache 2.0 define el pool de servidores para ambos MPMs: `prefork` y `worker`.

La sección siguiente lista las directrices encontradas dentro de los contenedores del pool de

servidores específicos al MPM.

MaxClients. La directriz `MaxClients` establece un límite en el número total de procesos del servidor o clientes conectados simultáneamente que se pueden ejecutar a la vez. El propósito principal de esta directriz es prevenir que un Servidor HTTP Apache descontrolado vuelva inestable el sistema operativo. Para los servidores muy ocupados este valor debería ser un valor alto. El valor por defecto es 150, sin importar el MPM que se utilice. Sin embargo, no se recomienda que el valor del comando `MaxClients` supere `256` cuando se utilice el MPM `prefork`.

MaxRequestsPerChild. `MaxRequestsPerChild` establece el número máximo de peticiones que cada proceso de servidor hijo procesa antes de morir. La principal razón para configurar `MaxRequestsPerChild` es evitar que procesos de larga vida gasten memoria. El valor predeterminado de `MaxRequestsPerChild` para el MPM `prefork` es de `4000` y, para el MPM `worker`, es `0`.

MinSpareServers y MaxSpareServers. Estos valores solamente se utilizan con el MPM `prefork`. Ellos ajustan como el Servidor HTTP Apache se adapta dinámicamente a la carga percibida manteniendo un número apropiado de procesos de servidor extras o de repuesto basado en el número de peticiones entrantes. El servidor comprueba el número de servidores que esperan peticiones y elimina algunos si el número es más alto que `MaxSpareServers` o crea algunos si el número de servidores es menor que `MinSpareServers`.

El valor predeterminado de `MinSpareServers` es `5` y el de `MaxSpareServers` es `20`. Estos valores predeterminados son suficientes en la mayoría de los casos. Tenga cuidado de no incrementar el número de `MinSpareServers` a un número muy elevado ya que creará una gran carga de procesamiento, incluso cuando el tráfico fuese bajo.

MinSpareThreads y MaxSpareThreads. Estos valores solamente son utilizado con el MPM `worker`. Ellos ajustan como el Servidor HTTP Apache se adapta dinámicamente a la carga percibida manteniendo un número apropiado de hilos de servidores extras basado en el número de peticiones entrantes. El servidor comprueba el número de hilos de servidores que esperan peticiones y elimina algunos si el número es más alto que `MaxSpareThreads` o crea algunos si el número de servidores es menor que `MinSpareThreads`.

El valor predeterminado de `MinSpareThreads` es `25` y el de `MaxSpareThreads` es `75`. Estos valores predeterminados son apropiados en la mayoría de los casos. El valor para `MaxSpareThreads` debe ser mayor o igual que la suma de `MinSpareThreads` y `ThreadsPerChild`, de lo contrario el Servidor HTTP Apache lo corregirá automáticamente.

StartServers. La directriz `StartServers` establece cuántos procesos de servidor serán creados al arrancar. Ya que el servidor Web crea y elimina dinámicamente procesos de servidor según el tráfico, no se necesitará cambiar este parámetro. El servidor web está configurado para arrancar `8` procesos del servidor al arrancar para el MPM `prefork` y `2` para el MPM `worker`.

ThreadsPerChild. Este valor solamente es utilizado con el MPM `worker`. Configura el número de hilos dentro de cada proceso hijo. El valor por defecto para esta directriz es `25`.

6. Añadir módulos

El Servidor HTTP Apache se distribuye con un número de módulos. Para obtener más información sobre los módulos HTTP Apache diríjase a http://httpd.apache.org/docs/2.2/mod/.

El Servidor HTTP Apache soporta *Objetos Compartidos Dinámicamente* (Dynamically Shared Objects, *DSO*s) o módulos, los cuales se pueden cargar fácilmente en el momento de ejecución.

El Proyecto Apache proporciona Documentación DSO completa en línea en http://httpd.apache.org/docs/2.2/dso.html. Si el paquete `http-manual` está instalado, se puede encontrar documentación sobre DSOs en http://localhost/manual/mod/.

Para que el Servidor HTTP Apache utilice un DSO, debe estar especificado en una directriz `LoadModule` dentro de `/etc/httpd/conf/httpd.conf`; si el módulo es proporcionado por un paquete separado, la línea debe aparecer dentro del archivo de configuración de módulos en el directorio `/etc/httpd/conf.d/`. Refiérase a la LoadModule para obtener más información.

Si está añadiendo o eliminando módulos desde `http.conf`, debe recargar o volver a iniciar el Servidor HTTP Apache como se explica en la Sección 3, “Arrancar y detener httpd”.

Si está creando un nuevo módulo, instale primero el paquete `httpd-devel` pues contiene los archivos include, las cabeceras de archivos así como también la aplicación *APache eXtenSion* (`/usr/sbin/apxs`), la cual utiliza los archivos include y las cabeceras para compilar DSOs.

Después de escribir un módulo, utilice `/usr/sbin/apxs` para compilar las fuentes del módulo fuera del árbol de fuentes Apache. Para obtener más información sobre el uso del comando `/usr/sbin/apxs`, vea la documentación de Apache en línea en http://httpd.apache.org/docs/2.2/dso.html y en la página man de `apxs`.

Una vez compilado, coloque el módulo en el directorio `/usr/lib/httpd/modules/`. Para las plataformas RHEL que utilizan el espacio de usuario de 64 bits predeterminado (x86_64, ia64, ?) esta ruta será `/usr/lib64/httpd/modules/`. Luego añada una línea `LoadModule` al archivo `httpd.conf` usando la siguiente estructura:

```
LoadModule <module-name> <path/to/module.so>
```

Donde `<module-name>` es el nombre del módulo y `<path/to/module.so>` a la ruta del DSO.

7. Hosts virtuales

La característica incorporada del Servidor HTTP Apache de máquinas virtules permite al servidor rpoporcionar diferente información basado en cuál dirección IP, nombre de host o puerto está siendo solicitado. Un manual completo para el uso de hosts virtuales está disponible en http://httpd.apache.org/docs/2.2/vhosts/.

7.1. Configuración de máquinas virtuales

Para crear un host virtual basado en nombre, lo mejor es utilizar el contenedor del host virtual proporcionado en `httpd.conf` como un ejemplo.

El ejemplo de máquina virtual se lee como sigue:

```
#NameVirtualHost *:80 # #<VirtualHost *:80> # ServerAdmin webmaster@dummy-host.example.com # DocumentRoot /
```

Para activar máquinas virtuales basadas en nombre, quite los comentarios de la línea `NameVirtualHost` eliminando el símbolo de numeral o almohadilla (`#`) y reemplazando el asterísco (`*`)

con la dirección IP asignada a la máquina.

Luego, configure un host virtual, quitando los comentarios y personalizando el contenedor `<VirtualHost>`.

En la línea `<VirtualHost>`, cámbie el asterísco (`*`) a la dirección IP del servidor. Cambie el `ServerName` al nombre DNS *válido* asignado a la máquina y configure las otras directrices si es necesario.

El contenedor `<VirtualHost>` es altamente personalizable y acepta casi cada directriz dentro de la configuración del servidor principal.

Sugerencia

Si se está configurando un host virtual para que escuche en un puerto no predeterminado, se debe agregar ese puerto a la directriz `Listen` en la sección de configuraciones globales del archivo `/etc/httpd/conf/http.conf`.

Para activar un host virtual creado recientemente, el Servirdor HTTP Apache se debe volver a cargar o a reiniciar. Consulte la Sección 3, “Arrancar y detener httpd” para ver las instrucciones sobre como hacer esto.

Se proporciona información completa sobre la creación y configuración de máquinas virtuales basadas en nombre y en dirección IP en http://httpd.apache.org/docs/2.2/vhosts/.

8. Configuración del Servidor Seguro Apache HTTP

Este capítulo proporciona información básica sobre SErvidor HTTP Apache con el módulo de seguridad `mod_ssl` activado para utilizar las bibliotecas y el conjunto de herramientas de OpenSSL. La combinación de estos tres componentes se conocen en este capítulo como el servidor Web seguro o simplemente como el servidor seguro.

El módulo `mod_ssl` es un módulo de seguridad para el Servidor HTTP Apache. El módulo `mod_ssl` utiliza las herramientas proporcionadas por el Proyecto OpenSSL para añadir una caracteríStcia muy importante al Servidor HTTP Apache— la habilidad de encriptar comunicaciones. Por el contrario, las comunicaciones HTTP comunes entre un navegador y un servidor Web se envían en texto plano, el cual lo puede interceptar y leer alguien en la ruta entre el navegador y el servidor.

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 en 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` se encuentra en `/etc/httpd/conf.d/ssl.conf`. Para cargar este archivo y hacer que `mod_ssl` funcione tiene que tener la declaración `Include conf.d/*.conf` en el archivo `/etc/httpd/conf/httpd.conf`. Esta declaración esta incluída por defecto en el archivo de configuración predeterminado del Servidor HTTP Apache.

8.1. Vista preliminar de los paquetes relacionados con la seguridad

Para habilitar el servidor seguro tiene que tener los siguientes paquetes instalados como mínimo:

`httpd`
: El paquete `httpd` contiene el demonio `httpd` y herramientas relacionadas, archivos de configuración, iconos, módulos del Servidor HTTP Apache, páginas man y otros archivos qu el Servidor HTTP apache utiliza.

`mod_ssl`
: El paquete `mod_ssl` incluye el módulo`mod_ssl` que proporciona criptografía fuerte para el Servidor HTTP Apache a través de los protocolos SSL, Secure Sockets Layer y TLS, Transport Layer Security.

`openssl`
: El paquete `openssl` contiene el kit de herramientas OpenSSL. Este kit implementa los protocolos SSL y TLS y también incluye una biblioteca criptográfica de uso general.

`crypto-utils`
: El paquete `crypto-utils` proporciona un grupo de herramientas para generar y administrar certificados SSL y llaves privadas. Entre estas herramientas se encuentra `genkey`.

Adicionalmente, otros paquetes de software pueden proporcionar ciertas funcionalidades de seguridad (pero que no son requeridas para que funcione el servidor seguro):

8.2. Vista preliminar de certificados y seguridad

Su servidor seguro proporciona seguridad utilizando una combinación del protocolo SSL (del inglés Secure Sockets Layer) y (en la mayoría de los casos) un certificado digital de una Autoridad de Certificación (AC). SSL aneja la comunicación encriptada así como la autenticación mutua entre los navegadores y su servidor seguro. El certificado digital AC aprobado proporciona autenticación para su servidor seguro (el AC pone su reputación detras de su certificación de la identidad de su organización). Cuando su navegador se comunica utilizando el ncriptamiento SSL, se utiliza el prefijo `https://` al comienzo del Localizador Unificado de Recursos (URL por sus siglas en inglés) 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.

De otra forma puede crear su propio certificado auto-firmado. Sin embargo, observe que estos certificados auto-firmados no se deben utilizar en la mayoría de los entornos de producción. Los certificados auto-firmados no son aceptados automáticamente por el usuario de un navegador — el navegaodr le pide a los usuarios que acepte el certificado y que cree una conexión segura. Para obtener más información sobre las diferencias entre certificados auto-firmados y los firmados por ACs vaya a Sección 8.4, “Tipos de certificados”.

Una vez que haya obtenido un certificado auto-firmado o un certificado firmado del AC que haya escogido, tiene que instalarlo en su servidor seguro.

8.3. Uso de claves y certificados preexistentes

Si ya tiene una llave y un certificado (por ejemplo si está instalando el servidor seguro para reemplazar el producto del servidor seguro de otra compañia), probablemente podrá utilizar su llave y cetificado existentes con el servidor seguro. Las siguientes dos situaciones proporcionan ejemplos de cuando ustes no puede utilizar su certificado o llave extistentes:

- *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/pki/tls/private/server.key
```

Mueva su archivo de certificado existente a:

```
/etc/pki/tls/certs/server.crt
```

Si está actualizando desde el Servidor Web Seguro de 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/pki/tls/private/server.key mv /etc/httpd/conf/httpsd.crt /etc/pki/tls/c
```

Después inicie su servidor seguro con el comando:

```
/sbin/service httpd start
```

8.4. Tipos de certificados

Si ha instalado su servidor seguro desde el paquete RPM proporcionado por Red Hat se genera una llave aleatoria y un certificado de prueba y son puestos en sus directorios apropiados. Sin embargo, antes de que empiece a usar su servidor seguro necesitará generar su propia llave y obtener un certificado que identifique correctamente su servidor.

Necesita una llave 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 auto-firmado para su servidor seguro pero tenga en cuenta de que un certificado auto-firmado no proporciona la misma funcionalidad que un certificado firmado por un AC. Un certificado auto-firmado no es reconocido automáticamente por la mayoría de los navegadores y no proporciona ninguna garantía en realción con la identidad de la organización que proporciona el sitio web. UN certificado firmado por un AC proporciona estas dos habilidades tan importantes para un servidor seguro. Si va a utilizar su servidor seguro en un entorno de producción se recomienda que tenga un certificado firmado por AC.

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. Envíe el pedido de certificado junto con los documentos que prueban su identidad a AC. Red Hat no hace recomendaciones sobre el tipo de autoridad de certificado que debe escoger. Su decisión debe estar basada en experiencias previas, experiencias de amigos o colegas o incluso en factores monetarios.

   Una vez que haya decidido por un CA, necesitará seguir las instrucciones que se le indiquen para obtener un certificado de ellos.

4. Cuando la AC se encuentra satisfecha con su presumible identidad ellos le proporcionarán un certificado digital.

5. Instale este certificado en su servidor seguro y comience a manejar transacciones seguras.

Ya sea que usted vaya a adquirir un certificado de una AC o vaya a generar su propio certificado auto-firmado, el primer paso es generar una llave. Refiérase a Sección 8.5, “Generar una clave” para obtener las instrucciones.

8.5. Generar una clave

Tiene que ser root para generar una clave.

Primero, utilice el comando `cd` para cambiar al directorio `/etc/httpd/conf/`. Con los siguientes comandos elimine la llave y el certificado falso que se generaron durante la instalación:

```
rm ssl.key/server.keyrm ssl.crt/server.crt
```

El paquete `crypto-utils` contiene la herramienta `genkey`, la cual se puede utilizar para generar llaves, así como lo implica su nombre. Para crear su propia llave privada asegúrese de que el paquete `crypto-utils` se encuentre instalado. Puede encontrar más opciones si escribe `man genkey` en su terminal. Asumiendo de que usted quiere generar llaves para www.example.com utilizando la herramienta `genkey` escriba el siguiente comando en su terminal:

```
genkey www.example.com
```

Observe que el proceso basado en `make` ya no se incluye junto con RHEL 5. Esto iniciará la interfaz gráfica de usuario `genkey`. La figura que se encuentra a continuación ilustra la primera pantalla. Para navegar utilice las flechas y tab. Estas ventanas indican en donde se almacenará su llave y le preguntará si desea continuar o cancelar la operación. Para proceder al siguiente paso seleccione **Siguiente** y oprima la tecla Intro.

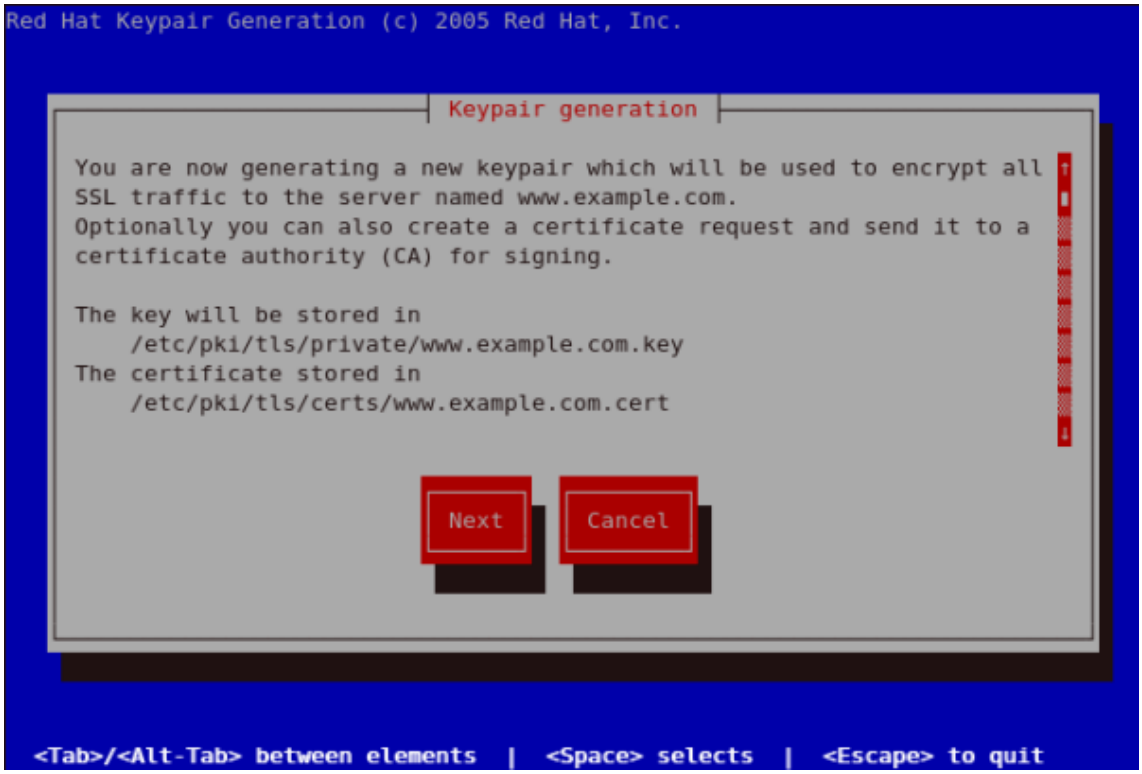


Figura 7.11. Generación del Keypair

La siguiente pantalla le pedirá que seleccione el tamaño de su llave. Como se indicó anteriormente entre más pequeña sea su llave recibirá más rápido respuesta de su servidor y su nivel de seguridad será menor. Utilice las flechas para seleccionar el tamaño de la llave y haga clic en **Siguiente** para proceder al siguiente paso. La figura a continuación ilustra la pantalla de selección del tamaño de la llave.

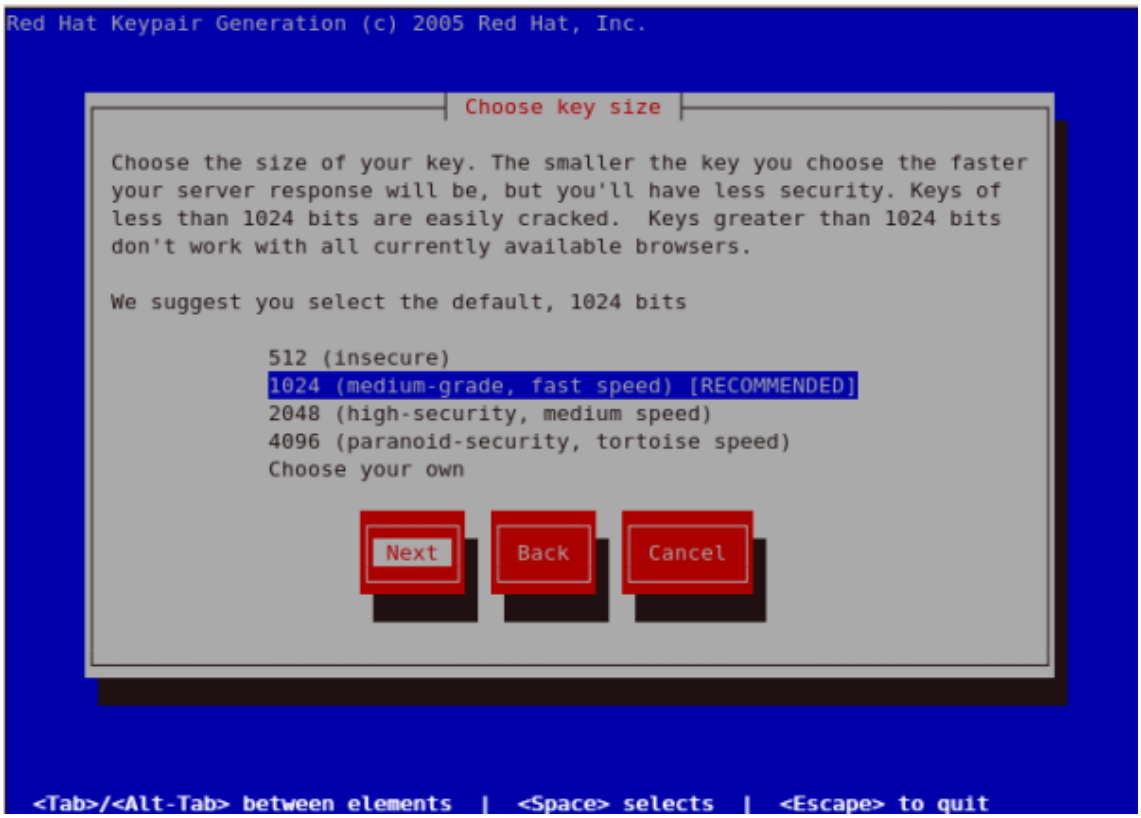


Figura 7.12. Selección del tamaño de la llave

Al seleccionar el siguiente paso se iniciará el proceso de generación de bits que puede llegar a tomar un poco de tiempo dependiendo del tamaño de la llave que seleccionó. Entre más grande sea su llave más tiempo se tomará en generarla.

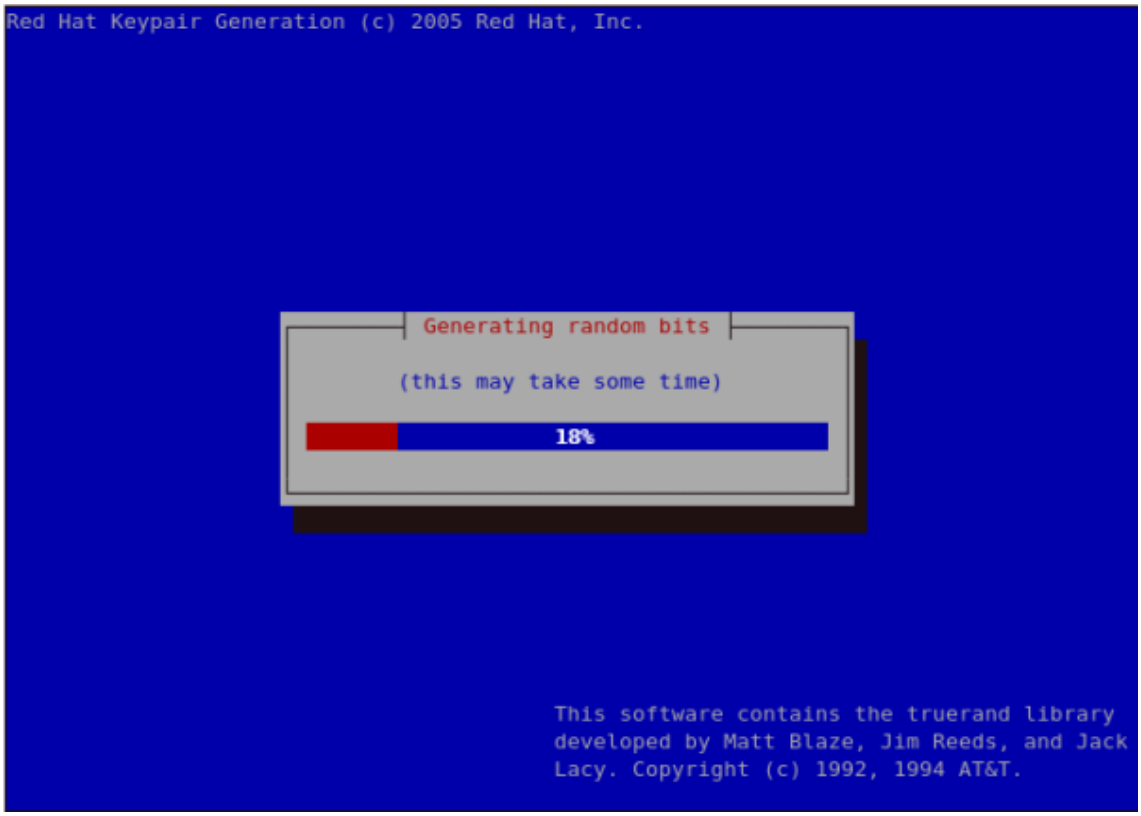


Figura 7.13. Generación de bits aleatorios

Al generar su llave se le pedirá que envie un Pedido de Certificado a una Autoridad de Certificación (AC).

Figura 7.14. Generar CSR

Al seleccionar **Sí** le pedirá que seleccione la Autoridad de Certificación a la cual usted le desea enviar la petición. Al seleccionar **No** le permitirá generar un certificado auto-firmado. El siguiente paso se encuentra ilustrado en Figura 7.17, “Generación de un certificado auto-firmado para su servidor”.

Figura 7.15. Seleccionar una Autoridad de Certificación (AC)

En Selección de su opción preferida escoja **Siguiente** para proceder al siguiente paso. La siguiente pantalla le permititrá ingresar los detalles de su certificado.

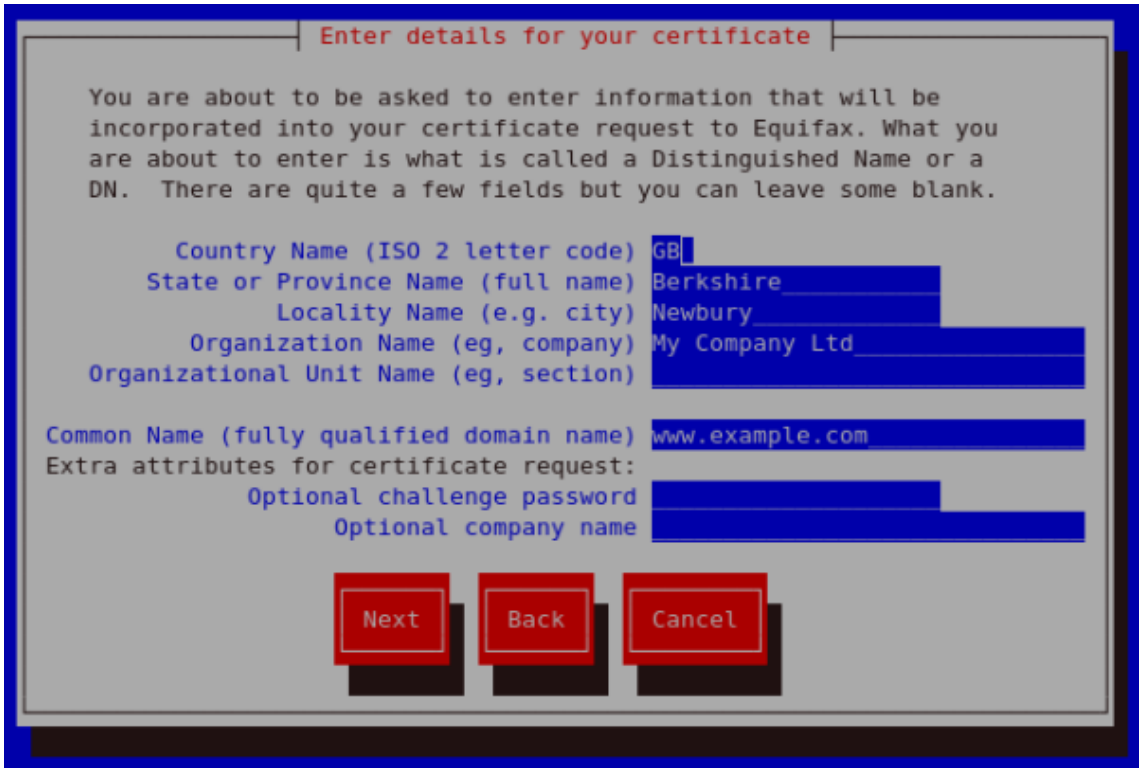


Figura 7.16. Ingrese los detalles para su certificado

Si prefiere generar un par de claves con un certificado de auto-firma no debe generar un CSR. Para hacer esto, selccione **No** como su opción prefeerida en la pantalla para Generación de CSR. Esto le presentará la siguiente figura desde la cual usted puede ingresar los detalles de su certificado. Al ingresar estos detalles y al oprimir la tecla intro verá la Figura 7.19, “Protección de su llave privada” desde donde puede escoger el encriptar o no su llave privada.

Figura 7.17. Generación de un certificado auto-firmado para su servidor

Al ingresar los detalles de su certificado seleccione **Siguiente** para continuar. La figura que se encuentra a continuación ilustra un ejemplo de la pantalla siguiente que aparecerá después de completar los detalles para un certificado que se va a enviar a Equifax. Observe que esta pantalla no aparecerá si se encuentra generando una llave auto-firmada para su servidor.

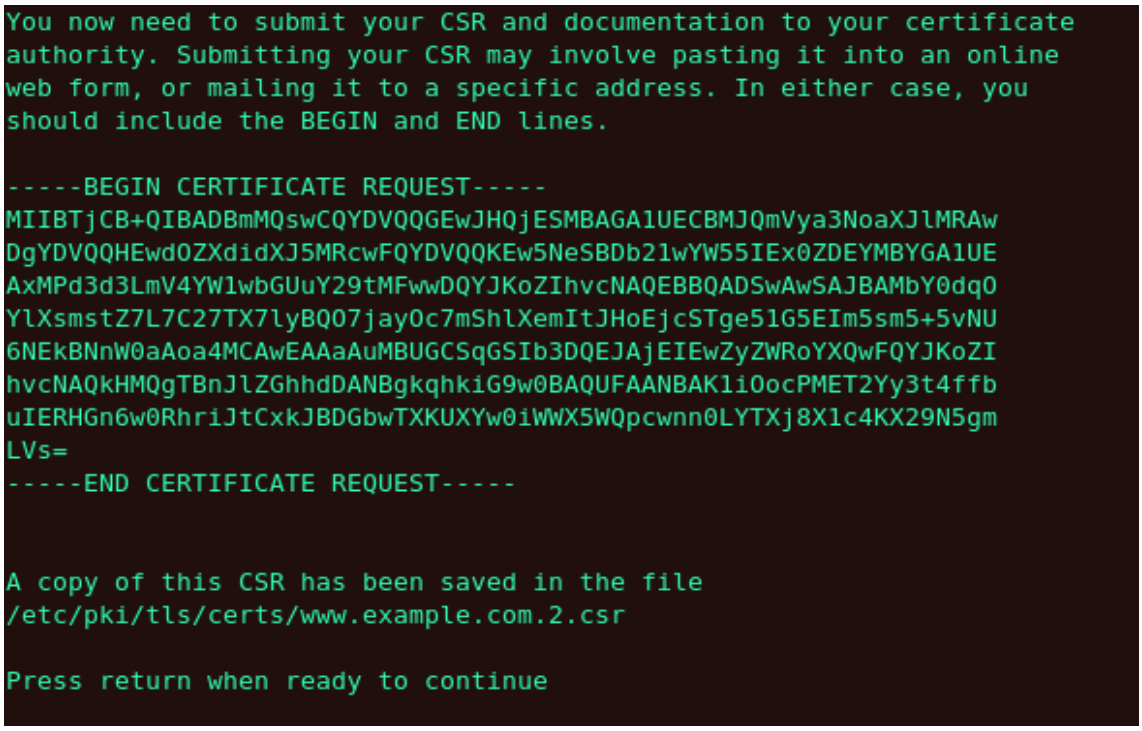


Figura 7.18. Inicie pedido de certificado

Al oprimir la tecla intro aparecerá la siguiente pantalla desde la cual puede habilitar o deshabilitar la opción de encriptar la llave privada. Utilice la barra espaciadora para escoger. Cuando se encuentra habilitada aparecerá un caracter [*]. Al seleccionar su opción preferida seleccione **Siguiente** para continuar al siguiente paso.

Figura 7.19. Protección de su llave privada

La siguiente pantalla le permitirá configurar la contraseña de la llave.

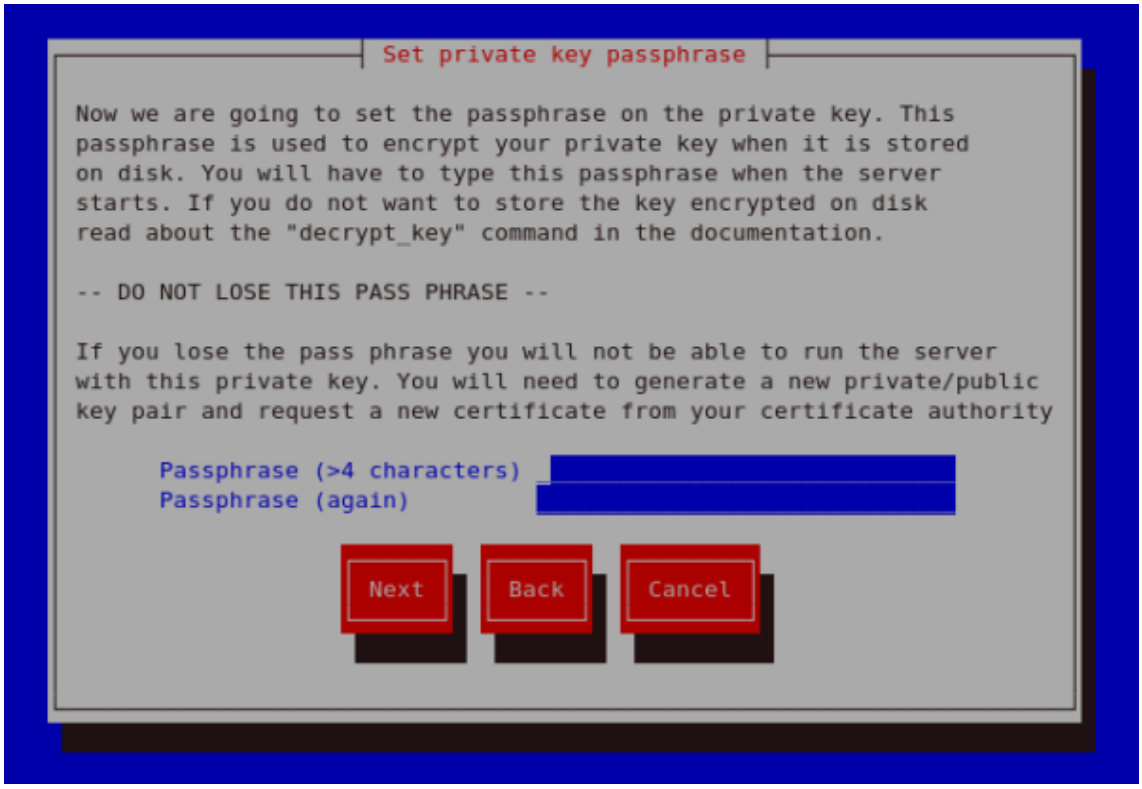


Figura 7.20. Configurar contraseña

Si trata de ejecutar `genkey makeca` en un servidor que ya tiene una pareja de llaves existentes aparecerá un mensaje de error como se ilustra a continuación. Necesita borrar su archivo de llave existente como se indica para poder generar un nuevo par de llaves.

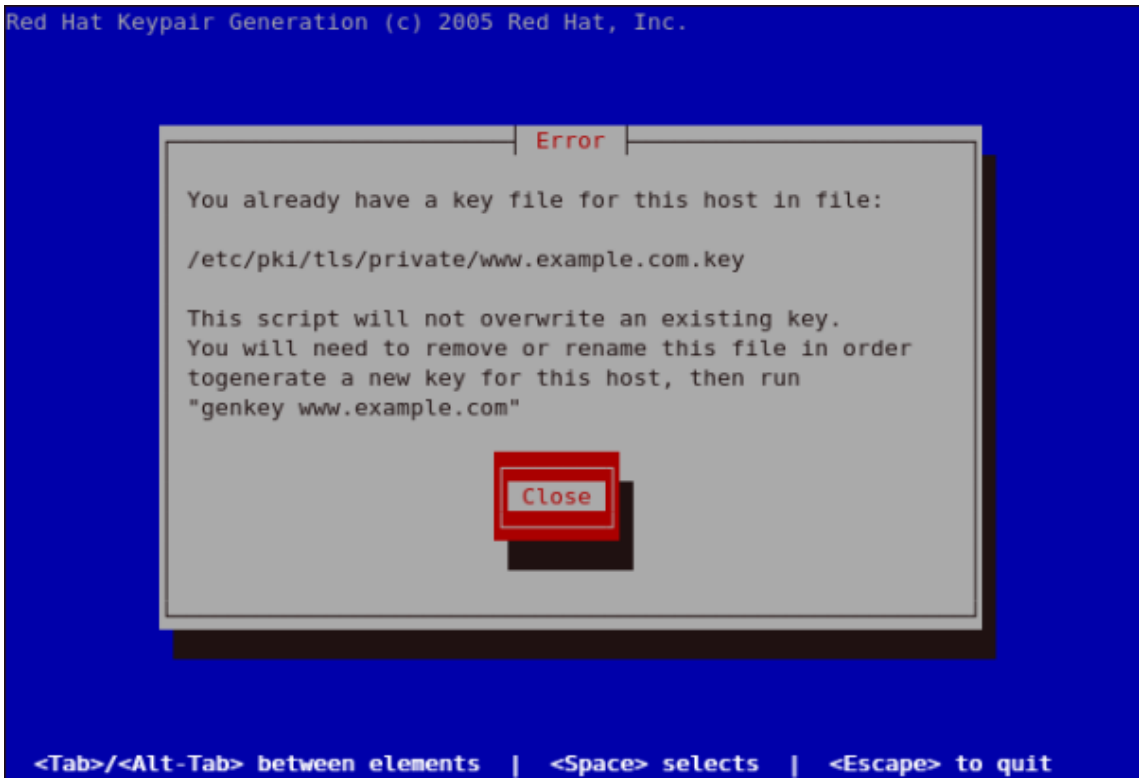


Figura 7.21. genkey error

- http://httpd.apache.org/docs/2.2/ssl/
- http://httpd.apache.org/docs/2.2/vhosts/

8.6. Cómo configurar el servidor para utilizar la nueva clave

Los pasos para configurar el Servidor HTTP Apache para poder utilizar la nueva llave son los siguientes:

- Obtenga el certificado firmado del AC después de enviar el CSR.
- Copie el certificado a la ruta, por ejemplo `/etc/pki/tls/certs/www.example.com.crt`
- Modifique `/etc/httpd/conf.d/ssl.conf`. Cambie las líneas del SSLCertificateFile y SSLCertificateKey para que reflejen:

  ```
  SSLCertificateFile /etc/pki/tls/certs/www.example.com.crt
  SSLCertificateKeyFile /etc/pki/tls/private/www.example.com.key
  ```

  en donde la parte "www.example.com" debe concordar con el argumento pasado en el comando `genkey`.

9. Recursos adicionales

Para mayor información sobre el Servidor HTTP Apache consulte los siguientes recursos:

9.1. Sitios Web de utilidad

- http://httpd.apache.org/ — El sitio oficial para el Servidor HTTP Apache con documentación sobre todas las directrices y módulos predeterminados.
- http://www.modssl.org/ — El sitio oficial para `mod_ssl`.
- http://www.apacheweek.com/ — Información semanal completa sobre todas las cosas de Apache.

Capítulo 8. FTP

El Protocolo de transferencia de archivos (FTP) es uno de los protocolos más viejos y populares que se encuentran en la Internet hoy día. Su objetivo es el de transmitir archivos exitósamente entre máquinas en una red sin que el usuario tenga que iniciar una sesión en el host remoto o que requiera tener conocimientos sobre cómo utilizar el sistema remoto. FTP permite a los usuarios acceder a archivos en sistemas remotos usando un conjunto de comandos estándar muy simples.

Este capítulo describe los elementos básicos de este protocolo, así como también las opciones de configuración para el servidor FTP primario que se entrega con Red Hat Enterprise Linux, `vsftpd`.

1. El Protocolo de Transferencia de Archivos

Sin embargo, puesto que FTP está tan extendido en la Internet, se requiere a menudo para compartir archivos con el público. Por lo tanto, los administradores de sistemas deberían estar conscientes de las características únicas del protocolo FTP.

1.1. Puertos múltiples, modos múltiples

A diferencia de la mayoría de los protocolos utilizados en Internet, FTP requiere de múltiples puertos de red para funcionar correctamente. Cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor — conocido como el *puerto de comandos*. Se utiliza este puerto para arrojar todos los comandos al servidor. Cualquier petición de datos desde el servidor se devuelve al cliente a través del *puerto de datos*. El número de puerto para las conexiones de datos y la forma en la que las conexiones son inicializadas varía dependiendo de si el cliente solicita los datos en modo *activo* o en modo *pasivo*.

A continuación se describen estos modos:

modo activo
: El modo activo es el método original utilizado por el protocolo FTP para la transferencia de datos a la aplicación cliente. Cuando el cliente FTP inicia una transferencia de datos, el servidor abre una conexión desde el puerto 20 en el servidor para la dirección IP y un puerto aleatorio sin privilegios (mayor que 1024) especificado por el cliente. Este arreglo implica que la máquina cliente debe poder aceptar conexiones en cualquier puerto superior al 1024. Con el crecimiento de las redes inseguras, tales como Internet, es muy común el uso de cortafuegos para proteger las máquinas cliente. Debido a que estos cortafuegos en el lado del cliente normalmente rechazan las conexiones entrantes desde servidores FTP en modo activo, se creó el modo pasivo.

modo pasivo
: La aplicación FTP cliente es la que inicia el modo pasivo, de la misma forma que el modo activo. El cliente FTP indica que desea acceder a los datos en modo pasivo y el servidor proporciona la dirección IP y el puerto aleatorio, sin privilegios (mayor que 1024) en el ser-

vidor. Luego, el cliente se conecta al puerto en el servidor y descarga la información requerida.

Mientras que el modo pasivo resuelve el problema de la interferencia del cortafuegos en el lado del cliente con las conexiones de datos, también puede complicar la administración del cortafuegos del lado del servidor. Una de las formas de limitar el número de puertos abiertos en el servidor es limitando el rango de puertos sin privilegios en el servidor FTP. Esta acción también simplificará la tarea de crear reglas para el cortafuegos del servidor. Consulte la Sección 5.8, “Opciones de red” para más detalles sobre cómo limitar puertos pasivos.

2. Servidores FTP

Red Hat Enterprise Linux se entrega con dos servidores FTP diferentes:

- **Acelerador de Contenidos Red Hat** — Un servidor Web basado en el kernel que ofrece un servidor web y servicios FTP de alto rendimiento. Puesto que la velocidad es su objetivo principal de diseño, su funcionalidad es limitada y solamente se ejecuta como FTP anónimo. Para más información sobre la configuración y administración del **Acelerador de Contenidos Red Hat**, consulte la documentación disponible en línea en http://www.redhat.com/docs/manuals/tux/.
- `vsftpd` — un demonio FTP rápido y seguro. Este es el preferido en Red Hat Enterprise Linux. El resto de este capítulo se enfoca en `vsftpd`.

2.1. `vsftpd`

El demonio FTP `vsftpd` (o Very Secure FTP Daemon) está diseñado desde sus fundamentos para ser rápido, estable y lo más importante, seguro. Su habilidad para manejar grandes números de conexiones de forma eficiente y segura es lo que hace que `vsftpd` sea el único FTP independiente distribuido con Red Hat Enterprise Linux.

El modelo de seguridad utilizado por `vsftpd` tiene tres aspectos principales:

- *Clara separación de procesos privilegiados y sin privilegios* — Procesos separados manejan tareas diferentes y cada uno de estos procesos se ejecuta con los privilegios mínimos requeridos para la tarea.
- *Las tareas que requieren altos privilegios son manejadas por procesos con los mínimos privilegios necesarios* — Influenciando las compatibilidades encontradas en la biblioteca `libcap`, las tareas que usualmente requieren privilegios de superusuario se pueden ejecutar de forma más segura desde un proceso menos privilegiado.
- *La mayoría de los procesos se ejecutan enjaulados en un ambiente `chroot`* — Siempre que sea posible, se cambia la raíz de los procesos al directorio compartido; este directorio se considera luego como la jaula `chroot`. Por ejemplo, si el directorio `/var/ftp/` es el directorio compartido principal, `vsftpd` reasigna `/var/ftp/` al nuevo directorio raíz, conocido como `/`. Esto previene actividades maliciosas de cualquier hacker potencial en algún directorio que no estén por debajo del nuevo directorio root.

El uso de estas prácticas de seguridad tiene el efecto siguiente en cómo `vsftpd` trata con las peticiones:

- *El proceso padre se ejecuta con el mínimo de privilegios requerido* — El proceso padre calcula dinámicamente el nivel de privilegios requerido para minimizar el nivel de riesgos. Los procesos hijo manejan la interacción directa con los clientes FTP y se ejecutan casi sin ningún privilegio.
- *Todas las operaciones que requieren altos privilegios son manejadas por un pequeño proceso padre* — Similar a Servidor HTTP Apache, `vsftpd` lanza procesos hijos sin privilegios para manejar las conexiones entrantes. Esto permite al proceso padre privilegiado, ser tan pequeño como sea posible y manejar relativamente pocas tareas.
- *El proceso padre no confia en ninguna de las peticiones desde procesos hijos sin privilegios* — Las comunicaciones con procesos hijos se reciben sobre un socket y la validez de cualquier información desde un proceso hijo es verificada antes de proceder.
- *La mayor parte de la interacción con clientes FTP la manejan procesos hijo sin privilegios en una jaula `chroot`.* — Debido a que estos procesos hijo no tienen privilegios y solamente tienen acceso al directorio que está siendo compartido, cualquier proceso fallido solamente permitirá al atacante acceder a los archivos compartidos.

3. Archivos instalados con `vsftpd`

El RPM `vsftpd` instala el demonio (`/usr/sbin/vsftpd`), su archivo de configuración y otros archivos relacionados, así como también los directorios FTP en el sistema. La siguiente es una lista de los archivos y directorios considerados más a menudo cuando se configura `vsftpd`:

- `/etc/rc.d/init.d/vsftpd` — El *script de inicialización* (*initscript*) utilizado por el comando `/sbin/service` para iniciar, detener o volver a cargar `vsftpd`. Consulte la Sección 4, “Iniciar y detener vsftpd” para obtener mayor información sobre el uso de este script.
- `/etc/vsftpd/vsftpd.conf` — El archivo de configuración para `vsftpd`. Consulte la Sección 5, “Opciones de configuración vsftpd” para una lista de las opciones importantes que se encuentran en este archivo.
- `/etc/vsftpd.ftpusers` — Una lista de los usuarios que no tienen permitido conectarse a `vsftpd`. Por defecto esta lista incluye a los usuarios `root`, `bin` y `daemon`, entre otros.
- `/etc/vsftpd.user_list` — Este archivo se puede configurar para negar o permitir el acceso a los usuarios listados, dependiendo de si la directriz `userlist_deny` está configurada a `YES` (por defecto) o a `NO` en `/etc/vsftpd/vsftpd.conf`. Si se utiliza `/etc/vsftpd.user_list` para permitir acceso a los usuarios, los nombres de usuarios listados *no* deben aparecer en `/etc/vsftpd.ftpusers`.
- El directorio `/var/ftp/` — El directorio que contiene los archivos servidos por `vsftpd`. También contiene el directorio `/var/ftp/pub/` para los usuarios anónimos. Ambos directorios están disponibles para la lectura de todos, pero sólo el superusuario o root puede escribir en el.

4. Iniciar y detener vsftpd

El RPM `vsftpd` instala el script `/etc/rc.d/init.d/vsftpd`, al cual se puede acceder usando el comando `/sbin/service`.

Para iniciar el servidor, escriba como usuario root, lo siguiente:

```
/sbin/service vsftpd start
```

Para detener el servidor, como root escriba:

```
/sbin/service vsftpd stop
```

La opción `restart` es un atajo para detener y volver a iniciar `vsftpd`. Esta es la forma más efectiva para que los cambios de configuración tomen efecto luego de modificar el archivo de configuración para `vsftpd`.

Para reiniciar el servidor, escriba como root:

```
/sbin/service vsftpd restart
```

La opción `condrestart` (*reinicio condicional*) solamente arranca `vsftpd` si está ejecutándose en ese momento. Esta opción es muy útil para scripts, puesto que no arranca el demonio si este no se está ejecutando.

Para reiniciar el servidor de forma condicional, escriba como usuario root:

```
/sbin/service vsftpd condrestart
```

4.1. Iniciar múltiples copias de vsftpd

En ocasiones, se utiliza un computador para servir varios dominios FTP. Esta es una técnica que se conoce como *multihoming* (multi-anfitrión). Una forma de hacer multihome usando `vsftpd` es ejecutando múltiples copias del demonio, cada uno con su propio archivo de configuración.

Para hacerlo, primero asigne todas las direcciones IP relevantes a los dispositivos de red o a los alias de dispositivos en el sistema. Consulte el Capítulo 2, *Configuración de la red* para obtener mayor información sobre la configuración de dispositivos de red y aliases. Se puede encontrar información adicional sobre los scripts de configuración de red en el Capítulo 1, *Interfaces de red*.

Luego, el servidor DNS para los dominios FTP debe ser configurados para hacer referencia a la máquina correcta. Para obtener mayor información sobre BIND y sus archivos de configuración, consulte el Capítulo 4, *Berkeley Internet Name Domain (BIND)*.

Para que `vsftpd` responda a las peticiones en diferentes direcciones IP, deben estar ejecutándose múltiples copias del demonio. La primera copia se debe ejecutar usando el initiscript `vsftpd`, como se describe en la Sección 4, “Iniciar y detener vsftpd”. Esta copia utiliza el archivo de configuración estándar, `/etc/vsftpd/vsftpd.conf`.

Cada sitio FTP adicional debe tener un archivo de configuración con un nombre único en el directorio `/etc/vsftpd/`, tal como `/etc/vsftpd/vsftpd-site-2.conf`. Cada archivo de configuración

sólo debería de ser legído y escrito por root. Dentro de cada archivo de configuración para cada servidor FTP que se encuentre escuchando en la red IPv4, la siguiente directriz debe ser única:

```
listen_address=N.N.N.N
```

Reemplace *N.N.N.N* con la *única* dirección IP para el sitio FTP que está siendo servido. Si el sitio en cuestión está utilizando IPv6, utilice la directriz `listen_address6`.

Una vez que cada servidor adicional tenga su archivo de configuración, el demonio `vsftpd` se debe lanzar desde un indicador de comandos shell usando el comando siguiente:

```
vsftpd /etc/vsftpd/<configuration-file> [amp   ]
```

En el comando de arriba, reemplace *<configuration-file>* con el nombre único para el archivo de configuración, tal como `/etc/vsftpd/vsftpd-site-2.conf`.

Otras directrices que podría considerar modificar en una base de por servidor son:

- `anon_root`
- `local_root`
- `vsftpd_log_file`
- `xferlog_file`

Para una lista detallada de las directrices disponibles dentro del archivo de configuración `vsftpd`, consulte el Sección 5, “Opciones de configuración vsftpd”.

Para configurar servidores adicionales para que se inicien de forma automática al momento del arranque, añada el comando que se muestra arriba al final del archivo `/etc/rc.local`.

5. Opciones de configuración `vsftpd`

Aún cuando `vsftpd` quizás no ofrezca el nivel de personalización que otros servidores FTP disponible globalmente tienen, `vsftpd` ofrece suficientes opciones para satisfacer la mayoría de las necesidades de un administrador. El hecho de que no está sobrecargado de funcionalidades limita los errores de configuración y de programación.

Toda la configuración de `vsftpd` es manejada por su archivo de configuración, `/etc/vsftpd/vsftpd.conf`. Cada directriz está en su propia línea dentro del archivo y sigue el formato siguiente:

```
<directive>=<value>
```

Para cada directriz, reemplace *<directive>* con una directriz válida y *<value>* con un valor válido.

Importante

No deben existir espacios entre la *<directive>*, el símbolo de igualdad y el *<value>* en una directriz.

Se debe colocar el símbolo de almohadilla (#) antes de una línea en comentarios. El demonio ignorará cualquier línea en comentarios.

Para una lista completa de las directrices disponibles, consulte las páginas man para `vsftpd.conf`.

A continuación se presenta una lista de las directrices más importantes dentro de `/etc/vsftpd/vsftpd.conf`. Todas las directrices que no se encuentren explícitamente dentro del archivo de configuración de `vsftpd` se colocan a sus valores por defecto.

5.1. Opciones de demonios

La lista siguiente presenta las directrices que controlan el comportamiento general del demonio `vsftpd`.

- `listen` — Cuando esta directriz está activada `vsftpd` se ejecuta en modo independiente. Red Hat Enterprise Linux establece este valor a `YES`. Esta directriz no se puede utilizar junto con la directriz `listen_ipv6`.

  El valor predeterminado es `NO`.

- `listen_ipv6` — Cuando esta directriz está activada `vsftpd` se ejecuta en modo independiente, pero solamente escucha a los sockets IPv6. Esta directriz no se puede utilizar junto con la directriz `listen`.

  El valor predeterminado es `NO`.

5.2. Opciones de conexión y control de acceso

La siguiente es una lista de las directrices que controlan el comportamiento de los inicios de sesión y los mecanismos de control de acceso.

- `anonymous_enable` — Al estar activada, se permite que los usuarios anónimos se conecten. Se aceptan los nombres de usuario `anonymous` y `ftp`.

  El valor por defecto es `YES`.

  Consulte la Sección 5.3, “Opciones de usuario anónimo” para una lista de las directrices que afectan a los usuarios anónimos.

- `banned_email_file` — Si la directriz `deny_email_enable` tiene el valor de `YES`, entonces esta directriz especifica el archivo que contiene una lista de contraseñas de correo anónimas que no tienen permitido acceder al servidor.

El valor predeterminado es `/etc/vsftpd.banned_emails`.

- `banner_file` — Especifica un archivo que contiene el texto que se mostrará cuando se establece una conexión con el servidor. Esta opción supersede cualquier texto especificado en la directriz `ftpd_banner`.

  Esta directriz no tiene un valor predeterminado.

- `cmds_allowed` — Especifica una lista delimitada por comas de los comandos FTP que permite el servidor. Se rechaza el resto de los comandos.

  Esta directriz no tiene un valor predeterminado.

- `deny_email_enable` — Si está activada, se le niega el acceso al servidor a cualquier usuario anónimo que utilice contraseñas de correo especificadas en `/etc/vsftpd.banned_emails`. Se puede especificar el nombre del archivo al que esta directriz hace referencia usando la directriz `banned_email_file`.

  El valor predeterminado es `NO`.

- `ftpd_banner` — Si está activada, se muestra la cadena de caracteres especificada en esta directriz cuando se establece una conexión con el servidor. `banner_file` puede sobreescribir esta opción.

  Por defecto, `vsftpd` muestra su pancarta estándar.

- `local_enable` — Al estar activada, los usuarios locales pueden conectarse al sistema.

  El valor por defecto es `YES`.

  Consulte la Sección 5.4, “Opciones del usuario local” para una lista de las directrices que afectan a los usuarios locales.

- `pam_service_name` — Especifica el nombre de servicio PAM para `vsftpd`.

  El valor predeterminado es `ftp`, sin embargo, bajo Red Hat Enterprise Linux, el valor es `vsftpd`.

- El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux, el valor está configurado a `YES`.

- `userlist_deny` — Cuando se utiliza en combinación con la directriz `userlist_enable` y con el valor de `NO`, se les niega el acceso a todos los usuarios locales a menos que sus nombres esten listados en el archivo especificado por la directriz `userlist_file`. Puesto que se niega el acceso antes de que se le pida la contraseña al cliente, al configurar esta directriz a `NO` previene a los usuarios locales a proporcionar contraseñas sin encriptar sobre la red.

  El valor por defecto es `YES`.

- `userlist_enable` — Cuando está activada, se les niega el acceso a los usuarios listados en el archivo especificado por la directriz `userlist_file`. Puesto que se niega el acceso al cliente antes de solicitar la contraseña, se previene que los usuarios suministren contraseñas sin encriptar sobre la red.

El valor predeterminado es NO, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a YES.

- userlist_file — Especifica el archivo al que vsftpd hace referencia cuando la directriz userlist_enable está activada.

  El valor predeterminado es /etc/vsftpd.user_list y es creado durante la instalación.

- cmds_allowed — Especifica una lista separada por comas de los comandos FTP que permite el servidor. Cualquier otro comando es rechazado.

  Esta directriz no tiene un valor predeterminado.

5.3. Opciones de usuario anónimo

A continuación, se presenta una lista de las directrices que controlan el acceso de usuarios anónimos al servidor. Para utilizar estas opciones, la directriz anonymous_enable debe tener el valor de YES.

- anon_mkdir_write_enable — Cuando se activa en combinación con la directriz write_enable, los usuarios anónimos pueden crear nuevos directorios dentro de un directorio que tiene permisos de escritura.

  El valor predeterminado es NO.

- anon_root — Especifica el directorio al cual vsftpd cambia luego que el usuario anónimo se conecta.

  Esta directriz no tiene un valor predeterminado.

- anon_upload_enable — Cuando se usa con la directriz write_enable, los usuarios anónimos pueden cargar archivos al directorio padre que tiene permisos de escritura.

  El valor predeterminado es NO.

- anon_world_readable_only — Si está activada, los usuarios anónimos solamente pueden descargar archivos legibles por todo el mundo.

  El valor por defecto es YES.

- ftp_username — Especifica la cuenta del usuario local (listada en /etc/passwd) utilizada por el usuario FTP anónimo. El directorio principal especificado en /etc/passwd para el usuario es el directorio raíz del usuario FTP anónimo.

  El valor por defecto es ftp.

- no_anon_password — Cuando está activada, no se le pide una contraseña al usuario anónimo.

  El valor predeterminado es NO.

- secure_email_list_enable — Cuando está activada, solamente se aceptan una lista de contraseñas especificadas para las conexiones anónimas. Esto es una forma conveniente de

ofrecer seguridad limitada al contenido público sin la necesidad de usuarios virtuales.

Se previenen las conexiones anónimas a menos que la contraseña suministrada esté listada en `/etc/vsftpd.email_passwords`. El formato del archivo es una contraseña por línea, sin espacios al comienzo.

El valor predeterminado es `NO`.

5.4. Opciones del usuario local

La siguiente es una lista de las directrices que caracterizan la forma en que los usuarios locales acceden al servidor. Para utilizar estas opciones, la directriz `local_enable` debe estar a `YES`.

- `chmod_enable` — Cuando está activada, se permite el comando FTP `SITE CHMOD` para los usuarios locales. Este comando permite que los usuarios cambien los permisos en los archivos.

  El valor por defecto es `YES`.

- `chroot_list_enable` — Cuando está activada, se coloca en una prisión de `chroot` a los usuarios locales listados en el archivo especificado en la directriz `chroot_list_file`.

  Si se utiliza en combinación con la directriz `chroot_local_user`, los usuarios locales listados en el archivo especificado en la directriz `chroot_list_file`, *no* se colocan en una prisión `chroot` luego de conectarse.

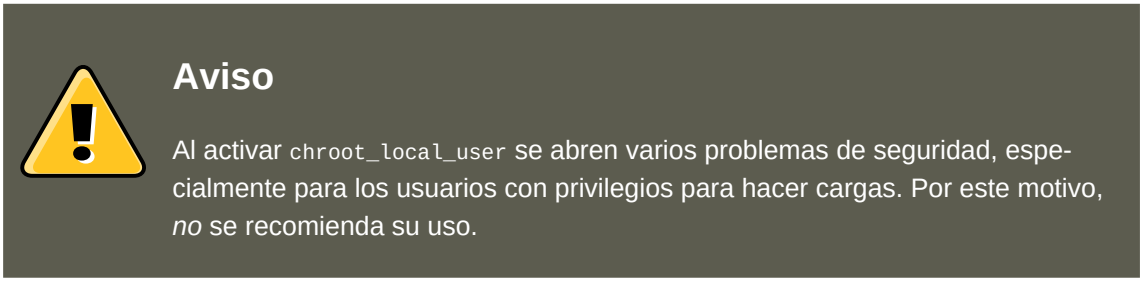
  El valor predeterminado es `NO`.

- `chroot_list_file` — Especifica el archivo que contiene una lista de los usuarios locales a los que se hace referencia cuando la directriz `chroot_list_enable` está en `YES`.

  El valor por defecto es `/etc/vsftpd.chroot_list`.

- `chroot_local_user` — Si está activada, a los usuarios locales se les cambia el directorio raíz (se hace un chroot) a su directorio principal luego de la conexión.

  El valor predeterminado es `NO`.



- `guest_enable` — Al estar activada, todos los usuarios anónimos se conectan como `guest`, el cual es el usuario local especificado en la directriz `guest_username`.

  El valor predeterminado es `NO`.

- `guest_username` — Especifica el nombre de usuario al cual `guest` está asignado.

El valor por defecto es `ftp`.

- `local_root` — Especifica el directorio al cual `vsftpd` se cambia después de que el usuario se conecta.

  Esta directriz no tiene un valor predeterminado.

- `local_umask` — Especifica el valor de umask para la creación de archivos. Observe que el valor por defecto está en forma octal (un sistema numérico con base ocho), que incluye un prefijo de "0". De lo contrario el valor es tratado como un valor entero de base 10.

  El valor por defecto `022`.

- `passwd_chroot_enable` — Cuando se activa junto con la directriz `chroot_local_user`, `vsftpd` cambia la raiz de los usuarios locales basado en la ocurrencia de `/./` en el campo del directorio principal dentro de `/etc/passwd`.

  El valor predeterminado es `NO`.

- `user_config_dir` — Especifica la ruta a un directorio que contiene los archivos de configuración con los nombres de los usuarios locales. Contiene información específica sobre ese usuario. Cualquier directriz en el archivo de configuración del usuario ignora aquellas encontradas en `/etc/vsftpd/vsftpd.conf`.

  Esta directriz no tiene un valor predeterminado.

5.5. Opciones de directorio

La siguiente es una lista de directrices que afectan a los directorios.

- `dirlist_enable` — Al estar activada, los usuarios pueden ver los listados de directorios.

  El valor por defecto es `YES`.

- `dirmessage_enable` — Al estar activada, se mostrará un mensaje cada vez que un usuario entra en un directorio con un archivo de mensaje. Este mensaje se encuentra dentro del directorio al que se entra. El nombre de este archivo se especifica en la directriz `message_file` y por defecto es `.message`.

  El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux, el valor está configurado a `YES`.

- `force_dot_files` — Al estar activada, se listan en los listados de directorios los mensajes que comienzan con un punto (`.`), a excepción de los archivos `.` y `..`.

  El valor predeterminado es `NO`.

- `hide_ids` — Cuando está activada, todos los listados de directorios muestran `ftp` como el usuario y grupo para cada archivo.

  El valor predeterminado es `NO`.

- `message_file` — Especifica el nombre del archivo de mensaje cuando se utiliza la directriz

`dirmessage_enable`.

El valor predeterminado es `.message`.

- `text_userdb_names` — Cuando está activado, se utilizan los nombres de usuarios y grupos en lugar de sus entradas UID o GID. Al activar esta opción puede que reduzca el rendimiento del servidor.

  El valor predeterminado es `NO`.

- `use_localtime` — Al estar activada, los listados de directorios revelan la hora local para el computador en vez de GMT.

  El valor predeterminado es `NO`.

5.6. Opciones de transferencia de archivos

La siguiente es una lista de directrices que afectan a los directorios.

- `download_enable` — Cuando está activada, se permiten las descargas de archivos.

  El valor por defecto es `YES`.

- `chown_uploads` — Si está activada, todos los archivos cargados por los usuarios anónimos pertenecen al usuario especificado en la directriz `chown_username`.

  El valor predeterminado es `NO`.

- `chown_username` — Especifica la propiedad de los archivos cargados anónimamente si está activada la directriz `chown_uploads`.

  El valor predeterminado es `root`.

- `write_enable` — Cuando está activada, se permiten los comandos FTP que pueden modificar el sistema de archivos, tales como `DELE`, `RNFR` y `STOR`.

  El valor por defecto es `YES`.

5.7. Opciones de conexión

A continuación se presenta una lista con las directrices que afectan el comportamiento de conexión de `vsftpd`.

- `dual_log_enable` — Cuando se activa en conjunto con `xferlog_enable`, `vsftpd` escribe simultáneamente dos archivos: un registro compatible con `wu-ftpd` al archivo especificado en la directriz `xferlog_file` (por defecto `/var/log/xferlog`) y un archivo de registro estándar `vsftpd` especificado en la directriz `vsftpd_log_file` (por defecto `/var/log/vsftpd.log`).

  El valor predeterminado es `NO`.

- `log_ftp_protocol` — Cuando está activado en conjunto con `xferlog_enable` y con `xferlog_std_format` configurada a `NO`, se registran todos los comandos y respuestas. Esta directriz es muy útil para propósitos de depuración.

El valor predeterminado es NO.

- syslog_enable — Cuando se activa en conjunto con xferlog_enable, todos los registros que normalmente se escriben al archivo estándar vsftpd especificado en la directriz vsftpd_log_file, se envían al registro del sistema bajo la facilidad FTPD.

  El valor predeterminado es NO.

- vsftpd_log_file — Especifica el archivo de registro de vsftpd. Para que se utilice este archivo, xferlog_enable debe estar activado y xferlog_std_format debe ser bien sea NO o, si está en YES, entonces dual_log_enable debe estar activado. Es importante resaltar que si syslog_enable está en YES, se utiliza el registro del sistema en lugar del archivo especificado en esta directriz.

  El valor por defecto es /var/log/vsftpd.log.

- xferlog_enable — Cuando se activa, vsftpd registra las conexiones (solamente formato vsftpd) y la información de transferencia, al archivo de registro especificado en la directriz vsftpd_log_file (por defecto es /var/log/vsftpd.log). Si xferlog_std_format está configurada a YES, se registra la información de transferencia de archivo pero no las conexiones y en su lugar se utiliza el archivo de registro especificado en xferlog_file (por defecto /var/log/xferlog). Es importante observar que se utilizan ambos archivos y formatos de registro si dual_log_enable tiene el valor de YES.

  El valor predeterminado es NO, sin embargo, bajo Red Hat Enterprise Linux, el valor está configurado a YES.

- xferlog_file — Especifica el archivo de registro compatible con wu-ftpd. Para que se utilice este archivo, xferlog_enable debe estar activado y xferlog_std_format debe tener el valor de YES. También se utiliza si dual_log_enable tiene el valor de YES.

  El valor por defecto es /var/log/xferlog.

- xferlog_std_format — Cuando se activa en combinación con xferlog_enable, sólo se escribe un archivo de registro compatible con wu-ftpd al archivo especificado en la directriz xferlog_file (por defecto /var/log/xferlog). Es importante resaltar que este archivo solamente registra transferencias de archivos y no las conexiones al servidor.

  El valor predeterminado es NO, sin embargo, bajo Red Hat Enterprise Linux, el valor está configurado a YES.

Importante

Para mantener la compatibilidad con los archivos de registro escritos por el servidor FTP más antiguo wu-ftpd, se configura la directriz xferlog_std_format a YES bajo Red Hat Enterprise Linux. Sin embargo, esta configuración implica que las conexiones al servidor no son registradas.

Para registrar ambas conexiones en formato vsftpd y mantener un archivo de registro de transferencia compatible con wu-ftpd, configure dual_log_enable a YES.

Si no es de importancia mantener un archivo de registro de transferencias compatible con `wu-ftpd`, entonces configure `xferlog_std_format` a `NO`, comente la línea con un carácter de almohadilla (`#`) o borre completamente la línea.

5.8. Opciones de red

Lo siguiente lista las directrices que afectan cómo `vsftpd` interactua con la red.

- `accept_timeout` — Especifica la cantidad de tiempo para un cliente usando el modo pasivo para establecer una conexión.

  El valor por defecto `60`.

- `anon_max_rate` — Especifica la cantidad máxima de datos transmitidos por usuarios anónimos en bytes por segundo.

  El valor por defecto es `0`, lo que no limita el ratio de transferencia.

- `connect_from_port_20` — Cuando está activada, `vsftpd` se ejecuta con privilegios suficientes para abrir el puerto 20 en el servidor durante las transferencias de datos en modo activo. Al desactivar esta opción, se permite que `vsftpd` se ejecute con menos privilegios, pero puede ser incompatible con algunos clientes FTP.

  El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux, el valor está configurado a `YES`.

- `connect_timeout` — Especifica la cantidad máxima de tiempo que un cliente usando el modo activo tiene para responder a una conexión de datos, en segundos.

  El valor por defecto `60`.

- `data_connection_timeout` — Especifica la cantidad máxima de tiempo que las conexiones se pueden aplazar en segundos. Una vez lanzado, se cierra la conexión con el cliente remoto.

  El valor predeterminado es `300`.

- `ftp_data_port` — Especifica el puerto utilizado por las conexiones de datos activas cuando `connect_from_port_20` está configurado a `YES`.

  El valor predeterminado es `20`.

- `idle_session_timeout` — Especifica la cantidad máxima de tiempo entre comandos desde un cliente remoto. Una vez disparado, se cierra la conexión al cliente remoto.

  El valor predeterminado es `300`.

- `listen_address` — Especifica la dirección IP en la cual `vsftpd` escucha por las conexiones de red.

  Esta directriz no tiene un valor predeterminado.

Sugerencia

Si se están ejecutando varias copias de `vsftpd` sirviendo diferentes direcciones IP, el archivo de configuración para cada copia del demonio `vsftpd` debe tener un valor diferente para esta directriz. Consulte la Sección 4.1, “Iniciar múltiples copias de vsftpd” para más información sobre servidores FTP multihome.

- `listen_address6` — Especifica la dirección IPv6 en la cual `vsftpd` escucha por conexiones de red cuando `listen_ipv6` está configurada a `YES`.

  Esta directriz no tiene un valor predeterminado.

Sugerencia

Si se están ejecutando varias copias de `vsftpd` sirviendo diferentes direcciones IP, el archivo de configuración para cada copia del demonio `vsftpd` debe tener un valor diferente para esta directriz. Consulte la Sección 4.1, “Iniciar múltiples copias de vsftpd” para más información sobre servidores FTP multihome.

- `listen_port` — Especifica el puerto en el cual `vsftpd` escucha por conexiones de red.

  El valor predeterminado es `21`.

- `local_max_rate` — Especifica la taza máxima de transferencia de datos para los usuarios locales conectados en el servidor en bytes de segundo.

  El valor por defecto es `0`, lo que no limita el ratio de transferencia.

- `max_clients` — Especifica el número máximo de clientes simultáneos que tienen permitido conectarse al servidor cuando se ejecuta en modo independiente. Cualquier conexión adicional resultará en un mensaje de error.

  El valor predeterminado es `0`, lo que no limita las conexiones.

- `max_per_ip` — Especifica el máximo número de clientes que tienen permitido conectarse desde la misma dirección IP fuente.

  El valor predeterminado es `0`, lo que no limita las conexiones.

- `pasv_address` — Especifica la dirección IP para la IP del lado público del servidor para los servidores detrás de cortafuegos Network Address Translation (NAT). Esto permite que `vsftpd` entregue la dirección correcta de retorno para las conexiones pasivas.

  Esta directriz no tiene un valor predeterminado.

- `pasv_enable` — Cuando está activa, se permiten conexiones en modo pasivo.

  El valor por defecto es `YES`.

- `pasv_max_port` — Especifica el puerto más alto posible enviado a los clientes FTP para las conexiones en modo pasivo. Esta configuración es utilizada para limitar el intervalo de puertos para que las reglas del cortafuegos sean más fáciles de crear.

  El valor predeterminado es `0`, lo que no limita el rango de puertos pasivos más alto. El valor no puede exceder de `65535`.

- `pasv_min_port` — Especifica el puerto más bajo posible para los clientes FTP para las conexiones en modo pasivo. Esta configuración es utilizada para limitar el intervalo de puertos para que las reglas del cortafuego sean más fáciles de implementar.

  El valor predeterminado es `0`, lo que no limita el intervalo de puertos pasivos más bajo. El valor no debe ser menor que `1024`.

- `pasv_promiscuous` — Cuando está activada, las conexiones de datos no son verificadas para asegurarse de que se originan desde la misma dirección IP. Este valor solamente es útil para ciertos tipos de tunneling.

  Atención

  No active esta opción a menos que sea absolutamente necesario ya que desactiva una funcionalidad de seguridad muy importante la cual verifica que las conexiones en modo pasivo partan desde la misma dirección IP que la conexión de control que inicia la transferencia de datos.

  El valor predeterminado es `NO`.

- `port_enable` — Cuando está activada, se permiten las conexiones en modo activo.

  El valor por defecto es `YES`.

6. Recursos adicionales

Para más información sobre `vsftpd`, consulte los recursos siguientes.

6.1. Documentación instalada

- El directorio `/usr/share/doc/vsftpd-<version-number>/` — Reemplace `<version-number>` con la versión instalada del paquete `vsftpd`. Este directorio contiene un archivo `LEAME` con información básica sobre el software. El archivo `TUNING` contiene sugerencias básicas para refinar el rendimiento y el directorio `SECURITY/` contiene información sobre el modelo de seguridad empleado por `vsftpd`.

- Páginas man relacionadas con `vsftpd` — Hay varias páginas man para este demonio y los archivos de configuración. Lo siguiente lista algunas de las más importantes.

  Aplicaciones de servidor

- `man vsftpd` — Describe las opciones de línea de comandos disponibles para `vsftpd`.

Archivos de configuración

- `man vsftpd.conf` — Contiene una lista detallada de las opciones disponibles dentro del archivo de configuración para `vsftpd`.
- `man 5 hosts_access` — Describe el formato y las opciones disponibles dentro de los archivos de configuración de TCP wrappers: `hosts.allow` and `hosts.deny`.

6.2. Sitios web de utilidad

- http://vsftpd.beasts.org/ — La página del proyecto `vsftpd` es un excelente lugar para ubicar la documentación más reciente y para contactar al autor del software.
- http://slacksite.com/other/ftp.html — Este sitio proporciona una explicación completa de las diferencias entre el modo activo y pasivo de FTP.
- http://www.ietf.org/rfc/rfc0959.txt — Una lista completa de las *Request for Comments* (*RFCs*) del protocolo FTP desde IETF.

Capítulo 9. Correo electrónico

El nacimiento del correo electrónico (*email*) ocurrió a principios de los años 60. El buzón era un archivo en el directorio principal de un usuario al cual sólo el mismo podía acceder. Las aplicaciones de correo primitivas anexaban nuevos mensajes de texto a la parte inferior de un archivo, y el usuario tenía que buscar a lo largo del archivo en constante crecimiento para encontrar un mensaje particular. Este sistema sólo era capaz de enviar mensajes a usuarios en el mismo sistema.

La primera transferencia verdadera de correo electrónico en la red se llevó a cabo en 1971 cuando un ingeniero de computación llamado Ray Tomlinson envió un mensaje de prueba entre dos máquinas a través de ARPANET — el precursor de Internet. La comunicación a través de correo electrónico rápidamente se volvió muy popular, pasando a formar el 75 por ciento del tráfico de ARPANET en menos de dos años.

Hoy día los sistemas de correo electrónico basados en protocolos de red se han convertido en uno de los servicios más usados de la Internet. Red Hat Enterprise Linux ofrece muchas aplicaciones avanzadas para servir y acceder a correo electrónico.

En este capítulo se analizan los protocolos de correo electrónico modernos conocidos actualmente, así como algunos programas diseñados para recibir y enviar correo electrónico.

1. Protocolos de correo electrónico

Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.

Los protocolos que se indican a continuación son los que más se utilizan para transferir correo electrónico.

1.1. Protocolos de transporte de correo

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el *Protocolo simple de transferencia de correo* (*Simple Mail Transfer Protocol* o *SMTP*).

1.1.1. SMTP

El objetivo principal del protocolo simple de transferencia de correo, SMTP, es transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envia el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.

Bajo Red Hat Enterprise Linux, un usuario puede configurar un servidor SMTP en la máquina local para manejar la entrega de correo. Sin embargo, también es posible configurar servidores remotos SMTP para el correo saliente.

Un punto importante sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en Internet puede enviar correo a cualquier otra persona o inclusive a grandes grupos de personas. Esta característica de SMTP es lo que hace posible el correo basura o *spam*. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen tales restricciones son llamados servidores *open relay*.

Por defecto se utiliza Sendmail (`/usr/sbin/sendmail`) como su programa SMTP bajo Red Hat Enterprise Linux. Sin embargo, también está disponible una aplicación más simple de servidor de correo llamada Postfix (`/usr/sbin/postfix`).

1.2. Protocolos de acceso a correo

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el *Post Office Protocol* (*POP*) y el *Internet Message Access Protocol* (*IMAP*).

1.2.1. POP

El servidor por defecto POP bajo Red Hat Enterprise Linux es `/usr/lib/cyrus-imapd/pop3d` y es proporcionado por el paquete `cyrus-imapd`. Cuando utilice un servidor POP, los mensajes de correo son descargados a través de las aplicaciones de correo del cliente. Por defecto, la mayoría de los clientes de correo POP son configurados automáticamente para borrar el mensaje en el servidor de correo después que éste ha sido transferido exitósamente, sin embargo esta configuración se puede cambiar.

POP es completamente compatible con estándares importantes de mensajería de Internet, tales como *Multipurpose Internet Mail Extensions* (*MIME*), el cual permite los anexos de correo.

POP funciona mejor para usuarios que tienen un sistema en el cual leer correo. También funciona bien para usuarios que no tienen una conexión permanente a la Internet o a la red que contiene el servidor de correo. Desafortunadamente para aquellos con conexiones lentas, POP requiere que luego de la autenticación los programas cliente descarguen el contenido completo de cada mensaje. Esto puede tomar un buen tiempo si algún mensaje tiene anexos grandes.

La versión más reciente del protocolo estándar POP es POP3.

Sin embargo, también existen una variedad de variantes del protocolo POP que no son tan populares:

- *APOP* — POP3 con autenticación MDS. En este protocolo, el cliente de correo envía un hash codificado de la contraseña al servidor en lugar de enviar una contraseña encriptada.
- *RPOP* — POP3 con autenticación RPOP, que utiliza un identificador de usuario similar a una contraseña para autenticar las peticiones POP. No obstante, este ID no esta encriptado por tanto RPOP no es más seguro que el estándar POP.

Para añadir seguridad, es posible utilizar la encriptación *Secure Socket Layer* (*SSL*) para la autenticación del cliente y las sesiones de transferencias de datos. Esto se puede activar usando el servicio `ipop3s` o mediante el uso del programa `/usr/sbin/stunnel`. Refiérase a la Sección 6.1, “Comunicación segura” para obtener mayor información.

1.2.2. IMAP

El servidor por defecto IMAP bajo Red Hat Enterprise Linux es `/usr/lib/cyrus-imapd/imapd` y es proporcionado por el paquete `cyrus-imapd`. Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios los pueden leer y borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.

Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.

IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

Para seguridad adicional, es posible utilizar la encriptación *SSL* para la autenticación de clientes y para las sesiones de transferencia de datos. Esto se puede activar usando el servicio `imaps` o mediante el uso del programa `/usr/sbin/stunnel`. Refiérase a la Sección 6.1, “Comunicación segura” para obtener mayor información.

También están disponibles otros clientes y servidores de correo IMAP gratuítos así como también comerciales, muchos de los cuales extienden el protocolo IMAP y proporcionan funcionalidades adicionales. Una lista completa sobre esto se puede encontrar en http://www.imap.org/products/longlist.htm.

1.2.3. Dovecot

Los demonios `imap-login` y `pop3-login`, los cuales implementan los protocolos IMAP y POP3 se encuentran incluidos en el paquete `dovecot`. El uso de IMAP y POP se configura a través de `dovecot`; por defecto, `dovecot` ejecuta sólamente IMAP. Para configurar `dovecot` para que utilice POP:

1. Modifique `/etc/dovecot.conf` para que tenga la siguiente línea:

   ```
   protocols = imap imaps pop3 pop3s
   ```

2. Para hacer ese cambio operacional para la sesión actual ejecute el comando:

   ```
   /sbin/service dovecot restart
   ```

3. Haga que ese cambio sea operacional después del siguiente reinicio ejecutando el coman-

do:

```
chkconfig dovecot on
```

Observe que `dovecot` sólamente reporta que inició el servidor IMAP pero también inicia el servidor POP3.

A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red sin encriptar.

Para configurar SSL en dovecot:

- Modifique el archivo de configuración `dovecot/etc/pki/dovecot/dovecot-openssl.conf` como desee. Sin embargo, en una instalación típica este archivo no necesita modificación.
- Renombra, mueve o borra los archivos `/etc/pki/dovecot/certs/dovecot.pem` y `/etc/pki/dovecot/private/dovecot.pem`.
- Ejecute el script `/usr/share/doc/dovecot-1.0/examples/mkcert.sh`, el cual crea certificados auto-firmados dovecot. Estos certificados se copian en los directorios `/etc/pki/dovecot/certs` y `/etc/pki/dovecot/private`. Para implementar los cambios reinicie `dovecot` (`/sbin/service dovecot restart`).

Encontrará más información sobre `dovecot` en http://www.dovecot.org.

2. Clasificaciones de los programas de correo

En general, todas las aplicaciones de email caen en al menos una de tres clasificaciones. Cada clasificación juega un papel específico en el proceso de mover y administrar los mensajes de correo. Mientras que la mayoría de los usuarios sólo están al tanto del programa de correo específico que usan para recibir o enviar mensajes, cada uno es importante para asegurar que el mensaje llegue a su destino correcto.

2.1. Agente de Transporte de Correo

Un *Agente de Transporte de Correo* (*MTA*) transfiere mensajes de correo electrónico entre hosts usando SMTP. Un mensaje puede involucrar varios MTAs a medida que este se mueve hasta llegar a su destino.

Aunque la entrega de mensajes entre máquinas puede parecer bien simple, el proceso completo de decidir si un MTA particular puede o debería aceptar un mensaje para ser repartido, es más bien complicado. Además, debido a los problemas de spam, el uso de un MTA particular está usualmente restringido por la configuración del MTA o por la configuración de acceso a la red en la que reside el MTA.

Muchos programas clientes de correo modernos pueden actuar como un MTA cuando estén enviando correo. Sin embargo, no se debería confundir esta acción con el papel de un verdadero MTA. La única razón por la que los programas de correo cliente son capaces de enviar men-

sajes como un MTA es porque el host ejecutando la aplicación no tiene su propio MTA. Esto es particularmente cierto para programas de correo cliente o para sistemas que no están basados en el sistema operativo UNIX. Sin embargo, estos programas clientes sólo envían mensajes salientes a un MTA para el cual estan autorizados a utilizar y no entregan el mensaje directamente al servidor de correos del recipiente.

Puesto que Red Hat Enterprise Linux instala dos MTAs, Sendmail y Postfix, los programas cliente de correo electrónico no son comúnmente requeridos que actúen como un MTA. Red Hat Enterprise Linux también incluye un MTA de propósitos especiales llamado Fetchmail.

Para obtener mayor información sobre Sendmail, Postfix y Fetchmail consulte la Sección 3, “Agentes de transporte de correo”.

2.2. Agente de entrega de correos

Un MTA invoca a un *Agente de entrega de correos* (*MDA*) para archivar el correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un *Agente de entregas local* (*LDA*), tal como `mail` o Procmail.

Cualquier programa que maneje la entrega de mensajes hasta el punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA. Por esta razón, algunos MTAs (tales como Sendmail y Postfix) pueden tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario. En general, los MDAs no transportan mensajes entre sistemas tampoco proporcionan una interfaz de usuario; los MDAs distribuyen y clasifican mensajes en la máquina local para que lo accese una aplicación cliente de correo.

2.3. Agente de usuario de correo

Un *agente de usuario de correo* (*MUA*) es sinónimo con una aplicación cliente de correo. Un MUA es un programa que, al menos, le permite a los usuarios leer y redactar mensajes de correo. Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA.

Los MUAs pueden ser de interfaz gráfica tal como Evolution o tener una interfaz basada en texto muy sencilla tal como `mutt`.

3. Agentes de transporte de correo

Red Hat Enterprise Linux incluye dos tipos primarios de MTAs, Sendmail y Postfix. Sendmail es configurado como el MTA predetermiando aún cuando es fácil cambiar el MTA predeterminado a Postfix.

3.1. Sendmail

El propósito principal de Sendmail, como cualquier otro MTA, es el de transferir correo de forma segura entre hosts, usualmente usando el protocolo SMTP. Sin embargo, Sendmail es altamente configurable, permitiendo el control sobre casi cada aspecto del manejo de correos, incluyendo el protocolo utilizado. Muchos administradores de sistemas seleccionan Sendmail como su

MTA debido a su poder y escalabilidad.

3.1.1. Propósitos y limitaciones

Es importante estar conscientes de qué es Sendmail y de lo que puede hacer al contrario de lo que no es. En estos tiempos de aplicaciones monolíticas que cubren varios papeles, Sendmail puede parecer la única aplicación necesitada para ejecutar un servidor de correo en una organización. Esto técnicamente es verdad, puesto que Sendmail puede colocar correo en los directorios de cada usuario y entregar el correo saliente para los usuarios. Sin embargo, la mayoría de los usuarios requieren normalmente mucho más que la entrega de correos. Ellos usualmente quieren interactuar con su correo usando un MUA, que utiliza POP o IMAP, para descargar sus mensajes a sus máquinas locales. O prefieren una interfaz tipo web para ganar acceso a sus buzones. Estas otras aplicaciones pueden funcionar en conjunto con Sendmail, pero ellas existen en realidad por otras razones y pueden operar separadamente una de la otra.

Está más allá del ámbito de esta sección explicar todo lo que Sendmail debería o podría hacer. Literalmente hay cientos de opciones diferentes y reglas para configurar, existen libros dedicados completamente a explicar todo lo que se puede hacer y como solucionar problemas cuando las cosas salen mal. Consulte la Sección 7, “Recursos adicionales” para obtener una lista de los recursos de Sendmail.

Esta sección revisa los archivos instalados con Sendmail por defecto y revisa los cambios básicos a la configuración, incluyendo cómo detener correo no deseado (spam) y también cómo extender Sendmail con el *Lightweight Directory Access Protocol (LDAP)*.

3.1.2. La instalación de Sendmail por defecto

El ejecutable de Sendmail es `/usr/sbin/sendmail`.

El largo y detallado archivo de configuración de Sendmail es `/etc/mail/sendmail.cf`. Evite modificar el archivo `sendmail.cf` directamente. Para realizar cambios de configuración en Sendmail modifique el archivo `/etc/mail/sendmail.mc`, haga una copia de seguridad del `/etc/mail/sendmail.cf` original y utilice las siguientes alternativas para generar un nuevo archivo de configuración:

- Utilice el makefile en `/etc/mail` (`make all -C /etc/mail`) para crear un nuevo archivo de configuración `/etc/mail/sendmail.cf`. Todos los otros archivos generados en `/etc/mail` (archivos db) serán regenerados si es necesario. Los viejos comandos makemap todavía se pueden utilizar. `service sendmail start | restart | reload` utilizará automáticamente el comando make si el paquete `make` es instalado.

- Alternativamente puede utilizar el procesador de macros `m4` incluído para crear un nuevo `/etc/mail/sendmail.cf`.

Para obtener más información sobre como configurar Sendmail visite Sección 3.1.3, “Cambios comunes de configuración de Sendmail”.

Varios archivos de configuración de Sendmail son instalados en el directorio `/etc/mail/` incluyendo:

- `access` — Especifica los sistemas que pueden utilizar Sendmail para enviar correo saliente.

- `domaintable` — Le permite crear asignaciones de nombres de dominio.
- `local-host-names` — Especifica aliases para el host.
- `mailertable` — Especifica instrucciones para ignorar la ruta de determinados dominios.
- `virtusertable` — Le permite especificar una forma de alias para dominios específicos, permitiendo a múltiples dominios virtuales ser hospedados en una misma máquina.

Muchos de los archivos de configuración en `/etc/mail/`, tales como `access`, `domaintable`, `mailertable` y `virtusertable`, deben en realidad almacenar su información en archivos de bases de datos antes de que Sendmail puede usar algún cambio de configuración. Para incluir cambios hechos a estas configuraciones en sus archivos de bases de datos, ejecute el comando

```
makemap hash /etc/mail/<name> < /etc/mail/<name>
```

donde *<name>* es reemplazado con el nombre del archivo de configuración a convertir.

Por ejemplo, para tener todos los correos direccionados al dominio `example.com` entregados a `<bob@other-example.com>` , añada la línea siguiente al archivo `virtusertable`:

```
@example.com bob@other-example.com
```

Para finalizar el cambio, se debe actualizar el archivo `virtusertable.db` usando el comando siguiente como root:

```
makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable
```

Esto crea un archivo `virtusertable.db` actualizado conteniendo la nueva configuración.

3.1.3. Cambios comunes de configuración de Sendmail

Cuando se esté modificando el archivo de configuración de Sendmail, es mejor generar un archivo completamete nuevo `/etc/mail/sendmail.cf` en vez de modificar el existente.

Atención

Es una muy buena idea hacer una copia de respaldo del archivo `sendmail.cf` antes de cambiarlo.

Para añadir funcionalidad a Sendmail, modifique el archivo `/etc/mail/sendmail.mc` como usuario root. Cuando termine, utilice el procesador de macros `m4` para generar un nuevo `sendmail.cf` ejecutando el comando siguiente:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Por defecto, el procesador de macros `m4` es instalado con Sendmail pero es parte del paquete `m4`.

Después de crear un archivo `/etc/mail/sendmail.cf` nuevo, reinicie Sedmail para que los cam-

bios tomen efecto. La forma más fácil de hacer esto es ejecutando el comando siguiente:

```
/sbin/service sendmail restart
```

Importante

El archivo por defecto `sendmail.cf` no permite que Sendmail acepte conexiones de red desde ningún host mas que la máquina local. Para configurar Sendmail como un servidor para otros clientes, modifique `/etc/mail/sendmail.mc` y cambie la dirección especificada en la opción `Addr=` de la directriz `DAEMON_OPTIONS` a la dirección IP de un dispositivo de red activo o coloque en comentarios toda esta opción colocando `dnl` al comienzo de la línea. Luego, vuelva a generar `/etc/mail/sendmail.cf` ejecutando el comando siguiente:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

La configuración predetermianda que viene con Red Hat Enterprise Linux funciona para la mayoría de los sitios puramente SMTP. Sin embargo, no funciona con sitios UUCP (Copia UNIX a UNIX). Si está utilizando transferencias de correo UUCP, se debe reconfigurar el archivo `/etc/mail/sendmail.mc` y se debe generar un nuevo `/etc/mail/sendmail.cf`.

Consulte el archivo `/usr/share/sendmail-cf/README` antes de modificar cualquier archivo en los directorios bajo el directorio `/usr/share/sendmail-cf`, pues ellos pueden afectar la futura configuración de los archivos `/etc/mail/sendmail.cf`.

3.1.4. Creación de máscaras

Una configuración común de Sendmail es tener una sola máquina actuando como el gateway de correo para todas las máquinas en la red. Por ejemplo, una compañía puede querer tener una máquina llamada `mail.example.com` que maneja todo su correo y asigna una dirección de retorno consistente para todo el correo saliente.

En esta situación, el servidor Sendmail debe enmascarar los nombres de las máquinas en la red de la compañía para que la dirección de retorno sea `user@example.com` en vez de `user@host.example.com`.

Para hacer esto, añada las líneas siguientes `/etc/mail/sendmail.mc`:

```
FEATURE(always_add_domain)dnl FEATURE(`masquerade_entire_domain') dnl FEATURE(`masquerade_envelope') dnl FE
```

Después de generar un nuevo `sendmail.cf` usando `m4`, esta configuración hará que todo el correo dentro de la red aparezca como que si se hubiese enviado desde `bigcorp.com`.

3.1.5. Detener el correo basura

El correo basura se puede definir como correo no deseado e innecesario recibido por un usuario que nunca solicitó tal comunicación. Es un abuso costoso y molesto de las comunicaciones de Internet estándar.

Sendmail hace relativamente fácil bloquear nuevas técnicas de difusión de correo basura. Has-

ta bloquea por defecto muchos de los métodos comunes de difusión de correo basura. Las principales características anti-spam disponibles en sendmail son *verificación de cabeceras, retransmisión de rechazo (por defecto desde la versión 8.9), acceso a bases de datos y verificación de la información del remitente.*

Por ejemplo, el reenvío de mensajes SMTP, también conocido como relaying, está por defecto desactivado en Sendmail desde la versión 8.9. Antes de que se produjese este cambio, Sendmail indicaba al host (`x.edu`) que aceptara mensajes desde un ente (`y.com`) y que los enviara a un ente diferente (`z.net`). Ahora, sin embargo, se debe configurar Sendmail para permitir que cualquier dominio transmita correo a través del servidor. Para configurar dominios de transmisión, modifique el archivo `/etc/mail/relay-domains` y reinicie Sendmail.

Sin embargo, en muchas ocasiones, los usuarios reciben bombardeos de correo basura de otros servidores a través de Internet. En estos casos, puede utilizar las funciones de control de acceso de Sendmail que están disponibles en el archivo `/etc/mail/access` para prevenir conexiones desde host indeseados. El ejemplo siguiente ilustra como este archivo puede ser usado para bloquear y también para permitir el acceso al servidor Sendmail:

```
badspammer.com ERROR:550 "Go away and do not spam us anymore" tux.badspammer.com OK 10.0 RELAY
```

Este ejemplo indica que cualquier correo que se envia desde `badspammer.com` se bloqueará con un código de error 550 RFC-821, con un mensaje para el emisor. Los correos enviados desde el sub-dominio `tux.badspammer.com`, seran aceptados. La última línea muestra que cualquier correo enviado desde la red 10.0.*.* se puede transmitir a través del servidor de correo.

Debido a que `/etc/mail/access.db` es una base de datos, use `makemap` para activar los cambios. Haga esto usando el comando siguiente como root:

```
makemap hash /etc/mail/access < /etc/mail/access
```

El análisis de la cabecera del mensaje le permite rechazar correo con base en el contenido de este. Los servidores SMTP almacenan información sobre el recorrido de un correo electrónico en la cabecera del mensaje. Mientras que el mensaje va de una MTA a otra cada una de estas pone una cabecera que dice "Recibido" encima de las otras cabeceras que dicen lo mismo. Sin embargo, es importante observar que los que envían estos correos no deseados pueden alterar esta información.

Este ejemplo sólo muestra una mínima parte de lo que Sendmail puede hacer en cuanto a permitir o bloquear el acceso. Para obtener más información y ejemplos consulte `/usr/share/sendmail-cf/README`.

Puesto que Sendmail llama a Procmail MDA cuando está entregando correo también es posible utilizar un programa de filtrado de correo basura, tal como SpamAssassin para identificar y archivar correo basura por los usuarios. Consulte la Sección 5.2.6, “Filtros de correo basura” obtener para más detalles sobre SpamAssassin.

3.1.6. Uso de Sendmail con LDAP

Usando el *Lightweight Directory Access Protocol (LDAP)* es una forma rápida y poderosa de encontrar información específica sobre un usuario particular desde un grupo mucho más grande. Por ejemplo, un servidor LDAP puede ser usado para buscar una dirección de correo particular desde un directorio corporativo usando el apellido del usuario. En este tipo de implemen-

tación, LDAP esta bastante separado de Sendmail, con LDAP la información de usuario de forma jerárquica y Sendmail sólo recibiendo el resultado de las consultas de LDAP en mensajes de correo pre-direccionados.

Sin embargo, Sendmail admite mucha más integración con LDAP y utiliza este protocolo para sustituir archivos mantenidos independientemente, como `aliases` y `virtusertables`, que se ubican en servidores de correo diferentes que funcionan juntos para soportar una organización de nivel medio a corporativo. A modo de resumen, puede usar LDAP para separar el nivel de enrutamiento desde Sendmail y sus archivos de configuración separados a un cluster LDAP poderoso que pueden utilizar distintas aplicaciones.

La versión actual de Sendmail es compatible con LDAP. Para ampliar el servidor de Sendmail y usar LDAP, primero debe obtener un servidor LDAP, como **OpenLDAP**, ejecutarlo y configurarlo correctamente. A continuación, modifique `/etc/mail/sendmail.mc` para incluir lo siguiente:

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

Nota

Esta es sólo una configuración muy básica de Sendmail con LDAP. Su configuración puede ser muy diferente de la indicada según la implementación específica de LDAP, especialmente si configura varias máquinas de Sendmail para que utilicen un servidor LDAP común.

Consulte `/usr/share/sendmail-cf/README` para obtener instrucciones y ejemplos detallados de configuración de enrutamiento de LDAP.

Luego vuelva a crear el archivo `/etc/mail/sendmail.cf` ejecutando `m4` y reiniciando Sendmail. Consulte la Sección 3.1.3, “Cambios comunes de configuración de Sendmail” para obtener detalles sobre cómo hacer esto.

Para obtener mayor información sobe LDAP vea el Capítulo 10, *Protocolo Ligero de Acceso a Directorios (LDAP)*.

3.2. Postfix

Postfix, originalmente desarrollado en IBM por el experto de seguridad y programador Wietse Venema, es un MTA compatible con Sendmail diseñado para ser seguro, rápido y fácil de configurar.

Postfix utiliza un diseño modular para mejorar la seguridad, en el que los procesos pequeños con privilegios limitados son lanzados por un demonio *master*. Los procesos más pequeños, con menos privilegios, realizan tareas muy específicas relacionada con las diferentes etapas de la entrega de correos y se ejecutan en un ambiente de cambio de root para limitar los efectos de ataques.

Configurar Postfix para que acepte conexiones de red desde otros hosts además de la computadora local sólo toma unos pequeños cambios en su archivo de configuración. Para aquellos con necesidades más complejas, Postfix ofrece una variedad de opciones de configuración, así

como también complementos de terceros que lo hacen un MTA rico en funcionalidades.

Los archivos de configuración de Postfix son legibles y aceptan hasta 250 directrices. A diferencia de Sendmail, no se requiere procesar ninguna macro para que los cambios tomen efecto y la mayoría de las opciones usadas frecuentemente se describen en archivos muy bien comentados.

Importante

Antes de utilizar Postfix, se debe cambiar la MTA predeterminada de Sendmail a Postfix.

3.2.1. La instalación predeterminada de Postfix

El ejecutable de Postfix es `/usr/sbin/postfix`. Este demonio lanza todos los procesos relacionados necesarios para manejar la entrega de correos.

Postfix almacena sus archivos de configuración en el directorio `/etc/postfix/`. A continuación se muestra una lista de los archivos usados más a menudo:

- `access` — Utilizado para el control de acceso, este archivo especifica los sistemas que pueden conectarse a Postfix.
- `aliases` — Una lista configurable que el protocolo de correo requiere.
- `main.cf` — El archivo global de configuración de Postfix. La mayoría de las opciones de configuración se especifican en este archivo.
- `master.cf` — Especifica la forma en que Postfix interactua con diferentes procesos para lograr la entrega de correo.
- `transport` — Hace las correspondencias entre direcciones de correo electrónico y los hosts de transmisiones.

Importante

El archivo predeterminado `/etc/postfix/main.cf` no permite que Postfix acepte conexiones de red desde ningún otro host que no sea la máquina local. Consulte la Sección 3.2.2, “Configuración básica de Postfix” para ver las instrucciones sobre cómo configurar Postfix como un servidor para otros clientes.

A veces, puede ser necesario reiniciar el servicio `postfix` cuando se cambien algunas opciones dentro de archivos en el directorio `/etc/postfix/` para que se apliquen los cambios. La forma más fácil de lograr esto es a través del comando:

```
/sbin/service postfix restart
```

3.2.2. Configuración básica de Postfix

Por defecto, no acepta conexiones de red desde ningún otro host excepto la máquina local. Ejecute los pasos siguientes como superusuario para activar la entrega de correo desde otros hosts en la red:

- Modifique el archivo `/etc/postfix/main.cf` con un editor de texto, tal como `vi`.
- Quite el comentario de la línea `mydomain` removiendo la almohadilla (`#`) y reemplace *`domain.tld`* con el dominio que está sirviendo el servidor de correo, tal como `example.com`.
- Quite el comentario de la línea `myorigin = $mydomain`.
- Elimine el comentario de la línea `myhostname` y reemplace *`host.domain.tld`* con el nombre de host para la máquina.
- Elimine el comentario de la línea `mydestination = $myhostname, localhost.$mydomain`.
- Elimine el comentario de la línea `mynetworks` y sustituya *`168.100.189.0/28`* con un valor de red válido para que los hosts se puedan conectar al servidor.
- Remueva el comentario de la línea `inet_interfaces = all`.
- Reinicie el servicio `postfix`.

Luego de completar estos pasos, el host acepta correos externos.

Postfix tiene una gran variedad de opciones de configuración. Una de las mejores formas de aprender cómo configurar Postfix es leer los comentarios dentro de `/etc/postfix/main.cf`. En http://www.postfix.org/ puede encontrar recursos adicionales incluyendo información sobre la integración de LDAP y SpamAssassin.

3.3. Fetchmail

Fetchmail es un MTA que recupera el correo desde servidores remotos y los entrega al MTA local. Muchos usuarios aprecian la capacidad de separar el proceso de descarga de mensajes ubicados en un servidor remoto del proceso de lectura y organización de correo en un MUA. Se ha diseñado teniendo presente las necesidades de los usuarios de acceso telefónico a redes. Fetchmail se conecta y descarga rápidamente todos los mensajes al archivo spool de correo mediante el uso de diversos protocolos, entre los que se incluyen POP3 e IMAP. Incluso permite reenviar los mensajes de correo a un servidor SMTP si es necesario.

Fetchmail es configurado para cada usuario a través del uso de un archivo `.fetchmailrc` en el directorio principal del usuario.

Mediante el uso de preferencias en el archivo `.fetchmailrc`, Fetchmail comprobará si hay correo en un servidor remoto e intentará descargarlo. Luego lo entrega al puerto 25 de la máquina local utilizando el agente MTA local para dirigir el correo al archivo de spool del usuario correcto. Si Procmail está disponible, se ejecuta para filtrar el correo y colocarlo en un buzón para que lo pueda leer un MUA.

3.3.1. Opciones de configuración de Fetchmail

Aunque se pueden pasar todas las opciones necesarias en la línea de comandos para comprobar si hay correo en un servidor remoto al ejecutar Fetchmail, el uso de `.fetchmailrc` proporciona un método más sencillo. Coloque todas las opciones de configuración deseadas en el archivo `.fetchmailrc` y estas se utilizarán cada vez que se ejecute el comando `fetchmail`. Es posible ignorar estas opciones en tiempo de ejecución especificando alguna opción en la línea de comandos.

Un archivo `.fetchmailrc` de usuario contiene tres clases de opciones de configuración:

- *opciones globales* — Indican a Fetchmail las instrucciones que controlan el funcionamiento del programa o proporcionan las configuraciones para cada conexión que verifica por correo.
- *opciones de servidor* — Especifican información necesaria sobre el servidor, como nombre de host, así como las preferencias para un servidor de correo particular, tal como el puerto a verificar o el número de segundos a esperar antes de un timeout. Estas opciones afectan a cada opción de usuario usado con ese servidor.
- *opciones de usuario* — Contienen información, tal como nombre de usuario y contraseña, que es necesaria para autenticar y comprobar si hay correo utilizando un servidor de correo concreto.

Las opciones globales se encuentran en la parte superior del archivo `.fetchmailrc`, seguidas de una o varias opciones de servidor con las que se designa cada uno de los servidores de correo diferentes que debería comprobar Fetchmail. Por último, se encuentran las opciones de usuario específicas de cada cuenta de usuario que desea comprobar en el servidor de correo. Al igual que las opciones de servidor, se pueden especificar varias opciones de usuario para utilizarlas con un servidor determinado así como también comprobar varias cuentas de correo electrónico en el mismo servidor.

Las opciones de servidor se llaman para ejecución en el archivo `.fetchmailrc` mediante el uso de una opción especial, `poll` o `skip`, que precede cualquier información de servidor. La acción `poll` indica a Fetchmail que use esta opción de servidor cuando se ejecute, lo que en realidad verifica por correo usando las opciones de usuario. Cualquier opción de servidor luego de una acción `skip`, sin embargo, no se verificará a menos que este nombre de host sea especificado cuando se llama Fetchmail. La opción `skip` es muy útil cuando se evalúan configuraciones en `.fetchmailrc` pues sólo chequea servidores saltados cuando se invoquen específicamente, y no afecta ninguna configuracion en funcionamiento actualmente.

Un archivo `.fetchmailrc` de ejemplo se vería así:

```
set postmaster "user1" set bouncemail poll pop.domain.com proto pop3 user 'user1' there with password 'sec
```

En este ejemplo, las opciones globales establecen que se le envíe correo al usuario en última instancia (opción `postmaster`) y que todos los errores de correo se manden al postmaster en lugar de al emisor (opción `bouncemail`). La acción `set` indica a Fetchmail que esta línea contiene una opción global. A continuación, se especifican dos servidores de correo: uno para que compruebe si hay correo con el protocolo POP3 y otro para que pruebe a usar varios protocolos para encontrar uno que funcione. Se comprueba el correo de dos usuarios con la segunda opción de servidor, pero todo el correo que se encuentre se envía al spool de correo del `user1`. Esto permite comprobar varios buzones en diversos servidores como si se tratara de un único buzón

MUA. La información específica de cada usuario comienza con la acción `user`.

Nota

No es necesario que los usuarios coloquen sus contraseñas en el archivo `.fetchmailrc`. El omitir la sección `with password '<password>'` causa que Fetchmail solicite una contraseña cuando es lanzado.

Fetchmail contiene muchas opciones diferentes globales, de servidor y locales. Muchas de estas opciones casi nunca se usan o sólo se aplican en situaciones muy específicas. La página del manual de `fetchmail` explica cada opción en detalle, pero las usadas más a menudo se listan aquí.

3.3.2. Opciones globales

Cada opción global debería ser colocada en una línea individual después de una acción `set`.

- `daemon <seconds>` — Indica a Fetchmail usar el modo de demonio, con el que estará en segundo plano. Reemplace `<seconds>` con el número de segundos que Fetchmail debe esperar antes de consultar el servidor.
- `postmaster` — Indica a Fetchmail un usuario local para enviar el correo en caso de problemas de entrega.
- `syslog` — Indica a Fetchmail el registro de mensajes de error y de estado. Por defecto, es `/var/log/maillog`.

3.3.3. Opciones de servidor

Las opciones de servidor deben ser colocadas en su propia línea en `.fetchmailrc` después de una acción `poll` o `skip`.

- `auth <auth-type>` — Especifica el tipo de autenticación que se utilizará. Por defecto, se utiliza la autenticación por `password` pero algunos protocolos admiten también otros tipos de autenticación, entre los que se incluyen `kerberos_v5`, `kerberos_v4` y `ssh`. Si se usa el tipo de autenticación `any`, Fetchmail primero usará métodos que no necesiten contraseña y luego otros que creen máscara para la contraseña. Finalmente, intentará enviar la contraseña sin encriptar para ser autenticada al servidor.
- `interval <number>` — Registra el servidor especificado cada `<number>` de veces que verifica por correo en todos los servidores configurados. Esta opción es generalmente utilizada por servidores de correo donde el usuario rara vez recibe mensajes.
- `port <port-number>` — Reemplace `<port-number>` con el número de puerto. Este valor sobreescribe el número de puerto por defecto para un protocolo especificado.
- `proto <protocol>` — Sustituya `<protocol>` con el protocolo, tal como `pop3` or `imap`, a utilizar cuando se verifique por mensajes en el servidor.

- `timeout <seconds>` — Sustituya `<seconds>` con el número de segundos de inactividad del servidor después de los cuales Fetchmail abandonará el intento de conexión. Si no se define este valor, se asume un valor de `300` segundos.

3.3.4. Opciones de usuario

Las opciones de usuario se pueden insertar en sus propias líneas debajo de una opción de servidor o en la misma línea que la opción de servidor. En cualquier caso, las opciones definidas van después de la opción `user` (definida más abajo).

- `fetchall` — Ordena a Fetchmail descargar todos los mensajes en cola, incluidos los mensajes que ya se han visto. Por defecto, Fetchmail sólo lo hace con los nuevos mensajes.
- `fetchlimit <number>` — Sustituya `<number>` con el número de mensajes a recuperar antes de detenerse.
- `flush` — Elimina todos los mensajes en cola que ya se han visto antes de descargar mensajes nuevos.
- `limit <max-number-bytes>` — Reemplace `<max-number-bytes>` con el tamaño máximo en bytes que pueden tener los mensajes recuperados por Fetchmail. Esta opción es útil con enlaces lentos, cuando un mensaje largo toma mucho tiempo en descargarse.
- `password '<password>'` — Reemplace `<password>` con la contraseña del usuario.
- `preconnect "<command>"` — Sustituya `<command>` con un comando a ejecutar antes de recuperar los mensajes de este usuario.
- `postconnect "<command>"` — Sustituya `<command>` con el comando a ejecutar después de recuperar los mensajes de este usuario.
- `ssl` — Activa la encriptación SSL.
- `user "<username>"` — Reemplace `<username>` con el nombre de usuario que Fetchmail usa para recuperar los mensajes. *Esta opción debe listarse antes de cualquier otra opción de usuario.*

3.3.5. Opciones de comando de Fetchmail

La mayoría de las opciones de Fetchmail utilizadas en la línea de comando al ejecutar el comando `fetchmail`, reflejan las opciones de configuración de `.fetchmailrc`. Esto se realiza para que se pueda usar Fetchmail con o sin un archivo de configuración. La mayoría de los usuarios no usan estas opciones en la línea de comandos porque les resulta más sencillo dejarlas en el archivo `.fetchmailrc`.

Sin embargo, en ocasiones puede estar interesado en ejecutar el comando `fetchmail` con otras opciones para un fin concreto. Es posible producir opciones de comando para que temporalmente se ignore una configuración `.fetchmailrc` que está causando un error, puesto que cualquier opción especificada en la línea de comandos sobreescribe las opciones del archivo de configuración.

3.3.6. Opciones de depuración o información

Algunas opciones usadas luego del comando `fetchmail` pueden suministrar información importante.

- `--configdump` — Muestra cada opción posible en función de la información de `.fetchmailrc` y los valores por defecto de Fetchmail. No se recupera correo de ningún usuario al usar esta opción.
- `-s` — Ejecuta Fetchmail en modo silencioso, con lo cual se evita que aparezcan mensajes, excepto errores, después del comando `fetchmail`.
- `-v` — Ejecuta Fetchmail en modo detallado y muestra todas las comunicaciones entre Fetchmail y los servidores de correo remotos.
- `-V` — Hace que Fetchmail muestre información de versión detallada, una lista de las opciones globales y los parámetros que se utilizarán con cada usuario, incluido el protocolo de correo y el método de autenticación. No se recupera correo de ningún usuario al usar esta opción.

3.3.7. Opciones especiales

Estas opciones son en ocasiones útiles para sobrescribir los valores por defecto que a menudo contiene el archivo `.fetchmailrc`.

- `-a` — Indica a Fetchmail que descargue todos los mensajes del servidor de correo remoto, ya se hayan o no visto antes. Por defecto, Fetchmail sólo descarga los mensajes nuevos.
- `-k` — Hace que Fetchmail deje una copia de los mensajes en el servidor de correo remoto después de descargarlos. Esta opción sobrescribe el comportamiento por defecto de eliminar los mensajes después de descargarlos.
- `-l <max-number-bytes>` — Indica a Fetchmail que no descargue mensajes con un tamaño superior al indicado y dejarlos en el servidor de correo remoto.
- `--quit` — Sale del proceso de demonio de Fetchmail.

Se pueden encontrar más comandos y opciones de `.fetchmailrc` en la página del manual de `fetchmail`.

4. Configuración del Agente de Transporte de Correo (MTA)

Un *Agente de Transporte de Correo* (MTA) es esencial para enviar correos electrónicos. Un *Agente Usario de Correo* (MUA) tal como **Evolution**, **Thunderbird** y **Mutt** se utiliza para leer y componer correos electrónicos. Cuando un usuario envía un correo electrónico desde un MUA el mensaje se entrega al MTA, el cual envía el mensaje por medio de una serie de MTAs hasta que alcanza su destino.

Si un usuario no tiene previsto enviar un email desde el sistema, algunas tareas automatizadas o programas del sistema utilizarán el comando `/bin/mail` para enviar un correo electrónico que

contenga mensajes de registro para el usuario root del sistema local.

Red Hat Enterprise Linux 5 tiene tres MTAs: Sendmail, Postfix y Exim. Si los tres están instalados, `sendmail` es el MTA predeterminado. El **Conmutador del Agente de Transporte de Correos** le permite a un usuario seleccionar o `sendmail`, `postfix`, o `exim` como el MTA predeterminado para el sistema.

El paquete RPM `system-switch-mail` tiene que ser instalado para utilizar la versión basada en texto del programa **Conmutador del Agente de Transporte de Correos**. Si quiere utilizar la versión gráfica también tiene que tener instaldo el paquete `system-switch-mail-gnome`.

Nota

Para obtener mayor información sobre la instalación de los paquetes RPM consulte ???.

Para iniciar **Conmutador de Agente de Transporte de Correo** seleccione **Sistema** (el menú principal en el panel) => **Administración** => **Conmutador de Agente de Transporte de Correo** o escriba el comando `system-switch-mail` en el intérprete de comandos de shell (por ejemplo, en una terminal XTerm o GNOME).

El programa detecta automáticamente si el sistemas de ventanas X se está ejecutando. Si si lo está haciendo, el programa inicia en modo gráfico como se muestra en Figura 9.1, “Conmutador de Agente de Transporte de Correo”. Si X no es detectado, inicia en modo de texto. Para forzar al **Conmutador del Agente de Transporte de Correo** a que ejecute en modo de texto utilice el comando `system-switch-mail-nox`.

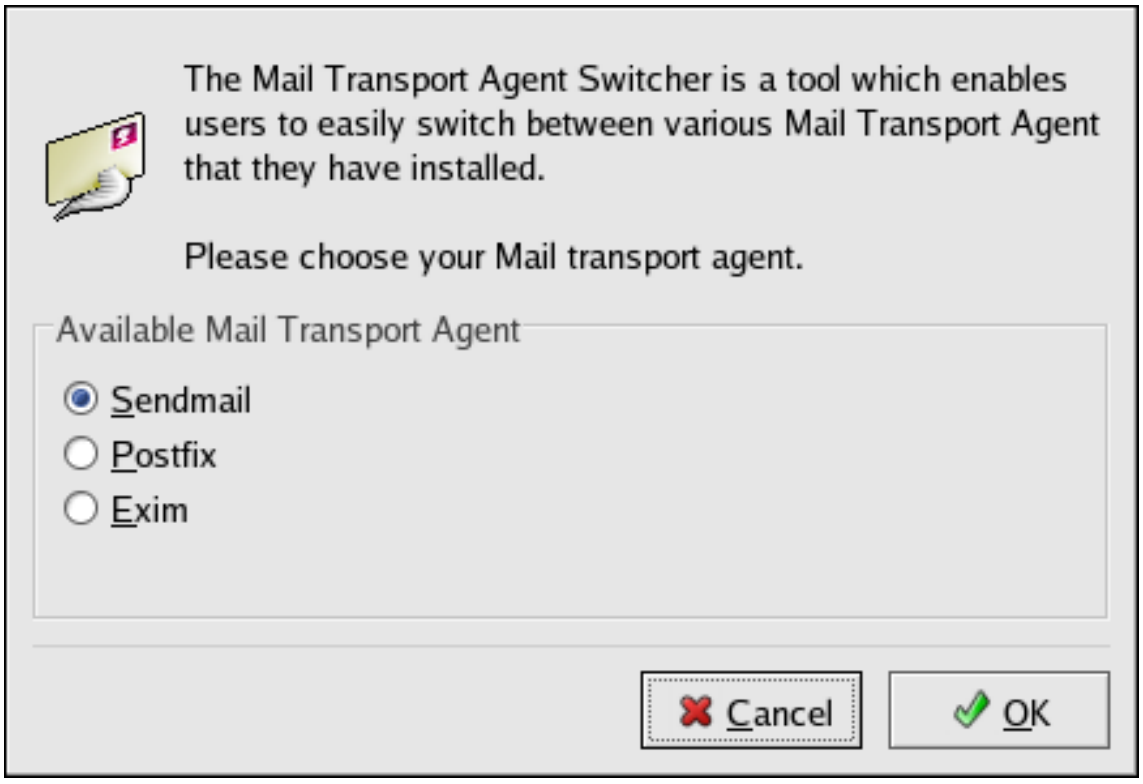


Figura 9.1. Conmutador de Agente de Transporte de Correo

Si selecciona **OK** para cambiar el MTA el demonio de correo seleccionado es habilitado para iniciar en tiempo de arranque y los demonios de correo que no se han seleccionado son deshabilitados para que no inicen en tiempo de arranque. El demonio de correo seleccionado es iniciado y cualquier otro demonio de correo será detenido lo cual hará que los cambios sean efectivos inmediatamente.

5. Agente de entrega de correo

Red Hat Enterprise Linux incluye dos MDAs principales, Procmail y `mail`. Ambas aplicaciones son consideradas Agentes de entrega local (LDAs) y ambas mueven el correo desde el archivo spool MTA al buzón de correo del usuario. Sin embargo, Procmail proporciona un sistema robusto de filtrado de correo.

Esta sección detalla solamente Procmail. Para información sobre el comando `mail`, consulte su página man.

Procmail entrega y filtra correo mientras es colocado en el archivo spool de correo de la máquina local. Es una herramienta eficaz, que hace un uso adecuado de los recursos del sistema y de amplio uso. Procmail desempeña un papel crítico en la entrega de correo a ser leído por las aplicaciones clientes de correo.

Procmail se puede invocar de muchas formas diferentes. Cada vez que un MTA coloca un correo en el archivo spool de correo, Procmail es lanzado. Procmail luego filtra y archiva el correo para el MUA y sale. Alternativamente, el MUA puede ser configurado para ejecutar Procmail cada vez que se recibe un mensaje y así los mensajes son movidos en sus buzones correctos. Por defecto, la presencia de un archivo `/etc/procmailrc` o `.procmailrc` (también llamado archivo *rc*) en el directorio principal del usuario llamará a Procmail cada vez que un MTA reciba un nuevo mensaje.

Las acciones que toma Procmail con un correo dependen de si el mensaje coincide con un grupo de condiciones o de *recetas* particulares en el archivo `rc`. Si un mensaje coincide con la receta o regla, entonces el correo se ubicará en un determinado archivo, se eliminará o se procesará.

Cuando Procmail arranca, lee el mensaje de correo y separa el cuerpo de la información de cabecera. A continuación, busca los archivos `/etc/procmailrc` y `rc` en el directorio por defecto `/etc/procmailrcs`, de todo el sistema, así como las variables de entorno Procmail y reglas. Luego busca si hay un archivo `.procmailrc` en el directorio principal del usuario. Muchos usuarios también crean archivos `rc` adicionales para Procmail a los que se hace referencia dentro de `.procmailrc` en su directorio principal.

Por defecto, no hay archivos `rc` aplicables a todo el sistema en el directorio `/etc/` y ningún archivo de `.procmailrc` existe en ningún directorio de usuarios. Por lo tanto, para comenzar a usar Procmail, cada usuario debe construir un archivo `.procmailrc` con variables de entorno y reglas particulares.

5.1. Configuración de Procmail

El archivo de configuración de Procmail contienen variables de entorno importantes. Estas variables especifican cosas tales como, qué mensajes deben ordenarse, qué hacer con los mensajes que no coinciden con ninguna receta, etc.

Estas variables de entorno normalmente aparecen al principio del archivo `.procmailrc` con el siguiente formato:

```
<env-variable>="<value>"
```

En este ejemplo, `<env-variable>` es el nombre de la variable y `<value>` define la variable.

La mayor parte de los usuarios de Procmail no utilizan muchas variables de entorno y muchas de las variables de entorno más importantes ya están definidas con un valor por defecto. La mayoría de las veces tratará con las siguientes variables:

- `DEFAULT` — Establece el buzón por defecto en el que se ubicarán los mensajes que no coincidan con ninguna receta.

  El valor por defecto `DEFAULT` es el mismo que `$ORGMAIL`.

- `INCLUDERC` — Especifica archivos `rc` adicionales que contienen más recetas para los que deben comprobarse los mensajes. Esto permite desglosar las listas de recetas de Procmail en archivos individuales que cumplen papeles diferentes, tales como como bloquear correo basura y gestionar listas de correo, que se pueden activar o desactivar con caracteres de comentario en el archivo de usuario `.procmailrc`.

  Por ejemplo, las líneas en el archivo `.procmailrc` del usuario se pueden parecer a lo siguiente:

  ```
  MAILDIR=$HOME/Msgs INCLUDERC=$MAILDIR/lists.rc INCLUDERC=$MAILDIR/spam.rc
  ```

  Si el usuario desea desactivar el filtro de Procmail para las listas de correo, pero quiere controlar el correo basura, solamente deberá comentar la primera línea `INCLUDERC` con un carácter `#`.

- `LOCKSLEEP` — Establece cuanto tiempo, en segundos, entre los intentos de Procmail de usar un lockfile concreto. El valor por defecto es ocho segundos.

- `LOCKTIMEOUT` — Establece la cantidad de tiempo, en segundos, que debe transcurrir después de modificar un lockfile para que Procmail asuma que este lockfile es antiguo y que se puede eliminar. El valor por defecto es 1024 segundos.

- `LOGFILE` — El archivo que contendrá los mensajes de error o de información de Procmail.

- `MAILDIR` — Establece el directorio de trabajo actual de Procmail. Si se define este directorio, todas las otras rutas de Procmail serán relativas a este directorio.

- `ORGMAIL` — Especifica el buzón original u otro lugar para colocar los mensajes si no se pueden ubicar en la ubicación de receta o por defecto.

  Por defecto, se utiliza un valor de `/var/spool/mail/$LOGNAME`.

- `SUSPEND` — Establece la cantidad de tiempo, en segundos, que Procmail se detendrá si no

está disponible un recurso necesario, tal como espacio de intercambio (swap).

- SWITCHRC — Permite a un usuario especificar un archivo externo que contiene recetas de Procmail adicionales, como la opción INCLUDERC, excepto que la verificación de recetas es en realidad detenida en el archivo de configuración referido y sólo se usan las recetas en el archivo SWITCHRC especificado.

- VERBOSE — Hace que Procmail registre mucha más información. Esta opción es útil para procesos de depuración.

Otras variables de entorno importantes se extraen del shell, tal como LOGNAME, que es el nombre de conexión, HOME, que es la ubicación del directorio principal y SHELL, que es el shell por defecto.

Hay una explicación completa de todas las variables de entorno y sus valores por defecto en la página man de procmailrc.

5.2. Recetas de Procmail

Con frecuencia los usuarios nuevos consideran que la creación de recetas es la parte más difícil de Procmail. En cierto modo, esto es lógico, ya que las recetas comparan los mensajes con las *expresiones regulares*, el cual es un formato específico que se utiliza para especificar calificaciones para una cadena coincidente. Sin embargo, las expresiones regulares no son difíciles de crear, e incluso es más fácil entenderlas cuando se leen. Además, la consistencia en la forma en que las recetas de Procmail están escritas, independientemente de las expresiones regulares, facilita aprender a través de ejemplos. Para ver ejemplos de recetas consulte Sección 5.2.5, “Ejemplos de recetas”.

Una receta de Procmail tiene la siguiente estructura:

```
:0<flags>: <lockfile-name> * <special-condition-character><condition-1> * <special-condition-character><co
```

Los dos primeros caracteres de una receta de Procmail son dos puntos y un cero. Opcionalmente, se pueden insertar varios indicadores después del cero para controlar cómo Procmail procesa la receta. Dos puntos después de la sección *<flags>* especifica que se creará un lockfile para este mensaje. Si se crea un lockfile, debe especificar su nombre en el espacio *<lockfile-name>*.

Una receta puede contener varias condiciones con las que se comparará el mensaje. Si no tiene condiciones, cada mensaje coincide la receta. Las expresiones regulares se insertan en algunas condiciones para facilitar su comparación con un mensaje. Si se usan varias condiciones, todas ellas deben coincidir para que se realice una acción. Las condiciones se comprueban en función de los indicadores establecidos en la primera línea de la receta. El uso de caracteres especiales opcionales que se insertan después del carácter * permiten controlar todavía más la condición.

La opción *<action-to-perform>* especifica lo que le ocurrirá a un mensaje si coincide con una de las condiciones. Sólo puede haber una acción por receta. En muchos casos, se usa aquí el nombre de un buzón para dirigir los mensajes que coinciden con ese archivo con el fin de ordenar de una manera eficaz el correo. También se pueden utilizar caracteres de acción especiales antes de especificar la acción. Consulte la Sección 5.2.4, “Condiciones y acciones especia-

les" para obtener mayor información.

5.2.1. Recetas de entrega vs. recetas de no entrega

La acción usada si la receta coincide con un mensaje concreto determina si la receta se considera de *entrega* o de *no entrega*. Una receta de entrega contiene una acción que registra el mensaje a un archivo, envía el mensaje a otro programa o reenvía el mensaje a otra dirección de correo. Una receta de no entrega cubre cualquier otra acción, como el uso de un *bloque de anidamiento*. Un bloque de anidamiento es un conjunto de acciones entre llaves `{}`, que designa las acciones adicionales que deben realizarse en los mensajes que cumplen las condiciones de la receta. Los bloques de anidamiento pueden ser anidados uno entre otro, lo cual proporciona un mayor control a la hora de identificar y realizar acciones en los mensajes.

Cuando los mensajes coinciden con una receta de entrega, Procmail lleva a cabo la acción especificada y deja de comparar el mensaje con otras recetas. Los mensajes que coinciden con recetas de no entrega siguen siendo comparados contra otras recetas.

5.2.2. Indicadores

Los indicadores son muy importantes para determinar cómo o si se compararán las condiciones de una receta con un mensaje. Los siguientes indicadores son de uso común:

- `A` — Especifica que esta receta sólo se usará si la receta anterior sin un indicador `A` o `a` también coincidió con este mensaje.
- `a` — Especifica que esta receta sólo se usará si la receta anterior con un indicador `A` o `a` también coincidió con este mensaje *y* se completó exitosamente.
- `B` — Analiza el cuerpo del mensaje y busca condiciones coincidentes.
- `b` — Utiliza el cuerpo en cualquier acción resultante, como escribir el mensaje a un archivo o reenviarlo. Este es el comportamiento por defecto.
- `c` — Genera una copia al carbón (CC) del correo. Es útil para la entrega de recetas, puesto que la acción necesaria se puede realizar en el mensaje y se puede seguir procesando una copia del mensaje en los archivos `rc`.
- `D` — Hace una comparación `egrep` que distingue entre mayúsculas y minúsculas. Por defecto, el proceso de comparación no distingue entre mayúsculas y minúsculas.
- `E` — Similar al indicador `A`, con la diferencia de que las condiciones de la receta sólo se comparan con el mensaje si la receta inmediatamente anterior sin un indicador `E` no coincide. Se puede comparar con la acción *else*.
- `e` — Solamente se compara la receta con el mensaje si la acción especificada en la receta inmediatamente anterior falla.
- `f` — Usa la canalización (pipes) como filtro.
- `H` — Analiza la cabecera del mensaje y busca condiciones coincidentes. Este es el comportamiento por defecto.
- `h` — Usa la cabecera en la acción resultante. Este es el comportamiento por defecto.

- `w` — Indica a Procmail que debe esperar a que finalice el proceso del filtro o programa especificado, y que cree un informe indicando si tuvo éxito o no antes de considerar el mensaje como filtrado.
- `W` — Esto es idéntico a `w` excepto que se eliminan los mensajes "Program failure".

Para una lista detallada de los indicadores asicionales, consulte la página man de `procmailrc`.

5.2.3. Especificación de un Lockfile local

Los archivos lockfiles son muy útiles en Procmail para garantizar que no más de un proceso intenta alterar un mensaje concreto al mismo tiempo. Puede especificar un lockfile local si inserta un carácter de dos puntos (`:`)después de cualquier indicador en la primera línea de una receta. Con esto se creará un lockfile local basado en el nombre de archivo de destino más cualquier otro valor definido en la variable de entorno global `LOCKEXT`.

Como alternativa, puede especificar el nombre del lockfile local que se usará con esta receta después del carácter `:`.

5.2.4. Condiciones y acciones especiales

El uso de caracteres especiales antes de las condiciones y acciones de recetas de Procmail cambian el modo en que se interpretan.

Los siguientes caracteres se pueden usar después del carácter `*` al principio de una línea de condición de receta:

- `!` — En la línea de condición, invierte la condición y ocasiona que sólo se produzca una coincidencia si la condición no coincide con el mensaje.
- `<` — Comprueba si el mensaje está por debajo de un número especificado de bytes.
- `>` — Comprueba si el mensaje está sobre un número especificado de bytes.

Los siguientes caracteres se utilizan para realizar acciones especiales:

- `!` — En la línea de acción, este carácter le indica a Procmail que reenvie el mensaje a las direcciones de correo especificadas.
- `$` — Hace referencia a una variable establecida anteriormente en el archivo `rc`. Se usa normalmente para configurar un buzón común que utilizarán varias recetas.
- `|` — Inicia un programa especificado para procesar el mensaje.
- `{` y `}` — Crea un bloque de anidamiento que se usa para contener recetas adicionales a aplicar a los mensajes coincidentes.

Si no se utiliza un carácter especial al principio de la línea de acción, Procmail asume que la línea de acción está especificando el buzón en donde registrar el mensaje.

5.2.5. Ejemplos de recetas

Procmail es un programa extremadamente flexible. Sin embargo, como resultado de esta flexibilidad, la composición de una receta de Procmail desde cero para alcanzar un objetivo concreto, puede resultar una labor muy complicada para los usuarios nuevos.

La mejor forma de desarrollar habilidades para construir recetas Procmail parte de un buen entendimiento de las expresiones regulares combinadas con la revisión de ejemplos construídos por otros. No entra en el ámbito de este capítulo ofrecer una explicación extensa sobre las expresiones regulares. La estructura de las recetas de Procmail es más importante y hay ejemplos útiles de ellas en varios sitios de Internet (por ejemplo en http://www.iki.fi/era/procmail/links.html). Se puede obtener el uso y la adaptación adecuada de las expresiones regulares contenidas en estos ejemplos observando estos ejemplos de recetas. Puede encontrar información básica sobre las reglas de expresiones regulares en las páginas man de `grep`.

Los ejemplos siguientes demuestran la estructura básica de las recetas Procmail y pueden suministrar la base para construcciones más elaboradas.

Una receta básica puede que ni siquiera tenga condiciones, como se demuestra en el siguiente ejemplo:

```
:0: new-mail.spool
```

La primera línea especifica que se cree un lockfile local pero sin indicar un nombre, de modo que Procmail utilice el nombre del archivo de destino y anexa el valor especificado en la variable de ambiente `LOCKEXT`. No se especifica ninguna condición y, por tanto, cada mensaje coincide con esta receta y se insertará en el archivo de spool denominado `new-mail.spool`, que se encuentra dentro del directorio especificado por la variable de entorno `MAILDIR`. Un agente MUA puede a continuación ver los mensajes de este archivo.

Se puede colocar una receta básica como esta, al final de todos los archivos `rc` para dirigir los mensajes a una ubicación por defecto.

El ejemplo siguiente coincide los mensajes provenientes de una dirección de correo específica y los descarta.

```
:0 * ^From: spammer@domain.com /dev/null
```

Con este ejemplo, cualquier mensaje enviado por `spammer@domain.com` se mueve inmediatamente al dispositivo `/dev/null`, eliminándolos.

Atención

Asegúrese de que una regla funciona adecuadamente antes de mover los mensajes a `/dev/null`, que supone una eliminación permanente. Si las condiciones de receta "atrapan" inadvertidamente mensajes no destinados correctamente y estos mensajes desaparecen sin dejar rastro, entonces se hace más difícil revisar problemas en la regla.

Una solución mejor es dirigir la acción de la receta a un buzón especial que compruebe de vez en cuando para buscar positivos falsos. Una vez comprobado que

no se han coincidido por error los mensajes, puede eliminar el buzón y dirigir la acción para enviar los mensajes a `/dev/null`.

La receta siguiente atrapa el correo enviado a una lista de correo particular y lo coloca en una carpeta indicada.

```
:0: * ^(From|CC|To).*tux-lug tuxlug
```

Cualquier mensaje enviado desde la lista de distribución `tux-lug@domain.com` se colocará automáticamente en el buzón `tuxlug` para el agente MUA. Tenga en cuenta que la condición de este ejemplo comparará el mensaje si tiene la dirección de correo de la lista de distribución en las líneas `Desde`, `CC`, o `Para`.

Para obtener más detalles consulte los muchos recursos disponibles para Procmail en línea en la Sección 7, “Recursos adicionales”.

5.2.6. Filtros de correo basura

Puesto que Procmail es llamado por Sendmail, Postfix y Fetchmail cuando reciben nuevos correos, se puede usar también como una herramienta poderosa para combatir correo basura.

Esto es particularmente cierto cuando Procmail es usado en conjunto con SpamAssassin. Cuando se usan juntos, estas dos aplicaciones pueden identificar rápidamente correo basura y ordenarlos o destruirlos.

SpamAssassin usa análisis de las cabeceras, de texto, listas negras, una base de datos de seguimiento de correo basura y el análisis de correo basura Bayesiano de autoaprendizaje, para identificar y marcar efectivamente el correo basura.

La forma más fácil para que un usuario local use SpamAssassin es colocar la siguiente línea cerca de la parte superior del archivo `~/.procmailrc`:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc
```

El `/etc/mail/spamassassin/spamassassin-default.rc` contiene una regla simple de Procmail que activa SpamAssassin para todo el correo entrante. Si un correo es identificado como basura, se marca en la cabecera como tal y en el título se coloca:

```
*****SPAM*****
```

El cuerpo del mensaje es también marcado al principio con una lista de qué elementos provocaron que fuese considerado basura.

Para archivar correo marcado como basura, se puede usar una regla similar a lo siguiente:

```
:0 Hw * ^X-Spam-Status: Yes spam
```

Esta regla archiva todo el correo marcado como basura en el buzón de correo llamado `spam`.

Puesto que SpamAssassin es un script Perl, puede ser necesario en servidores ocupados usar

un demonio binario SpamAssassin (`spamd`) y la aplicación cliente (`spamc`). Configurar SpamAssassin de esta forma requiere acceso root.

Para arrancar el demonio `spamd`, escriba el siguiente comando como usuario root:

```
/sbin/service spamassassin start
```

Para iniciar el demonio SpamAssassin cuando se inicia el sistema, use una utilidad initscript, tal como la **Herramienta de Configuración de Servicios** (`system-config-services`), para activar el servicio `spamassassin`. Consulte la para más información sobre las utilidades initscript.

Para configurar Procmail a usar la aplicación cliente SpamAssassin en vez de un script Perl, coloque la siguiente línea cerca de la parte superior del archivo `~/.procmailrc` . Para una configuración global del sistema, colóquela en `/etc/procmailrc`:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-spamc.rc
```

6. Agentes de usuario de correo

Hay muchos programas de correo disponibles bajo Red Hat Enterprise Linux. Hay programas gráficos de clientes de correo con características completas tal como **Ximian Evolution** así como también programas basados en texto, tales como `mutt`.

El resto de esta sección se enfoca en asegurar la comunicación entre el cliente y el servidor.

6.1. Comunicación segura

Los MUAs populares incluidos con Red Hat Enterprise Linux tales como **Ximian Evolution** y `mutt` ofrecen sesiones de correo electrónico encriptadas con SSL.

Al igual que otros servicios existentes en una red no cifrada, la información de correo electrónico importante, como nombres de usuario, contraseñas y mensajes, se puede interceptar y ver sin que tenga conocimiento el servidor o el cliente de correo. Al usar los protocolos estándar POP e IMAP, toda la información de autenticación se envía "limpiamente", sin encriptar, por lo que es posible para un intruso ganar acceso a las cuentas de usuarios reuniendo los nombres de los usuarios y sus contraseñas cuando estos son transmitidos sobre la red.

6.1.1. Clientes de correo electrónico seguros

Afortunadamente, la mayoría de los agentes MUA de Linux diseñados para comprobar correo en servidores remoto utilizan SSL. Para usar SSL al recuperar el correo, se debe activar esta opción en el cliente y en el servidor de correo.

SSL se activa muy fácilmente en el cliente, normalmente basta con pulsar un botón en el área de configuración del agente MUA o mediante una opción en el archivo de configuración del MUA. Los protocolos IMAP y POP seguros tienen números de puerto conocidos (993 y 995, respectivamente) que el MUA utiliza para autenticar y descargar los mensajes.

6.1.2. Asegurar las comunicaciones de cliente de correo

Ofrecer cifrado SSL a los usuarios de IMAP y POP del servidor de correo es muy sencillo.

Primero, cree un certificado SSL. Esto se puede hacer de dos formas: solicitando a una *Certificate Authority* (*CA*) por un certificado SSL o mediante la creación de un certificado auto-firmado.

Atención

Los certificados auto-firmados solamente deberían ser usados para propósitos de prueba. Cualquier servidor usado en un ambiente de producción debería usar un certificado SSL emitido por una CA.

Para crear un certificado SSL con firma propia para IMAP, cámbiese al directorio `/etc/pki/tls/certs/` y escriba el comando siguiente como root:

```
rm -f cyrus-imapd.pem make cyrus-imapd.pem
```

Conteste todas las preguntas para completar el proceso.

Para crear un certificado SSL con firma propia para POP, cámbiese al directorio `/etc/pki/tls/certs/` y escriba los siguientes comandos como usuario root:

```
rm -f ipop3d.pem make ipop3d.pem
```

Una vez más, conteste todas las preguntas para completar el proceso.

Importante

Asegúrese de eliminar los archivos predeterminados `imapd.pem` y `ipop3d.pem` antes de ejecutar el comando `make`.

Una vez finalizado, ejecute el comando `/sbin/service xinetd restart` para reiniciar el demonio `xinetd` que controla `imapd` y `ipop3d`.

Alternativamente, el comando `stunnel` puede ser usado como una envoltura de criptación SSL con el estándar, para los demonios no seguros, `imapd` o `pop3d`.

El programa `stunnel` utiliza bibliotecas OpenSSL externas incluidas con Red Hat Enterprise Linux para proporcionar una criptografía robusta y proteger las conexiones. Es mejor solicitar a una Autoridad de Certificación (Certificate Authority, CA) un certificado SSL, pero también es posible crear un certificado auto-firmado.

Para crear un certificado SSL auto-firmado, cámbiese al directorio `/etc/pki/tls/certs/` y escriba el `/etc/pki/tls/certs/` siguiente comando:

```
make stunnel.pem
```

Una vez más, conteste todas las preguntas para completar el proceso.

Una vez que el certificado es generado, es posible usar el comando `stunnel` para iniciar el demonio de correo `imapd` usando el comando siguiente:

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd imapd
```

Una vez que este comando es emitido, es posible abrir un cliente de correo IMAP y conectarse al servidor de correo usando una encriptación SSL.

Para arrancar `pop3d` usando el comando `stunnel`, escriba el comando siguiente:

```
/usr/sbin/stunnel -d 995 -l /usr/sbin/pop3d pop3d
```

Para más información sobre el uso de `stunnel`, lea la página man `stunnel` o refiérase a los documentos en el directorio `/usr/share/doc/stunnel-<version-number>/`, donde *<version-number>* es el número de versión para `stunnel`.

7. Recursos adicionales

La siguiente es una lista con la documentación adicional sobre las aplicaciones de correo.

7.1. Documentación instalada

- Información sobre la configuración de Sendmail es incluida con los paquetes `sendmail` y `sendmail-cf`.

  - `/usr/share/sendmail-cf/README` — Contiene información sobre `m4`, ubicaciones de archivos para Sendmail, transportadores de correo soportados, cómo acceder a las características avanzadas y más.

  Además, las páginas man de `sendmail` y `aliases` contienen información útil sobre varias opciones de Sendmail y la configuración adecuada del archivo Sendmail `/etc/mail/aliases`.

- `/usr/share/doc/postfix-<version-number>/` — Este directorio contiene una gran cantidad de información sobre Postfix. Reemplace *<version-number>* con el número de la versión de Postfix.

- `/usr/share/doc/fetchmail-<version-number>` — Contiene una lista completa de las características de Fetchmail en el archivo `FEATURES` y un documento `FAQ` introductorio. Reemplace *<version-number>* con el número de versión de Fetchmail.

- `/usr/share/doc/procmail-<version-number>` — Contiene un archivo `README` que proporciona una visión general de Procmail, un archivo `FEATURES` que explora cada característica del programa y una sección `FAQ` con respuestas a muchas de las pregunas comunes. Reemplace *<version-number>* con el número de versión de Procmail.

  Mientras aprende cómo Procmail funciona y cómo crear nuevas recetas, las siguientes páginas man son de gran utilidad:

  - `procmail` — Proporciona una vista general de cómo Procmail funciona y los pasos implicados cuando se esté filtrando correo.

- `procmailrc` — Explica el formato del archivo `rc` usado para construir recetas.
- `procmailex` — Proporciona un número de ejemplos de la vida real de recetas Procmail.
- `procmailsc` — Explica la técnica de puntaje por pesos usada por Procmail para ver si una receta particular coincide un mensaje.
- `/usr/share/doc/spamassassin-<version-number>/` — Este directorio contiene una gran cantidad de información sobre SpamAssassin. Reemplace `<version-number>` con el número de la versión del paquete `spamassassin`.

7.2. Sitios web útiles

- http://www.sendmail.org/ — Ofrece un desglose completo de las características técnicas de Sendmail y ejemplos de configuración.
- http://www.sendmail.com/ — Contiene noticias, entrevistas y artículos concernientes a Sendmail, incluyendo una vista ampliada de las muchas opciones disponibles.
- http://www.postfix.org/ — La página principal para el proyecto Procmail con mucha información sobre Postfix. La lista de correo es un buen lugar para comenzar a buscar información.
- http://fetchmail.berlios.de/ — La página principal para Fetchmail, presentando un manual en línea y una sección Preguntas Frecuentes (FAQ) completa.
- http://www.procmail.org/ — La página principal para Procmail con enlaces a listas de correo varias dedicadas a Procmail así como también varios documentos FAQ.
- http://partmaps.org/era/procmail/mini-faq.html — Una sección FAQ excelente de Procmail, ofrece sugerencias para la solución de problemas, detalles sobre bloqueo de archivos y el uso de comodines.
- http://www.uwasa.fi/~ts/info/proctips.html — Contiene docenas de sugerencias que hacen el uso de Procmail mucho más fácil. Incluye instrucciones sobre cómo probar los archivos `.procmailrc` y usar el puntaje de Procmail para decidir si una acción particular debería ser tomada.
- http://www.spamassassin.org/ — El sitio oficial del proyecto SpamAssassin.

7.3. Libros relacionados

- *Sendmail Milters: A Guide for Fighting Spam* por Bryan Costales y Marcia Flynt; Addison-Wesley — Un buen manual sobre Sendmail que le puede ayudar a personalizar sus filtros de correo.
- *Sendmail* por Bryan Costales con Eric Allman et al; O'Reilly & Associates — Una buena referencia sobre Sendmail escrita con la ayuda del creador original de Delivermail y Sendmail.
- *Removing the Spam: Email Processing and Filtering* por Geoff Mulligan; Addison-Wesley Publishing Company — Un volumen que muestra varios métodos usados por los administradores de correo usando herramientas establecidas, tales como Sendmail y Procmail, para

manejar los problemas del correo basura.

- *Internet Email Protocols: A Developer's Guide* por Kevin Johnson; Addison-Wesley Publishing Company — Proporciona una revisión profunda de los principales protocolos y la seguridad que éstos proporcionan.
- *Managing IMAP* por Dianna Mullet y Kevin Mullet; O'Reilly & Associates — Detalla los pasos necesarios para configurar un servidor IMAP.

Capítulo 10. Protocolo Ligero de Acceso a Directorios (LDAP)

El *Protocolo Ligero de Acceso a Directorios* (en inglés, *Lightweight Directory Access Protocol*, *LDAP*) es un conjunto de protocolos abiertos usados para acceder información almacenada centralmente a través de la red. Está basado en el estándar *X.500* para compartir directorios, pero es menos complejo e intensivo en el uso de recursos. Por esta razón, a veces se habla de LDAP como "*X.500 Lite*." El estándar X.500 es un directorio que contiene información de forma jerárquica y categorizada que puede incluir nombres, directorios y números telefónicos.

Como X.500, LDAP organiza la información en un modo jerárquico usando directorios. Estos directorios pueden almacenar una gran variedad de información y se pueden incluso usar de forma similar al Servicio de información de red (NIS), permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina en la red acreditada con LDAP.

Sin embargo, en la mayoría de los casos, LDAP se usa simplemente como un directorio telefónico virtual, permitiendo a los usuarios acceder fácilmente la información de contacto de otros usuarios. Pero LDAP va mucho más lejos que un directorio telefónico tradicional, ya que es capaz de propagar su consulta a otros servidores LDAP por todo el mundo, proporcionando un repositorio de información ad-hoc global. Sin embargo, en este momento LDAP se usa más dentro de organizaciones individuales, como universidades, departamentos del gobierno y compañías privadas.

LDAP es un sistema cliente/servidor. El servidor puede usar una variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápidas y en gran volúmen. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede, o bien consultar un directorio, o intentar modificarlo. En el evento de una consulta, el servidor, puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta. Si la aplicación cliente está intentando modificar información en un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información.

Este capítulo hace referencia a la configuración y uso de OpenLDAP 2.0, una implementación de código abierto de los protocolos LDAPv2 y LDAPv3.

1. Razones por las cuales usar LDAP

La mayor ventaja de LDAP es que se puede consolidar información para toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central, accesible desde cualquier parte de la red. Puesto que LDAP soporta la Capa de conexión segura (SSL) y la Seguridad de la capa de transporte (TLS), los datos confidenciales se pueden proteger de los curiosos.

LDAP también soporta un número de bases de datos back-end en las que se guardan directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar. También, ya

que LDAP tiene una interfaz de programación de aplicaciones (API) bien definida, el número de aplicaciones acreditadas para LDAP son numerosas y están aumentando en cantidad y calidad.

1.1. Características de OpenLDAP

OpenLDAP incluye un número de características importantes.

- *Soporte LDAPv3* — OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL), entre otras mejoras. Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.
- *Soporte IPv6* — OpenLDAP soporta la próxima generación del protocolo de Internet versión 6.
- *LDAP sobre IPC* — OpenLDAP se puede comunicar dentro de un sistema usando comunicación interproceso (IPC). Esto mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.
- *API de C actualizada* — Mejora la forma en que los programadores se conectan para usar servidores de directorio LDAP.
- *Soporte LDIFv1* — Provee compatibilidad completa con el formato de intercambio de datos, Data Interchange Format (LDIF) versión 1.
- *Servidor Stand-Alone mejorado* — Incluye un sistema de control de acceso actualizado, conjunto de hilos, herramientas mejoradas y mucho más.

2. Terminología LDAP

Cualquier discusión sobre LDAP requiere un entendimiento básico del conjunto de términos específicos de LDAP:

- *entrada* — una entrada es una unidad en un directorio LDAP. Cada entrada se identifica por su único *Nombre distinguido* (*Distinguished Name (DN)*).
- *atributos* — Los atributos son piezas de información directamente asociada con la entrada. Por ejemplo, una organización puede ser representada como una entrada LDAP. Los atributos asociados con la organización pueden ser su número de fax, su dirección, etc. En un directorio LDAP las entradas pueden ser también personas, con atributos comunes como el número de teléfono y la dirección de e-mail.

  Algunos atributos son obligatorios mientras que otros son opcionales. Una definición *objectclass* determina los atributos que se necesitan y los que no para cada entrada. Las definiciones de objectclass se encuentran en varios archivos de esquema dentro del directorio `/etc/openldap/schema/`. Para obtener mayor información consulte la Sección 5, “El directorio /etc/openldap/schema/”.

  La afirmación de un atributo y su valor correspondiente también se conocen como *Nombre*

Distinguido Relativo (RDN). Un RDN sólamente es único por entrada mientras que un DN es unico globalmente.

- *LDIF* — El *Formato de intercambio de datos de LDAP* (LDIF) es una representación de texto ASCII de entradas LDAP. Los archivos usados para importar datos a los servidores LDAP deben estar en formato LDIF. Una entrada LDIF se ve similar al ejemplo siguiente:

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

  Una entrada puede contener tantos pares `<attrtype>: <attrvalue>` como sean necesarios. Una línea en blanco indica el final de una entrada.

Aviso

Todas las parejas `<attrtype>` y `<attrvalue>`*deben* estar definidas en el archivo esquema correspondiente para usar esta información.

  Cualquier valor comprendido dentro de `<` y `>` es una variable y puede ser configurado cuando se cree una nueva entrada LDAP. Sin embargo, esta regla no se aplica a `<id>`. El `<id>` es un número determinado por la aplicación que se usa para modificar la entrada.

3. Demonios y utilidades OpenLDAP

El grupo de bibliotecas y herramientas OpenLDAP están incluidas en los paquetes siguientes:

- `openldap` — Contiene las librerías necesarias para ejecutar las aplicaciones del servidor y cliente OpenLDAP.
- `openldap-clients` — Contiene herramientas de línea de comandos para visualizar y modificar directorios en un servidor LDAP.
- `openldap-server` — Contiene los servidores y otras utilidades necesarias para configurar y ejecutar un servidor LDAP.

Hay dos servidores contenidos en el paquete `openldap-servers`: el *Demonio independiente LDAP* (`/usr/sbin/slapd`) y el *Demonio independiente de actualización de réplicas LDAP* (`/usr/sbin/slurpd`).

El demonio `slapd` es el servidor independiente LDAP mientras que el demonio `slurpd` es usado para sincronizar los cambios desde un servidor LDAP a otro en la red. El demonio `slurpd` sólo es usado cuando se trabaja con múltiples servidores LDAP.

Para llevar a cabo tareas administrativas, el paquete `openldap-server` instala las utilidades siguientes en el directorio `/usr/sbin/`:

- `slapadd` — Añade entradas desde un archivo LDIF a un directorio LDAP. Por ejemplo, el comando `/usr/sbin/slapadd -l ldif-input` leerá en el archivo LDIF, *`ldif-input`*, que contiene las nuevas entradas.

Importante

Debe ser usuario root para usar `/usr/sbin/slapadd`. Sin embargo, el servidor de directorio se ejecuta como usuario `ldap`. Por lo tanto, el servidor de directorio no podrá modificar ningún archivo creado por `slapadd`. Para corregir este problema, después que haya terminado de usar `slapadd`, escriba el comando siguiente:

```
chown -R ldap /var/lib/ldap
```

- `slapcat` — Extrae entradas de un directorio LDAP en el formato por defecto *Sleepycat Software's Berkeley DB*, y las guarda en un archivo LDIF. Por ejemplo, el comando `/usr/sbin/slapcat -l ldif-output` tendrá como resultado un archivo LDIF llamado `ldif-output` que contendrá las entradas para el directorio LDAP.
- `slapindex` — Re-indexa el directorio `slapd` basado en el contenido actual. Esta herramienta se debería ejecutar siempre que se cambien las opciones de indexado dentro de `/etc/openldap/slapd.conf`.
- `slappasswd` — Genera un valor de contraseña encriptada de usuario para ser usada con `ldapmodify` o el valor `rootpw` en el archivo de configuración `slapd`, `/etc/openldap/slapd.conf`. Ejecute el comando `/usr/sbin/slappasswd` para crear la contraseña.

Aviso

Asegúrese de detener `slapd` ejecutando `/sbin/service lapd stop` antes de usar `slapadd`, `slapcat` o `slapindex`. De otro modo se pondrá en riesgo la integridad del directorio LDAP.

Para más información sobre cómo utilizar estas utilidades, consulte sus páginas del manual respectivas.

El paquete `openldap-clients` instala herramientas utilizadas para agregar, modificar y borrar entradas en un directorio LDAP dentro de `/usr/bin/` Estas herramientas incluyen lo siguiente:

- `ldapadd` — Agrega entradas a un directorio LDAP aceptando entradas vía archivo o entrada estándar; `ldapadd` es en realidad un enlace duro a `ldapmodify -a`.
- `ldapdelete` — Borra entradas de un directorio LDAP al aceptar instrucciones del usuario por medio de la entrada desde el indicador de comandos o por medio de un archivo.
- `ldapmodify` — Modifica las entradas en un directorio LDAP, aceptando la entrada por medio de un archivo o entrada estándar.
- `ldappasswd` — Configura una contraseña para un usuario LDAP.

- `ldapsearch` — Busca por entradas en el directorio LDAP usando un indicador de comandos shell.
- `ldapcompare` — Abre una conexión a un servidor LDAP, se vincula y hace una comparación utilizando parámetros especificados.
- `ldapwhoami` — Abre una conexión en un servidor LDAP, se vincula y realiza una operación `whoami`.
- `ldapmodrdn` — Abre una conexión en un servidor LDAP, se vincula y modifica los RDNs de entradas.

Con la excepción de `ldapsearch`, cada una de estas utilidades se usa más fácilmente haciendo referencia a un archivo que contiene los cambios que se deben llevar a cabo, que escribiendo un comando para cada entrada que se desea cambiar en un directorio LDAP. El formato de dicho archivo está esquematizado en las páginas del manual sobre cada utilidad.

3.1. NSS, PAM, y LDAP

Además de los paquetes OpenLDAP, Red Hat Enterprise Linux incluye un paquete llamado `nss_ldap`, el cual mejora la habilidad de LDAP para integrarse tanto en Linux como en otros ambientes UNIX.

El paquete `nss_ldap` provee los siguientes módulos (en donde `<version>` se refiere a la versión de `libnss_ldap` en uso):

- `/lib/libnss_ldap-<version>.so`
- `/lib/security/pam_ldap.so`

El paquete `nss_ldap` provee los siguientes módulos para las arquitecturas Itanium o AMD64.

- `/lib64/libnss_ldap-<version>.so`
- `/lib64/security/pam_ldap.so`

El módulo `libnss_ldap-<version>.so` permite a las aplicaciones buscar usuarios, grupos, hosts y otra información utilizando un directorio LDAP por medio de la interfaz de `glibc`*Nameservice Switch* (NSS). NSS permite a las aplicaciones autenticarse usando LDAP junto con el servicio de nombres de NIS y archivos de autenticación planos.

El módulo `pam_ldap` permite que las aplicaciones PAM puedan validar usuarios utilizando la información almacenada en el directorio LDAP. Las aplicaciones PAM incluyen conexiones desde la consola, servidores de correo POP e IMAP y Samba. Al desarrollar un servidor LDAP en una red, se pueden autentificar todas estas aplicaciones usando la misma combinación de nombre de usuario y contraseña, simplificando en gran medida la administración.

3.2. PHP4, LDAP y el Servidor HTTP Apache

Red Hat Enterprise Linux incluye también un paquete que contiene un módulo LDAP para el lenguaje de comandos del servidor PHP.

El paquete `php-ldap` añade soporte LDAP al lenguaje incluido en HTML, PHP4 a través del módulo `/usr/lib/php4/ldap.so`. Este módulo permite a los scripts PHP4 acceder a información almacenada en un directorio LDAP.

Red Hat Enterprise Linux se entrega con el módulo `mod_authz_ldap` para el Servidor HTTP Apache. Este módulo utiliza la forma corta del nombre distinguido para un sujeto y el emisor del certificado de cliente SSL para determinar el nombre distinguido de un usuario dentro de un directorio LDAP. También es capaz de autorizar usuarios basado en los atributos de esa entrada del usuario del directorio LDAP, determinando el acceso a los activos basado en los privilegios de usuario y grupo de ese activo y negando el acceso a los usuarios con contraseñas caducadas. Se requiere el módulo `mod_ssl` cuando se utilice el módulo `mod_authz_ldap`.

Importante

El módulo `mod_authz_ldap` no autentica a un usuario en un directorio LDAP usando un hash de contraseña encriptado. Esta funcionalidad es proporcionada por el módulo experimental `mod_auth_ldap`, el cual no está incluido con Red Hat Enterprise Linux. Para más detalles sobre el estado de este módulo vea el sitio web de la Apache Software Foundation en http://www.apache.org/.

3.3. Aplicaciones cliente LDAP

Existen clientes gráficos de LDAP que soportan la creación y modificación de directorios, pero *no* se entregan con Red Hat Enterprise Linux. Una de estas aplicaciones es **LDAP Browser/Editor** — Una herramienta basada en Java que está disponible en línea en http://www.iit.edu/~gawojar/ldap/.

Otros clientes LDAP acceden a directorios como sólo lectura, utilizándolos como referencia, pero sin alterar información a lo largo de la organización. Algunos ejemplos de tales aplicaciones son Sendmail, **Mozilla**, **Gnome Meeting**, and **Evolution**.

4. Archivos de configuración de OpenLDAP

Los archivos de configuración OpenLDAP son instalados dentro del directorio `/etc/openldap/`. A continuación aparece una lista breve marcando los directorios y archivos más importantes:

- `/etc/openldap/ldap.conf` — Este es el archivo de configuración para todas las aplicaciones *cliente* que usan las bibliotecas OpenLDAP tales como `ldapsearch`, `ldapadd`, Sendmail, **Pine**, **Balsa**, **Evolution**, y **Gnome Meeting**.
- `/etc/openldap/slapd.conf` — Este es el archivo configuración para el demonio `slapd`. Vea la Sección 6.1, “Modificar /etc/openldap/slapd.conf” para obtener más información sobre este archivo.
- Directorio `/etc/openldap/schema/`— Este subdirectorio contiene el esquema utilizado por el demonio `slapd`. Vea la Sección 5, “El directorio /etc/openldap/schema/” para obtener más información sobre este directorio.

Nota

Si está instalado el paquete `nss_ldap` creará un archivo llamado `/etc/ldap.conf`. Este archivo es usado por los módulos PAM y NSS proporcionados por el paquete `nss_ldap`. Vaya a Sección 7, “Configurar un sistema para la autenticación mediante OpenLDAP” para obtener más información.

5. El directorio `/etc/openldap/schema/`

El directorio `/etc/openldap/schema/` almacena las definiciones LDAP, previamente ubicadas en los archivos `slapd.at.conf` y `slapd.oc.conf`. El directorio `/etc/openldap/schema/redhat/` guarda esquemas personalizados distribuidos por Red Hat para Red Hat Enterprise Linux.

Todas las *definiciones de sintaxis de atributos* y las *definiciones de objectclass* son ahora ubicadas en los diferentes archivos de esquema. Los archivos de esquemas son referenciados en `/etc/openldap/slapd.conf` usando líneas `include`, como se muestra en este ejemplo:

```
include /etc/openldap/schema/core.schema include /etc/openldap/schema/cosine.schema include /etc/openldap/
```

Aviso

No modifique ninguno de los ítems de esquemas definidos en los archivos de esquemas instalados por OpenLDAP.

Puede extender el esquema usado por OpenLDAP para soportar tipos de atributos adicionales y clases de objetos usando los archivos de esquema por defecto como una guía. Para lograr esto, cree un archivo `local.schema` en el directorio `/etc/openldap/schema`. Referencie este nuevo esquema dentro de `slapd.conf` agregando la línea siguientes debajo de las líneas `include` por defecto:

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

Luego, defina nuevos tipos de atributos y clases de objetos dentro del archivo `local.schema`. Muchas organizaciones usan los tipos de atributos existentes a partir de los archivos esquema instalados por defecto y agregan nuevas clases de objeto al archivo `local.schema`.

Ampliar esquemas para cubrir requerimientos específicos es un poco complicado y está más allá del ámbito de éste capítulo. Visite http://www.openldap.org/doc/admin/schema.html para más información.

6. Descripción general de la configuración de OpenLDAP

Esta sección explica rápidamente la instalación y la configuración del directorio OpenLDAP. Pa-

ra más información, consulte las URLs siguientes:

- http://www.openldap.org/doc/admin/quickstart.html — El manual *Quick-Start Guide* en el sitio web de OpenLDAP.
- http://www.tldp.org/HOWTO/LDAP-HOWTO/index.html — The *LDAP Linux HOWTO* del Proyecto de Documentación de Linux.

Los pasos básicos para crear un servidor LDAP son los siguientes:

1. Instale los RPMs `openldap`, `openldap-servers` y `openldap-clients`.
2. Modifique el archivo `/etc/openldap/slapd.conf` para referenciar su dominio y servidor LDAP. Para obtener mayor información consulte la Sección 6.1, “Modificar /etc/openldap/slapd.conf”.
3. Inicie `slapd` con el comando:

   ```
   /sbin/service ldap start
   ```

   Después de configurar LDAP, puede usar `chkconfig`, `/usr/sbin/ntsysv`, o **Herramienta de configuración de servicios**para configurar LDAP para que se inicie en el momento de arranque. Para obtener más información sobre cómo configurar servicios refiérase al capítulo Capítulo 3, *Control de acceso a servicios*.
4. Agregue entradas a un directorio LDAP con `ldapadd`.
5. Use `ldapsearch` para ver si `slapd` accede a la información correctamente.
6. Llegados a este punto, su directorio LDAP debería estar funcionando correctamente y se puede configurar con aplicaciones capacitadas para LDAP.

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

Para poder usar el servidor LDAP `slapd`, tendrá que modificar su archivo de configuración, `/etc/openldap/slapd.conf` para especificar el dominio y servidor correcto.

La línea de `suffix` nombra el dominio para el cual el servidor LDAP proveerá información y deberá ser cambiado de:

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

Modifiquelo para que refleje un nombre de dominio completamente calificado. Por ejemplo:

```
suffix "dc=example,dc=com"
```

La entrada `rootdn` es el Nombre distinguido (DN) para un usuario que no está restringido por el control de acceso o los parámetros de límites administrativos fijados para operaciones en el directorio LDAP. Se puede pensar en el usuario `rootdn` como el usuario root para el directorio LDAP. En el archivo de configuración, cambie la línea `rootdn` de su valor por defecto a algo similar a lo siguiente:

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

Cuando esté poblando el directorio LDAP sobre una red, cambie la línea `rootpw` — reemplazando el valor por defecto con una cadena de contraseña encriptada. Para crear una cadena de contraseña encriptada, escriba el comando siguiente:

```
slappasswd
```

Se le pedirá ingresar y re-ingresar la contraseña, luego el programa muestra la contraseña resultante encriptada al terminal.

Luego, copie la nueva contraseña encriptada en el archivo `>/etc/openldap/slapd.conf` en alguna de las líneas `rootpw` y elimine el símbolo de almohadilla (`#`).

Cuando termine, la línea debería de verse como el ejemplo siguiente:

```
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

Aviso

Las contraseñas LDAP, incluyendo la directiva `rootpw` especificada en `/etc/openldap/slapd.conf`, son enviadas sobre la red *sin encriptar*, a menos que active la encriptación TLS.

Para activar la encriptación TLS, revise los comentarios en `/etc/openldap/slapd.conf` y vea la página del manual para `slapd.conf`.

Para mayor seguridad, la directriz `rootpw` debería ser colocada entre comentarios después de poblar el directorio LDAP simplemente escribiendo el símbolo de almohadilla (`#`).

Cuando utilice la herramienta de línea de comandos `/usr/sbin/slapadd` localmente para poblar el directorio LDAP, el uso de la directiva `rootpw` no es necesario.

Importante

Debe ser usuario root para usar `/usr/sbin/slapadd`. Sin embargo, el servidor de directorio se ejecuta como usuario `ldap`. Por lo tanto, el servidor de directorio no podrá modificar ningún archivo creado por `slapadd`. Para corregir este problema, después que haya terminado de usar `slapadd`, escriba el comando siguiente:

```
chown -R ldap /var/lib/ldap
```

7. Configurar un sistema para la autenticación mediante OpenLDAP

Este sección ofrece una perspectiva general de cómo configurar la autenticación usando OpenLDAP. A menos que usted sea un experto en OpenLDAP necesitará más información de

la que le proporcionamos aquí. Para obtener más información consulte las referencias proporcionadas en Sección 9, “Recursos adicionales”.

Instale los paquetes LDAP Necesarios. Primero, debería asegurarse de tener los paquetes apropiados en ambos, el servidor LDAP y las máquinas cliente LDAP. El servidor LDAP requiere el paquete `openldap-server`.

Los paquetes `openldap`, `openldap-clients`, y `nss_ldap` necesitan estar instalados en todas las máquinas LDAP clientes.

Modifique los Archivos de Configuración.

- En el servidor, modifique el archivo `/etc/openldap/slapd.conf` en el servidor LDAP para asegurarse de que corresponde con las especificaciones de su organización. Por favor refiérase a Sección 6.1, “Modificar /etc/openldap/slapd.conf” para obtener instrucciones sobre la modificación de `slapd.conf`.
- En las máquinas clientes, ambos archivos `/etc/ldap.conf` y `/etc/openldap/ldap.conf` necesitan contener el servidor apropiado y la información base de búsqueda para la organización.

  Para hacer esto, ejecute **Herramienta de Configuración de Autenticación** (`system-config-authentication`) y seleccione **Activar Soporte LDAP** bajo la pestaña **Información de Usuario**.

  También puede editar estos archivos manualmente.
- En las máquinas clientes, el archivo `/etc/nsswitch.conf` debe ser editado para usar LDAP.

  Para hacer esto, ejecute **Herramienta de Configuración de Autenticación** (`system-config-authentication`) y seleccione **Activar Soporte LDAP** bajo la pestaña **Información de Usuario**.

  Si está modificando el archivo `/etc/nsswitch.conf` manualmente, agregue `ldap` a las líneas adecuadas.

  Por ejemplo:

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

7.1. PAM y LDAP

7.2. Migrar la información de autenticación antigua al formato LDAP

El directorio `/usr/share/openldap/migration/` contiene un conjunto de scripts de shell y Perl para la migración de información de autenticación en el formato LDAP.

Nota

Debe tener Perl instalado en su sistema para usar estos scripts.

Primero, modifique el archivo `migrate_common.ph` para que refleje el dominio correcto. El dominio DNS por defecto debería ser modificado desde su valor por defecto a algo como lo siguiente:

```
$DEFAULT_MAIL_DOMAIN = "example";
```

La base por defecto también debería ser modificada para que se parezca a:

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

La tarea de migrar una base de datos de usuario a un formato que pueda leer LDAP le corresponde a un grupo de scripts de migración instalado en el mismo directorio. Usando la Sección 4, “Pluggable Authentication Modules (PAM)” decida cúal script va a ejecutar para poder migrar su base de datos de usuario.

Ejecute el script apropiado basándose en el nombre del servicio actual.

Los archivos `README` y `migration-tools.txt` en el directorio `/usr/share/openldap/migration/` dan más detalles sobre cómo migrar la información.

Nombre del servicio actual	¿Está LDAP ejecutándose?	Utilice este script
`/etc` archivos planos	si	`migrate_all_online.sh`
`/etc` archivos planos	no	`migrate_all_offline.sh`
NetInfo	si	`migrate_all_netinfo_online.sh`
NetInfo	no	`migrate_all_netinfo_offline.sh`
NIS (YP)	si	`migrate_all_nis_online.sh`
NIS (YP)	no	`migrate_all_nis_offline.sh`

Tabla 10.1. Scripts de migración de LDAP

8. Migración de directorios desde versiones anteriores

Con Red Hat Enterprise Linux, OpenLDAP utiliza el sistema Sleepycat Software de Berkeley DB como su formato de almacenamiento en disco para directorios. Las versiones anteriores de OpenLDAP utilizaban el *Administrador de bases de datos GNU* (*gdbm*). Por esta razón, antes de actualizar una implementación LDAP a Red Hat Enterprise Linux 5.0.0, se deberían exportar

los datos LDAP originales antes de la actualización y luego reimportarlos. Esto se puede lograr realizando los pasos siguientes:

1. Antes de actualizar el sistema operativo, ejecute el comando `/usr/sbin/slapcat -l ldif-output`. Esto produce un archivo LDIF llamado *`ldif-output`* que contendrá las entradas del directorio LDAP.
2. Actualice el sistema operativo, teniendo cuidado de no reformatear la partición que contiene el archivo LDIF.
3. Vuelva a importar el directorio LDAP al formato Berkeley DB actualizado ejecutando el comando `/usr/sbin/slapadd -l ldif-output`.

9. Recursos adicionales

Los recursos siguientes ofrecen información adicional sobre LDAP. Por favor revise estas fuentes, especialmente el sitio web de OpenLDAP y la sección HOWTO de LDAP, antes de configurar LDAP en su sistema.

9.1. Documentación instalada

- `/usr/share/docs/openldap-<versionnumber>/` directory — Contiene un documento `README` e información general.
- Páginas man relacionadas con LDAP — Existen varias páginas man para las diferentes aplicaciones y archivos de configuración relacionados con LDAP. La lista siguiento muestra algunas de las páginas man más importantes.

  Aplicaciones cliente

  - `man ldapadd` — Describe cómo añadir entradas a un directorio LDAP.
  - `man ldapdelete` — Describe cómo eliminar entradas dentro de un directorio LDAP.
  - `man ldapmodify` — Describe cómo modificar entradas en un directorio LDAP.
  - `man ldapsearch` — Describe cómo buscar entradas en un directorio LDAP.
  - `man ldappasswd` — Describe cómo configurar o cambiar la contraseña de un usuario LDAP.
  - `man ldapcompare` — Describe como utilizar la herramienta `ldapcompare`.
  - `man ldapwhoami` — Describe como utilizar la herramienta `ldapwhoami`.
  - `man ldapmodrdn` — Describe como modificar los RDNs de entradas.

  Aplicaciones servidor

  - `man slapd` — Describe las opciones de línea de comandos disponibles para un servidor LDAP.

- `man slurpd` — Describe las opciones de línea de comandos disponibles para el servidor de réplicas LDAP.

Aplicaciones administrativas

- `man slapadd` — Describe las opciones de línea de comandos utilizadas para añadir entradas a la base de datos `slapd`.
- `man slapcat` — Describe las opciones de línea de comandos utilizadas para generar un archivo LDIF desde una base de datos `slapd`.
- `man slapindex` — Describe las opciones de línea de comando usadas para regenerar un índice basado en los contenidos de una base de datos `slapd`.
- `man slappasswd` — Describe las opciones de línea de comandos utilizadas para generar contraseñas de usuarios para directorios LDAP.

Archivos de configuración

- `man ldap.conf` — Describe el formato y las opciones disponibles dentro del archivo de configuración para clientes LDAP.
- `man slapd.conf` — Describe el formato y las opciones disponibles dentro del archivo de configuración referenciado por las aplicaciones del servidor LDAP (`slapd` y `slurpd`) y por las herramientas administrativas LDAP (`slapadd`, `slapcat` y `slapindex`).

9.2. Sitios web útiles

- http://www.openldap.org/ [http://www.openldap.org] — Hogar del Proyecto OpenLDAP. Este sitio web contiene una gran variedad de información sobre la configuración de OpenLDAP así como también una guía para los futuros cambios de versiones.
- http://www.padl.com/ [http://www.padl.com] — Desarrolladores de `nss_ldap` y `pam_ldap`, entre otras herramientas útiles de LDAP.
- http://www.kingsmountain.com/ldapRoadmap.shtml — Jeff Hodges' LDAP Road Map contiene enlaces a muchas secciones FAQs de utilidad y a noticias recientes concernientes al protocolo LDAP.
- http://www.ldapman.org/articles/ — Articulos que ofrecen una buena introducción a LDAP, incluyendo métodos para diseñar un árbol y personalizar estructuras de directorios.

9.3. Libros relacionados

- *OpenLDAP by Example* por John Terpstra y Benjamin Coles; Prentice Hall.
- *Implementing LDAP* de Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* por Tim Howes et al.; Macmillan Technical Publishing.

Capítulo 11. Configuración de la autenticación

Cuando un usuario se conecta a un sistema Red Hat Enterprise 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 servidores Hesiod para recuperar información del usuario así como también para configurar LDAP, Kerberos y SMB como protocolos de autenticación.

Nota

Si configuró un nivel de seguridad medio o alto durante la instalación (o con la **Herramienta de configuración del nivel de seguridad**) entonces el cortafuegos no permitirá la autenticación NIS (Servicio de Información de la Red).

Este capítulo no explica cada uno de los diferentes tipos de autenticación en detalle. En vez de eso explica cómo usar la **Herramienta de configuración de autenticación** para configurarlos.

Para iniciar la versión gráfica de la **Herramienta de configuración de autenticación** desde el escritorio, seleccione el System (on the panel) => **Administración** => **Authenticación** o escriba el comando `system-config-authentication` en el intérprete de comandos (por ejemplo en una terminal **XTerm** o **GNOME**).

Importante

Después de salir del programa de autenticación, los cambios tendrán efecto de inmediato.

1. Información del usuario

La pestaña de **Información del Usuario** le permite configurar la manera en que los usuarios deben ser autenticados y tiene varias 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 11.1. Información del usuario

La lista siguiente explica lo que configura cada una de las opciones:

NIS. La opción **Habilitar Soporte NIS** configurar el sistema para conectarse a un servidor NIS (como un cliente 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 está activado, los servicios `portmap` y `ypbind` serán iniciados y también estarán habilitados para arrancar en el momento de inicio del sistema.

LDAP. La opción **Habilitar el soporte LDAP** le ordena al sistema que recupere información del usuario a través de LDAP. Haga click en el botón **Configurar LDAP...** para especificar lo siguiente:

- **DN de Base de Búsqueda LDAP** — Recupera la información del usuario por medio de su nombre distinguido, Distinguished Name (DN).
- **Servidor LDAP** — Especifique la dirección IP del servidor LDAP.
- **Use TLS para encriptar conexiones** — Cuando se encuentra habilidata, se utilizará la Seguridad de la Capa de Transporte para encriptar las contraseñas enviadas al servidor LDAP. La opción **Descargar Certificado AC** le permite especificar una URL desde donde se podrá descargar un *Certificado AC (Autoridad de Certificación)* válido. Un Certificado CA válido tiene que estar en formato PEM (del inglés Correo con Privacidad Mejorada).

Debe tener instalado el paquete `openldap-clients` para que esta opción funcione.

Hesiod. La opción **Habilitar soporte Hesiod** configura el sistema para recuperar información (incluyendo información del usuario) desde una base de datos remota Hesiod. Haga clic en el botón **Configurar Hesiod...** para especificar lo siguiente:

- **Hesiod LHS** — Especifica el prefijo del dominio que se utiliza para consultas Hesiod.
- **Hesiod RHS** — Especifica el dominio Hesiod predeterminado.

El paquete `hesiod` debe estar instalado para que esta opción funcione.

Para obtener más información sobre Hesiod vaya a su página man utilizando el comando `man hesiod`. También se puede referir a la página man `man hesiod`. (`man hesiod.conf`) para obtener más información sobre LHS y RHS.

Winbind. La opción **Habilitar Soporte Winbind** configura el sistema para conectarse a un controlador de dominio Windows o Windows Active Directory. Se puede acceder a la información de los usuarios y configurar las opciones de autenticación del servidor. Haga click en el botón **Configurar Winbind...** para especificar lo siguiente:

- **Dominio Winbind** — Especifica el Windows Active Directory o el controlador de dominio al cual conectarse.
- **Modelo de Seguridad** — le permite seleccionar un modelo de seguridad, el cual configura la manera en que los clientes deben responder a Samba. La lista desplegable le permite seleccionar cualquiera de los siguientes:
  - **usuario** — Este es el modo predeterminado. Con este nivel de seguridad, el cliente debe iniciar la sesión con una nombre de usuario y una contraseña válidas. Este modo de seguridad también permite el uso de contraseñas encriptadas.
  - **server** — En este modo, Samba tratará de validar el nombre de usuario/contraseña autenticándolos a través de otro servidor SMB (por ejemplo, un Servidor Windows NT). Si no tiene exito tendrá efecto el modo **user**.
  - **domain** — En este modo Samba intentará validar el nombre de usuario/contraseña autenticándolos a través de Windows NT Primary o un Controlador de Dominio de Respaldo (Backup Domain Controller) de manera similar a lo que haría un Servidor Windows NT.

  - **ads** — Este modo le ordena a Samba que se comporte como un miembro de dominio en un Active Directory Server (ADS). Para operar de este modo necesita tener instalado el paquete `krb5-server` y Kerberos debe estar configurado apropiadamente.

- **Winbind ADS Realm** — cuando se selecciona el Modelo de Seguridad **ads**, esto le permite especificar el Dominio ADS en el que el servidor Samba debe desempeñarse como un miembro de dominio.

- **Template Shell** — Cuando llene la información del usuario para un usuario de Windows NT, el demonio `winbindd` utiliza el valor seleccionado aquí para especificar el shell de registro para ese usuario.

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.

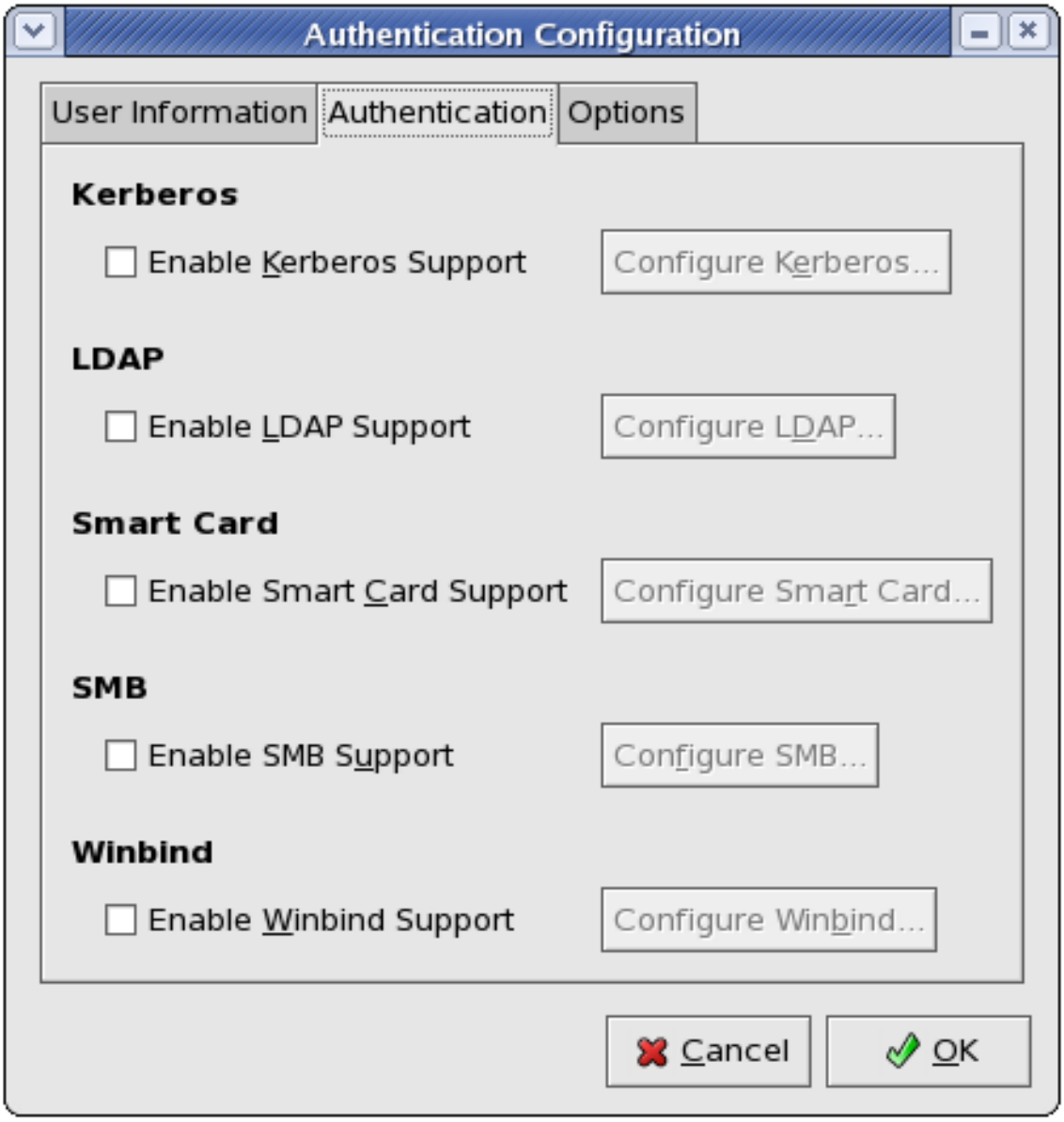


Figura 11.2. Autenticación

A continuación se explica lo que configura cada opción:

Kerberos. La opción **Habilitar el Soporte de Kerberos** habilita la autenticación de Kerberos. Haga click en **Configurar Kerberos...** para abrir el diálogo **Configuración de Kerberos Settings** para configurar:

- **Entorno** — Configure el entorno para el servidor de Kerberos. El entorno o reino es la red que Kerberos utiliza, 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 de Kerberos.

- **Servidores de Administración** — Especifica el o los servidores de administración ejecutando `kadmind`.

El diálogo **Configuración de Kerberos** también le permite utilizar DNS para resolver hosts en entornos y localizar KDCs para entornos.

LDAP. La opción **Habilitar el soporte LDAP** le ordena a las aplicaciones estándares PAM habilitadas para que utilicen LDAP para la autenticación. El botón **Configurar LDAP...** le permite configurar el soporte LDAP con opciones identicas a aquellas que se encuentran en **Configurar LDAP...** bajo la pestaña **Information de Usuario**. Para obtner mayor información sobre estas opciones vaya a Sección 1, “Información del usuario”.

Debe tener instalado el paquete `openldap-clients` para que esta opción funcione.

Tarjeta Inteligente. La opción **Habilitar el soporte SMB** habilita la autenticación por medio de tarjetas inteligentes. Esto permite que los usuarios inicien sesión utilizando un certificado y una llave asociada alamacenados en una tarjeta inteligente. Haga click en el botón **Configurar SMB** para ver más opciones.

SMB. La opción **Habilitar el soporte SMB** configura PAM para utilizar un servidor SMB para autentificar a los usuarios. SMB se refiere a un protocolo del servidor del cliente utilizado para la comunicación entre sistemas y Samba también lo utiliza para parecer como un servidor Windows para los clientes Windows. Haga click en el botón **Configurar SMB** para especificar:

- **Grupo de trabajo** — Especifica el grupo de trabajo SMB a utilizar.
- **Controladores de Dominio** — Especifica los controladores de dominio SMB a utilizar.

Winbind. La opción **Habilitar el soporte Winbind** configura la conexión del sistema con Windows Active Directory o con un controlador de dominios de Windows. Se puede acceder a la información de los usuarios y configurar las opciones de autenticación del servidor.

Las opciones **Configurar Winbind...** son idénticas a las del botón **Configurar Winbind...** en la pestaña **Información de Usuario**. Para obtener mayor información vaya a Winbind (bajo Sección 1, “Información del usuario”).

3. Options

Esta pestaña contiene otras opciones para configuración:

Figura 11.3. Opciones

Información del Usuario de la Caché. 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. Para obtener más detalles sobre `nscd` vaya a su página man utilizando el comando `man nscd`.

Utilice 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.

Utilice Contraseñas MD5. Seleccione esta opción para habilitar las contraseñas MD5, lo cual permite que las contraseñas tengan hasta 256 en vez de 8 o menos. Esta opción es seleccionada por defecto durante la instalación y se recomienda su uso para mayor seguridad.

Authorization local es suficiente para usuarios locales. Cuano esta opción se encuentra habilitada, el sistema no verificará la autorización desde los servicios de red (tal como LDAP o Kerberos) para las cuentas de usuarios mantenidas en su archivo `/etc/passwd`.

Autenticar cuentas del sistema por medio de servicios de red. Al habilitar esta opción se configura el sistema para permitir servicios de red (tal como LDAP o Kerberos) para autenticar cuentas del sistema (incluído root) en la máquina.

4. 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 11.1, “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.

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

Opción	Descripción
`--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
`--enablekrb5kdcdns`	Habilitar el uso de DNS para encontrar Kerberos KDCs
`--disablekrb5kdcdns`	Deshabilitar el uso de DNS para encontrar Kerberos KDCs
`--enablekrb5realmdns`	Habilitar el uso de DNS para encontrar Kerberos realms
`--disablekrb5realmdns`	Deshabilitar el uso de DNS para encontrar Kerberos realms
`--enablesmbauth`	Habilita SMB
`--disablesmbauth`	Inhabilita SMB
`--smbworkgroup=<workgroup>`	Specify SMB workgroup
`--smbservers=<server>`	Especifica servidores SMB
`--enablewinbind`	Habilitar winbind para la información del usuario por defecto
`--disablewinbind`	Inhabilitar winbind para información del usuario por defecto
`--enablewinbindauth`	Habilitar winbindauth para la autenticación por defecto
`--disablewinbindauth`	Inhabilitar winbindauth para la autenticación por defecto
`--smbsecurity=<user|server|domain|ads>`	Modos de seguridad para usar Samba y windbind
`--smbrealm=<STRING>`	Campo por defecto para Samba y winbind cuando `security=ads`
`--smbidmapuid=<lowest-highest>`	Rango UID que winbind asigna al dominio o usuario ADS
`--smbidmapgid=<lowest-highest>`	Rango GID que winbind asigna al

Opción	Descripción
	dominio o usuario ADS
`--winbindseparator=<\>`	Caracter usado para separar la parte del usuario y del dominio de los nombres de usuario de winbind si `winbindusedefaultdomain` no está habilitado
`--winbindtemplatehomedir=</home/%D/%U>`	Directorio de inicio de los usuarios winbind
`--winbindtemplateprimarygroup=<nobody>`	Grupo primario de los usuarios winbind
`--winbindtemplateshell=</bin/false>`	Shell por defecto de los usuarios winbind
`--enablewinbindusedefaultdomain`	Configurar winbind para asumir que los usuarios sin dominio en sus nombres de usuarios son usuarios con dominio
`--disablewinbindusedefaultdomain`	Configurar winbind para asumir que los usuarios sin dominio en sus nombres de usuarios son usuarios sin dominio
`--winbindjoin=<Administrator>`	Unir el dominio winbind o campo ADS como este administrador
`--enablewins`	Habilitar WINS para la resolución del nombre de host
`--disablewins`	Inhabilitar WINS para la resolución del nombre de host
`--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 11.1. Opciones de línea de comandos

Parte II. Configuración del sistema

Parte del trabajo de un administrador de sistemas es configurar el sistema para varias tareas, tipos de usuarios y configuraciones de hardware. Esta sección explica cómo configurar un sistema Red Hat Enterprise Linux.

Capítulo 12. El directorio `sysconfig`

El directorio `/etc/sysconfig/` contiene una gran variedad de archivos de configuración para Red Hat Enterprise Linux.

Este capítulo resalta algunos de los archivos encontrados en el directorio `/etc/sysconfig/`, su función, y sus contenidos. La información en este capítulo no pretende ser exhaustiva, pues muchos de estos archivos tienen una variedad de opciones que sólo son usadas en circunstancias muy específicas.

1. Archivos en el directorio `/etc/sysconfig/`

Las secciones siguientes ofrecen descripciones de los archivos que normalmente se encuentran en el directorio `/etc/sysconfig/`. Los archivos que no se listan aquí, así como las opciones adicionales para los archivos, se pueden encontrar en el archivo `/usr/share/doc/initscripts-<número-versión>/sysconfig.txt` (reemplace `<número-versión>` con la versión del paquete `initscripts`). Alternativamente, puede ser útil revisar los initscripts en el directorio `/etc/rc.d/`.

Nota

Si alguno de los archivos aquí listados no está presente en el directorio `/etc/sysconfig/`, entonces el programa correspondiente podría no estar instalado.

1.1. `/etc/sysconfig/amd`

El archivo `/etc/sysconfig/amd` contiene varios parámetros usados por `amd`, que permiten el montaje y desmontaje automático de sistemas de archivos.

1.2. `/etc/sysconfig/apmd`

El archivo `/etc/sysconfig/apmd` es usado por `apmd` para configurar que valores de energía iniciar/detener/cambiar en el estado suspendido o reanudar. Este archivo configura como funciona `apmd` al momento del arranque, dependiendo de si el hardware soporta la *Administración avanzada de energía* (*Advanced Power Management*, *APM*), o si el usuario ha configurado o no el sistema para usarla. El demonio `apm` es un programa de supervisión que funciona con el código de administración de energía dentro del kernel de Linux. Es capaz de alertar a los usuarios sobre la condición de energía baja en la batería en las computadoras portátiles y otras configuraciones relacionadas con la energía del sistema.

1.3. `/etc/sysconfig/arpwatch`

El archivo `/etc/sysconfig/arpwatch` es usado para pasar argumentos al demonio `arpwatch` durante el arranque. El demonio `arpwatch` mantiene una tabla de direcciones MAC Ethernet y sus direcciones pares IP. Por defecto, este archivo coloca como propietario del proceso `arpwatch` al

usuario `pcap`, así como también envía todos los mensajes a la cola de mensajes de `root`. Para obtener mayor información sobre los parámetros disponibles para este archivo, vea la página man de `arpwatch`.

1.4. `/etc/sysconfig/authconfig`

El archivo `/etc/sysconfig/authconfig` configura el tipo de autorización a ser usada en el host. Contiene una o más de las líneas siguientes:

- `USEMD5=<valor>`, donde `<valor>` es uno de los siguientes:
  - `yes` — Se utiliza MD5 para la autentificación.
  - `no` — No se utiliza MD5 para la autentificación.
- `USEKERBEROS=<valor>`, donde `<valor>` es uno de los siguientes:
  - `yes` — Se utiliza Kerberos para la autentificación.
  - `no` — No se utiliza Kerberos para la autentificación.
- `USELDAPAUTH=<valor>`, donde `<valor>` es uno de los siguientes:
  - `yes` — Se utiliza LDAP para la autentificación.
  - `no` — No se usa LDAP para la autentificación.

1.5. `/etc/sysconfig/autofs`

El archivo `/etc/sysconfig/autofs` define opciones de personalización para el montaje automático de dispositivos. Este archivo controla la operación de los demonios de automontaje, los cuales montan automáticamente los sistemas de archivos cuando los utiliza y los desmonta luego de un período de inactividad. Los sistemas de archivos pueden incluir sistemas de archivos de redes, CD-ROMS, disquetes y otros tipos de media.

El archivo `/etc/sysconfig/autofs` puede contener lo siguiente:

- `LOCALOPTIONS="<valor>"`, donde `<valor>` es una cadena de caracteres que especifica reglas de montaje. El valor por defecto es una cadena de caracteres vacía (`""`).
- `DAEMONOPTIONS="<valor>"`, donde `<valor>` es la duración del tiempo de espera en segundos antes de desmontar el dispositivo. El valor por defecto es 60 segundos (`"--timeout=60"`).
- `UNDERSCORETODOT=<valor>`, donde `<valor>` es un valor binario que controla si se deben convertir los guiones bajos en los nombres de archivos en puntos. Por ejemplo, `auto_home` a `auto.home` y `auto_mnt` a `auto.mnt`. El valor por defecto es 1 (verdadero).
- `DISABLE_DIRECT=<valor>`, donde `<valor>` es un valor binario que controla si se desactiva o no el soporte para el montaje directo, ya que la implementación de Linux no sigue el comportamiento de automontaje de Sun Microsystems. El valor por defecto es 1 (verdadero), que permite la compatibilidad con la sintaxis de especificación de opciones de automontaje de

Sun.

1.6. /etc/sysconfig/clock

El archivo `/etc/sysconfig/clock` controla la interpretación de los valores leídos desde el reloj del sistema.

Los valores correctos son:

- `UTC=<valor>`, donde `<valor>` es uno de los siguientes valores boleanos:
  - `true` o `yes` — El reloj del hardware está configurado a Universal Time.
  - `false` o `no` — El reloj del hardware está configurado a la hora local.
- `ARC=<valor>`, donde `<valor>` es uno de los siguientes:
  - `false` o `no` — Este valor indica que la época UNIX normal está en uso. Otros valores son usados por sistemas no soportados por Red Hat Enterprise Linux.
- `SRM=<valor>`, donde `<valor>` es uno de los siguientes:
  - `false` o `no` — Este valor indica que la época UNIX normal está en uso. Otros valores son usados por sistemas no soportados por Red Hat Enterprise Linux.
- `ZONE=<nombre-archivo>` — El archivo de zona horaria bajo `/usr/share/zoneinfo` del cual `/etc/localtime` es una copia. El archivo contiene información tal como:

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

  Note que el parámetro `ZONE` es leído por **Herramienta de propiedades de fecha y hora** (`system-config-date`), y la edición manual de éste no cambia el huso horario del sistema.

Ediciones previas de Red Hat Enterprise Linux usaban los valores siguientes (las cuales ya no son aprobadas):

- `CLOCKMODE=<valor>`, donde `<valor>` es uno de los siguientes:
  - `GMT` — El reloj está colocado al Universal Time (Greenwich Mean Time).
  - `ARC` — El desplazamiento (time offset) de 42 años de la consola ARC está en efecto (sólo para sistemas basados en Alpha).

1.7. /etc/sysconfig/desktop

El archivo `/etc/sysconfig/desktop` especifica el escritorio para los nuevos usuarios y el gestor de pantallas a ser ejecutado, cuando se entra al nivel de ejecución 5.

Los valores correctos son:

- `DESKTOP="<valor>"`, donde `"<valor>"` es uno de los siguientes:
  - `GNOME` — Selecciona el entorno de escritorio de **GNOME**.
  - `KDE` — Selecciona el entorno de escritorio **KDE**.
- `DISPLAYMANAGER="<valor>"`, donde `"<valor>"` es uno de los siguientes:
  - `GNOME` — Selecciona el **gestor de pantallas de GNOME**.
  - `KDE` — Selecciona el **gestor de pantallas de KDE**.
  - `XDM` — Selecciona el **gestor de pantallas de X**.

Para obtener mayor información, consulte el Capítulo 15, *El Sistema X Window*.

1.8. `/etc/sysconfig/dhcpd`

El archivo `/etc/sysconfig/dhcpd` es usado para pasar argumentos al demonio `dhcpd` en el momento de arranque. El demonio `dhcpd` implementa el Protocolo dinámico de configuración de host (DHCP) y el Internet Bootstrap Protocol (BOOTP). DHCP y BOOTP asignan nombres de host a las máquinas en la red. Para más información sobre qué parámetros están disponibles en este archivo, consulte la página del manual de `dhcpd`.

1.9. `/etc/sysconfig/exim`

El archivo `/etc/sysconfig/exim` permite enviar mensajes a uno o más clientes, enrutando el mensaje sobre todas las redes que sean necesarias. El archivo configura los valores predeterminados para que la aplicación exim se ejecute. Sus valores por defecto son configurados para ejecutarse como un demonio en el fondo y verificar su cola una vez cada hora en caso de que algo se haya acumulado.

Los valores incluidos son:

- `DAEMON=<valor>`, donde `<valor>` es uno de los siguientes:
  - `yes` — `exim` debería ser configurado para escuchar en el puerto 25 para el correo entrante. `yes` implica el uso de las opciones `-bd` de Exim.
  - `no` — `exim` no debería ser configurado para escuchar en el puerto 25 para el correo entrante.
- `QUEUE=1h` que se entrega a `exim` como `-q$QUEUE`. La opción `-q` no es dada a `exim` si `/etc/sysconfig/exim` existe y `QUEUE` es vacío o no está definida.

1.10. `/etc/sysconfig/firstboot`

La primera vez que el sistema arranca, el programa `/sbin/init` llama al script `etc/rc.d/init.d/firstboot` que luego lanza **Agente de configuración**. Esta aplicación permite al usuario instalar las últimas actualizaciones y cualquier aplicación o documentación adicional.

El archivo `/etc/sysconfig/firstboot` le dice a la aplicación **Agente de configuración** que no se ejecute en los subsecuentes reinicios. Para ejecutarlo la próxima vez que el sistema arranca, elimine `/etc/sysconfig/firstboot` y ejecute `chkconfig --level 5 firstboot on`.

1.11. /etc/sysconfig/gpm

El archivo `/etc/sysconfig/gpm` es usado para pasar argumentos al demonio `gpm` en el momento de arranque. El demonio `gpm` es el servidor del ratón que permite la aceleración del ratón y el pegado con el botón del medio. Para más información sobre qué parámetros están disponibles para este archivo, consulte la página del manual de `gpm`. Por defecto, la directriz `DEVICE` se configura a `/dev/input/mice`.

1.12. /etc/sysconfig/hwconf

El archivo `/etc/sysconfig/hwconf` lista todo el hardware que `kudzu` detectó en su sistema, así como también los controladores usados, ID de los fabricantes e información de ID de los dispositivos. El programa `kudzu` detecta y configura el hardware nuevo o modificado en su sistema. El archivo `/etc/sysconfig/hwconf` se supone que no es para ser modificado manualmente. Si se edita, los dispositivos se pueden repentinamente mostrar como que han sido agregados o eliminados.

1.13. /etc/sysconfig/i18n

El archivo `/etc/sysconfig/i18n` configura el idioma predeterminado, cualquier idioma soportado y la fuente predeterminada del sistema. Por ejemplo:

```
LANG="en_US.UTF-8"
SUPPORTED="en_US.UTF-8:en_US:en"
SYSFONT="latarcyrheb-sun16"
```

1.14. /etc/sysconfig/init

El archivo `/etc/sysconfig/init` controla cómo el sistema aparecerá y funcionará durante el momento de arranque.

Se usan los siguientes valores:

- `BOOTUP=<valor>`, donde `<valor>` es uno de los siguientes:
  - `color` — El color estándar de la visualización, cuando la falla o éxito de un dispositivo se muestra en colores diferentes al momento de arranque, donde el éxito o falla de dispositivos y servicios al iniciarse es mostrado en diferentes colores.
  - `verbose` — Es un tipo de despliegue viejo, que proporciona más información que el simple mensaje de éxito o falla.
  - Cualquier otra cosa significa un nuevo despliegue, pero sin el formato ANSI.
- `RES_COL=<valor>`, donde `<valor>` es el número de la columna de la pantalla para comenzar las etiquetas de estado. Está predeterminado a 60.

- `MOVE_TO_COL=<valor>`, donde `<valor>` mueve el cursor al valor en la línea `RES_COL` a través del comando `echo -en`.
- `SETCOLOR_SUCCESS=<valor>`, donde `<valor>` configura el color a un color que indica el éxito a través del comando `echo -en`. El color predeterminado es verde.
- `SETCOLOR_FAILURE=<valor>`, donde `<valor>` coloca el color para indicar falla a través del comando `echo -en`. Por defecto el color es rojo.
- `SETCOLOR_WARNING=<valor>`, donde `<valor>` coloca el color para indicar advertencia a través del comando `echo -en`. Por defecto el color es amarillo.
- `SETCOLOR_NORMAL=<valor>`, donde `<valor>` reconfigura el color a "normal" a través de `echo -en`.
- `LOGLEVEL=<valor>`, donde `<valor>` configura el nivel de conexión de la consola inicial para el kernel. El valor por defecto es 3; 8 significa cualquier cosa (incluyendo depuración); 1 significa pánico del kernel. El demonio `syslogd` ignora esta configuración una vez que se ha arrancado.
- `PROMPT=<valor>`, donde `<valor>` es uno de los siguientes valores boleanos:
  - `yes` — Activa la verificación de claves para el modo interactivo.
  - `no` — Desactiva la verificación de claves para el modo interactivo.

1.15. /etc/sysconfig/ip6tables-config

El archivo `/etc/sysconfig/ip6tables-config` guarda información usada por el kernel para configurar los servicios de filtrado de paquetes IPv6 en el momento de arranque o cuando se arranque el servicio `ip6tables`.

No modifique este archivo manualmente a menos que esté familiarizado con la construcción de reglas `ip6tables`. Se pueden crear reglas manualmente también usando el comando `/sbin/ip6tables`. Una vez creado, añada las reglas al archivo `/etc/sysconfig/ip6tables` escribiendo el comando siguiente:

```
/sbin/service ip6tables save
```

Una vez que este archivo existe, cualquier regla de firewall guardadas en él, persisten a través de los reinicios del sistema o de un servicio.

1.16. /etc/sysconfig/iptables-config

El archivo `/etc/sysconfig/iptables-config` guarda información usada por el kernel para configurar los servicios de filtrado de paquetes en el momento de arranque o cuando se arranque un servicio.

No modifique este archivo manualmente a menos que esté familiarizado con la forma de construir reglas `iptables`. La forma más fácil de agregar reglas es usando la **Herramienta de configuración del nivel de seguridad** (`system-config-selinux`) para crear un cortafuegos. Esta aplicación automáticamente edita este archivo al final del proceso.

Las reglas también se pueden crear manualmente usando `/sbin/iptables`. Una vez creadas, añada la(s) regla(s) al archivo `/etc/sysconfig/iptables` escribiendo el comando siguiente:

```
/sbin/service iptables save
```

Una vez que este archivo existe, cualquier regla de firewall guardadas en él, persisten a través de los reinicios del sistema o de un servicio.

1.17. `/etc/sysconfig/irda`

El archivo `/etc/sysconfig/irda` controla cómo los dispositivos infrarojos en el sistema son configurados en el arranque.

Se usan los siguientes valores:

- `IRDA=<valor>`, donde `<valor>` es uno de los siguientes valores boleanos:
  - `yes` — `irattach` se ejecutará, lo que verifica periódicamente si hay algo tratando de conectarse al puerto infrarojo, tal como otra laptop tratando de hacer una conexión de red. Para que los dispositivos infrarojos funcionen en su sistema, se debe colocar esta línea a `yes`.
  - `no` — `irattach` no se ejecuta, impidiendo la comunicación de dispositivos infrarojos.
- `DEVICE=<valor>`, donde `<valor>` es el dispositivo (usualmente un puerto serial) que maneja las conexiones infrarojas. Un ejemplo de entrada de dispositivo serial podría ser `/dev/ttyS2`.
- `DONGLE=<valor>`, donde `<valor>` especifica el tipo de "dongle" que está siendo usado para la comunicación infraroja. Este valor existe para los casos en que se usan dongles seriales en vez de puertos infrarojos reales. Un dongle es un dispositivo que es conectado a un puerto serial tradicional para comunicar a través de infrarojo. Esta línea se coloca en comentarios por defecto porque las computadoras portátiles con puertos infrarojos reales son mucho más populares que las que tienen dongles agregados. Una entrada de ejemplo para dongle podría ser `actisys+`.
- `DISCOVERY=<valor>`, donde `<valor>` es uno de los siguientes valores boleanos:
  - `yes` — Arranca `irattach` en modo 'discovery', o de descubrimiento, lo que significa que está activamente buscando otros dispositivos infrarojos. Este valor necesita ser activado para que la máquina esté buscando activamente por una conexión infraroja (el par que no inicia la conexión).
  - `no` — No arranca `irattach` en modo discovery.

1.18. `/etc/sysconfig/keyboard`

El archivo `/etc/sysconfig/keyboard` controla el comportamiento del teclado. Se pueden usar los siguientes valores:

- `KEYBOARDTYPE="sun|pc"`, donde `sun` significa que un teclado Sun está conectado en `/dev/kbd`,

o `pc` significa que hay un teclado PS/2 conectado al puerto PS/2.

- `KEYTABLE="<archivo>"`, donde `<archivo>` es el nombre de un archivo de tabla de teclas.

  Por ejemplo: `KEYTABLE="us"`. Los archivos que pueden ser usados como tabla de teclas comienzan en `/lib/kbd/keymaps/i386` y se extienden en diferentes disposiciones de teclados desde aquí, a todos los etiquetados `<archivo>.kmap.gz`. El primer archivo encontrado debajo `/lib/kbd/keymaps/i386` que coincide con la configuración `KEYTABLE` es usado.

1.19. /etc/sysconfig/kudzu

El archivo `/etc/sysconfig/kuzdu` dispara una exploración segura del hardware del sistema mediante `kudzu` en el momento de arranque. time. Una exploración segura es una que desactiva el sondeo del puerto serial.

- `SAFE=<valor>`, donde `<valor>` es uno de los siguientes:

  - `yes` — `kuzdu` hace una exploración segura.
  - `no` — `kuzdu` realiza una exploración normal.

1.20. /etc/sysconfig/named

El archivo `/etc/sysconfig/named` es usado para pasar argumentos al demonio `named` en el momento de arranque. El demonio `named` es un servidor *Domain Name System* (*DNS*) que implementa la distribución *Berkeley Internet Name Domain* (*BIND*) versión 9. Este servidor mantiene una tabla de cuales hosts están asociados con direcciones IP en la red.

Actualmente, sólo los valores siguientes son usados:

- `ROOTDIR="</algun/lugar>"`, donde `</algun/lugar>` se refiere a la ruta completa del directorio de un ambiente chroot bajo el cual `named` se ejecuta. Este ambiente chroot debe ser configurado primero. Escriba `info chroot` para ver más información.
- `OPTIONS="<valor>"`, donde `<valor>` es cualquier opción listada en la página del manual para `named` excepto `-t`. En lugar de `-t`, use la línea `ROOTDIR`.

Para obtener mayor información sobre los parámetros disponibles para este archivo, consulte la página man de `named`. Para obtener información detallada sobre cómo configurar un servidor BIND DNS, vea el Capítulo 4, *Berkeley Internet Name Domain (BIND)*. Por defecto, el archivo no contiene parámetros.

1.21. /etc/sysconfig/netdump

El archivo `/etc/sysconfig/netdump` es el archivo de configuración para el servicio `/etc/init.d/netdump`. El servicio `netdump` envía ambos datos oops y escombros de memoria sobre la red. En general, `netdump` no es un servicio requerido; sólo ejecútelo si es absolutamente necesario. Para más información sobre los parámetros disponibles para este archivo, consulte la página del manual de `netdump`.

1.22. /etc/sysconfig/network

El archivo `/etc/sysconfig/network` es usado para especificar información sobre la configuración de red deseada. Se pueden usar los valores siguientes:

- `NETWORKING=<valor>`, donde `<valor>` es uno de los siguientes valores boleanos:
  - `yes` — Se debería configurar el servicio de red.
  - `no` — No se debería configurar el servicio de red.
- `HOSTNAME=<valor>`, donde `<valor>` debería ser el *Fully Qualified Domain Name* (*FQDN*), nombre de dominio cualificado completo, tal como `hostname.expample.com`, pero puede ser cualquier nombre de host necesario.
- `GATEWAY=<valor>`, donde `<valor>` es la dirección IP de la gateway (compuerta) de la red.
- `GATEWAYDEV=<valor>`, donde `<valor>` es el dispositivo gateway, tal como `eth0`.
- `NISDOMAIN=<valor>`, donde `<valor>` es el nombre del dominio NIS.

1.23. /etc/sysconfig/ntpd

El archivo `/etc/sysconfig/ntpd` es usado para pasar argumentos al demonio `ntpd` en el momento de arranque. El demonio `ntpd` configura y mantiene el reloj del sistema para sincronizar con un servidor de hora estándar de Internet. Implementa la versión 4 del protocolo de hora de red (Network Time Protocol, NTP). Para más información sobre los parámetros disponibles para este archivo, apunte su navegador al siguiente archivo: `/usr/share/doc/ntp-<version>/ntpd.htm` (donde `<version>` es el número de versión de `ntpd`). Por defecto, este archivo configura el propietario del proceso `ntpd` al usuario de `ntp`.

1.24. /etc/sysconfig/radvd

El archivo `/etc/sysconfig/radvd` es usado para pasar argumentos al demonio `radvd` en el momento de arranque. El demonio `radvd` escucha por peticiones del enrutador y envía notificaciones del enrutador para el protocolo IP versión 6. Este servicio permite a los host en una red cambiar dinámicamente sus enrutadores predeterminados basados en estas notificaciones del enrutador. Para más información sobre qué parámetros están disponibles para este archivo, vea la página del manual de `radvd`. Por defecto, este archivo coloca como propietario del proceso `radvd` al usuario `radvd`.

1.25. /etc/sysconfig/samba

El archivo `/etc/sysconfig/samba` es usado para pasar argumentos a los demonios `smbd` y `nmbd` en el momento de arranque. El demonio `smbd` ofrece conectividad de archivos compartidos para los clientes Windows en la red. El demonio `nmbd` ofrece servicios de nombres NetBIOS sobre IP. Para más información sobre los parámetros disponibles para este archivo, consulte la página de manual de `smbd`. Por defecto este archivo configura `smbd` y `nmbd` para que se ejecuten en modo demonio.

1.26. /etc/sysconfig/selinux

El archivo `/etc/sysconfig/selinux` contiene las opciones de configuración básicas para SELinux. Este archivo es un enlace simbólico a `/etc/selinux/config`.

1.27. /etc/sysconfig/sendmail

El archivo `/etc/sysconfig/sendmail` permite enviar mensajes a uno o más clientes, enrutando el mensaje sobre todas las redes que sean necesarias. El archivo configura los valores predeterminados para que la aplicación **Sendmail** se ejecute. Los valores predeterminados son ejecutarse como un demonio en el fondo y verificar la cola una vez cada hora en caso de que algo se haya acumulado.

Los valores incluyen:

- `DAEMON=<valor>`, donde `<valor>` es uno de los siguientes:
  - `yes` — **Sendmail** debería ser configurado para escuchar en el puerto 25 para el correo entrante. `yes` implica el uso de las opciones `-bd` de **Sendmail** .
  - `no` — **Sendmail** no debería ser configurado para escuchar en el puerto 25 para el correo entrante.
- `QUEUE=1h` que es entregado a **Sendmail** como `-q$QUEUE`. La opción `-q` no es dada a **Sendmail** si `/etc/sysconfig/sendmail` existe y `QUEUE` es vacío o no está definida.

1.28. /etc/sysconfig/spamassassin

El archivo `/etc/sysconfig/spamassassin` se utiliza para pasar argumentos al demonio `spamd` (una versión endemoniada de **Spamassassin**) al momento del arranque. **Spamassassin** es una aplicación de filtro de correo basura. Para obtener una lista de las opciones disponibles, consulte la página man de `spamd`. Por defecto, se configura `spamd` para ejecutarse en modo demonio, crear las preferencias del usuario y autocrear whitelists (permitir remitentes con envíos por montones).

Para obtener mayor información sobre **Spamassassin**, consulte la Sección 5.2.6, “Filtros de correo basura”.

1.29. /etc/sysconfig/squid

El archivo `/etc/sysconfig/squid` es usado para pasar argumentos al demonio `squid` al momento de arranque. El demonio `squid` es un servidor proxy caching para las aplicaciones cliente Web. Para más información sobre cómo configurar un servidor proxy `squid`, use un navegador Web para abrir el directorio `/usr/share/doc/squid-<version>/` (reemplace `<version>` con el número de la versión de `squid` instalado en su sistema). Por defecto, este archivo configura `squid` para arrancar en modo demonio y establecer la cantidad de tiempo antes de que se cierre asímismo.

1.30. /etc/sysconfig/system-config-selinux

1.31. /etc/sysconfig/system-config-users

El archivo `/etc/sysconfig/system-config-users` es el archivo de configuración para la **Administrador de usuarios**. Este archivo es usado para filtrar usuarios del sistema tal como `root`, `daemon` o `lp`. Este archivo se edita mediante el menú desplegable **Preferencias** => **Filtrar usuarios y grupos del sistema** en la **Administrador de usuarios** y nunca se debería modificar manualmente. Para obtener mayor información sobre el uso de esta aplicación, consulte la Sección 1, “Configuración de grupos y de usuarios”

1.32. /etc/sysconfig/system-logviewer

El archivo `/etc/sysconfig/system-logviewer` es el archivo de configuración para la aplicación gráfica interactiva de visualización del registro, **Visor de registros**. Este archivo se puede modificar mediante el menú desplegable **Editar** => **Preferencias** en la **Visor de registros** y no debería ser modificado manualmente. Para obtener mayor información sobre el uso de esta aplicación, consulte el Capítulo 19, *Archivos de registro*.

1.33. /etc/sysconfig/tux

El archivo `/etc/sysconfig/tux` es el archivo de configuración para el Acelerador de contenidos de Red Hat, en inglés Red Hat Content Accelerator (anteriormente conocido como **TUX**), el servidor Web basado en el kernel. Para obtener mayor información sobre la configuración de Red Hat Content Accelerator, use un navegador de Web para abrir `/usr/share/doc/tux-<versión>/tux/index.html` (reemplace `<versión>` con el número de versión de TUX instalado en su sistema). Los parámetros disponibles para este archivo están listados en `/usr/share/doc/tux-<versión>/tux/parameters.html`.

1.34. /etc/sysconfig/vncservers

El archivo `/etc/sysconfig/vncservers` configura la forma en que el servidor *Virtual Network Computing* (*VNC*) arranca.

VNC es un sistema de despliegue remoto el cual permite a los usuarios ver el ambiente de escritorio no sólo en la máquina en que se está ejecutando sino también a través de las diferentes redes en una variedad de arquitecturas.

Puede contener lo siguiente:

- `VNCSERVERS=<valor>`, donde `<valor>` está configurado a algo parecido a `"1:fred"`, para indicar que el servidor VNC debería ser arrancado por el usuario fred en el despliegue :1. El usuario fred debe haber establecido una contraseña VNC usando el comando `vncpasswd` antes de intentar conectarse al servidor VNC remoto.

2. Directorios en el directorio /etc/sysconfig/

Los siguientes directorios se encuentran normalmente en `/etc/sysconfig/`.

`apm-scripts/`
: Este directorio contiene el script para suspender/reanudar APM de Red Hat. No modifique

estos archivos directamente. Si se necesita personalizar APM, cree un archivo llamado `/etc/sysconfig/apm-scripts/apmcontinue`. Este será ejecutado al final del script. También es posible controlar el script editando `/etc/sysconfig/apmd`.

`cbq/`
Este directorio contiene los archivos de configuración necesarios para hacer *Class Based Queuing* para la administración del ancho de banda en las interfaces de red. CBQ divide el tráfico en una jerarquía de clases basada en cualquier combinación de direcciones IP, protocolos y tipos de aplicación.

`networking/`
Este directorio es usado por la **Herramienta de administración de red** (`system-config-network`) y sus contenidos no se deberían modificar manualmente. Para obtener mayor información sobre la configuración de interfaces de red usando la **Herramienta de administración de red**, consulte el Capítulo 2, *Configuración de la red*.

`network-scripts/`
Este directorio contiene los siguientes archivos de configuración relacionados con la red:

- Archivos de configuración de red para cada interfaz de red configurada, tal como `ifcfg-eth0` para la interfaz de red Ethernet `eth0`.
- Scripts usado para activar y desactivar interfaces de red, tales como `ifup` e `ifdown`.
- Scripts usados para activar y desactivar las interfaces ISDN, tales como `ifup-isdn` e `ifdown-isdn`.
- Varios scripts de funciones de red compartidas los cuales no deberían ser modificados manualmente.

Para obtener mayor información sobre el directorio `network-scripts`, consulte el Capítulo 1, *Interfaces de red*.

`rhn/`
Este directorio contiene los archivos de configuración y claves GPG para Red Hat Network. Ningún archivo en este directorio debería ser modificado manualmente. Para obtener mayor información sobre Red Hat Network, consulte el sitio web de Red Hat Network en https://rhn.redhat.com/.

3. Recursos adicionales

Este capítulo sólo tiene la intención de servir de introducción para los archivos en el directorio `/etc/sysconfig/`. Las siguientes fuentes contienen información más detallada.

3.1. Documentación instalada

- `/usr/share/doc/initscripts-<numero-version>/sysconfig.txt` — Este archivo contiene un listado autorizado de los archivos encontrados en el directorio `/etc/sysconfig/` y de las opciones de configuración disponibles para ellos. El `<numero-version>` en la ruta a este archivo corresponde a la versión del paquete `initscripts` instalado.

Capítulo 13. Configuración de la fecha y hora

La **Herramienta de propiedades de fecha y hora** le permite al usuario cambiar la fecha y la hora del sistema para configurar la zona horaria utilizada en el sistema. Además le permite definir el demonio NTP (Network Time Protocol) para sincronizar el reloj del sistema con un servidor horario.

Para utilizar esta herramienta, usted debe tener privilegios de root y debe estar utilizando el sistema de ventanas **X**. Hay tres maneras para iniciar la aplicación.

- Desde el escritorio, vaya a Applications (the main menu on the panel) => **Configuración del sistema** => **Fecha & Hora**
- Desde el escritorio, haga clic con el botón derecho del ratón sobre la fecha y seleccione **Ajustar fecha y hora**.
- Escriba el comando `system-config-date`, `system-config-time`, o `dateconfig` en el interprete de comandos (por ejemplo, en una terminal **XTerm** o una terminal **GNOME**).

1. Propiedades de hora y fecha

Como se muestra en la Figura 13.1, “Propiedades de hora y fecha”, la primera ventana que aparece es para configurar la fecha y la hora del sistema.

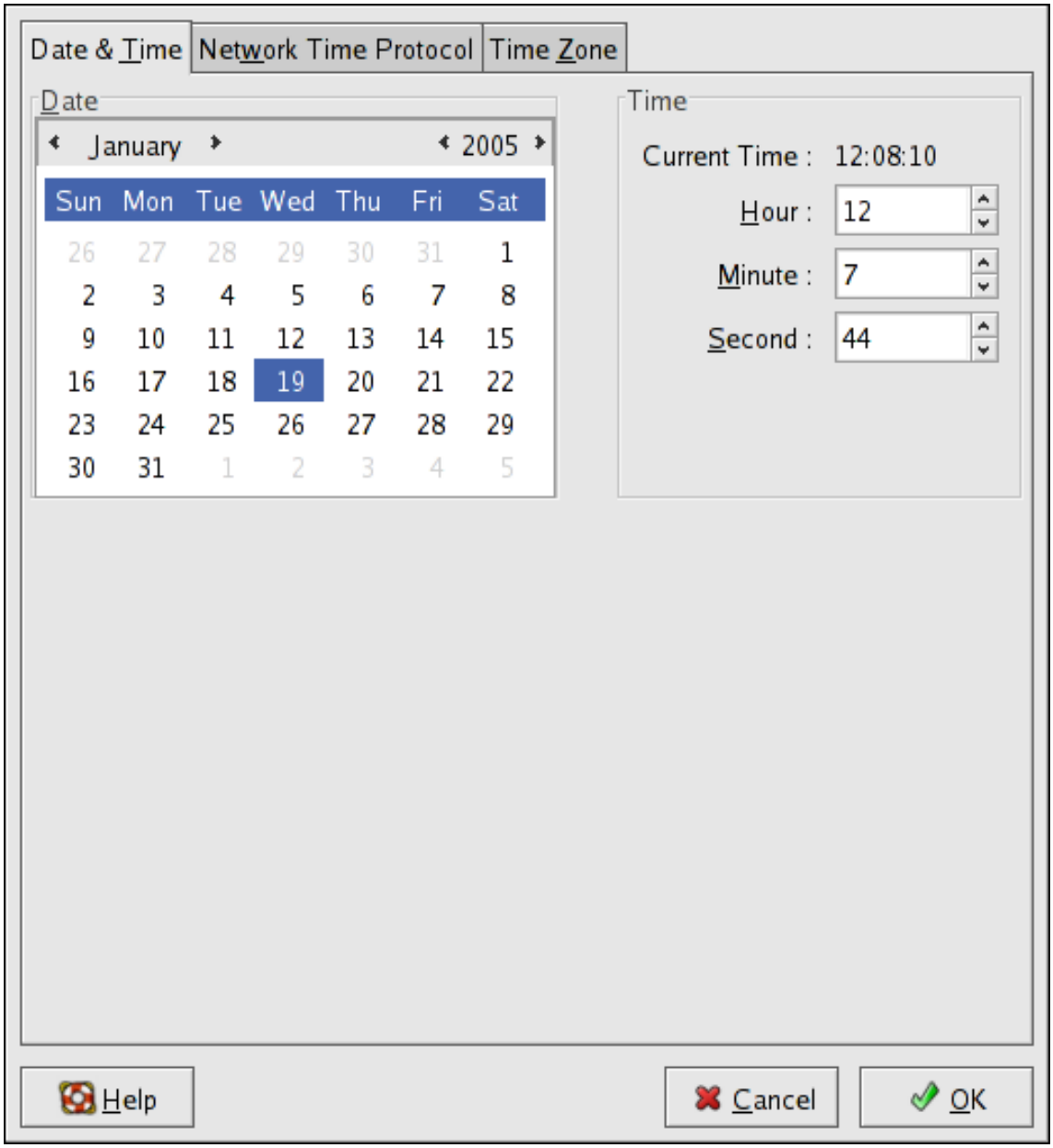


Figura 13.1. Propiedades de hora y fecha

Para cambiar la fecha, utilice las flechas a izquierda y derecha del mes que desea cambiar, utilice las flechas a izquierda y derecha del año y pulse en el día de la semana a establecer.

Para cambiar la hora, use las flechas arriba y abajo situadas junto a **Hora**, **Minuto** y **Segundos** en la sección **Hora**.

Haciendo clic sobre **OK** aplicará cualquier cambio que haya realizado a la fecha y a la hora, a las configuraciones del demonio NTP y a las configuraciones de zona horaria. Tras esta acción se saldrá del programa.

2. Propiedades del protocolo de tiempo de

red (NTP)

Como se muestra en la Figura 13.1, “Propiedades de hora y fecha”, la segunda ventana que aparece es para configurar NTP.

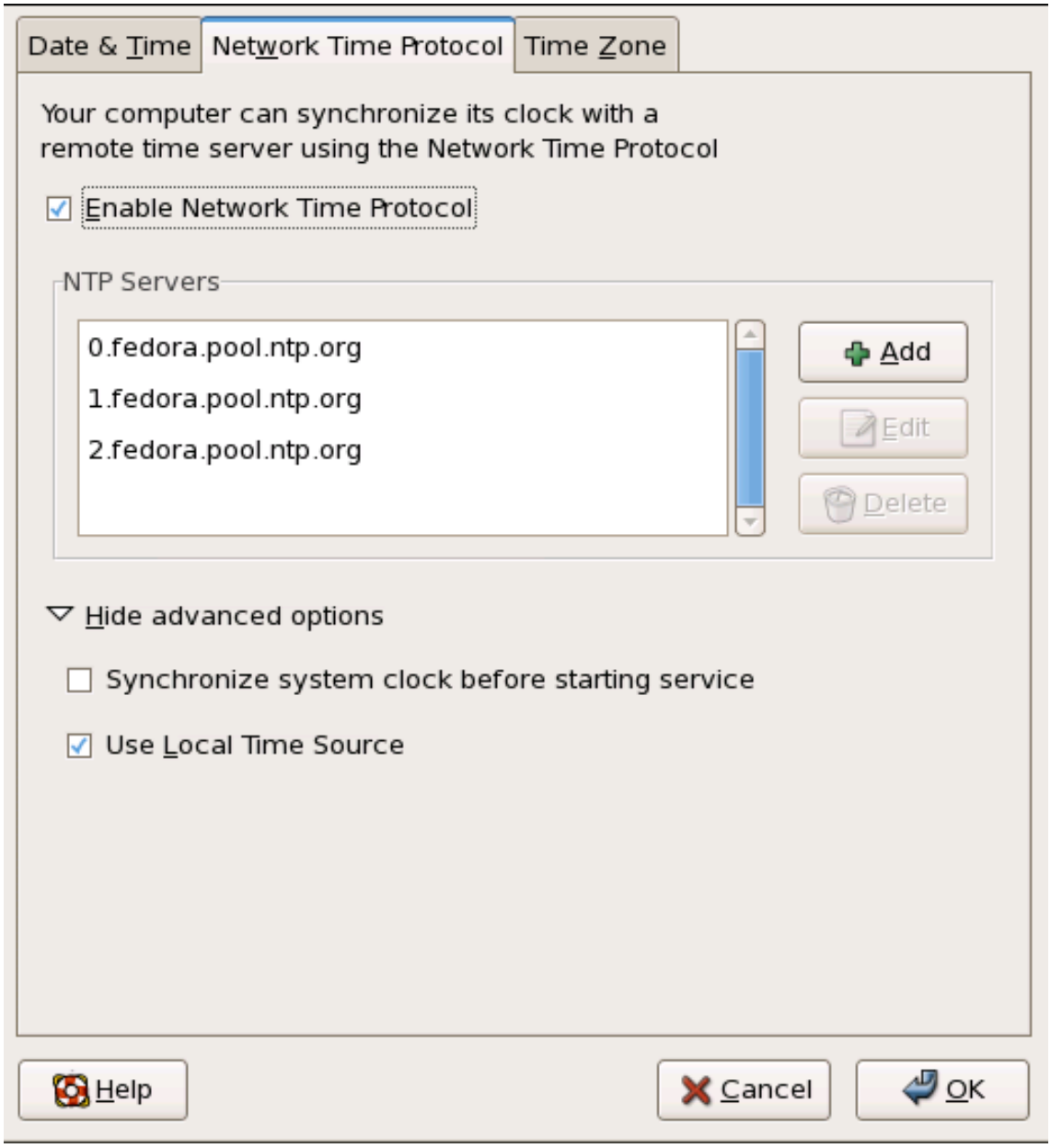


Figura 13.2. Propiedades de NTP

El demonio Network Time Protocol (NTP) sincroniza el reloj del sistema con un servidor horario remoto o con una fuente horaria. La aplicación le permite configurar el demonio NTP para sincronizar el reloj del sistema con un servidor remoto. Para activar esta función, haga clic en el botón **Activar el Protocolo de tiempo de red**. Esto activará la lista de**Servidores NTP** y otras opciones. Puede seleccionar uno de los servidores predefinidos, editar un servidor predefinido haciendo clic en **Editar** o añadir un nuevo servidor haciendo clic en **Añadir**. El sistema no iniciará la sincronización con el servidor NTP hasta que haga clic en **OK**. Después de hacer clic

en **OK**, se guardará la configuración y se iniciará (o reiniciará si ya se está ejecutando) el demonio NTP.

Haciendo clic sobre **OK** aplicará cualquier cambio que haya realizado a la fecha y a la hora, a las configuraciones del demonio NTP y a las configuraciones de zona horaria. Tras esta acción se saldrá del programa.

3. Configuración de la zona horaria

Como se muestra en la Figura 13.1, “Propiedades de hora y fecha”, la tercera ventana que aparece es para configurar la zona horaria del sistema.

Para configurar la zona horaria del sistema, haga clic en la pestaña **Zona horaria**. La zona horaria se puede cambiar utilizando el mapa interactivo o seleccionando la zona horaria deseada en la lista situada debajo del mapa. Para usar el mapa, haga clic en la ciudad que representa la zona horaria deseada. Aparecerá una **X** de color rojo y la selección de la zona horaria cambiará en la lista situada debajo del mapa.

Además, puede utilizar la lista ubicada bajo el mapa. De la misma manera, la región es escogida antes de la ciudad. La lista de zonas horarias está ahora construida como una lista de árbol, en donde las ciudades y países están agrupados por continentes específicos. Zonas horarias no geográficas también han sido añadidas para resolver necesidades en la comunidad científica.

Haga clic sobre **OK** para aplicar cualquier cambio que haya realizado y para salir del programa.

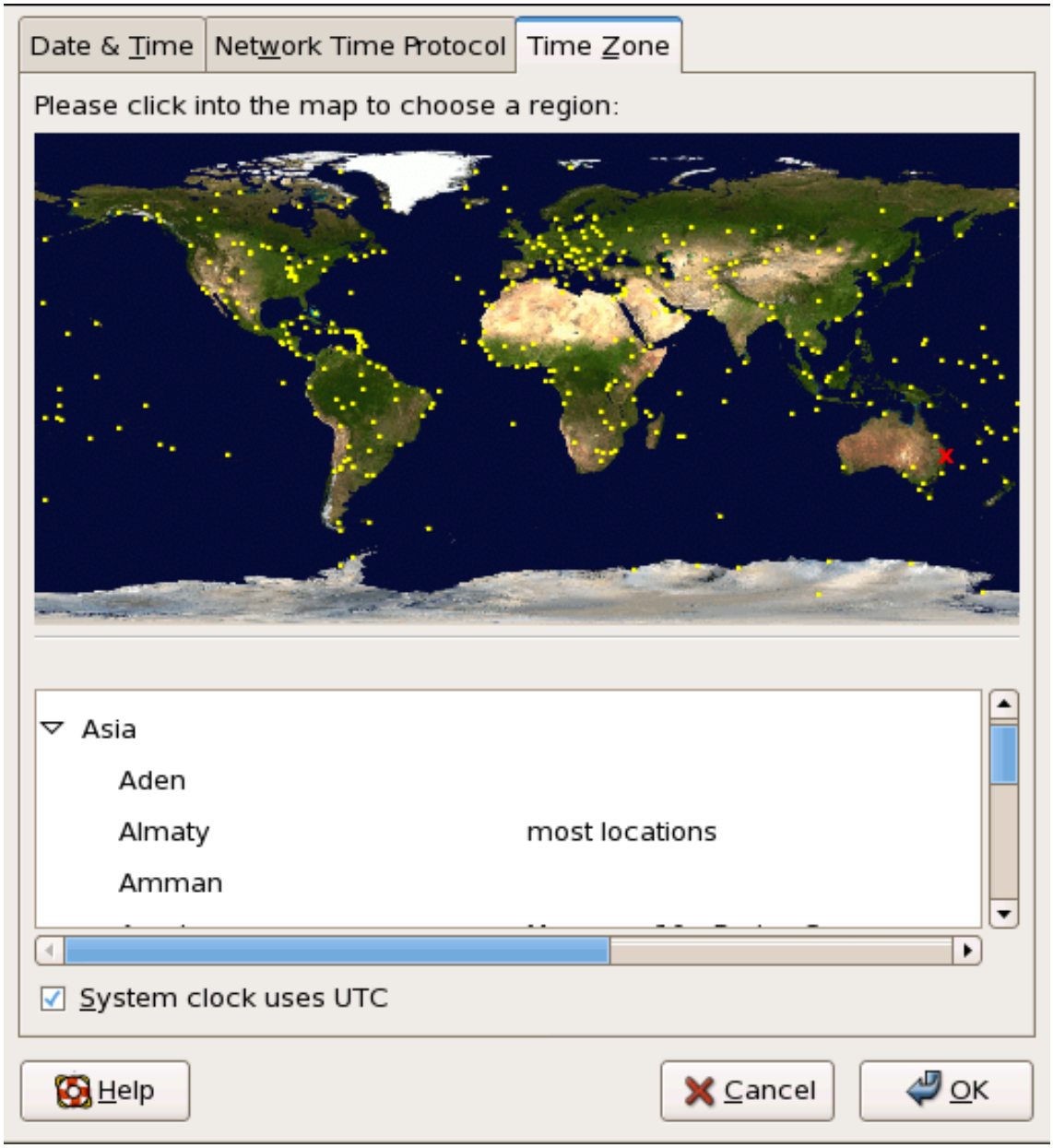


Figura 13.3. Propiedades de la zona horaria

Si su sistema está configurado para usar UTC, seleccione la opción **El reloj del sistema utiliza UTC**. UTC proviene de *Universal Time zone*, también conocido como Greenwich mean time (GMT). Las otras zonas horarias son determinadas sumando o restando de la hora UTC.

Capítulo 14. Configuración del Teclado

El programa de instalación le permite configurar una distribución del teclado para su sistema. Para configurar una distribución del teclado diferente después de la instalación utilice la **Herramienta de configuración del teclado**.

Para iniciar la **Herramienta de configuración del teclado**, seleccione System (on the panel) => **Administración** => **Teclado** o escriba el comando `system-config-keyboard` en el intérprete de comandos de shell.

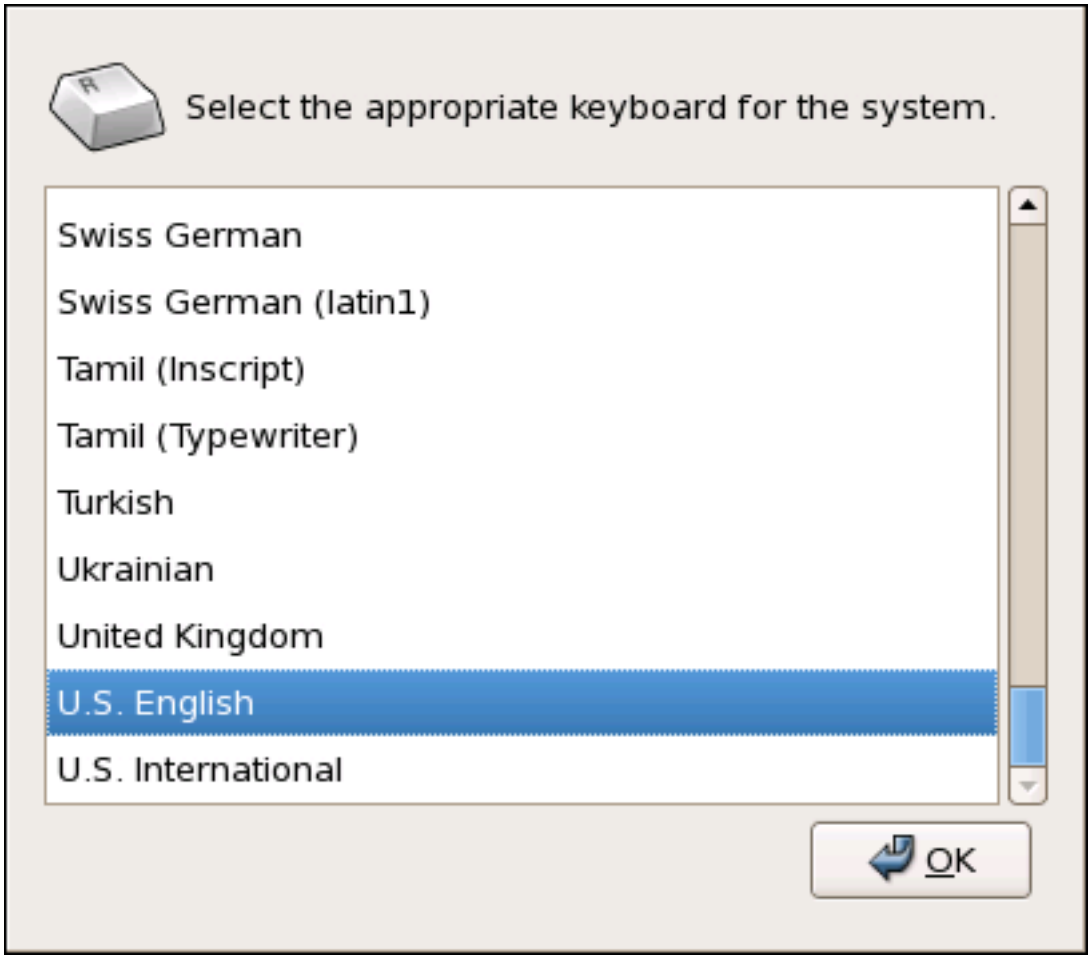


Figura 14.1. Herramienta de Configuración del Teclado

Seleccione una distribución de teclado de la lista (por ejemplo, **U.S. English**) y pulse **OK**.

Los cambios se efectúan inmediatamente.

Capítulo 15. El Sistema X Window

Mientras que el corazón de Red Hat Enterprise Linux es el kernel, para muchos usuarios, la cara del sistema operativo es el entorno gráfico proporcionando por el *Sistema de ventanas X*, también llamado simplemente *X*.

Han existido otros entornos de ventanas en UNIX, algunos de ellos precursores del sistema de ventanas X lanzado en Junio de 1984. Por mucho tiempo, X ha sido el entorno gráfico predeterminado de muchos sistemas operativos tipo UNIX, incluyendo Red Hat Enterprise Linux.

El entorno gráfico de Red Hat Enterprise Linux es suministrado por la *Fundación X.Org*, una organización de código abierto creada para manejar el desarrollo del sistema de ventanas X y otras tecnologías asociadas. X.Org es un proyecto a gran escala con un gran número de desarrolladores en todo el mundo. Presenta una amplia gama de soporte para diferentes dispositivos de hardware y arquitecturas. Puede ser ejecutado en diferentes sistemas operativos y plataformas. Este lanzamiento de Red Hat Enterprise Linux incluye específicamente el lanzamiento X11R7.1 del sistema de ventanas X.

El sistema X Window utiliza una arquitectura cliente-servidor. El *servidor de X* (el binario `Xorg`) escucha por conexiones desde las aplicaciones *cliente X* a través de la red o una interfaz local de loopback. El servidor gestiona la comunicación con el hardware, que puede ser una tarjeta gráfica, un monitor, un teclado o un ratón. Las aplicaciones cliente de X existen en el espacio del usuario, creando una *interfaz gráfica del usuario* (*GUI*) y pasando peticiones al servidor de X.

1. El lanzamiento X11R7.1

Red Hat Enterprise Linux 5.0.0 utiliza el lanzamiento X11R7.1 del sistema de ventanas X. Este lanzamiento incluye varios controladores de vídeo, EXA, soporte mejorado de plataformas en comparación con versiones anteriores y otras características. Además, este lanzamiento incluye varias funciones de configuración automática para el servidor X.

X11R7.1 es el primer lanzamiento que aprovecha la modularización del sistema de ventanas X. Esta modularización, que divide X en módulos lógicamente distintos, permite que los desarrolladores contribuyan al sistema de una manera más fácil.

Importante

ya noRed Hat Enterprise Linux proporciona los paquetes del servidor XFree86™. Antes de actualizar un sistema con la última versión de Red Hat Enterprise Linux, verifique la lista de compatibilidad de hardware de Red Hat localizada en http://hardware.redhat.com/ para asegurar que la tarjeta de vídeo es compatible con el lanzamiento X11R7.1.

En el lanzamiento X11R7.1, todas las bibliotecas, archivos de cabecera, y archivos binarios se encuentran en `/usr/` y no en `/usr/X11R6`. El directorio `/etc/X11/` contiene archivos de configura-

ción para los clientes X y las aplicaciones del servidor. Entre estos archivos se encuentran los archivos de configuración del servidor mismo, del servidor de fuentes `xfs`, de los administradores de visualización X y de otros componentes base.

El archivo de configuración para la nueva arquitectura de fuentes basado en Fontconfig es `/etc/fonts/fonts.conf`. Para obtener mayor información sobre la configuración y sobre los modos de añadir fuentes tipográficas, vea la Sección 4, “Fuentes”.

Ya que el servidor X ejecuta tareas avanzadas sobre una amplia variedad de hardware, éste requiere información detallada sobre el hardware sobre el cual trabaja. El servidor X detecta automáticamente gran parte de esta información. Sin embargo, algunos detalles deben ser configurados.

El programa de instalación instala y configura X automáticamente, a menos que los paquetes del lanzamiento X11R7.1 no sean seleccionados para la instalación. Sin embargo, si la tarjeta de vídeo o el monitor cambian, X debe ser reconfigurado. La manera más apropiada de reconfigurar el servidor es a través de **&RHXFREE86TOOL;** (`system-config-display`), particularmente para dispositivos que no se detectan automáticamente.

En el entorno gráfico predeterminado de Red Hat Enterprise Linux, la **&RHXFREE86TOOL;** está disponible en System (on the panel) => **Administración** => **Visualización**.

Los cambios hechos a **&RHXFREE86TOOL;**, surten efecto después de terminar e iniciar una sesión.

Para obtener mayor información sobre **&RHXFREE86TOOL;**, consulte el Capítulo 16, *Configuración del Sistema X Window*.

En algunas circunstancias, la reconfiguración del servidor X puede requerir la edición manual del archivo de configuración, `/etc/X11/xorg.conf`. Para mayor información sobre la estructura de este archivo, consulte la Sección 3, “Archivos de configuración del servidor X”.

2. Entornos de escritorio y gestores de ventanas

Una vez que un servidor X está siendo ejecutando, las aplicaciones cliente X pueden conectarse a éste y crear interfaces gráficas para el usuario. En Red Hat Enterprise Linux existe un amplio rango de GUIs, desde el rudimentario *Administrador de pestañas de ventanas* hasta un entorno de escritorio altamente desarrollado e interactivo como *GNOME*, con el que la mayoría de los usuarios de Red Hat Enterprise Linux están familiarizados.

Para crear éste último, una GUI más completa, se deben conectar dos clases principales de aplicaciones clientes X al servidor X: un *entorno de escritorio* y un *gestor de ventanas*.

2.1. Entornos de escritorio

Un entorno de escritorio integra diferentes clientes X para crear un entorno gráfico común de usuario y una plataforma de desarrollo.

Los entornos de escritorio tienen características avanzadas las cuales permiten a los clientes X y a otros procesos en ejecución, comunicarse unos con otros a la vez que se permite a todas

las aplicaciones escritas para funcionar en ese ambiente a que realicen tareas avanzadas, tales como operaciones de arrastrar y soltar.

Red Hat Enterprise Linux proporciona dos entornos de escritorio:

- *GNOME* — Es el entorno de escritorio predeterminado de Red Hat Enterprise Linux. Está basado en el conjunto de herramientas gráficas GTK+ 2.
- *KDE* — Un entorno de escritorio alternativo basado en el conjunto de herramientas gráficas Qt 3.

Tanto GNOME como KDE tienen aplicaciones de productividad avanzadas, tales como procesadores de palabras, hojas de cálculo y navegadores Web. Los dos contienen herramientas para personalizar la apariencia de la GUI. Adicionalmente, si ambas bibliotecas están presentes, GTK+ 2 y Qt, las aplicaciones KDE pueden ejecutarse en GNOME y viceversa.

2.2. Gestores de ventanas

Los *gestores de ventanas* son programas clientes de X que pueden ser parte del entorno de escritorio o pueden ser programas independientes. Su propósito principal es controlar la forma en que las ventanas gráficas son posicionadas, redimensionadas o desplazadas. Los gestores de ventanas controlan las barras de títulos, el comportamiento del foco, los vínculos del botón del ratón y teclas especificadas por el usuario.

Se incluyen cuatro gestores de ventanas con Red Hat Enterprise Linux:

`kwin`
: El gestor de ventanas *KWin* es el gestor predeterminado de KDE. Es un gestor de ventanas eficiente que soporta temas personalizados.

`metacity`
: El gestor de ventanas *Metacity* es el gestor de ventanas predeterminado del entorno GNOME. Es un gestor de ventanas sencillo y eficiente que también soporta temas personalizados. Para ejecutar este gestor de ventanas necesitará instalar el paquete `metacity`.

`mwm`
: El gestor de ventanas *Motif* (`mwm`) es un gestor básico e independiente. Puesto que está diseñado para ser un gestor que se ejecuta de forma independiente, no se debería utilizar en conjunto con los entornos de escritorios GNOME o KDE. Para ejecutar este gestor de ventanas, tendrá que instalar el paquete `openmotif`.

`twm`
: El minimalista *Administrador de pestañas de ventanas* (`twm`), el cual proporciona el conjunto de herramientas básicas de cualquier gestor de ventanas, puede ser usado bien sea de forma independiente o con un entorno de escritorio. Es instalado como parte del lanzamiento X11R7.1.

Para ejecutar cualquiera de los gestores de ventanas anteriormente mencionados, tendrá que iniciar el nivel de ejecución 3. Para obtener instrucciones sobre cómo cambiar el nivel de ejecución, consulte la Sección 1, “Niveles de ejecución”.

Una vez haya iniciado una sesión en el nivel de ejecución 3, verá un intérprete de comandos en vez de un entorno gráfico. Para iniciar un gestor de ventanas, escriba `xinit -e <ruta-al-gestor-ventanas>` en el intérprete de comandos.

`<ruta-al-gestor-ventanas>` es la ubicación del archivo binario de gestor de ventanas. Se puede encontrar el archivo binario escribiendo `which <nombre-de-gestor-ventanas>`, donde `<nombre-de-gestor-ventanas>` es el nombre del gestor de ventanas que desea ejecutar.

Por ejemplo:

```
user@host# which twm/usr/bin/twm
user@host# xinit -e /usr/bin/twm
```

El primer comando retorna la ruta absoluta del gestor de ventanas `twm`, el segundo comando inicia `twm`.

Para salir de un gestor de ventanas, cierra la última ventana o presione **Ctrl**-**Alt**-**Backspace**. Una vez haya salido del gestor de ventanas, puede regresar al nivel de ejecución 5 escribiendo `startx` en el intérprete de comandos.

3. Archivos de configuración del servidor X

El servidor X es un binario ejecutable (`/usr/bin/Xorg`). Los archivos de configuración asociados se almacenan en el directorio `/etc/X11/` (es un enlace simbólico — X — que apunta a `/usr/bin/Xorg`). El archivo de configuración para el servidor X es `/etc/X11/xorg.conf`.

El directorio `/usr/lib/xorg/modules/` contiene los módulos del servidor X que pueden ser cargados dinámicamente en tiempo de ejecución. Por defecto, el servidor X sólo carga algunos de los módulos en `/usr/lib/xorg/modules/`.

Para cargar módulos opcionales, éstos deben ser especificados en el archivo de configuración del servidor X, `/etc/X11/xorg.conf`. Para mayor información sobre cómo cargar los módulos, consulte la Sección 3.1.5, “Module”.

Cuando se instala Red Hat Enterprise Linux 5.0.0, los archivos de configuración para X son creados con la información sobre el hardware del sistema reunida durante el proceso de instalación.

3.1. `xorg.conf`

Mientras que casi nunca se necesita editar manualmente el `/etc/X11/xorg.conf`, es muy útil conocer sobre las diferentes secciones y los parámetros opcionales disponibles, especialmente cuando se estén solucionando problemas.

3.1.1. La estructura de XFree86

El archivo `/etc/X11/xorg.conf` está formado de muchas secciones diferentes las cuales hacen referencia a aspectos específicos del hardware del sistema.

Cada sección comienza con una línea `Section "<nombre-de-sección>"` (donde `<nombre-de-sección>` es el título para la sección) y termina con una línea `EndSection`. Dentro de cada sección hay líneas que contienen los nombres de las opciones y uno o más valores para

la opción. Estos últimos van, ocasionalmente, entre comillas (").

Las líneas que comienzan con un símbolo de almohadilla (#) no son leídas por el servidor X y son usadas como comentarios legibles.

Algunas opciones dentro del archivo `/etc/X11/xorg.conf` aceptan un interruptor boleano el cual activa o desactiva la característica. Los valores boleanos aceptados son:

- `1`, `on`, `true`, o `yes` — Activa la opción.
- `0`, `off`, `false`, o `no` — Desactiva la opción.

Lo siguiente son algunas de las secciones más importantes ordenadas como aparecen en un archivo `/etc/X11/xorg.conf` típico. Se puede encontrar más información detallada sobre el archivo de configuración del servidor X en la página man de `xorg.conf`.

3.1.2. `ServerFlags`

La sección opcional `ServerFlags` contiene varios parámetros globales del servidor X. Cualquier parámetro en esta sección puede ser sobreescrito por las opciones ubicadas en la sección `ServerLayout` (consulte la Sección 3.1.3, “ServerLayout” para obtener mayor información).

Cada entrada dentro de la sección `ServerFlags` están en sus propias líneas y comienzan con el término `Option` seguido por una opción encerrada en dobles comillas **"**.

A continuación un ejemplo de la sección `ServerFlags`:

```
Section "ServerFlags" Option "DontZap" "true" EndSection
```

La siguiente es una lista de las opciones más útiles:

- `"DontZap" "<boleano>"` — Cuando el valor de `<boleano>` está configurado a verdadero, esta configuración previene el uso de la combinación de teclas **Ctrl**-**Alt**-**Retroceso** para terminar inmediatamente el servidor X.
- `"DontZoom" "<boleano>"` — Cuando el valor de `<boleano>` está colocado a verdadero, esta configuración previene moverse a lo largo de las resoluciones de vídeo configuradas usando las combinaciones de teclas **Ctrl**-**Alt**-**Keypad-Plus** y **Ctrl**-**Alt**-**Keypad-Minus**.

3.1.3. `ServerLayout`

La sección `ServerLayout` vincula los dispositivos de entrada y salida controlados por el servidor X. Como mínimo, esta sección debe especificar un dispositivo de salida y un dispositivo de entrada. Por defecto se especifica un monitor (dispositivo de salida) y un teclado (dispositivo de entrada).

El ejemplo siguiente ilustra una sección `ServerLayout` típica:

```
Section "ServerLayout" Identifier "Default Layout" Screen 0 "Screen0" 0 0 InputDevice "Mouse0" "CorePointe
```

Las entradas siguientes son usadas a menudo en la sección `ServerLayout`:

- `Identifier` — Especifica un nombre único para esta sección `ServerLayout`.

- `Screen` — Especifica el nombre de la sección `Screen` a ser usado con el servidor X. Pueden estar presentes más de una opción `Screen`.

  Lo siguiente es un ejemplo de una entrada `Screen` típica:

  ```
  Screen 0 "Screen0" 0 0
  ```

  El primer número en esta entrada de ejemplo `Screen` (`0`) indica que el primer conector del monitor o *head* en la tarjeta de vídeo usa la configuración especificada en la sección `Screen` con el identificador `"Screen0"`.

  Un ejemplo de la sección `Screen` con el identificador `"Screen0"` se puede encontrar en la Sección 3.1.9, “Screen”.

  Si la tarjeta de vídeo tiene más de una cabeza, será necesaria otra entrada `Screen` con un número diferente y un identificador de sección `Screen`.

  Los números a la derecha de `"Screen0"` proporcionan las coordenadas absolutas X y Y para la esquina superior izquierda de la pantalla (`0 0` por defecto).

- `InputDevice` — Especifica el nombre de una sección `InputDevice` a ser usada con el servidor X.

  Se recomienda utilizar al menos dos entradas `InputDevice`: una para el ratón y una para el teclado. Las opciones `CorePointer` y `CoreKeyboard` indican que estos son el ratón y el teclado principal.

- `Option "<nombre-opcion>"` — Una entrada opcional que especifica parámetros extra para esta sección. Cualquier sección listada aquí sobreescriben aquellas listadas en la sección `ServerFlags`.

  Reemplace `<nombre-opcion>` con una opción válida listada para esta sección en la página man de `xorg.conf`.

Es posible crear más de una sección `ServerLayout` en el archivo `/etc/X11/xorg.conf`. Sin embargo, el servidor sólo leerá la primera sección que aparezca.

Si hay una sección `ServerLayout` alternativa, ésta se puede especificar como argumento en la línea de comandos cuando inicie la sesión X.

3.1.4. `Files`

La sección `Archivos` establece rutas importantes para el funcionamiento del servidor X (como por ejemplo la ruta de las fuentes tipográficas). Esta sección es opcional, estas rutas son normalmente detectadas de forma automática. Esta sección puede ser usada para sobreescribir las rutas detectadas automáticamente.

El siguiente ejemplo ilustra una sección `Files`:

```
Section "Files" RgbPath "/usr/share/X11/rgb.txt" FontPath "unix/:7100" EndSection
```

Las siguientes entradas son usadas comúnmente en la sección `Files`:

- `RgbPath` — Especifica la ubicación de la base de datos de colores RGB. Esta base de datos define todos los esquemas de color en X y los junta para valores RGB especificos.
- `FontPath` — Especifica dónde el servidor X debe ser conectado para obtener las fuentes tipográficas desde el servidor de fuentes `xfs`.

  Por defecto, la `FontPath` es `unix/:7100`. Esto le dice al servidor X que obtenga información de fuentes usando sockets de dominio UNIX para la comunicación entre procesos (IPC) en el puerto 7100.

  Consulte la Sección 4, “Fuentes” para obtener mayor información concerniente a X y fuentes tipográficas.
- `ModulePath` — Un parámetro opcional el cual especifica directorios alternativos que almacenan módulos de servidor X.

3.1.5. `Module`

Por defecto, el servidor X carga automáticamente los siguientes módulos desde el directorio `/usr/lib/xorg/modules/`:

- `extmod`
- `dbe`
- `glx`
- `freetype`
- `type1`
- `record`
- `dri`

El directorio predeterminado para cargar estos módulos puede modificarse a través del parámetro opcional `ModulePath` en la sección `Files`. Consulte la Sección 3.1.4, “Files” para obtener mayor información sobre esta sección.

Si se añade una sección `Module` a `/etc/X11/xorg.conf`, el servidor X cargará los módulos listados en esta sección *en vez de* los módulos predeterminados.

Por ejemplo, la siguiente sección `Module`:

```
Section "Module" Load "fbdevhw" EndSection
```

indica al servidor X que cargue `fbdevhw` en vez de los módulos predeterminados.

Por lo cual, si añade una sección `Module` a `/etc/X11/xorg.conf`, deberá especificar cualquier módulo predeterminado que desea cargar además de los módulos adicionales.

3.1.6. `InputDevice`

Cada sección `InputDevice` configura un dispositivo de entrada para el servidor X. Los sistemas

típicamente tienen al menos una sección `InputDevice` para el teclado. Es normal no tener una entrada para el ratón. La mayoría de parámetros del ratón son detectados automáticamente.

El siguiente ejemplo ilustra una sección `InputDevice` típica para el teclado:

```
Section "InputDevice" Identifier "Keyboard0" Driver "kbd" Option "XkbModel" "pc105" Option "XkbLayout" "us
```

Las entradas siguientes son comúnmente usadas en la sección `InputDevice`:

- `Identifier` — Especifica un nombre único para esta sección `InputDevice`. Esto es una entrada requerida.
- `Driver` — Especifica el nombre del controlador del dispositivo que X debe cargar para el dispositivo.
- `Option` — Especifica las opciones necesarias pertinentes al dispositivo.

  Un ratón puede ser especificado para sobrescribir cualquier parámetro predeterminado para el dispositivo. Las siguientes opciones son normalmente incluidas cuando se añade un ratón en `xorg.conf`:

  - `Protocol` — Indica el protocolo usado por el ratón, tal como `IMPS/2`.
  - `Device` — Indica la ubicación del dispositivo físico.
  - `Emulate3Buttons` — Especifica si se permite que un ratón de dos botones se comporte como uno de tres cuando se presionan ambos botones simultáneamente.

  Consulte la página man de `xorg.conf` para una lista de las opciones válidas para esta sección.

3.1.7. `Monitor`

Cada sección `Monitor` configura un tipo de monitor utilizado por el sistema. Esta también es una entrada opcional, ya que la mayoría de monitores son detectados automáticamente.

La forma más sencilla de configurar un monitor es durante el proceso de instalación o usando la **&RHXFREE86TOOL;**. Para obtener mayor información sobre el uso de la **&RHXFREE86TOOL;**, consulte el Capítulo 16, *Configuración del Sistema X Window*.

Este ejemplo muestra una sección de `Monitor` típica:

```
Section "Monitor" Identifier "Monitor0" VendorName "Monitor Vendor" ModelName "DDC Probed Monitor - ViewSo
```

Aviso

Tenga cuidado si está modificando manualmente los valores en la sección `Monitor` de `/etc/X11/xorg.conf`. Valores inapropiados pueden dañar o destruir su monitor. Consulte la documentación de su monitor para un listado de parámetros seguros.

A continuación se muestran entradas comunes usadas en la sección `Monitor`:

- `Identifier` — Proporciona un nombre único para esta sección `Monitor`. Esta es una entrada requerida.
- `VendorName` — Parámetro opcional que muestra el nombre del fabricante del monitor.
- `ModelName` — Parámetro opcional que muestra el nombre del modelo del monitor.
- `DisplaySize` — Un parámetro opcional que especifica, en milímetros, el tamaño físico del área de dibujo del monitor.
- `HorizSync` — Especifica el rango de la frecuencia de sincronización horizontal compatible con el monitor, en kHz. Estos valores ayudan al servidor X a determinar la validez de las entradas `Modeline` especificadas o incorporadas para el monitor.
- `VertRefresh` — Especifica los rangos de frecuencias de actualización verticales soportados por el monitor, en Hz. Estos valores ayudan a que el servidor X determine la validez de las entradas incorporadas o especificadas en `Modeline` para este monitor.
- `Modeline` — Un parámetro opcional el cual especifica los modos de vídeo adicionales para el monitor en resoluciones particulares, con ciertas resoluciones de refrescamiento vertical y sincronización horizontal. Vea la página man de `xorg.conf` para una explicación más detallada de las entradas `Modeline`.
- `Option "<nombre-opcion>"` — Una entrada opcional que especifica parámetros extra para la sección. Reemplace `<nombre-opcion>` con una opción válida listada para esta sección en la página man de `xorg.conf`.

3.1.8. `Device`

Cada sección `Device` configura una tarjeta de vídeo en el sistema. Aunque una sección `Device` es lo mínimo, también se pueden tener instancias adicionales para cada tarjeta de vídeo instalada en la máquina.

La mejor forma de configurar una tarjeta de vídeo es configurando X durante el proceso de instalación o usando la **&RHXFREE86TOOL;**. Para obtener mayor información sobre el uso de la **&RHXFREE86TOOL;** consulte el Capítulo 16, *Configuración del Sistema X Window*.

El siguiente ejemplo ilustra una sección `Device` típica para una tarjeta de vídeo:

```
Section "Device" Identifier "Videocard0" Driver "mga" VendorName "Videocard vendor" BoardName "Matrox Mill
```

Las siguientes entradas son usadas comúnmente en la sección `Device`:

- `Identifier` — Especifica un nombre único para esta sección `Device`. Esta es una entrada requerida.
- `Driver` — Especifica cuál controlador debe cargar el servidor X para poder utilizar la tarjeta de vídeo. Se puede encontrar una lista de los controladores en `/usr/share/hwdata/videodrivers`, el cual es instalado con el paquete `hwdata`.

- `VendorName` — Un parámetro opcional el cual especifica el fabricante de la tarjeta de vídeo.
- `BoardName` — Un parámetro opcional el cual especifica el nombre de la tarjeta de vídeo.
- `VideoRam` — Un parámetro opcional el cual especifica la cantidad de RAM disponible en la tarjeta de vídeo en kilobytes. Este valor sólo es necesario para tarjetas de vídeo que el servidor X no puede probar para detectar la cantidad de RAM.
- `BusID` — Una entrada que especifica la ubicación del bus de la tarjeta de vídeo. En sistemas con tan sólo una tarjeta de vídeo, la entrada `BusID` es opcional y puede no aparecer en el archivo `/etc/X11/xorg.conf` predeterminado. Sin embargo, en sistemas con más de una tarjeta de vídeo, la entrada `BusID` debe estar presente.
- `Screen` — Una entrada opcional la cual especifica que conector de monitor o cabezal en la tarjeta de vídeo configura la sección `Device`. Esta opción es útil solamente para tarjetas de vídeo con múltiples cabezales.

  Si múltiples monitores son conectados a diferentes cabezales en la misma tarjeta de vídeo, deben existir secciones `Device` separadas y cada una de estas secciones debe tener un valor `Screen` diferente.

  Los valores para la entrada `Screen` deben ser enteros. El primer cabezal en la tarjeta de vídeo tiene un valor de `0`. El valor para cada cabezal adicional incrementa este valor en uno.
- `Option "<nombre-opcion>"` — Una entrada opcional que especifica parámetros extra para la sección. Reemplace `<nombre-opcion>` con una opción válida listada para esta sección en la página man de `xorg.conf`.

  Una de las opciones más comunes es `"dpms"` (del ingés Display Power Management Signaling, un estándar VESA). Esta opción activa la configuración de conformidad de energía Service Star para el monitor.

3.1.9. `Screen`

Cada sección `Screen` vincula una tarjeta de vídeo (o cabezal) a un monitor referenciando la sección `Device` y la sección `Monitor` para cada uno. Mientras que una sección `Screen` es lo mínimo, pueden ocurrir instancias adicionales para cada combinación de tarjeta de vídeo y monitor presente en la máquina.

El ejemplo siguiente ilustra una sección `Screen` típica:

```
Section "Screen" Identifier "Screen0" Device "Videocard0" Monitor "Monitor0" DefaultDepth 16 SubSection "D
```

Las siguientes entradas son usadas a menudo en la sección `Screen`:

- `Identifier` — Especifica un nombre único para esta sección `Screen`. Esta es una entrada requerida.
- `Device` — Especifica el nombre único de una sección `Device`. Esta es una entrada requerida.
- `Monitor` — Especifica el nombre único de la sección `Monitor`. Esto sólo es requerido si se especifica una sección `Monitor` en el archivo `xorg.conf`. Normalmente, los monitores son detectados automáticamente.

- `DefaultDepth` — Especifica la profundidad del color por defecto en bits. En el ejemplo anterior, el valor por defecto es `16` (lo cual proporciona miles de colores). Sólo una entrada `DefaultDepth` es permitida, pero ésta puede ser sobrescrita por la opción de la línea de comandos `-depth <n>`, en donde `<n>` es cualquier profundidad adicional especificada.

- `SubSection "Display"` — Especifica los modos de la pantalla disponibles en una profundidad de color particular. Una sección `Screen` puede tener múltiples subsecciones `Display`. Éstas son opcionales ya que los modos de la pantalla son automáticamente detectados.

  Esta subsección es generalmente usada para sobrescribir modos automáticamente detectados.

- `Option "<nombre-opcion>"` — Una entrada opcional que especifica parámetros extra para la sección. Reemplace `<nombre-opcion>` con una opción válida listada para esta sección en la página man de `xorg.conf`.

3.1.10. DRI

La sección opcional `DRI` especifica parámetros para *Direct Rendering Infrastructure* (*DRI*). DRI es una interfaz que permite a las aplicaciones de software 3D sacar provecho de las capacidades de aceleración de hardware 3D incorporadas en la mayoría del hardware moderno de vídeo. Además, DRI puede mejorar el rendimiento de 2D a través de la aceleración de hardware, si es soportado por el controlador de la tarjeta.

Esta sección aparece raramente ya que el grupo y el modo DRI son automáticamente inicializados a sus valores predeterminados. Si se desea un grupo o modo diferente, los valores añadidos a esta sección en `xorg.conf` sobreescribirán los valores predeterminados.

El ejemplo siguiente muestra una sección `DRI` típica:

```
Section "DRI" Group 0 Mode 0666 EndSection
```

Puesto que tarjetas de vídeo diferentes utilizan DRI de formas diferentes, no modifique estos valores para esta sección sin primero consultar http://dri.sourceforge.net/.

4. Fuentes

Red Hat Enterprise Linux utiliza dos sistemas para administrar y visualizar fuentes tipográficas bajo X: *Fontconfig* y `xfs`

El subsistema de fuentes Fontconfig simplifica la gestión de fuentes y proporciona características de visualización avanzadas, tales como anti-aliasing. Este sistema es usado automáticamente para aplicaciones programadas usando el conjunto de herramientas gráficas Qt 3 o GTK+ 2.

Por compatibilidad, Red Hat Enterprise Linux incluye el subsistema de fuentes original, llamado el subsistema de fuentes núcleo de X. Este sistema, el cual tiene más de 15 años, está basado en el *Servidor de fuentes de X* (*xfs*).

Esta sección discute cómo configurar fuentes para X usando ambos sistemas.

4.1. Fontconfig

El subsistema de fuentes Fontconfig permite a las aplicaciones accesar directamente fuentes en el sistema y usar Xft u otros mecanismos de traducción de fuentes para interpretar fuentes Fontconfig con anti-aliasing avanzados. Las aplicaciones gráficas pueden usar la librería Xft con Fontconfig para dibujar texto a la pantalla.

Con el tiempo, el subsistema de fuentes Fontconfig/Xft reemplazará el subsistema de fuentes base de X.

Importante

El subsistema de fuentes Fontconfig aún no funciona para **OpenOffice.org**, el cual tiene sus propias tecnologías de interpretación de fuentes tipográficas.

Es importante resaltar que Fontconfig utiliza el archivo de configuración `/etc/fonts/fonts.conf` el cual no se debería modificar manualmente.

Sugerencia

Debido a la transición al nuevo sistema de fuentes, las aplicaciones GTK+ 1.2 no son afectadas por ningún cambio realizado a través del diálogo **Preferencias de tipografía** (al cual se accede a través de System (on the panel) => **Preferencias** => **Tipografía**). Para estas aplicaciones, se puede configurar una fuente añadiendo las líneas siguientes al archivo `~/.gtkrc.mine`:

```
style "user-font" { fontset = "<font-specification>" } widget_class "*" style "
```

Sustituya `<font-specification>` con una especificación de fuente en el estilo utilizado por las aplicaciones X tradicionales, tales como `-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*`. Se puede obtener una lista completa de las fuentes base ejecutando `xlsfonts` o creándolas interactivamente usando el comando `xfontsel`.

4.1.1. Añadir fuentes a Fontconfig

Añadir fuentes al subsistema Fontconfig es un proceso bastante directo.

1. Para añadir fuentes tipográficas globales al sistema, copie las fuentes al directorio `/usr/share/fonts/`. Es una buena idea crear un nuevo subdirectorio, tal como `local/` o similar, para ayudar a distinguir entre las fuentes del usuario y las instaladas por defecto.

   Para añadir fuentes para un usuario individual, copie las nuevas fuentes en el directorio `.fonts/` en el directorio principal del usuario.

2. Utilice el comando `fc-cache` para actualizar la información caché de la fuente, como en el

ejemplo siguiente:

```
fc-cache <ruta-directorio-fuentes>
```

En este comando, sustituya *<path-to-font-directory>* con el directorio conteniendo las nuevas fuentes (bien sea `/usr/share/fonts/local/` o `/home/<user>/.fonts/`).

Sugerencia

Usuarios individuales también pueden instalar fuentes tipográficas gráficamente, escribiendo `fonts:///` en la barra de direcciones de **Nautilus** y arrastrando los nuevos archivos de fuentes allí.

Importante

Si el nombre del archivo de fuentes termina con una extensión `.gz`, está comprimido y no puede ser usado hasta que se descomprima. Para hacer esto, utilice el comando `gunzip` o haga doble-clic sobre el archivo y arrastre la fuente a un directorio en **Nautilus**.

4.2. Sistema de fuentes base de X

Por compatibilidad, Red Hat Enterprise Linux proporciona el subsistema de fuentes tipográficas núcleo de X, el cual utiliza el servidor de fuentes X (`xfs`) para proporcionar fuentes tipográficas a las aplicaciones clientes X.

El servidor X busca un servidor de fuentes tipográficas especificado en la directiva `FontPath` bajo la sección `Files` del archivo de configuración `/etc/X11/xorg.conf`. Consulte la Sección 3.1.4, “Files” para obtener mayor información sobre la entrada `FontPath`.

El servidor X se conecta al servidor `xfs` en un puerto especificado para adquirir la información sobre las fuentes tipográficas. Por esta razón, el servicio `xfs` debe estar ejecutándose para que X pueda arrancar. Para obtener mayor información sobre cómo configurar servicios en los diferentes niveles de ejecución, consulte Capítulo 3, *Control de acceso a servicios*.

4.2.1. Configuración de `xfs`

El script `/etc/rc.d/init.d/xfs` inicia el servidor `xfs`. Se pueden configurar muchas opciones dentro del archivo `/etc/X11/fs/config`.

La siguiente es una lista de algunas opciones comunes:

- `alternate-servers` — Especifica una lista de servidores alternativos de fuentes tipográficas que podrán ser utilizados en el caso de que el servidor actual no esté disponible. Los diferentes servidores deberán estar separados por comas.

- `catalogue` — Especifica una lista ordenada de rutas que contienen las fuentes tipográficas a utilizar. Cada ruta hacia las fuentes deberá estar separada por una coma en la lista.

  Puede utilizar la cadena `:unscaled` inmediatamente después de la ruta hacia las fuentes para hacer que las fuentes no escalables se carguen primero. Entonces, podrá especificar la ruta completa de nuevo de tal forma que las otras fuentes que sean escalables puedan ser cargadas también.

- `client-limit` — Configura el número máximo de clientes que el servidor de fuentes podrá servir. El número por defecto es `10`.

- `clone-self` — Permite al servidor de fuentes clonar una nueva versión de sí mismo si se llega al límite definido por el parámetro `client-limit`. Por defecto, esta opción está configurada como `on`.

- `default-point-size` — Configura el tamaño de punto por defecto para cualquier fuente que no especifique este valor. El valor de esta opción está estimado en décimas de puntos. El valor por defecto de `120` se corresponde a fuentes de 12 puntos.

- `default-resolutions` — Especifica una lista de las resoluciones soportadas por el servidor X. Cada resolución de la lista debe estar separada por una coma.

- `deferglyphs` — Especifica si retrasar la carga de *glyphs* (el gráfico usado para visualmente representar una fuente). Para desactivar esta característica utilice `none`, para activarla para todas las fuentes utilice `all`, o para activar esta característica solamente para fuentes de 16-bit use `16`.

- `error-file` — Le permite especificar la ruta y el nombre de archivo donde se almacenarán los informes de error de `xfs`.

- `no-listen` — Dice a `xfs` que no escuche determinados protocolos. Por defecto, esta opción está configurada con `tcp` para evitar que `xfs` escuche utilizando puertos TCP, por motivos de seguridad.

Sugerencia

Si está utilizando `xfs` para servir fuentes sobre la red, elimine esta línea.

- `port` — Especifica el puerto TCP en el cual `xfs` escuchará si `no-listen` no existe o está entre comentarios.

- `use-syslog` — Especifica si utilizar el registro de errores del sistema.

4.2.2. Añadir fuentes a `xfs`

Para añadir fuentes al subsistema base de fuentes de X (`xfs`), siga los pasos siguientes:

1. Si aún no existe, cree un directorio llamado `/usr/share/fonts/local/` usando el comando siguiente como usuario root:

```
mkdir /usr/share/fonts/local/
```

Si es necesario la creación del directorio `/usr/share/fonts/local/`, se debe añadir a la ruta `xfs` usando el comando siguiente como root:

```
chkfontpath --add /usr/share/fonts/local/
```

2. Copie el nuevo archivo de fuente en el directorio `/usr/share/fonts/local/`
3. Actualice la información de la fuente emitiendo el siguiente comando como root:

```
ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale
```

4. Vuelva a cargar el archivo de configuración del servidor de fuentes `xfs`, utilizando el comando siguiente como root:

```
service xfs reload
```

5. Niveles de ejecución y X

En la mayoría de los casos, la instalación por defecto de Red Hat Enterprise Linux configura una máquina para iniciar en un entorno de conexión gráfico, conocido como *nivel de ejecución 5*. Es posible, sin embargo, arrancar en el modo multiusuario de sólo texto llamado *nivel de ejecución 3* y comenzar una sesión X desde allí.

Para obtener mayor información sobre los niveles de ejecución, consulte la Sección 1, “Niveles de ejecución”.

Las siguientes subsecciones revisan cómo inicia X en los niveles de ejecución 3 y 5.

5.1. Nivel de ejecución 3

Cuando estamos en el nivel de ejecución 3, la forma habitual de iniciar una sesión X es escribiendo el comando `startx`. El comando `startx` es una interfaz del programa `xinit` el cual lanza el servidor X (`Xorg`) y conecta aplicaciones clientes X al mismo. Puesto que el usuario ya está conectado al sistema en el nivel de ejecución 3, `startx` no lanzará un gestor de visualización o autenticará al usuario. Consulte la Sección 5.2, “Nivel de ejecución 5” para obtener mayor información sobre los gestores de visualización.

Cuando se ejecuta el comando `startx`, se busca el archivo `.xinitrc` en el directorio principal del usuario para definir el entorno de escritorio y posiblemente otras aplicaciones clientes X a ejecutar. Si este archivo `.xinitrc` no se encuentra, se utilizará el archivo por defecto `/etc/X11/xinit/xinitrc`.

El script `xinitrc` predeterminado buscará luego los archivos definidos por el usuario y archivos de sistema por defecto, incluyendo `.Xresources`, `.Xmodmap` y `.Xkbmap` en el directorio principal del usuario y `Xresources`, `Xmodmap` y `Xkbmap` en el directorio `/etc/X11/`. Si existen los archivos `Xmodmap` y `Xkbmap`, estos son usados por la utilidad `xmodmap` para configurar el teclado. El archivo `Xresources` es leído para asignar valores de preferencia específicos a las aplicaciones.

Después de configurar estas opciones, el script `xinitrc` ejecuta todos los scripts localizados en

el directorio `/etc/X11/xinit/xinitrc.d/`. Un script muy importante en este directorio es `xinput.sh`, el cual configura parámetros como el idioma por defecto.

Luego, el script `xinitrc` intenta ejecutar `.Xclients` en el directorio principal del usuario y cambia a `/etc/X11/xinit/Xclients` si no lo puede encontrar. El propósito del archivo `Xclients` es arrancar el entorno de escritorio o, posiblemente, sólo un gestor de ventanas básico. El script `.Xclients` en el directorio principal del usuario inicia el entorno de escritorio especificado por el usuario en el archivo `.Xclients-default`. Si `.Xclients` no existe en el directorio principal del usuario, el script estándar `/etc/X11/init/Xclients` intenta iniciar otro entorno de escritorio, intentando primero con GNOME y luego con KDE seguido por `twm`.

Cuando se está en el nivel de ejecución 3, el usuario es devuelto a una sesión en modo texto después de desconectarse de X.

5.2. Nivel de ejecución 5

Cuando el sistema arranca en el nivel de ejecución 5, se lanza una aplicación cliente de X especial llamada *gestor de visualización*. El usuario debe autenticarse usando el gestor de visualización antes de que se inicien cualquier entorno de escritorio o gestores de ventanas.

Dependiendo de los entornos de escritorio instalados en su máquina, están disponibles tres gestores de visualización diferentes para manejar la autenticación de los usuarios.

- `GNOME` — Es el gestor de visualización por defecto para Red Hat Enterprise Linux y permite que el usuario configure los parámetros de idioma, cierre del sistema, reinicio o conexión al sistema.
- `KDE` — El gestor de visualización de KDE que permite a los usuarios apagar, reiniciar o conectarse al sistema.
- `xdm` — Este es un gestor de visualización muy básico que sólo permite que el usuario se conecte al sistema.

Cuando arranque en el nivel de ejecución 5, el script `prefdm` determina el gestor de visualización preferido haciendo referencia al archivo `/etc/sysconfig/desktop`. Una lista de opciones para este archivo está disponible en:

`/usr/share/doc/initscripts-<`*`número-versión`*`>/sysconfig.txt`

en donde `<`*`número-versión`*`>` es el número de la versión del paquete `initscripts`.

Cada uno de los gestores de visualización hace referencia al archivo `/etc/X11/xdm/Xsetup_0` para configurar la pantalla de conexión. Una vez que el usuario se conecte al sistema, el script `/etc/X11/xdm/GiveConsole` corre para asignar la propiedad de la consola al usuario. Luego, el script `/etc/X11/xdm/Xsession` se ejecuta para llevar a cabo muchas de las tareas que son normalmente realizadas por el script `xinitrc` cuando arranca X desde el nivel de ejecución 3, incluyendo la configuración del sistema y los recursos del usuario, así como también ejecutar los scripts en el directorio `/etc/X11/xinit/xinitrc.d/`.

El usuario puede especificar cuál entorno de escritorio desea utilizar cuando se autentican usando los gestores de visualización `GNOME` o `KDE`, seleccionándolo desde el menú **Sesiones** (a través de System (on the panel) => **Preferencias** => **Más preferencias** => **Sesiones**). Si el en-

torno de escritorio no es especificado en el gestor de visualización, el script `/etc/X11/xdm/Xsession` verificará los archivos `.xsession` y `.Xclients` en el directorio principal del usuario para decidir cuál entorno de escritorio cargar. Como último recurso, se utiliza el archivo `/etc/X11/xinit/Xclients` para seleccionar un entorno de escritorio o gestor de ventanas para usarse de la misma forma que en el nivel de ejecución 3.

Cuando el usuario termina una sesión X en la visualización por defecto (`:0`) y se desconecta, el script `/etc/X11/xdm/TakeConsole` se ejecuta y vuelve a asignar la propiedad de la consola al usuario root. El gestor de visualización original, que continúa ejecutándose después de que el usuario se conecta, toma el control al liberar un nuevo gestor de visualización. Esto reinicia el servidor X, despliega una nueva ventana de conexión y reinicia el proceso completo otra vez.

El usuario es devuelto al gestor de visualización después de desconectarse de X desde el nivel de ejecución 5.

Para obtener mayor información sobre cómo los gestores de visualización controlan la autenticación de los usuarios, consulte `/usr/share/doc/gdm-<número-versión>/README` (donde `<número-versión>` es el número de la versión para el paquete `gdm` instalado) y la página man de `xdm`.

6. Recursos adicionales

Se podría decir mucho más sobre el servidor X, los clientes que se conectan a él y la variada gama de entornos de escritorio y gestores de ventanas.

6.1. Documentación instalada

- `/usr/share/X11/doc/` — Contiene documentación detallada sobre la arquitectura del sistema de ventanas X, así como la manera de obtener información adicional como nuevo usuario.
- `man xorg.conf` — Contiene información sobre los archivos de configuración `xorg.conf` incluyendo el significado y la sintaxis para las diversas secciones dentro de los archivos.
- `man Xorg` — Describe el servidor de visualización `Xorg`.

6.2. Sitios Web útiles

- http://www.X.org/ — Página principal de la Fundación X.Org, que produce el lanzamiento X11R7.1 del sistema de ventanas X. El lanzamiento X11R6.8 se proporciona junto con Red Hat Enterprise Linux para controlar el hardware necesario y proporcionar un entorno gráfico.
- http://dri.sourceforge.net/ — Página principal del proyecto DRI (Direct Rendering Infrastructure). DRI es el corazón del componente de aceleración 3D de X.
- http://www.gnome.org/ [http://www.gnome.org] — Página principal del proyecto GNOME.
- http://www.kde.org/ [http://www.kde.org] — Página principal del entorno de escritorio KDE.

Capítulo 16. Configuración del Sistema X Window

Durante la instalación se configura el monitor del sistema, la tarjeta de vídeo y los parámetros de la visualización. Para cambiar cualquiera de estos valores después de la instalación, utilice la **&RHXFREE86TOOL;**.

Para arrancar la **&RHXFREE86TOOL;**, vaya al System (on the panel) => **Administración** => **Visualización**, o escriba el comando `system-config-display` en un intérprete de comandos de shell (por ejemplo, en un XTerm o en una terminal GNOME). Si el Sistema X Window no se está en ejecución, se iniciará una pequeña versión de X para ejecutar el programa.

Después de cambiar cualquiera de estas configuraciones, cierre la sesión del escritorio gráfico y vuelva a conectarse para activar los cambios.

1. Configuraciones de la visualización

La pestaña **Configuración** le permite a los usuarios cambiar la *resolución* y la *profundidad del color*. La visualización de un monitor consiste en pequeños puntos llamados *píxeles*. El número de píxeles desplegados a la vez es llamado resolución. Por ejemplo, la resolución de 1024x768 significa que se utilizan 1024 píxeles horizontales y 768 píxeles verticales. Mientras más alto los números de resolución, más imágenes el monitor puede mostrar en un momento.

La profundidad del color de una visualización determina cuántos colores posibles son mostrados. Mientras más alto sea la profundidad del color, habrá más contraste entre colores.

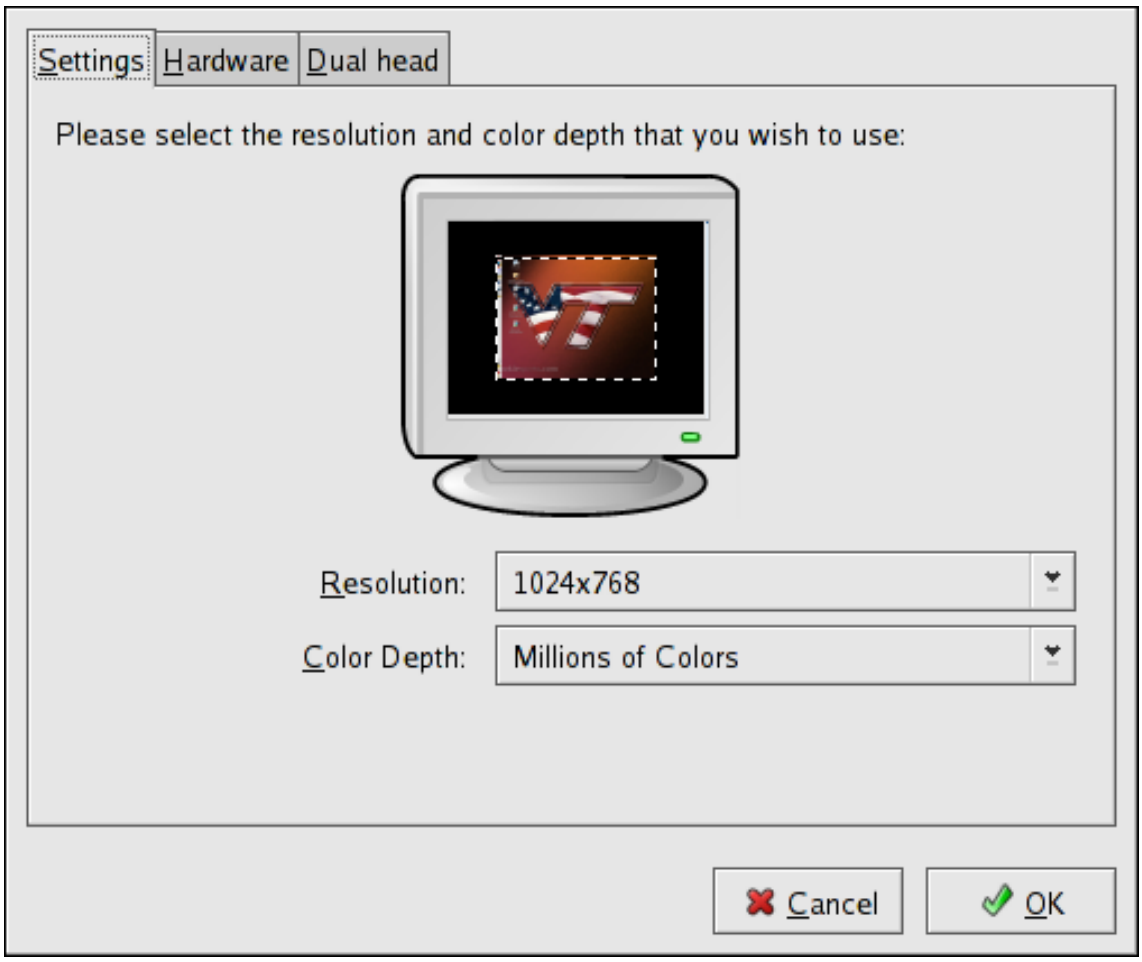


Figura 16.1. Configuraciones de la visualización

2. Configuraciones del hardware de visualización

La aplicación **&RHXFREE86TOOL;** prueba el monitor y la tarjeta de vídeo una vez iniciada. Si el hardware es probado adecuadamente, la información es mostrada en la pestaña **Hardware** como se muestra en la Figura 16.2, “Configuraciones del hardware de visualización”.

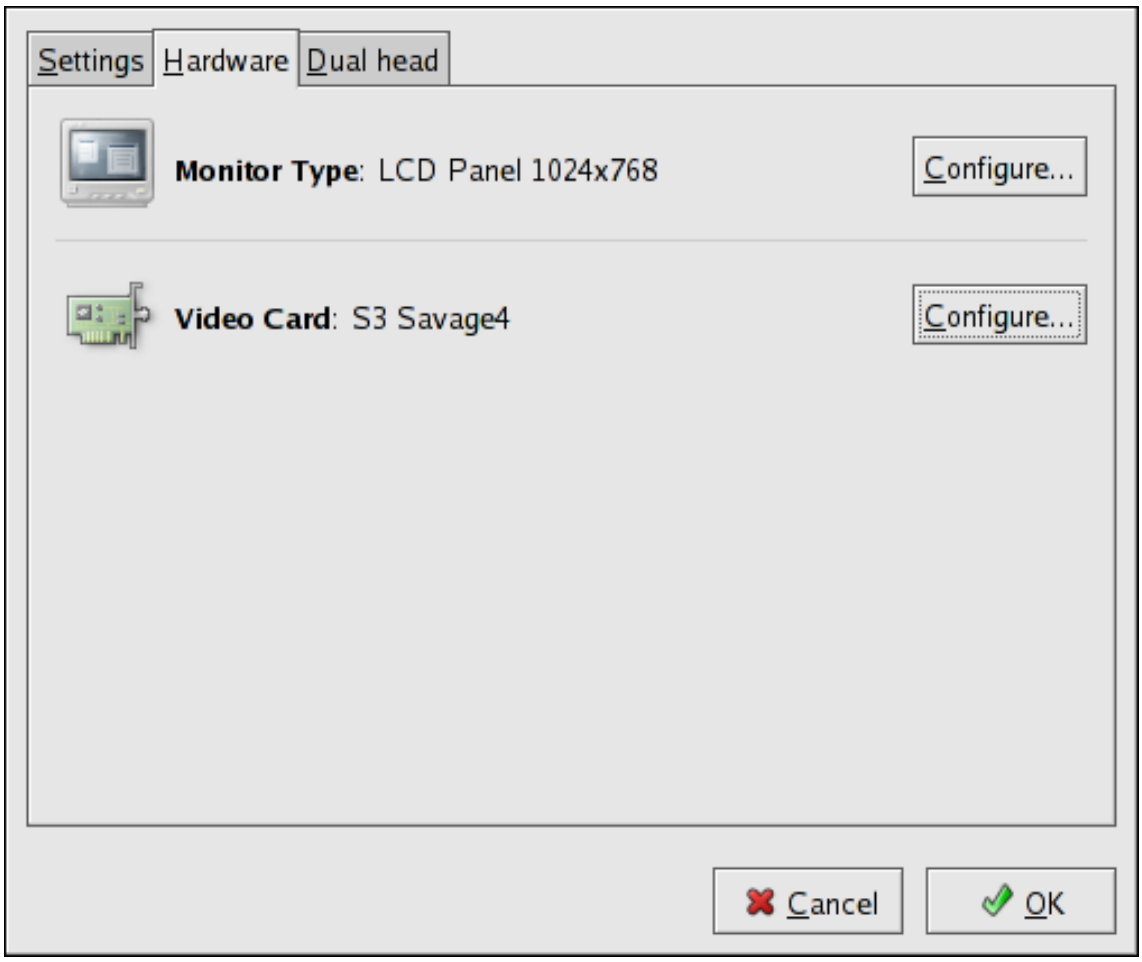


Figura 16.2. Configuraciones del hardware de visualización

Para cambiar el tipo de monitor o cualquiera de sus propiedades, haga click en el botón **Configurar** correspondiente. Para cambiar el tipo de tarjeta de vídeo o cualquiera de sus valores, haga click en el botón **Configurar** al lado de sus configuraciones.

3. Configuraciones de visualización en dos pantallas

Si varias tarjetas de vídeo son instaladas en el sistema, el soporte de dos pantallas estará disponible y podrá ser configurado a través de la pestaña **Dos pantallas** como se muestra en la Figura 16.3, “Configuraciones de visualización en dos pantallas”.

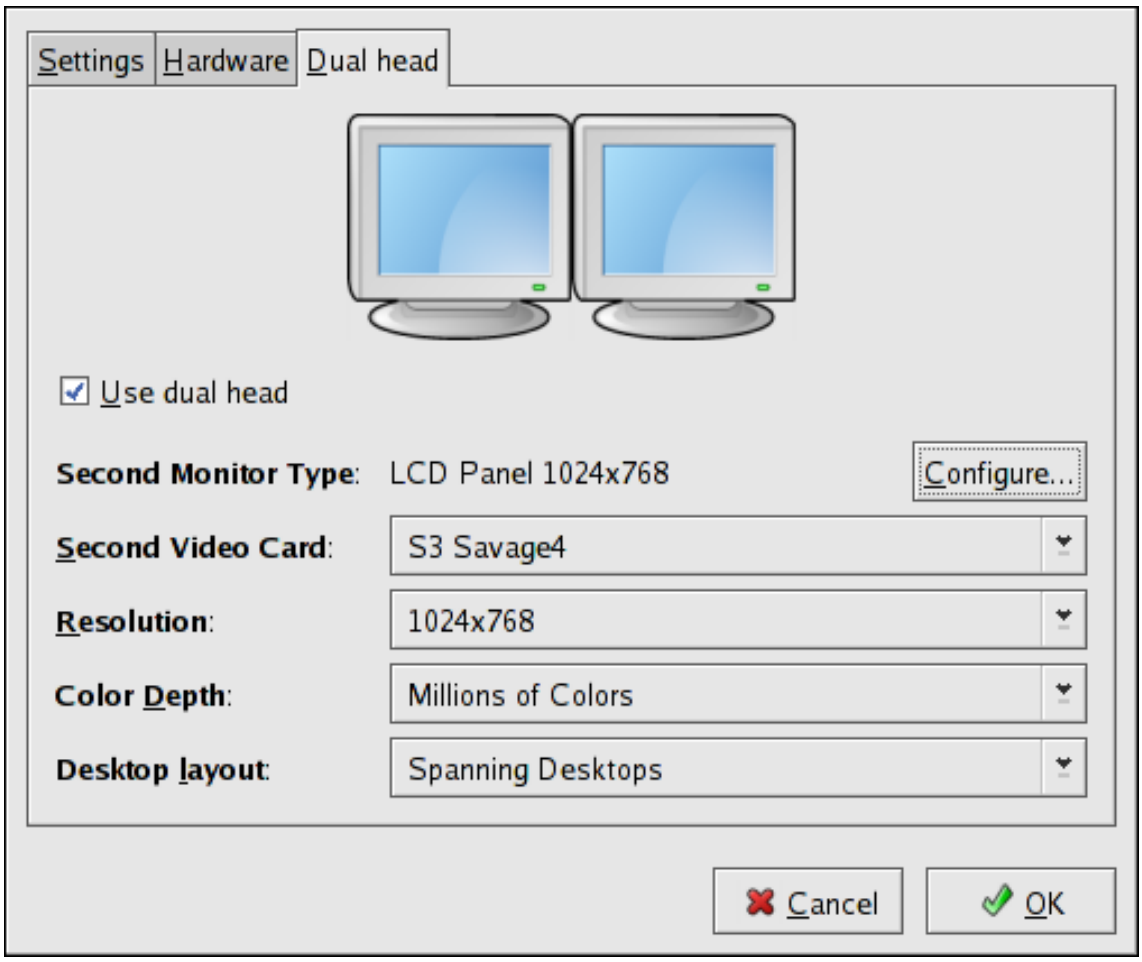


Figura 16.3. Configuraciones de visualización en dos pantallas

Para activar el uso de dos pantallas, seleccione la casilla de verificación **Utilizar dos pantallas**.

Para configurar el segundo tipo de monitor, haga clic en el botón **Configurar** correspondiente. También puede configurar los otros parámetros de visualización en dos pantallas si utiliza la lista en el menú desplegable.

Para la opción **Disposición del escritorio**, seleccione **Extendiendo escritorios** para que ambas pantallas utilicen un espacio de trabajo extendido. Seleccione **Escritorios individuales** para compartir el ratón y el teclado en las diferentes pantallas. Esta última opción restringe las ventanas a una sola pantalla.

Capítulo 17. Usuarios y grupos

El control de los *usuarios* y *grupos* es un elemento clave en la administración de sistemas de Red Hat Enterprise Linux.

Los *Usuarios* pueden ser gente real, es decir, cuentas ligadas a un usuario físico en particular, o cuentas que existen para ser usadas por aplicaciones específicas.

Los *Grupos* son expresiones lógicas de organización, reuniendo usuarios para un propósito común. Los usuarios dentro de un mismo grupo pueden leer, escribir o ejecutar archivos que pertenecen a ese grupo.

Cada usuario y grupo tiene un número de identificación único llamado *identificador de usuario* (*UID*) y un *identificador de grupo* (*GID*) respectivamente.

Un usuario que crea un archivo se convierte en el propietario y el grupo propietario de ese archivo. Al archivo también se le asignan permisos separados de lectura, escritura y ejecución para el propietario del archivo, para el grupo y para cualquier otro usuario. Solamente el superusuario (root) puede cambiar el propietario de un archivo. Los permisos de acceso pueden ser cambiados tanto por el superusuario como por el creador del archivo.

1. Configuración de grupos y de usuarios

El **Administrador de usuarios** le permite ver, modificar, añadir y borrar los usuarios y grupos locales.

Para usar el **Administrador de usuarios**, debe estar ejecutando el sistema de ventanas X, tener privilegios de root y tener el paquete RPM `system-config-users` instalado. Para iniciar el **Administrador de usuarios** desde el escritorio, vaya a System (on the panel) => **Administración** => **Usuarios y grupos**. También puede escribir el comando `system-config-users` en el intérprete del comandos (en un terminal XTerm o GNOME, por ejemplo).

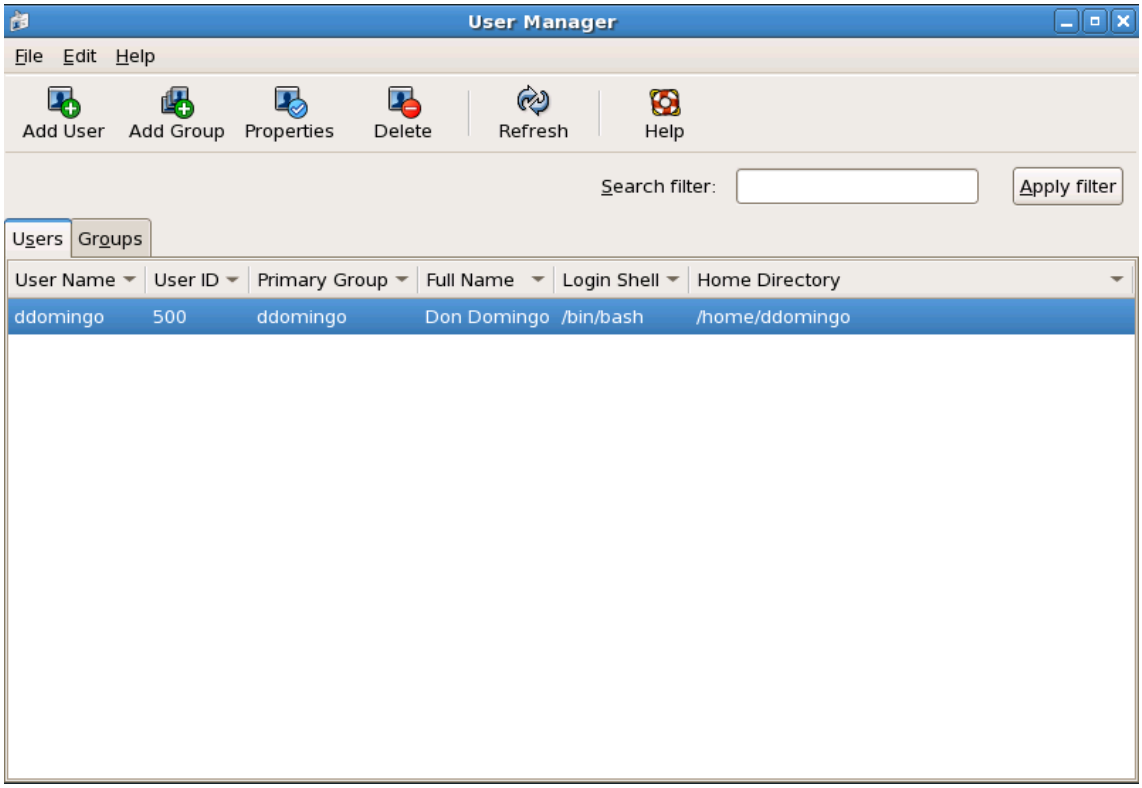


Figura 17.1. Administrador de usuarios

Para ver una lista de los usuarios locales del sistema, haga click en la pestaña **Usuarios**. Para visualizar una lista de 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 **Filtro de búsqueda**. Pulse **Intro** o pulse en el botón **Aplicar filtro**. Aparecerá la lista filtrada.

Para ordenar los usuarios o grupos, haga click en el nombre de la columna. Los usuarios o grupos son clasificados por el valor en esa columna.

Red Hat Enterprise Linux reserva los IDs de usuario por debajo de 500 para los usuarios del sistema. Por defecto, la **Administrador de usuarios** no muestra los usuarios del sistema. Para ver todos los usuarios, incluyendo los usuarios del sistema, vaya a **Editar** => **Preferencias** y anule la selección de **Ocultar usuarios y grupos del sistema**

1.1. Añadir un nuevo usuario

Para añadir un nuevo usuario, haga clic en el botón **Añadir usuario**. Aparecerá una ventana como la mostrada en la Figura 17.2, “Nuevo usuario”. 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 tener al menos seis caracteres.

Sugerencia

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 basada en un término del diccionario 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 principal**.

Si seleccionó crear el directorio principal, los archivos de configuración por defecto son copiados desde el directorio `/etc/skel` en el nuevo directorio principal.

Red Hat Enterprise 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 grupo privado 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 Enterprise Linux se reserva los IDs de usuario por debajo de 500 para los usuarios de sistemas; no es aconsejable usar números menores a 500.

Haga clic en **OK** para crear el usuario.

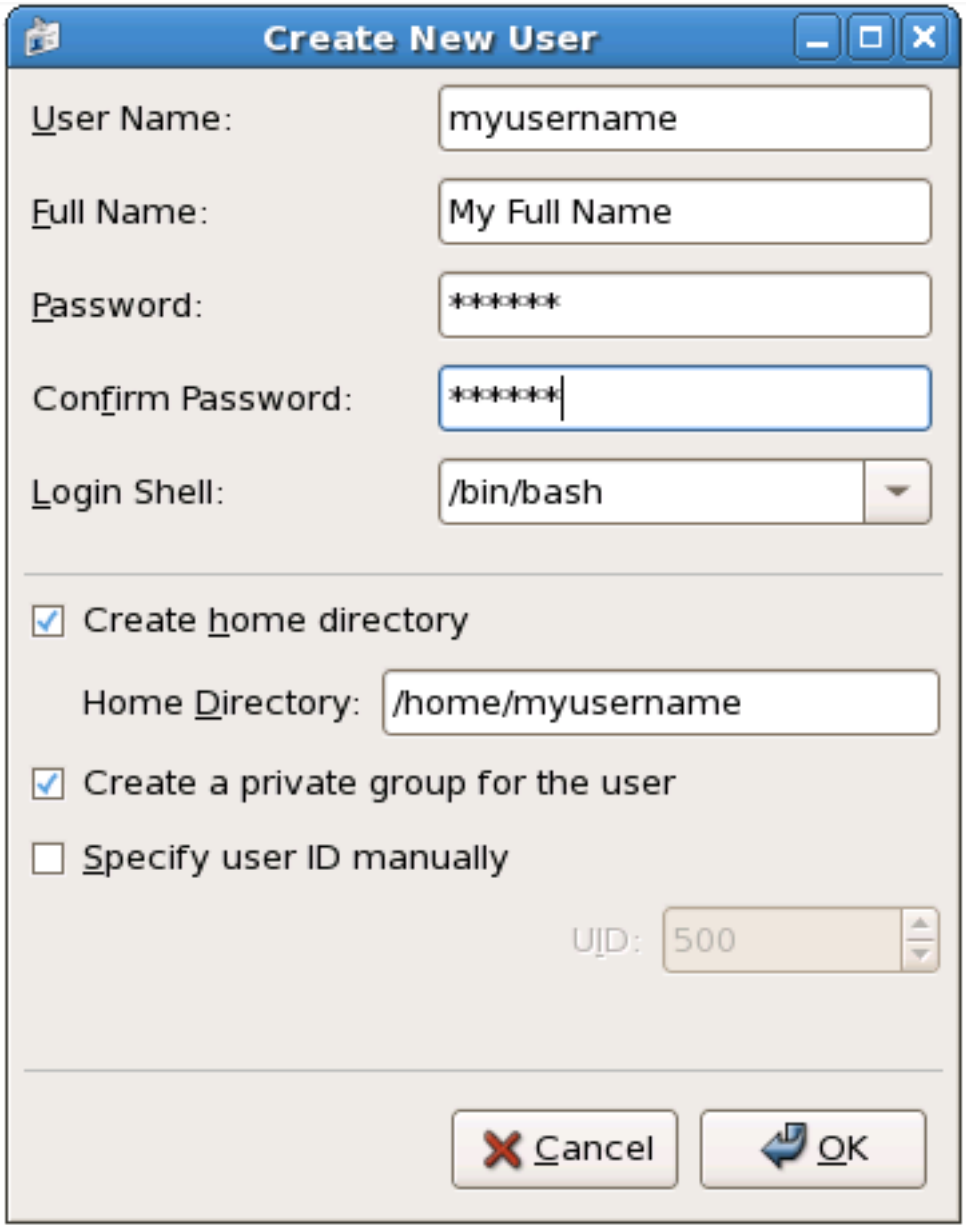


Figura 17.2. Nuevo usuario

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 1.2, “Modificar las propiedades del usuario” para más información.

1.2. Modificar las propiedades del usuario

Para ver las propiedades de un usuario ya existente, haga clic en la pestaña **Usuarios**, seleccione el usuario de la lista de usuarios y haga clic en **Propiedades** desde el menú (o escoja **Fichero** = > **Propiedades** desde el menú desplegable). Aparecerá una ventana parecida a la Figura 17.3, “Propiedades del usuario”.

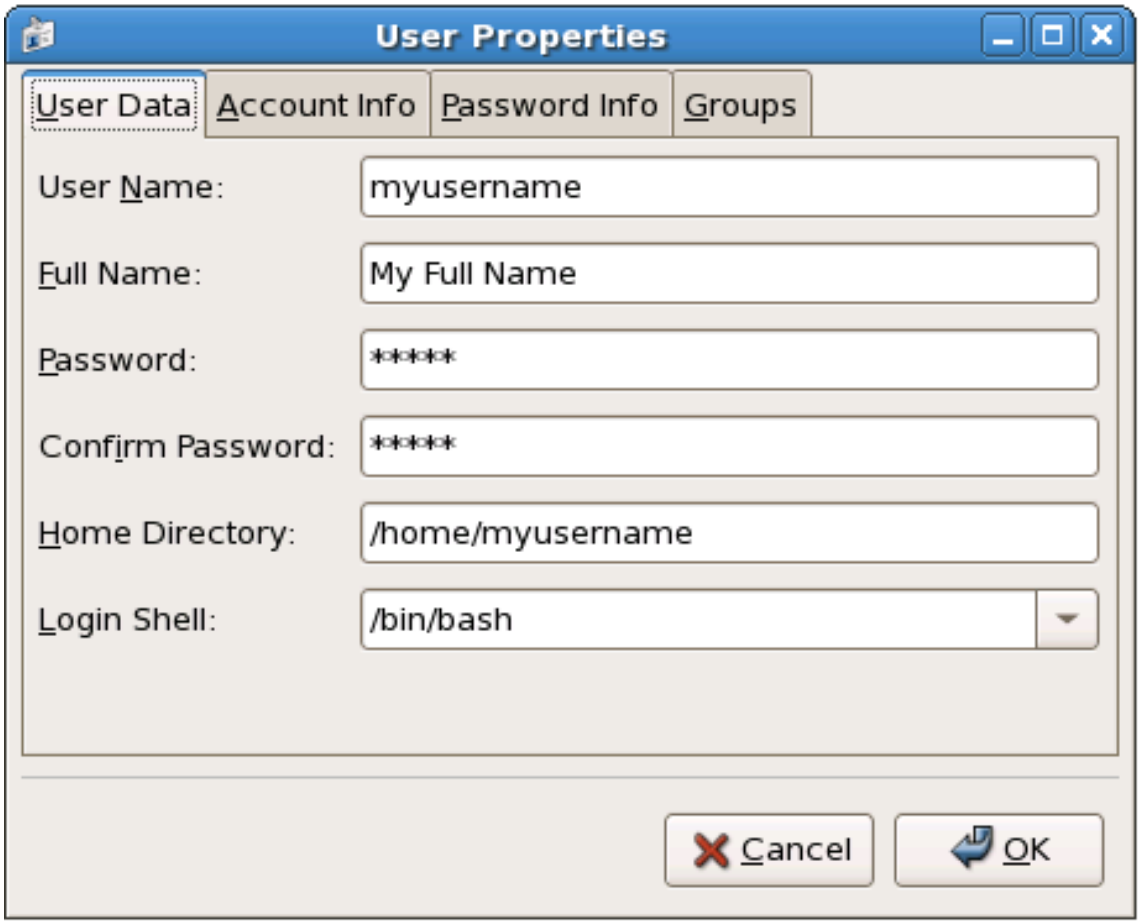


Figura 17.3. Propiedades del usuario

La ventana **Propiedades de los usuarios** está dividida en múltiples 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** e introduzca un valor en el campo **Días requeridos antes de cambiar**. Podrá establecer el número de días antes de que la contraseña del usuario caduque, 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** — Le permite ver y configurar el Grupo primario del usuario y los otros grupos a los cuales desea que el usuario pertenezca.

1.3. Añadir un nuevo grupo

Para añadir un nuevo grupo de usuarios, pulse el botón **Añadir Grupo**. Aparecerá una ventana parecida a la Figura 17.4, “Nuevo grupo”. Escriba el nombre del nuevo grupo 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 Enterprise Linux reserva los IDs de grupo menores de 500 para los grupos de sistemas.

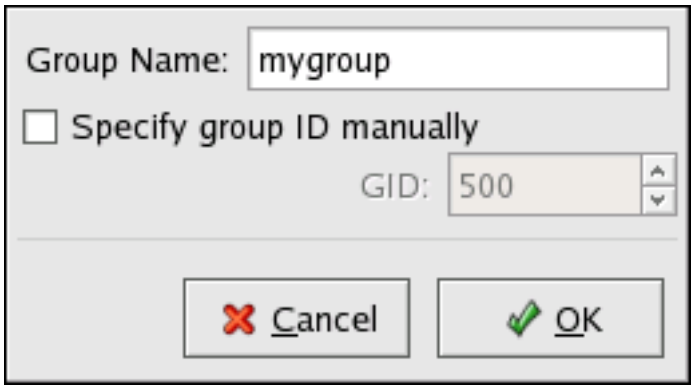


Figura 17.4. Nuevo grupo

Haga clic en **OK** para crear el grupo. Aparecerá un grupo nuevo en la lista.

1.4. 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 17.5, “Propiedades del grupo”.

Figura 17.5. Propiedades del grupo

La pestaña **Usuarios del grupo** visualiza qué usuarios son miembros del grupo. Utilice esta pestaña para añadir o borrar usuarios del grupo. Haga clic en **OK** para guardar las modificaciones.

2. Herramientas de administración de usuarios y grupos

La gestión de usuarios y grupos puede llegar a ser una tarea tediosa; es por esto que Red Hat Enterprise Linux proporciona herramientas y convenciones que facilitan su gestión.

La forma más fácil de manejar usuarios y grupos es a través de la aplicación gráfica, **Administrador de usuarios** (`system-config-users`). Para obtener mayor información sobre la **Administrador de usuarios**, consulte la Sección 1, “Configuración de grupos y de usuarios”.

Las siguientes herramientas de línea de comandos también se pueden utilizar para manejar usuarios y grupos:

- `useradd`, `usermod` y `userdel` — Métodos estándar de la industria para añadir, eliminar y modificar cuentas de usuarios.
- `groupadd`, `groupmod` y `groupdel` — Métodos estándar de la industria para añadir, eliminar y modificar grupos de usuarios.

- `gpasswd` — Un comando para administrar el archivo `/etc/group`.
- `pwck`, `grpck` — Herramientas para la verificación de contraseñas, grupo y archivos shadow asociados.
- `pwconv`, `pwunconv` — Herramientas para la conversión de contraseñas a contraseñas shadow y de vuelta a contraseñas estándar.

2.1. Configuración desde la línea de comandos

Si prefiere las herramientas de línea de comandos o no tiene el sistema X Window instalado, use esta sección para configurar usuarios y grupos.

2.2. Añadir un usuario

Para añadir un usuario al sistema:

1. Ejecute el comando `useradd` para crear una cuenta de usuario bloqueada:

   ```
   useradd <nombre-usuario>
   ```

2. Desbloquee la cuenta ejecutando el comando `passwd` para asignar una contraseña y configurar el vencimiento de la misma:

   ```
   passwd <nombre-usuario>
   ```

Las opciones de línea de comandos para `useradd` están detalladas en la Tabla 17.1, “Opciones de línea de comandos para useradd”.

Opciones	Descripción
`-c '<comentario>'`	donde `<comentario>` puede ser cualquier cadena de caracteres. Esta opción es generalmente usada para especificar el nombre completo del usuario.
`<directorio-principal -d>`	El directorio principal a ser usado en vez del directorio predeterminado `/home/<nombre-usuario>`
`-e<fecha>`	Fecha en que la cuenta será desactivada usando el formato de fecha AAAA-MM-DD
`-f<días>`	Número de días que pasarán después de que la contraseña ha caducado hasta que la cuenta se desactive. Si se especifica **`0`**, la cuenta será desactivada inmediatamente después de que la contraseña expire. Si se especifica **`-1`**, la cuenta no se desactivará después de que la contraseña caduque.
`-g<nombre-grupo>`	Nombre o número del grupo para el grupo predeterminado del usuario. El grupo debe existir antes de que sea especificado aquí.
`-G<lista-grupos>`	Lista de nombres de los grupos adicionales (además del predeterminado), separados por comas, de los cuales el usuario es miembro. Los grupos deben existir antes que sea especificado aquí.

Opciones	Descripción
`-m`	Crea el directorio principal si no existe
`-M`	No crea el directorio principal.
`-n`	No crea un grupo privado de usuario para el usuario
`-r`	Crea una cuenta de sistema con un UID menor que 500 y sin un directorio principal
`-p<contraseña>`	La contraseña encriptada con `crypt`
`-s`	Shell de registro del usuario, predeterminada a `/bin/bash`
`-u<uid>`	ID del usuario, el cual debe ser único y mayor que 499

Tabla 17.1. Opciones de línea de comandos para `useradd`

2.3. Añadir un grupo

Para agregar un grupo al sistema, use el comando `groupadd`:

```
groupadd <nombre-grupo>
```

Las opciones de la línea de comando para `groupadd` están detalladas en la Tabla 17.2, “Opciones de línea de comando para groupadd”.

Opciones	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`	Cuando se utiliza con `-g<gid>` y `<gid>` ya existe, `groupadd` escogerá otro `<gid>` único para el grupo.

Tabla 17.2. Opciones de línea de comando para `groupadd`

2.4. Vencimiento de la contraseña

Por razones de seguridad, se aconseja que los usuarios cambien sus contraseñas periódicamente. Esto se puede realizar añadiendo o editando un usuario en la pestaña **Información de la contraseña** en la **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 de las opciones de la Tabla 17.3, “Opciones de línea de comando de chage”, seguido por el nombre del usuario.

Importante

La contraseña oculta debe estar activada para poder usar el comando `chage`.

Opciones	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 el 1 de enero de 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 AAAA-MM-DD. También se puede usar el número de días transcurridos desde el 1 de enero de 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 17.3. Opciones de línea de comando de `chage`

Sugerencia

Si el comando `chage` está seguido directamente por un nombre de usuario (sin opciones), mostrará los valores de vencimiento de la contraseña actual y permitirá cambiar estos valores.

Usted puede configurar una contraseña para que caduque la primera vez que el usuario inicie una sesión. Esto obliga al usuario a cambiar la contraseña la primera vez que se registre.

Nota

Este proceso no funcionará si el usuario inicia la sesión a través del protocolo

SSH.

1. *Bloquear la contraseña del usuario* — Si el usuario no existe, use el comando `useradd` para crear la cuenta del usuario. No establezca ninguna contraseña para que la cuenta permanezca bloqueada.

   Si la contraseña ya está activa, bloquéela con el comando:

   ```
   usermod -L <nombre-usuario>
   ```

2. *Obligar el vencimiento inmediato de la contraseña* — Escriba el comando siguiente:

   ```
   chage -d 0 <nombre-usuario>
   ```

   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 Python con el comando `python`. Se mostrará lo siguiente:

  ```
  Python 2.4.3 (#1, Jul 21 2006, 08:46:09) [GCC 4.1.1 20060718 (Red Hat 4.1.1-9)] on linux2 Type "he
  ```

- En la línea de comandos, escriba lo siguiente. Reemplace `<contraseña>` con la contraseña a encriptar y `<sal>` con una combinación de exáctamente 2 caracteres en mayúsculas o minúsculas, números, el carácter punto (.) o la barra (/):

  ```
  import crypt; print crypt.crypt("<contraseña>","<sal>")
  ```

  La salida es la contraseña encriptada, similar a `12CsGd8FRcMSM`.

- Presione **Ctrl**-**D** para salir del intérprete de Python.

- En la shell, introduzca el siguiente comando (reemplazando `<contraseña-encriptada>` con el resultado dado en el intérprete de Python):

  ```
  usermod -p "<contraseña-encriptada>" <nombre-usuario>
  ```

Alternativamente, usted puede asignar una contraseña vacía en vez de la contraseña inicial. Para hacerlo, utilice el siguiente comando:

```
usermod -p "" <nombre-usuario>
```

Atención

A pesar de que el uso de una contraseña nula es conveniente tanto para el administrador como para el usuario, es una práctica insegura. Un tercero puede conectarse primero y acceder al sistema usando el número de usuario inseguro. Asegúrese de que el usuario está listo para registrarse antes de desbloquear una cuenta con una contraseña vacía.

En cualquier caso, luego de la conexión inicial, se le pedirá al usuario una nueva contraseña.

2.5. 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 el sistema está usando contraseñas ocultas.
   - Se crea un UID igual o mayor que 499. (Bajo Red Hat Enterprise Linux UIDs y GIDs debajo de 500 se reservan para uso del sistema.)
   - Se crea un GID por encima de 499.
   - La información para el GECOS óptimo se deja en blanco.
   - El directorio principal para `juan` se establece en `/home/juan/`.
   - El intérprete de comandos predeterminado se establece 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 obtener mayor información sobre los grupos de usuario privados, consulte la Sección 1.1, “Añadir un nuevo usuario”.

   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. Se crea 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/` (el cual contiene la configuración predeterminadas del usuario) se copian en el nuevo directorio `/home/juan/`.

En este punto, existe una cuenta bloqueada 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.

3. Usuarios estándar

Tabla 17.4, “Usuarios estándar” lista los usuarios estándar configurados en el archivo `/etc/passwd` por una instalación con **Todo**. El groupid (GID) en esta tabla es el *grupo primario* para el usuario. Vea la Sección 4, “Grupos estándar” para una lista de los grupos estándar.

Usuario	UID	GID	Directorio principal	Shell
root	0	0	/root	/bin/bash
bin	1	1	/bin	/sbin/nologin
daemon	2	2	/sbin	/sbin/nologin
adm	3	4	/var/adm	/sbin/nologin
lp	4	7	/var/spool/lpd	/sbin/nologin
sync	5	0	/sbin	/bin/sync
shutdown	6	0	/sbin	/sbin/shutdown
halt	7	0	/sbin	/sbin/halt
mail	8	12	/var/spool/mail	/sbin/nologin
news	9	13	/etc/news	
uucp	10	14	/var/spool/uucp	/sbin/nologin
operator	11	0	/root	/sbin/nologin
games	12	100	/usr/games	/sbin/nologin
gopher	13	30	/var/gopher	/sbin/nologin
ftp	14	50	/var/ftp	/sbin/nologin
nobody	99	99	/	/sbin/nologin
rpm	37	37	/var/lib/rpm	/sbin/nologin
vcsa	69	69	/dev	/sbin/nologin
dbus	81	81	/	/sbin/nologin
ntp	38	38	/etc/ntp	/sbin/nologin
canna	39	39	/var/lib/canna	/sbin/nologin
nscd	28	28	/	/sbin/nologin
rpc	32	32	/	/sbin/nologin
postfix	89	89	/var/spool/postfix	/sbin/nologin
mailman	41	41	/var/mailman	/sbin/nologin
named	25	25	/var/named	/bin/false
amanda	33	6	var/lib/amanda/	/bin/bash
postgres	26	26	/var/lib/pgsql	/bin/bash
exim	93	93	/var/spool/exim	/sbin/nologin
sshd	74	74	/var/empty/sshd	/sbin/nologin

Usuario	UID	GID	Directorio principal	Shell
rpcuser	29	29	`/var/lib/nfs`	`/sbin/nologin`
nsfnobody	65534	65534	`/var/lib/nfs`	`/sbin/nologin`
pvm	24	24	`/usr/share/pvm3`	`/bin/bash`
apache	48	48	`/var/www`	`/sbin/nologin`
xfs	43	43	`/etc/X11/fs`	`/sbin/nologin`
gdm	42	42	`/var/gdm`	`/sbin/nologin`
htt	100	101	`/usr/lib/im`	`/sbin/nologin`
mysql	27	27	`/var/lib/mysql`	`/bin/bash`
webalizer	67	67	`/var/www/usage`	`/sbin/nologin`
mailnull	47	47	`/var/spool/mqueue`	`/sbin/nologin`
smmsp	51	51	`/var/spool/mqueue`	`/sbin/nologin`
squid	23	23	`/var/spool/squid`	`/sbin/nologin`
ldap	55	55	`/var/lib/ldap`	`/bin/false`
netdump	34	34	`/var/crash`	`/bin/bash`
pcap	77	77	`/var/arpwatch`	`/sbin/nologin`
radiusd	95	95	`/`	`/bin/false`
radvd	75	75	`/`	`/sbin/nologin`
quagga	92	92	`/var/run/quagga`	`/sbin/login`
wnn	49	49	`/var/lib/wnn`	`/sbin/nologin`
dovecot	97	97	`/usr/libexec/dovecot`	`/sbin/nologin`

Tabla 17.4. Usuarios estándar

4. Grupos estándar

Tabla 17.5, “Grupos estándar” lista los grupos estándar configurados por una instalación con **Todo**. Los grupos son almacenados en el archivo `/etc/group`.

Grupo	GID	Miembros
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon

Grupo	GID	Miembros
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail, postfix, exim
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
usuarios	100	
rpm	37	
utmp	22	
floppy	19	
vcsa	69	
dbus	81	
ntp	38	
canna	39	
nscd	28	
rpc	32	
postdrop	90	
postfix	89	

Grupo	GID	Miembros
mailman	41	
exim	93	
named	25	
postgres	26	
sshd	74	
rpcuser	29	
nfsnobody	65534	
pvm	24	
apache	48	
xfs	43	
gdm	42	
htt	101	
mysql	27	
webalizer	67	
mailnull	47	
smmsp	51	
squid	23	
ldap	55	
netdump	34	
pcap	77	
quaggavt	102	
quagga	92	
radvd	75	
slocate	21	
wnn	49	
dovecot	97	
radiusd	95	

Tabla 17.5. Grupos estándar

5. Grupos de usuario privado

Red Hat Enterprise Linux utiliza un esquema de *grupo privado de usuario* (*UPG*), lo que hace más fácil de manejar los grupos de UNIX.

Se crea un UPG siempre que se añade un nuevo usuario al sistema. Un UPG tiene el mismo nombre que el usuario para el cual se crea y ese usuario es el único miembro de ese UPG.

Los UPGs hacen que sea más seguro configurar los privilegios por defecto para un nuevo archivo o directorio. Esto permite a ambos, tanto al usuario como al *grupo de ese usuario* hacer modificaciones al archivo o directorio.

El parámetro que determina qué permisos son aplicados a un nuevo archivo o directorio es llamado un *umask* y se configura en el archivo `/etc/bashrc`. Tradicionalmente en sistemas UNIX, el `umask` es configurado a `022`, lo que sólo permite al usuario que creó el archivo o directorio realizar modificaciones. Bajo este esquema, todos los demás usuarios *incluyendo miembros del grupo del creador* no tienen derecho a realizar ninguna modificación. Sin embargo, bajo el esquema UPG, esta "protección de grupo" no es necesaria puesto que cada usuario tiene su propio grupo privado.

5.1. Directorios de grupos

Muchas organizaciones de Tecnologías de Información prefieren crear un grupo para cada proyecto importante y luego asignar personas al grupo si estos necesitan acceso a los archivos de ese proyecto. Usando este esquema tradicional, el manejo de archivos ha sido difícil pues cuando alguien crea un archivo, este es asociado con el grupo primario al cual ellos pertenecen. Cuando una persona individual trabaja en múltiples proyectos, se hace difícil asociar los archivos correctos con el grupo correcto. Usando el esquema UPG, sin embargo, los grupos son automáticamente asignados a archivos creados dentro de un directorio con el bit *setgid* configurado. El bit setgid hace muy simple el manejo de proyectos de grupos que comparten un directorio común, pues cualquier archivo creado dentro del directorio es propiedad del grupo que posee el directorio.

Digamos, por ejemplo, que un grupo de personas trabajan con archivos en el directorio `/usr/lib/emacs/site-lisp/`. Algunas personas son de confianza y pueden modificar el directorio, pero ciertamente no todos. Entonces, primero cree un grupo `emacs`, como se muestra en el siguiente comando:

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

Para asociar los contenidos del directorio con el grupo `emacs`, escriba:

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

Ahora es posible añadir los usuarios adecuados al grupo con el comando `gpasswd`:

```
/usr/bin/gpasswd -a <nombre-usuario> emacs
```

Para permitir que los usuarios creen archivos dentro del directorio, utilice el comando siguiente:

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

Cuando un usuario crea un nuevo archivo, se le asigna el grupo del grupo por defecto privado del usuario. Luego, configure el bit setgid, el cual asigna que todo lo que se cree en el directorio la misma permisología de grupo del directorio mismo (`emacs`). Use el comando siguiente:

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

En este punto, puesto que cada usuario tiene por defecto su umask en 002, todos los miembros del grupo `emacs` pueden crear y modificar archivos en el directorio `/usr/lib/emacs/site-lisp/` sin que el administrador tenga que cambiar los permisos de los archivos cada vez que un usuario escriba nuevos archivos.

6. Contraseñas Shadow

En entornos multiusuario es muy importante utilizar *contraseñas shadow* también conocido como *Oscurecimiento de contraseñas*, (proporcionadas por el paquete `shadow-utils`). Haciendo esto se mejora la seguridad de los archivos de autenticación del sistema. Por esta razón, el programa de instalación activa por defecto las contraseñas shadow.

Lo siguiente es una lista de las ventajas de las contraseñas shadow sobre el método tradicional de almacenar contraseñas en los sistemas basados en UNIX:

- Mejora la seguridad del sistema al mover las contraseñas encriptadas desde el archivo `/etc/passwd` que puede leer todo el mundo, a `/etc/shadow`, el cual sólo puede ser leído por el usuario root.
- Almacena información sobre la vigencias de las contraseñas.
- Permite el uso del archivo `/etc/login.defs` para reforzar las políticas de seguridad.

La mayoría de las utilidades proporcionadas por el paquete `shadow-utils` funcionan adecuadamente sin importar si las contraseñas shadow están activadas o no. Sin embargo, puesto que la información sobre la vigencia de las contraseñas es almacenada exclusivamente en el archivo `/etc/shadow`, cualquier comando que cree o modifique la información sobre la vigencia de las contraseñas, no funcionará.

Abajo se muestra una lista de los comandos que no funcionan a menos que se activen primero las contraseñas shadow:

- `chage`
- `gpasswd`
- Las opciones `/usr/sbin/usermod -e` o `-f`
- Las opciones `/usr/sbin/useradd -e` o `-f`

7. Recursos adicionales

Para más información sobre usuarios y grupos y las herramientas para administrarlos, consulte los recursos siguientes.

7.1. Documentación instalada

- Páginas man relacionadas — Hay varias páginas man para las diferentes aplicaciones y archivos de configuración relacionados con el manejo de usuarios y grupos. La siguiente es una lista de algunas de las páginas más importantes:

  Aplicaciones administrativas de usuarios y grupos

  - `man chage` — Un comando para modificar las políticas de vigencia y expiración de las cuentas.
  - `man gpasswd` — Un comando para administrar el archivo `/etc/group`.
  - `man groupadd` — Un comando para añadir grupos.
  - `man grpck` — Un comando para verificar el archivo `/etc/group`.
  - `man groupdel` — Un comando para eliminar grupos.
  - `man groupmod` — Un comando para modificar la membrecía de grupos.
  - `man pwck` — Comando que se utiliza para verificar los archivos `/etc/passwd` y `/etc/shadow`.
  - `man pwconv` — Una herramienta para la conversión de contraseñas estándar a contraseñas shadow.
  - `man pwunconv` — Una herramienta para la conversión de contraseñas shadow a contraseñas estándar.
  - `man useradd` — Un comando para añadir usuarios.
  - `man userdel` — Un comando para eliminar usuarios.
  - `man usermod` — Comando para modificar usuarios.

  Archivos de configuración

  - `man 5 group` — El archivo que contiene información del grupo para el sistema.
  - `man 5 passwd` — El archivo que contiene información del usuario para el sistema.
  - `man 5 shadow` — El archivo que contiene información de contraseñas y vigencia de cuentas para el sistema.

Capítulo 18. 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 o cuando el promedio de carga del sistema está por debajo de un número dado. Red Hat Enterprise Linux es preconfigurado para ejecutar determinadas tareas del sistema de modo que éste se mantenga actualizado. Por ejemplo, la base de datos slocate utilizada por el comando `locate`,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 Enterprise Linux contiene varias utilidades de tareas automáticas: `cron`, `at` y `batch`.

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 encendido de forma continua. Si el sistema no está activo cuando está programada una tarea, Cron no se ejecuta. Para programar tareas que se ejecutan una sola vez, consulte la Sección 2, “At y Batch”.

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`.

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 usadas para configurar el entorno en el cual 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 archivo `/etc/crontab` representa una tarea y tiene el formato siguiente:

```
minuto   hora   día   mes   díaDeLaSemana   comando
```

- `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 un comando propiamente dicho como `ls /proc >> /tmp/proc` o el comando para ejecutar un script personalizado.)

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 oblícua (/) puede utilizarse para especificar valores de salto. El valor de un número entero se puede saltar dentro de un rango si se indica a continuación del rango con ***`/<número entero>`***. Por ejemplo, **`0-59/2`** puede usarse para definir cada otro minuto en el campo minuto. Los valores de salto también pueden utilizarse con un asterisco. Por ejemplo, el valor **`*/3`** puede usarse en el campo de mes para ejecutar la tarea cada tercer mes.

Las líneas que empiezan por almohadilla o símbolo numeral (#) son comentarios y no se procesan.

Como se muestra en el archivo `/etc/crontab`, el script `run-parts` ejecuta 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 archivos en 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`. Vaya al Ejemplo 18.1, “Ejemplos de Crontab” para ver más ejemplos.

```
# Registra el uso de memoria del sistema cada lunes
# a las 3:30AM en el archivo /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# Ejecuta el script personalizado el primer día de cada mes a las 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

Ejemplo 18.1. 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 cargan en la memoria. De este modo, el demonio no necesita ser reiniciado si se cambia un fichero crontab.

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, a todos los usuarios listados en `cron.deny` no se les permite usar cron.

2. At y Batch

Mientras que cron es utilizado para programar tareas recurrentes, 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 única tarea cuando la carga promedio de los sistemas esten por debajo de 0.8.

Para poder usar `at` o `batch` debe tener el paquete RPM `at` instalado y el servicio `atd` en funcionamiento. Para determinar si el paquete está instalado, utilice el comando `rpm -q at`. Para determinar si el servicio se está ejecutando,utilice el comando `/sbin/service atd status`.

2.1. 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 señala las 4:00AM. Si se inserta el tiempo, se ejecuta en la hora específica del siguiente día.
- midnight — Especifica 12:00 a.m.

- noon — Especifica 12:00 p.m.
- teatime — Especifica las 4:00 p.m.
- 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 2002.
- now + time — el tiempo está en minutos, horas, días o semanas. Por ejemplo, now + 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 2.3, “Visualización de las tareas pendientes” para más información.

El uso del comando `at` puede ser restringido. Remítase a la Sección 2.5, “Control de acceso a At y Batch” para más detalles.

2.2. 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 2.3, “Visualización de las tareas pendientes” para más información.

El uso del comando `batch` puede ser restringido. Remítase a la Sección 2.5, “Control de acceso a At y Batch” para más detalles.

2.3. Visualización de las tareas pendientes

Para visualizar las tareas pendientes `at` y `batch`, use el comando `atq`. Muestra una lista de las tareas pendientes, con cada trabajo en una línea. Cada línea sigue el formato de número de tarea, la fecha, la hora, el tipo de tarea y 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 de todos los usuarios.

2.4. 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 18.1. Opciones de línea de comandos `at` y `batch`

2.5. 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 los usuarios listados en `at.deny` no se les permitirá usar `at` o `batch`.

3. Recursos adicionales

Para obtener más información sobre cómo configurar tareas automáticas, consulte los recursos siguientes.

3.1. 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 de manual `at` — descripción de `at` y `batch` y las opciones de la línea de comandos.

Capítulo 19. 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`.

1. Localizar archivos de registro

La mayoría de los archivos de registro 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 registro (log).

Encontrará multiples archivos con números en el directorio de archivos de registro. Estos se crean cuando se rotan los archivos de registro. Los archivos de registro se rotan para que los tamaños de los archivos no se vuelvan muy grandes. El paquete `logrotate` contiene una tarea cron que rota automáticamente los archivos de registro de acuerdo con el archivo de configuración `/etc/logrotate.conf` y los archivos de configuración en el directorio `/etc/logrotate.d/`. Por defecto se encuentra configurado para rotar todas las semanas y mantener cuatro semanasde archivos de registro previos.

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 ver los archivos de registro del sistema en una aplicación en tiempo real e interactiva utilice **System Log Viewer**. Para iniciar la aplicación a **Aplicaciones** (el menú principal en el panel) => **Sistema** => **Registros de Sistema**, o escriba el comando `gnome-system-log` en el intérprete de comandos.

La aplicación sólo muestra los archivos de registro que existen; por lo tanto, la lista puede ser diferente a la que aparece en la Figura 19.1, “Sistema de Registro”.

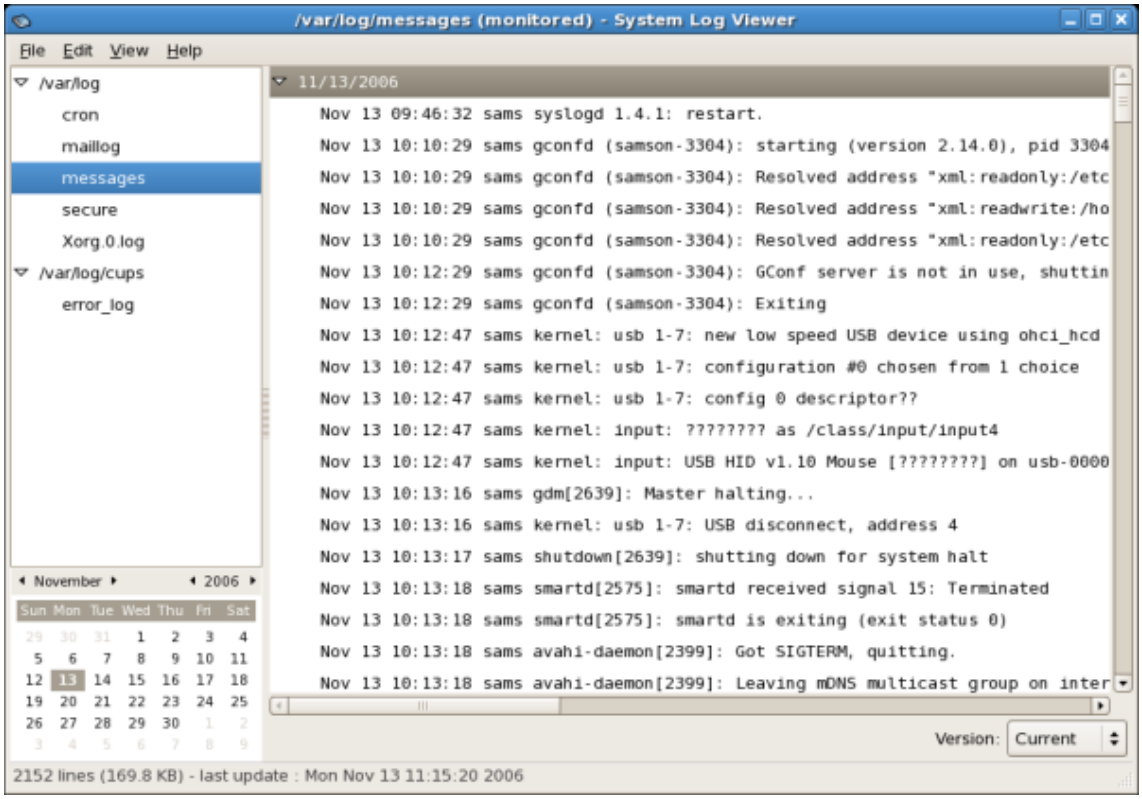


Figura 19.1. Sistema de Registro

Para filtrar el contenido de un archivo de registro seleccionado haga click en **Vista** desde el menú y seleccione **Filtro** como se meustra a continuación.

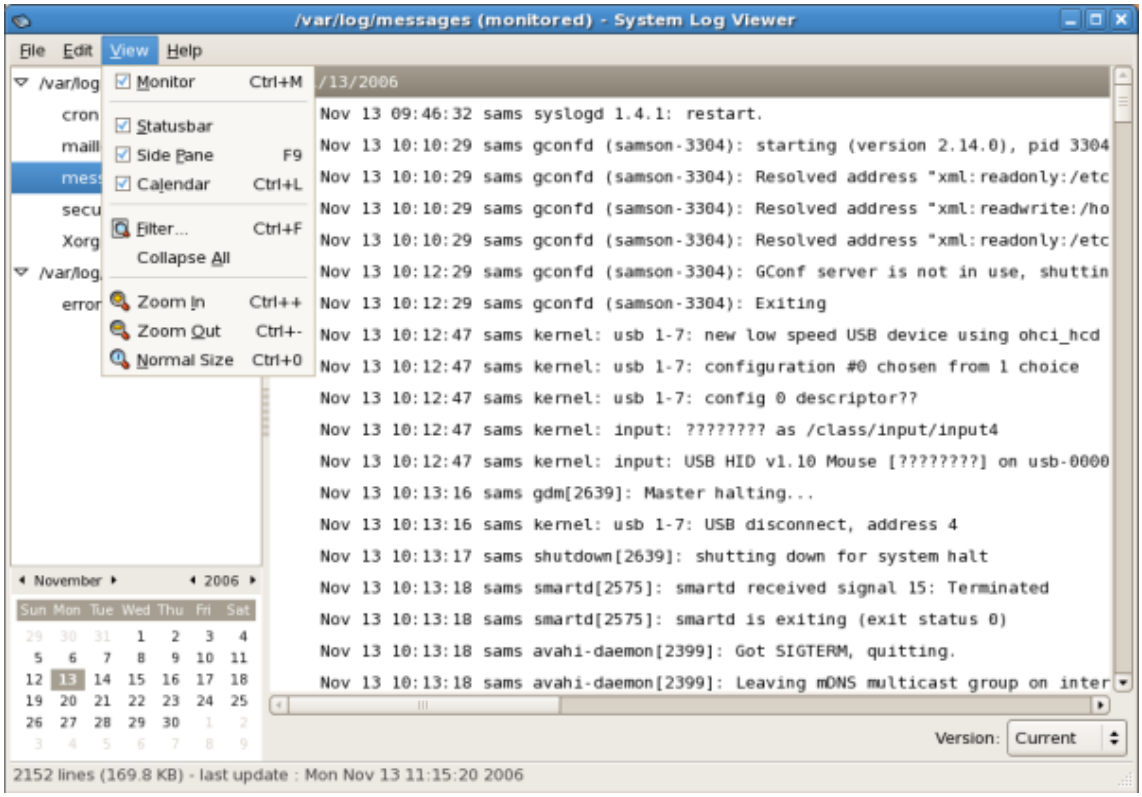


Figura 19.2. Registro del Sistema - Menú Vista

Al seleccionar en el menú **Filtro** esto mostrará el campo de texto **Filter** en donde puede escribir las palabras que desea utilizar para su filtro. Para dejar el filtro en blanco haga click en el botón **Borrar**. La figura a continuación muestra un filtro de ejemplo:

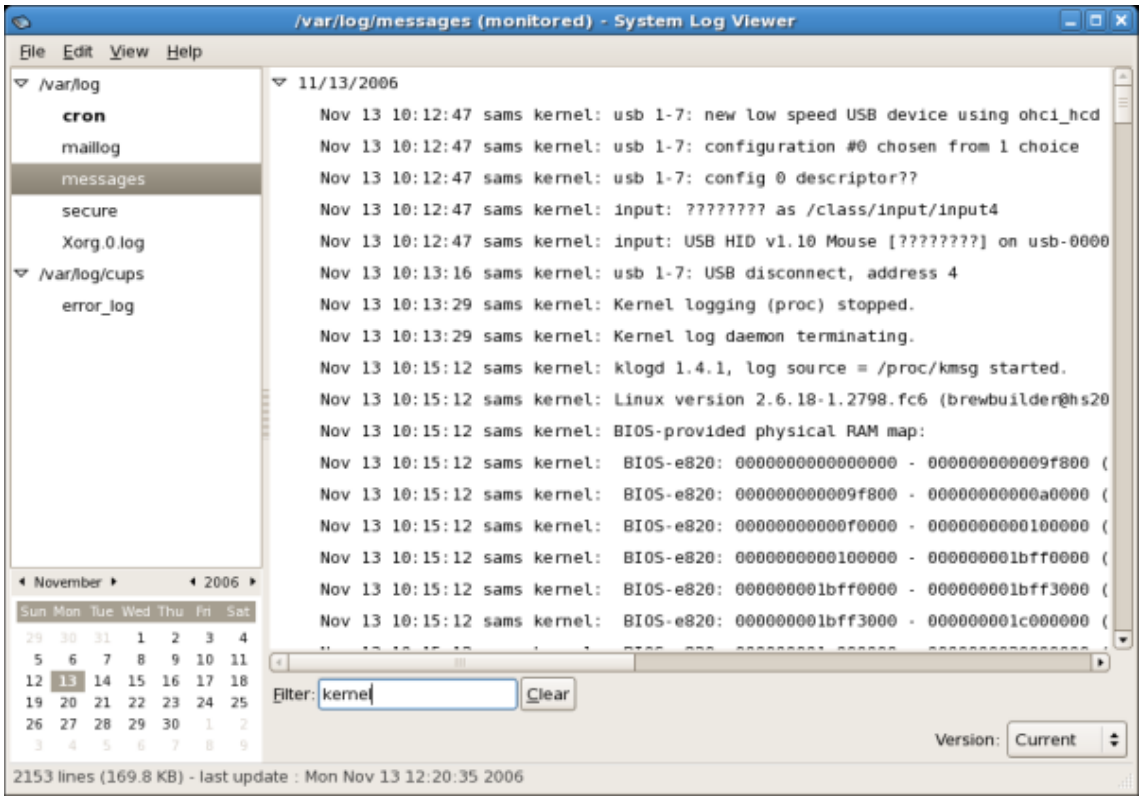


Figura 19.3. Sistema de Registro - Filtro

3. Añadir un archivo de registro

Para añadir un archivo de registro para poder verlo en la lista seleccione **Archivo** => **Abrir**. Aparecerá la ventana **Abrir Registro** en donde podrá seleccionar el directorio y el nombre del archivo del archivo de registro que desea ver. La figura a continuación muestra la ventana **Abrir Registro**.

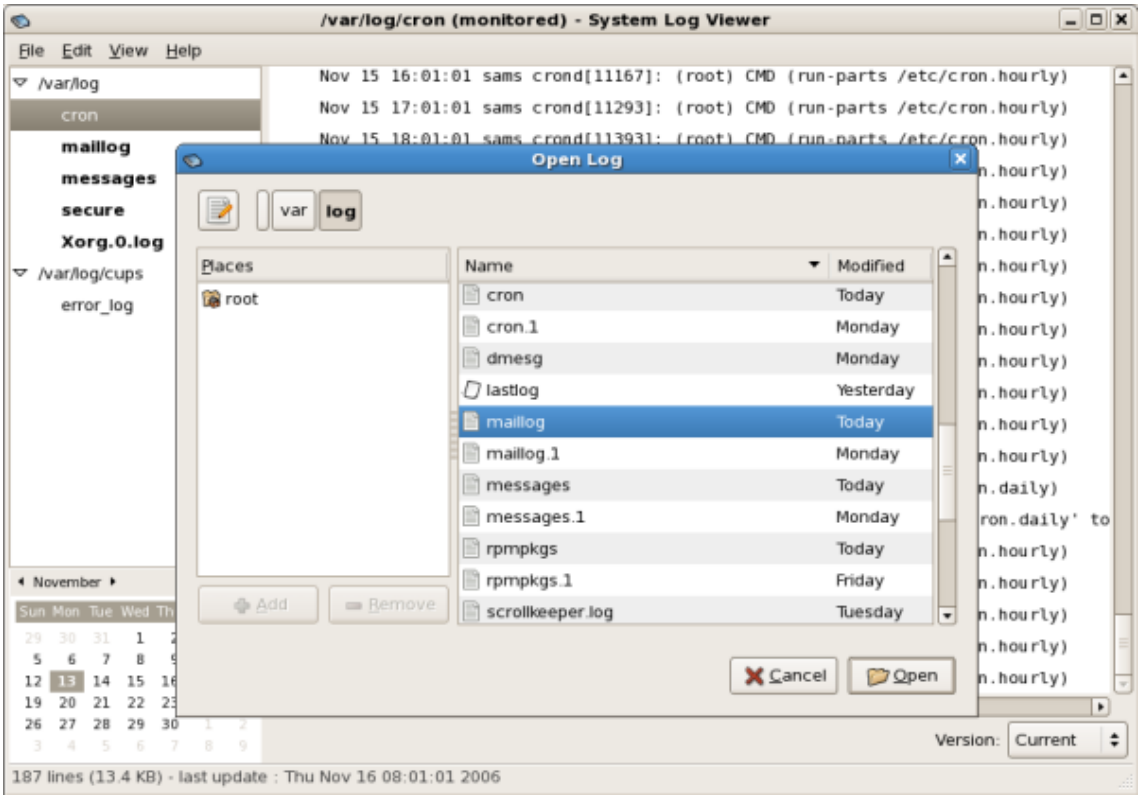


Figura 19.4. Añadir un archivo de registro

Haga click en el botón **Abrir** para abrir este archivo. El archivo es añadido inmediatamente a la lista en donde puede seleccionarlo y ver el contenido.

Observe también que el Registro de Sistema le permite abrir registros comprimidos cuyos nombres terminan en ".gz".

4. Control de Archivos de Registro

Registro del Sistema por defecto monitorea todos los registros abiertos. Si se le añade una línea nueva a un archivo de registro monitoreado, el nombre de registro aparece en negrilla en la lista de registros. Si el archivo de registro es seleccionado, las nuevas líneas aparecerán en negrilla al final del archivo de registro y pasados cinco minutos aparecerán en formato normal. La siguiente figura ilustra esto y muestra una nueva alerta en el archivo de registro **mensajes**. El archivo de registro aparece en negrilla en la lista.

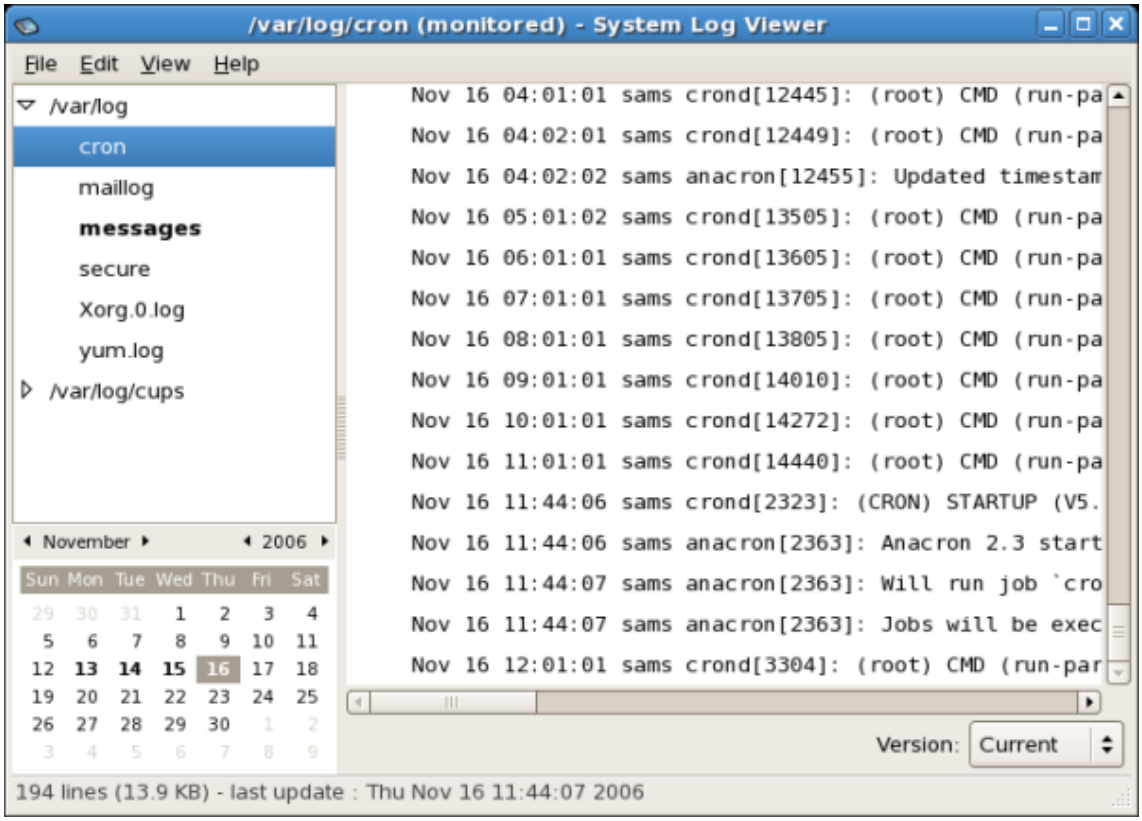


Figura 19.5. Alerta del Archivo de Registro

Al hacer click en el archivo de registro de **messages** aparecerán los registros en el archivo con las nuevas líneas en negrilla como se muestra a continuación:

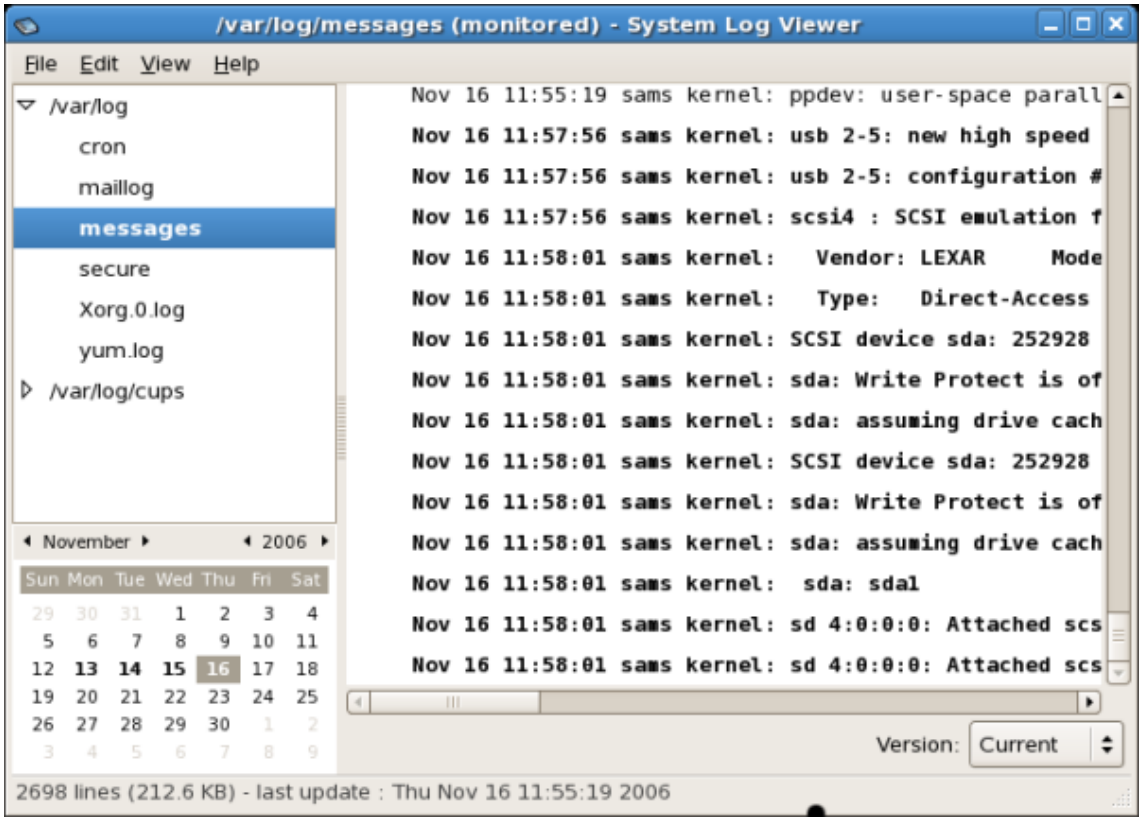


Figura 19.6. Contenido del archivo de registro

Las nuevas líneas se presentan en negrilla durante cinco segundos y después aparecen en letra normal.

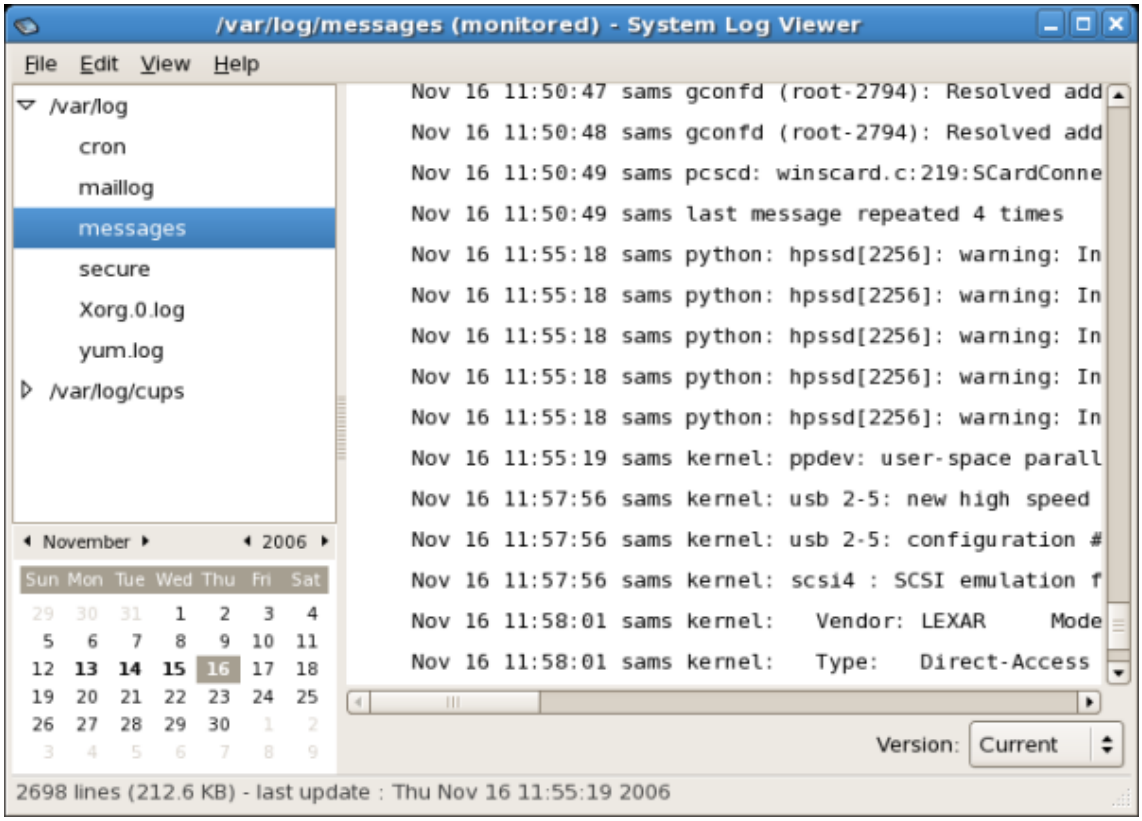


Figura 19.7. Contenido del archivo de registro después de cinco segundos

Parte III. Seguridad y autenticación

Ya sea que los administradores necesiten asegurar los sistemas de misión crítica, servicios o datos, Red Hat Enterprise Linux proporciona una variedad de herramientas y métodos que pueden formar parte de una estrategia de seguridad completa.

Este capítulo proporciona una introducción general acerca de la seguridad, especialmente en las particularidades de los sistemas Red Hat Enterprise Linux. Proporciona información conceptual sobre las áreas de evaluaciones de seguridad, vulnerabilidades comunes, intrusión y respuesta a incidentes. También proporciona información de configuración específica y conceptual para mejorar la seguridad en las estaciones de trabajo, servidores, VPN, cortafuegos y otras implementaciones utilizando SELinux.

Este capítulo asume un conocimiento básico de seguridad informática y, consecuentemente, cubre someramente prácticas comunes de seguridad como el control de acceso físico, cumplimiento de procedimientos y políticas, auditorías, etc. En donde sea apropiado, se harán referencias a recursos externos para esta y otra información relacionada.

Capítulo 20. Generalidades concernientes a la seguridad

Debido a la creciente confianza que se tiene en las poderosas computadoras conectadas en redes para ayudar a los negocios y para llevar un seguimiento de nuestra información personal, las industrias se forman alrededor de las prácticas de seguridad de la computación y de las redes. Las corporaciones solicitan el conocimiento y las habilidades de los expertos en seguridad para auditar los sistemas y ajustar soluciones que satisfagan los requerimientos operativos de la organización. Ya que la mayoría de las organizaciones son dinámicas por naturaleza, con empleados que acceden a los recursos informáticos de la organización tanto local como remotamente, la necesidad de ambientes computacionales seguros es cada vez más relevante.

Desafortunadamente, la mayoría de las organizaciones (así como los usuarios individuales) consideran la seguridad en un segundo plano, dándole mayor importancia al poder, productividad y preocupaciones presupuestarias. La implementación adecuada de la seguridad es a menudo realizada *postmortem* — después de que ocurre una intrusión no autorizada. Los expertos de seguridad consideran que el establecimiento de medidas adecuadas antes de conectar un sitio a una red insegura tal como la Internet, es una forma efectiva de frustrar la mayoría de los intentos de intrusión.

1. Evaluación de vulnerabilidad

Con el tiempo suficiente, los recursos y la motivación, un intruso puede violar casi cualquier sistema. Al final del día, todos los procedimientos de seguridad y la tecnología disponible actualmente no pueden garantizar que sus sistemas estén seguros de un ataque. Los enrutadores lo pueden ayudar a asegurar sus puertas de enlace (gateways) a la Internet. Los cortafuegos (firewalls) le permiten asegurar el borde de su red. Las redes privadas virtuales pueden pasar con seguridad sus datos en un flujo encriptado. Los sistemas de detección de intrusos pueden advertirlo de actividades maliciosas. Sin embargo, el éxito de cada una de estas tecnologías depende de un número de variables, incluyendo:

- La experiencia del personal responsable de la configuración, supervisión y mantenimiento de las tecnologías.
- La habilidad de remendar y actualizar servicios y kernels rápida y eficientemente.
- La habilidad de aquellos responsables de mantener vigilancia constante sobre la red.

Dado el estado dinámico de los sistemas de datos y tecnologías, asegurar sus recursos corporativos puede ser bien complejo. Debido a esta complejidad, puede ser difícil encontrar recursos expertos para todos sus sistemas. Mientras que es posible tener personal con conocimientos en muchas áreas de seguridad de información a un nivel alto, es difícil mantener personal que sea experto en más de unas pocas áreas particulares. Esto se debe principalmente a que cada área en particular de seguridad de la información requiere constante atención y foco. La seguridad de información no se queda quieta.

1.1. Pensando como el enemigo

Imagine que usted administra una red corporativa. Tales redes usualmente estan formadas de sistemas operativos, aplicaciones, servidores, monitores de red, cortafuegos, sistemas de detección de intrusos y más. Ahora imagínese el tratar de mantenerse actualizado con cada uno de estos. Dada la complejidad de los ambientes de software y de redes de hoy, los ataques y los bugs son una posibilidad constante. El tratar de mantenerse actualizado con las mejoras y actualizaciones para la red completa puede ser una tarea abrumadora cuando se trata de una organización grande y con sistemas heterogéneos.

Combine los requerimientos de experiencia con la tarea de mantenerse actualizado y es inevitable que incidentes adversos ocurrirán, habrá sistemas violados, se perderán datos y se interrumpe el servicio.

Para incrementar su tecnología de seguridad y ayudar a proteger los sistemas, redes y datos, piense como un cyberpirata (cracker) y estime la seguridad de los sistemas revisando sus debilidades. Las evaluaciones de vulnerabilidad preventivas contra sus propios sistemas y recursos de red pueden revelar problemas potenciales que se pueden solucionar antes de que un cyberpirata los descubra.

Si usted tuviese que realizar una evaluación de la vulnerabilidad de su hogar, probablemente verificará cada puerta de su casa para ver si estas se encuentran cerradas y aseguradas. Quizás también verificará cada ventana, asegurándose de que estas se encuentren bien cerradas y con seguro. Este mismo concepto aplica a los sistemas, redes y datos electrónicos. Los usuarios maliciosos son los ladrones y vándalos de sus datos. Fíjese en sus herramientas, mentalidad y motivaciones y podrá responder rápidamente a sus acciones.

1.2. Definición de la evaluación y pruebas

Las evaluaciones de vulnerabilidad se pueden dividir en dos grandes categorias: *Desde afuera viendo hacia adentro* y *Desde adentro viendo alrededor*.

Cuando se lleva a cabo una evaluación de vulnerabilidad desde el exterior, usted está tratando de comprometer sus sistemas desde afuera. Al posicionarse desde afuera de la compañía puede ver las cosas desde el punto de vista del intruso. Usted ve lo que un intruso ve — direcciones IP públicas, sistemas en su *DMZ*, las interfaces externas de su cortafuegos y más. DMZ viene de "zona desmilitarizada" lo que corresponde a un computador o a una pequeña subred que se coloca entre la red confiable interna, tal como la LAN corporativa, y una red externa no confiable, tal como la Internet. Típicamente, la DMZ contiene dispositivos accesibles al tráfico de la Internet, tal como servidores Web (HTTP), FTP, SMTP (correo electrónico) y servidores DNS.

Cuando realiza una evaluación de vulnerabilidad desde adentro, de alguna forma usted tiene una ventaja puesto que ya está adentro y su estatus es elevado y de confianza. Este es el punto de vista suyo y de sus compañeros de trabajo una vez que se conectan a los sistemas. Puede ver los servidores de impresión, servidores de archivos, bases de datos y otros recursos.

Hay diferencias importantes entre estos dos tipos de evaluación de vulnerabilidad. Por el hecho de ser parte de la compañía, usted tiene mayores privilegios que cualquier persona del exterior. Hoy día, en la mayoría de las organizaciones, la seguridad es configurada para mantener a los intrusos afuera. Se hace muy poco para asegurar la parte interna de la organización (tales como cortafuegos departamentales, controles de acceso a nivel de usuario, procedimientos de autenticación para recursos internos y más). Típicamente, hay muchos más recursos cuando

se mira desde adentro, ya que la mayoría de los recursos son internos a la compañía. Una vez que se encuentra fuera de la compañía, inmediatamente se le da la condición de no fiable. Los sistemas y recursos que tiene disponibles son generalmente mucho más limitados.

Considere la diferencia entre las evaluaciones de vulnerabilidad y las *pruebas de penetración*. Piense en una evaluación de vulnerabilidad como el primer paso de una prueba de penetración. La información reunida a partir de la evaluación será usada en las pruebas. Mientras que la evaluación de vulnerabilidad busca huecos y vulnerabilidades potenciales, las pruebas de penetración tratan de explotar los resultados.

El acceso a la infraestructura de red es un proceso dinámico. La seguridad, tanto de información como física, es dinámica. Al realizar una evaluación, se tiene una vista general, la cual puede arrojar falsos positivos y falsos negativos.

Los administradores de seguridad son buenos en la medida que también lo sean las herramientas que usen y el conocimiento que posean. Tome por ejemplo cualquier herramienta de evaluación disponible en el mercado y ejecútela en su sistema. Es casi que garantizado que encontrará al menos algunos falsos positivos. Bien sea por un error del programa o del usuario, el resultado es el mismo. La herramienta puede encontrar vulnerabilidades que en realidad no existen (falsos positivos), o peor aún, la herramienta puede que no encuentre vulnerabilidades que actualmente si existen (falsos negativos).

Ahora que ya estan definidas las diferencias entre evaluaciones de vulnerabilidad y pruebas de penetración, es una buena idea reunir las conclusiones de la evaluación y revisarlas cuidadosamente antes de llevar a cabo una prueba de penetración como parte de sus nuevos buenos hábitos.

Aviso

Intentar explotar las vulnerabilidades sobre recursos en producción puede tener resultados adversos a la productividad y eficiencia de sus sistemas y redes.

A continuación se presenta una lista con algunas ventajas de llevar a cabo evaluaciones de vulnerabilidad.

- Crea un enfoque proactivo en la seguridad de la información
- Se pueden encontrar los puntos de explotación potenciales antes de que un intruso los encuentre
- Genera sistemas actualizados y con las últimas revisiones de software
- Promociona el crecimiento y ayuda en el desarrollo de la experiencia del personal
- Reduce las pérdidas financieras y la publicidad negativa

1.2.1. Establecimiento de una metodología

Para facilitar en la selección de herramientas para las evaluaciones de vulnerabilidad, es útil

establecer una metodología de evaluación de vulnerabilidad. Desafortunadamente, no existe actualmente una metodología predefinida o aprobada por la industria; sin embargo, el sentido común y los buenos hábitos pueden actuar como una guía completa.

¿Cuál es el objetivo? Se trata de sólo un servidor, o de la red completa y todo lo que esta dentro de ella? Somos internos o externos a la compañía? Las respuestas a estas preguntas son importantes pues le ayudaran a determinar no solamente cuáles herramientas seleccionar sino también la forma en que serán usadas.

Para aprender un poco más sobre el establecimiento de metodologías, refiérase a los siguientes sitios web:

- http://www.isecom.org/projects/osstmm.htm — *The Open Source Security Testing Methodology Manual* (OSSTMM)
- http://www.owasp.org/ — *El Proyecto de seguridad de aplicaciones Web abiertas*

1.3. Evaluación de herramientas

Una evaluación típica puede comenzar usando alguna herramienta para reunir información. Cuando se esté evaluando la red completa, haga un dibujo de la red primero para identificar las máquinas que estan en ejecución. Una vez identificadas, examine cada máquina individualmente. Para enfocarse en esas máquinas se requiere de otro conjunto de herramientas. Conocer cuál herramienta utilizar puede ser el paso más importante al encontrar vulnerabilidades.

Así como en todos los aspectos de la vida, hay muchas herramientas diferentes que pueden hacer el mismo trabajo. Este concepto también aplica al realizar evaluaciones de vulnerabilidad. Hay herramientas específicas al sistema operativo, aplicaciones y hasta redes (basadas en los protocolos utilizados). Algunas herramientas son gratuitas, mientras que otras no. Algunas herramientas son intuitivas y fáciles de utilizar, mientras que otras son enigmáticas y muy mal documentadas pero tienen características que las otras no.

Encontrar la herramienta adecuada puede ser una tarea abrumadora. Al final, la experiencia cuenta. Si es posible, configure un laboratorio de pruebas y evalue tantas herramientas como pueda, anotando las fortalezas y debilidades de cada una. Revise el archivo README o la página man de la herramienta. Además revise la internet para más información, tales como artículos, guías paso a paso, o inclusive listas de correo específicas a la herramienta.

Las herramientas que se discuten a continuación son sólo una pequeña muestra de las herramientas disponibles.

1.3.1. Explorar hosts con Nmap

Nmap es una popular herramienta incluida en Red Hat Enterprise Linux que puede ser usada para determinar la distribución de la red. Nmap ha estado disponible por muchos años y es probablemente la herramienta más usada para obtener información. Se incluye una página man excelente con una descripción detallada de sus opciones y uso. Los administradores pueden usar Nmap en una red para encontrar sistemas host y puertos abiertos en esos sistemas.

Nmap es un buen primer paso para una evaluación de vulnerabilidad. Puede mapear todos los hosts dentro de la red y hasta puede pasar una opción que le permite tratar de identificar el sis-

tema operativo que se está ejecutando en un host en particular. Nmap es un buen fundamento para establecer una política de uso de servicios seguros y detener servicios que no se esten usando.

1.3.1.1. Uso de Nmap

Nmap se puede ejecutar desde un intérprete de comandos ejecutando el comando `nmap` seguido del nombre o la dirección IP de la máquina que desea explorar.

```
nmap foo.example.com
```

Los resultados de la exploración (lo cual puede tomar varios minutos, dependiendo de la ubicación de la máquina) se deberían ver similar a lo siguiente:

```
Starting nmap V. 3.50 ( www.insecure.org/nmap/ ) Interesting ports on localhost.localdomain (127.0.0.1): (
```

Nmap prueba los puertos de comunicación de red más comunes por servicios en espera o escuchando. Este conocimiento puede ser útil para un administrador que desea cerrar servicios que no sean necesarios o que no se estén utilizando.

Para más información sobre el uso de Nmap, refiérase a la página oficial en la siguiente URL:

http://www.insecure.org/

1.3.2. Nessus

Nessus es un explorador de seguridad de servicio completo. La arquitectura de extensiones de Nessus permite a los usuarios personalizarlo para sus sistemas y redes. Como cualquier otro explorador, Nessus es bueno sólo si la base de datos de firmas es buena. Afortunadamente, Nessus es actualizado con frecuencia. Esta caracterizado por tener facilidades completas de informes, exploración de hosts y búsquedas de vulnerabilidades en tiempo real. Recuerde que pueden existir falsos positivos y falsos negativos, aún en una herramienta tan poderosa y tan actualizada como Nessus.

Nota

Nessus no está incluido y no es soportado en Red Hat Enterprise Linux. Ha sido incluido en este documento como una referencia a los usuarios que estén interesados en usar esta aplicación.

Para más información sobre el uso de Nessus, refiérase a la página oficial en la siguiente URL:

http://www.nessus.org/

1.3.3. Nikto

Nikto es un escaneador de scripts CGI excelente. Nikto tiene la capacidad de no sólo probar vulnerabilidades de CGI sino también que lo hace de forma evasiva, evitando los sistemas de detección de intrusos. Viene con una documentación muy completa, la cual es recomendable revisar antes de ejecutar el programa. Si sus servidores web están sirviendo scripts CGI, Nikto

puede ser un recurso excelente para chequear la seguridad de estos servidores.

Nota

Nikto no está incluido y no es soportado en Red Hat Enterprise Linux. Ha sido incluido en este documento como una referencia a los usuarios que estén interesados en usar esta aplicación.

Se puede encontrar más información sobre Nikto en el siguiente URL:

http://www.cirt.net/code/nikto.shtml

1.3.4. VLAD the Scanner

VLAD es un explorador desarrollado por el equipo RAZOR en Bindview, Inc. que puede ser utilizado para verificar vulnerabilidades. comunes de seguridad de la lista Top Ten de SANS (problemas de SNMP, problemas de compartición de archivos, etc.). Aún cuando no tiene tantas funcionalidades como Nessus, vale la pena investigar VLAD.

Nota

VLAD no está incluido y no es soportado en Red Hat Enterprise Linux. Ha sido incluido en este documento como una referencia a los usuarios que puedan estar interesados en utilizar esta aplicación.

Se puede encontrar más información sobre VLAD en el sitio web del equipo RAZOR en el siguiente URL:

http://www.bindview.com/Support/Razor/Utilities/

1.3.5. Anticipándose a sus futuras necesidades

Hay muchas herramientas disponibles, dependiendo de su objetivo y recursos. Existen herramientas para redes inalámbricas, redes Novell, sistemas Windows, sistemas Linux y más. Otra parte esencial al realizar evaluaciones de seguridad puede incluir revisar la seguridad física, selección de personal o evaluaciones de red de voz/PBX. Hay algunos nuevos conceptos tales como *war walking* — explorar el perímetro de la estructura física de su corporación por vulnerabilidades de red inalámbrica — que también puede investigar y, si lo requiere, incorporar en sus evaluaciones. La imaginación y exposición son los únicos límites al planear y conducir una evaluación de vulnerabilidades.

2. Ataques y vulnerabilidades

Para poder planear e implementar una buena estrategia de seguridad, primero debe tener en cuenta algunos de los problemas que un atacante motivado y determinado explota para com-

prometer sus sistemas. Pero antes de detallar estos problemas, debemos definir la terminología usada para identificar un atacante.

2.1. Una breve historia sobre los hackers

El significado moderno del término *hacker* tiene sus origenes en los años 60 y en el Club de Modelaje de Trenes del Instituto de Tecnología de Massachusetts (MIT), el cual diseñaba conjuntos de trenes de gran escala y detalle. Hacker fue el nombre usado para nombrar aquellos miembros del club que descubrían un truco brillante o que resolvían un problema muy complicado.

Desde ese momento el término hacker se ha utilizado para describir desde un aficionado a las computadoras hasta un programador virtuoso. Un rasgo característico de un hacker es su disposición de explorar en detalle cómo funcionan los sistemas de computación con poca o ninguna motivación externa. Los desarrolladores de software de la comunidad de Código Abierto (Open Source), a menudo se consideran a si mismos y a sus colegas como hackers, como una forma de respeto.

Generalmente, los hackers siguen una forma de *ética de hackers*. Ésta declara que la búsqueda de información y experiencia es esencial y que compartir ese conocimiento es el compromiso de todo hacker con la comunidad. Durante esa búsqueda de conocimiento, algunos hackers disfrutan los retos académicos de burlar los controles de seguridad en sistemas de computación. Por esta razón, la prensa usualmente utiliza este término para describir aquellos que acceden ilegalmente a sistemas y redes con intenciones maliciosas o criminales. El término más adecuado para este tipo de hacker de computadoras es *cracker* o *maleante informático* (también se les conoce como *pirata informático*, *ciberpirata*, etc.) — un término creado por los hackers en la mitad de los 80 para diferenciar a las dos comunidades.

2.1.1. Escalas de grises

Hay varios grupos distinto dentro de la comunidad de individuos que intentan encontrar y explotar las vulnerabilidades en sistemas y redes. Estos grupos se describen por el color del sombrero que ellos "usan" cuando realizan sus investigaciones de seguridad. El color es un indicativo de su intención.

Un *hacker de sombrero blanco* es aquel que prueba sistemas y redes para examinar su rendimiento y determinar que tan vulnerables son éstos ante un intruso. Usualmente, los hackers de sombrero blanco tratan de violar sus propios sistemas o los sistemas de un cliente que los ha empleado para propósitos de auditoría de seguridad. Los investigadores de seguridad y los consultores de seguridad profesional son dos ejemplos de hackers de sombrero blanco.

Un *hacker de sombrero negro* es sinónimo de un cracker. Generalmente, los crackers están menos enfocados a la programación y al lado de académico de violar un sistema. Con frecuencia los crackers utilizan programas especializados para violar vulnerabilidades conocidas en los sistemas para así descubrir información confidencial para beneficio personal o para producir daños a un sistema o a una red.

Por otro lado, un *hacker de sombrero gris*, tiene las habilidades e intenciones de un hacker de sombrero blanco pero en la mayoría de las situaciones utiliza ese conocimiento para propósitos menos nobles. Un hacker de sombrero gris se puede ver como un hacker de sombrero blanco que usa un sombrero negro para ejecutar su propia agenda.

Los hackers de sombrero gris usualmente se suscriben a otra forma de código ético que señala que es aceptable entrar en un sistema siempre y cuando el hacker no cometa robo o viole la confidencialidad. Sin embargo, otros argumentan que el sólo hecho de violar un sistema es por sí mismo anti-ético.

No importa cual sea la intención, es importante conocer las debilidades que un pirata intentará explotar. El resto del capítulo se basará en estos problemas.

2.2. Amenazas a la Seguridad de la red

Los malos hábitos cuando se configuran los siguientes aspectos de una red pueden incrementar los riesgos de ataques.

2.2.1. Arquitecturas inseguras

Una red mal configurada es un punto de entrada para usuarios no autorizados. Al dejar una red local abierta, confiable, vulnerable a la inseguridad de la Internet, es como dejar una puerta abierta en un vecindario con alta criminalidad — puede que no ocurra nada durante un cierto tiempo, pero *eventualmente* alguien intentará aprovecharse de la oportunidad.

2.2.1.1. Redes de difusión

Los administradores de sistemas a menudo fallan al darse cuenta de la importancia del hardware de la red en sus esquemas de seguridad. El hardware simple, como concentradores y enrutadores, a menudo se basa en broadcast (difusión) o en el principio de sin-interruptores; esto es, cada vez que un nodo transmite datos a través de la red a un nodo recipiente, el concentrador o enrutador hace una difusión de los paquetes de datos hasta que el nodo recipiente recibe y procesa los datos. Este método es el más vulnerable para hacer engaños de direcciones (spoofing) al protocolo de resolución de direcciones (*arp*) o control de acceso a la media (*MAC*) tanto por intrusos externos como por usuarios no autorizados.

2.2.1.2. Servidores centralizados

Otra falla potencial de redes es el uso de computación centralizada. Una forma común de reducir costos para muchos negocios, es el de consolidar todos los servicios a una sola máquina poderosa. Esto puede ser conveniente porque es fácil de manejar y cuesta considerablemente menos que una configuración de múltiples servidores. Sin embargo, un servidor centralizado introduce un punto único de falla en la red. Si el servidor central está comprometido, puede dejar la red totalmente inútil o peor aún, sensible a la manipulación o robo de datos. En estas situaciones un servidor central se convierte en una puerta abierta, permitiendo el acceso a la red completa.

2.3. Amenazas a la seguridad de servidores

La seguridad de servidores es tan importante como la seguridad de la red debido a que los servidores usualmente contienen una gran cantidad de información vital de la organización. Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que un pirata los manipule o robe a su gusto. Las siguientes secciones detallan algunos de los problemas más importantes.

2.3.1. Servicios inutilizados y puertos abiertos

Una instalación completa de Red Hat Enterprise Linux contiene más de 1000 paquetes de aplicaciones y bibliotecas. Sin embargo, la mayoría de los administradores de servidores optan por no instalar todos los paquetes de la distribución, prefiriendo una instalación de paquetes base que incluye varias aplicaciones para servidores.

2.3.2. Servicios sin sus parches

La mayoría de las aplicaciones de servidores incluidas en la instalación por defecto, son piezas de software robustas y sólidas que ya han sido probadas. Estas han sido usadas en ambientes de producción por varios años y su código ha sido refinado en detalle y muchos de los errores han sido encontrados y reparados.

Sin embargo, no hay tal cosa como un software sin errores y siempre hay espacio para mejorar o refinarlo. Más aún, el nuevo software usualmente no es probado tan rigurosamente como uno se esperaría, debido a su reciente llegada al ambiente de producción o porque quizás no es tan popular como otras aplicaciones de servidores.

Los desarrolladores y administradores de sistemas a menudo encuentran fallas (bugs) en las aplicaciones de servidores y publican la información de la falla en sitios webs de seguimiento de errores y seguridad, tales como la lista de correo Bugtraq (http://www.securityfocus.com) o al sitio web del Equipo de Respuestas a Emergencias de Computación (Computer Emergency Response Team, CERT) (http://www.cert.org). Aún cuando estos mecanismos constituyen una forma efectiva de alertar a la comunidad sobre vulnerabilidades de seguridad, depende de los administradores de sistemas el aplicar los parches de sistemas a tiempo. Esto es particularmente cierto puesto que los crackers tienen acceso a las mismas fuentes e intentarán utilizar esta información para violar sistemas que no hayan sido emparchados. Una buena administración de sistemas requiere vigilancia, seguimiento constante de errores y un mantenimiento de sistemas apropiado para asegurar un ambiente computacional seguro.

Consulte el Sección 4, “Actualizaciones de seguridad” para obtener mayor información sobre cómo mantener el sistema actualizado.

2.3.3. Administración desatendida

Una de las amenazas más grandes a la seguridad de los servidores son los administradores distraídos que olvidan remendar sus sistemas. De acuerdo al *Instituto de Seguridad y Administración de Sistemas de Redes* (*System Administration Network and Security Institute*, *SANS*), la causa primaria de la vulnerabilidad de seguridad de los sistemas es «asignar personal poco entrenado para mantener la seguridad y no proporcionar ni el entrenamiento ni el tiempo para permitir que ejecuten su trabajo»[5] Esto aplica tanto a los administradores nuevos como a aquellos demasiado confiados o poco motivados.

Algunos administradores fallan en emparchar sus servidores y estaciones de trabajo, mientras que otros fallan en leer los mensajes del registro de eventos del kernel del sistema o tráfico de la red. Otro error común es dejar las contraseñas o llaves a servicios sin modificar. Por ejemplo, algunas bases de datos tienen contraseñas administrativas por defecto porque sus desarrolladores asumen que el administrador de sistemas cambiará estas contraseñas inmediátamente luego de la instalación. Si un administrador de bases de datos no cambia las contraseñas, hasta un cracker sin mucha experiencia puede utilizar una contraseña conocida por todo el mundo para ganar acceso con privilegios administrativos a la bases de datos. Estos son sólo unos

[5] Fuente: http://www.sans.org/newlook/resources/errors.html [http://www.sans.org/newlook/resources/errors.htm]

ejemplos de como una administración descuidada puede llevar a servidores comprometidos.

2.3.4. Servicios intrínsecamente inseguros

Aún hasta la organización más atenta y vigilante puede ser victima de vulnerabilidades si los servicios de red que seleccionen son intrínsecamente inseguros. Por ejemplo, hay muchos servicios desarrollados bajo la suposición de que serían usados en una red confiable; sin embargo, esta supuesto falla tan pronto como el servicio se vuelve disponible sobre la Internet — la cual es por sí misma insegura.

Una categoría de servicios de red inseguros son aquellos que requieren nombres y contraseñas de usuario sin encriptar para la autenticación.Telnet y FTP son dos de estos servicios. Un software de huzmeo de paquetes que esté monitoreando el tráfico entre un usuario remoto y tal servicio, puede fácilmente robarse los nombres de usuario y contraseña.

Tales servicios pueden también ser presa fácil de lo que en términos de seguridad se conoce como un ataque de *hombre en el medio*. En este tipo de ataque, un pirata redirige el tráfico de la red a que apunte a su máquina en vez del servidor destino. Una vez que alguien abre una sesión remota con el servidor, la máquina del atacante actua como un conductor invisible, quedándose tranquilamente capturando la información entre el servicio remoto y el usuario inocente. De esta forma un pirata puede reunir contraseñas administrativas y datos sin que el servidor o el usuario se den cuenta.

En otro categoría de servicios inseguros se incluyen los sistemas de archivos de red y servicios de información tales como NFS o NIS, los cuales son desarrollados específicamente para ser usados en una LAN pero que son, desafortunadamente, extendidos para incluir WANs (para los usuarios remotos). NFS, por defecto, no tiene ningún tipo de autenticación o mecanismos de seguridad configurado para prevenir que un pirata monte un directorio compartido NFS y a partir de allí acceder a cualquier cosa dentro de él. NIS también tiene información vital que debe ser conocida por cada computador de la red, incluyendo contraseñas y permisos de archivos, dentro de una base de datos de texto plano ACSII o DBM (derivado de ASCII). Un cracker que gana acceso a esta base de datos puede tener acceso a todas las cuentas de usuarios en la red, incluyendo la cuenta del administrador.

2.4. Amenazas a la seguridad de estaciones de trabajo y PCs del hogar

Las estaciones de trabajo y PCs del hogar a menudo no son tan susceptibles a ataques como las redes o servidores, pero puesto que a menudo estas contienen información confidencial, tales como información de tarjetas de credito, pueden ser blancos para los crackers de sistemas. Las estaciones de trabajo también pueden ser manipuladas sin que el usuario se de cuenta por un atacante y ser utilizadas como máquinas «esclavas» en ataques coordinados. Por estas razones, conociendo las vulnerabilidades de una estación de trabajo puede ahorrar a los usuarios el dolor de cabeza de reinstalar el sistema operativo o peor aún, recuperarse del robo de datos.

2.4.1. Malas contraseñas

2.4.2. Aplicaciones cliente vulnerables

A pesar de que un administrador puede tener un servidor completamente actualizado y seguro,

eso no significa que un usuario remoto esté seguro cuando accese al mismo. Por ejemplo, si el servidor ofrece servicios Telnet o FTP sobre una red pública, un atacante puede capturar el texto plano de los nombres de usuarios y contraseñas cuando estos son transmitidos a través de la red y luego usar la información de la cuenta para acceder a la estación de trabajo remota del usuario.

Aún cuando se utilicen protocolos seguros, tales como SSH, un usuario remoto puede ser vulnerable a ciertos ataques si no mantienen sus aplicaciones cliente actualizadas. Por ejemplo, clientes v.1 SSH son vulnerables a un ataque de redireccionamiento de X desde un servidor SSH malicioso. Una vez conectado al servidor, el atacante puede de manera cuidadosa capturar los golpes de teclas y los clics del ratón hechos por el cliente sobre la red. Este problema se reparó con el protocolo v.2 SSH, pero depende del usuario hacer un seguimiento de qué aplicaciones tienen tales vulnerabilidades y actualizarlas si es necesario.

3. Ataques y agresiones comunes

Tabla 20.1, “Agresiones comunes” detalla algunas de las agresiones y puntos de entrada más comunes que los intrusos utilizan para acceder a los recursos de red de la organización. La clave para prevenir estas agresiones es entender cómo se realizan y cómo los administradores puedes proteger sus redes en contra de estos ataques.

Agresiones	Descripción	Notas
Contraseñas nulas o por defecto	Dejar las contraseñas administrativas en blanco o usar la contraseña predeterminada proporcionada por el fabricante. Esto sucede frecuentemente en hardware como enrutadores y cortafuegos, aunque algunos servicios que corren en Linux pueden contener contraseñas administrativas predeterminadas (Red Hat Enterprise Linux 5 no se entrega con ellas).	Asociado generalmente con hardware de red como enrutadores, cortafuegos, VPNs y redes de almacenamiento adjunto (NAS). Frecuente en sistemas operativos de legado, especialmente aquellos que contienen servicios (tales como UNIX y Windows). Algunas veces los administradores crean de prisa cuentas de usuarios privilegiados y dejan la contraseña vacía, un punto de entrada perfecto para usuarios malignos que descubren la cuenta.
Contraseñas compartidas por defecto	Hay servicios seguros que a veces incluyen llaves de seguridad por defecto para propósitos de desarrollo o de prueba. Si estas llaves se dejan sin modificar y se colocan en un ambiente de producción en la Internet, *todos* los usuarios con la misma llave por defecto tienen acceso a ese recurso y a toda la información confidencial que pueda contener.	Comunes en puntos de acceso inalámbrico y productos para servidores de seguridad preconfigurados.

Agresiones	Descripción	Notas
IP Spoofing (Engaño de IPs)	Una máquina remota actúa como un nodo en su red local, encuentra vulnerabilidades con sus servidores e instala un programa en el fondo o un caballo de troya para ganar control sobre los recursos de su red.	Un "Spoofing" es bastante difícil de ejecutar, ya que envuelve la predicción del número TCP/IP SYN-ACK por parte del atacante para coordinar una conexión al sistema objetivo. Sin embargo, hay varias herramientas disponibles que ayudan a los crackers en la ejecución de este ataque. Depende de los servicios ejecutándose en el sistema objetivo (tales como `rsh`, `telnet`, FTP y otros) que usan técnicas de autenticación *basadas en fuente*, las cuales no son recomendables si se les compara con PKI u otras formas de autenticación encriptada como las utilizadas por `ssh` o SSL/TLS.
Intercepción pasiva	Reunir datos que pasan entre dos nodos activos en una red mediante el rastreo de la conexión entre los dos nodos.	Este tipo de ataque funciona con protocolos de transmisión de texto llano tales como Telnet, FTP, y transferencias HTTP. Los atacantes remotos deben tener acceso a un sistema comprometido en un LAN para poder ejecutar dicho ataque; generalmente el cracker ha utilizado un ataque activo (tal como IP spoofing o man-in-the-middle) para comprometer un sistema en un LAN. Entre las medidas preventivas se incluyen los servicios con cambios de llaves encriptadas, contraseñas de un solo uso o autenticación encriptada para prevenir la captura de contraseñas (snooping). Es asimismo recomendable la encriptación severa durante la transmisión.
Vulnerabilidades de servicios	Un atacante encuentra una falla o un hueco en un servicio que se ejecuta en la Internet; a través de esa vulnerabilidad, el atacante puede comprometer el sistema completo y cualquier dato que contenga. También podría comprometer otros sis-	Los servicios basados en HTTP, como por ejemplo CGIs, son vulnerables a la ejecución de comandos remotos e incluso al acceso interactivo a la shell. Incluso cuando el servicio HTTP es ejecutado por un

Agresiones	Descripción	Notas
	temas en la red.	usuario sin privilegios, como "nobody", es posible leer información incluida en archivos de configuración y mapas de red. El atacante puede también iniciar un ataque de negación de servicio que consume los recursos del sistema o convierte estos recursos como inalcanzables para otros usuarios. En algunas ocasiones, los servicios pueden presentar vulnerabilidades que pasan inadvertidas durante los periodos de desarrollo y prueba; estas vulnerabilidades (como el *buffer overflows*, en donde los atacantes congelan el servicio utilizando valores arbitrarios que llenan el buffer de memoria de una aplicación, dando al atacante un entrada de comandos interactiva desde la cual pueden ejecutar comandos arbitrarios) pueden dar control administrativo completo a un atacante. Los administradores deben asegurarse de no ejecutar los servicios como usuarios root. Asimismo, los administradores deben permanecer pendientes de los parches y actualizaciones de erratas de aplicaciones que son expedidos por distribuidores u organizaciones de seguridad como CERT y CVE.
Vulnerabilidades de las aplicaciones	Los atacantes encuentran fallas en aplicaciones de escritorio y de estaciones de trabajo (tales como clientes de correo electrónico) y ejecutan código arbitrario, implantan caballos de troya para comprometer los sistemas en un futuro o dañan los sistemas. Pueden ocurrir otras agresiones si la estación de trabajo tiene privilegios administrativos sobre el resto de la red.	Las estaciones de trabajo y los escritorios son más susceptibles de ataques porque los empleados no tienen la suficiente experiencia para prevenir o detectar una máquina comprometida. Es importante informar a las personas sobre los riesgos de instalar software no autorizado o de abrir correo no solicitado. Se pueden implementar medidas de seguridad, evitar, por ejemplo, que el cliente de correo abra automáticamente o ejecute los anexos. Adicionalmente, las actualizaciones au-

Agresiones	Descripción	Notas
		tomáticas de software de las estaciones de trabajo a través de Red Hat Network u otros servicios de administración de sistemas pueden aliviar la carga de las distribuciones de seguridad en múltiples puestos.
Ataques de rechazo de servicio (DoS, Denial of Service)	Un atacante o grupo de atacantes pueden coordinar un ataque a la red o a los recursos de un servidor de una organización, mediante el envío de paquetes a la máquina objetivo (bien sea un servidor, enrutador o estación de trabajo). El recurso queda así deshabilitado para validar usuarios.	El caso más conocido y reportado de un ataque DoS ocurrió en los Estados Unidos en 2000. Varios sitios comerciales y gubernamentales permanecieron no disponibles debido a un ataque coordinado que utilizó varios sistemas comprometidos con conexiones de ancho de banda amplia que actuaron como *zombies*, o nodos de redirección de emisión. Los paquetes fuentes son frecuentemente bifurcados (o redirigidos) para dificultar la investigación de la verdadera fuente del ataque. Avances en filtrados de entradas (IETF rfc2267) utilizando `iptables` y Network IDSes tales como `snort` asisten a los administradores con el seguimiento y prevención de ataques DoS.

Tabla 20.1. Agresiones comunes

4. Actualizaciones de seguridad

A medida que se descubren fallas de seguridad en el software, éste debe ser actualizado para sellar cualquier posible riesgo de seguridad. Si el paquete es parte de una distribución de Red Hat Enterprise Linux actualmente soportada, Red Hat, Inc. está en la obligación de producir los paquetes de actualización que reparen las vulnerabilidades tan pronto como sea posible. A menudo, el anuncio de una falla de seguridad viene acompañado de un parche (o el código fuente que repara el problema). Este parche es aplicado al paquete de Red Hat Enterprise Linux, probado por el equipo de control de calidad de Red Hat y luego distribuido como una actualización de erratas. Sin embargo, si el anuncio no incluye un parche, un desarrollador de Red Hat trabajará con la persona encargada de mantener el software con el fin de reparar el problema. Después de la reparación del problema, el paquete es probado y distribuido como una actualización de errata.

Si se ha distribuido una actualización de errata para algún software usado en su sistema, se le

recomienda que actualice los paquetes afectados tan pronto como estos sean publicados para minimizar el tiempo en que su sistema está potencialmente vulnerable.

4.1. Actualización de paquetes

Cuando actualice software en un sistema, es importante descargar la actualización desde una fuente confiable. Un intruso puede fácilmente reconstruir una versión de un paquete con el mismo número de versión como el que se supone va a reparar el problema, pero con una agresión de seguridad diferente en el paquete y distribuirlo en Internet. Si ésto ocurre, no se detectará la agresión cuando se utilicen medidas de seguridad tales como la verificación de archivos contra el RPM original. Por esta razón, es muy importante que solamente descargue RPMs desde fuentes confiables, tales como Red Hat, Inc. y verifique la firma del paquete para asegurarse de su integridad.

Red Hat proporciona dos maneras de encontrar información sobre las actualizaciones de erratas:

1. Listadas y disponibles para su descarga desde Red Hat Network
2. Listadas y desvinculadas del sitio web de Erratas de Red Hat

Nota

A partir de la línea de productos Red Hat Enterprise Linux, solamente se pueden descargar los paquetes de actualizaciones desde Red Hat Network. Aunque el sitio web de erratas de Red Hat contiene información sobre las actualizaciones, no contiene los paquetes para ser descargados.

4.1.1. Utilizando Red Hat Network

Red Hat Network le permite automatizar la mayoría de los procesos de actualización. Determina cuáles paquetes RPM son necesarios para el sistema, los descarga desde repositorios seguros, verifica la firma del RPM para asegurarse de que no han sido dañados y los actualiza. La instalación del paquete puede ocurrir de inmediato o puede ser planificada durante un cierto período de tiempo.

Red Hat Network requiere un *Perfil del sistema* para cada máquina que desea actualizar. El Perfil del Sistema contiene la información del hardware y software del sistema. Esta información se mantiene como confidencial y no se entrega a nadie más. Sólo se utiliza para determinar cuales actualizaciones de errata son aplicables a cada sistema. Sin esta información, Red Hat Network no puede determinar si su sistema necesita actualizaciones. Cuando una errata de seguridad (o cualquier tipo de errata) es publicada, Red Hat Network le enviará un correo electrónico con una descripción de la errata así como también cuáles de sus sistemas son afectados. Para aplicar la actualización, puede utilizar el **Red Hat Update Agent** o planificar para que el paquete sea actualizado a través del sitio web http://rhn.redhat.com.

Sugerencia

Red Hat Enterprise Linux includes the **Red Hat Network Alert Notification Tool**, a convenient panel icon that displays visible alerts when there is an update for a registered Red Hat Enterprise Linux system. Refer to the following URL for more information about the applet: https://rhn.redhat.com/rhn/help/quickstart.jsp

Importante

Antes de instalar cualquier errata de seguridad, asegúrese de leer cualquier instrucción especial contenida en el informe de errores y ejecútelas de la forma adecuada. Consulte la Sección 4.1.5, “Aplicar los cambios” para ver instrucciones generales sobre cómo aplicar los cambios de una actualización de errores.

4.1.2. Utilizando el sitio web de Erratas de Red Hat

Cuando se lanzan los informes de errata, estos son publicados en el sitio web de Erratas de Red Hat en http://www.redhat.com/security/. Desde esta página, seleccione el producto y la versión de su sistema y luego seleccione **seguridad** en la parte superior de la página para sólo desplegar los Advertencia de seguridad de Red Hat Enterprise Linux. Si la sinopsis de alguna de las recomendaciones describe un paquete usado en su sistema, pulse en la sinopsis para ver más detalles.

La página de detalles describe las violaciones de seguridad y cualquier instrucción especial que se deba llevar a cabo adicionalmente para actualizar el paquete y reparar el hueco de seguridad.

Para descargar el paquete actualizado, pulse en el enlace para iniciar una sesión en Red Hat Network, luego pulse el nombre del paquete y guárdelo al disco duro. Se recomienda que cree un nuevo directorio tal como `/tmp/updates` y guarde todos los paquetes descargados en él.

4.1.3. Verificar paquetes firmados

Todos los paquetes de Red Hat Enterprise Linux están firmados con la llave *GPG* de Red Hat, Inc. GPG viene de GNU Privacy Guard, o GnuPG, un paquete de software libre utilizado para asegurarse de la autenticidad de los paquetes distribuidos. Por ejemplo, una llave privada (llave secreta) de Red Hat bloquea el paquete mientras que la llave pública desbloquea y verifica el paquete. Si la llave pública distribuida por Red Hat no coincide con la llave privada durante la verificación de RPM, puede que el paquete haya sido alterado y por lo tanto no se puede confiar en el.

La utilidad de RPM dentro de Red Hat Enterprise Linux trata automáticamente de verificar la firma GPG de un paquete RPM antes de instalarlo. Si no tiene la llave GPG de Red Hat instalada, instálela desde una ubicación segura y estática tal como un CD-ROM de instalación de Red Hat Enterprise Linux.

Asumiendo que el CD-ROM se encuentra montado en `/mnt/cdrom`, utilice el siguiente comando para importarla a su *llavero* (una base de datos de llaves confiables en el sistema):

```
rpm --import /mnt/cdrom/RPM-GPG-KEY
```

Para desplegar una lista de todas las llaves instaladas para ser verificadas por RPM, ejecute el comando:

```
rpm -qa gpg-pubkey*
```

Para la llave de Red Hat, la salida incluirá lo siguiente:

```
gpg-pubkey-db42a60e-37ea5438
```

Para desplegar detalles sobre una llave específica, utilice el comando `rpm -qi` seguido de la salida del comando anterior, como se muestra en este ejemplo:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

Es extremadamente importante que verifique la firma de sus archivos RPM antes de instalarlos para asegurarse de que la llave no ha sido alterada desde la publicación de los paquetes por Red Hat. Para verificar todos los paquetes descargados de una vez, escriba el comando siguiente:

```
rpm -K /tmp/updates/*.rpm
```

Para cada paquete, si se verifica exitósamente la llave GPG, el comando devuelve `gpg OK`. Si no es así, asegúrese de estar utilizando la llave pública correcta de Red Hat, así como también verificar la fuente del contenido. No se deberían instalar paquetes que no pasan las verificaciones de GPG pues pueden haber sido alterados por terceros.

Después de verificar la llave GPG y descargar todos los paquetes asociados con el informe de errores, instálelos como usuario root desde un shell.

4.1.4. Instalación de paquetes firmados

La instalación para la mayoría de los paquetes se puede hacer sin percances (excepto para los paquetes kernel), con el comando siguiente:

```
rpm -Uvh /tmp/updates/*.rpm
```

Para los paquetes del kernel utilice el comando que sigue:

```
rpm -ivh /tmp/updates/<kernel-package>
```

Reemplace `<kernel-package>` en el ejemplo anterior con el nombre del RPM del kernel.

Una vez que la máquina ha sido reiniciada sin problemas usando el nuevo kernel, se puede eliminar el viejo kernel utilizando el comando siguiente:

```
rpm -e <old-kernel-package>
```

Reemplace `<old-kernel-package>` en el ejemplo anterior con el nombre del RPM del kernel vie-

jo.

Nota

No se requiere que elimine el viejo kernel. El gestor de arranque por defecto, GRUB, permite tener instalados múltiples kernels y seleccionarlos desde el menú durante el arranque.

Importante

Antes de instalar cualquier errata de seguridad, asegúrese de leer cualquier instrucción especial contenida en el informe de errores y ejecútelas de la forma adecuada. Consulte la Sección 4.1.5, “Aplicar los cambios” para ver instrucciones generales sobre cómo aplicar los cambios de una actualización de errores.

4.1.5. Aplicar los cambios

Después de descargar e instalar las erratas de seguridad a través de Red Hat Network o del sitio web de Erratas de Red Hat, es importante que detenga el uso del software viejo y comience a utilizar el nuevo software. Como se lleve esto a cabo va a depender del tipo de software que se haya actualizado. La lista siguiente muestra las diferentes categorías generales de software y proporciona instrucciones para utilizar las versiones actualizadas luego de una actualización de paquetes.

Nota

En general, la forma más segura de asegurarse que se está utilizando la versión más reciente de un paquete de software es reiniciando el sistema; sin embargo, esta opción no siempre está disponible para el administrador del sistema.

Aplicaciones
: Las aplicaciones del espacio de usuario son cualquier programa que puede ser iniciado por un usuario del sistema. Generalmente, tales aplicaciones son solamente utilizadas cuando un usuario, script o tarea automática las lanza y no persisten por largos períodos de tiempo.

  Una vez que tal aplicación del espacio de usuario es actualizada, detenga cualquier instancia de la aplicación en el sistema y lance el programa nuevamente para así utilizar la versión actualizada.

Kernel
: El kernel es el componente de software central para el sistema operativo de Red Hat Enterprise Linux. Éste se encarga de manejar el acceso a la memoria, el procesador y los perifé-

ricos así como también, planifica todas las tareas.

Debido a su rol central, el kernel no puede reiniciarse sin detener el computador. Por lo tanto, una versión actualizada del kernel no puede ser usada hasta que el sistema no se reinicie.

Bibliotecas compartidas

Las bibliotecas compartidas son unidades de código, tales como `glibc`, que son usadas por un número de aplicaciones y servicios. Las aplicaciones que utilizan una biblioteca compartida típicamente cargan el código compartido cuando la aplicación es inicializada, así cualquier aplicación que esté utilizando la biblioteca debe ser detenida y relanzada.

Para determinar cuáles aplicaciones en ejecución estan enlazadas a una biblioteca en particular, utilice el comando `lsof`, como se muestra en el ejemplo:

```
lsof /usr/lib/libwrap.so*
```

Este comando devuelve una lista de todos los programas en ejecución que están usando TCP wrappers para el control de acceso a máquinas. Por lo tanto, cualquier programa listado debe ser detenido y relanzado si el paquete `tcp_wrappers` es actualizado.

Servicios SysV

Los servicios SysV son programas del servidor persistentes, que son lanzados durante el proceso de arranque. Ejemplos de servicios SysV incluyen `sshd`, `vsftpd` y `xinetd`.

Debido a que estos programas usualmente persisten en memoria, siempre y cuando la máquina esté encendida, cada servicio SysV actualizado, debe ser detenido y relanzado después de una actualización de paquetes. Esto se puede hacer usando la **Herramienta de configuración de servicios** o conectándose como root en un indicador de comandos shell y ejecutando el comando `/sbin/service` como se muestra en el ejemplo siguiente:

```
/sbin/service <service-name> restart
```

En el ejemplo anterior, reemplace *<service-name>* con el nombre del servicio, tal como `sshd`.

Servicios `xinetd`

Los servicios controlados por el super servicio `xinetd` sólo funcionan cuando hay una conexión activa. Ejemplos de servicios controlados por `xinetd` incluyen Telnet, IMAP, y POP3.

Puesto que `xinetd` lanza nuevas instancias de estos servicios cada vez que se recibe una nueva petición, las conexiones que ocurren después de una actualización son manejadas por el software actualizado. Sin embargo, si hay conexiones activas en el momento en que el servicio controlado por `xinetd` es actualizado, estas son servidas por la versión vieja del software.

Para matar todas las instancias viejas de un servicio controlado por `xinetd`, actualice el paquete para el servicio y luego detenga todos los procesos que se esten ejecutando en ese momento. Para determinar si el proceso está en ejecución, utilice el comando `ps` y luego use `kill` o `killall` para detener todas las instancias actuales del servicio.

Por ejemplo, si hay erratas de seguridad para paquetes `imap`, actualice los paquetes, luego escriba el comando siguiente como root en un indicador de comandos:

```
ps -aux | grep imap
```

Este comando devuelve todas las sesiones activas de IMAP. Las sesiones individuales pueden ser terminadas luego usando el comando que sigue:

```
kill <PID>
```

Si la sesión no es finalizada después de ejecutar este comando, utilice el comando siguiente:

```
kill -9 <PID>
```

En el ejemplo anterior, reemplace `<PID>` con el número de identificación del proceso (encontrado en la segunda columna del comando `ps`) para una sesión IMAP.

Para matar todas las sesiones IMAP activas, utilice el comando que sigue:

```
killall imapd
```

Capítulo 21. Aseguramiento de su Red

1. Seguridad en las estaciones de trabajo

La seguridad del ambiente Linux comienza en la estación de trabajo. Bien sea que esté bloqueando su propia máquina personal o asegurando un sistema corporativo, una buena política de seguridad comienza con el computador personal. Después de todo, una red es tan segura como su nodo más débil.

1.1. Evaluando la seguridad en la estación de trabajo

Cuando evalúe la seguridad de una estación de trabajo Red Hat Enterprise Linux, considere lo siguiente:

- *Seguridad del BIOS y del gestor de arranque* — ¿Puede un usuario no autorizado acceder físicamente a la máquina e iniciar una sesión como usuario único o en modo de rescate sin una contraseña?
- *Seguridad de la contraseña* — ¿Qué tan seguras son las cuentas de usuarios en la máquina?
- *Controles administrativos* — ¿Quién tiene una cuenta en el sistema y cuánto control administrativo tienen?
- *Servicios de red disponibles* — ¿Qué servicios están escuchando peticiones desde la red que realmente deberían estar en ejecución?
- *Cortafuegos personales* — ¿Qué tipo de cortafuego o firewall, si existe, es necesario?
- *Herramientas de comunicación para mejor seguridad* — ¿Qué herramientas debería utilizar para comunicarse entre estaciones de trabajo y cuáles se deberían evitar?

1.2. Seguridad del BIOS y del gestor de arranque

La protección con contraseñas para el BIOS (o equivalentes al BIOS) y para el gestor de arranque pueden ayudar a prevenir el acceso físico a sus sistemas por parte de usuarios no autorizados. Asimismo evita que los sistemas sean iniciados desde medios removibles o que se obtenga acceso como root a través del modo monousuario. Sin embargo, las medidas de seguridad que uno debería tomar para protegerse contra tales ataques dependen tanto de la confidencialidad de la información que las estaciones tengan como de la ubicación de la máquina.

Por ejemplo, si se utiliza una máquina en una exhibición y ésta no contiene datos confidenciales, entonces puede que no sea crítico prevenir tales ataques. Sin embargo, si en la misma exhibición se deja sin cuidado el portátil de uno de los empleados que contiene llaves privadas SSH sin encriptar pertenecientes a la red corporativa, se puede conducir a una violación de seguridad importante para toda la compañía.

Por otro lado, si la estación de trabajo está localizada en un lugar donde sólo los usuarios autorizados o de confianza tienen acceso, entonces la seguridad del BIOS o del gestor de arranque puede no ser necesaria.

1.2.1. Contraseñas del BIOS

Las dos razones básicas por las cuales se debe proteger la BIOS de una computadora con una contraseña son[6]:

1. *Prevenir cambios a las configuraciones del BIOS* — Si un intruso tiene acceso a la BIOS, puede configurarlo para que arranque desde un diskette o CD-ROM. Esto permite entrar en modo de rescate o monousuario, lo que a su vez les permite plantar programas dañinos en el sistema o copiar datos confidenciales.

2. *Prevenir el arranque del sistema* — Algunas BIOSes le permiten proteger el proceso de arranque con una contraseña. Cuando está funcionalidad está activada, un atacante esta forzado a introducir una contraseña antes de que el BIOS lanze el gestor de arranque.

Debido a que los métodos para colocar contraseñas del BIOS varían entre fabricantes de equipos, consulte el manual de su computador para ver las instrucciones específicas.

Si olvida su contraseña del BIOS, usualmente esta se puede reconfigurar bien sea a través de los jumpers en la tarjeta madre o desconectando la batería CMOS. Por esta razón, es una buena idea bloquear el chasis del computador si es posible. Sin embargo, consulte el manual del computador o tarjeta madre antes de proceder a desconectar la batería CMOS.

1.2.1.1. Aseguramiento de plataformas diferentes a x86

Otras arquitectura utilizan programas diferentes para llevar a cabo tareas de bajo nivel similares a las del BIOS en sistemas x86. Por ejemplo, las computadoras basadas en Intel®Itanium utilizan la shell *Extensible Firmware Interface* (*EFI*).

Para ver las instrucciones sobre cómo proteger con contraseñas estos programas, consulte las instrucciones del fabricante.

1.2.2. Contraseñas del gestor de arranque

A continuación se muestran las razones principales por las cuales se debe proteger el gestor de arranque de Linux:

1. *Previene el acceso en modo monousuario* — Si un atacante puede arrancar en modo monousuario, se convierte en el superusuario de forma automática sin que se le solicite la contraseña de acceso.

2. *Previene el acceso a la consola de GRUB* — Si la máquina utiliza GRUB como el gestor de arranque, un atacante puede usar la interfaz del editor para cambiar su configuración o para reunir información usando el comando `cat`.

3. *Previene el acceso a sistemas operativos inseguros* — Si es un sistema de arranque dual, un atacante puede seleccionar un sistema operativo en el momento de arranque, tal como

[6] Debido a que los sistemas BIOS varían de acuerdo al fabricante, puede que algunos no soporten la protección con contraseñas de ningún tipo, mientras que otros pueden soportar un tipo pero no el otro.

DOS, el cual ignora los controles de acceso y los permisos de archivos.

Red Hat Enterprise Linux para la plataforma x86 se entrega con el gestor de arranque GRUB. Consulte el Manual de Instalación de Red Hat si desea una visión más profunda de GRUB.

1.2.2.1. Protegiendo GRUB con contraseñas

Puede configurar GRUB para solucionar los primeros dos problemas listados en la Sección 1.2.2, “Contraseñas del gestor de arranque” añadiendo una directriz de contraseña a su archivo de configuración. Para hacer esto, primero seleccione una contraseña, luego abra un intérprete de comandos, conéctese como root y escriba:

```
/sbin/grub-md5-crypt
```

Cuando se le pida, escriba la contraseña GRUB y presione **Intro**. Esto retornará un hash MD5 para la contraseña.

Luego, modifique el archivo de configuración GRUB `/boot/grub/grub.conf`. Abra el archivo y debajo de la línea `timeout` en la sección principal del documento, añada la siguiente línea:

```
password --md5 <contraseña-hash>
```

Reemplace `<contraseña-hash>` con el valor que `/sbin/grub-md5-crypt` retornó[7].

La próxima vez que el sistema arranque, el menú de GRUB no le permitirá acceder al editor o a la interfaz de comandos si no presiona primero **p** seguido por la contraseña de GRUB.

Lamentablemente, esta solución no previene a un atacante arrancar en un sistema operativo inseguro si se está en un ambiente de arranque dual. Para esto, necesita editar una parte diferente del archivo `/boot/grub/grub.conf`.

Busque la línea `title` del sistema operativo inseguro y añada una línea que diga `lock` directamente debajo de ella.

Para un sistema DOS, debería comenzar con algo similar a:

```
title DOS lock
```

Advertencia

Debe tener una línea `password` en la sección principal del archivo `/boot/grub/grub.conf` para que este mecanismo funcione adecuadamente. De lo contrario, un atacante podrá acceder a la interfaz del editor de GRUB y eliminar la línea de bloqueo.

Para crear una contraseña diferente para un kernel o sistema operativo particular, añada una línea `lock`, seguida por una línea de contraseña.

Cada entrada que proteja con una contraseña única debería comenzar con líneas similares a

[7] GRUB también acepta contraseñas no encriptadas, pero se recomienda que utilice un hash md5 para mayor seguridad.

las del ejemplo siguiente:

```
title DOS lock password --md5 <contraseña-hash>
```

1.3. Seguridad de contraseñas

Las contraseñas son el método principal que Red Hat Enterprise Linux utiliza para verificar la identidad de los usuarios. Por esta razón la seguridad de las contraseñas es de suma importancia para la protección del usuario, la estación de trabajo y la red.

Por razones de seguridad, el programa de instalación configura el sistema para usar el *Message-Digest Algorithm* (*MD5*) y contraseñas shadow. Se recomienda que no cambie esta configuración.

Si quita la selección de MD5 durante la instalación, se utilizará el formato *Data Encryption Standard* (*DES*). Este formato limita las contraseñas a ocho caracteres alfanuméricos (no permite caracteres de puntuación o especiales) y proporciona un modesto nivel de encriptación de 56-bits.

Si usted deselecciona las contraseñas shadow durante la instalación, todas las contraseñas son almacenadas como hash de una sola vía en el archivo `/etc/passwd`, lo que hace al sistema vulnerable a ataques de piratas fuera de línea. Si un intruso obtiene acceso a la máquina como un usuario regular, puede también copiar el archivo `/etc/passwd` a su propia máquina y ejecutar cualquier cantidad de programas de descifrado de contraseñas contra él. Si hay una contraseña insegura en el archivo, es cuestión de tiempo antes de que el maleante informático la descubra.

Las contraseñas shadow eliminan este tipo de ataques, almacenando los hash de las contraseñas en el archivo `/etc/shadow`, el cual sólo es leído por el usuario root.

Esto obliga al atacante potencial a intentar descubrir la contraseña remotamente mediante la conexión a un servicio de la red en la máquina, tal como SSH o FTP. Este tipo de ataques de fuerza bruta son mucho más lentos y dejan rastros obvios, pues los intentos fallidos de conexión son registrados a los archivos del sistema. Por supuesto, si el maleante o cracker comienza un ataque durante la noche y usted tiene contraseñas débiles, éste podría obtener acceso antes del amanecer y editar el archivo de registro para borrar sus rastros.

Además del formato y el almacenamiento, está el problema del contenido. Lo más importante que un usuario puede hacer para proteger su cuenta contra un ataque de piratas, es crear una contraseña robusta.

1.3.1. Creación de contraseñas robustas

Cuando se cree una contraseña segura, es una buena idea seguir las siguientes pautas:

- *No utilice solamente palabras o números* — Nunca debería utilizar únicamente letras o sólo números en una contraseña.

  Algunos ejemplos inseguros incluyen:

  - 8675309

  - juan
  - atrapame

- *No utilice palabras reconocibles* — Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, incluso si utiliza números al final de éstos.

  Algunos ejemplos inseguros incluyen:

  - john1
  - DS-9
  - mentat123

- *No utilice palabras en idiomas extranjeros* — Los programas de descifrado de contraseñas a menudo verifican listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.

  Algunos ejemplos inseguros incluyen:

  - cheguevara
  - bienvenue1
  - 1dumbKopf

- *No utilice terminología de hackers* — Si piensa que usted pertenece a una élite porque utiliza terminología hacker — también llamado hablar l337 (LEET) — en su contraseña, piense otra vez. Muchas listas de palabras incluyen lenguaje LEET.

  Algunos ejemplos inseguros incluyen:

  - H4X0R
  - 1337

- *No utilice información personal* — Mantengase alejado de la información personal. Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:

  Algunos ejemplos inseguros incluyen:

  - Su nombre
  - El nombre de sus mascotas
  - El nombre de los miembros de su familia
  - Fechas de cumpleaños

  - Su número telefónico o código postal

- *No invierta palabras reconocibles* — Los buenos verificadores de contraseñas siempre invierten las palabras comunes; por tanto, invertir una mala contraseña no la hace para nada más segura.

  Algunos ejemplos inseguros incluyen:

  - R0X4H
  - nauj
  - 9-DS

- *No escriba su contraseña* — Nunca guarde su contraseña en un papel. Es mucho más seguro memorizarla.
- *No utilice la misma contraseña para todas las máquinas* — Es importante que cada máquina tenga una contraseña diferente. De esta forma, si un sistema es comprometido, no todas sus máquinas estarán en peligro inmediato.

Las siguientes pautas lo ayudarán a crear una contraseña robusta:

- *Cree contraseñas de al menos ocho caracteres* — Mientras más larga sea la contraseña, mejor. Si está usando contraseñas MD5, debería ser de 15 caracteres de largo o más. Con las contraseñas DES, use el largo máximo (ocho caracteres).
- *Mezcle letras mayúsculas y minúsculas* — Red Hat Enterprise Linux distingue entre mayúsculas y minúsculas, por la tanto mezcle las letras para reforzar su contraseña.
- *Mezcle letras y números* — Agregando números a las contraseñas, especialmente cuando se añaden en el medio (no solamente al comienzo o al final), puede mejorar la fortaleza de su contraseña.
- *Incluya caracteres no alfanuméricos* — Los caracteres especiales tales como &, $, y > pueden mejorar considerablemente su contraseña (esto no es posible si esta usando contraseñas DES).
- *Seleccione una contraseña que pueda recordar* — La mejor contraseña en el mundo será de poca utilidad si usted no puede recordarla. Por lo tanto utilice acrónimos u otros dispositivos nemónicos que lo ayuden a memorizar las contraseñas.

Con todas estas reglas, puede parecer difícil crear una contraseña que reuna todos estos requisitos y evite, a la vez, los rasgos de las malas contraseñas. Afortunadamente, hay algunos pasos que uno puede tomar para generar una contraseña segura y fácil de recordar.

1.3.1.1. Metodología para la creación de contraseñas seguras

Hay muchos métodos que la gente utiliza para crear contraseñas seguras. Uno de los métodos más populares incluyen acrónimos. Por ejemplo:

- Piense en una frase memorable, tal como:

  "Es más fácil creer que pensar con espíritu crítico."

- Luego, cámbielo a un acrónimo (incluyendo la puntuación).

  emfcqpcec.

- Añada un poco de complejidad sustituyendo números y símbolos por letras en el acrónimo. Por ejemplo, sustituya**7** por **e** y el símbolo arroba (**@**) por **c**:

  7mf@qp@7@.

- Añada un poco más de complejidad colocando mayúscula al menos a una letra, tal como **M**.

  7Mf@qp@7@.

- *Por último, no utilice esta contraseña de ejemplo en ninguno de sus sistemas*.

Mientras que la creación de contraseñas seguras es imperativo, manejarlas adecuadamente es también importante, especialmente para los administradores de sistemas dentro de grandes organizaciones. La próxima sección detalla buenos hábitos en la creación y manejo de contraseñas de usuarios dentro de una organización.

1.3.2. Creación de cuentas de usuario dentro de la organización

Si hay un número significativo de usuarios dentro de una organización, los administradores de sistemas tienen dos opciones básicas disponibles para forzar el uso de buenas contraseñas. Ellos pueden crear contraseñas para el usuario o dejar que los usuarios crean sus propias contraseñas, a la vez que verifican que las contraseñas sean de calidad aceptable.

Al crear las contraseñas para los usuarios se asegura de que las contraseñas sean buenas, pero se vuelve una tarea agotadora a medida que la organización crece. También incrementa el riesgo de que los usuarios escriban sus contraseñas en papel.

Por estas razones, la mayoría de los administradores de sistemas prefieren dejar que los usuarios creen sus propias contraseñas, pero verifican de una forma activa que las contraseñas sean buenas y, en algunos casos, obligan a los usuarios a cambiarlas periódicamente haciéndolas caducar.

1.3.2.1. Forzar la creación de contraseñas robustas

Para proteger la red contra intrusos, es aconsejable que los administradores de sistemas verifiquen que las contraseñas usadas dentro de la organización sean robustas. Cuando se les pide a los usuarios crear o modificar sus contraseñas, ellos pueden utilizar la aplicación de la línea de comandos `passwd`, la cual reconoce *PAM* (*Pluggable Authentication Manager*) y por lo tanto verificará si la contraseña es fácil de descifrar o si es demasiado corta, a través del módulo PAM `pam_cracklib.so`. Puesto que PAM es personalizable, es posible añadir más verificaciones para la integridad de la contraseña, tales como `pam_passwdqc` (disponible en http://www.openwall.com/passwdqc/) o escribir un nuevo módulo. Para una lista de los módulos PAM disponibles, consulte http://www.kernel.org/pub/linux/libs/pam/modules.html. Para obtener mayor información sobre PAM, consulte el Sección 4, “Pluggable Authentication Modules (PAM)”.

Sin embargo, es importante resaltar que la verificación realizada en las contraseñas al momento de su creación, no descubren las malas contraseñas de forma tan efectiva como lo haría un programa específico para descifrado ejecutado sobre las contraseñas dentro de la organización.

Hay muchos programas de descifrado de contraseñas que corren bajo Red Hat Enterprise Linux, aunque ninguno es suministrado con el sistema operativo. Abajo se muestra una breve lista de algunos de los programas de descifrado de contraseñas más populares:

Nota

Ninguna de estas herramientas son suministradas con Red Hat Enterprise Linux y, por lo tanto, no son soportadas por Red Hat, Inc. de ninguna manera.

- ***John The Ripper*** — Un programa rápido y flexible de descifrado de contraseñas. Permite el uso de múltiples listas de palabras y es capaz de usar descifrado de contraseñas con fuerza bruta. Está disponible en http://www.openwall.com/john/.
- ***Crack*** — Quizás el software más conocido sobre descifrado de contraseñas; muy rápido, pero no tan fácil de usar como **John The Ripper**. Se puede encontrar en línea desde http://www.crypticide.com/users/alecm/.
- ***Slurpie*** — **Slurpie** es similar a **John The Ripper** y a **Crack** excepto que está diseñado para ejecutarse en varias máquina simultáneamente, creando un ataque de contraseñas distribuido. Se puede encontrar junto a otros grupos de herramientas de evaluación de ataques distribuidos a la seguridad en http://www.ussrback.com/distributed.htm.

Advertencia

Siempre obtenga autorización por escrito antes de intentar descifrar las contraseñas dentro de la organización.

1.3.2.2. Envejecimiento de las contraseñas

El envejecimiento de contraseñas es una técnica utilizada por los administradores de sistemas para defenderse de las malas contraseñas dentro de la organización. El envejecimiento de contraseñas significa que luego de un tiempo determinado (usualmente 90 días) se le pide al usuario que creee una nueva contraseña. La teoría detrás de esto es que si un usuario es forzado a cambiar su contraseña periódicamente, una contraseña que ha sido descifrada por un cracker sólo le es útil por un tiempo determinado. La desventaja del envejecimiento de contraseñas, es que los usuarios tienden a escribir sus contraseñas.

Existen dos programas principales usados para especificar la caducidad de contraseñas bajo Red Hat Enterprise Linux, el comando `chage` o la aplicación gráfica **Gestor de usuarios** (`system-config-users`).

La opción `-M` del comando `chage` especifica el número de días máximo en que la contraseña será válida. Por lo tanto, si desea que la contraseña de un usuario expire en 90 días, escriba el comando siguiente:

```
chage -M 90 <usuario>
```

En el comando anterior, reemplace `<usuario>` con el nombre del usuario. Para desactivar la expiración de contraseñas, es común utilizar un valor de `99999` después de la opción `-M` (esto equivale a un poco más de 273 años).

También puede utilizar el comando `chage` en modo interactivo para modificar múltiples envejecimientos de contraseñas y otros detalles de la cuenta. Utilice el siguiente comando para entrar en modo interactivo:

```
chage <usuario>
```

El siguiente es un ejemplo de una sesión interactiva utilizando este comando:

```
[root@interch-dev1 ~]# chage davido Changing the aging information for davido Enter the new value, or pres
```

Consulte las páginas man de chage para obtener información sobre las opciones disponibles.

También puede utilizar la aplicación gráfica **Gestor de usuarios** para crear políticas de envejecimiento de contraseñas. Tenga en cuenta que usted necesitará privilegios administrativos para utilizar este procedimiento.

1. En el panel, haga clic en **Sistema**, vaya a **Administración** y haga clic en **Usuarios y grupos** para iniciar el Gestor de usuarios. También puede escribir el comando `system-config-users` en el intérprete de comandos.
2. Haga clic en la pestaña **Usuarios** y seleccione el usuario requerido en la liste de usuarios.
3. Haga clic en **Propiedades** en la barra de herramientas para ver las propiedades de usuario (o escoja **Propiedades** en el menú **Archivo**).
4. Luego haga clic en la pestaña **Información de la contraseña** y seleccione la casilla para **Activar expiración de contraseña**.
5. Introduzca el valor requerido en el campo **Días requeridos antes de cambiar** y haga clic en **OK**.

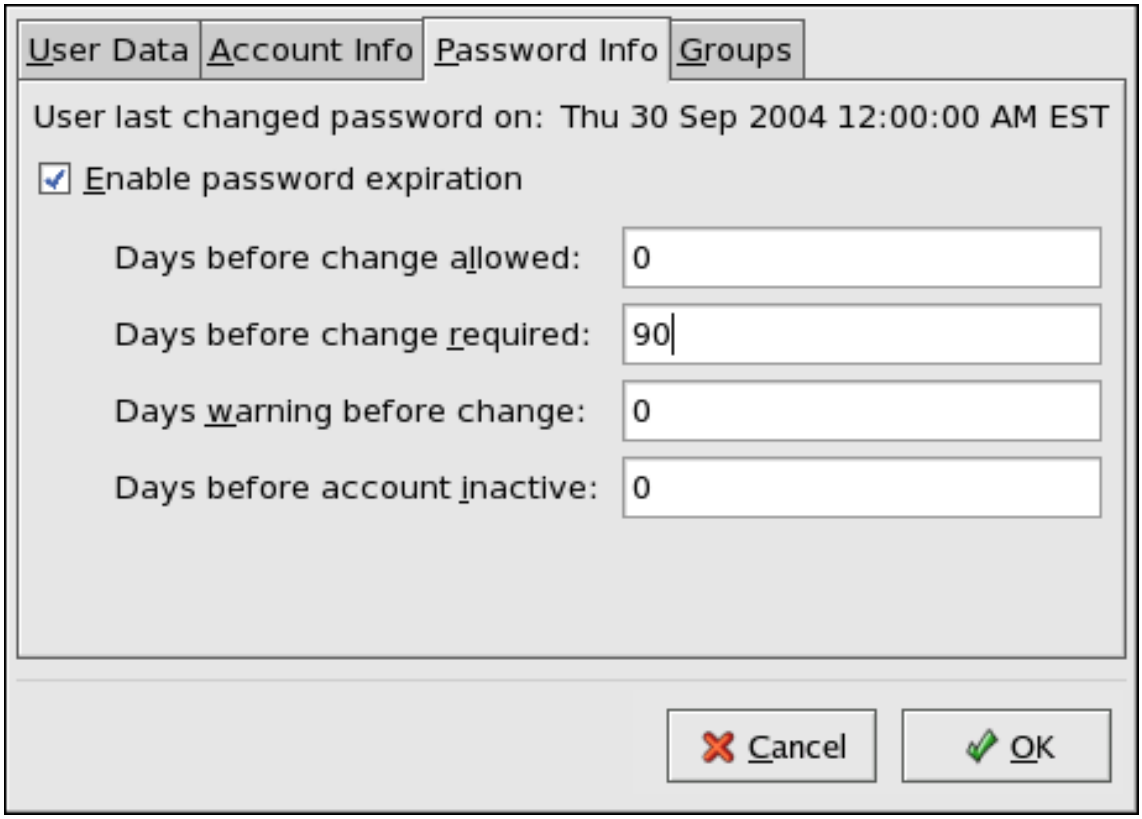


Figura 21.1. Especificando las opciones de envejecimiento de contraseñas

1.4. Controles administrativos

Cuando se está administrando una máquina casera, el usuario tiene que llevar a cabo algunas tareas como usuario root o adquiriendo privilegios de root a través de programas *setuid* como `sudo` o `su`. Un programa setuid es aquel que opera con el ID (*UID*) del usuario del dueño del programa en vez del usuario que esté operando el programa. Tales programas son denotados con una `s` en minúscula en la sección del dueño de un listado de formato largo:

```
-rwsr-xr-x 1 root root 47324 May 1 08:09 /bin/su
```

Nota

La `s` puede estar en mayúsculas o minúsculas. Si aparece en mayúsculas significa que el bit de permisos no ha sido establecido.

Sin embargo, los administradores de sistemas de una organización deben decidir cuánto acceso administrativo se le otorga a los usuarios dentro de la organización a sus máquinas. A través de un módulo PAM llamado `pam_console.so`, se le permite al primer usuario que se conecte en la consola física realizar algunas actividades normalmente reservadas para el superusuario, tales como el reinicio o el montaje de media removible (consulte el Sección 4, “Pluggable Authen-

tication Modules (PAM)" para obtener mayores detalles sobre el módulo `pam_console.so`). Sin embargo, otras tareas importantes de administración de sistemas, tales como la modificación de las configuraciones de la red, configurar un nuevo ratón o montar dispositivos de red, son imposibles sin privilegios administrativo. En consecuencia, los administradores deben decidir cuanto acceso administrativo deberían recibir los usuarios en su red.

1.4.1. Permitir el acceso como root

Si los usuarios dentro de la organización son de confianza y saben de computación, entonces darles acceso root quizás no sea una mala idea. Permitir el acceso root a los usuarios significa que los pequeños problemas, tales como añadir dispositivos o configurar interfaces de red, pueden ser manejados por los usuarios individuales, dejando a los administradores de sistemas libres para manejar la seguridad de la red y otras cosas de mayor importancia.

Por otro lado, dar acceso de superusuario a usuarios individuales puede conllevar a los siguientes problemas:

- *Configuración errónea de las máquinas* — Los usuarios con acceso root pueden configurar las máquinas de forma errónea y luego necesitar asistencia o peor aún, abrir huecos de seguridad sin saberlo.
- *Ejecutar servicios inseguros* — Los usuarios con acceso root pueden correr servicios inseguros en sus máquinas, tales como FTP o Telnet, colocando potencialmente los nombres de usuarios y sus contraseñas en riesgo. estos servicios transmiten la información a través de la red en texto llano.
- *Ejecutar anexos de correo electrónico como root* — Aún cuando es muy raro, si existen virus que afectan Linux. La única vez en que se convierten en una amenaza, es cuando son ejecutados por el usuario root.

1.4.2. Desactivación del acceso root

Si un administrador no está cómodo con permitir a los usuarios tener acceso como root por estas u otras razones, entonces la contraseña de root debería mantenerse en secreto y deshabilitar el acceso a nivel uno o en modo monousuario a través de la protección con contraseñas del gestor de arranque (consulte la Sección 1.2.2, "Contraseñas del gestor de arranque" para más detalles sobre este tema).

Tabla 21.1, "Métodos para deshabilitar la cuenta root" muestra las formas en que un administrador puede asegurar aún más que las conexiones como root estén prohibidas.

Método	Descripción	Efectos	No afecta
Cambiar el shell de root.	Modifique el archivo `/etc/passwd` y cambie el shell de `/bin/bash` a `/sbin/nologin`.	Previene el acceso a la shell de root y registrar cualquier intento de hacerlo. Se previene el acceso a la cuenta root a los siguientes programas: · `login`	Programas que no requieren una shell, como clientes FTP, clientes de correo y varios programas setuid. A los siguientes programas *no* se les previene el acceso a la cuenta root:

Método	Descripción	Efectos	No afecta
		· gdm · kdm · xdm · su · ssh · scp · sftp	· sudo · clientes FTP · Clientes de correo-e
Deshabilitar el acceso root a través de cualquier dispositivo de consola (tty).	Un archivo /etc/securetty vacío previene la conexión como root en cualquier dispositivo conectado a la computadora.	Prevenir el acceso a la cuenta root a través de la consola o la red. A los siguientes programas se les previene el acceso a la cuenta root: · login · gdm · kdm · xdm · Otros servicios de red que abren una tty	Los programas que no inician una sesión como root pero que ejecutan tareas de administración a través de setuid u otros mecanismos. A los siguientes programas *no* se les previene el acceso a la cuenta root: · su · sudo · ssh · scp · sftp
Deshabilitar conexiones root SSH.	Modifique el archivo /etc/ssh/sshd_config y configure el parámetro PermitRootLogin a no.	Previene el acceso a root a través del conjunto de herramientas OpenSSH. A los siguientes programas se les previene el acceso a la cuenta de root: · ssh · scp · sftp	Esto sólo previene el acceso root al conjunto de herramientas OpenSSH.
Utilizar PAM para limitar el acceso a servicios desde root.	Modifique el archivo para el servicio objetivo en el directorio /etc/pam.d/. Asegúrese que pam_listfile.so sea requerido para la autenticación.[a]	Prevenir el acceso a root a los servicios de red que reconocen PAM. A los siguientes servicios se les previene el acceso a la cuenta root: · clientes FTP · Clientes de correo-e · login · gdm · kdm · xdm · ssh · scp	Programas y servicios que no reconozcan PAM.

Método	Descripción	Efectos	No afecta
		· `sftp` · Cualquier servicio que reconozca PAM	

Tabla 21.1. Métodos para deshabilitar la cuenta root

[a] Consulte la Sección 1.4.2.4, “Deshabilitar root utilizando PAM” para obtener mayores detalles.

1.4.2.1. Deshabilitar el shell de root

Para prevenir que los usuarios se conecten directamente como root, el administrador del sistema puede configurar el shell de la cuenta root a `/sbin/nologin` en el archivo `/etc/passwd`. Esto impedirá el acceso a la cuenta root a través de comandos que requieren un shell, tal como los comandos `su` y `ssh`.

Importante

Los programas que no requieren acceso al shell, tales como los clientes de correo electrónico o el comando `sudo`, aún pueden tener acceso a la cuenta root.

1.4.2.2. Deshabilitar las sesiones root

Para limitar aún más el acceso a la cuenta root, los administradores pueden desactivar las conexiones root en la consola, editando el archivo `/etc/securetty`. Este archivo lista todos los dispositivos a los cuales el usuario root puede conectarse. Si el archivo no existe, el usuario puede conectarse a través de cualquier dispositivo de comunicación en el sistema, bien sea a través de la consola o una interfaz de red sin configurar. Esto es peligroso porque un usuario puede hacer Telnet en su máquina como root, enviando su contraseña sobre la red en texto plano. Por defecto, el archivo `/etc/securetty` de Red Hat Enterprise Linux,, sólo permite que el usuario root se conecte en la consola conectada físicamente a la máquina. Para prevenir que el usuario root se conecte, elimine los contenidos de este archivo escribiendo el comando siguiente:

```
echo > /etc/securetty
```

Advertencia

Un archivo `/etc/securetty` en blanco *no* previene al usuario root conectarse remotamente usando el conjunto de herramientas OpenSSH, ya que la consola no se abre sino hasta después de que se obtenga la autenticación.

1.4.2.3. Deshabilitar conexiones root SSH

Para prevenir las conexiones de root a través del protocolo SSH, modifique el archivo de configuración del demonio SSH (`/etc/ssh/sshd_config`). Cambie la línea que dice:

```
# PermitRootLogin yes
```

para que diga lo siguiente:

```
 PermitRootLogin no
```

1.4.2.4. Deshabilitar root utilizando PAM

PAM, a través del módulo `/lib/security/pam_listfile.so`, otorga gran flexibilidad en negar cuentas específicas. Esto permite al administrador apuntar el módulo a una lista de usuarios que no tienen derecho a conectarse. Abajo se muestra un ejemplo de cómo el módulo es usado por el servidor FTP `vsftpd` en el archivo de configuración PAM `/etc/pam.d/vsftpd` (el caracter `\` al final de la primera línea en el ejemplo siguiente *no* es necesario si la directiva esta en una sola línea):

```
auth required /lib/security/pam_listfile.so item=user \ sense=deny file=/etc/vsftpd.ftpusers onerr=succeed
```

Esto le dice a PAM que consulte el archivo `/etc/vsftpd.ftpusers` y que niegue el acceso al servicio a cualquier usuario que esté listado allí. El administrador tiene la libertad de cambiar el nombre de este archivo y de mantener una lista separada para cada servicio o de usar una lista central para negar el acceso a múltiples servicios.

Si el administrador desea negar el acceso a múltiples servicios, se puede añadir una línea similar a los servicios de configuración PAM, tales como `/etc/pam.d/pop` y `/etc/pam.d/imap` para los clientes de correo o `/etc/pam.d/ssh` para los clientes SSH.

Para obtener mayor información sobre PAM, consulte Sección 4, “Pluggable Authentication Modules (PAM)”.

1.4.3. Limitar el acceso root

En vez de negar completamente el acceso al superusuario, el administrador puede permitir el acceso solamente a través de programas setuid, tales como `su` o `sudo`.

1.4.3.1. El comando `su`

Después de ejecutar el comando `su`, se le solicita al usuario la contraseña de root y, luego de la autenticación, se le presenta un intérprete de comandos de shell.

Una vez conectado a través de `su`, el usuario se *convierte* en el superusuario y tiene acceso administrativo absoluto al sistema[8]. Además, una vez que el usuario obtiene acceso root es posible, en algunos casos, usar el comando `su` para cambiarse a cualquier otro usuario en el sistema sin que se le solicite una contraseña.

Debido a que este programa es tan poderoso, los administradores dentro de la organización pueden desear limitar el acceso a este comando.

Una de las formas más fáciles de hacer esto es añadir usuarios al grupo administrativo especial llamado *wheel*. Para añadirlos, escriba el siguiente comando como root:

[8] Este acceso está sujeto a las restricciones impuestas por SELinux, si éste está activado.

```
usermod -G wheel <usuario>
```

En el comando anterior, cambie `<usuario>` con el nombre del usuario que desea añadir al grupo `wheel`.

También puede utilizar el **Gestor de usuarios** para modificar las membresías a grupos. Tenga en cuenta que necesitará privilegios administrativos para ejecutar este procedimiento.

1. En el panel, haga clic en **Sistema**, vaya a **Administración** y haga clic en **Usuarios y grupos** para iniciar el Gestor de usuarios. También puede escribir el comando `system-config-users` en el intérprete de comandos.
2. Haga clic en la pestaña **Usuarios** y seleccione el usuario requerido en la liste de usuarios.
3. Haga clic en **Propiedades** en la barra de herramientas para ver las propiedades de usuario (o escoja **Propiedades** en el menú **Archivo**).
4. Luego seleccione la pestaña **Grupos** y seleccione la casilla de verificación para el grupo wheel. Haga clic en **OK** para finalizar. Observe la Figura 21.2, “Añadiendo usuarios al grupo "wheel".”.
5. Luego, abra el archivo de configuración PAM para `su` (`/etc/pam.d/su`) en un editor de texto y elimine el caracter de comentario # desde la línea siguiente:

   ```
   auth  required /lib/security/$ISA/pam_wheel.so use_uid
   ```

   Este cambio significa que sólo los miembros del grupo administrativo `wheel` pueden utilizar el programa.

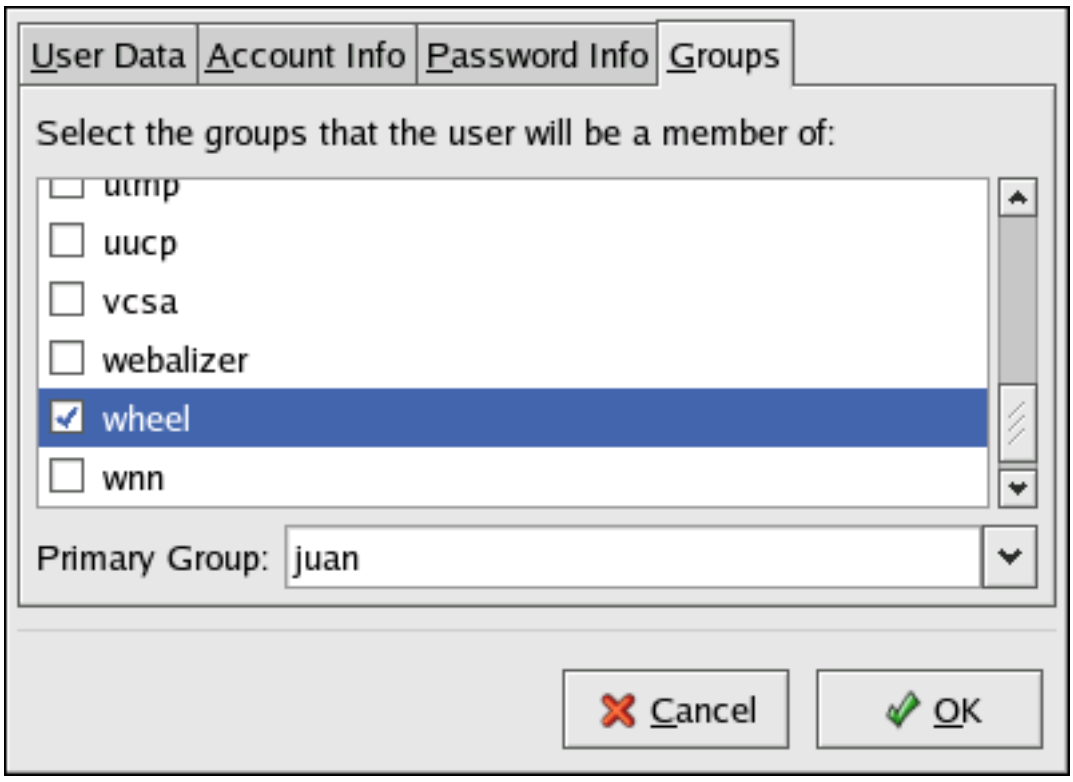


Figura 21.2. Añadiendo usuarios al grupo "wheel".

Nota

El usuario root es parte del grupo `wheel` por defecto.

1.4.3.2. El comando `sudo`

El comando `sudo` ofrece otra solución para otorgar acceso administrativo a los usuarios. Cuando un usuario de confianza antecede un comando administrativo con `sudo`, se le pide *su propia* contraseña. Luego, una vez autenticado y asumiendo que el comando es permitido, el comando administrativo es ejecutado como que si se tratase del usuario root.

El formato básico del comando `sudo` es el siguiente:

```
sudo <comando>
```

En el ejemplo anterior, `<comando>` sería reemplazado por un comando normalmente reservado para el usuario root, tal como `mount`.

Importante

Los usuarios del comando `sudo` deberían tener cuidado adicional al desconectarse antes de abandonar sus máquinas puesto que otros pueden utilizar el comando nuevamente sin que se les solicite contraseña alguna por un período de hasta cinco minutos. Esta configuración se puede alterar a través del archivo de configuración, `/etc/sudoers`.

El comando `sudo` permite un gran nivel de flexibilidad. Por ejemplo, solo los usuarios listados en el archivo de configuración `/etc/sudoers` tienen permitido utilizar el comando `sudo` y el comando es ejecutado en el shell *del usuario*, no en el shell de root. Esto significa que el shell de root podría ser desactivado completamente, como se muestra en la Sección 1.4.2.1, “Deshabilitar el shell de root”.

El comando `sudo` también proporciona un rastro completo para auditoría. Cada autenticación exitosa es registrada al archivo `/var/log/messages` y el comando emitido junto con el nombre del usuario se registran en el archivo `/var/log/secure`.

Otra ventaja del comando `sudo` es que un administrador puede permitir a usuarios diferentes acceso a comandos específicos basado en sus necesidades.

Los administradores que deseen modificar el archivo de configuración de `sudo`, `/etc/sudoers`, deberían usar el comando `visudo`.

Para otorgarle a un usuario privilegios administrativos completos, escriba `visudo` y añada una lí-

nea similar a la siguiente en la sección de especificación de privilegios del usuario:

```
juan ALL=(ALL) ALL
```

Este ejemplo establece que el usuario, `juan`, puede utilizar `sudo` desde cualquier máquina y ejecutar cualquier comando.

El ejemplo dado a continuación muestra qué tan detallado puede llegar a ser la configuración de `sudo`:

```
%users localhost=/sbin/shutdown -h now
```

Este ejemplo establece que cualquier usuario puede emitir el comando `/sbin/shutdown -h now` siempre y cuando sea emitido desde la consola.

La página de manual para `sudoers` tiene un listado detallado de las opciones para este archivo.

1.5. Servicios de red disponibles

Mientras que el acceso de usuarios a los controles administrativos es un aspecto importante para los administradores de sistemas dentro de una organización, también es de suma importancia para el que instala o maneja un sistema Linux mantener un registro sobre cuáles servicios de red están activos.

Muchos servicios bajo Red Hat Enterprise Linux se comportan como servidores de red. Si un servicio de red está ejecutándose en una máquina, entonces hay una aplicación de servidor (llamada *demonio*) escuchando por conexiones en uno o más puertos de red. Cada uno de estos servidores debería ser tratado como una avenida potencial de ataque.

1.5.1. Riesgos a los servicios

Los servicios de red pueden implicar muchos riesgos para los sistemas Linux. Abajo se muestra una lista de algunos de los principales problemas:

- *Ataques de rechazo de servicio (Denial of Service, DoS)* — Inundando un servicio con peticiones se puede producir un ataque de rechazo de servicio que llevaría al sistema a un estado suspendido, mientras éste intenta responder a cada petición.
- *Ataques de vulnerabilidad de scripts* — Si un servidor esta usando scripts para ejecutar acciones del lado del servidor, como usualmente hacen los servidores Web, un pirata puede montar un ataque a los scripts que no hayan sido escritos de forma apropiada. Estos ataques de vulnerabilidad de scripts podrían llevar a una condición de desbordamiento del buffer o permitir al atacante alterar archivos en el sistema.
- *Ataques de desbordamiento del buffer* — Los servicios que se conectan a puertos del 0 al 1023 deben ser ejecutados como un usuario administrativo. Si la aplicación tiene un posible desbordamiento del buffer, un atacante podría ganar acceso al sistema como el usuario ejecutando el demonio. Debido a que los desbordamientos del buffer existen, los maleantes informáticos usan herramientas automatizadas para identificar vulnerabilidades en los sistemas y una vez que han obtenido acceso, utilizan kits automatizados para mantener su acceso al sistema.

Nota

ExecShield puede mitigar las amenazas de un desbordamiento de la memoria intermedia en Red Hat Enterprise Linux. ExecShield es un ejecutable de segmentación de memoria y una tecnología de protección soportado por los kernels en uni o multi-procesadores x86. ExecShield reduce el riesgo del desbordamiento de memoria intermedia al separar la memoria virtual en segmentos ejecutables y no ejecutables. Cualquier código de programa que trate de ejecutarse en el segmento ejecutable (como por ejemplo, código malicioso inyectado desde un ataque de memoria intermedia) disparará una falla de segmentación y se cerrará.

ExecShield también incluye el soporte para la tecnología *No eXecute* (NX) en las plataformas AMD64 y la tecnología *eXecute Disable* (XD), en los sistemas Itanium y sistemas de 64 bits de Intel®. Estas tecnologías funcionan en conjunto con ExecShield para prevenir que el código malicioso se ejecute en la porción ejecutable de la memoria virtual con una granularidad de 4KB de código ejecutable, reduciendo el riesgo de un ataque desde un desbordamiento de búfer.

Concejo

Para limitar la exposición de ataques sobre la red, se deberían apagar todos los servicios que no se estén usando.

1.5.2. Identificación y configuración de servicios

Para mejorar la seguridad, la mayoría de los servicios de red instalados con Red Hat Enterprise Linux están desactivados por defecto. Sin embargo, hay algunas excepciones importantes:

- `cupsd` — El servidor de impresión por defecto para Red Hat Enterprise Linux.
- `lpd` — Un servidor de impresión alternativo.
- `xinetd` — Un super servidor que controla las conexiones a una serie de servidores subordinados, tal como `gssftp` y `telnet`.
- `sendmail` — El agente de transporte de correos Sendmail (MTA por sus siglas en inglés,*Mail Transport Agent*) está activado por defecto, pero sólo escucha conexiones desde localhost.
- `sshd` — El servidor OpenSSH, el cual es un reemplazo seguro para Telnet.

Cuando se está determinando si se deben dejar estos servicios en ejecución, es mejor usar el sentido común y pecar por el lado de la cautela. Por ejemplo, si usted no tiene impresora, no deje `cupsd` ejecutándose. Lo mismo para `portmap`. Si no tiene volúmenes NFSv3 o utiliza NIS (el servicio `ypbind`), entonces portmap también debería esta desactivado.

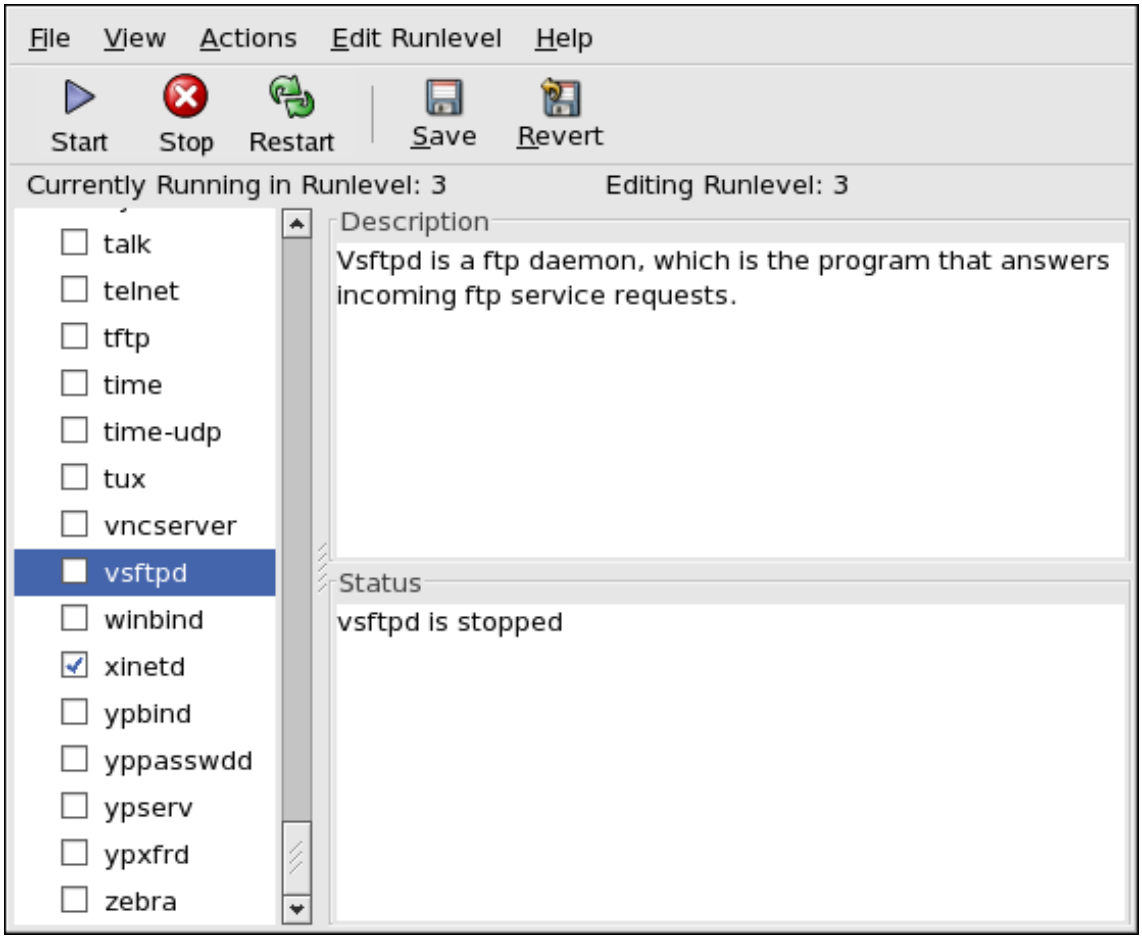


Figura 21.3. Herramienta de configuración de servicios

Si no está seguro del propósito de un servicio particular, la **Herramienta de configuración de servicios**, tiene un campo de descripción, mostrado en la Figura 21.3, “Herramienta de configuración de servicios”, que puede ser de ayuda.

Pero el verificar cuáles servicios están disponibles al momento del arranque no es suficiente. Los buenos administradores de sistemas deberían verificar cuáles puertos están abiertos y escuchando. Consulte la Sección 2.8, “Verificar cuáles puertos están escuchando” para obtener mayor información.

1.5.3. Servicios inseguros

Algunos protocolos de red son inherentemente más inseguros que otros. Esto incluye cualquier servicio que:

- *Pase los nombres de usuarios y contraseñas sobre la red sin encriptar* — Mucho protocolos viejos, tales como Telnet y FTP, no encriptan la sesión de autenticación y deberían ser evitados siempre que sea posible.
- *Pase datos confidenciales sobre la red sin encriptar* — Muchos protocolos pasan información sobre la red sin encriptar. Estos protocolos incluyen Telnet, FTP, HTTP y SMTP. Muchos sistemas de archivos de red, tales como NFS y SMB también pasan la información so-

bre la red sin encriptar. Cuando se estén usando estos protocolos es responsabilidad del usuario limitar el tipo de datos que se transmite.

Los servicios de volcado de memoria remota, como `netdump`, pasan los contenidos de la memoria sobre la red sin encriptar. Los volcados de memoria pueden contener contraseñas o, peor aún, entradas de la base de datos u otra información confidencial.

Otros servicios como `finger` y `rwhod` revelan información sobre los usuarios del sistema.

Ejemplos de servicios inherentemente inseguros incluyen:

- `rlogin`
- `rsh`
- `telnet`
- `vsftpd`

Todos los programas de conexión y de shell remotos (`rlogin`, `rsh` y `telnet`), deberían ser evitados en favor de SSH. (consulte la Sección 1.7, “Herramientas de mejoramiento de la seguridad” para más información sobre `sshd`).

FTP no es tan inherentemente peligroso para la seguridad de los sistemas como lo son los shells remotos, pero los servidores FTP deben ser configurados y monitoreados cuidadosamente para evitar problemas. Consulte la Sección 2.6, “Protección de FTP” para obtener mayor información sobre cómo asegurar los servidores FTP.

Los servicios que deberían ser implementados con sumo cuidado y colocados detrás de un cortafuegos incluyen:

- `finger`
- `authd` (era llamado `identd` en versiones anteriores de Red Hat Enterprise Linux).
- `netdump`
- `netdump-server`
- `nfs`
- `rwhod`
- `sendmail`
- `smb` (Samba)
- `yppasswdd`
- `ypserv`
- `ypxfrd`

En el Sección 2, “Seguridad de servidores” puede encontrar más información sobre el asegura-

miento de los servicios de red.

La próxima sección discute las herramientas disponibles para configurar un cortafuegos sencillo.

1.6. Cortafuegos personales

Una vez configurados los servicios de red *necesarios*, es importante implementar un cortafuegos.

Importante

Se debe configurar los servicios necesarios e implementar un cortafuegos *antes* de conectar el sistema a Internet o a otra red no confiable.

Los cortafuegos previenen que los paquetes de red accedan a la interfaz de la red del sistema. Si se hace una petición a un puerto que está bloqueado por un cortafuegos, se ignorará la petición. Si un servicio está escuchando en uno de estos puertos bloqueados, no recibirá paquetes y estará efectivamente inhabilitado. Por esta razón, se debe tener cuidado cuando se configure un cortafuegos para bloquear el acceso a los puertos que no se usen, a la vez que no se bloquea el acceso a los puertos usados por los servicios configurados.

Para la mayoría de los usuarios, la mejor herramienta para configurar un cortafuegos es la herramienta de configuración gráfica que viene con Red Hat Enterprise Linux: la **Herramienta de configuración del nivel de seguridad** (`system-config-selinux`). Esta herramienta crea reglas `iptables` amplias para un cortafuegos de propósito general, utilizando una interfaz de panel de control.

1.7. Herramientas de mejoramiento de la seguridad

En la medida que el tamaño y la popularidad de la Internet crece, así también ha crecido la interceptación de la comunicación. A lo largo de los años se han desarrollado herramientas para encriptar la comunicación cuando estas son llevadas sobre la red.

Red Hat Enterprise Linux se entrega con dos herramientas básicas que usan algoritmos de encriptación basados en criptografía de llaves pública de alto nivel para proteger la información a medida que ésta viaja sobre la red.

- *OpenSSH* — Una implementación del protocolo SSH gratuita para la encriptación de las comunicaciones de la red.
- *Gnu Privacy Guard (GPG)* — Una implementación gratuita de la aplicación de encriptación PGP (Pretty Good Privacy) para la encriptación de datos.

OpenSSH es una forma más segura de acceder a una máquina remota. Reemplaza los servicios no encriptados anteriores como `telnet` y `rsh`. OpenSSH incluye el servicio de red llamado `sshd` y tres aplicaciones cliente de línea de comandos:

- `ssh` — Un cliente seguro de acceso a consola remota.
- `scp` — Un comando seguro para hacer copias remotas.
- `sftp` — Un cliente seudo ftp que permite sesiones de transferencia de archivos interactivas.

GPG es una excelente forma de asegurar las comunicaciones de correo electrónico. Puede ser usado tanto para enviar información confidencial a través de correo sobre redes públicas, como para proteger los datos confidenciales en los discos duros.

2. Seguridad de servidores

Cuando un sistema es usado como un servidor en una red pública, se convierte en un objetivo de ataques. Por esta razón, es de suma importancia para el administrador fortalecer el sistema y bloquear servicios.

Antes de extendernos en problemas particulares, debería revisar los siguientes consejos generales para mejorar la seguridad del servidor:

- Mantenga todos los servicios actualizados para así protegerse de las últimas amenazas informáticas.
- Utilice protocolos seguros siempre que sea posible.
- Proporcione sólo un tipo de servicio de red por máquina siempre que sea posible.
- Supervise todos los servidores cuidadosamente por actividad sospechosa.

2.1. Asegurando los servicios con TCP Wrappers y xinetd

Los *TCP wrappers* proporcionan control de acceso a una variedad de servicios. La mayoría de los servicios modernos de redes, tales como SSH, Telnet y FTP, utilizan TCP wrappers como guardias entre las peticiones entrantes y el servicio solicitado.

Los beneficios ofrecidos por TCP wrappers son mejorados cuando se usan en conjunto con `xinetd`, un super servicio que proporciona acceso adicional, conexión, enlace, redirección y control de la utilización de recursos.

Las siguientes subsecciones asumen que ya se tiene un conocimiento básico de cada tópico y se enfoca en opciones de seguridad específicas.

2.1.1. Mejorar la seguridad con TCP Wrappers

Los TCP Wrappers son capaces de mucho más que simplemente negar el acceso a servicios. Esta sección ilustra cómo se pueden usar para enviar pancartas de conexión, avisar sobre ataques desde hosts particulares y mejorar la funcionalidad de conexión. Para una lista detallada de la funcionalidad y el lenguaje de control de los TCP Wrappers, consulte la página del manual de `hosts_options`.

2.1.1.1. Los TCP Wrappers y las pancartas de conexión

Al mostrar una pancarta apropiada cuando los usuarios se conectan a un servicio es una buena

forma de advertir a cualquier atacante potencial que el administrador del sistema está atento y vigilante. También se puede controlar la información del sistema que se presenta a los usuarios. Para implementar un mensaje de TCP wrapper para un servicio, utilice la opción `banner`.

Este ejemplo implementa una pancarta para `vsftpd`. Para comenzar, debe crear un archivo de pancartas. Este puede estar en cualquier lugar en el sistema, pero debe tener el mismo nombre que el demonio. Para este ejemplo, el archivo se llamará `/etc/banners/vsftpd`.

```
220-Hello, %c 220-All activity on ftp.example.com is logged. 220-Inappropriate use will result in your ac
```

La señal `%c` proporciona una variedad de información del cliente, tal como el nombre de usuario y del host o el nombre del usuario y la dirección IP para hacer la conexión aún más intimidante.

Para que esta pancarta sea presentada a las conexiones entrantes, añada la siguiente línea al archivo `/etc/hosts.allow`:

```
vsftpd : ALL : banners /etc/banners/
```

2.1.1.2. TCP Wrappers y las advertencias de ataques

Si se ha detectado a un host particular o a una red tratando de atacar al servidor, se pueden usar los TCP Wrappers para advertir de ataques subsecuentes desde esa máquina o red a través de la directiva `spawn`.

En este ejemplo, se asume que se ha detectado al cracker en la red 206.182.68.0/24 intentando atacar el servidor. Colocando la siguiente línea en el archivo `/etc/hosts.deny`, se niega el intento de conexión desde la red y se registra a un archivo especial:

```
ALL : 206.182.68.0 : spawn /bin/ 'date' %c %d >> /var/log/intruder_alert
```

La señal `%d` suministra el nombre del servicio que el atacante estaba tratando de acceder.

Para permitir la conexión y registrarla, coloque la directiva `spawn` en el archivo `/etc/hosts.allow`.

Nota

Puesto que la directiva `spawn` ejecuta cualquier comando del shell, puede crear un script especial para notificar al administrador o ejecutar una cadena de comandos en el evento de que un cliente particular intente conectarse al servidor.

2.1.1.3. TCP Wrappers y el mejoramiento de la conexión

Si ciertos tipos de conexión son de mayor preocupación que otros, se puede subir el nivel de conexión para ese servicio a través de la opción `severity`.

En este ejemplo, se asume que cualquiera que esté intentando conectarse al puerto 23 (el puerto de Telnet) en un servidor FTP, es un cracker. Para resaltarlo, coloque una bandera `emerg` en los archivos de registro en vez de la bandera por defecto, `info`, y niegue la conexión.

Para hacerlo, escriba la siguiente línea en `/etc/hosts.deny`:

```
in.telnetd : ALL : severity emerg
```

Esto usará la facilidad de conexión por defecto `authpriv`, pero subirá el nivel de prioridad del valor por defecto de `info` a `emerg`, lo cual manda los mensajes de registro directamente a la consola.

2.1.2. Aumentando la seguridad con xinetd

Esta sección se centra en el uso de `xinetd` para establecer un servicio trampa y controlar el nivel de recursos disponibles para cualquier servicio `xinetd`. Al establecer límites de recursos para los servicios dificulta los ataques de *denegación de servicios* (DoS). Para una lista de las opciones disponibles, consulte las páginas man de `xinetd` y `xinetd.conf`.

2.1.2.1. Colocando una Trampa

Una característica importante de `xinetd` es la habilidad de añadir hosts a una lista global de `no_access`. A los hosts en esta lista se les negará conexiones a los servicios manejados por `xinetd` por un tiempo determinado o hasta que se reinicie `xinetd`. Esto se logra usando el atributo `SENSOR`. Esta técnica es una forma fácil de bloquear máquinas que intenten escanear un puerto del servidor.

El primer paso en configurar un `SENSOR` es seleccionar un servicio que no planea utilizar. Para este ejemplo, se utilizará Telnet.

Modifique el archivo `/etc/xinetd.d/telnet` y cambie la línea `flags` para que muestre lo siguiente:

```
flags           = SENSOR
```

Agregue la línea siguiente:

```
deny_time       = 30
```

Esto negará al host el acceso al puerto por 30 minutos. Otros valores aceptables para el atributo `deny_time` son FOREVER, que mantiene el bloqueo hasta que se reinicie `xinetd`, y NEVER, que permite la conexión y la registra.

Finalmente, la última línea debería mostrar lo siguiente:

```
disable         = no
```

Esta línea activa la trampa.

Aún cuando el uso de `SENSOR` es una buena forma de detectar y detener conexiones de máquinas dañinas, tiene dos desventajas:

- No funcionará contra escaneos sigilosos.
- Un atacatante que sabe que usted está ejecutando un `SENSOR` puede montar un ataque DoS en contra de un host particular falsificando sus direcciones IP y conectándose al puerto prohibido.

2.1.2.2. Control de recursos del servidor

Otra característica importante de `xinetd` es la capacidad de controlar la cantidad de recursos que los servicios bajo su control pueden utilizar.

Esto se hace a través de las siguientes directrices:

- `cps = <number_of_connections> <wait_period>` — Limita la tasa de conexiones entrantes. Esta directiva acepta dos argumentos:
  - `<number_of_connections>` — El número de conexiones por segundo que serán manejadas. Si la tasa de conexiones entrantes es mayor que el número de conexiones, el servicio es temporalmente inhabilitado. El valor por defecto es (50).
  - `<wait_period>` — El número de segundos de espera antes de activar el servicio cuando éste ha sido deshabilitado. El intervalo predeterminado son (10) segundos.
- `instances = <number_of_connections>` — Indica el número total de conexiones permitidas al servicio. Esta directiva acepta bien sea un valor entero o `UNLIMITED`.
- `per_source = <number_of_connections>` — Especifica el número de conexiones permitidas al servicio por cada host. Esta directiva acepta un valor entero o `UNLIMITED`.
- `rlimit_as = <number[K|M]>` — Indica la cantidad de espacio de direcciones de memoria -en kilobytes o megabytes- que el servicio puede ocupar. Esta directiva acepta valores enteros o `UNLIMITED`.
- `rlimit_cpu = <number_of_seconds>` — Indica la cantidad de tiempo en segundos que un servicio puede ocupar el CPU. Esta directiva acepta un valor entero o `UNLIMITED`.

El uso de estas directivas ayuda a prevenir que cualquier servicio `xinetd` sobresature el sistema, resultando en una denegación de servicio.

2.2. Protección de Portmap

El servicio `portmap` es un demonio de asignación de puertos dinámico para servicios RPC, tales como NIS y NFS. Tiene mecanismos de autenticación débiles y la habilidad de asignar un amplio rango de puertos para los servicios que controla. Por estas razones, es difícil de asegurar.

Nota

El asegurar `portmap` solamente afecta a las implementaciones de NFSv2 y NFSv3 , puesto que NFSv4 ya no lo requiere. Si planea implementar un servidor NFSv2 o NFSv3, entonces se requiere `portmap`. La sección siguiente es relevante en dicho caso.

Si está ejecutando servicios RPC, debería seguir algunas reglas básicas.

2.2.1. Proteja portmap con TCP Wrappers

Es importante utilizar TCP Wrappers para limitar las redes o máquinas que tienen acceso al servicio `portmap` puesto que éste no posee autenticación incorporada.

Además, utilice *solamente* direcciones IP cuando esté limitando el acceso al servicio. Evite los nombres de hosts, pues estos pueden ser falsificados a través de envenenamiento de DNS y otros métodos.

2.2.2. Proteja portmap con iptables

Para restringir más aún el acceso al servicio `portmap`, es aconsejable añadir reglas de iptables al servidor para así limitar el acceso a redes específicas.

A continuación se muestran dos ejemplos de comandos iptables. El primero permite conexiones TCP al puerto 111 (usado por el servicio `portmap`) desde la red 192.168.0/24. El segundo permite conexiones TCP al mismo puerto desde el host local. Esto es necesario para el servicio `sgi_fam` utilizado por **Nautilus**. Todos los demás paquetes son descartados.

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24 --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1  --dport 111 -j ACCEPT
```

Para limitar el tráfico UDP de forma similar, utilice el comando siguiente.

```
iptables -A INPUT -p udp -s! 192.168.0.0/24  --dport 111 -j DROP
```

2.3. Protección de NIS

El *servicio de información de redes* (NIS) es un servicio RPC llamado `ypserv`. Éste es usado en conjunto con `portmap` y otros servicios relacionados para distribuir mapas de nombres de usuarios, contraseñas y otra información confidencial a cualquier computador que se encuentre dentro de su dominio.

Un servidor NIS esta compuesto de varias aplicaciones. Ellas incluyen las siguientes:

- `/usr/sbin/rpc.yppasswdd` — También llamado el servicio `yppasswdd`, este demonio permite a los usuarios cambiar sus contraseñas NIS.
- `/usr/sbin/rpc.ypxfrd` — También llamado `ypxfrd`, es el demonio responsable de las transferencias de mapas NIS sobre la red.
- `/usr/sbin/yppush` — Esta aplicación propaga las bases de datos NIS modificadas a múltiples servidores NIS.
- `/usr/sbin/ypserv` — Este es el demonio del servidor NIS.

NIS es inseguro según los estándares actuales. No tiene mecanismos de autenticación de host y pasa toda la información sobre la red sin encriptación -incluyendo las contraseñas. Como consecuencia, se debe tener extremo cuidado cuando se configure una red que utilice NIS. Además, la configuración por defecto de NIS es insegura en sí misma.

Se recomienda que cualquiera que este planeando implementar un servidor NIS, primero ase-

gure el servicio `portmap` como se describió en la Sección 2.2, “Protección de Portmap” y luego considere los siguientes aspectos.

2.3.1. Planee la red cuidadosamente

Debido a que NIS pasa información confidencial sin encriptar sobre la red, es importante que se ejecute el servicio detrás de un cortafuegos y en una red segmentada y segura. Cada vez que se transmite información NIS a través de una red insegura, hay riesgos de que sea interceptada. Un cuidadoso diseño de la red en este aspecto puede ayudar a prevenir violaciones de la seguridad.

2.3.2. Utilice un nombre de dominio NIS y de host de tipo contraseña

Cualquier máquina dentro de un dominio NIS puede usar comandos para extraer información desde el servidor sin necesidad de autenticación, siempre y cuando el usuario conozca el nombre DNS y del dominio del servidor NIS.

Por ejemplo, si alguien conecta una portátil a la red o irrumpe en la red desde afuera (y logra simular una dirección IP interna), el comando siguiente revelará el mapa `/etc/passwd`:

```
ypcat -d <NIS_domain> -h <DNS_hostname> passwd
```

Si este atacante es un usuario root, podrá obtener el archivo `/etc/shadow` escribiendo el comando siguiente:

```
ypcat -d <NIS_domain> -h <DNS_hostname> shadow
```

Nota

Si se utiliza Kerberos, el archivo `/etc/shadow` no se almacena dentro del mapa NIS.

Para hacer el acceso a los mapas NIS más difícil para un atacante, cree una cadena de caracteres aleatoria para el nombre DNS de la máquina, tal como `o7hfawtgmhwg.domain.com`. De la misma manera, cree un nombre aleatorio *diferente* para el nombre de dominio NIS. Esto hará mucho más difícil a un atacante accesar el servidor NIS.

2.3.3. Modifique el archivo `/var/yp/securenets`

NIS escuchará a todas las redes si el archivo `/var/yp/securenets` está en blanco o no existe (este es el caso predeterminado después de una instalación). Una de las primeras cosas que debería hacer es colocar los pares máscaras/redes en el archivo para que `ypserv` sólo responda a las peticiones desde la red adecuada.

A continuación se muestra una entrada de ejemplo de un archivo `/var/yp/securenets`:

```
255.255.255.0     192.168.0.0
```

Aviso

Nunca arranque el servidor NIS por primera vez sin crear el archivo `/var/yp/securenets`.

Esta técnica no proporciona protección ante un ataque de simulación de IP (IP spoofing), pero al menos coloca límites en qué redes servirá el servidor NIS.

2.3.4. Asigne puertos estáticos y uso de reglas iptables

A todos los servidores relacionados con NIS se les pueden asignar puertos específicos excepto por `rpc.yppasswdd` — el demonio que permite a los usuarios cambiar sus contraseñas de conexión. Asignar puertos a los otros dos demonios de servidores NIS, `rpc.ypxfrd` y `ypserv`, permite crear reglas de cortafuegos para proteger aún más los demonios del servidor NIS contra los intrusos.

Para hacer esto, añada las líneas siguientes a `/etc/sysconfig/network`:

```
YPSERV_ARGS="-p 834" YPXFRD_ARGS="-p 835"
```

Las siguientes reglas iptables se pueden emitir para establecer la red a la cual el servidor escucha a través de estos puertos:

```
iptables -A INPUT -p ALL -s! 192.168.0.0/24  --dport 834 -j DROP
iptables -A INPUT -p ALL -s! 192.168.0.0/24  --dport 835 -j DROP
```

Lo que significa que el servidor solo permite conexiones a los puertos 834 y 835 si las peticiones provienen de la red 192.168.0.0/24 y sin importar el protocolo.

2.3.5. Utilice autenticación Kerberos

Una de las debilidades inherentes más resaltantes cuando se utiliza NIS para autenticación, es que cada vez que un usuario se conecta a una máquina se envia el hash de la contraseña desde `/etc/shadow` a través de la red. Si un intruso obtiene acceso a un dominio NIS y rastrea el tráfico de la red, puede reunir fácilmente los nombres de usuarios y contraseñas. Con el tiempo suficiente, un programa de descifrado de contraseñas puede adivinar las contraseñas débiles y el atacante puede obtener acceso a una cuenta válida en la red.

2.4. Protección de NFS

Importante

La versión de NFS incluida en Red Hat Enterprise Linux, NFSv4, ya no requiere del servicio `portmap` como se describe en la Sección 2.2, “Protección de Portmap”. El tráfico NFS ahora utiliza TCP en todas las versiones, en vez de UDP, y se requiere cuando se utiliza NFSv4. NFSv4 incluye la autenticación de usuarios y grupos de Kerberos, como parte del módulo `RPCSEC_GSS`. Aún se incluye la información

sobre `portmap`, puesto que Red Hat Enterprise Linux es compatible con NFSv2 y NFSv3 y estos lo necesitan.

2.4.1. Planee la red cuidadosamente

Debido a que NFSv4 tiene la habilidad de pasar toda la información encriptada sobre la red usando Kerberos, es importante que el servicio sea configurado correctamente si se encuentra detrás de un cortafuegos o en un segmento de la red. NFSv2 y NFSv3 aún envían la información de forma insegura. Un diseño cuidadoso en este aspecto puede ayudar a prevenir violaciones de la seguridad.

2.4.2. Cuidado con los errores sintácticos

El servidor NFS determina cuáles sistemas de archivos exportar y a cuáles máquinas exportar estos directorios a través del archivo `/etc/exports`. Tenga cuidado de no añadir espacios adicionales cuando edite este archivo.

Por ejemplo, la línea siguiente en el archivo `/etc/exports` comparte el directorio `/tmp/nfs/` al host `bob.example.com` con permisos de lectura y escritura.

```
/tmp/nfs/     bob.example.com(rw)
```

Por otro lado, esta línea en el archivo `/etc/exports`, comparte el mismo directorio con el host `bob.example.com` con permisos de sólo lectura y lo comparte con *todo el mundo* con permisos de lectura y escritura debido al espacio en blanco luego del nombre de la máquina.

```
/tmp/nfs/     bob.example.com (rw)
```

Es un buen hábito verificar cualquier directorio compartido NFS usando el comando `showmount` para verificar que está siendo compartido:

```
showmount -e <hostname>
```

2.4.3. No utilice la opción `no_root_squash`

Por defecto, los directorios compartidos NFS cambian el usuario root por el usuario `nfsnobody`, una cuenta de usuario sin privilegios. De esta forma, todos los archivos creados por root son propiedad del usuario `nfsnobody`, lo que previene la carga de programas con el bit setuid establecido.

Si se utiliza `no_root_squash`, los usuarios remotos podrán cambiar cualquier archivo en el sistema de archivos compartido y dejar aplicaciones con troyanos para que otros usuarios las ejecuten inadvertidamente.

2.5. Protegiendo el servidor Apache HTTP

El Servidor Apache HTTP es uno de los servicios más estables y seguros que se entregan con Red Hat Enterprise Linux. Hay una cantidad impresionante de opciones y técnicas disponibles para asegurar el servidor Apache HTTP — demasiadas para verlas en profundidad en este do-

cumento.

Los administradores de sistemas deben ser cuidadosos cuando utilicen las siguientes opciones de configuración:

2.5.1. `FollowSymLinks`

Esta directiva está activada por defecto, por lo tanto tenga cuidado al crear enlaces simbólicos al documento raíz del servidor Web. Por ejemplo, es una mala idea proporcionar un enlace simbólico a `/`.

2.5.2. La directiva `Indexes`

Esta directiva está activada por defecto, pero puede que no sea recomendable. Si no desea que los usuarios hojeen los archivos en el servidor, es mejor que elimine esta directiva.

2.5.3. La directiva `UserDir`

La directiva `UserDir` está desactivada por defecto porque puede confirmar la presencia de una cuenta de usuario en el sistema. Si desea activar la navegación del directorio del usuario en el servidor, utilice las directivas siguientes:

```
UserDir enabled
UserDir disabled root
```

Estas directivas activan la navegación del directorio del usuario para todos los directorios de usuarios excepto `/root`. Si desea añadir usuarios a la lista de cuentas deshabilitadas, añada una lista de usuarios separadas por espacios en la línea `UserDir disabled`.

2.5.4. No elimine la directiva `IncludesNoExec`

Por defecto, el módulo *Server-Side Includes* (SSI no pueden ejecutar comandos. No se recomienda modificar esta configuración a menos que tenga absoluta necesidad de hacerlo, puesto que potencialmente habilita a que un atacante pueda ejecutar comandos en el sistema.

2.5.5. Limite los permisos para los directorios ejecutables

Asegúrese de que solamente el usuario root tenga permisos de escritura para cualquier directorio que contenga scripts o CGIs. Esto se puede lograr escribiendo los comandos siguientes:

```
chown root <directory_name>
chmod 755 <directory_name>
```

Importante

Verifique que cualquier script que esté ejecutando en el sistema funcione como se espera *antes* de colocarlos en producción.

2.6. Protección de FTP

El *Protocolo de transferencia de archivos* (*FTP*), es un protocolo TCP antiguo diseñado para transferir archivos sobre la red. Debido a que todas las transacciones con el servidor no son encriptadas, incluyendo la autenticación de usuarios, se considera un protocolo inseguro y debería ser configurado cuidadosamente.

Red Hat Enterprise Linux proporciona tres servidores FTP.

- `gssftpd` — Un demonio FTP kerberizado basado en `xinetd` que no pasa información de autenticación sobre la red.
- **Red Hat Content Accelerator** (`tux`) — Un servidor Web con espacio kernel que posee capacidades de FTP.
- `vsftpd` — Una implementación de servicio FTP independiente y orientado a la seguridad.

Las siguientes pautas de seguridad son para la configuración del servicio FTP `vsftpd`.

2.6.1. Pancarta de saludo de FTP

Antes de suministrar un nombre de usuario y contraseña, a todos los usuarios se les presenta una pancarta de saludo. Por defecto, esta pancarta incluye información relacionada con la versión, lo que es útil para los maleantes informáticos que estén intentando averiguar las debilidades del sistema.

Para cambiar la pancarta de bienvenida para `vsftpd`, añada la directiva siguiente a `/etc/vsftpd/vsftpd.conf`:

```
ftpd_banner=<insert_greeting_here>
```

Reemplace `<insert_greeting_here>` en la directiva de arriba con el texto de su mensaje de bienvenida.

Para pancartas de varias líneas, es mejor utilizar un archivo de pancartas. Para simplificar la administración de múltiples pancartas, coloque todas las pancartas en un nuevo directorio llamado `/etc/banners/`. El archivo de pancartas para las conexiones FTP en este ejemplo será `/etc/banners/ftp.msg`. Abajo se muestra un ejemplo de como se vería tal archivo:

```
######### # Hola, toda actividad en ftp.example.com es registrada. #########
```

Nota

No es necesario comenzar cada línea del archivo con `220` como se especifica en la Sección 2.1.1.1, “Los TCP Wrappers y las pancartas de conexión”.

Para hacer referencia a este archivo de pancartas desde `vsftpd`, añada la siguiente directiva al archivo `/etc/vsftpd/vsftpd.conf`:

```
banner_file=/etc/banners/ftp.msg
```

También es posible enviar pancartas adicionales a las conexiones entrantes usando TCP wrappers como se describió en la Sección 2.1.1.1, “Los TCP Wrappers y las pancartas de conexión”.

2.6.2. Acceso anónimo

La presencia del directorio `/var/ftp/` activa la cuenta anónima.

La forma más fácil de crear este directorio es instalando el paquete `vsftpd`. Este paquete configura un árbol de directorios y configura los permisos en estos directorios como de sólo lectura para los usuarios anónimos.

Por defecto los usuarios anónimos no pueden escribir a estos directorios.

Atención

Si está activando el acceso anónimo a un servidor FTP, tenga cuidado de dónde guarda información confidencial.

2.6.2.1. Carga anónima

Si desea permitir a los usuarios anónimos que carguen archivos al servidor, se recomienda que cree un directorio de sólo escritura dentro de `/var/ftp/pub/`.

Utilice el comando siguiente.

```
mkdir /var/ftp/pub/upload
```

Luego, cambie los permisos para que los usuarios anónimos no puedan ver qué hay dentro del directorio:

```
chmod 730 /var/ftp/pub/upload
```

Un listado de formato largo del directorio debería verse como:

```
drwx-wx---    2 root     ftp          4096 Feb 13 20:05 upload
```

Aviso

Los administradores que permiten a los usuarios anónimos leer y escribir en directorios, a menudo encuentran que sus servidores se convierten en depósitos de software robado.

Adicionalmente, bajo `vsftpd`, añada la línea siguiente a `/etc/vsftpd/vsftpd.conf`:

```
anon_upload_enable=YES
```

2.6.3. Cuentas de usuarios

Debido a que FTP pasa los nombres de usuarios y contraseñas sobre redes inseguras sin encriptar, es una buena idea negar a los usuarios del sistema el acceso al servidor desde sus cuentas de usuario.

Para inhabilitar las cuentas de usuarios en `vsftpd`, añada la siguiente directiva a `/etc/vsftpd/vsftpd.conf`:

```
local_enable=NO
```

2.6.3.1. Restringir cuentas de usuarios

También es posible desactivar las cuentas de usuario dentro de cada servicio directamente.

Para deshabilitar una cuenta de usuario específica en `vsftpd`, añada el nombre de usuario a `/etc/vsftpd.ftpusers`.

2.6.4. Usar TCP Wrappers para controlar el acceso

Utilice TCP Wrappers para controlar el acceso a cualquier demonio FTP como se describió en la Sección 2.1.1, “Mejorar la seguridad con TCP Wrappers”.

2.7. Asegurando Sendmail

Sendmail es un Agente de transporte de correos (MTA) que utiliza el protocolo simple de transferencia de correo electrónico (SMTP, según sus siglas en inglés) para entregar mensajes electrónicos entre otros MTA y a clientes de correo o agentes de entrega. Aún cuando muchos MTAs son capaces de encriptar el tráfico entre unos y otros, la mayoría no lo hacen, por tanto el envío de correos electrónicos sobre redes públicas es considerado una forma insegura de comunicación.

Se recomienda que cualquiera que esté planeando implementar un servidor Sendmail, tenga en cuenta los siguientes problemas.

2.7.1. Limitar los Ataques de Rechazo de Servicio (DoS)

Debido a la naturaleza del correo electrónico, un atacante determinado puede inundar fácilmente el servidor con correos y de esta manera causar un rechazo de servicio. Se puede limitar la efectividad de tales ataques colocando límites a las siguientes directrices en `/etc/mail/sendmail.mc`.

- `confCONNECTION_RATE_THROTTLE` — El número de conexiones que el servidor puede recibir por segundo. Por defecto, Sendmail no limita el número de conexiones. Si se establece un límite y este es alcanzado, las conexiones siguientes son retrasadas.
- `confMAX_DAEMON_CHILDREN` — El máximo número de procesos hijo que se pueden producir por el servidor. Por defecto, Sendmail no asigna un límite al número de procesos hijos. Si se coloca un límite y este es alcanzado, las conexiones siguientes son retrasadas.
- `confMIN_FREE_BLOCKS` — El número mínimo de bloques libres que debe haber disponible para

que el servidor acepte correos. Por defecto es 100 bloques.

- `confMAX_HEADERS_LENGTH` — El tamaño máximo aceptable (en bytes) para la cabecera de un mensaje.
- `confMAX_MESSAGE_SIZE` — El tamaño máximo aceptable (en bytes) para cualquier mensaje.

2.7.2. NFS y Sendmail

Nunca coloque el directorio spool de correos, `/var/spool/mail/`, en un volumen compartido NFS.

Debido a que NFSv2 y NFSv3 no mantiene un control sobre los IDs de usuarios y de grupos, dos o más usuarios pueden tener el mismo UID y, por tanto, recibir y leer los correos electrónicos del otro.

Nota

Con NFSv4 usando Kerberos, este no es el caso, puesto que el módulo del kernel `SECRPC_GSS` no utiliza una autenticación basándose en UID. Sin embargo, se considera una buena práctica el *no* ubicar el directorio spool de correos en un volumen compartido NFS.

2.7.3. Usuarios de correo únicamente

Para ayudar a prevenir explotaciones del usuario local en el servidor Sendmail, es mejor que los usuarios de correo electrónico solamente accedan al servidor Sendmail usando un programa de correo. No deberían permitirse las cuentas shell en el servidor de correo y todos los usuarios shell en el archivo `/etc/passwd` deberían ser colocados a `/sbin/nologin` (con la posible excepción del usuario root).

2.8. Verificar cuáles puertos están escuchando

Una vez que haya configurado los servicios en la red, es importante poner atención sobre cuáles puertos estan escuchando en realidad en las interfaces de red del sistema. Cualquier puerto abierto puede ser una evidencia de una intrusión.

Existen dos soluciones básicas para listar los puertos que están escuchando en la red. La solución menos confiable es consultar la pila de la red escribiendo comandos tales como `netstat -an` o `lsof -i`. Este método es menos confiable puesto que estos programas no conectan a la máquina desde la red, solo verifican que está ejecutándose en el sistema. Por esta razón, estas aplicaciones son objetivos frecuentes de atacantes que reemplazan `netstat` y `lsof` con sus propias versiones para intentan cubrir sus rastros cuando abren puertos no autorizados.

Una forma más confiable de verificar qué puertos están escuchando en la red es usar un escaner de puertos como `nmap`.

El comando siguiente ejecutado desde la consola, determina cuáles puertos están escuchando por conexiones TCP desde la red:

```
nmap -sT -O localhost
```

La salida de este comando es parecida a lo siguiente:

```
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-24 13:49 EDT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
113/tcp   open  auth
631/tcp   open  ipp
834/tcp   open  unknown
2601/tcp  open  zebra
32774/tcp open  sometimes-rpc11
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 12.857 days (since Sat Sep 11 17:16:20 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 5.190 seconds
```

Esta salida muestra que el sistema está ejecutando `portmap` debido a la presencia del servicio `sunrpc`. Sin embargo, existe también un servicio misterioso en el puerto 834. Para verificar si el puerto está asociado con la lista oficial de servicios conocidos, escriba:

```
cat /etc/services | grep 834
```

Este comando no devuelve ninguna salida. Esto indica que aunque el puerto está en el rango reservado (es decir del 0 al 1023) y requiere acceso root para ser abierto, no está asociado con un servicio conocido.

Luego, puede verificar la información sobre el puerto usando `netstat` o `lsof`. Para verificar el puerto 834 usando `netstat`, utilice el comando siguiente:

```
netstat -anp | grep 834
```

El comando devuelve la siguiente salida:

```
tcp   0    0 0.0.0.0:834    0.0.0.0:*   LISTEN   653/ypbind
```

La presencia de un puerto abierto en `netstat` es tranquilizante puesto que un maleante abriendo un puerto furtivamente en un sistema violado, posiblemente no se revelaría a través de este comando. Además, la opción `[p]` revela el id del proceso (PID) del servicio que abrió el puerto. En este caso, el puerto abierto pertenece a `ypbind` (NIS), que es un servicio RPC manejado en conjunto con el servicio `portmap`.

El comando `lsof` revela información similar a la dada por `netstat` puesto que es capaz de enlazar puertos abiertos a servicios:

```
lsof -i | grep 834
```

A continuación se encuentra la porción relevante de la salida de este comando:

```
ypbind      653        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      655        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      656        0    7u  IPv4       1319                TCP *:834 (LISTEN)
ypbind      657        0    7u  IPv4       1319                TCP *:834 (LISTEN)
```

Estas herramientas pueden revelar bastante información sobre el estado de los servicios ejecutándose en la máquina. Estas herramientas son flexibles y pueden proporcionar gran cantidad de información sobre los servicios de red y la configuración. Se recomienda la revisión de las páginas man para `lsof`, `netstat`, `nmap`, y `services`.

3. Single Sign-on (SSO)

3.1. Introducción

La funcionalidad SSO de Red Hat Enterprise Linux reduce el número de veces que los usuarios de escritorios Red Hat Enterprise Linux deben introducir sus contraseñas. Varias aplicaciones utilizan los mismos mecanismos de autenticación y autorización para que los usuarios puedan registrarse en Red Hat Enterprise Linux desde una pantalla de registro y luego no tengan que introducir la contraseña de nuevo. Estas aplicaciones se detallan a continuación.

Además, los usuarios pueden registrarse a sus máquinas incluso si no existe una red (*modo fuera de línea*) o donde la conexión a la red no es confiable, como es el caso del acceso inalámbrico. En este último caso, los servicios son degradados progresivamente.

3.1.1. Aplicaciones soportadas

Las siguientes aplicaciones están actualmente soportadas por el esquema de registro unificado en Red Hat Enterprise Linux:

- Registro
- Salvapantalla
- Firefox y Thunderbird

3.1.2. Mecanismos de autenticación soportados

Red Hat Enterprise Linux actualmente soporta los siguientes mecanismos de autenticación:

- Registro nombre/contraseña de Kerberos
- Tarjetas inteligentes/PIN

3.1.3. Tarjetas inteligentes soportadas

Red Hat Enterprise Linux has sido verificado con tarjetas y lectores Cyberflex e-gate pero cualquier tarjata que acate las especificaciones Java card 2.1.1 y Global Platform 2.0.1 debe operar correctamente. Así mismo, cualquier lector que es soportado por PCSC-lite debe funcionar.

Red Hat Enterprise Linux también ha sido probado con tarjetas de acceso común (CAC por sus siglas en inglés). El lector soportado para CAC es SCM SCR 331 USB Reader.

3.1.4. Ventajas de SSO en Red Hat Enterprise Linux

Actualmente existen varios mecanismos de seguridad que utilizan un gran número de protocolos y credenciales. Entre éstos se encuentran SSL, SSH, IPsec y Kerberos. SSO de Red Hat Enterprise Linux pretende unificar estos esquemas para soportar los requerimientos listados anteriormente. Esto no significa reemplazar Kerberos con certificados X.509v3, pero unificarlos para reducir la carga tanto en los usuarios de los sistemas como de los administradores que los administran.

Para alcanzar este objetivo, Red Hat Enterprise Linux:

- Proporciona una biblioteca compartida NSS crypto única en cada sistema operativo.
- Entrega el sistema de certificados cliente de seguridad empresarial ESC (por sus siglas en inglés Enterprise Security Client) con el sistema operativo base. La aplicación ESC verifica los eventos de inserción de tarjetas inteligentes.Si se detecta que el usuario ha insertado una tarjeta inteligente que fue diseñada para ser usada en el producto servidor de sistema de certificado de Red Hat Enterprise Linux, se mostrará una interfaz de usuario con instrucciones sobre cómo inscribir esa tarjeta inteligente.
- Unifica Kerberos y NSS para que los usuarios que se registran en el sistema operativo utilizando una tarjeta inteligente también puedan obtener las credenciales de Kerberos (lo cual les permitirá registrarse en servidores de archivos y otros).

3.2. Iniciando con su nueva tarjeta inteligente

Antes de que pueda utilizar la tarjeta inteligente para registrarse a su sistema y aprovechar las ventajas de seguridad que esta tecnología proporciona, usted tendrá que ejecutar algunas tareas básicas de instalación y configuración. Estas tareas se describen a continuación:

Nota

Esta sección proporciona una visión general de la utilización de tarjetas inteligentes. Información más detallada puede encontrarse en el Manual de Clientes de Seguridad Empresarial del Sistema de Certificados de Red Hat.

1. Registrese con su nombre y contraseña de Kerberos
2. Asegúrese de que el paquete `nss-tools` esté cargado.
3. Descargue e instale su certificado root específico para la corporación. Utilice el siguiente comando para instalar el certificado CA root:

   ```
   certutil -A -d /etc/pki/nssdb -n "root ca cert" -t "CT,C,C" -i ./ca_cert_in_base64_format.crt
   ```

4. Verifique que tiene los siguientes RPM instalados en su sistema: esc, pam_pkcs11, coolkey, ifd-egate, ccid, gdm, authconfig y authconfig-gtk.
5. Activar el soporte de registro de la tarjeta inteligente

a. En la barra de menú de Gnome, seleccione Sistema->Administración->Autenticación.

b. Escriba la contraseña de root de su máquina si ésta es necesaria.

c. En el diálogo de configuración de la autenticación, haga clic en la pestaña **Autenticación**.

d. Seleccione la casilla de verificación **Activar soporte de tarjetas inteligentes**.

e. Haga clic en el botón **Configurar tarjeta inteligente...** para ver el diálogo de parámetros de la tarjeta inteligente y especifique los parámetros requeridos:

- **Requiere tarjeta inteligente para entrar** — Desactive esta casilla de verificación. Una vez usted ha iniciado una sesión de forma satisfactoria con la tarjeta inteligente, usted puede seleccionar esta opción para prevenir que los usuarios se registren sin tarjetas inteligentes.
- **Acción de remoción de tarjeta** — Esto controla la acción a tomar una vez usted remueva la tarjeta inteligente después de haber iniciado la sesión. Las opciones disponibles son:
  - **Lock** — Al remover la tarjeta se bloqueará la pantalla X.
  - **Ignore** — La remoción de la tarjeta no tiene ningún efecto.

6. Si necesita activar el Online Certificate Status Protocol (OCSP), abra el archivo `/etc/pam_pkcs11/pam_pkcs11.conf` y ubique la línea siguiente:

```
enable_ocsp = false;
```

Cambie este valor a "true", como se señala a continuación:

```
enable_ocsp = true;
```

7. Inscriba su tarjeta inteligente

8. Si está utilizando una tarjeta CAC, deberá también ejecutar los siguientes pasos:

a. Desde una cuenta de root cree un archivo llamado `/etc/pam_pkcs11/cn_map`.

b. Añada la siguiente entrada al archivo `cn_map`:

```
<MY.CAC_CN.123454> -> <mi-login-id>
```

Donde *<MY.CAC_CN.123454>* es el nombre común en su CAC y *<mi-login-id>* es su login ID de UNIX.

9. Logout

3.2.1. Solución de problemas

Si tiene problemas al tratar de hacer funcionar su tarjeta inteligente, intente el siguiente comando para ubicar la fuente del problema:

```
pklogin_finder debug
```

Si ejecuta la herramienta `pklogin_finder` en modo de depuración mientras un tarjeta inteligente inscrita está conectada, se intentará obtener la información sobre la validez de los certificados y verificará si se puede relacionar el login ID con uno de los certificados presentes en la tarjeta.

3.3. Cómo funciona la inscripción de las tarjetas inteligentes

Las tarjetas inteligentes están *inscritas* cuando han recibido un certificado firmado por una autoridad certificadora (CA por sus siglas en inglés,Certificate Authority). Este proceso incluye los pasos que se describen a continuación:

1. El usuario introduce la tarjeta inteligente en el lector de tarjatas de la estación de trabajo. Este evento es reconocido por el cliente de seguridad empresarial (ESC).
2. Se muestra la página de inscripción en el escritorio del usuario. El usuario completa la infromación requerida y el sistema del usuario se conecta al sistema de procesamiento de Token (TPS por sus siglas en inglés, Token Processing System) y al CA.
3. El TPS inscribe la tarjeta inteligente utilizando el certificado firmado por el CA.

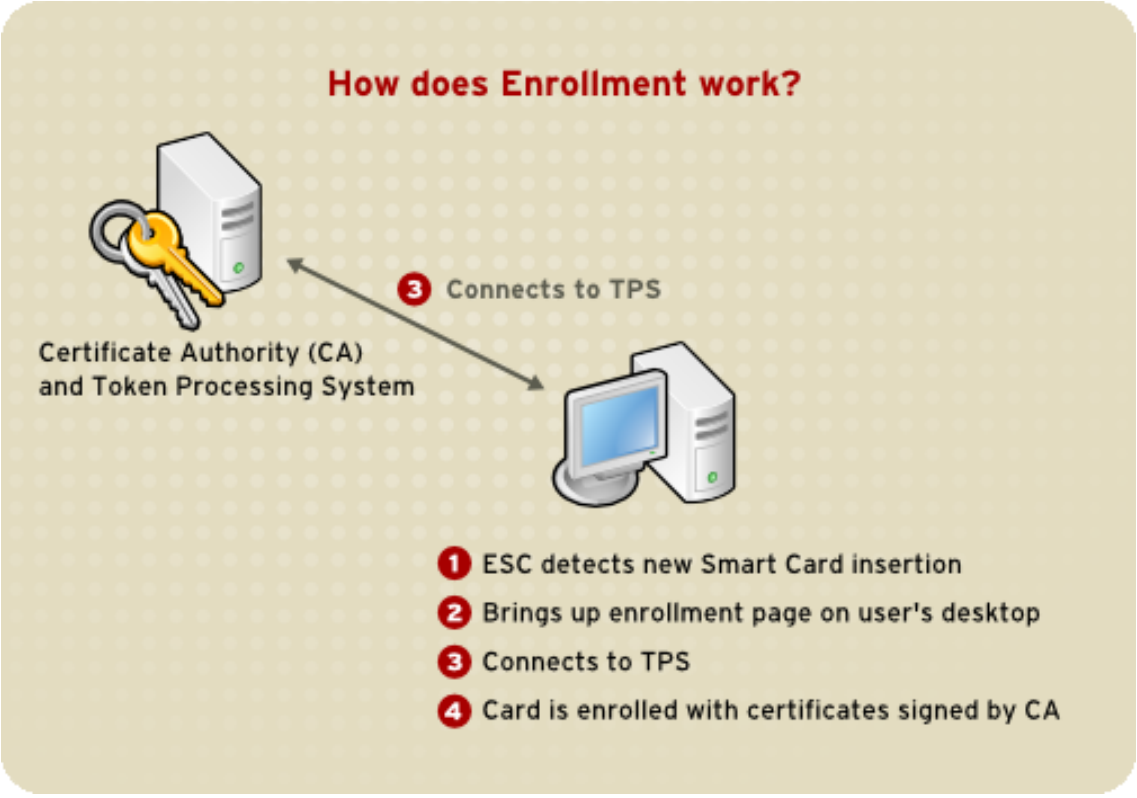


Figura 21.4. Cómo funciona la inscripción de las tarjetas inteligentes

3.4. Cómo funciona el registro de las tarjetas inteligentes

Esta sección describe brevemente el proceso de registro utilizando una tarjeta inteligente.

1. Cuando el usuario inserta la tarjeta inteligente en el lector, la facilidad PAM reconoce el evento y solicita el PIN del usuario.
2. El sistema luego busca el certificado actual del usuario y verifica su validez. El certificado es luego relacionado con el UID del usuario.
3. Éste es validado con el KDC y el login es concedido.

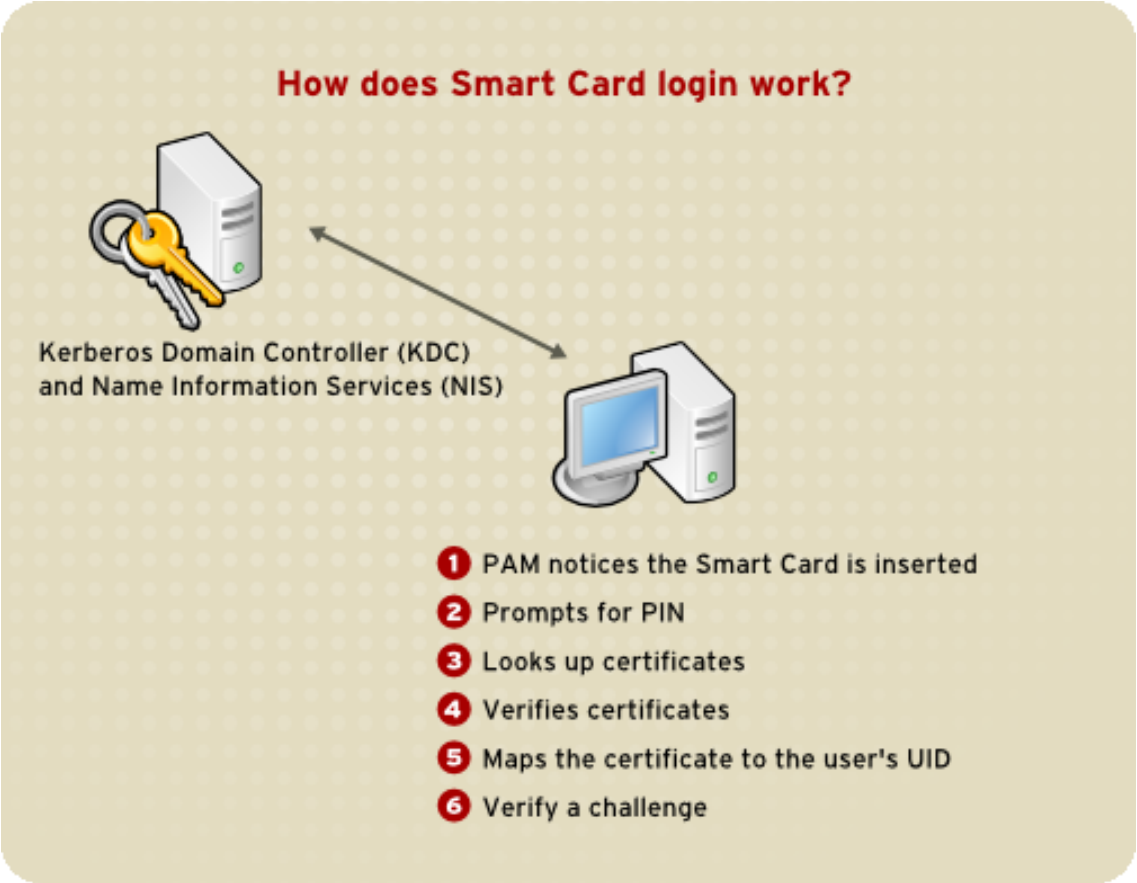


Figura 21.5. Cómo funciona el registro de las tarjetas inteligentes

Nota

Usted no puede registrarse con una tarjeta que no ha sido inscrita, incluso si ésta tiene el formato correcto. Deberá registrarse con una tarjeta formateada e inscrita -o con otro método diferente, antes de inscribir una nueva tarjeta.

3.5. Configuración de Firefox para utilizar Kerberos con

SSO

Usted puede configurar Firefox para utilizar Kerberos con SSO. Para que esta funcionalidad funcione apropiadamente, tendrá que configurar su navegador para que envíe credenciales Kerberos al KDC apropiado.

1. En la barra de direcciones de Firefox, escriba **`about:config`** para ver la lista de opciones de configuración actuales.
2. En el campo **Filter** escriba **`negotiate`** para restringir la lista de opciones.
3. Haga doble clic en la entrada *network.negotiate-auth.trusted-uris* para ver la ventana de diálogo *Enter string value*.
4. Introduzca el nombre del dominio desde el cual desea llevar a cabo la autenticación (p. ej. *`.ejemplo.com`*).
5. Repita el procedimiento anterior para la entrada *network.negotiate-auth.delegation-uris* y utilice el mismo dominio.

Nota

Puede dejar este valor en blanco ya que el pase de tiquetes de Kerberos no es requerido.

Si no encuentra estas dos opciones listadas, su versión de Firefox es demasiado vieja y podría no soportar la negociación de la autenticación. En dicho caso, usted debería considerar actualizar Firefox.

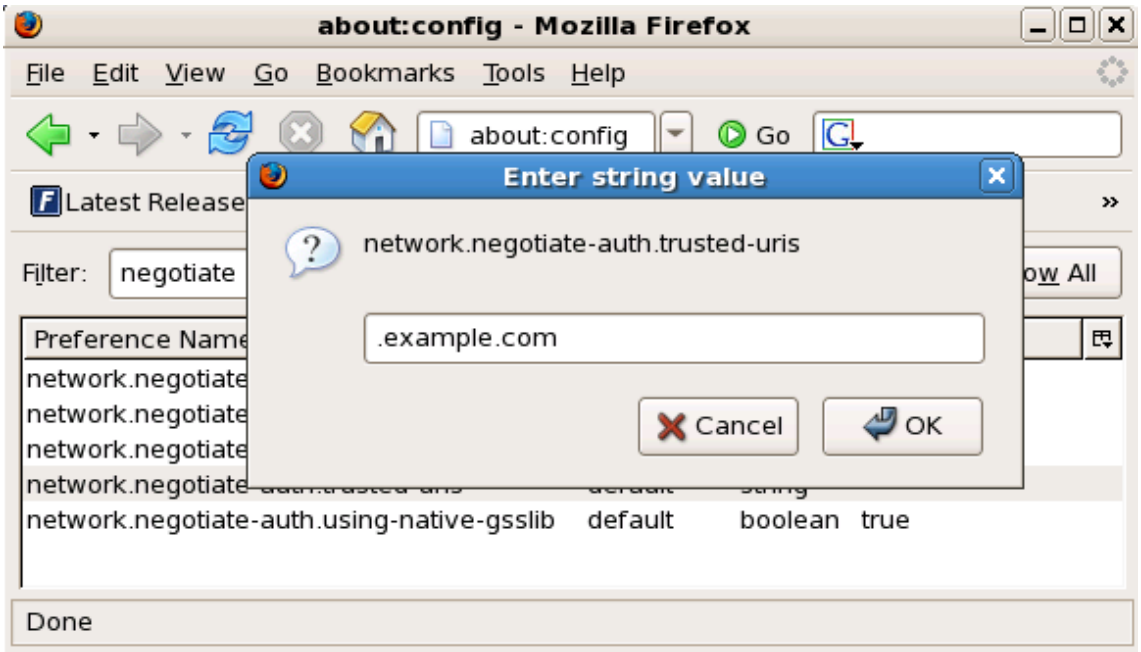


Figura 21.6. Configuración de Firefox para SSO con Kerberos

Ahora debe asegurarse de tener tickets de kerberos. En un intérprete de comandos de shell escriba `kinit` para obtener tickets de Kerberos. Para ver la lista de tickets disponibles escriba `klist`. A continuación se presenta un ejemplo de la respuesta de dicho comando:

```
[user@host ~] $ kinit
Password for user@EXAMPLE.COM:

[user@host ~] $ klist
Ticket cache: FILE:/tmp/krb5cc_10920
Default principal: user@EXAMPLE.COM

Valid starting     Expires            Service principal
10/26/06 23:47:54  10/27/06 09:47:54  krbtgt/USER.COM@USER.COM
        renew until 10/26/06 23:47:54

Kerberos 4 ticket cache: /tmp/tkt10920
klist: You have no tickets cached
```

3.5.1. Solución de problemas

Si ha seguido los pasos de configuración anteriores y la negociación de la autenticación no está funcionando, puede activar la salida verbosa del registro del proceso de autenticación. Esto puede ayudarlo a encontrar la causa del problema. Para activar la salida verbosa del registro, utilice el siguiente procedimiento:

1. Cierre todas las ventanas de Firefox.

2. Abra una consola e introduzca el siguiente comando:

   ```
   export NSPR_LOG_MODULES=negotiateauth:5
   export NSPR_LOG_FILE=/tmp/moz.log
   ```

3. Reinicie Firefox *desde esa consola* y visite el sitio web al cual no pudo autenticarse anteriormente. La información será registrada en `/tmp/moz.log`. Ésta le dará pistas sobre el problema. Por ejemplo:

   ```
   -1208550944[90039d0]: entering nsNegotiateAuth::GetNextToken()
   -1208550944[90039d0]: gss_init_sec_context() failed: Miscellaneous failure
   No credentials cache found
   ```

   Esto indica que usted no tiene tickets de Kerberos y necesita ejecutar `kinit`.

Si puede ejecutar `kinit` satisfactoriamente desde su máquina pero no puede autenticarse, verá un mensaje similar al siguiente en el archivo de registro:

```
-1208994096[8d683d8]: entering nsAuthGSSAPI::GetNextToken()
-1208994096[8d683d8]: gss_init_sec_context() failed: Miscellaneous failure
Server not found in Kerberos database
```

Esto generalmente indica que hay un problema en la configuración de Kerberos. Asegúrese de tener las entradas correctas en la sección [domain_realm] del archivo `/etc/krb5.conf`. Por ejemplo:

```
.ejemplo.com = EJEMPLO.COM
ejemplo.com = EJEMPLO.COM
```

Si nada aparece el el archivo de registro es posible que usted esté conectándose a un proxy y que éste está cortando las cabeceras HTTP requeridas para la negociación de la autenticación. Para solucionar este problema, usted puede conectarse al servidor utilizando HTTPS; esto permitirá que la solicitud pase sin ser modificada. Luego continúe con la depuración utilizando el archivo de registro como se describió anteriormente.

4. Pluggable Authentication Modules (PAM)

Los programas que conceden accesos a usuarios en un sistema utilizan *autenticación* para verificar sus identidades (para establecer que un usuario es quien dice ser).

Históricamente, cada programa tiene su forma particular de realizar la autenticación. Bajo Red Hat Enterprise Linux, muchos programas son configurados para usar un proceso de autenticación centralizado llamado PAM (*Pluggable Authentication Modules*).

PAM utiliza una arquitectura conectable y modular, que otorga al administrador del sistema de una gran flexibilidad en establecer las políticas de autenticación para el sistema.

En la mayoría de los casos, el archivo de configuración PAM predeterminado para una aplicación que soporta PAM es suficiente. Sin embargo, algunas veces es necesario modificar el archivo de configuración. Debido a que un error en la configuración de PAM puede comprometer la seguridad del sistema, es importante que comprenda la estructura del estos archivos antes de hacer cualquier modificación. Consulte Sección 4.3, “Formato del archivo de configuración PAM” para obtener mayor información.

4.1. Las ventajas de PAM

PAM ofrece las ventajas siguientes:

- un esquema de autenticación común que se puede usar con una gran variedad de aplicaciones.
- gran flexibilidad y control de la autentificación tanto para los administradores de sistemas como para los desarrolladores de la aplicación.
- una biblioteca bien documentada que permite a los desarrolladores de aplicaciones desarrollar programas sin tener que crear sus propios esquemas de autenticación.

4.2. archivos de configuración PAM

El directorio `/etc/pam.d/` contiene los archivos de configuración de PAM para cada aplicación tipo PAM. En versiones antiguas de PAM se utilizaba `/etc/pam.conf`, pero este archivo ya no se utiliza y solamente es usado si el directorio `/etc/pam.d/` no existe.

4.2.1. Archivos de servicios PAM

Cada aplicación tipo PAM o *servicios* tiene un archivo dentro del directorio `/etc/pam.d/`. Cada uno de estos archivos llevan el nombre del servicio para el cual controla el acceso.

Depende del programa tipo PAM definir el nombre de su servicio e instalar su archivo de configuración en el directorio `/etc/pam.d/`. Por ejemplo, el programa `login` define su nombre de servicio como login e instala el archivo de configuración PAM `/etc/pam.d/login`.

4.3. Formato del archivo de configuración PAM

Cada archivo de configuración PAM contiene un grupo de directivas formateadas como sigue:

```
<module interface><control flag><module name><module arguments>
```

En las siguientes secciones se explican cada uno de estos elementos.

4.3.1. Interfaz de módulo

Hay cuatro tipos de módulos PAM disponibles. Cada uno corresponde con un aspecto diferente del proceso de autorización:

- `auth` — Esta interfaz de módulo autentifican el uso. Por ejemplo, solicita y verifica la validez de una contraseña. Los módulos con esta interfaz también pueden establecer credenciales, tales como membrecías de grupo o tickets Kerberos.
- `account` — Esta interfaz de módulo verifica que sea permitido el acceso. Por ejemplo, puede verificar que la cuenta no haya caducado o que el usuario tenga permiso de iniciar sesiones a una hora del día particular.
- `password` — Este módulo se usa para establecer y verificar contraseñas.
- `session` — Esta interfaz de módulo configura y administra las sesiones de usuarios. Los módulos con esta interfaz también pueden realizar tareas adicionales que son requeridas para permitir acceso, como el montaje de directorios principales de usuarios y hacer el buzón de correo del usuario disponible.

Nota

Un módulo individual puede proporcionar una o todas las interfaces de módulos mencionadas anteriormente. Por ejemplo, `pam_unix.so` proporciona todas las cuatro interfaces.

En un archivo de configuración PAM, la interfaz del módulo es el primer campo a definir. Por ejemplo, una línea típica de una configuración sería:

```
auth        required        pam_unix.so
```

Esto provoca que PAM utilice la interfaz `pam_unix.so` del módulo `auth`.

4.3.1.1. Apilar interfaces de módulos

Las directivas de interfaces de módulos pueden ser *apiladas* o colocadas una sobre otra para que se puedan usar múltiples módulos para un mismo propósito. Si la opción de control de un

módulo utiliza los valores "sufficient" o "requisite" (consulte la Sección 4.3.2, “Indicadores de control” para obtener información acerca de estos valores) el orden de una pila de módulos es importante en el procedimiento de autenticación.

El hecho de apilarlos hace que sea más fácil para que el administrador exija diversas condiciones antes de permitir la autenticación del usuario. Por ejemplo, el comando `reboot` utiliza generalmente una pila de módulos, como se ve en su archivo de configuración:

```
[root@MyServer ~]# cat /etc/pam.d/reboot
#%PAM-1.0
auth        sufficient        pam_rootok.so
auth        required        pam_console.so
#auth        include        system-auth
account        required        pam_permit.so
```

- La primera línea es un comentario y no es procesada.
- `auth sufficient pam_rootok.so` — Esta línea utiliza el módulo `pam_rootok.so` para revisar si el usuario actual es root, verificando que su UID sea igual a 0. Si esta prueba tiene éxito, ningún otro módulo es consultado y el comando es ejecutado. De lo contrario se consultará el siguiente módulo.
- `auth required pam_console.so` — Esta línea utiliza el módulo `pam_console.so` para intentar autenticar al usuario. Si este usuario ya tiene una sesión en la consola, `pam_console.so` revisa si hay un archivo en el directorio `/etc/security/console.apps/` con el mismo nombre que el servicio (reboot). Si dicho archivo existe, la autenticación pasa y el control es pasado al siguiente módulo.
- `#auth include system-auth` — Esta línea es un comentario y no será procesada.
- `account required pam_permit.so` — Esta línea utiliza el módulo `pam_permit.so` para permitir que el usuario root o cualquiera con una sesión en la consola puede reiniciar el sistema.

4.3.2. Indicadores de control

Todos los módulos PAM generan un resultado de éxito o fracaso cuando se les llama. Los indicadores de control le dicen a PAM qué hacer con el resultado. Como los módulos pueden apilarse en un determinado orden, los indicadores de control le dan la posibilidad de fijar la importancia de un módulo con respecto al objetivo final del proceso de autenticación para el servicio.

Hay cuatro indicadores de control definidos:

- `required` — El resultado del módulo debe ser exitoso para que la autenticación continue. Si la prueba falla, el usuario no es notificado hasta que los resultados en todos los módulos referenciando esa interfaz sean completados.
- `requisite` — El resultado del módulo debe ser exitoso para que la autenticación continúe. Sin embargo, si la prueba falla, el usuario es notificado inmediatamente con un mensaje reflejando el primer módulo `required`*o*`requisite` fallido.
- `sufficient` — El resultado del módulo es ignorado si falla. Pero si el resultado del módulo con el indicador `sufficient` es exitoso *y* ningún módulo con indicador `required` ha fallado, entonces no se requiere ningún otro resultado y el usuario es autenticado para el servicio.

- `optional` — Se ignora el resultado del módulo.Un módulo con una bandera `optional` sólo es necesario para la autenticación exitosa cuando no hay otros módulos haciendo referencia a la interfaz.

Importante

El orden en el cual se llaman los módulos `required` no es crítico. Las banderas o indicadores de control `sufficient` y `requisite` provocan que el orden se vuelva importante.

Ahora PAM dispone de una nueva sintaxis de control de banderas que permite un control más preciso.

La página man de `pam.d` y la documentación de PAM, ubicadas en directorio `/usr/share/doc/pam-<version-number>/` (donde `<version-number>` es el número de versión para PAM) describe esta nueva sintaxis detalladamente.

4.3.3. Nombre del módulo

El nombre del módulo le proporciona a PAM el nombre del módulo que contiene la interfaz del módulo especificada. Bajo las versiones anteriores de Red Hat Enterprise Linux, se proporcionaba la ruta completa al módulo dentro del archivo de configuración PAM. Sin embargo, desde el advenimiento de sistemas *multilib*, que almacenan módulos PAM de 64-bits dentro del directorio `/lib64/security/`, el nombre del directorio es omitido debido a que las aplicaciones son enlazadas a la versión apropiada de `libpam`, el cual puede ubicar la versión correcta del módulo.

4.3.4. Argumentos de módulo

PAM utiliza *argumentos* para transmitir información a un módulo conectable durante la autenticación para algunos módulos.

Por ejemplo, el módulo `pam_userdb.so` usa información almacenados en un archivo Berkeley DB para autenticar a los usuarios. La base de datos Berkeley DB es una base de datos de código abierto incorporada en muchas aplicaciones. El módulo toma un argumento `db` para que la base de datos Berkeley DB conozca qué base de datos usar para el servicio solicitado.

La línea `pam_timestamp` siguiente es común en la configuración PAM. El `<path-to-file>` es la ruta completa al archivo de base de datos Berkeley DB:

```
auth        required        pam_userdb.so db=<path-to-file>
```

Los argumentos inválidos *generalmente* son ignorados y no afectan en ningún modo el éxito o fracaso del módulo PAM. Sin embargo, algunos módulos reportarán un error al archivo `/var/log/secure`.

4.4. Muestras de archivos de configuración PAM

A continuación se presenta una muestra de archivo de configuración de la aplicación PAM:

```
#%PAM-1.0
auth        required  pam_securetty.so
auth        required  pam_unix.so nullok
auth        required  pam_nologin.so
account        required  pam_unix.so
password        required  pam_cracklib.so retry=3
password        required  pam_unix.so shadow nullok use_authtok
session        required  pam_unix.so
```

- La primera línea es un comentario como lo es toda línea que inicie con el carácter `#`.
- Las líneas dos, tres y cuatro apilan tres módulos a usar para autentificaciones de inicio de sesión.

  `auth required pam_securetty.so` — Este módulo se asegura de que *si* el usuario está tratando de conectarse como root, el tty en el cual el usuario se está conectando está listado en el archivo `/etc/securetty`, *si* ese archivo existe.

  Si el tty no se lista en el archivo, cualquier intento de iniciar una sesión como root fallará con el mensaje `Login incorrect`.

  `auth required pam_unix.so nullok` — Este módulo le solicita al usuario una contraseña y luego verifica la contraseña usando la información almacenada en `/etc/passwd` y, si existe, en `/etc/shadow`.

  - El argumento `nullok` instruye al módulo `pam_unix.so` a que permita una contraseña en blanco.

- `auth required pam_nologin.so` — Este es el paso final de la autenticación. Verifica si el archivo `/etc/nologin` existe. Si existe y el usuario no es root, la autenticación falla.

Nota

En este ejemplo, los tres módulos `auth` son revisados, aún si el primer módulo `auth` falla. Esto previene que el usuario sepa en qué nivel la autenticación falla. Tal conocimiento en las manos de una persona mal intencionada le permitiría violar el sistema fácilmente.

- `account required pam_unix.so` — Este módulo realiza cualquier verificación de cuenta necesaria. Por ejemplo, si las contraseñas shadow han sido activadas, el componente de la cuenta del módulo `pam_unix.so` verificará para ver si la cuenta ha expirado o si el usuario no ha cambiado la contraseña dentro del período de gracia otorgado.
- `password required pam_cracklib.so retry=3` — Si la contraseña ha expirado, el componente de la contraseña del módulo `pam_cracklib.so` le pide una nueva contraseña. Luego evalúa la nueva contraseña para ver si puede ser fácilmente determinada por un programa que descubre las contraseñas basadas en diccionarios.

  - El argumento `retry=3` especifica que si la prueba falla la primera vez, el usuario tiene

dos opciones más para crear una contraseña mejor.

- `password required pam_unix.so shadow nullok use_authtok` — Esta línea especifica que si el programa cambia la contraseña del usuario, debe utilizar la interfaz `password` del módulo `pam_unix.so` para hacerlo.

  - El argumento `shadow` le dice al módulo que cree contraseñas shadow cuando se actualiza la contraseña del usuario.

  - El argumento `nullok` indica al módulo que permita al usuario cambiar su contraseña *desde* una contraseña en blanco, de lo contrario una contraseña vacía o en blanco es tratada como un bloqueo de cuenta.

  - El argumento final de esta línea, `use_authtok`, proporciona un buen ejemplo de la importancia del orden al apilar módulos PAM. Este argumento advierte al módulo a no solicitar al usuario una nueva contraseña. En su lugar se acepta cualquier contraseña que fue registrada por un módulo de contraseña anterior. De este modo, todas las nuevas contraseñas deben pasar el test de `pam_cracklib.so` para contraseñas seguras antes de ser aceptado.

- `session required pam_unix.so` — La última línea especifica que el componente de la sesión del módulo `pam_unix.so` gestionará la sesión. Este módulo registra el nombre de usuario y el tipo de servicio a `/var/log/secure` al inicio y al final de cada sesión. Puede ser complementado apilándolo con otros módulos de sesión si necesita más funcionalidad.

4.5. Creación de módulos PAM

Puede crear o añadir nuevos módulos PAM en cualquier momento para utilizar con aplicaciones que soporten PAM.

Por ejemplo, un desarrollador puede crear un método de creación de contraseña de una sola vez y escribir un módulo PAM que lo soporte. Los programas que soporten PAM pueden inmediatamente usar el nuevo módulo y el método de contraseña sin tener que compilar de nuevo o realizar alguna otra modificación.

Esto le permite a los desarrolladores y administradores de sistemas mezclar y coincidir, así como también evaluar, métodos de autenticación para programas diferentes sin tener que compilarlos nuevamente.

La documentación acerca de cómo escribir módulos se incluye en el directorio `/usr/share/doc/pam-<version-number>/`, en donde `<version-number>` es el número de versión de PAM.

4.6. PAM y el caché de credenciales administrativas

Varias herramientas gráficas administrativas bajo Red Hat Enterprise Linux otorgan a los usuarios privilegios especiales por un tiempo máximo de 5 minutos a través del módulo `pam_timestamp.so`. Es importante entender cómo funciona este mecanismo puesto que un usuario que deja su terminal mientras `pam_timestamp.so` está en efecto, deja la máquina abierta a la manipulación por cualquiera con acceso físico a la consola.

Bajo el esquema de marcas de tiempo de PAM, la aplicación administrativa gráfica pide al usuario la contraseña de root cuando se ejecuta. Una vez autenticado, el módulo `pam_timestamp.so` crea un archivo de marca de tiempo (timestamp) dentro del directorio `/var/run/sudo/` por defecto. Si el archivo timestamp ya existe, otros programas gráficos administrativos no le pedirán la contraseña. En vez de esto, el módulo `pam_timestamp.so` refrescará el archivo timestamp, reservando unos cinco minutos extra de acceso administrativo para el usuario.

Puede verificar el estado actual del archivo timestamp inspeccionando el archivo `/var/run/sudo/<user>`. Para el escritorio, el archivo relevante es `unknown:root`. Si está presenta y la marca de tiempo es menos de cinco minutos, las credenciales son válidas.

La existencia de archivos timestamp se indica con un icono de autenticación que aparece en el área de notificación del panel.

Figura 21.7. El icono de autenticación

4.6.1. Eliminar el archivo timestamp

Es recomendable que antes de dejar desatendida una consola donde está activo un timestamp PAM, se destruya el archivo timestamp. Para hacerlo desde un ambiente gráfico, pulse en el icono de autenticación en el panel. Cuando aparezca una ventana de diálogo, pulse en el botón **Olvidar autorización**

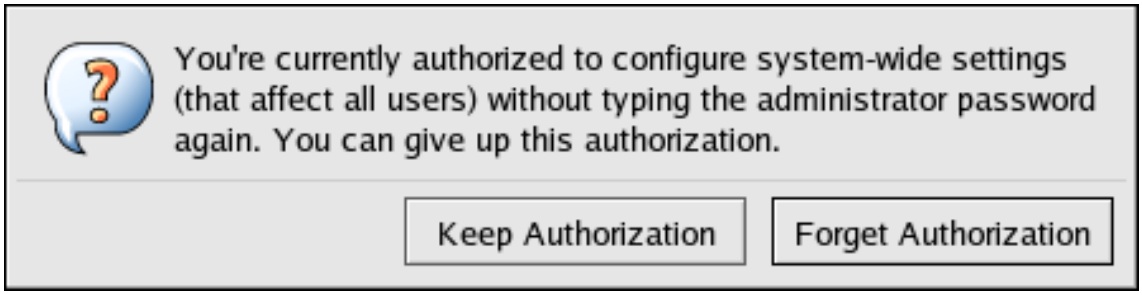


Figura 21.8. Diálogo de rechazo de la autenticación

Debe tener en cuenta los siguientes siguientes aspectos acerca del archivo timestamp de PAM:

- Si está conectándose a un sistema remotamente usando `ssh`, utilice el comando `/sbin/pam_timestamp_check -k root` para destruir el archivo timestamp.
- Debe ejecutar el comando `/sbin/pam_timestamp_check -k root` desde la misma ventana de terminal desde la cual usted ejecutó la acción privilegiada.
- Debe estar conectado como el usuario que invocó originalmente el módulo `pam_timestamp.so` para poder utilizar el comando `/sbin/pam_timestamp_check -k`. No se conecte como usuario root para ejecutar este comando.

- Si desea eliminar las credenciales en el escritorio (sin utilizar **Olvidar autorización** en el icono), utilice el siguiente comando:

  ```
  /sbin/pam_timestamp_check -k root </dev/null >/dev/null 2>/dev/null
  ```

  Si el uso de este comando falla, sólo se removerá la credencial (si ésta existe) del pty donde se ejecuta el comando.

Para información sobre cómo destruir el archivo timestamp usando `pam_timestamp_check`, refiérase a la página man de `pam_timestamp_check`.

4.6.2. Directivas pam_timestamp comunes

El módulo `pam_timestamp.so` acepta muchas directivas. Abajo están las opciones más comúnmente usadas:

- `timestamp_timeout` — Especifica el número de segundos durante los cuales el archivo timestamp es válido. El valor por defecto es 300 segundos (cinco minutos).
- `timestampdir` — Especifica el directorio en el cual se almacena el archivo de estampilla de tiempo. El valor por defecto es `/var/run/sudo`.

Para más información sobre el control del módulo `pam_timestamp.so`, refiérase a la Sección 4.8.1, “Documentación instalada”.

4.7. PAM y propiedad del dispositivo

Red Hat Enterprise Linux permite que el primer usuario que se conecte en una consola física de la máquina pueda manipular algunos dispositivos y realizar algunas tareas normalmente reservadas para el usuario root. Esto es controlado por un módulo PAM llamado `pam_console.so`.

4.7.1. Propiedad del dispositivo

Cuando un usuario inicia una sesión en un sistema Red Hat Enterprise Linux, el módulo `pam_console.so` es llamado por `login` o los programas de inicio de sesión gráfica, **gdm**, **kdm** y **xdm**. Si este usuario es el primero en conectarse en la consola física — llamado *usuario de consola* — el módulo le concede al usuario la propiedad de algunos dispositivos que normalmente pertenecen a root. El usuario de la consola posee estos dispositivos hasta que la última sesión local para ese usuario finalice. Una vez que el usuario se ha desconectado, la propiedad de los dispositivos vuelve a root.

Los dispositivos afectados incluyen, pero no son limitados, las tarjetas de sonido, las unidades de disco y las unidades de CD-ROM.

Esto permite que el usuario local manipule estos dispositivos sin llegar a tener acceso root simplificando así las tareas comunes para el usuario de la consola.

Puede modificar la lista de dispositivos controlados por `pam_console.so` si se editan las siguientes lineas:

- `/etc/security/console.perms`

- `/etc/security/console.perms.d/50-default.perms`

Usted puede cambiar los permisos de diferentes dispositivos que aquellos listados en los archivos anteriores o sobreescribir las especificaciones predeterminadas. En vez de modificar el archivo `50-default.perms`, usted debe crear un nuevo archivo (por ejemplo, *xx*`-name.perms`) e introducir la modificación requerida. El número del nuevo archivo predeterminado debe iniciar con un número superior a 50 (por ejemplo `51-default.perms`). Esto sobreescribirá los valores predeterminados en el archivo `50-default.perms`

Atención

Si el archivo de configuración del gestor de ventanas **gdm**, **kdm** o **xdm** ha sido alterado para permitir a los usuarios remotos conectarse *y* la máquina está configurada para ejecutarse en el nivel de ejecución 5, se recomienda cambiar las directivas `<console>` y `<xconsole>` dentro de `/etc/security/console.perms` a los valores siguientes:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :0\.[0-9] :0
<xconsole>=:0\.[0-9] :0
```

Ésto previene que los usuarios remotos obtengan acceso a los dispositivos y a las aplicaciones restringidas en la máquina.

Si el archivo de configuración del gestor de ventanas **gdm**, **kdm** o **xdm** ha sido alterado para permitir a los usuarios remotos conectarse *y* la máquina está configurada para ejecutarse en un nivel diferente al 5, se recomienda cambiar las directivas `<xconsole>` y `<console>` a los valores siguientes:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

4.7.2. Acceso de la aplicación

También se le permite al usuario de la consola el acceso a ciertos programas configurados para este fin en `/etc/security/console.apps/`.

Este directorio contiene archivos de configuración que permiten que el usuario de la consola ejecute ciertas aplicaciones en `/sbin` y `/usr/sbin`.

Estos archivos de configuración tienen el mismo nombre que las aplicaciones que configuran.

Un grupo notable de aplicaciones a las que tiene acceso el usuario de la consola son tres programas que cierran o abren el sistema:

- `/sbin/halt`
- `/sbin/reboot`
- `/sbin/poweroff`

Debido a que estas aplicaciones soportan PAM, ellas llaman al módulo `pam_console.so` como un requerimiento para el uso.

Para mayor información, consulte la Sección 4.8.1, “Documentación instalada”.

4.8. Recursos adicionales

Los siguientes recursos explican los métodos para el uso y configuración de PAM. Además de estos recursos, lea los archivos de configuración de PAM en el sistema para entender mejor como están estructurados.

4.8.1. Documentación instalada

- Las páginas man relacionadas con PAM — Hay un número de páginas man para las diferentes aplicaciones y archivos de configuración relacionados con PAM. :La lista siguiente muestra algunas de las páginas man más importantes.

  Archivos de configuración

  - `pam` — Información de introducción sobre PAM. Incluye la estructura y propósitos de los archivos de configuración de PAM.

    Tenga en cuenta que esta página man discute tanto `/etc/pam.conf` como los archivos de configuración individuales en el directorio `/etc/pam.d/`. Por defecto, Red Hat Enterprise Linux utiliza los archivos de configuración individuales en el directorio `/etc/pam.d/`, ignorando `/etc/pam.conf` incluso si éste existe

  - `pam_console` — Describe el propósito del módulo `pam_console.so`. También describe la sintaxis adecuada para una entrada en el archivo de configuración PAM.

  - `console.apps` — Describe el formato y las opciones disponibles dentro de `/etc/security/console.apps`, el archivo de configuración que define cuáles aplicaciones permiten acceso al usuario de la consola asignado por PAM.

  - `console.perms` — Describe el formato y las opciones disponibles dentro de `/etc/security/console.perms`, el archivo de configuración para los permisos del usuario de la consola asignado por PAM.

  - `pam_timestamp` — Describe el módulo `pam_timestamp.so`.

- `/usr/share/doc/pam-<version-number>`— Contiene un *Manual para administradores de sistemas*, un *Manual para escritores de módulos* y el *Manual para los desarrolladores de aplicaciones*, así como también una copia del estándar PAM, DCE-RFC 86.0 (reemplace `<version-number>` con el número de la versión de PAM).

- `/usr/share/doc/pam-<version-number>/txts/README.pam_timestamp` — Contiene información sobre el módulo PAM `pam_timestamp.so`, en donde `<version-number>` es el número de versión de PAM.

4.8.2. Sitios web útiles

- http://www.kernel.org/pub/linux/libs/pam/ — El sitio web de distribución primario para el proyecto Linux-PAM, conteniendo información sobre varios módulos PAM, una sección FAQ y documentación PAM adicional.

Nota

La documentación en el sitio web mencionado anteriormente describe la última versión de PAM y puede que no sea completamente compatible con la versión de PAM incluida en Red Hat Enterprise Linux.

5. TCP Wrappers y xinetd

El control del acceso a los servicios de red es una de las tareas de seguridad más importantes que un administrador de servidores debe enfrentar. Red Hat Enterprise Linux, proporciona un gran número de herramientas encargadas de ésta tarea. Por ejemplo, un cortafuegos basado en `iptables` deja afuera los paquetes de red que no son bienvenidos dentro de la pila de red del kernel. Para los servicios de red que lo utilizan, los *TCP wrappers* añaden una capa adicional de protección mediante la definición de cuáles hosts tienen permitido conectarse a los servicios de red encapsulados ("*wrapped*"). Uno de los servicios de red wrapped es el *super servicio*`xinetd`. Este servicio se le llama super servicio porque controla la conexión a un subconjunto de servicios de red y refina aún más el control de acceso.

Figura 21.9, “Control de acceso a los servicios de red” es una ilustración básica de cómo estas herramientas funcionan para proteger los servicios de red.

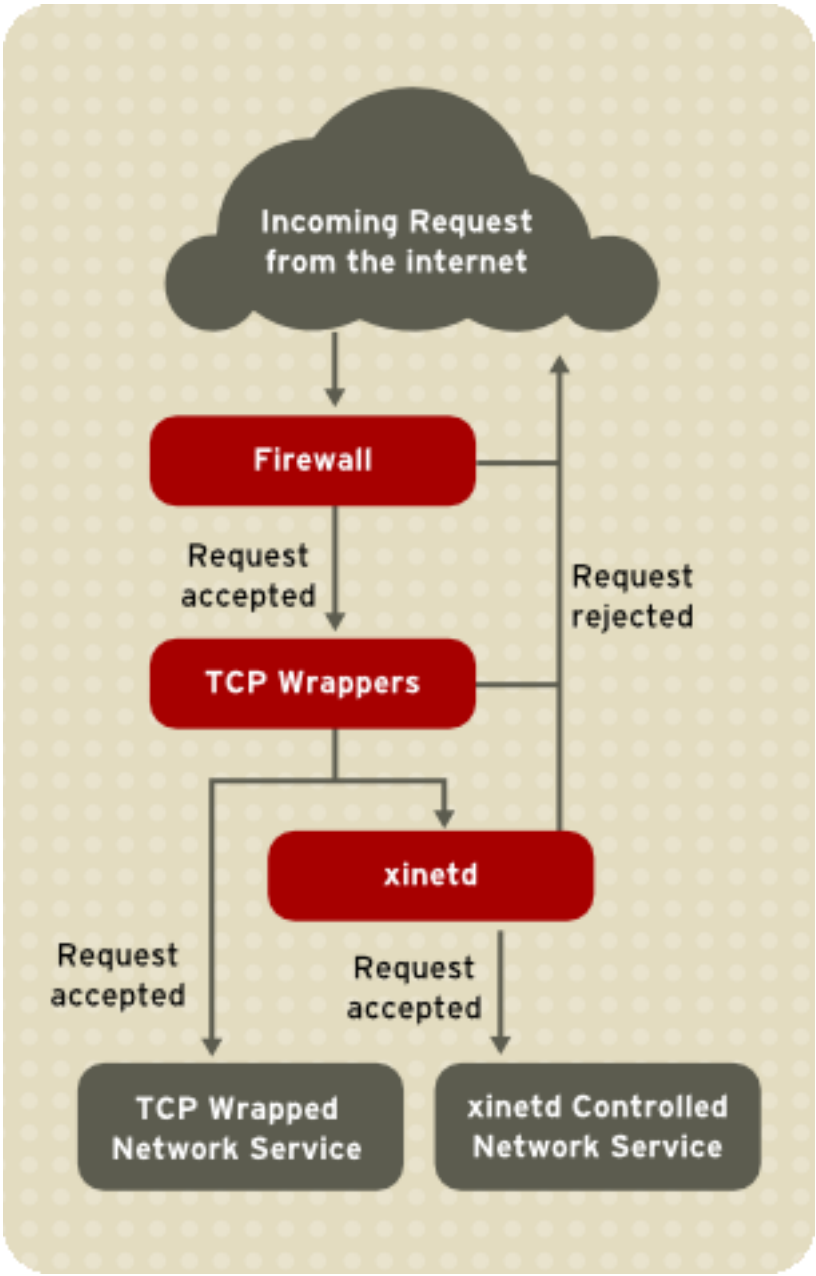


Figura 21.9. Control de acceso a los servicios de red

5.1. Wrappers TCP

El paquete TCP wrappers (`tcp_wrappers`) está instalado por defecto y proporciona control de acceso basado en host a los servicios de red. El componente más importante dentro del paquete es la biblioteca `/usr/lib/libwrap.a`. En términos generales, un servicio TCP wrapped es uno que ha sido compilado con la biblioteca `libwrap.a`.

Cuando un intento de conexión es hecho a un servicio encapsulado con TCP-wrappers, el servicio referencia primero los archivos de acceso a host (`/etc/hosts.allow` y `/etc/hosts.deny`) para determinar si el cliente tiene permitido conectarse. En la mayoría de los casos, se utiliza luego el demonio syslog (`syslogd`) para escribir el nombre del host solicitante y el servicio solicita-

do a `/var/log/secure` o `/var/log/messages`.

Si a un cliente se le permite conectarse, los TCP Wrappers liberan el control de la conexión al servicio solicitado y no interfieren más con la comunicación entre el cliente y el servidor.

Además del control de acceso y registro, los TCP Wrappers pueden activar comandos para interactuar con el cliente antes de negar o liberar el control de la conexión al servicio solicitado.

Puesto que los TCP Wrappers son una utilidad de gran valor dentro de las herramientas de seguridad de cualquier administrador de servidores, la mayoría de los servicios de red dentro de Red Hat Enterprise Linux están enlazados con la biblioteca `libwrap.a`. Algunas de tales aplicaciones incluyen `/usr/sbin/sshd`, `/usr/sbin/sendmail`, y `/usr/sbin/xinetd`.

Nota

Para determinar si un servicio de red binario está enlazado con la librería `libwrap.a`, escriba el comando siguiente como usuario root:

```
ldd <binary-name> | grep libwrap
```

Reemplace *<binary-name>* con el nombre del binario de servicio de red.

Si el comando retorna al intérprete de comandos sin ninguna salida, entonces el servicio de red *no* está enlazado con `libwrap.a`.

El siguiente ejemplo muestra que `/usr/sbin/sshd` está enlazado a `libwrap.a`:

```
[root@myserver ~]# ldd /usr/sbin/sshd | grep libwrap
        libwrap.so.0 =
> /usr/lib/libwrap.so.0 (0x00655000)
[root@myserver ~]#
```

5.1.1. Ventajas de los TCP Wrappers

Los TCP Wrappers ofrecen las siguientes ventajas básicas comparado con las otras técnicas de control de servicios de red:

- *Transparencia tanto para el host cliente y el servicio de red encapsulado* — Tanto el cliente que está realizando la conexión como el servicio de red encapsulado no están al tanto de que TCP Wrappers está siendo usado. Los usuarios legítimos son registrados y conectados al servicio solicitado mientras que las conexiones de clientes prohibidos fallan.
- *Administración centralizada de múltiples protocolos.* — Los TCP Wrappers operan separadamente de los servicios de red que ellos protegen, permitiendo a muchas aplicaciones de servidor compartir un conjunto común de archivos de configuración para una administración más sencilla.

5.2. Archivos de configuración de Wrappers TCP

Para determinar si una máquina cliente tiene permitido conectarse a un servicio, los TCP Wrap-

pers consultan los siguientes dos archivos, los cuales se conocen comúnmente como archivos de *acceso a host*:

- `/etc/hosts.allow`
- `/etc/hosts.deny`

Cuando un servicio que usa TCP-wrappers recibe una petición de un cliente, se siguen los siguientes pasos:

1. *Referencias a `/etc/hosts.allow`.* — El servicio wrapped TCP analiza secuencialmente el archivo `/etc/hosts.allow` y aplica la primera regla especificada para ese servicio. Si encuentra una regla que coincide, permite la conexión. De lo contrario continúa con el paso siguiente.
2. *Referencia a `/etc/hosts.deny`.* — El servicio wrapped TCP analiza secuencialmente el archivo `/etc/hosts.deny`. Si encuentra una regla que coincide, rechaza la conexión. De lo contrario, el acceso al servicio es coincidido.

Los puntos siguientes se deben considerar cuando se usen TCP-wrappers para proteger servicios de red:

- Puesto que las reglas de acceso en `hosts.allow` son aplicadas primero, ellas toman precedencia sobre las reglas en `hosts.deny`. Por lo tanto, si se permite el acceso a un servicio en `hosts.allow`, una regla negando el acceso al mismo servicio en `hosts.deny` es ignorada.
- Las reglas en cada archivo son leídas de arriba hacia abajo y la primera regla que coincida para un servicio dado es la única aplicada. Por lo tanto el orden de las reglas es extremadamente importante.
- Si no se encuentra ninguna regla para el servicio en ninguno de los archivos, o si no existe ninguno de los archivos, se concede el acceso al servicio.
- Los sevicios encapsulados con TCP wrappers no hacen caché de las reglas desde los archivos de acceso de host, por lo tanto cualquier cambio a `hosts.allow` o a `hosts.deny` tomarán efecto de inmediato sin tener que reiniciar el servicio de red.

Aviso

Si la última línea de un archivo de acceso a host no es un caracter de nueva línea (creado al presionar la tecla **Intro**), la última regla en el archivo fallará y se registrará un error bien sea a `/var/log/messages` o a `/var/log/secure`. Este es también el caso para reglas que se expanden en múltiples líneas sin usar la barra oblicua. El ejemplo siguiente ilustra la porción relevante del mensaje registrado por una falla de una regla debido a alguna de estas circunstancias:

```
warning: /etc/hosts.allow, line 20: missing newline or line too long
```

5.2.1. Formatear reglas de acceso

Los formatos para `/etc/hosts.allow` y `/etc/hosts.deny` son idénticos. Cualquier línea en blanco o que comience con un símbolo de numeral (#) será ignorada.

Las reglas se tienen que formatear de la siguiente manera:

```
<daemon list>: <client list> [: <option>: <option>: ...]
```

- *<daemon list>* — Una lista separada por comas de los nombres de procesos (*no* de los nombres de servicios) o el comodín `ALL` (consulte Sección 5.2.1.4, “Operadores”) para permitir mayor flexibilidad.
- *<client list>* — Una lista separada por comas de nombres de host, direcciones IP, patrones especiales o comodines que identifican los hosts afectados por la regla. La lista de clientes también acepta operadores listados en la Sección 5.2.1.4, “Operadores” para permitir mayor flexibilidad.
- *<option>* — Una acción opcional o una lista separada con puntos y comas de acciones realizadas cuando la regla es activada. Los campos de opciones soportan expansiones, lanzan comandos desde el shell, otorgan o prohiben el acceso y alteran el comportamiento de la conexión.

Nota

En esta guía puede encontrar mayor información sobre los términos especializados arriba mencionados:

- Sección 5.2.1.1, “Comodines”
- Sección 5.2.1.2, “Patrones”
- Sección 5.2.2.4, “Expansiones”
- Sección 5.2.2, “Campos de opciones”

A continuación una muestra básica de una regla de acceso:

```
vsftpd : .example.com
```

Esta regla instruye a los TCP Wrappers a que estén atentos por conexiones al demonio FTP (`vsftpd`) desde cualquier host en el dominio `example.com`. Si esta regla aparece en `hosts.allow`, la conexión será aceptada. Si esta regla aparece en `hosts.deny`, la conexión será rechazada.

El próximo ejemplo de regla de acceso es un poco más compleja y utiliza dos campos de opciones:

```
sshd : .example.com  \ : spawn /bin/echo `/bin/date` access denied>>/var/log/sshd.log \ : deny
```

Note que cada campo de opción está precedido por una barra oblicua invertida (\). Use la barra para prevenir que falle la regla debido al largo de la misma.

Esta regla de ejemplo indica que si una conexión al demonio SSH (`sshd`) se intenta desde un host en el dominio `example.com`, el comando `echo` es ejecutado para añadir el intento a un archivo de registro especial y la conexión es rechazada. Puesto que se usa la directiva opcional `deny`, esta línea rechazará el acceso aún si aparece en el archivo `hosts.allow`. Para más detalles sobre las opciones disponibles, consulte la Sección 5.2.2, “Campos de opciones”.

5.2.1.1. Comodines

Los comodines permiten a los TCP Wrappers coincidir más fácilmente grupos de demonios o hosts. Son usados con mayor frecuencia en el campo de lista de cliente de las reglas de acceso.

Se pueden utilizar los siguientes comodines:

- `ALL` — Hace corresponder todo. Se puede usar tanto para la lista de demonios como para la lista de clientes.
- `LOCAL` — Hace corresponder todos los nombres de máquinas que no contengan un punto (.), tal como localhost.
- `KNOWN` — Hace corresponder todas las máquinas cuyos nombres y direcciones son conocidos o donde el usuario es conocido.
- `UNKNOWN` – Hace corresponder todas las máquinas cuyos nombres y direcciones sean desconocidas o en el caso en el que se desconozca el usuario.
- `PARANOID` — Hace corresponder todas las máquinas cuyo nombre no se corresponda con la dirección.

Atención

Los comodines `KNOWN`, `UNKNOWN` y `PARANOID` que usarse con cuidado ya que dependen de servidores DNS en funcionamiento para una correcta operación. Cualquier error en la resolución de nombres puede impedir que usuarios legítimos accedan al servicio.

5.2.1.2. Patrones

Los patrones se pueden utilizar en el campo de lista de cliente de las reglas de acceso para especificar de forma más precisa grupos de host clientes.

La siguiente es una lista de los patrones más comúnmente aceptados para una entrada de lista de cliente:

- *Nombre de host comenzando con un punto (.)* — Al colocar un punto al comienzo de un nombre de host, se hace coincidir todos los hosts compartiendo los componentes listados

del nombre. El ejemplo siguiente aplicaría a cualquier host dentro del dominio `example.com`:

```
ALL : .example.com
```

- *Dirección IP que termina con un punto (.)* — Al colocar un punto al final de una dirección IP hace corresponder todos los hosts compartiendo el grupo numérico inicial de una dirección IP. El ejemplo siguiente aplicará a cualquier host dentro de la red `192.168.x.x`:

  ```
  ALL : 192.168.
  ```

- *Par dirección IP/máscara* — Las expresiones de máscaras de red también pueden ser usadas como un patrón de control de acceso a un grupo particular de direcciones IP. El ejemplo siguiente aplicaría a cualquier host con una dirección de `192.168.0.0` hasta `192.168.1.255`:

  ```
  ALL : 192.168.0.0/255.255.254.0
  ```

Importante

Cuando se esté trabajando en el espacio de direcciones de IPv4, no se soporta el largo del par dirección/prefijo (*prefixlen*). Sólo las reglas IPv6 pueden utilizar este formato.

- *Par [Dirección IPv6]/prefixlen* — Los pares [net]/prefixlen también pueden ser usadas como un patrón de control de acceso a un grupo particular de direcciones IPv6. El ejemplo siguiente aplicaría a cualquier host con una dirección de `3ffe:505:2:1::` hasta 3ffe:505:2`:1:ffff:ffff:ffff:ffff`:

  ```
  ALL : [3ffe:505:2:1::]/64
  ```

- *El asterisco (*)* — Los asteriscos pueden ser usados para coincidir grupos completos de nombres de host o direcciones IP, siempre y cuando no se mezclen en la lista de cliente conteniendo otros tipos de patrones. El ejemplo siguiente aplicaría a cualquier host dentro del dominio `example.com`:

  ```
  ALL : *.example.com
  ```

- *La barra oblicua (/)* — Si una lista de cliente inicia con una barra, ésta es tratada como un nombre de archivo. Esta característica es útil si se necesitan reglas que especifiquen un gran número de hosts. El ejemplo siguiente se refiere a los TCP Wrappers en el archivo `/etc/telnet.hosts` para todas las conexiones de Telnet:

  ```
  in.telnetd : /etc/telnet.hosts
  ```

Otros patrones menos usados son también aceptados por los TCP Wrappers. Consulte la página man (5) de `hosts_access` para obtener mayor información.

Aviso

Preste espacial atención al usar nombres de host y de dominio. Los invasores pueden usar una variedad trucos para burlar las resolución de nombres. Además, cualquier interrupción en el servicio DNS podría impedir el acceso a servicios incluso a la usuarios que tienen el permiso. Lo mejor es utilizar direcciones IP siempre que sea posible.

5.2.1.3. Portmap y Wrappers TCP

La implementación `Portmap` de TCP Wrappers no soporta búsquedas de host, lo cual quiere decir que `portmap` no puede utilizar hostnames para identificar hosts. Por lo cual, las reglas de control de acceso para portmap en `hosts.allow` o `hosts.deny` deben usar direcciones IP, o la palabra clave `ALL`, para especificar los hosts.

Cambios a las reglas de control de acceso de `portmap` pueden que no tomen efecto de inmediato. Usted si no se reinicia el servicio `portmap`.

Los servicios ampliamente usados, tales como NIS y NFS, dependen de `portmap` para funcionar, por lo tanto esté consciente de estas limitaciones.

5.2.1.4. Operadores

Actualmente, las reglas de control de acceso aceptan un operador, `EXCEPT`. Se puede usar tanto en la lista de demonios como en la lista de cliente de una regla.

El operador `EXCEPT` permite excepciones específicas a coincidencias más amplias dentro de la misma regla.

En el ejemplo siguiente desde un archivo `hosts.allow`, todos los hosts de `example.com` pueden conectarse a todos los servicios excepto `cracker.example.com`:

```
ALL: .example.com EXCEPT cracker.example.com
```

En el otro ejemplo desde un archivo `hosts.allow`, clientes desde la red `192.168.0.x` pueden usar todos los servicios excepto para FTP:

```
ALL EXCEPT vsftpd: 192.168.0.
```

Nota

Organizacionalmente, a menudo es más fácil evitar el uso de operadores `EXCEPT`. Esto permite a otros administradores escanear rápidamente los archivos adecuados para ver qué hosts deberían tener o no acceso a los servicios, sin tener que revisar varios operadores `EXCEPT`.

5.2.2. Campos de opciones

Además de las reglas básicas para permitir o prohibir el acceso, la implementación de Red Hat Enterprise Linux de TCP Wrappers soporta extensiones al lenguaje de control de acceso a través de los *campos de opciones*. Mediante el uso de campos de opciones dentro de las reglas de acceso al host, los administradores pueden llevar a cabo una gran variedad de tareas tales como alterar el comportamiento del registro, consolidar el control de acceso y lanzar comandos del shell.

5.2.2.1. Registro

Los campos de opciones le permiten a los administradores cambiar fácilmente la facilidad de registro y el nivel de prioridad para una regla usando la directiva `severity`.

En el ejemplo siguiente, las conexiones al demonio SSH desde cualquier host en el dominio `example.com` son registrados a la facilidad por defecto `authprivsyslog` (debido a que no se especifica un valor de facilidad) con una prioridad de `emerg`:

```
sshd : .example.com : severity emerg
```

Es también posible especificar una facilidad utilizando la opción `severity`. El ejemplo siguiente registra cualquier intento de conexión SSH por cualquier hosts desde el dominio `example.com` a la facilidad `local0` con una prioridad de `alert`:

```
sshd : .example.com : severity local0.alert
```

Nota

En práctica, este ejemplo no funcionará hasta que el demonio syslog (`syslogd`) sea configurado para registrar a la facilidad `local0`. Consulte la página del manual de `syslog.conf` para información sobre la configuración de las facilidades de registro personalizadas.

5.2.2.2. Control de acceso

Los campos de opciones también le permiten a los administradores explícitamente otorgar o prohibir el acceso de máquinas en un sola regla, añadiendo la directiva `allow` o `deny` al final de la opción.

Por ejemplo, las dos reglas siguientes permiten conexiones SSH desde `client-1.example.com`, pero prohiben conexiones desde `client-2.example.com`:

```
sshd : client-1.example.com : allow
sshd : client-2.example.com : deny
```

Al permitir el control de acceso por regla, el campo de opciones permite a los administradores consolidar todas las reglas de acceso en un sólo archivo: bien sea `hosts.allow` o `hosts.deny`. Algunos consideran que esta es una forma más fácil de organizar reglas de acceso.

5.2.2.3. Comandos de la Shell

Los campos de opciones permiten a las reglas de acceso lanzar comandos de la shell a través

de las directivas siguientes:

- `spawn` — Lanza un comando de la shell como un proceso hijo. Esta directiva de opción puede realizar tareas como el uso de `/usr/sbin/safe_finger` para obtener más información sobre el cliente solicitante o la creación de archivos de registro especiales usando el comando `echo`.

  En el ejemplo siguiente, los clientes intentando acceder a servicios de Telnet desde el dominio `example.com` son registrados discretamente a un archivo especial:

  ```
  in.telnetd : .example.com \
          : spawn /bin/echo `/bin/date` from %h>>/var/log/telnet.log \
          : allow
  ```

- `twist` — Reemplaza el servicio solicitado con el comando especificado. Esta directriz se utiliza a menudo para colocar trampas para intrusos (también llamados "potes de miel"). También se puede utilizar para enviar mensajes a los clientes que se estan conectando. La directriz `twist` debe estar al final de la línea de la regla.

  En el ejemplo siguiente, los clientes que intentan acceder al servicio FTP desde el dominio `example.com` se les envía un mensaje a través del comando `echo`:

  ```
  vsftpd : .example.com \
          : twist /bin/echo "421 This domain has been black-listed. Access denied!"
  ```

Para obtener mayor información sobre las opciones de comando de la shell, consulte la página del manual de `hosts_options`.

5.2.2.4. Expansiones

Las expansiones, cuando se utilizan en conjunto con las directrices `spawn` y `twist`, proporcionan información sobre el cliente, servidor y los procesos relacionados.

A continuación se presenta una lista de las expansiones soportadas:

- `%a` — Suministra la dirección IP del cliente.
- `%A` — Suministra la dirección IP del servidor.
- `%c` — Proporciona información variada sobre el cliente, como el nombre de usuario y el de la máquina o el nombre del usuario y la dirección IP.
- `%d` — Proporciona el nombre del proceso demonio.
- `%h` — Suministra el nombre de la máquina del cliente (o la direccción IP, si el nombre de la máquina no está disponible).
- `%H` — Suministra el nombre de la máquina del servidor (o la dirección IP si el nombre de la máquina no está disponible).
- `%n` — Proporciona el nombre de la máquina del cliente. Si no está disponible aparecerá `unknown`. Si el nombre de la máquina y la dirección de la máquina no corresponden, aparecerá `paranoid`.

- %N — Proporciona el nombre de la máquina del servidor. Si no está disponible aparecerá unknown. Si el nombre de la máquina y su dirección no coinciden, aparecerá paranoid.
- %p — Suministra el ID del proceso demonio.
- %s — Suministra información varia del servidor como el proceso demonio y la máquina o la dirección IP del servidor.
- %u — Proporciona el nombre de usuario del cliente. Si no está disponible aparecerá unknown.

El ejemplo siguiente usa una expansión en conjunto con el comando spawn para identificar el host cliente en un archivo de registro personalizado.

Cuando se intentan conexiones al demonio SSH (sshd) desde un host en el dominio example.com, ejecute el comando echo para registrar el intento, incluyendo el nombre del host cliente (usando la expansión %h), a un archivo especial:

```
sshd : .example.com  \
        : spawn /bin/echo `/bin/date` access denied to %h>>/var/log/sshd.log \
        : deny
```

De forma similar, las expansiones se pueden utilizar para personalizar mensajes de vuelta al cliente. En el ejemplo siguiente, los clientes que intentan acceder al servicio FTP desde el dominio example.com son informados que se les ha prohibido acceder al servidor:

```
vsftpd : .example.com \
: twist /bin/echo "421 %h has been banned from this server!"
```

Para una explicación completa de las expansiones disponibles, así como también opciones de control de acceso adicionales, revise la sección 5 de la página man para hosts_access (man 5 hosts_access) y la página man de hosts_options.

Consulte Sección 5.5, “Recursos adicionales” para obtener mayor información sobre TCP Wrappers.

5.3. xinetd

El demonio xinetd es un *super servicio* que utiliza TCP-wrappers. Éste controla el acceso a un subconjunto de servicios de red populares incluyendo FTP, IMAP y Telnet. También proporciona opciones de configuración específicas al servicio para el control de acceso, registro mejorado, redireccionamiento y control de utilización de recursos.

Cuando un cliente intenta conectarse a un servicio de red controlado por xinetd, el super servicio recibe la petición y revisa las reglas de control de acceso de TCP Wrappers.

Si el acceso es permitido, xinetd verifica que la conexión este permitida bajo sus propias reglas de acceso para ese servicio. Asimismo verifica que el servicio no tiene más recursos asignados a él y que éste cumpla las reglas definidas.

Si todas estas condiciones son cumplidas (se permite al acceso al servicio; el servicio no ha llegado a su límite de recursos; y el servicio no viola ninguna regla), xinetd inicia una instancia del servicio solicitado y pasa el control de la conexión a éste. Una vez la conexión se ha establecido, xinetd no toma parte en la comunicación entre el servidos y el cliente.

5.4. Archivos de configuración de xinetd

Los archivos de configuración para `xinetd` son los siguientes:

- `/etc/xinetd.conf` — El archivo de configuración global de `xinetd`.
- `/etc/xinetd.d/` — El directorio que contiene todos los archivos específicos al servicio.

5.4.1. El archivo /etc/xinetd.conf

El archivo `/etc/xinetd.conf` contiene parámetros de configuración generales los cuales afectan cada servicio bajo el control de `xinetd`. Se lee una vez cuando el servicio `xinetd` es iniciado, por esto, para que los cambios de la configuración tomen efecto, el administrador debe reiniciar el servicio `xinetd`. Abajo se muestra un ejemplo del archivo `/etc/xinetd.conf`:

```
defaults
{
         instances               = 60
         log_type                = SYSLOG        authpriv
         log_on_success          = HOST PID
         log_on_failure          = HOST
         cps                     = 25 30
}
includedir /etc/xinetd.d
```

Estas líneas controlan los siguientes aspectos de `xinetd`:

- `instances` — Configura el máximo número de peticiones que `xinetd` puede manejar simultáneamente.
- `log_type` — Configura `xinetd` para usar la facilidad de registro `authpriv`, el cual escribe las entradas de registro al archivo `/var/log/secure`. Al agregar una directiva tal como `FILE / var/log/xinetdlog` aquí, creará un archivo de registro personalizado llamado `xinetdlog` en el directorio `/var/log/`.
- `log_on_success` — Configura `xinetd` a registrar si la conexión es exitosa. Por defecto, la dirección IP del host remoto y el ID del proceso del servidor procesando la petición son grabados.
- `log_on_failure` — Configura `xinetd` para registrar si hay una falla de conexión o si la conexión no es permitida.
- `cps` — Configura `xinetd` para no permitir más de 25 conexiones por segundo a cualquier servicio dado. Si se alcanza este límite, el servicio es retirado por 30 segundos.
- `includedir/etc/xinetd.d/` — Incluye las opciones declaradas en los archivos de configuración específicos del servicio localizados en el directorio `/etc/xinetd.d/`. Consulte la Sección 5.4.2, “El directorio /etc/xinetd.conf” para más información sobre este directorio.

Nota

A menudo, las configuraciones `log_on_success` y `log_on_failure` en `/`

`etc/xinetd.conf` son modificadas aún más en los archivos de registro específicos al servicio. Por esta razón, puede que aparezca más información en el registro de un servicio dado que lo que puede indicar el archivo`/etc/xinetd.conf`. Consulte la Sección 5.4.3.1, “Opciones de registro” para más información.

5.4.2. El directorio /etc/xinetd.conf

El directorio `/etc/xinetd.d/` contiene los archivos de configuración para cada servicio manejado por `xinetd` y los nombres de los archivos que se correlacionan con el servicio. Como sucede con `xinetd.conf`, este archivo sólo es leído cuando el servicio `xinetd` es arrancado. Para que los cambios tengan efecto, el administrador debe reiniciar el servicio `xinetd`.

El formato de los archivos en el directorio `/etc/xinetd.d/` usan las mismas convenciones que `/etc/xinetd.conf`. La razón principal por la que la configuración para cada servicio es almacenada en un archivo separado es hacer más fácil la personalización y que sea menos probable afectar otros servicios.

Para tener una idea de cómo estos archivos están estructurados, considere el archivo `/etc/xinetd.d/krb5-telnet`:

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/kerberos/sbin/telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Estas líneas controlan varios aspectos del servicio `telnet`:

- `service` — Define el nombre del servicio, usualmente uno listado en el archivo `/etc/services`.
- `flags` — Configura cualquier número de atributos para la conexión. `REUSE` instruye `xinetd` a reutilizar el socket para una conexión Telnet.

Nota

La opción `REUSE` está fuera de uso. Todos los servicios utilizan implicitamente la opción `REUSE`.

- `socket_type` — Configura el socket de red a escribir a `stream`.
- `wait` — Define si el servicio es de un sólo hilo (`yes`) o de múltiples hilos (`no`).
- `user` — Define bajo qué ID de usuario se ejecutará el proceso.

- `server` — Define el binario ejecutable a lanzar.
- `log_on_failure` — Define los parámetros de registro para `log_on_failure` además de aquellos ya definidos en `xinetd.conf`.
- `disable` — Especifica si el servicio está desactivado (`yes`) o activado (`no`).

Consulte la página man de `xinetd.conf` para obtener mayor información sobre estas opciones y su uso.

5.4.3. Modificando los archivos de configuración de xinetd

Existe una gran cantidad de directivas disponibles para los servicios protegidos por `xinetd`. Esta sección resalta algunas de las opciones usadas más comúnmente.

5.4.3.1. Opciones de registro

Las siguientes opciones de registro están disponibles para `/etc/xinetd.conf` y los archivos de configuración específicos al servicio en el directorio `/etc/xinetd.d/`.

A continuación se presenta una lista de las opciones de registro usadas más comúnmente:

- `ATTEMPT` — Indica que se intentó realizar una conexión pero que ésta falló (`log_on_failure`).
- `DURATION` — Indica el tiempo que un sistema remoto usa un servicio (`log_on_success`).
- `EXIT` — Indica el estado de salida o la señal de término del servicio (`log_on_success`).
- `HOST` — Indica la dirección IP de la máquina remota (`log_on_failure` y `log_on_success`).
- `PID` — Indica el ID del proceso del servidor que recibe la petición (`log_on_success`).
- `USERID` — Registra el usuario remoto que está usando el método definido en RFC 1413 para todos los servicios de multi procesos (`log_on_failure` y `log_on_success`).

Para obtener una lista completa de las opciones de registro, consulte la página de manual de `xinetd.conf`.

5.4.3.2. Opciones de control de acceso

Los usuarios de servicios `xinetd` pueden seleccionar usar reglas de acceso TCP Wrappers a hosts, proporcionar control de acceso a través de los archivos de configuración `xinetd`, o una mezcla de ambos. La información concerniente al uso de los archivos de control de acceso TCP Wrappers a hosts se puede encontrar en la Sección 5.2, “Archivos de configuración de Wrappers TCP”.

Esta sección discute el uso de `xinetd` para controlar el acceso a servicios.

Nota

A diferencia de los TCP Wrappers, los cambios al control de acceso sólo tengan

efecto si el administrador de `xinetd` reinicia el servicio `xinetd`.

A diferencia de los TCP Wrappers, el control de acceso a través de `xinetd` sólo afecta a los servicios controlados por `xinetd` mismo.

El control de acceso de `xinetd` es diferente del método usado por los TCP Wrappers. Mientras que los TCP Wrappers colocan toda la configuración del acceso dentro de dos archivos, `/etc/hosts.allow` y `/etc/hosts.deny`, el control de acceso de `xinetd` se encuentra en el archivo de configuración de cada servicio dentro del directorio `/etc/xinetd.d`.

Las opciones de acceso a host siguientes son soportadas por `xinetd`:

- `only_from` — Sólo permite que las máquinas específicas usen el servicio.
- `no_access` — Impide que estas máquinas usen el servicio.
- `access_times` — Especifica el intervalo de tiempo en el que un determinado servicio puede ser usado. El rango de tiempo debe especificarse en formato de 24 horas, HH:MM-HH:MM.

Las opciones `only_from` y `no_access` pueden usar una lista de direcciones IP o nombres de hosts, o pueden especificar una red completa. Como los TCP Wrappers, combinando el control del acceso `xinetd` con una configuración de conexión apropiada puede mejorar la seguridad mediante el bloqueo de peticiones de hosts vetados mientras que graba cada intento de conexión.

Por ejemplo, el siguiente archivo `/etc/xinetd.d/telnet` puede ser usado para bloquear el acceso a Telnet desde un un grupo de red particular y restringir el rango de tiempo general que inclusive los usuarios permitidos pueden conectarse:

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/kerberos/sbin/telnetd
        log_on_failure  += USERID
        no_access       = 172.16.45.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

En este ejemplo, cuando un sistema cliente desde la red `10.0.1.0/24`, tal como `10.0.1.2`, intenta acceder el servicio Telnet, recibirá un mensaje indicando lo siguiente:

```
Connection closed by foreign host.
```

Además, sus intentos de conexión son registrados en `/var/log/messages` como sigue:

```
Sep  7 14:58:33 localhost xinetd[5285]: FAIL: telnet address from=172.16.45.107
Sep  7 14:58:33 localhost xinetd[5283]: START: telnet pid=5285 from=172.16.45.107
Sep  7 14:58:33 localhost xinetd[5283]: EXIT: telnet status=0 pid=5285 duration=0(sec)
```

Cuando esté usando TCP Wrappers en conjunto con controles de acceso `xinetd`, es importante entender la relación entre los dos mecanismos de control de acceso.

A continuación se muestra el orden de las operaciones seguido por `xinetd` cuando un cliente solicita una conexión:

1. El demonio `xinetd` accede a las reglas de acceso a hosts TCP Wrappers a través de una llamada a la librería `libwrap.a`. Si alguna regla de rechazo coincide con el host cliente, la conexión se rechaza. Si una regla de aceptación coincide con el host cliente, la conexión pasa a `xinetd`.

2. El demonio `xinetd` verifica sus propias reglas de acceso para el servicio `xinetd` y el servicio solicitado. Si una regla de rechazo coincide con el host cliente la conexión es rechazada. De lo contrario, `xinetd` inicia una instancia del servicio solicitado y pasa el control de la conexión al mismo.

Importante

Se debe tener especial cuidado cuando se use el control de acceso wrappers TCP en conjunto con los controles `xinetd`. Un error en la configuración puede generar resultados no deseados.

5.4.3.3. Vincular y redirigir opciones

Los ficheros de configuración de servicios para el comando `xinetd` también soportan la vinculación del servicio a una dirección IP y el desvío de las peticiones entrantes para dicho servicio a otra dirección IP, nombre de la máquina o puerto.

La vinculación es controlada con la opción `bind` que se encuentra en el archivo de configuración específico del servicio, y une específicamente el servicio a una dirección IP del sistema. Una vez configurada, la opción `bind` sólo permite peticiones para la dirección IP apropiada para acceder al servicio. De esta forma se pueden vincular servicios diferentes a interfaces de red diferentes según sea necesario.

Esto es útil sobre todo para los sistemas con múltiples adaptadores de red o con múltiples direcciones IP. En tales sistemas, los servicios inseguros como Telnet, se pueden configurar de modo que solo escuche a la interfaz conectada a una red privada, y no a la interfaz conectada a Internet.

La opción `redirect` acepta la dirección IP o el nombre de la máquina seguido del número de puerto. Dice al servicio que desvíe todas las peticiones para dicho servicio a una localización y número de puerto específicos. Esta característica se usa para establecer otro número de puerto en el mismo sistema, desviar la petición a otra dirección IP en la misma máquina, cambiar la petición a otro sistema y puerto completamente diferentes o con la combinación de cualquiera de estas opciones. De esta manera, un usuario que está conectado a un determinado servicio en un sistema puede ser redirigido a otro sistema sin ninguna interrupción.

El demonio `xinetd` lleva a cabo este desvío lanzando un proceso que mantenga la conexión entre la máquina cliente que está mandando la petición y la máquina que está dando en ese momento el servicio, transfiriendo los datos de un sistema a otro.

El mayor beneficio de estas dos opciones (`bind` y `redirect`) se obtiene cuando se usan juntas. Vinculando un servicio a una dirección IP determinada en un sistema y luego desviando las peticiones de dicho servicio a una segunda máquina que sólo puede ver la primera máquina, se puede usar un sistema interno que ofrezca servicios para una red completamente diferente. Alternativamente, estas opciones se pueden usar para limitar la exposición de un servicio determinado a una dirección IP conocida, así como desviar todas las peticiones a ese servicio a otra máquina configurada específicamente para ese objetivo.

Por ejemplo, considere un sistema que se usa como firewall con la característica siguiente para su servicio Telnet:

```
service telnet
{
        socket_type               = stream
        wait                       = no
        server                       = /usr/kerberos/sbin/telnetd
        log_on_success               += DURATION USERID
        log_on_failure               += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 23
}
```

Las opciones `bind` y `redirect` en este archivo aseguran que el servicio Telnet en la máquina esté enlazado con la dirección IP externa (`123.123.123.123`), la que se encarga de Internet. Además, todas las peticiones del servicio Telnet enviadas a `123.123.123.123` son redirigidas a través de una segunda tarjeta de red a una dirección IP interna (`10.0.1.13`) a la que solo tienen acceso el firewall y los sistemas internos. El firewall manda luego la comunicación entre los dos sistemas y el sistema que se está conectando piensa que está conectado a `123.123.123.123` mientras que, de hecho, está conectado a otra máquina.

Esta característica es útil para los usuarios con conexiones de banda ancha y con una única dirección IP fija. Cuando se usa la NAT (de las siglas en inglés de Network Address Translation), los sistemas detrás de la máquina gateway, que están usando direcciones IP internas, no están disponibles desde afuera del sistema gateway. Sin embargo, cuando determinados servicios controlados por `xinetd` son configurados con las opciones `bind` y `redirect`, la máquina gateway puede funcionar como un proxy entre los sistemas externos y una máquina interna particular configurada para proporcionar el servicio. Además, las opciones de control de acceso `xinetd` y de conexión están también disponibles para protección adicional.

5.4.3.4. Opciones de administración de recursos

El demonio `xinetd` puede añadir un nivel básico de protección de un ataque Denial of Service (DoS). Abajo se encuentra una lista de las directivas que pueden ayudar en limitar la efectividad de tales ataques:

- `per_source` — Define el número máximo de instancias para un servicio por dirección IP. Acepta sólo enteros como argumentos y puede ser usado en `xinetd.conf` y los archivos de configuración específicos al servicio `xinetd.d/`.

- `cps` — Define el máximo número de conexiones por segundo. Esta directiva toma dos argumentos enteros separados por un espacio en blanco. El primero es el número máximo de conexiones permitidas por segundo. El segundo es el número de segundos que `xinetd` debe esperar antes de reactivar el servicio. Sólo acepta enteros como argumentos y puede ser usado en ambos `xinetd.conf` y los archivos de configuración específicos al servicio en el directorio `xinetd.d/`.

- `max_load` — Indica el umbral de uso del CPU para un servicio. Acepta un argumento en forma de número de punto flotante.

  El promedio de carga es una medición aproximada del número de procesos que están activos en un tiempo dado. Vea los comandos `uptime`, `who`, `procinfo` para obtener mayor información sobre el promedio de carga.

Hay más opciones de administración de recursos disponibles para `xinetd`. Consulte la página del manual de `xinetd.conf`.

5.5. Recursos adicionales

En la documentación del sistema y en el web puede encontrar información adicional concerniente a los TCP Wrappers y a `xinetd`.

5.5.1. Documentación instalada

La documentación en su sistema es un buen lugar para comenzar a buscar información sobre los Wrappers TCP, `xinetd` y las opciones de control de acceso.

- `/usr/share/doc/tcp_wrappers-<version>/` — Contiene un archivo `README` que discute cómo los TCP Wrappers funcionan y los diferentes riesgos de spoofing de host y de direcciones IP que existen.

- `/usr/share/doc/xinetd-<version>/` — Incluye un archivo `README` que discute aspectos del control de acceso y un archivo `sample.conf` con varias ideas para la modificación de archivos de configuración específicos al servicio en el directorio `/etc/xinetd.d/`.

- Las páginas man relacionadas a TCP wrappers y `xinetd` — Hay un buen número de páginas man para las varias aplicaciones y archivos de configuración relacionados con TCP wrappers y `xinetd`. La siguiente es una lista con las páginas man más importantes.

  Aplicaciones de servidor

  - `man xinetd` — La página del manual para `xinetd`.

  Archivos de configuración

  - `man 5 hosts_access` — La página del manual para los archivos de control de acceso TCP Wrappers.

  - `man hosts_options` — La página del manual para los campos de opciones de TCP Wrappers.

- `man xinetd.conf` — La página del manual listando las opciones de configuración `xinetd`.

5.5.2. Sitios Web de utilidad

- http://www.xinetd.org/ [http://www.xinetd.org] — El sitio principal de `xinetd`, contiene archivos de configuración de ejemplo, una lista completa de las características y una sección de Preguntas más frecuentes FAQ.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Un tutorial completo que discute las diferentes formas de ajustar los archivos de configuración `xinetd` por defecto para cubrir objetivos específicos.

5.5.3. Libros relacionados

- *Hacking Linux Exposed* por Brian Hatch, James Lee y George Kurtz; Osbourne/McGraw-Hill — Un recurso excelente de seguridad con información sobre TCP Wrappers y `xinetd`.

6. Redes privadas virtuales (VPNs)

Las organizaciones con varias oficinas satelitales se conectan a menudo con líneas dedicadas para proteger los datos confidenciales en tránsito. Por ejemplo, muchos negocios utilizan frame relay o líneas ATM (*Asynchronous Transfer Mode*), como una solución de redes para enlazar una oficina con las otras. Esto puede ser una propuesta costosa, especialmente para negocios pequeños o medianos (SMB) que desean extenderse sin tener que pagar los altos costos asociados a circuitos digitales dedicados de nivel corporativo.

Para resolver este problema, se desarrollaron las *Redes privadas virtuales* (VPN). Siguiendo los mismos principios funcionales de los circuitos dedicados, las VPN permiten una comunicación digital segura entre dos partes (o redes), creando una *red de área amplia* (WAN) a partir las *Redes de área local* (LAN) existentes. La diferencia con respecto a frame relay o ATM está en el medio de transporte. Las VPN transmiten sobre IP usando datagramas como capa de transporte, haciendo un conducto seguro a través de la Internet hasta la dirección de destino. La mayoría de las implementaciones de software libre de VPN incorporan estándares abiertos y encriptación para enmascarar aún más el tránsito de datos.

Algunas organizaciones emplean soluciones de hardware VPN para aumentar la seguridad, mientras que otras utilizan las implementaciones basadas en software o protocolos. Hay muchos fabricantes con soluciones de hardware VPN tales como Cisco, Nortel, IBM y Checkpoint. Hay una solución libre de VPN basada en software para Linux llamada FreeS/Wan que utiliza una implementación estandarizada de IPSec (o *Protocolo de Seguridad de Internet*). Estas soluciones VPN, sin importar si están basadas en hardware o software, actúan como enrutadores especializados que se colocan entre la conexión IP desde una oficina a la otra.

6.1. ¿Cómo funciona un VPN?

Cuando un paquete es transmitido desde un cliente, éste se envía a través de un router o gateway VPN, el cual añade el *Encabezado de autenticación* (AH) para enrutamientos y autenticación. Los datos son luego encriptados y, finalmente, cerrados con una *Carga de seguridad de*

encapsulación (ESP). Esta última constituye las instrucciones de control y desencriptación.

El enrutador VPN receptor extrae la información, desencripta los datos y la enruta a su destino (bien sea una estación de trabajo o un nodo en la red). Usando una conexión de red-a-red, el nodo receptor en la red local recibe los paquetes descifrados y listos para ser procesados. El proceso de encriptación/descifrado en una conexión VPN de red-a-red es transparente al nodo local.

Con tal nivel de seguridad, un cracker debe no sólo interceptar un paquete, sino además descifrarlo. Los intrusos que empleen el tipo de ataque "Hombre en el medio" entre un servidor y el cliente deben también tener acceso al menos a una de las llaves privadas para la autenticación de sesiones. Puesto que solamente emplean varias capas de autenticación y encriptación, las VPN son una forma efectiva y segura de conectar nodos remotos múltiples para actuar como una única Intranet.

6.2. VPNs y Red Hat Enterprise Linux

Red Hat Enterprise Linux proporciona varias opciones para implementar una solución de software para conectarse de forma segura a sus WAN. El *Internet Protocol Security* o IPsec es la implementación *VPN* soportada por Red Hat Enterprise Linux que resuelve de forma completa las necesidades de utilización de las organizaciones con sucursales o con usuarios remotos.

6.3. IPsec

Red Hat Enterprise Linux es compatible con IPsec para la conexión entre hosts y redes remotos utilizando un túnel seguro en un transportador de red común tal como la Internet. IPsec se puede implementar usando una conexión host-a-host (una computadora a la otra) o de red-a-red (una LAN/WAN a la otra).

La implementación IPsec en Red Hat Enterprise Linux utiliza el *Intercambio de llaves en Internet* (*IKE*), el cual es un protocolo implementado por el Internet Engineering Task Force (IETF), a ser usado para la autenticación mutua y asociaciones seguras entre sistemas conectándose.

6.4. Creando una conexión IPsec

Una conexión IPsec se divide en dos fases lógicas. En la fase 1, un nodo IPsec inicializa la conexión con el nodo o red remota. El nodo/red remota verifica las credenciales del nodo solicitante y ambos lados negocian el método de autenticación para la conexión.

En sistemas Red Hat Enterprise Linux, una conexión IPsec utiliza el método de *llave precompartida* de autenticación de nodo IPsec. En una conexión IPsec de llaves precompartidas, ambos hosts deben utilizar la misma llave para pasar a la fase dos de la conexión IPsec.

Es en la fase 2 de la conexión IPsec donde se crea una *asociación de seguridad* (SA) entre nodos IPsec. Esta fase establece una base de datos SA con información de configuración, tal como el método de encriptación, parámetros de intercambio de llaves secretas y más. Esta fase maneja realmente la conexión IPsec entre nodos remotos y redes.

La implementación de Red Hat Enterprise Linux de IPsec utiliza IKE para compartir las llaves entre hosts a través de la Internet. El demonio de manejo de llaves `racoon` se encarga de la distribución e intercambio de llaves IKE. Consulte las páginas man de `racoon` para obtener mayor información sobre este demonio.

6.5. Instalación de IPsec

La implementación de IPsec requiere que esté instalado el paquete RPM `ipsec-tools` en todos los hosts IPsec (si se está utilizando una configuración de host-a-host) o enrutadores (si se está usando una configuración de red-a-red). El paquete RPM contiene las bibliotecas esenciales, los demonios y los archivos de configuración para ayudar en la configuración de una conexión IPsec, incluyendo:

- `/sbin/setkey` — manipula la administración de llaves y los atributos de seguridad de IPsec en el kernel. Este ejecutable es controlado por el demonio de manejo de llaves `racoon`. Para más información sobre `setkey`, consulte la página man `setkey`(8).
- `/sbin/racoon` — El demonio de administrador de llave IKE, utilizado para administrar y controlar asociaciones de seguridad y llaves compartidas entre sistemas conectados a través de IPsec.
- `/etc/racoon/racoon.conf` — El archivo de configuración del demonio `racoon` utilizado para configurar los diferentes aspectos de la conexión IPsec, incluyendo los métodos de autenticación y algoritmos de encriptación usados en la conexión. Para ver un listado completo de las directivas disponibles, consulte la página man de `racoon.conf`(5).

Para configurar IPsec en Red Hat Enterprise Linux, usted puede utilizar la **Herramienta de administración de red** o editar manualmente los archivos de configuración de red y IPsec.

- Para conectar dos host conectados a redes a través de IPsec, consulte la Sección 6.6, “Configuración IPsec de host-a-host ”.
- Para conectar una LAN/WAN a otra a través de IPsec, vaya a la Sección 6.7, “Configuración de IPsec de red-a-red”.

6.6. Configuración IPsec de host-a-host

IPsec se puede configurar para conectar un escritorio o estación de trabajo a otro a través de una conexión host-a-host. Este tipo de conexión utiliza la red a la cual están conectados los hosts para crear un túnel seguro entre ellos. Los requerimientos de una conexión host-a-host son mínimos, como lo es la configuración de IPsec en cada host. Los hosts solamente necesitan una conexión dedicada al transportador de red (tal como la Internet) y Red Hat Enterprise Linux para crear la conexión IPsec.

6.6.1. Configuración host-a-host

Una conexión IPsec host-a-host en una conexión encriptada entre dos sistemas que ejecutan IPsec con la misma llave de autenticación. Con la conexión IPsec activa, todo el tráfico de red entre los dos hosts es encriptada.

Para configurar una conexión IPsec, utilice los siguientes pasos para cada host:

Nota

Debe ejecutar los siguientes pasos en la máquina que esta configurando. Evite configurar y establecer conexiones IPsec remotamente.

1. En un intérprete de comandos escriba `system-config-network` para iniciar la **Herramienta de administración de redes**.
2. En la pestaña **IPsec**, haga clic en **Nuevo** para iniciar el ayudante de configuración.
3. Haga clic en **Adelante** para iniciar la configuración de una conexión IPsec de host-a-host:
4. Introduzca un nombre único para la conexión, por ejemplo, **`ipsec0`**. Si se requiere, seleccione la casilla de verificación para automáticamente activar la conexión cuando el computador inicie. Haga clic en **Adelante** para continuar.
5. Seleccione **Encriptación de host a host** como tipo de conexión y haga clic en **Adelante**.
6. Seleccione el tipo de encriptación a usar: manual o automática.

   Si selecciona encriptación manual, una llave de encriptación debe ser proporcionada posteriormente. Si selecciona encriptación automática, el demonio `racoon` administra la llave de encriptación. El paquete `ipsec-tools` debe ser instalado si desea utilizar encriptación automática.

   Haga clic en **Adelante** para continuar.
7. Introduzca la dirección IP del host remoto.

   Para determinar la dirección IP del host remoto, utilice el siguiente comando *en el host remoto*:

   ```
   [root@myServer ~] # /sbin/ifconfig <device>
   ```

   en donde `<device>` es el dispositivo Ethernet que usted desea utilizar para la conexión VPN. Si sólo una tarjeta Ethernet existe en su sistema, el nombre de dispositivo es generalmente eth0. El siguiente ejemplo muestra la información relevante de este comando (tenga en cuenta que es un ejemplo de la salida únicamente):

   ```
   eth0      Link encap:Ethernet  HWaddr 00:0C:6E:E8:98:1D
             inet addr:172.16.44.192  Bcast:172.16.45.255  Mask:255.255.254.0
   ```

   La dirección IP es el número que va después de `inet addr:`

   Haga clic en **Adelante** para continuar.
8. Si la encriptación manual fue seleccionada en el paso 6, especifique la llave de encriptación a usar o haga clic en **Generar** para crear una llave.

   a. Especifique una llave de autenticación o haga clic en **Generar** para generar una llave. Puede ser cualquier combinación de números y letras.

b. Haga clic en **Adelante** para continuar.

9. Verifique la información en la página **IPsec — Resumen** y haga clic en **Aplicar**.

10. Haga clic en **Archivo** => **Guardar** para guardar la configuración.

    Podría tener que reiniciar la red para que los cambios surtan efecto. Para reiniciar la red utilice el siguiente comando:

    ```
    [root@myServer ~]# service network restart
    ```

11. Seleccione la conexión IPsec desde la lista y haga clic en **Activar**.

12. Repita todo el procedimiento para el otro host. Es importante que se utilice la misma llave del paso 8 en los otros hosts. De lo contrario IPsec no funcionará.

Después de configurar la conexión IPsec, aparecerá en la lista IPsec tal y como se muestra en la Figura 21.10, “Conexión IPsec”.

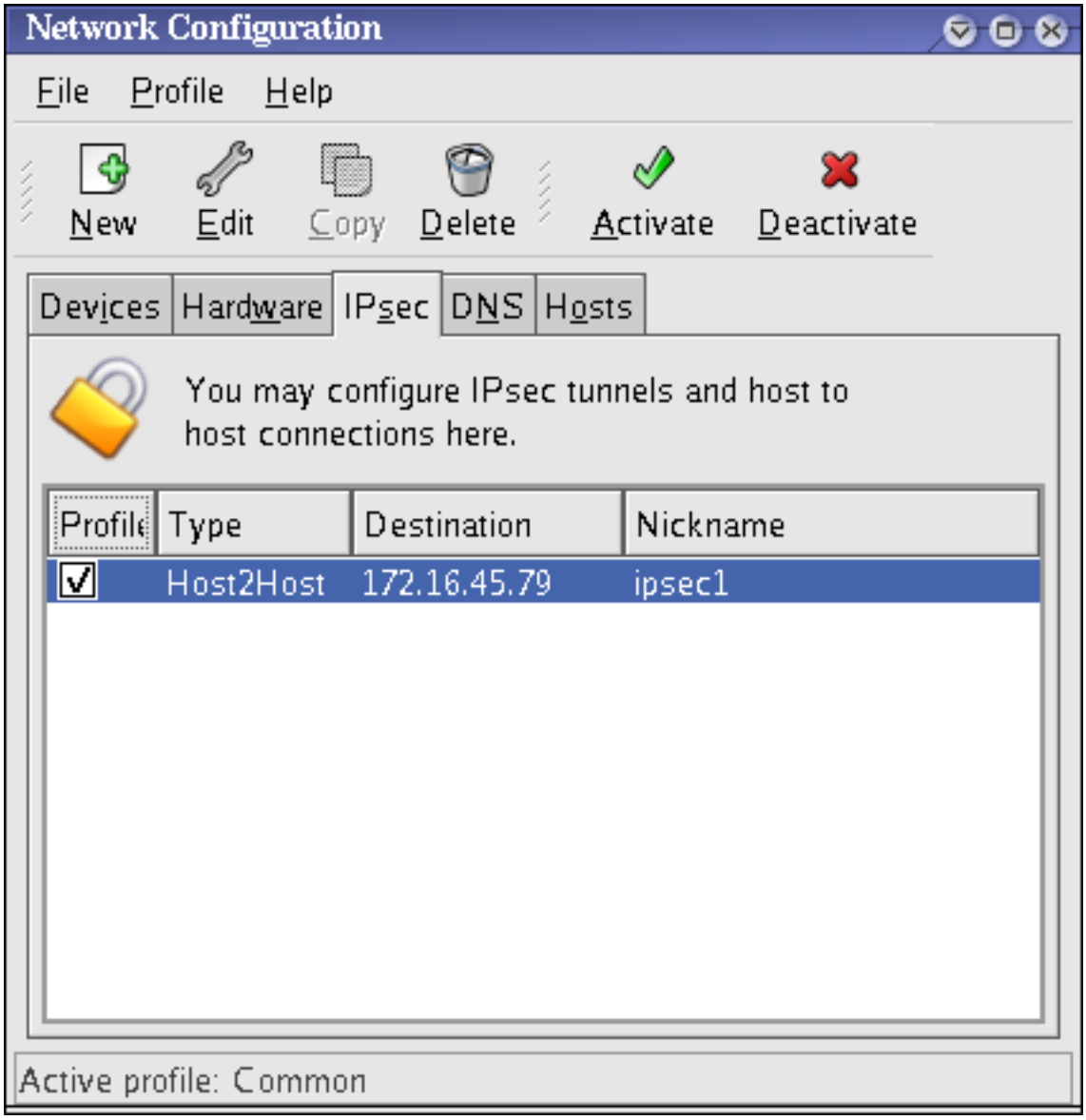


Figura 21.10. Conexión IPsec

Los siguientes archivos son creados cuando la conexión IPsec es configurada:

- `/etc/sysconfig/network-scripts/ifcfg-<nickname>`
- `/etc/sysconfig/network-scripts/keys-<nickname>`
- `/etc/racoon/<remote-ip>.conf`
- `/etc/racoon/psk.txt`

Si se selecciona la encriptación automática, el archivo `/etc/racoon/racoon.conf` es también creado.

Cuando la interfaz está activa, `/etc/racoon/racoon.conf` se modifica para incluir `<remote-ip>.conf`.

6.6.2. Configuración manual de IPsec de host-a-host

El primer paso en la creación de una conexión es reunir la información del sistema y de la red de cada estación de trabajo. Para una conexión host-a-host, necesita la información siguiente:

- La dirección IP para ambos hosts
- Un nombre único, por ejemplo, `ipsec1`. Éste es utilizado para identificar la conexión IPsec y para distinguirla de otros dispositivos y conexiones.
- Una llave encriptada fija o una generada automáticamente por `racoon`
- Una llave de autenticación pre-compartida que se utiliza para iniciar la conexión e intercambiar las llaves de encriptación durante la sesión

Por ejemplo, suponga que la Estación A y la Estación B desean conectarse a través de un túnel IPsec. Ellas desean conectarse usando una llave pre-compartida con el valor de `Key_Value01` y los usuarios acuerdan dejar que `racoon` automáticamente genere y comparta una llave de autenticación entre cada host. Ambos usuarios de los hosts deciden nombrar sus conexiones como `ipsec1`.

Nota

Usted debería escoger un PSK que utilice mayúsculas y minúsculas, números y caracteres de puntuación. Un PSK que sea fácil de adivinar constituye un riesgo de seguridad.

No es necesario utilizar el mismo nombre de conexión para cada host. Debería escoger un nombre que es significativo y conveniente para su instalación.

El siguiente es el archivo de configuración IPsec para una conexión IPsec de host-a-host para la Estación A con la Estación B. El nombre único para identificar la conexión en este ejemplo es *ipsec1*, por lo cual el archivo resultante es llamado `/etc/sysconfig/network-scripts/ifcfg-ipsec1`

```
DST=X.X.X.X
TYPE=IPSEC
ONBOOT=no
IKE_METHOD=PSK
```

Para la Estación A, *x.x.x.x* es la dirección IP de la Estación B. Para la Estación B, *x.x.x.x* es la dirección IP de la Estación A. Esta conexión no está configurada para iniciarse durante el inicio del sistema (`ONBOOT=no`) y utiliza el método de autenticación de llave pre-compartida (`IKE_METHOD=PSK`).

El siguiente es el contenido del archivo de llave pre-compartida (llamado `/etc/sysconfig/network-scripts/keys-ipsec1`) que ambas estaciones de trabajo necesitan para autenticarse mutuamente. Los contenidos de este archivo deberían ser idénticos en ambas estaciones de trabajo y solamente el usuario root debería ser capaz de leer o escribir en el mismo.

```
IKE_PSK=Key_Value01
```

Importante

Para cambiar el archivo `keys-ipsec1` para que solamente el usuario root pueda leerlo o modificarlo, ejecute el comando siguiente después de crear el archivo:

```
[root@myServer ~] # chmod 600 /etc/sysconfig/network-scripts/keys-ipsec1
```

Para cambiar la llave de autenticación en cualquier momento, modifique el archivo `keys-ipsec1` en ambas estaciones de trabajo. *Ambas llaves deben ser idénticas para una conectividad apropiada*.

El siguiente ejemplo muestra la configuración específica para la fase 1 de la conexión al host remoto. El archivo es llamado *x.x.x.x*`.conf` (reemplace *x.x.x.x* con la dirección IP del enrutador IPsec remoto). Observe que este archivo es generado automáticamente una vez que el túnel IPsec es activado y no se debería modificar directamente.

```
remote X.X.X.X
{
         exchange_mode aggressive, main;
         my_identifier address;
         proposal {
                  encryption_algorithm 3des;
                 hash_algorithm sha1;
                 authentication_method pre_shared_key;
                 dh_group 2 ;
        }
}
```

El archivo de configuración predeterminado para la fase 1 creado cuando se inicializa una co-

nexión IPsec contiene las siguientes declaraciones utilizadas por la implementación Red Hat Enterprise Linux de IPsec:

remote *x.x.x.x*
: Especifica que las estrofas subsecuentes de este archivo de configuración sólo se aplican al nodo remoto identificado por la dirección IP *x.x.x.x*

exchange_mode aggressive
: La configuración predeterminada para IPsec en Red Hat Enterprise Linux utiliza un método de autenticación agresivo, que reduce la sobrecarga de la conexión a la vez que permite la configuración de muchas conexiones IPsec con múltiples hosts.

my_identifier address
: Define el método de autenticación a utilizar cuando se autentifican nodos. Red Hat Enterprise Linux utiliza direcciones IP para identificar a los nodos.

encryption_algorithm 3des
: Define el cifrado de encriptación utilizado durante la autenticación. Por defecto, se utiliza *Triple Data Encryption Standard* (3DES).

hash_algorithm sha1;
: Especifica el algoritmo hash utilizado durante la negociación de la fase 1 entre nodos. Por defecto, se utiliza el Secure Hash Algorithm versión 1.

authentication_method pre_shared_key
: Define el método de autenticación utilizado durante la negociación de nodos. Por defecto, Red Hat Enterprise Linux utiliza llaves pre-compartidas para la autenticación.

dh_group 2
: Especifica el número de grupo Diffie-Hellman para establecer llaves de sesión generadas dinámicamente. Por defecto, se utiliza modp1024 (grupo 2).

6.6.2.1. El archivo de configuración de Racoon

El archivo `/etc/racoon/racoon.conf` debería ser idéntico en todos los nodos IPsec *excepto* por la declaración `include "/etc/racoon/x.x.x.x.conf"`. Esta declaración (y el archivo que referencia) es generado cuando se activa el túnel IPsec. Para la Estación A, *x.x.x.x* en la declaración `include`, es la dirección IP de la Estación B. Lo contrario es también cierto para la Estación B. A continuación se muestra un archivo `racoon.conf` típico cuando se activa la conexión IPsec.

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour ;
        encryption_algorithm 3des, blowfish 448, rijndael ;
        authentication_algorithm hmac_sha1, hmac_md5 ;
        compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf";
```

Este archivo `racoon.conf` predeterminado incluye rutas definidas para la configuración de IPsec, archivos de llaves pre-compartidas y certificados. Los campos en `sainfo anonymous` describen la fase 2 SA entre nodos IPsec — la naturaleza de la conexión IPsec (incluyendo los algoritmos de encriptación soportados) y el método de intercambio de llaves. La lista siguiente define los campos de la fase 2.

sainfo anonymous
: Denota que SA puede inicializarse de forma anónima con cualquier par siempre que las credenciales IPsec coincidan.

pfs_group 2
: Define el protocolo de intercambio de llaves Diffie-Hellman, el cual determina el método en el cual los nodos IPsec establecen una sesión temporal mutua para la segunda fase de conectividad de IPsec. Por defecto, la implementación de Red Hat Enterprise Linux de IPsec utiliza el grupo 2 (o `modp1024`) de los grupos de intercambio de llaves criptográficas de Diffie-Hellman. El grupo 2 utiliza un exponente modular de 1024 bits que evita que los atacantes descifren transmisiones IPsec previas aún si una llave privada está comprometida.

lifetime time 1 hour
: Este parámetro especifica el ciclo de vida de un SA y se puede cuantificar por veces o por bytes de datos. La implementación predeterminada de Red Hat Enterprise Linux de IPsec especifica un tiempo de vida de una hora.

encryption_algorithm 3des, blowfish 448, rijndael
: Especifica los códigos de encriptación soportados para la fase 2. Red Hat Enterprise Linux soporta 3DES, 448-bit Blowfish y Rijndael (el código utilizado en el *Advanced Encryption Standard* o AES).

authentication_algorithm hmac_sha1, hmac_md5
: Lista los algoritmos hash soportados para la autenticación. Los modos soportados son los códigos de autenticación de mensajes en hash (HMAC) sha1 y md5.

compression_algorithm deflate
: Define el algoritmo de compresión Deflate para el soporte de IP Payload Compression (IPCOMP), lo que permite transmisiones potenciales más rápidas de datagramas IP sobre conexiones más lentas.

Para iniciar la conexión, utilice el siguiente comando en cada host:

```
[root@myServer ~]# /sbin/ifup <nickname>
```

en donde <nickname> es el nombre que especificó para la conexión IPsec.

Para verificar la conexión IPsec, ejecute la utilidad `tcpdump` para ver los paquetes de red que están siendo transferidos entre los hosts y verificar que están encriptados con IPsec. El paquete debería incluir una cabecera AH y se deberían mostrar como paquetes ESP. ESP significa que están encriptados. Por ejemplo:

```
[root@myServer ~]# tcpdump -n -i eth0 host <targetSystem>

IP 172.16.45.107
```

```
> 172.16.44.192: AH(spi=0x0954ccb6,seq=0xbb): ESP(spi=0x0c9f2164,seq=0xbb)
```

6.7. Configuración de IPsec de red-a-red

IPsec también se puede configurar para conectar una red completa (tal como una LAN o una WAN) a una red remota a través de una conexión red-a-red. Una conexión de red-a-red requiere la configuración de enrutadores IPsec en cada lado de las redes conectantes para procesar y enrutar la información de forma transparente desde un nodo en una LAN a otro nodo en una LAN remota. La Figura 21.11, “Una conexión en túnel IPsec de red-a-red” muestra una conexión IPsec de red-a-red en túnel.

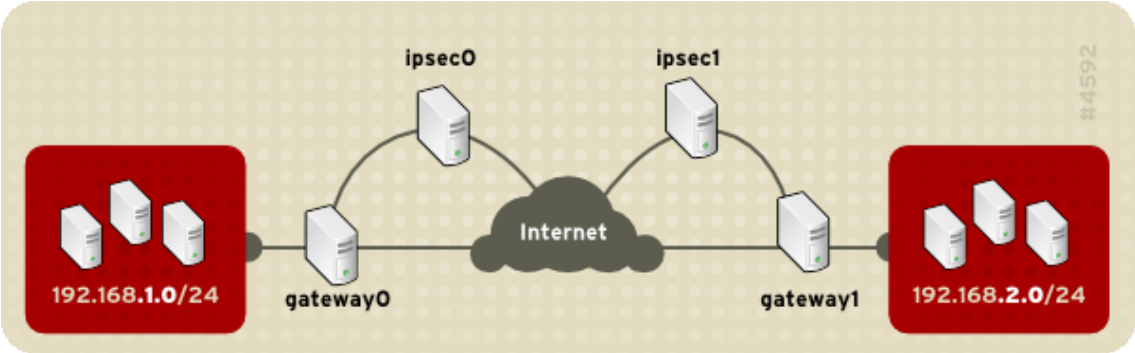


Figura 21.11. Una conexión en túnel IPsec de red-a-red

El diagrama muestra dos LAN separadas por la Internet. Estas LAN utilizan enrutadores IPsec para autenticar e iniciar una conexión usando un túnel seguro a través de la Internet. Los paquetes que son interceptados en tránsito requerirán un descifrado de fuerza bruta para poder descifrar el código protegiendo los paquetes entre las LAN. El proceso de comunicación desde un nodo en el intervalo IP 192.168.1.0/24 al otro en 192.168.2.0/24 es completamente transparente a los nodos puesto que el procesamiento, encriptación/descifrado y el enrutamiento de los paquetes IPsec es manejado completamente por el enrutador IPsec.

La información necesaria para la conexión red-a-red incluye:

- Las direcciones IP accesibles externamente de los enrutadores IPsec dedicados
- Los intervalos de direcciones de red de las LAN/WAN servidas por los enrutadores IPsec (tales como 192.168.0.0/24 o 10.0.1.0/24)
- Las direcciones IP de los dispositivos de puertas de enlace que enrutan los datos desde un nodo de la red a la Internet:
- Un nombre único, por ejemplo, `ipsec1`. Éste es utilizado para identificar la conexión IPsec y para distinguirla de otros dispositivos y conexiones.
- Una llave encriptada fija o una generada automáticamente por `racoon`
- Una llave de autenticación pre-compartida que se utiliza para iniciar la conexión e intercambiar las llaves de encriptación durante la sesión

6.7.1. Conexión (VPN) de red-a-red

Una conexión IPsec de red-a-red utiliza dos routers IPsec, uno para cada red, por los cuales el tráfico de red para la subred privada es dirigido.

Por ejemplo, como se muestra en la figura Figura 21.12, “IPsec de red-a-red”, si la red privada 192.168.1.0/24 envía tráfico de red a la red privada 192.168.2.0/24, los paquetes pasan por gateway0, a ipsec0, a través de Internet, a ipsec1, a gateway1, y a la subred 192.168.2.0/24.

Los enrutadores IPsec requieren direcciones IP públicamente accesibles y un segundo dispositivo de Ethernet conectado a sus respectivas redes privadas. El tráfico sólo pasa a través de enrutador IPsec si es dirigido a otro enrutador IPsec con el cual tiene una conexión encriptada.

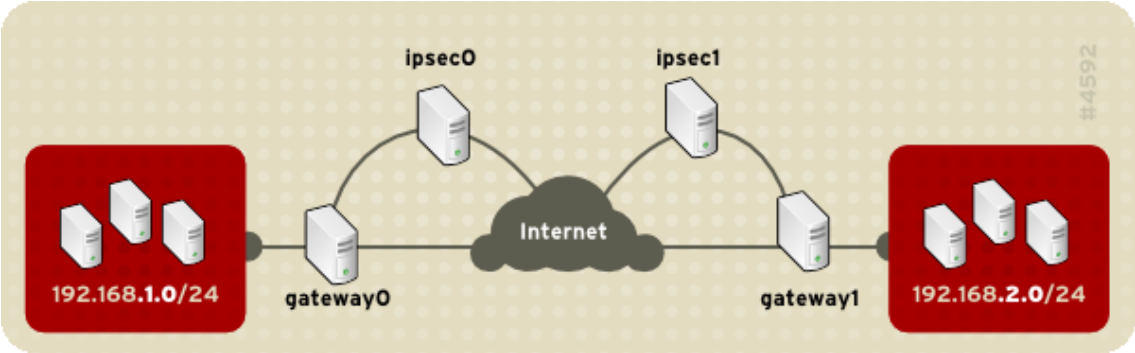


Figura 21.12. IPsec de red-a-red

Entre las opciones de configuración de red alternativas se encuentra un cortafuego entre cada enrutador IP y la Internet y un cortafuegos de intranet entre cada enrutador IPsec y la puerta de enlace de la subred. El enrutador IPsec y la puerta de enlace para la subred pueden ser un sistema con dos dispositivos Ethernet: uno con una dirección IP pública que actúa como enrutador IPsec y otro con una dirección IP privada que actúa como puerta de enlace para la subred privada. Cada enrutador IPsec puede utilizar la puerta de enlace para su red privada o una puerta de enlace pública para enviar los paquetes al otro enrutador IPsec.

Utilice el siguiente procedimiento para configurar una conexión IPsec de red-a-red:

1. En un intérprete de comandos escriba `system-config-network` para iniciar la **Herramienta de administración de redes**.
2. En la pestaña **IPsec**, haga clic en **Nuevo** para iniciar el ayudante de configuración.
3. Haga clic en **Adelante** para iniciar la configuración de una conexión IPsec de red-a-red.
4. Introduzca un sobrenombre único para la conexión, por ejemplo, **`ipsec0`**. Si se requiere, seleccione la casilla de verificación para activar automáticamente la conexión cuando el computador inicie. Haga clic en **Adelante** para continuar.
5. Seleccione **Encriptación de red a red (VPN)** como el tipo de conexión y haga clic en **Adelante**.
6. Seleccione el tipo de encriptación a usar: manual o automática.

Si selecciona encriptación manual, una llave de encriptación debe ser proporcionada posteriormente. Si selecciona encriptación automática, el demonio `racoon` administra la llave de encriptación. El paquete `ipsec-tools` debe ser instalado si desea utilizar encriptación automática.

Haga clic en **Adelante** para continuar.

7. En la página **Red Local** introduzca la siguiente información:

   - **Dirección de red local** — La dirección IP del dispositivo en el enrutador IPsec conectado a la red privada.
   - **Máscara de subred local** — La máscara de subred de la dirección IP de la red local.
   - **Puerta de enlace local** — La puerta de enlace para la puerta de enlace privada.

   Haga clic en **Adelante** para continuar.

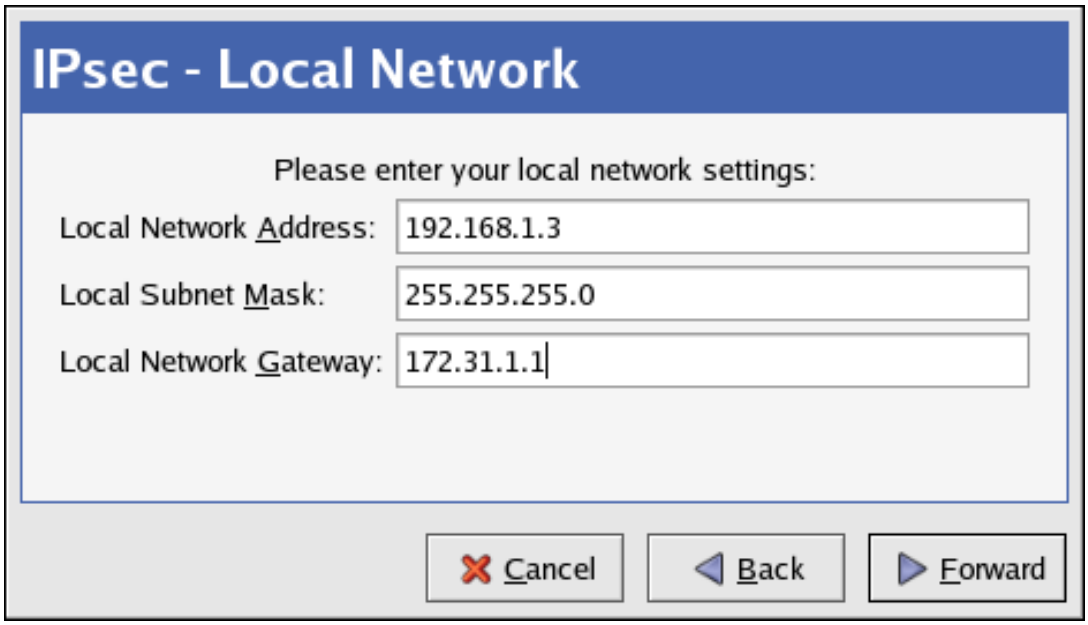


Figura 21.13. Información de red local

8. En la página **Red remota**, introduzca la siguiente información:

   - **Dirección IP remota** — La dirección IP públicamente accesibles del enrutador IPsec para la *otra* red privada. En nuestro ejemplo, para ipsec0, introduzca la dirección IP públicamente accesible de ipsec11 y viceversa.
   - **Dirección de red remota** — La dirección de red de la subred privada detrás del *otro* enrutador IPsec. En nuestro ejemplo, introduzca **`192.168.1.0`** si se está configurando ipsec1, e introduzca **`192.168.2.0`** si configura ipsec0.
   - **Máscara de subred remota** — La máscara de subred de la dirección IP remota.

- **Puerta de enlace remota** — La dirección IP de la puerta de enlace para la dirección de red remota.
- Si se seleccionó la encriptación manual en el 6, especifique la llave de encriptación a utilizar o haga clic en **Generar** para crear una nueva.

  Especifique una llave de autenticación o haga clic en **Generar** para generar una. Esta llave puede ser una combinación de números y letras.

Haga clic en **Adelante** para continuar.

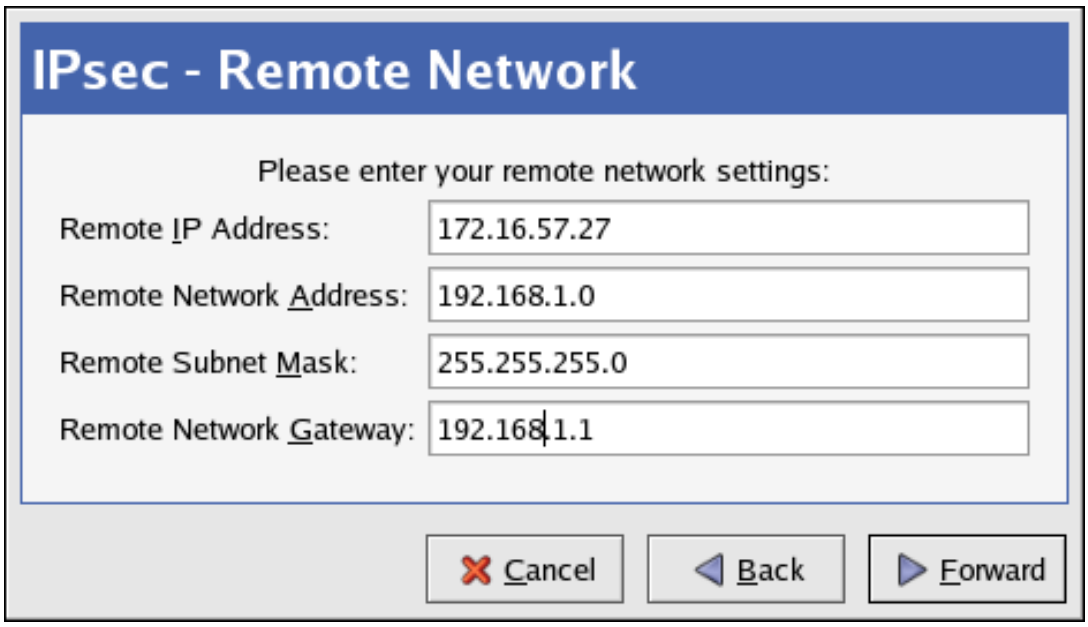


Figura 21.14. Información de red remota

9. Verifique la información en la página **IPsec — Resumen** y haga clic en **Aplicar**.
10. Seleccione **Archivo** => **Guardar** para guardar la configuración.
11. Seleccione la conexión IPsec desde la lista y haga clic en **Activar** para activar la conexión.
12. Activar reenvío IP

    a. Modifique `/etc/sysctl.conf` y configure `net.ipv4.ip_forward` a `1`.

    b. Utilice el siguiente comando para activar el cambio:

    ```
    [root@myServer ~]# /sbin/sysctl -p /etc/sysctl.conf
    ```

El script de red para activar la conexión IPsec crea automáticamente los enrutadores de red para enviar los paquetes a través del enrutador IPsec si es necesario.

6.7.2. Configuración manual de IPsec de red-a-red

Suponga que LAN A (lana.example.com) y LAN B (lanb.example.com) desean conectarse entre ellas a través de un túnel IPsec. La dirección de red para la LAN A están en el intervalo 192.168.1.0/24, mientras que LAN B utiliza el intervalo 192.168.2.0/24. La dirección IP de la puerta de enlace es 192.168.1.254 para LAN A y 192.168.2.254 para LAN B. Los enrutadores IPsec están separados de cada puerta de enlace de las LAN y utilizan dos dispositivos de redes: eth0 está asignado a una dirección IP estática accesible externamente que tiene acceso a la Internet, mientras que eth1 actúa como un punto de enrutamiento para procesar y transmitir paquetes LAN desde un nodo de la red a los nodos de redes remotos.

La conexión IPsec entre cada red utiliza una llave pre-compartida con el valor de `r3dh4tl1nux` y los administradores de A y B acuerdan dejar que `racoon` genere automáticamente y comparta una llave de autenticación entre cada enrutador IPsec. El administrador de la LAN A decide nombrar la conexión IPsec `ipsec0`, mientras que el administrador de la LAN B llama a su conexión IPsec `ipsec1`.

El siguiente ejemplo muestra el contenido de un archivo `ifcfg` para una conexión IPsec de red-a-red para la LAN A. El nombre único para identificar la conexión en este ejemplo es *`ipsec0`*, por lo que el archivo resultante es llamado `/etc/sysconfig/network-scripts/ifcfg-ipsec0`.

```
TYPE=IPSEC
ONBOOT=yes
IKE_METHOD=PSK
SRCGW=192.168.1.254
DSTGW=192.168.2.254
SRCNET=192.168.1.0/24
DSTNET=192.168.2.0/24
DST=X.X.X.X
```

La siguiente lista describe el contenido de este ejemplo:

TYPE=IPSEC
: Especifica el tipo de conexión.

ONBOOT=yes
: Especifica que la conexión debe ser iniciada durante el periodo de arranque.

IKE_METHOD=PSK
: Especifica que la conexión utiliza llaves el método de autenticación de llaves pre-compartidas.

SRCGW=192.168.1.254
: La dirección IP de la puerta de enlace fuente. Para LAN A, la puerta de enlace de LAN A, y para LAN B, la puerta de enlace LAN B.

DSTGW=192.168.2.254
: La dirección IP de la puerta de enlace del destino. Para LAN A, la puerta de enlace LAN B, para LAN B, la puerta de enlace LAN A.

SRCNET=192.168.1.0/24
: Especifica la red fuente para la conexión IPsec. En este ejemplo es el rango de red para LAN A.

DSTNET=192.168.2.0/24

Especifica la red de destino para la conexión IPsec. En este ejemplo es el rango de red para LAN B.

DST=X.X.X.X
: Las direcciones IP accesibles externamente de LAN B.

El siguiente ejemplo muestra el contenido de un archivo de llave pre-compartida llamado `/etc/sysconfig/network-scripts/keys-ipsec`*x* (donde *x* es 0 para la LAN A y 1 para la LAN B) que ambas redes utilizan para autenticarse mutuamente. Los contenidos de este archivo deberían ser idénticos y solamente el usuario root debería tener acceso a leer o escribir en este archivo.

```
IKE_PSK=r3dh4tl1nux
```

Importante

Para cambiar el archivo `keys-ipsec`*x* para que solamente el usuario root pueda leerlo o modificarlo, ejecute el comando siguiente después de crear el archivo:

```
chmod 600 /etc/sysconfig/network-scripts/keys-ipsec1
```

Para cambiar la llave de autenticación en algún momento, modifique el archivo `keys-ipsec`*x* en ambos enrutadores IPsec. *Ambas llaves deber ser idénticas para obtener una conectividad apropiada*.

El siguiente ejemplo muestra el contenido del archivo de configuración `/etc/racoon/racoon.conf` para la conexión IPsec. Observe que la línea `include` al final del archivo es generada automáticamente y solamente aparece si el tunel IPsec se está ejecutando.

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.
path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

sainfo anonymous
{
        pfs_group 2;
        lifetime time 1 hour ;
        encryption_algorithm 3des, blowfish 448, rijndael ;
        authentication_algorithm hmac_sha1, hmac_md5 ;
        compression_algorithm deflate ;
}
include "/etc/racoon/X.X.X.X.conf"
```

A continuación se muestra la configuración específica para la conexión a la red remota. El archivo es llamado *x.x.x.x*`.conf` (reemplace *x.x.x.x* con la dirección IP del enrutador IPsec remoto). Observe que este archivo es generado automáticamente una vez que el túnel IPsec es activado y no se debería modificar directamente.

```
remote X.X.X.X
{
        exchange_mode aggressive, main;
        my_identifier address;
        proposal {
```

```
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2 ;
        }
}
```

Antes de iniciar la conexión IPsec, se debería activar el reenvío IP en el kernel. Para activar el reenvío IP:

1. Modifique `/etc/sysctl.conf` y configure `net.ipv4.ip_forward` a **`1`**.
2. Utilice el siguiente comando para activar el cambio:

```
[root@myServer ~] # sysctl -p /etc/sysctl.conf
```

Para iniciar la conexión IPsec, ejecute el comando siguiente en cada enrutador:

```
[root@myServer ~] # /sbin/ifup ipsec0
```

Las conexiones son activadas y ambas LAN A y LAN B son capaces de comunicarse entre ellas. Los enrutadores se crean automáticamente a través del script de inicialización que se llama ejecutando `ifup` en la conexión IPsec. Para mostrar una lista de rutas para la red, ejecute el comando siguiente:

```
[root@myServer ~] # /sbin/ip route list
```

Para evaluar la conexión IPsec, ejecute la utilidad `tcpdump` en el dispositivo enrutable externamente (eth0 en este ejemplo) para así ver los paquetes de red que están siendo transmitidos entre los hosts (o redes) y verificar que están encriptados a través de IPsec. Por ejemplo, para verificar la conectividad IPsec de la LAN A, escriba lo siguiente:

```
[root@myServer ~] # tcpdump -n -i eth0 host lana.example.com
```

El paquete debería incluir una cabecera AH y se deberían mostrar como paquetes ESP. ESP significa que están encriptados. Por ejemplo (las barras oblícuas denotan la continuación de una línea):

```
12:24:26.155529 lanb.example.com > lana.example.com: AH(spi=0x021c9834,seq=0x358): \
        lanb.example.com > lana.example.com: ESP(spi=0x00c887ad,seq=0x358) (DF) \
        (ipip-proto-4)
```

6.8. Iniciando y deteniendo conexiones IPsec

Si la conexión IPsec no fue configurada para activar durante el inicio, usted puede controlarla desde la línea de comandos.

Para iniciar la conexión, utilice el siguiente comando para cada host en una conexión IPsec de host-a-host o cada enrutador IPsec para una conexión IPsec de red-a-red:

```
[root@myServer ~] # /sbin/ifup <nickname>
```

donde `<nickname>` es el apodo configurado anteriormente, por ejemplo `ipsec0`.

Para detener la conexión utilice el siguiente comando:

```
[root@myServer ~] # /sbin/ifdown <nickname>
```

7. IPTables

Red Hat Enterprise Linux contiene herramientas avanzadas para el *filtrado de paquetes* de red — el proceso de controlar los paquetes de red al entrar, mientras se mueven y cuando salen de la red dentro del kernel. Los kernels anteriores al 2.4 dependían en `ipchains` para el filtrado de paquetes y usaban listas de reglas aplicadas a los paquetes en cada paso del proceso de filtrado. La introducción de kernel 2.4 trajo consigo `iptables` (también llamado *netfilter*); aunque es similar a `ipchains`, expande enormemente el ámbito y el control disponible para el filtrado de paquetes de red.

Este capítulo se centra en las nocivas básicas del filtrado de paquetes, define las diferencias entre `ipchains` e `iptables`, explica las diferentes opciones disponibles con comandos `iptables` y muestra cómo se pueden preservar las reglas de filtrado durante reinicios del sistema.

Para instrucciones sobre cómo construir reglas `iptables` y configurar un cortafuegos basado en estas reglas, consulte la Sección 7.7, “Recursos adicionales”.

Aviso

El mecanismo predeterminado de cortafuegos en la versión 2.4 y posterior del kernel es `iptables`, pero éste no se puede usar si ya se está ejecutando `ipchains`. Si `ipchains` está presente durante el arranque, el kernel emitirá un error y no podrá arrancar `iptables`.

Estos errores no afectan la funcionalidad del comando `ipchains`.

7.1. Filtrado de paquetes

El kernel de Linux utiliza **Netfilter** para filtrar paquetes, permitiendo aceptar algunos de ellos en el sistema mientras que intercepta y detiene otros. Esta utilidad es interna en el kernel de Linux e incorpora las siguientes tres *tablas* o *listas de reglas*:

- `filter` — La tabla por defecto para el manejo de paquetes de red.
- `nat` — Usada para alterar paquetes que crean una nueva conexión y utilizada para la *Traducción de direcciones de red* (*Network Address Translation*, *NAT*).
- `mangle` — Usada por tipos específicos de alteración de paquetes.

Cada una de estas tablas tiene un grupo de *cadenas* incorporadas que corresponden a las acciones llevadas a cabo en el paquete por `netfilter`.

Las cadenas internas para la tabla `filtro` son las siguientes:

- *INPUT* — Aplica a los paquetes recibidos a través de una interfaz de red.

- *OUTPUT* — Esta cadena sirve para paquetes enviados por medio de la misma interfaz de red que recibió los paquetes.
- *FORWARD* — Esta cadena sirve para paquetes recibidos en una interfaz de red y enviados en otra.

Las cadenas internas para la tabla `nat` son las siguientes:

- *PREROUTING* — Altera los paquetes de red cuando estos llegan.
- *POSTROUTING* — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.
- *POSTROUTING* — Altera los paquetes de red cuando estos son enviados.

PREROUTING — Esta cadena altera paquetes recibidos por medio de una interfaz de red cuando llegan.

- *OUTPUT* — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.
- *POSTROUTING* — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.
- Las cadenas internas para la tabla `mangle` son las siguientes:
- *PREROUTING* — Esta cadena altera paquetes recibidos por medio de una interfaz de red antes de que sean dirigidos.
- *POSTROUTING* — Altera los paquetes de red cuando estos son enviados.

Cada paquete de red recibido o enviado desde un sistema Linux está sujeto a al menos una tabla. Sin embargo, un paquete puede estar sometido a múltiples reglas dentro de cada tabla antes de emerger al final de la cadena. La estructura y propósito de estas reglas puede variar, pero normalmente buscan identificar un paquete que viene de o se dirige hacia una direccción IP en particular, o un conjunto de direcciones, cuando utiliza un determinado protocolo y servicio de red.

Nota

Por defecto. las reglas del cortafuegos son guardadas en los archivos `/etc/sysconfig/iptables` o `/etc/sysconfig/ip6tables`.

El servicio `iptables` es iniciado antes que el resto de servicios relacionados con DNS cuando un sistema Linux es iniciado. Esto significa que las reglas del cortafuegos solo pueden ser referenciadas a través de las direcciones IP (por ejemplo 192.168.0.1). Los nombres de dominios (por ejemplo, host.example.com) en dichas reglas producen errores.

Independientemente de su destino, cuando un paquete cumple una regla en particular en una de las tablas, se les aplica un *objetivo (target)* o acción. Si la regla especifica un objetivo ACCEPT para un paquete que coincida, el paquete salta el resto de las verificaciones de la regla y se le permite continuar hacia su destino. Si una regla especifica un objetivo DROP, al paquete se le niega el acceso al sistema y no se envía nada de vuelta al servidor que envió el paquete. Si una regla especifica un objetivo QUEUE, el paquete pasa al espacio del usuario. Si una regla especifica el objetivo opcional REJECT, el paquete es descartado, pero se envía un paquete de error al que envió el paquete.

Cada cadena tiene una política por defecto de ACCEPT, DROP, REJECT, o QUEUE. Si ninguna de estas reglas en la cadena se aplican al paquete, entonces el paquete es tratado de acuerdo a la política por defecto.

El comando `iptables` configura estas tablas, así como también configura nuevas tablas si es necesario.

7.2. Diferencias entre IPTables y IPChains

Tanto `ipchains` como `iptables` usan cadenas de reglas que operan dentro del kernel de Linux para decidir qué hacer con los paquetes que cumplen determinadas reglas. Sin embargo, `iptables` proporciona un método de filtrado de paquetes que puede ser extendido más fácilmente, brindando al administrador un nivel de control mucho más refinado sin tener que aumentar la complejidad del sistema entero.

Tenga en cuenta las siguientes diferencias entre `iptables` y `ipchains`:

Si se utiliza `iptables`, cada paquete filtrado se procesa utilizando reglas de una cadena y no de múltiples cadenas.

Por ejemplo, un paquete FORWARD que llega a un sistema usando `ipchains` tendrá que pasar por las cadenas INPUT, FORWARD, y OUTPUT para llegar a su destino. Sin embargo, `iptables` sólo envía paquetes a la cadena INPUT si su destino es el sistema local y tan sólo los envía a la cadena OUTPUT si el sistema local es quien genera los paquetes. Por esta razón, es importante que coloque la regla designada para capturar un paquete particular dentro de la regla que en verdad maneja el paquete.

El objetivo DENY ha sido cambiado a DROP.

En `ipchains`, los paquetes que coincidan con una regla en una cadena podrían ser dirigidos al objetivo DENY. Este objetivo debe ser cambiado a DROP bajo `iptables`.

El orden de las opciones en una regla es importante.

En `ipchains`, el orden de las opciones de la regla no importa.

El comando `iptables` usa una sintaxis más estricta. En comandos `iptables`, el protocolo (ICMP, TCP o UDP) debe ser especificado antes del puerto fuente o destino.

Las interfaces de red deben ser asociadas con la cadena correcta en las reglas del cortafuegos.

Por ejemplo, las interfaces de entrada (opción `-i`) sólo pueden ser usadas en cadenas INPUT o FORWARD. Asimismo, interfaces de salida (opción `-o`) sólo pueden ser usadas en cadenas FORWARD o OUTPUT.

En otras palabras, las cadenas INPUT y las interfaces de entrada trabajan juntas; las cadenas OUTPUT y las interfaces de salida trabajan juntas. Las cadenas FORWARD trabajan tanto con las interfaces de entrada como con las interfaces de salida.

Las cadenas OUTPUT ya no se utilizan en interfaces de entrada; asimismo los paquetes que van a las interfaces de salida no ven las cadenas INPUT.

Esta no es una lista completa de los cambios. Consulte la Sección 7.7, “Recursos adicionales” para obtener mayor información.

7.3. Opciones de comandos para IPTables

Las reglas para el filtrado de paquetes se crean con el comando `iptables`. Las siguientes características del paquete son con frecuencia utilizadas como criterio:

- *Tipo de paquete* — Dicta qué tipo de paquetes filtra el comando.
- *Fuente/Destino del paquete* — Especifica cuáles paquetes filtra el comando basándose en el origen o destino del paquete.
- *Objetivo* — Indica qué acción es tomada en paquetes que cumplen los criterios mencionados anteriormente.

Consulte la Sección 7.3.4, “Opciones de coincidencia para IPTables” y la Sección 7.3.5, “Opciones del objetivo” para obtener mayor información sobre las opciones específicas que conciernen estos aspectos de un paquete.

Las opciones usadas con las reglas `iptables` dadas deben estar agrupadas lógicamente, basándose en el propósito y en las condiciones de la regla general, para que la regla sea válida. El resto de esta sección explica las opciones más usadas para el comando `iptables`.

7.3.1. Estructura de las opciones del comando para IPTables

Muchos comandos `iptables` tienen la siguiente estructura:

```
iptables [-t <table-name>] <command><chain-name> \ <parameter-1><option-1> \ <parameter-n><option-n>
```

`<table-name>` — Especifica la tabla sobre la cual la tabla es aplicada. Si se omite, se utiliza la tabla `filter`.

`<command>` — Especifica la acción a ejecutar,tal como la adición o borrado de reglas.

`<chain-name>` — Especifica la cadena a editar, crear o borrar.

`<parameter>-<option>` pareja — los parámetros y las opciones asociadas que especifican cómo procesar un paquete que coincide con la regla.

El largo y complejidad de un comando `iptables` puede cambiar significativamente según su propósito.

Por ejemplo, un comando para remover una regla de una cadena puede ser muy corto:

```
iptables -D <chain-name> <line-number>
```

En contraste, un comando que añade una regla que filtra paquetes desde una subnet particular utilizando una variedad de parámetros y opciones específicos puede ser bastante largo. Al construir comandos `iptables`, es importante recordar que algunos parámetros y opciones requieren parámetros y opciones adicionales para construir una regla válida. Esto puede producir una reacción en cadena, si el parámetro adicional requiere más parámetros. Hasta que no se satisfagan todos los parámetros y opciones, la regla no es válida.

Escriba `iptables -h` para ver una lista detallada de la estructura del comando `iptables`.

7.3.2. Opciones de comandos

Las opciones de comandos le dicen a `iptables` que realice una acción específica. Solo se permite una opción de comando por cada comando `iptables`. Excepto el comando de ayuda, todos los comandos se escriben en mayúsculas.

Los comandos de `iptables` son los siguientes:

- `-A` — Añade la regla al final de la cadena especificada. A diferencia de la opción `-I` descrita a continuación, no requiere un entero como argumento. Siempre añade una regla al final de la cadena especificada.
- `-C` — Verifica una regla en particular antes de añadirla en la cadena especificada por el usuario. Este comando puede ser de ayuda para construir reglas `iptables` complejas pidiéndole que introduzca parámetros y opciones adicionales.
- `-D <integer> | <rule>` — Borra una regla de una cadena en particular según su número (`5` para la quinta regla de una cadena). Puede también teclear la regla entera y `iptables` borrará la regla en la cadena que corresponda.
- `-E` — Renombra una cadena definida por el usuario. Una cadena definida por el usuario es cualquier cadena diferente a las cadenas predeterminadas. (Consulte la opción `-N`, para obtener mayor información sobre cómo crear cadenas definidas por el usuario.) Este es un cambio superficial que no afecta la estructura de la tabla.

Nota

Si usted intenta renombrar una de las cadenas predeterminadas, el sistema reportará el error `Match not found` (No se encontró una coincidencia). No se pueden renombrar las cadenas predeterminadas.

- `-F` — Libera la cadena seleccionada, borrando cada una de las reglas de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena.
- `-h` — Proporciona una lista de estructuras de comandos, así como también un resúmen rápido de parámetros de comandos y opciones.
- `-I [<integer>]` — Inserta una regla en una cadena en un punto especificado por un valor entero definido por el usuario. Si no se especifica ningún número, la regla será ubicada en la parte superior de la cadena.

Atención

Como se mencionó anteriormente, el orden de reglas en una cadena determina cuáles reglas se deben aplicar a cuáles paquetes. Esto es importante de recordar cuando se añaden reglas con la opción `-A` o `-I`.

Este factor es importante al añadir reglas utilizando `-I` con un entero. Si usted especifica un número existente al añadir una regla a una cadena, `iptables` añade una nueva regla *antes* (o después) de la regla existente.

- `-L` — Lista todas las reglas de la cadena especificada tras el comando. Para ver una lista de todas las reglas en todas las cadenas en la tabla por defecto `filter`, no especifique ninguna cadena o tabla. De lo contrario, la sintaxis siguiente deberá utilizarse para listar las reglas en una cadena específica en una tabla en particular:

  ```
  iptables -L <chain-name> -t <table-name>
  ```

  En la Sección 7.3.6, “Opciones de listado” se describen opciones adicionales para la opción de comando `-L`, que proporcionan números de reglas y permiten descripciones más detalladas.

- `-N` — Crea una nueva cadena con un nombre especificado por el usuario. El nombre de la cadena debe ser único, de lo contrario un mensaje de error será reportado.

- `-P` — Configura la política por defecto para una cadena en particular, de tal forma que, cuando los paquetes atraviesen la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular, como puedan ser ACCEPT o DROP.

- `-R` — Reemplaza una regla en una cadena particular. El número de la regla debe ser especificado después del nombre de la cadena. La primera regla en una cadena corresponde a la regla número uno.

- `-X` — Borra una cadena especificada por el usuario. No se permite borrar ninguna de las cadenas predefinidas.

- `-Z` — Pone ceros en los contadores de byte y de paquete en todas las cadenas de una tabla en particular.

7.3.3. Opciones de parámetros en IPTables

Una vez que se especifiquen ciertos comandos `iptables`, incluyendo aquellos para añadir, anexar, eliminar, insertar o reemplazar reglas dentro de una cadena, se requieren parámetros para construir una regla de filtrado de paquetes.

- `-c` — Resetea los contadores de una regla en particular. Este parámetro acepta las opciones `PKTS` y `BYTES` para especificar qué contador hay que resetear.

- `-d` — Configura el nombre de la máquina destino, dirección IP o red de un paquete que coincide con la regla. Cuando se coincida una red, se soportan los siguientes formatos de

direcciones IP o máscaras de red:

- *N.N.N.N/M.M.M.M* — Donde *N.N.N.N* es el rango de direcciones IP y *M.M.M.M* es la máscara de la red.
- *N.N.N.N/M* — Donde *N.N.N.N* es el rango de direcciones IP y *M* es la máscara de bit.

- `-f` — Aplica esta regla sólo a los paquetes fragmentados.

  Usando la opción `!` después de este parámetro, únicamente se harán coincidir los paquetes no fragmentados.

Nota

La distinción entre paquetes fragmentados y sin fragmentar es conveniente, sin importar que los paquetes fragmentados son parte del estándar del protocolo IP.

Originalmente diseñado para permitir que los paquetes IP viajen sobre redes con diferentes tamaños de marco, la fragmentación es comúnmente utilizada para generar ataques DoS (negación de servicio) con paquetes mal formados. Es importante tener en cuenta que IPv6 no permite la fragmentación.

- `-i` — Configura la interfaz de red entrante, tal como `eth0` o `ppp0`. Con `iptables`, este parámetro opcional puede ser usado solamente con las cadenas INPUT y FORWARD cuando es usado con la tabla `filter` y la cadena PREROUTING con las tablas `nat` y `mangle`.

  Este parámetro también soporta las siguientes opciones especiales:

  - El carácter de exclamación `!` — Invierte la directriz, es decir, se excluye de esta regla cualquier interfaz especificada.
  - El caráter de suma `+` — Un caracter tipo comodín utilizado para coincidir todas las interfaces con una cadena de caracteres especificada. Por ejemplo, el parámetro `-i eth+` aplicará esta regla a cualquier interfaz Ethernet pero excluirá cualquier otra interfaz, tal como, `ppp0`.

  Si el parámetro `-i` se utiliza sin especificar ninguna interfaz, todas las interfaces estarán afectadas por la regla.

- `-j` — Salta al objetivo especificado cuando un paquete coincide con una regla particular.

  Los objetivos estándar son `ACCEPT`, `DROP`, `QUEUE` y `RETURN`.

  Las opciones extendidas también están disponibles a través de los módulos cargados por defecto con el RPM de `iptables` en Red Hat Enterprise Linux. Entre los objetivos válidos de estos módulos están `LOG`, `MARK` y `REJECT`, entre otros. Consulte la página man de `iptables` para más información sobre esto y otros objetivos.

Esta opción puede ser usada para dirigir un paquete que coincide con una regla particular a una cadena definida por el usuario que se encuentra fuera de la cadena actual. De esta forma, otras reglas pueden ser aplicadas al paquete.

Si no especifica ningún objetivo, el paquete pasa la regla sin llevar a cabo ninguna acción. A pesar de todo, el contador para esta regla se sigue incrementando en uno.

- `-o` — Configura la interfaz de red de salida para una regla. Esta opción es válida únicamente con las cadenas OUTPUT y FORWARD en la tabla de `filter` y la cadena POSTROUTING en las tablas `nat` y `mangle`. Estos parámetros aceptan las mismas opciones que aquellos de la interfaz de entrada (`-i`).

- `-p` — Configura el protocolo IP afectado por la regla. Puede ser `icmp`, `tcp`, `udp`, o `all`; puede ser un valor numérico que representa uno de estos protocolos o uno diferente. Puede usar cualquier protocolo listado en `/etc/protocols`.

  El protocolo "`all`" significa que la regla es aplicable a todos los protocolos conocidos. Si no hay protocolos listados con esta regla, el valor predeterminado es "`all`".

- `-s` — Configura la fuente para un paquete particular usando la misma sintaxis que el parámetro (`-d`).

7.3.4. Opciones de coincidencia para IPTables

Diferentes protocolos de red proporcionan opciones especializadas de coincidencia que pueden ser configuradas para coincidir con un paquete particular usando ese protocolo. Sin embargo, primero se debe especificar el protocolo con el comando `iptables`. Por ejemplo, `-p <protocolo>` activa las opciones para el protocolo especificado. Tenga en cuenta que usted puede utilizar el ID del protocolo en vez del nombre. Revise los siguientes ejemplos, cada uno de éstos tiene el mismo efecto:

```
iptables -A INPUT -p icmp --icmp-type any -j ACCEPT  iptables -A INPUT -p 5813 --icmp-type any -j ACCEPT
```

La definición de servicios se proporciona en el archivo `/etc/services`. Para facilitar la lectura, se recomienda utilizar el nombre del servicio y no el número de puerto.

Importante

Asegure el archivo `/etc/services` para evitar que sea editado sin autorización. Si este archivo puede ser editado, crackers pueden utilizarlo para abrir puertos en su máquina que usted ha cerrado. Para asegurar este archivo, escriba el comando siguiente como root:

```
[root@myServer ~]# chown root.root /etc/services [root@myServer ~]# chmod 0644
```

Esto previene que el archivo sea renombrado, borrado o que se creen enlaces a éste.

7.3.4.1. Protocolo TCP

Estas opciones de identificación están disponibles en el protocolo TCP (opción `-p tcp`):

- `--dport` — Establece el puerto de destino para el paquete.

  Para configurar esta opción utilice el nombre del servicio (tal como www o smtp), un número de puerto o un rango de números de puertos.

  Para especificar un rango de números de puertos, separe los dos números con dos puntos (`:`), tal como `-p tcp --dport 3000:3200`. El rango más grande aceptable es `0:65535`.

  Use un carácter de exclamación (`!`) después de la opción `--dport` para que los paquetes que *no utilizan* el servicio de red o puerto coincidan.

  Para ver los nombres y aliases de los servicios de red y números de puertos que utilizan, revise el archivo `/etc/services`.

  La opción de coincidencia `--destination-port` es igual a `--dport`.

- `--sport` — Configura el puerto fuente del paquete usando las mismas opciones que `--dport`. La opción `--source-port` es sinónimo con `--sport`.

- `--syn` — Se aplica a todos los paquetes TCP designados a iniciar la comunicación, comúnmente llamados *paquetes SYN*. Cualquier paquete que esté llevando un payload de datos no será tocado.

  Utilice el carácter de exclamación (`!`) después de `--syn` para coincidir los paquetes que nos sean SYN.

- `--tcp-flags <tested flag list> <set flag list>` Permite a los paquetes TCP con bits o banderas específicas, ser coincididos con una regla.

  La opción `--tcp-flags` acepta dos parámetros. El primer parámetro es la máscara, una lista de banderas a ser examinadas en el paquete. El segundo parámetro es una lista de banderas separadas por comas que se deben establecer para que la regla coincida.

  Las banderas posibles son:

  - `ACK`
  - `FIN`
  - `PSH`
  - `RST`
  - `SYN`
  - `URG`
  - `ALL`
  - `NONE`

Por ejemplo, una regla `iptables` que contenga la siguiente especificación solo coincidirá con paquetes TCP que tengan la bandera SYN activa y las banderas ACK y FIN sin activar.

```
--tcp-flags ACK,FIN,SYN SYN
```

Usando el caracter de exclamación (`!`) después de `--tcp-flags` reversa el efecto de la opción de coincidencia.

- `--tcp-option` — Intenta seleccionar con opciones específicas de TCP que pueden estar activas en un paquete en particular. Esta opción se puede revertir con el punto de exclamación (`!`).

7.3.4.2. Protocolo UDP

Estas opciones de selección están disponibles para el protocolo UDP (`-p udp`):

- `--dport` — Especifica el puerto destino del paquete UDP, usando el nombre del servicio, número de puerto, o rango de números de puertos. La opción de coincidencia `--destination-port` es sinónimo con `--dport`.
- `--sport` — Configura el puerto fuente del paquete UDP, usando el nombre de puerto, número de puerto o rango de números de puertos. La opción `--source-port` es sinónimo con `--sport`.

Para especificar un rango de números de puertos para las opciones `--dport` y `--sport`, separe los dos números con dos puntos (:). Por ejemplo, `-p tcp --dport 3000:3200`. El rango más grande aceptable es 0:65535.

7.3.4.3. Protocolo ICMP

Las siguientes opciones de coincidencia están disponibles para el Protocolo de mensajes de Internet (ICMP) (`-p icmp`):

- `--icmp-type` — Selecciona el nombre o el número del tipo ICMP que concuerde con la regla. Se puede obtener una lista de nombres válidos ICMP escribiendo el comando `iptables -p icmp -h`.

7.3.4.4. Módulos con opciones de coincidencias adicionales

Opciones adicionales de coincidencia están disponibles a través de los módulos cargados por el comando `iptables`.

Para usar un módulo de opciones de coincidencia, cargue el módulo por nombre usando `-m <nombre-modulo>` (reemplazando `<nombre-modulo>` con el nombre del módulo).

Un gran número de módulos están disponibles por defecto. Es posible crear sus módulos para proporcionar funcionalidades adicionales.

Lo siguiente, es una lista parcial de los módulos usados más comúnmente:

- módulo `limit` — Permite colocar un límite en cuántos paquetes son coincididos a una regla

particular.

Cuando se usa en conjunto con el objetivo `LOG`, el módulo `limit` puede prevenir que una inundación de paquetes coincidentes sobrecarguen el registro del sistema con mensajes repetitivos o usen los recursos del sistema.

Consulte la Sección 7.3.5, “Opciones del objetivo” para obtener mayor información sobre los objetivos `LOG`.

El módulo `limit` habilita las opciones siguientes:

- `--limit` — Configura el número de coincidencias en un intervalo de tiempo, especificado con un número y un modificador de tiempo ordenados en el formato *<número>/<tiempo>*. Por ejemplo, si usamos `--limit 5/hour` sólo dejaremos que una regla sea efectiva cinco veces por hora.

  Se pueden especificar los periodos en segundos, minutos, horas o días.

  Si no se utiliza ningún número ni modificador de tiempo, se asume el siguiente valor por defecto: `3/hour`.

- `--limit-burst` — Configura un límite en el número de paquetes capaces de cumplir una regla en un determinado tiempo.

  Esta opción deberá ser usada junto con la opción `--limit`, y acepta un número entero.

  Si no se utiliza ningún valor, se asume el valor por defecto (5).

- módulo `state` — Habilita la coincidencia de estado.

  El módulo `state` tiene las siguientes opciones:

  - `--state` — coincide un paquete con los siguientes estados de conexión:

    - `ESTABLISHED` — El paquete coincidente se asocia con otros paquetes en una conexión establecida. Usted necesita aceptar este estado si desea mantener una conexión entre un cliente y un servidor.

    - `INVALID` El paquete seleccionado no puede ser asociado a una conexión conocida.

    - `NEW` — El paquete coincidente o bien está creando una nueva conexión o bien forma parte de una conexión de dos caminos que antes no había sido vista. Usted necesita aceptar este estado si desea permitir nuevas conexiones a un servicio.

    - `RELATED` — El paquete coincidente está iniciando una nueva conexión relacionada de alguna manera a una conexión existente.Un ejemplo es FTP, el cual utiliza una conexión para control de tráfico (puerto 21) y una conexión separada para transferencia de datos (puerto 20).

    Estos estados de conexión se pueden utilizar en combinación con otros separándolos mediante comas como en `-m state --state INVALID, NEW`.

- módulo `mac` — Habilita la coincidencia de direcciones MAC de hardware.

  El módulo `mac` activa las opciones siguientes:

  - `--mac-source` — Coincide una dirección MAC a la tarjeta de red que envió el paquete. Para excluir una dirección MAC de la regla, coloque un símbolo de exclamación (`!`) después de la opción `--mac-source`.

Consulte la página man de `iptables` para obtener más opciones disponibles a través de los módulos.

7.3.5. Opciones del objetivo

Una vez que un paquete ha coincidido con una regla, la regla puede dirigir el paquete a un número de objetivos diferentes que determinan la acción apropiada. Cada cadena tiene un objetivo por defecto, el cual es usado si ninguna de las reglas en esa cadena coinciden con un paquete o si ninguna de las reglas que coinciden con el paquete especifica un objetivo.

Los siguientes son los objetivos estándar:

- *`<user-defined-chain>`* — Una cadena definida por el usuario dentro de una tabla. Los nombres de cadenas definidas por el usuario deben ser únicos. Este objetivo pasa el paquete a la cadena especificada.
- `ACCEPT` — Permite que el paquete se mueva hacia su destino o hacia otra cadena.
- `DROP` — Deja caer el paquete sin responder al solicitante. El sistema que envia el paquete no es notificado de esta falla.
- `QUEUE` — El paquete se pone en una cola para ser manejado por una aplicación en el espacio de usuario.
- `RETURN` — Detiene la verificación del paquete contra las reglas de la cadena actual. Si el paquete con un destino `RETURN` cumple una regla de una cadena llamada desde otra cadena, el paquete es devuelto a la primera cadena para retomar la verificación de la regla allí donde se dejó. Si la regla `RETURN` se utiliza en una cadena predefinida y el paquete no puede moverse hacia la cadena anterior, el objetivo por defecto de la cadena actual es utilizado.

Además, hay otras extensiones que permiten especificar otros objetivos. Estas extensiones son llamadas módulos de objetivos o módulos de opciones de coincidencia. La mayoría sólo se aplican a tablas y situaciones especificas. Consulte la Sección 7.3.4.4, “Módulos con opciones de coincidencias adicionales” para obtener mayor información sobre los módulos de opciones de coincidencia.

Existen varios módulos extendidos de objetivos, la mayoría de los cuales tan sólo se aplican a tablas o situaciones específicas. Algunos de los módulos de objetivos más comunes incluidos en Red Hat Enterprise Linux son:

- `LOG` — Registra todos los paquetes que coinciden con esta regla. Puesto que los paquetes son registrados por el kernel, el archivo `/etc/syslog.conf` determina dónde estas entradas de registro serán escritas. Por defecto, son colocadas en el archivo `/var/log/messages`.

Se pueden usar varias opciones adicionales tras el objetivo `LOG` para especificar la manera en la que tendrá lugar el registro:

- `--log-level` — Configura el nivel de prioridad del registro de eventos. Una lista de los niveles de prioridad se puede encontrar en la página man de `syslog.conf`.
- `--log-ip-options` — Registra cualquier opción en la cabecera de un paquete IP.
- `--log-prefix` — Coloca una cadena de hasta 29 caracteres antes de la línea de registro cuando es escrita. Esto es muy útil para la escritura de filtros de syslog para usarlos en conjunto con el registro de paquetes.

Nota

Debido a un problema con esta opción, se debe añadir un espacio al valor *`log-prefix`*.

- `--log-tcp-options` — Cualquier opción colocada en la cabecera de un paquete TCP es registrada.
- `--log-tcp-sequence` Escribe el número de secuencia TCP del paquete en el registro del sistema.

- `REJECT` — Envia un paquete de error de vuelta al sistema remoto y deja caer el paquete.

  El objetivo `REJECT` acepta `--reject-with <tipo>` (donde `<tipo>` es el tipo de rechazo) el cual permite devolver información más detallada con el paquete de error. El mensaje `port-unreachable` es el tipo de error por defecto dado si no se usa otra opción. Para una lista completa de las opciones `<tipo>`, consulte la página man de `iptables`.

Otras extensiones de objetivos, incluyendo muchas que son útiles para el enmascaramiento de IP usando la tabla `nat` o con alteración de paquetes usando la tabla `mangle`, se puede encontrar en la página man de `iptables`.

7.3.6. Opciones de listado

El comando predeterminado para listar, `iptables -L [<nombre-cadena>]`, proporciona una vista muy básica de los filtros por defecto de las cadenas actuales de la tabla. Las opciones adicionales proporcionan más información:

- `-v` — Muestra la salida por pantalla con detalles, como el número de paquetes y bytes que cada cadena ha procesado, el número de paquetes y bytes que cada regla ha coincidido y qué interfaces se aplican a una regla en particular.
- `-x` — Expande los números en sus valores exactos. En un sistema ocupado, el número de paquetes y bytes vistos por una cadena en concreto o por una regla puede estar abreviado en `Kilobytes`, `Megabytes` o `Gigabytes`. Esta opción fuerza a que se muestre el número completo.

- `-n` Muestra las direcciones IP y los números de puertos en formato numérico, en lugar de utilizar el nombre del servidor y la red tal y como se hace por defecto.
- `--line-numbers` — Proporciona una lista de cada cadena junto con su orden numérico en la cadena. Esta opción puede ser útil cuando esté intentando borrar una regla específica en una cadena o localizar dónde insertar una regla en una cadena.
- `-t <nombre-tabla>` — Especifica un nombre de tabla. Si se omite, el valor predeterminado es la tabla de filtro (filter)

Los siguientes ejemplos ilustran el uso de varias de esas opciones. Note la diferencia en los byte mostrados al incluir la opción `-x`.

```
[root@myserver ~]# iptables -L OUTPUT -v -n -x Chain OUTPUT (policy ACCEPT 64005 packets, 6445791 bytes) p
```

7.4. Guardando reglas IPTables

Las reglas creadas con el comando `iptables` son almacenadas en memoria. Si el sistema es reiniciado antes de guardar el conjunto de reglas `iptables`, se perderán todas las reglas. Para que las reglas de filtrado de red persistan luego de un reinicio del sistema, éstas necesitan ser guardadas. Para hacerlo, escriba el siguiente comando como root:

```
/sbin/service iptables save
```

Esto ejecuta el script de inicio `iptables`, el cual ejecuta el programa `/sbin/iptables-save` y escribe la configuración actual de `iptables` a `/etc/sysconfig/iptables`. El archivo `/etc/sysconfig/iptables` existente es guardado como `/etc/sysconfig/iptables.save`.

La próxima vez que se inicie el sistema, el script de inicio de `iptables` volverá a aplicar las reglas guardadas en `/etc/sysconfig/iptables` usando el comando `/sbin/iptables-restore`.

Aún cuando siempre es una buena idea probar una regla de `iptables` antes de confirmar los cambios al archivo `/etc/sysconfig/iptables`, es posible copiar reglas `iptables` en este archivo desde otra versión del sistema de este archivo. Esto proporciona una forma rápida de distribuir conjuntos de reglas `iptables` a muchas máquinas.

Es posible guardar las reglas iptables en un archivo separado para ser distribuido, como copia de seguridad o bajo algún otro propósito. Para guardar sus reglas iptables, escriba el siguiente comando como root:

```
 [root@myserver ~]# iptables-save > <archivo>
en donde <archivo> es un nombre definido por el usuario para ese juego de reglas.
```

Importante

Si se está distribuyendo el archivo `/etc/sysconfig/iptables` a otras máquinas, escriba `/sbin/service iptables restart` para que las nuevas reglas surtan efecto.

Nota

Note la diferencia entre el *comando* `iptables` (`/sbin/iptables`), el cual es utilizado para manipular las tablas y las cadenas que constituyen la funcionalidad de `iptables`, y el *servicio* `iptables` (`/sbin/iptables service`), utilizado para activar o desactivar el servicio `iptables`.

7.5. Scripts de control de IPTables

Hay dos métodos básicos para controlar `iptables` en Red Hat Enterprise Linux:

- `/sbin/service iptables <opción>` — Utilizado para manipular varias funciones de `iptables` a través de su script de inicio. Dispone de las siguientes opciones:

  - `start` — Si se tiene un cortafuegos configurado (es decir, si `/etc/sysconfig/iptables` existe), todos los `iptables` en ejecución son detenidos completamente y luego arrancados usando el comando `/sbin/iptables-restore`. Esta opción solo funcionará si no se carga el módulo del kernel `ipchains`. Para revisar si este módulo está cargado, ejecute como root el siguiente comando:

    ```
    [root@MyServer ~]# lsmod | grep ipchains
    ```

    Si este comando no retorna ninguna salida, significa que el módulo no está cargado. De ser necesario, utilice `/sbin/rmmod` para remover el módulo.

  - `stop` — Si el cortafuegos está en ejecución, se descartan las reglas del cortafuegos que se encuentran en memoria y todos los módulos iptables y ayudantes son descargados.

    Si se cambia la directiva `IPTABLES_SAVE_ON_STOP` dentro del archivo de configuración `/etc/sysconfig/iptables-config` de su valor por defecto a `yes`, se guardan las reglas actuales a `/etc/sysconfig/iptables` y cualquier regla existente se moverá al archivo `/etc/sysconfig/iptables.save`.

    Para mayor información sobre el archivo de configuración `iptables-config`, consulte la Sección 7.5.1, “Archivo de configuración de scripts de control de IPTables”.

  - `restart` — Si el cortafuegos está en ejecución, las reglas del mismo que se encuentran en memoria se descartan y se vuelva a iniciar el cortafuegos si está configurado en `/etc/sysconfig/iptables`. La directriz `restart` sólo funcionará si no está cargado el módulo del kernel `ipchains`.

    Si la directiva `IPTABLES_SAVE_ON_RESTART` dentro del archivo de configuración `/etc/sysconfig/iptables-config` se cambia de su valor por defecto a `yes`, las reglas actuales son guardadas a `/etc/sysconfig/iptables` y cualquier regla existente se moverán al archivo `/etc/sysconfig/iptables.save`.

    Para mayor información sobre el archivo de configuración `iptables-config`, consulte la Sección 7.5.1, “Archivo de configuración de scripts de control de IPTables”.

- `status` — Muestra el estado del cortafuegos y lista todas las reglas activas.

  La configuración por defecto para esta opción muestra las direcciones IP en cada regla. Para mostrar el nombre de dominio y el nombre de host, edite el archivo `/etc/sysconfig/iptables-config` y cambie el valor de `IPTABLES_STATUS_NUMERIC` a `no`. Consulte la Sección 7.5.1, “Archivo de configuración de scripts de control de IPTables” para más información sobre el archivo `iptables-config`.

- `panic` — Descarta todas las reglas del cortafuegos. La política de todas las tablas configuradas es establecida a `DROP`.

  Esta opción puede ser útil si se sabe que un servidor está comprometido. En vez de desconectar físicamente el servidor de la red o apagar el sistema, usted puede utilizar esta opción para detener el tráfico pero dejando la máquina en un estado que puede ser utilizado para análisis.

- `save` — Guarda las reglas del cortafuegos a `/etc/sysconfig/iptables` usando `iptables-save`. Para más información, consulte la Sección 7.4, “Guardando reglas IPTables”.

Sugerencia

Para utilizar los mismos comandos initscript para controlar el filtrado de la red para IPv6, sustituya `ip6tables` por `iptables` en los comandos `/sbin/service` listados en esta sección. Para más información sobre IPv6 y el filtrado de red (netfilter), consulte la Sección 7.6, “IPTables y IPv6”.

7.5.1. Archivo de configuración de scripts de control de IPTables

El comportamiento de los scripts de inicio de `iptables` es controlado por el archivo de configuración `/etc/sysconfig/iptables-config`. A continuación se presenta una lista de las directivas contenidas dentro de este archivo:

- `IPTABLES_MODULES` — Especifica una lista separada por espacios de módulos `iptables` adicionales a cargar cuando se activa un cortafuegos. Esto puede incluir seguimiento de conexiones y ayudantes NAT.

- `IPTABLES_MODULES_UNLOAD` — Descarga los módulos al iniciar o al detenerse. Esta directiva acepta los valores siguientes:

  - `yes` — El valor por defecto. Esta regla debe establecerse para alcanzar un estado correcto para reiniciar o detener un cortafuegos.

  - `no` — Esta opción solamente debería ser configurada si hay problemas al descargar los módulos de filtrado de paquetes de red.

- `IPTABLES_SAVE_ON_STOP` — Guarda las reglas del cortafuegos actuales a `/etc/sysconfig/iptables` cuando se detiene el cortafuegos. Esta directiva acepta los valores

siguientes:

- `yes` — Guarda las reglas existentes a `/etc/sysconfig/iptables` cuando se detiene el cortafuegos, moviendo la versión anterior al archivo `/etc/sysconfig/iptables.save`.
- `no` — El valor por defecto. No guarda las reglas existentes cuando se detiene el cortafuegos.

- `IPTABLES_SAVE_ON_RESTART` — Guarda las reglas actuales del cortafuegos cuando este se reinicia. Esta directiva acepta los valores siguientes:
  - `yes` — Guarda las reglas existentes a `/etc/sysconfig/iptables` cuando se reinicia el cortafuegos, moviendo la versión anterior al archivo `/etc/sysconfig/iptables.save`.
  - `no` — El valor por defecto. No guarda las reglas existentes cuando se reinicia el cortafuegos.
- `IPTABLES_SAVE_COUNTER` — Guarda y restaura todos los paquetes y contadores de bytes en todas las cadenas y reglas. Esta directiva acepta los valores siguientes:
  - `yes` — Guarda los valores del contador.
  - `no` — El valor por defecto. No guarda los valores del contador.
- `IPTABLES_STATUS_NUMERIC` — Muestra direcciones IP en una salida de estado en vez de dominios y nombres de host. Esta directiva acepta los valores siguientes:
  - `yes` — El valor por defecto. Solamente devuelve direcciones IP dentro de una salida de estado.
  - `no` — Devuelve dominios o nombres de host en la salida de estado.

7.6. IPTables y IPv6

Si el paquete `iptables-ipv6` es instalado, netfilter en Red Hat Enterprise Linux puede filtrar el protocolo de Internet IPv6. El comando utilizado para manipular los filtros de red IPv6 es `ip6tables`.

La mayoría de las directivas para este comando son idéntica a aquellas usadas por `iptables`, excepto que la tabla `nat` aún no es compatible. Esto significa que todavía no es posible realizar tareas de traducción de direcciones de red IPv6, tales como enmascarado y reenvío de puertos.

Las reglas guardadas para `ip6tables` son almacenadas en el archivo `/etc/sysconfig/ip6tables`. Las reglas viejas guardadas por los scripts de inicio de `ip6tables` son guardadas en el archivo `/etc/sysconfig/ip6tables.save`.

Las opciones de configuración para los script de inicio de `ip6tables` es `/etc/sysconfig/ip6tables-config` y los nombres para cada directriz varían ligeramente de sus contrapartes en `iptables`.

Por ejemplo, la directriz `IPTABLES_MODULES` en `iptables-config` es la equivalente a `IP6TABLES_MODULES` en el archivo `ip6tables-config`.

7.7. Recursos adicionales

Consulte las fuentes siguientes para obtener información adicional sobre filtrado de paquetes con `iptables`.

7.7.1. Documentación instalada

- `man iptables` — Contiene una descripción de `iptables` así como también una lista detallada de objetivos, opciones y extensiones de coincidencia.

7.7.2. Sitios web útiles

- http://www.netfilter.org/ — El sitio principal del proyecto de netfilter/iptables. Contiene información varia sobre `iptables`, incluyendo una sección FAQ detallando problemas específicos y varias guías de ayuda escritas por Rusty Russell, el mantenedor del cortafuegos IP de Linux. Los documentos HOWTO del sitio cubren aspectos tales como conceptos básicos de redes, filtrado de paquetes del kernel y configuraciones NAT.
- http://www.linuxnewbie.org/nhf/Security/IPtables_Basics.html — una visión básica y general sobre la forma cómo los paquetes se mueven dentro del kernel de Linux, además de una introducción sobre cómo se construyen comandos `iptables` simples.

Capítulo 22. Referencias

Las siguientes referencias apuntan a información adicional que es relevante a SELinux y Red Hat Enterprise Linux pero que va más allá del propósito de este manual. Tenga en cuenta que debido al rápido desarrollo de SELinux, este material podría ser aplicable únicamente a un lanzamiento específico de Red Hat Enterprise Linux.

Libros

SELinux by Example
Mayer, MacMillan, and Caplan

Prentice Hall, 2007

Tutoriales y ayuda

Understanding and Customizing the Apache HTTP SELinux Policy
http://fedora.redhat.com/docs/selinux-apache-fc3/

Tutorials and talks from Russell Coker
http://www.coker.com.au/selinux/talks/ibmtu-2004/

Generic Writing SELinux policy HOWTO
https://sourceforge.net/docman/display_doc.php?docid=21959[amp]group_id=21266
[https://sourceforge.net/docman/display_doc.php?docid=21959[amp]group_id=21266]

Red Hat Knowledgebase
http://kbase.redhat.com/

Información general

Sitio web principal de NSA SELinux
http://www.nsa.gov/selinux/

NSA SELinux, Preguntas frecuentes
http://www.nsa.gov/selinux/info/faq.cfm

Fedora SELinux, Preguntas frecuentes
http://fedora.redhat.com/docs/selinux-faq-fc3/

SELinux NSA's Open Source Security Enhanced Linux
http://www.oreilly.com/catalog/selinux/

Tecnologías

An Overview of Object Classes and Permissions

http://www.tresys.com/selinux/obj_perms_help.html

Integrating Flexible Support for Security Policies into the Linux Operating System (una historia de la implementación de Flask en Linux, artículo en inglés)
http://www.nsa.gov/selinux/papers/slinux-abs.cfm

Implementing SELinux as a Linux Security Module
http://www.nsa.gov/selinux/papers/module-abs.cfm

A Security Policy Configuration for the Security-Enhanced Linux
http://www.nsa.gov/selinux/papers/policy-abs.cfm

Comunidad

Página de la comunidad SELinux
http://selinux.sourceforge.net

IRC
irc.freenode.net, #rhel-selinux

Historia

Quick history of Flask
http://www.cs.utah.edu/flux/fluke/html/flask.html

Full background on Fluke
http://www.cs.utah.edu/flux/fluke/html/index.html